ECRYPT CSA

H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

D5.4
Algorithms, Key Size and Protocols Report (2018)

Due date of deliverable: 28 February 2018
Actual submission date: 28 February 2018

Start date of project: 1 March 2015 Duration: 3 years

Lead contractor: University of Bristol (UNIVBRIS) Revision 1.0

Change log

Version	Contents
1.0	Comments given by several people on D5.2 have been integrated.

Project co-funded by the European Commission within the H2020 Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Algorithms, Key Size and Protocols Report (2018)

Editor
Nigel P. Smart (UNIV BRIS)

Contributors
Michel Abdalla, Tor Erling Bjørstad, Carlos Cid,
Benedikt Gierlichs, Andreas Hülsing, Atul Luykx,
Kenneth G. Paterson, Bart Preneel, Ahmad-Reza Sadeghi,
Terence Spies, Martijn Stam, Michael Ward,
Bogdan Warinschi, Gaven Watson.

28 February 2018

Revision 1.0

The work described in this report has in part been supported by the Commission of the European Communities through the H2020-ICT program under contract H2020-ICT-2014 no. 645421. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Contents

Acronyms

3DES	Triple DES
3GPP	3rd Generation Partnership Project (mobile phone system)
A5/X	Stream ciphers used in mobile phone protocols
ABE	Attribute Based Encryption
AE	Authenticated Encryption
AEAD	Authenticated Encryption with Auxillary Data
AES	Advanced Encryption Standard
AESKW	A Key Wrap Scheme
AH	Authentication Header
AKA	Authentication and Key Agreement
AKW1	A Key Wrap Scheme
AKW2	A Key Wrap Scheme
AMAC	ANSI Retail MAC
ANSI	American National Standards Institute
BB	Boneh–Boyen (ID based encryption)
BF	Boneh–Franklin (ID based encryption)
BPP	Binary Packet Protocol
BPR	Bellare, Pointcheval and Rogaway
BMP	Boyko, MacKenzie and Patel
CBC	Cipher Block Chaining (mode)
CCA	Chosen Ciphertext Attack
CCM	Counter with CBC-MAC (mode)
CFB	Cipher Feedback
CMA	Chosen Message Attack
CMAC	Cipher-based MAC
CPA	Chosen Plaintext Attack
CTR	Counter (mode)
CVA	Ciphertext Validity Attack
CWC	Carter–Wegman + Counter

DAA	Direct Anonymous Attestation
DEA	Data Encryption Algorithm
DEM	Data Encapsulation Mechanism
DES	Data Encryption Standard
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
E0	A stream cipher used in Bluetooth
EAX	Actually stands for nothing (mode)
EC2	Elastic Computing Cloud
ECB	Electronic Code Book (mode)
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECIES	Elliptic Curve Integrated Encryption Scheme
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EKE	Encrypted Key Exchange
EMAC	Encrypted CBC-MAC
EME	ECB-mask-ECB (mode)
EMV	Europay–Mastercard–Visa (chip-and-pin system)
ENISA	European Union Agency for Network and Information Security
ESP	Encapsulating Security Payload
FDH	Full Domain Hash
FHE	Fully Homomorphic Encryption
GCM	Galois Counter Mode
GDSA	German Digital Signature Algorithm
GMAC	The MAC part of the GCM block cipher mode
GSM	Groupe Spécial Mobile (mobile phone system)
HMAC	A hash based MAC algorithm

IAPM	Integrity Aware Parallelizable Mode
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IND	Indistinguishability of Encryptions
INT-CTXT	Integrity of Ciphertexts
IPsec	Internet Protocol Security
ISO	International Standards Organization
IV	Initialisation Vector (or Value)
J-PAKE	Password Authenticated Key Exchange by Juggling
KDSA	Korean Digital Signature Algorithm
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
KW	AES Key Wrap
KWP	AES Key Wrap with Padding
LAMP	Linux, Apache, MySQL, PHP
LTE	Long Term Evolution (mobile phone system)
LWE	Learning With Errors
MAC	Message Authentication Code
MOV	Menezes–Okamoto–Vanstone (attack)
MPC	Multi Party Computation
MQV	Menezes–Qu–Vanstone (protocol)
MS	Mobile Station (i.e. a phone in UMTS/LTE)
NIST	National Institute of Standards and Technology (US)
NMAC	Nested MAC
NTRU	A Post Quantum Encryption Algorithm

OAEP Optimal Asymmetric Encryption Padding
OCB Offset Code Book (mode)
OFB Output Feedback (mode)
OPE Order Preserving Encryption
ORAM Oblivious Random Access Memory
PACE Password Authenticated Connection Establishment
PAK Password Authenticated Key (PAK) Exchange
PAKE Password Authenticated Key Exchange
PEKS Public Key Encryption Keyword Search
PKCS Public Key Cryptography Standards
PKE Public Key Encryption
POR Proofs Of Retrievability
PRF Pseudo Random Function
PRNG Pseudo Random Number Generator
PRP Pseudo Random Permutation
PSEC Provable Secure Elliptic Curve (encryption)
PSS Probabilistic Signature Scheme
PV Pointcheval–Vaudenay (signatures)
RC4 Ron's Cipher Four (a stream cipher)
RDSA Russian Digital Signature Algorithm
RFC Request For Comments
RA Reset Attack
RAM Random Access Memory
ROM Random Oracle Model
RSA Rivest–Shamir–Adleman

SA	Security Association
SHA	Secure Hash Algorithm
SIMD	Single Instruction Multiple Data
SIV	Synthetic Initialization Vector
SK	Sakai–Kasahara (ID-based encryption)
SN	Serving Network (i.e. a provider in UMTS/LTE)
SPAKE	Single-Party Public-Key Authenticated Key Exchange
SPD	Security Policy Database
SQL	Structured Query Language
SSE	Symmetric Searchable Encryption
SSH	Secure Shell
SSL	Secure Sockets Layer
TKW	Triple-DEA Key Wrap
TDKW	A Key Wrap Scheme
TRNG	True Random Number Generator
UEA	UMTS Encryption Algorithm
UF	Universally Unforgeable
UIA	UMTS Integrity Algorithm
UMAC	Universal hashing based MAC
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XTS	XEX Tweakable Block Cipher with Ciphertext Stealing

Part I

General Discussion

Chapter 1

Executive Summary

This final report on Algorithms and Key Sizes builds on the previous report. In compiling this update, which details minor changes in our recommendations from previous years, we solicited feedback from the world wide cryptologic community via means of a Slack based discussion board. This was supplemented with email discussion and the solicitation of specific input directly from acknowledged experts.

This report on cryptographic algorithms, schemes, keysizes and protocols is a direct descendent of the reports produced by the ECRYPT-I and -II projects in the period 2004 to 2012, [184–191] and the ENISA reports produced in the period 2013-2014 [194–196]. As in the previous reports we provide rather conservative guiding principles, based on current state-of-the-art research, addressing construction of new systems with a long life cycle. This report is aimed to be a reference in the area, focusing on commercial online services that collect, store and process the data.

It should be noted that this is a technical document addressed to decision makers, in particular specialists designing and implementing cryptographic solutions, within commercial organisations. In this document we focus on just two decisions which we feel are more crucial to users of cryptography.

Firstly, whether a given primitive or scheme can be considered for continued use today if it is already deployed. We refer to such use as *legacy* use within our document. Our first guiding principle is that if a scheme is not considered suitable for legacy use, or is only considered for such use with certain caveats, then this should be taken as a strong advice that the primitive or scheme should be replaced as a matter of urgency.

Secondly, we consider the issue of whether a primitive or scheme is suitable for deployment in new or future systems. In some sense mechanisms which we consider usable for new and future systems meet cryptographic requirements described in this document; they generally will have proofs of security, will have key sizes equivalent to 128-bit symmetric security or more[1], will have no structural weaknesses, will have been well studied, will have been standardized, and will have a reasonably-sized existing user base. Thus the second guiding principle is that decision makers now make plans and preparations for the phasing out of what we term legacy mechanisms over a period of say 5-10 years, and replacing them with systems we deem secure for future use.

This document does not consider any mechanisms which are currently only of academic interest. In particular all the mechanisms we discuss have been standardized to some extent,

[1] See Section 4.6 for the equivalence mapping between symmetric key sizes and public key sizes

and have either been deployed, or are slated to be deployed, in real systems. This selection is a means of focusing the document on mechanisms which will be of interest to decision makers in industry and government.

Further limitations of scope are mentioned in the introductory chapter which follows. Further restrictions are mentioned in Chapter 2 “How to Read this Document”.

Chapter 2

How to Read this Document

This document collates a series of proposals for algorithm and keysizes. In some sense the current document supersedes the ECRYPT and ECRYPT2 "Yearly Report on Algorithms and Key Lengths" published between 2004 and 2012 [184–191] and the three associated ENISA reports [194–196]. However, it should be considered as completely distinct. The current document tries to provide a focused set of proposals in an easy to use form. The prior ECRYPT documents provided more general background information and discussions on general concepts with respect to key size choice, and tried to predict the future ability of cryptanalytic attacks via hardware and software.

In this document we focus on just two decisions which we feel are more crucial to users of cryptography. Firstly, whether a given primitive, scheme, protocol or keysize can be considered for continued use today if it is already deployed. We refer to such use as *legacy* use within our document. If a scheme is *not* considered suitable for legacy use, or is only considered for such use with certain caveats, then this should be taken as *strong advice* that the primitive, scheme or protocol be possibly *replaced* as a matter of urgency (or even that an attack exists). A system which we deem not secure for legacy use may still actually be secure if used within a specific environment, e.g. limited key life times, mitigating controls, or (in the case of hash functions) relying on properties other than collision resistance. However, in such instances we recommend the user to consult expert advice to see whether such specific details are indeed relevant.

Table 2.1: Summary of distinction between legacy and future use

Classification	Meaning
Legacy ✗	Attack exists or security considered not sufficient. Mechanism should be replaced in fielded products as a matter of urgency.
Legacy ✓	No known weaknesses at present. Better alternatives exist. Lack of security proof or limited key size.
Future ✓	Mechanism is well studied (often with security proof). Expected to remain secure in 10-50 year lifetime.

In particular, we stress, that schemes and protocols deemed to be legacy are considered to be secure currently, but that for future systems there are better choices available which

means that retaining schemes and protocols which we deem to be legacy in future systems is not best practice. We summarize this distinction in Table 2.1.

Secondly, we consider the issue of whether a primitive, scheme, protocol or key size is suitable for deployment in new or future systems. In some sense mechanisms which we consider usable for new and future systems meet a gold standard of cryptographic strength; they generally will have proofs of security (i.e., security reductions), will have key sizes equivalent to 128-bits symmetric security or more, will have no structural weaknesses, will have been well studied and standardized.

As a general rule of thumb we consider symmetric 80-bit security levels to be sufficient for legacy applications for the coming years, but consider 128-bit security levels to be the minimum requirement for new systems being deployed. Thus the key take home message is that decision makers now make plans and preparations for the phasing out of what we term legacy mechanisms over a period of say 5-10 years. In selecting key sizes for future applications we consider 128-bit to be sufficient for all but the most sensitive applications. Thus we make no distinction between high-grade security and low-grade security, since 128-bit encryption is probably secure enough in the near term.

However, one needs to also take into account the length of time data needs to be kept secure for. For example it may well be appropriate to use 80-bit encryption into the near future for transactional data, i.e. data which only needs to be kept secret for a very short space of time; but to insist on 128-bit encryption for long lived data. All proposals in this document need to be read with this in mind. We concentrate on proposals which imply a minimal security level across all applications; i.e. the most conservative approach. Thus this does not imply that a specific application cannot use security levels lower than considered here.

The document does not consider any mechanisms which are currently only of *academic* interest. In particular all the mechanisms we discuss have been standardized to some extent, and have either been deployed or are due to be deployed in real world systems. This is not a critique of academic research, but purely a means of focusing the document on mechanisms which will be of interest to decision makers in industry and government.

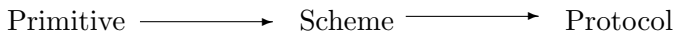
We also consider implementation issues such as side channels resulting from timing (including cache timing), power, electromagnetic radiation, etc., insufficient randomness generation and key life-cycle management; as well as implementation issues related to the mathematical instantiation of the scheme, such as padding oracle attacks etc.

As a restriction of scope, which we alluded to above, we do not make a comprehensive discussion on how key size equivalents are decided upon (e.g. what RSA key size corresponds to what AES key size). We refer to other comparisons in the literature in Section 4.1, but we feel repeating much of this analysis would detract from the focus of this document.

2.1 Understanding Terminology and Structure

The document divides cryptographic mechanisms into primitives (such as block ciphers, public key primitives and hash functions) and schemes (such as symmetric and public key encryption schemes, signature schemes etc). Protocols (such as key agreement, TLS, IPsec etc), are themselves built out of schemes, and schemes are themselves built out of primitives. At each stage of this process security needs to be defined, and the protocol or scheme needs to be proven to meet this definition, given the components it uses. So for example, just because a

scheme makes use of a secure primitive does not imply the scheme is secure; this needs to be demonstrated by a reduction proof. Luckily for most schemes in this report such reduction proofs do exist.



Cryptographic primitives are considered the basic building blocks upon which one needs to make some *assumption*. This assumption is the level of difficulty of breaking this precise building block; this assumption is always the cryptographic community's current "best guess". We discuss primitives in detail in Chapter 4.

In Chapter 5 we then go on to discuss basic cryptographic schemes, and in Chapter 6 we discuss more advanced or esoteric schemes. By a scheme we mean some method for taking a primitive, or set of primitives, and constructing a cryptographic service out of the primitive. Hence, a scheme could refer to a digital signature scheme or a mode of operation of a block cipher. It is considered good cryptographic practice to only use schemes for which there is a *well defined security proof* which reduces the security of the scheme to that of the primitive. So for example a chosen plaintext attack against CBC mode using AES should result in an attack against the AES primitive itself.

2.2 Making a Decision

Making the distinction between schemes and primitives means we can present schemes as general as possible and then allow users to instantiate them with secure primitives. However, this leads to the question of what generally should be the key size for a given primitive, if it is to be used within a scheme? This might seem a simple question, but it is one which divides the cryptographic community. There are two approaches to this problem:

1. A security proof which reduces security of a scheme to the security of an underlying primitive can introduce a *security loss*. The "loss" is the proportion of additional effort an attacker who can break the scheme needs to expend so as to break the primitive. This loss leads some cryptographers to state that the key size of the primitive should be chosen with respect to this loss. With such a decision, unless proofs are *tight*[1], the key sizes used in practice will be larger than one would normally expect. The best one can hope for is that the key size for the scheme matches that of the underlying primitive.

2. Another school of thought says that a proof is just a design validation, and the fact a tight proof does not exist may not be for fundamental reasons but could be because our proof techniques are not sufficiently advanced. They therefore suggest picking key sizes to just ensure the underlying primitive is secure.

It is this second, pragmatic, approach which we adopt in this document. It is also the approach commonly taken in industry.

The question then arises as to how to read this document? Whilst the order of the document is one of going from the ground up, the actual order of making a decision should be

[1] i.e. there is no noticeable security loss in the proof.

from the top down. We consider two hypothetical situations. One in which a user wishes to select a public key signature algorithm and another in which he wishes to select a public key encryption algorithm for use in a specific protocol. Let us not worry too much about which protocol is being used, but assume that the protocol says that one can select either RSA-PSS or EC-Schnorr as the public key signature algorithm, and either RSA-OAEP or ECIES as the public key encryption algorithm.

2.2.1 Public key signatures

We first examine the signature algorithm case. The reader should first turn to the section on signature schemes in Section 5.9. The reader should examine the discussion of both RSA-PSS and EC-Schnorr in Sections 5.9.2 and 5.9.7 respectively. One finds that both signature schemes are considered suitable for legacy applications and future applications. However, for "systems" reasons (probably the prevalence of RSA based digital certificates) the user decides to go for RSA-PSS. The RSA-PSS scheme is actually made up of two primitives; firstly the RSA primitive (discussed in Section 4.5.1) and secondly a hash function primitive (discussed in Section 4.3). Thus the user now needs to consider "which" RSA primitive to use (e.g. the underlying RSA key size) and which hash function to use. The scheme itself will impose some conditions on the relevant sizes so they match up, but this need not concern a reader of this document in most cases. Returning to RSA-PSS we see that the user should use 1024-bit RSA moduli only for legacy applications. If that is all the user requires then this document would support the user's decision. However, if the user is looking at creating a new system without any legacy concerns then this document cannot be used as a justification for using RSA moduli of 1024 bits. The user would instead be forced to consider RSA moduli of 3072 bits (or more) and a hash function such as the 256-bit variant of SHA-2.

2.2.2 Public key encryption

We now turn to comparing the choice of RSA-OAEP and the ECIES hybrid cipher. By examining Chapters 5 and 6 on schemes (in particular Section 5.7.2 for RSA-OAEP and Section 5.8 for ECIES) the user sees that whilst both schemes have security proofs and so can be used for future applications, ECIES is better suited to long messages. They therefore decide to proceed with ECIES, which means certain choices need to be made with respect to the various components. The ECIES public key encryption scheme, being a hybrid cipher, is made from the ECIES-KEM scheme (see Section 5.8.3), which itself makes use of a key derivation method (see Section 5.5 for various choices of key derivation methods) and a Data Encapsulation Method, or DEM. A DEM is a form of one-time authenticated symmetric encryption, see Section 5.4 for various possible instantiations. This creates a huge range of possible instantiations, for which we now outline a possible decision process and which we illustrate graphically in Figure 2.1. From examining Section 5.8.3 on ECIES-KEM and Section 5.4 on authenticated symmetric encryption the user sees that ECIES-KEM is supported for legacy and future use, and that so is Encrypt-Then-MAC as a DEM. Given these choices for the components the user then needs to instantiate Encrypt-Then-MAC, which requires the choice of an IND-CPA symmetric encryption scheme (i.e. a block cipher mode of operation from Section 5.2) and a MAC algorithm from Section 5.3. Looking at these sections the user then selects CTR mode (for use with some block cipher), and CMAC (again for use with some block cipher). The KEM also requires use of a key derivation function from Section

5.5, which will output a key for the block cipher in CTR mode and a separate key for the CMAC algorithm. The user at this point could select the key derivation function that we denote X9.63-KDF, which itself requires the use of a hash function. Only at this point does the user of this document examine Chapter 4 on primitives so as to instantiate the precise elliptic curve group, the precise hash function for use in the key derivation function and the block ciphers to be used in the CTR mode encryption and the CMAC function. At this point a valid choice (for future applications) could be a 256-bit elliptic curve group, the SHA-2 key derivation function, and the AES block cipher at 128-bit key-length.

We stress that the above decision, on how to instantiate ECIES, is just one possible amongst all the various methods which this document supports.

2.3 Comparison to Other Documents

This document is one of many which presents details on cryptographic primitives, key sizes, schemes and protocols. Each of these documents has a different audience and purpose; our goal has been to present an analysis of algorithms commonly used in current practice as well as providing state-of-the-art advice as to adoption of algorithms in future systems. Our choices are often rather conservative since we aim to give proposals for the constructions of systems with a long life cycle.

Various government organisations provide advice, see Annex A of [193], or mandates, in relation to key size and algorithm choice for their own internal purposes. In these documents, the choice of algorithms and key sizes is often done with an eye to internal systems and processes. The current document extends this scope to a wider area, e.g., internet communication and hence in addition considers algorithms deployed in various internet protocols.

Among the EU member states, there are a number of such documents including [35] published by France, and [126, 127] published by Germany. The key size recommendations of these three documents are in almost all cases consistent with our own proposals for symmetric key sizes, hash function sizes and elliptic curve key sizes. The documents [126] and [35] also mention integer factorisation based primitives; our proposals are more conservative than these two documents. Along with [35] we place a strong emphasis on using schemes with modern security proofs.

Further afield the US government maintains a similar document called Suite B [414], which presents recommended algorithms and key sizes for various governmental uses. Again our analysis is broadly consistent in terms of key sizes with this document. Note that the US government is now in the process of updating Suite B to encompass so-called post-quatnum algorithms (cf. Section 2.4).

All of these documents [35, 126, 127, 414] also detail a number of concrete cryptographic schemes. In this aspect our coverage is much wider due to our wider audience. For example all documents recommend the use of AES, SHA-2 and elliptic curve based primitives, and some integer factorisation based primitives. As well as these basic primitives we also mention a number of other primitives which are used in various deployed protocols, for example Camellia (in TLS), SNOW 3G (in GSM/LTE), as well as primitives used in systems designed a long time ago but which are still in use (e.g. MD5, SHA-1, DES etc).

In terms of cryptographic schemes our coverage is much wider than that of [126, 127, 414]; this is only to be expected as per our different audiences. As an example of this we cover a significant number of MAC functions, authenticated encryption modes, and key derivation

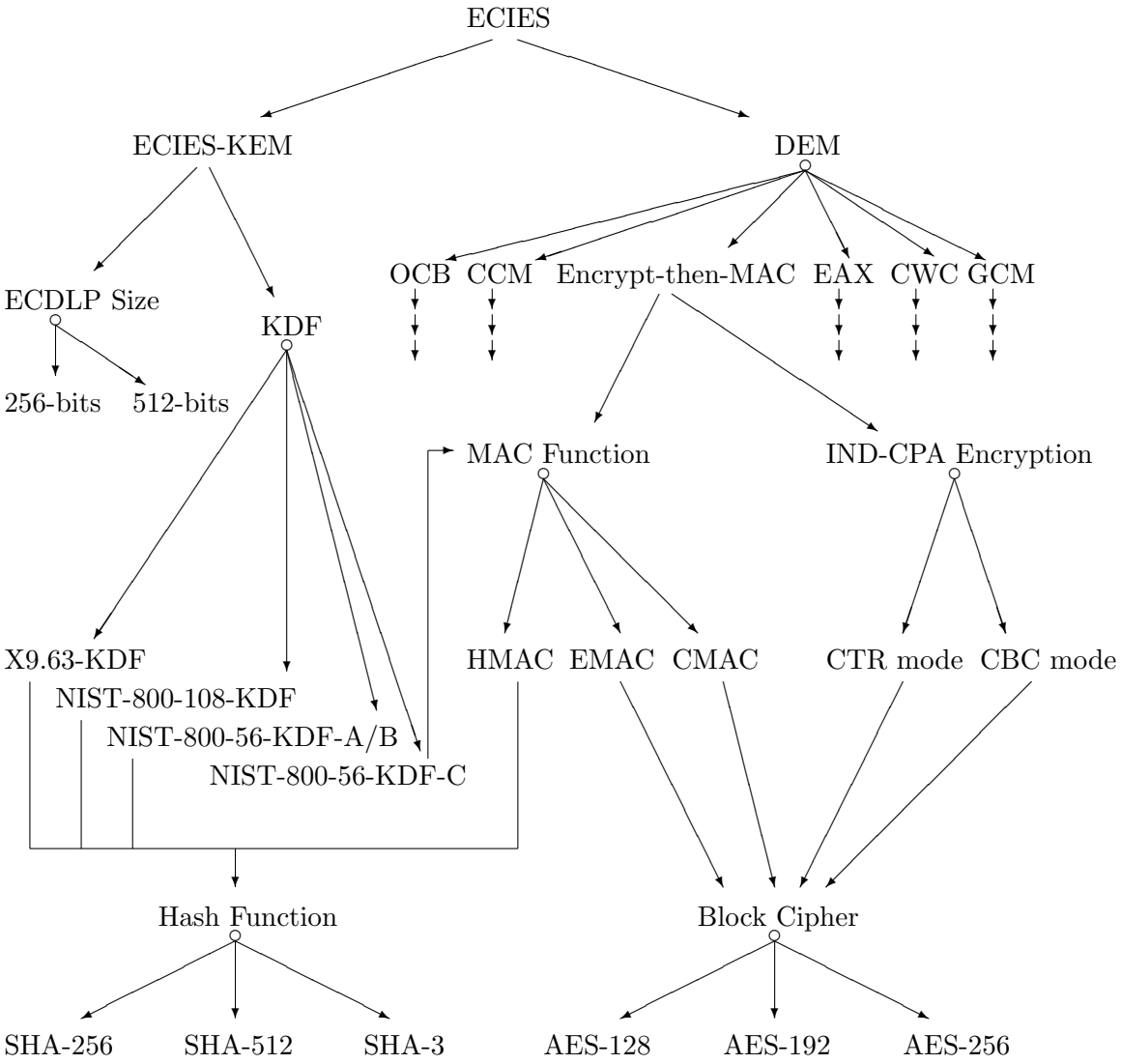


Figure 2.1: Just some of the design space for instantiating the ECIES public key encryption algorithm. Note, that not all standards documents will support all of these options. To read this diagram: A group of arrows starting with a circle implies the implementer needs to choose one of the resulting paths. A set of three arrows implies a part of the decision tree which we have removed due to space. In addition (again for reasons of space) we do not list all possible choices, e.g. some hash functions can be block cipher based. Even with these restrictions one can see the design space for a cipher as well studied and understood as ECIES can be quite complex.

functions compared to the other documents. In one aspect we diverge from [126, 127, 414] in that we propose the DSA algorithm, and many of its variants, for use in legacy systems only. This is because DSA only has a security proof in a relatively weak computational model [122]. For discrete logarithm based signatures we propose schemes such as Schnorr signatures [519], which have stronger provable security properties than DSA [417, 468].

Another form of comparison can be made with the documents of various standards organisations. The ones which have been most referred to in this report are those of IETF, ISO and NIST. Divergences from our analysis (if any) in these standards are again due to the distinct audiences. The IETF standardises the protocols which keeps the internet running, their main concern is hence interoperability. As we have seen in recent years, with attacks on TLS and IPsec, this often leads to compromises in algorithm selection and choice. The ISO takes a very liberal approach to standardising cryptographic algorithms, with far more algorithms standardized than a report like this could reasonably cover. We have selected algorithms from ISO (and dubbed them suitable/unsuitable for legacy and future use) due to our perception of their importance in other applications. Finally the NIST documents are more focused, with only a small subset of schemes being standardized. A major benefit in the NIST standardization is that when security proofs are available they are alluded to, and so one can judge the scientific basis of the recommendations.

Finally, we compare with the recommendations of the European Payments Council (EPC). In their document [201] the EPC also divide cryptographic systems into those for legacy and those for future use. They classify SHA-1, RSA moduli with 1024 bits, ECC keys of 160 bits as suitable for legacy use, and 3DES, AES-128, SHA-2 (256-bit and 512-bit variants), SHA-3, Whirlpool, RSA moduli with 2048 bits, ECC keys of 224 bits or more as suitable for future use. These are broadly in line with our analysis, although we no longer believe SHA-1 is suitable for legacy use.

2.4 Open Issues and Areas Not Covered

Much of the analysis in this document is focused on long term data protection issues (e.g. encrypted stored data, or long term signatures). Many cryptographic systems only need to protect transient data (i.e. transactional data) which has no long term value. In such situations some of the proposals with respect to key size etc. may need to be changed.

Due to constraints of space and time there are also a number of areas which we have not touched upon in this document. In terms of cryptographic schemes these contain, but are not limited to:

- Currently practical Post-Quantum Systems: There are many posibilities for hard problems for basing post-quantum systems on e.g. hash functions (signatures [83]), lattices (encryption [82, 259, 373, 377], signatures [177], key-agreement [22, 112]), coding theory (encryption [81]), and isogenies (key-exchange [156, 205]). The community is currently engaged in a debate as to what would be the best hard problem set to base systems on. There is even within a given family no consensus as to key sizes. NIST has just started a process to select a set of potential post-quantum secure systems, which will run for the next few years. At this point in time the lack of consensus means we do not feel confident to recommend a specific set of post-quantum systems[2]. The only exception are hash-based signatures. These are currently undergoing standardization within IRTF and are mentioned in this report.

- Short signatures and signatures with message recovery: Short signatures are used in multiple scenarios, and signatures with message recovery are used in currently deployed

[2]It is expected post-quantum systems to be standardized in the next couple of years will include encryption, signature and key exchange primitives.

systems such as the chip-and-pin system EMV. The current document does not cover such cryptographic schemes.

- Encryption schemes which enable de-duplication of ciphertexts: The use of such schemes, and other deterministic encryption schemes such as format preserving encryption, are becoming more used in real systems. Encryption which enables de-duplication is important to enable secure cloud backup.

Chapter 3

General Comments

Before proceeding with our main discussion of keysizes, scheme and protocols we discuss a number of general issues related to the deployment of cryptographic technology; namely we discuss hardware and software side-channels, random number generation and key life-cycle management.

3.1 Side-channels

Traditionally, cryptographic algorithms are designed and analysed in the black-box model. In this model, an algorithm is merely regarded as a mathematical function that will be applied to some input to generate some output, regardless of implementation details. An evaluation of a keyed algorithm in the black-box model assumes that an adversary knows the specification of the algorithm and can observe pairs of inputs I and outputs $O = E_k(I)$ of a black box implementing the algorithm.

When cryptography is implemented on embedded devices, black-box analysis is not sufficient to get a good picture of the security provided. The cryptographic algorithms are executed on a device that is in the possession and under the physical control of the user, who may have an interest in breaking the cryptography, e.g. in banking applications or digital rights management applications. The physical accessibility of embedded devices allows for a much wider range of attacks against the cryptographic system, not targeting the strength of the algorithm as an abstract mathematical object, but the strength of its concrete implementation in practice.

Classical examples for side-channels include the execution time of an implementation [344], the power consumption of a chip [345] and its eletromagnetic radiation [218]. More exotic examples include acoustics [39], temperature [121] and light emission [530]. Some side-channels can be observed only by means of an invasive attack, where the computing device is opened. Others can be observed in a passive attack, where the device is not damaged.

There are many reasons for side-channel leakage, including hardware circuit architectures, micro-architectural features and implementations. Interestingly, many side-channels arise from optimisations. For example, circuits in modern CMOS technology consume power only when the internal state changes. The amount of power consumed is proportional to the number of state bits that change. This clearly has the potential to become a side-channel. For other examples of the relation between optimisation and side-channels, please see Section 3.1.1.

Many cryptographic algorithms are constructed as *product ciphers* [525]: one or a few cryptographically weak functions are iterated many times such that the composition is secure. Other algorithms use a small number of complex operations. In order to implement such algorithms, however, these complex operations are usually broken down into sequences of less complex operations. Hence, their implementations are similar to product ciphers. Furthermore, in keyed algorithms (or their implementations), typically the key is introduced gradually: the dependence of the intermediate data on the key increases in the course of the algorithm (or implementation).

Side-channel attacks capitalise on this property of gradually increasing security. While it is (supposedly) hard to attack the full cryptographic algorithm, it is much easier to attack the cryptographically weak intermediate variables. Depending on the side-channel, measurements of the leakage contain information about the intermediate variables at each instance of time (e.g. power consumption), or about an aggregate form thereof (e.g. execution time). Thus, side-channel measurements allow an attacker to zoom in on the algorithm and to work on a few iterations only of the cryptographically weak functions. By working with intermediate variables that depend only on a fraction of the bits of the secret key, side-channel attacks allow an attacker to apply a divide-and-conquer strategy.

3.1.1 Countermeasures

Countermeasures against side-channel attacks can be classified into two categories. In the first category, one tries to eliminate or to minimise the leakage of information. This is achieved by reducing the signal-to-noise ratio of the side-channel signals. In the second category, one tries to ensure that the information that leaks through side-channels cannot be exploited to recover secrets. Typically, one will implement a combination of countermeasures. Increasing the key size will (in general) not improve the resilience against side-channel attacks.

Constant-time algorithms

The first academic publication of a physical attack is the timing attack on RSA [344]. In a naive implementation of modular exponentiation, the execution time depends on the value of the exponent, i.e. the private key. By observing the execution time of a series of decryptions or signatures, an adversary can easily deduce the value of the private key.

Hence, a first countermeasure to be taken is to ensure that the execution time of the cryptographic algorithm doesn't depend on the value of secret information. The difficulty of this task depends greatly on the features of the processor that the software will run on and the compiler that is being used to translate high-level code into low-level assembly instructions.

Simple processors and low-level programming languages give the programmer absolute access to the control flow of the program, making it possible to write code that executes in constant time. Modern pipelined processors contain units for branch prediction, out-of-order execution and other systems that may complicate the task of predicting the exact execution time of an algorithm or a subroutine. These units may interact with compiler options and settings in ways that are difficult to fully understand. In such environments, it may be difficult to achieve absolutely constant-time code.

Observe that constant-time code is usually slow code. Indeed, any optimisation that can be applied only for a fraction of the values that a secret variable can take, leads to non-constant execution time and therefore has to be excluded. However, some cryptographic

algorithms are designed so that constant-time code is fast.

Constant power consumption

For implementations in hardware, constant execution time is usually easy to achieve. However, the side-channels of hardware implementations typically leak much more information than the side-channels of software implementations. For example, the instantaneous power consumption signal not only leaks the execution time of the algorithm, but also its level of activity at each instant of time. Balanced circuits reduce the signal leaking from hardware implementations [542].

Reduce secret data-dependent branches

Branching instructions where the condition depends on the value of secret data are an obvious cause for differences in execution time. Since it is difficult to ensure that all branches execute in exactly the same time, it is recommended to prefer methods that have fewer data dependent branches. For example, instead of implementing an exponentiation by means of square-and-multiply (or double-and-add) techniques, one can employ the Montgomery ladder method, which behaves very regularly [314].

Reduce secret data-dependent lookups

Modern processors can execute instructions much faster than modern main memories can deliver new instructions and operands. In order to avoid that processors have to wait, memories are organised in a hierarchy. At the bottom are the very large and very slow disks. Above are layers of increasingly smaller and faster memory units: RAM, L2 cache, L1 cache. This memory architecture has as a side-effect that the time it takes to lookup data, is not constant. If the data is present in L1 cache, then the lookup goes faster than if it needs to be brought in from L2 cache or RAM.

Many implementations of cryptographic algorithms use lookup tables. Unless special precautions are taken, these lookup tables will not be present in L1 cache at the start of the execution of the algorithm. Sometimes the tables don't even fit into the L1 cache. This usually causes differences in execution time, which may lead to timing attacks [77, 545].

Bit-slice implementations are implementations that avoid table lookups. Instead they compute table elements on the fly [85]. In particular if the algorithm applies the same function to several parts of the input in parallel (SIMD parallelism), the performance of bit-slice implementations may be very competitive to table-based implementations [322]. For the specific case of AES (and other algorithms with the AES S-box), the AES-NI instructions can be used to avoid table lookups.

Masking

The purpose of masking is to ensure that the value of individual data elements is uncorrelated to secrets. Hence, if there is leakage on the value of individual data elements, this will not lead to recovery of the secrets. Clearly, if an attacker can combine signals of different elements, he can again start to recover the secrets, but the approach can be generalised to higher levels, making tuples, triplets, ... of data independent of the value of the secret [479]. Masking can be done for software implementations and for hardware implementations. A challenge in

practice is how to obtain a sufficient number of random bits for the masking – note that the generation of those bits may again be subject to side channel attacks.

In hardware, masking can be employed at gate level [274, 544], at algorithm level [16], or in combination with circuit design approaches [471].

The Threshold Implementation method is a masking approach that achieves provable security against some types of attacks based on secret sharing techniques at a moderate cost in hardware complexity [421, 472]. It can also be used to mask software implementations. An alternative approach based on Shamir's secret sharing scheme is presented in [229].

3.2 Random Number Generation

Randomness is needed in almost all cryptographic systems and protocols. For example, random numbers are needed for generating asymmetric key-pairs, for defining symmetric keys, for generating initialisation vectors (IVs) for cryptographic modes of operation, in challenge-response protocols, as additional inputs to most standardised public key encryption and signature algorithms, and to generate ephemeral values in key exchange protocols. The existence of suitable random sources is taken for granted in much of the research literature in cryptography, and almost all formal security analysis of cryptographic schemes fails if perfect randomness assumptions are not met. Yet there are many prominent examples of randomness failures with severe security consequences; examples include:

- Netscape's implementation of SSL, which was discovered in 1996 to make use of a random number generator in which the only sources of entropy used to seed the generator were the time of day, the process ID and the parent process ID [225].
- The Debian OpenSSL randomness failure, in which a patch applied by a Debian developer led to substantially reduced entropy being available for key generation in OpenSSL [164]. Affected keys included SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections, with all keys produced between September 2006 and May 2008 being potentially suspect.
- Two independent analyses of public keys found on the Internet [253, 367], which discovered, amongst other things, that many pairs of RSA public keys had common factors, making the derivation of the corresponding private keys a relatively trivial matter. The identified issues are at least in part attributable to poor randomness generation procedures, especially in the Linux kernel [253]. A follow-up study on a particular smart-card deployment involving RSA is reported in [80].
- Ristenpart and Yilek studied how randomness is handled across virtual machine resets [487], discovering that the state of the PRNG can often be predicted to the point where an attack against a DSA signing key can be mounted in the context of TLS (two signatures on distinct messages being produced with the same random input leading to immediate recovery of the DSA private key).

3.2.1 Terminology

We refer to Random Number Generators (RNGs), but these are also often referred to as Random Bit Generators in the literature. A suitable source of random bits can always be

turned into a source of random numbers that are approximately uniformly distributed in a desired range by various means (see [207, Section 10.8], [439, Appendix B] for extensive discussion of this important practical issue). In what follows we make extensive reference to the NIST standard [439], however the interested reader should also consult the ISO 18031 standard [283] and ANSI X9.82 [34].

We distinguish between True Random Number Generators (TRNGs) and Pseudo-Random Number Generators (PRNGs). TRNGs usually involve the use of special-purpose hardware (e.g. electronic circuits, quantum devices) followed by suitable post-processing of the raw output data to generate random numbers. In an ideal world, all random number requirements would be met by using TRNGs. But, typically, TRNGs operate at low output rates (relative to PRNGs) and are of moderate-to-high cost (relative to PRNGs which are usually implemented in software). A TRNG device might be used to generate highly sensitive cryptographic keys, for example system master keys, in a secured environment, but would be considered "overkill" for general-purpose use. PRNGs are suitable for general-purpose computing environments and usually involve a software-only approach. Here, the approach is to deterministically generate random-looking outputs from an initial seed value. We note that NIST [439] refer to PRNGs as DRBGs, where "D" stands for "deterministic", stressing the non-random nature of the generation process. Here, we focus on PRNGs, since TRNGs do not in general offer the flexibility and cost profile offered by (software) PRNGs.

A PRNG usually includes a capability for reseeding (or refreshing) the generator with a fresh source of randomness. The problem of obtaining suitable and assured high-quality randomness for the purposes of reseeding is one of the most challenging aspects of designing systems that use PRNGs.

PRNGs are sometimes described as being *blocking* or *non-blocking*. For example, the Linux kernel PRNG provides two different RNGs, one of each type. A blocking RNG will prevent outputs from the RNG from being delivered to the application requesting random numbers if it deems that doing so would be inappropriate for some reason.

3.2.2 Architectural model for PRNGs

An important basic architectural choice that is followed by most modern PRNGs is to separate the problems of entropy collection and generation of seeds from the problem of generating pseudo-random outputs as a function of the seed and generator state. NIST [439] provides a general functional model for describing and classifying PRNGs which makes this distinction clear. The components of this model include:

- **Entropy input**: this is provided to the PRNG for the purposes of generating the seed. This input is not guaranteed to be uniformly random, but is assumed to contain enough entropy that a seed of suitable quality can be extracted from it. This input must remain secret in order for the outputs of the PRNG to remain secure. This entropy input may initially be supplied by the user running the PRNG or may be harvested from the platform on which the PRNG is running.

- **Other inputs**: these might be time-based or take the form of a nonce. These inputs are not assumed to be secret. They are combined with the entropy input when generating seeds.

- **Personalisation string**: a further input to the seed generation process which is intended to provide further diversity for the generator outputs. For example, one might

use different strings for key generation for different algorithms here.

- **Internal state:** this represents the memory of the PRNG, including the data that is used as input (and possibly modified) during the generation of outputs. Clearly, this state must remain secret for the future outputs of the PRNG to remain secure.
- **Instantiate function**: this function acquires the entropy input, any other input and the personalisation string and combines them to create a seed from which the initial internal state is created.
- **Generate function**: this function uses the current internal state to generate pseudo-random output bits and to update the state for the next request for output bits. This function should maintain a counter indicating the number of requests serviced or blocks of output produced since the generator was first seeded or reseeded. This counter would enable the PRNG to block further requests once a preset limit on the amount of output produced has been reached.
- **Reseed function**: this function combines a new entropy input (and possibly further additional input) with the current internal state to create a new seed and a new internal state.
- **Uninstantiate function**: this function erases the internal state; its intended use is to ensure the safe decommissioning of a PRNG.
- **Health test function**: this function is intended to provide a mechanism by which the PRNG can be tested to be functioning correctly.

We note that the last two components are often not explicitly present in PRNG implementations. Moreover, many PRNGs do not have "other inputs" or allow the use of personalisation strings. Some generators in the literature do not fully separate the reseed and generate functions, mixing entropy directly into the state of the generator, for example.

3.2.3 Security Requirements for PRNGs

Until quite recently, formal security requirements for PRNGs were lacking, and the requirements were informally stated and driven by the security requirements of the applications in which their outputs are intended to be used. The informal requirements can be stated as follows:

- **Output indistinguishability**: Without knowledge of the initial seed or current state, it should be hard to distinguish the outputs of the generator from a truly random sequence of the same type, even when many previous outputs are known. For certain generators, this property can be proven based on some computational assumption (e.g. the outputs of the Blum-Blum-Shub generator [101] are pseudo-random assuming the hardness of the quadratic residuosity problem, which is closely related to the factoring problem). For fast, practical generators, built using hash functions and block ciphers, this property rests on unproven but reasonable security assumptions concerning these symmetric components (e.g. the NIST CTR PRNG from [439] has output indistinguishability that relies on the block cipher acting as a pseudo-random function; note that for an n-bit block cipher this requires that substantially less than $2^{n/2}$ outputs are generated with the same key).

- **Forward security**: Compromise of the internal state of the generator should not allow an attacker to compute previous outputs of the generator, nor to distinguish previous outputs from random. This requirement implies in particular that it must be hard to compute any previous state of the generator from its current state. In turn, this implies that the generator state must be updated after each output in a one-way manner.
- **Resistance to state-extension attacks**: In a state-extension attack [330], an attacker is assumed to compromise the state of the generator, and then try to learn future outputs of the generator (or distinguish them from random). Clearly, in the absence of reseeding, this is possible since the future states and outputs are then a deterministic function of the current state. Moreover, if the reseeding process is carried out, but has insufficient entropy in its input, then an attacker can try to calculate forwards through the reseeding process, trying all likely values for the unknown entropy inputs used during the reseeding, and testing for consistency with some known outputs. It is desirable that a PRNG should resist such attack, since the design intention of reseeding is that it should assist in recovering from state compromises.
- **Compromise of reseeding data should not lead to generator compromise**: In some attack scenarios, the entropy input used during reseeding may fail to have insufficient entropy, or become known to the attacker. In this situation, we would like to ensure that the attacker cannot learn the generator's new state after reseeding, nor predict its outputs after reseeding. For this to be achieved, the entropy input must be carefully combined with the current state during reseeding.

Note that none of these requirements directly refer to the quality of entropy inputs, but that this rapidly emerges as a key concern in meeting the requirements.

3.2.4 Theoretical models

Theoretical models for the analysis of PRNGs first emerged in [48] and were significantly developed in [173, 174]. Generators secure in the models presented in these papers provably provide all of the above informally-stated security properties. The differ considerably in the way that they treat the incorporation of new entropy in the reseeding step. Generators in these models also deviate from the NIST architectural view discussed in Section 3.2.2, in that they do not consider other inputs, personalisation strings, the uninstantiate function, or the health test function. They all suffer from the unnatural requirement of having a random seed for an extractor (which may be known to the adversary) as part of the public parameters of the generator. This can be avoided in practice by replacing the seeded extractor with a concrete hash function.

These sources [48, 173, 174] have in common with [439] that they deliberately separate the concern of randomness generation for seeding/reseeding from the question of designing a generator taking assumed-to-be-random seeds/reseeds as input. Indeed, there are many good designs solving the latter problem, but few general-purpose solutions to the former.

3.2.5 Implementation considerations

In addition to meeting the above security requirements, there are many implementation issues that need to be addressed when deploying a PRNG.

Entropy sources: Foremost amongst these implementation issues are the questions of how to identify suitable sources of entropy, how to manage and process these sources, and how (and indeed, whether) to assess the quality of the entropy that is extracted from these sources when reseeding a PRNG. A good general overview of these issues can be found in [183, 234].

Entropy estimation: There is some debate in the literature on whether an implementation should try to estimate how much entropy is available from these sources. Accurate (or at least, conservative) estimation of entropy is important because of state extension attacks: too little entropy, and a state compromise (or a default initial state) can lead to predictable generator outputs; on the other hand, waiting too long provides poor protection against state compromises, weakening forward security. The majority of practical PRNG designs do some form of entropy estimation. However, Ferguson *et al.* [207] contend that no procedure can accurately assess entropy (or rather, the amount of entropy unknown to an attacker) across all environments. Their `Fortuna` PRNG design attempts to get around the problem of entropy estimation by allocating gathered entropy, represented by events, to a sequence of entropy pools in order. The `Fortuna` generator then uses the pools at different intervals to reseed the generator. An analysis of this approach was provided in [174].

The `Fortuna` design sets out to avoid the need for entropy estimation whilst preventing state-extension attacks. As pointed out by Barak and Halevi [48], this approach works well so long as the entropy is well-spread across the different pools, but does not work well if the entropy is concentrated in one pool that is not often accessed when doing state refreshes. It is possible that an adversary could arrange for this to occur by generating large numbers of spurious events under his control. The view of Barak and Halevi is that it is better to accumulate entropy over a long period of time in a single pool and do infrequent reseeds, but without doing any entropy estimation, since in their view "*at best the entropy estimator provides a false sense of security*". A third approach is to perform conservative entropy estimation, and to reseed only when sufficient entropy is available – this is the approach taken in the Linux `dev/urandom` and `dev/random` PRNGs, for example.

Generator initialisation: An important special case of seeding is the setting of the initial state (which is done via the Instantiate function in the NIST model). A PRNG should be blocking until properly initialised, either with entropy supplied by the user, or with entropy gathered from the local environment. There is anecdotal evidence that this is not popular with software developers – see [253], where it is explained how one SSH implementation uses the non-blocking Linux `dev/urandom` PRNG in preference to the blocking `dev/random` one when generating cryptographic keys, because `dev/random` continues blocking after proper initialisation whenever it believes that the amount of requested output exceeds the total amount of entropy received. We reiterate that accessing a PRNG before it is properly seeded for the first time has been identified as a source of serious security problems, particularly in key generation [253], but it is safe for a properly seeded PRNG to generate a large amount of output if the PRNG is properly designed.

3.2.6 Specific PRNGs and their analyses

Library functions in programming languages such as `random()` in the C programming language must be avoided in cryptographic applications. In general, such functions tend to be

based on very weak generators such as Linear Congruential Generators. Dedicated cryptographic PRNG implementations are needed.

There are many operating-system-specific PRNGs. The Microsoft Windows PRNG has a closed-source implementation. An instance of this PRNG was reverse-engineered and found to have quite severe deficiencies in [175]. The Linux PRNG was analysed in [235], with significant attacks being found. The Linux PRNG has been modified as a result, and the current version was analysed in [356], with the previously reported weaknesses being found to have been largely addressed.

There are several PRNGs that are supplied as part of crypto libraries. Prominent amongst these is the OpenSSL PRNG. This generator has a rather ad hoc design. It was analysed in [503], and some changes were made as a result of this analysis. However, as far as we are aware, it has not been subjected to any further cryptographic analysis since then. Gutmann has designed a PRNG that is made available as part of his `cryptlib` software development kit[1]. This PRNG and its design are described in detail in [234].

The NIST special publication [439] contains several PRNG designs. A pseudo-randomness property was proven for the Dual Elliptic Curve generator in [123], based on some reasonable number-theoretic assumptions. However, the generator is relatively slow and known to have a small bias in its outputs. The generator has the potential to contain a backdoor, enabling its internal state to be reconstructed given sufficient output [529], and it is widely believed that this potential was exploited during the NIST standardisation process by NSA. A recent study [140] found the generator to be in surprisingly widespread use. The controversy surrounding this Dual Elliptic Curve generator led to the withdrawal of the generator from the NIST special publication [439] and the opening of a comment period on a revised version of the NIST document[2]. The HMAC-based DRBG has been analysed in [257] and the CTR-based design is analysed in [528].

These NIST PRNG designs do not include a full specification of how to gather and process entropy sources for seeding/reseeding purposes, which is consistent with the over-arching approach in [439].

The `Fortuna` generator from [207] incorporates learning from the earlier `Yarrow` design [328]. Its basic design of using entropy pools to collect entropy for reseeding at different rates was recently validated by the analysis of [174], whilst see [240, 528] for two analyses of Intel's hardware RNG.

3.2.7 Designing around bad randomness

Given that randomness failures seem to be hard to avoid in general, a number of authors have attempted to design cryptosystems that handle bad randomness to the extent that this is possible. Work in this direction can be summarised as follows:

- For signatures, there is a folklore de-randomisation technique which neatly sidesteps security issues arising from randomness failures: simply augment the signature scheme's private key with a key for a pseudo-random function (PRF), and derive any randomness needed during signing by applying this PRF to the message to be signed; meanwhile verification proceeds as normal.

[1] See `http://www.cryptlib.com/`

[2] See `http://www.nist.gov/itl/csd/sp800-90-042114.cfm`.

- In the symmetric encryption setting, Rogaway [495] argued for the use of nonce-based encryption, thus reducing reliance on randomness. Rogaway and Shrimpton [499] initiated the study of misuse-resistant authenticated encryption (AE), considering the residual security of AE schemes when nonces are repeated. Katz and Kamara [319] considered the security of symmetric encryption in a chosen-randomness setting, wherein the adversary has complete control over the randomness used for encryption (except for the challenge encryption which uses fresh randomness).
- In the public key encryption (PKE) setting, Bellare *et al.* [59] considered security under *chosen distribution attack*, wherein the joint distribution of message and randomness is specified by the adversary, subject to containing a reasonable amount of min entropy. Bellare *et al.* gave several designs for PKE schemes achieving this notion in the Random Oracle Model (ROM) and in the standard model. A follow-up work [484] considers a less restrictive adversarial setting.
- Also in the PKE setting, Yilek [569], inspired by virtual machine reset attacks in [487], considered the scenario where the adversary can force the reuse of random values that are otherwise well-distributed and unknown to the adversary. This is referred to in [569] as the *Reset Attack* (RA) setting. In [569], Yilek also gave a general construction achieving security for public key encryption in his RA setting. The RA setting was recently extended to a setting where the adversary can to a certain extent control the randomness that is used during encryption, the so-called Related Randomness Attack (RRA) setting [453].
- Ristenpart and Yilek [487] studied the use of "hedging" as a general technique for protecting against broad classes of randomness failures in already-deployed systems, and implemented and benchmarked this technique in OpenSSL. Hedging in the sense of [487] involves replacing the random value r required in some cryptographic scheme with a hash of r together with other contextual information, such as a message, algorithm or unique operation identifier, etc. Their results apply to a variety of different randomness failure types but have their security analyses restricted to the ROM.

3.3 Key Life Cycle Management

In this section we discuss general aspects related to key life cycle management. More information about key management techniques can be found in [446, Chapter 13], and in NIST-800-57 [437].

Objectives of Key Management

Cryptographic mechanisms reduce the problem of data security to the problem of key management. This is known as Kerckhoffs' principle: *the security of a cryptosystem should not rely on the secrecy of any of its workings, except for the value of the secret key.* It follows that good key management is essential in order to benefit from the introduction of cryptography. We distinguish the following objectives of key management:

1. Protecting the confidentiality and authenticity of secret and private keys, as well as protecting secret and private keys against unauthorised use.

2. Protecting the authenticity of public keys.
3. Ensuring the availability of secret and public keys.

To accomplish these three goals we need to examine the whole key life cycle; from generation of the key material through to destruction.

Key Generation

Secret keys and private keys need to be unpredictable. Symmetric primitives usually don't have additional requirements for the secret keys, except that some primitives have a small fraction of weak keys, which should not be used. Asymmetric primitives usually have additional requirements, both on their private and public keys. For example, they often require the generation of prime numbers that need to satisfy extra properties. Keys can either be generated at random in a protocol, in which case generating them with a sufficient amount of entropy turns out to be a very challenging task in practice, see Section 3.2, in other instances keys are derived from other data as part of the protocol definition. There are numerous well documented attacks on systems for which not enough entropy was used to generate the underlying key material.

Key Registration/Certification

Keys need to be associated with their owner (user). For example, public keys are linked to their owner by means of (public-key) certificates. Through the issuing of a certificate, a certification authority guarantees that a certain key belongs to a certain user, and associated policy statements specify for what purposes the owner may use the key. A certificate also has a validity period. Certificates are usually public documents. Their authenticity is ensured by means of a digital signature, placed by the certification authority. However, one needs to trust the certificate authority and its public key, which is itself authenticated by another certificate authority; creating a certificate chain. At the root of the chain is a root certificate authority. These root certificates can be distributed to relying parties and signatories alike by, for example including them in applications (as in a web browser) or having them downloaded from an authoritative source (e.g. a designated public authority), for the purpose of invoking trust.

Various issues have come to light in the last few years as to the ability for users to fully trust the root certificates in their browsers; e.g., false certificates have been issued by governments and companies that want to intercept connections; they have also been used by hackers who have managed to subvert CAs. Thus certification is a technology which is (still) not completely 100% reliable. Hence, when using certificates in a non-public application (e.g. in a corporate environment) care needs to be taken as to the underlying policy framework and how this is implemented and enforced. The security of certificates for public applications is also a matter of dispute.

Key Distribution and Installation

Keys need to be distributed to their users. For systems based on symmetric cryptography, both the sender and the receiver need to obtain a copy of the key, hence the key needs to be transported securely (protection of confidentiality and authenticity) at least once, or agreed

via means of a key agreement scheme. All the copies of the key need to be installed and stored securely. For systems based on asymmetric cryptography, the private key is often generated where it will be used, such that no transport is needed. In secure hardware, the functionality to export the private key of an asymmetric key pair is usually deliberately not implemented (again, this can be compromised by poorly implemented hardware in some cases and in other cases this may be offered as a functionality in order to allow redundancy purpopses). Otherwise, it needs to be protected like a symmetric key. The public key still needs to be transported, but only the authenticity (and hence the integrity) needs to be protected, which is achieved by the use of certificates.

In order to reduce the number of keys that need to be stored locally, one can use Key Distribution Centers, centrally managed key servers. Users share long-term keys with the Key Distribution Centers and trust the servers to provide them with the keys of the other users when they need them. Key Distribution Centers can manage both secret and public keys.

Key Use

The goal of key management is to put keys in place such that they can be used for a certain period of time. During the lifetime of a key, it has to be protected against unauthorised use by attackers. The key must also be protected against unauthorised uses by the owner of the key, e.g. even the owner of the key should not be allowed to export a key or to use it in an insecure environment. This protection can be provided by storing the key on secure hardware and by using secure software, which includes authorisation checks.

Key Storage

By using secure hardware, it is possible to store keys such that they can never be exported, and hence are very secure against theft or unauthorised use. However, sometimes keys get lost and it might be desirable to have a backup copy. Organisations might require backups of keys in order to be able to access data after employees leave. Similarly, expired keys might be archived in order to keep old data accessible. Finally, under certain conditions law enforcement agencies might request access to certain keys. Technical systems that implement access for law enforcement agencies are called key escrow mechanisms or key recovery mechanisms.

Backup, archival and escrow/recovery of keys complicate key management, because they increase the risk for loopholes for unauthorised access to keys. The advanced security requirement of non-repudiation requires that the owner of a key is the only one who has access to the key at all times from generation to key retirement. For example, keys that are used for advanced electronic signatures have to be under the sole control of the user. Archival, backup or storage of such keys is difficult. For use of the non-repudiation property in a court of law one may require special procedures for digital signature generation to be followed.

Revocation/Validation

Cryptographic keys expire and are replaced. Sometimes it can happen that keys have to be taken out of use before the planned end of their lifetime, e.g. if secret keys leak to outsiders or if developments in cryptanalysis make schemes insecure. This process is called revocation. In centralised systems, revocation can usually be achieved relatively easily, but in distributed systems special measures have to be implemented to avoid that people use or rely on keys that

have been expired early. In the context of revocation, validation has a very specific meaning. It means to check whether a cryptographic operation, e.g. placing a digital signature, was performed with a key that is valid, or was valid at the time the operation took place.

Key Archive/Destruction

When the lifetime of the key has expired, it has to be removed from the hardware. This requires a secure deletion process. In most operating systems and applications, the deletion of a file only clears a logic flag. It doesn't result in actual removal of the data until the disk space used to store the file is reclaimed and overwritten by another application. On many file storage media, even after a file has been overwritten, it is possible to recover the original file, using some moderately advanced equipment. This is called data remanence. Various techniques have been developed to counter data remanence. At the logical level, one can overwrite the disk space repeatedly with certain bit patterns in order to make recovery difficult; however, this fails for disks based on solid state memory. At the physical level, one can degauss (on magnetic media) or employ other operations that restore the storage media in pristine state, or one can physically destroy the storage media.

3.3.1 Key Management Systems

In many large organisations there is a need to systematise the above mentioned aspects of key life-cycle. This is usually done using a *Cryptographic Key Management System*; this is an automated system consisting of hardware and software components which implement the required policy to manage the above keys. Aspects including generation, storage, validation and use. For example if keys are held in hardware security modules, then it is common practice to only enable extraction of keys from the hardware modules under some form of key wrap algorithm. A cryptographic key management system ensures that such a policy is enforced, without the users being able to override it.

The NIST standard 800-130 [426] provides a framework for describing such key management systems in a way which enables a simpler validation that any specific key management system satisfies the given policy. The framework defines specific topics and for each topic defines a set of requirements which any framework needs to meet; from this any given system can be mapped onto the framework by stating how and in what way the specific system meets the given framework.

Part II

Cryptographic Primitives and Schemes

Chapter 4

Primitives

This chapter is about basic cryptographic building blocks, the atoms out of which all other cryptographic constructions are produced. In this section we include basic symmetric key building blocks, such as block ciphers, hash functions and stream ciphers; as well as basic public key building blocks such as factoring, discrete logarithms and pairings. With each of these building blocks there is some mathematical hard problem underlying the primitive. For example the RSA primitive is based on the difficulty of factoring, and the AES primitive is (usually) based on the difficulty of distinguishing it from a keyed pseudo-random permutation. That these problems are hard, or equivalently, the primitives are secure is an assumption which needs to be made. This assumption is often based on the specific parameters, or key lengths, used to instantiate the primitives.

Modern cryptography then takes these building blocks/primitives and produces cryptographic schemes out of them. The de facto methodology, in modern work, is to then show that the resulting scheme, when attacked in a specific cryptographic model, is secure assuming the underlying assumption on the primitive holds. So another way of looking at this chapter and the next, is that this chapter presents the constructions for which we cannot prove anything rigorously, whereas the next chapter presents the schemes which should have proofs relative to the primitives in this chapter actually being secure.

In each section we use the term *observation* to point out something which may point to a longer term weakness, or is purely of academic interest, but which is not a practical attack at the time of writing. In each section we also give a table, and group the primitives within the table in order of security strength (usually).

4.1 Comparison

In making a decision as to which cryptographic mechanism to employ, one first needs to choose the mechanism and then decide on the key length to be used. In later sections and chapters we focus on the mechanism choice, whereas in this section we focus just on the key size. In some schemes the effective key length is hardwired into the mechanism, in others it is a parameter to be chosen, in some there are multiple parameters which affect the effective key length.

There is common understanding that what we mean by an effective key length is that an attack should take 2^k operations for an effective key length of k. Of course this understanding is itself not well defined as we have not defined what an operation is; but as a rule of thumb it

should be the "basic" operation of the mechanism. This lack of definition of what is meant by an operation means that it is hard to compare one mechanism against another. For example the best attack against a block cipher of key length k_b should be equivalent to 2^{k_b} block cipher invocations, whereas the best known attack against an elliptic curve system with group order of k_e bits should be $2^{k_e/2}$ elliptic curve group operations. This often leads one to conclude that one should take $k_e = 2 \cdot k_b$, but this assumes that a block cipher call is about the same cost as an elliptic curve group operation (which may be true on one machine, but not true on another).

This has led authors and standards bodies to conduct a series of studies as to how key sizes should be compared across various mechanisms. The "standard" method is to equate an effective key size with a specific block cipher, (say 112 corresponds to two or three key Triple-DES, 128 corresponds to AES-128, 192 corresponds to AES-192, and 256 corresponds to AES-256), and then try to establish an estimate for another mechanisms key size which equates to this specific quanta of effective key size.

In comparing the different literature one meets a major problem in that not all studies compare the same base symmetric key sizes; or even do an explicit comparison. The web-site `http://www.keylength.com` takes the various proposed models from the literature and presents a mechanism to produce such a concrete comparison. In Table 4.1 we present either the concrete recommendations to be found in the literature, or the inferred recommendations presented on the web site `http://www.keylength.com`.

We focus on the symmetric key size k, the RSA modulus size $\ell(N)$ (which is also the size of a finite field for DLP systems) and the discrete logarithm subgroup size $\ell(q)$; all of which are measured in bits. Of course these are just crude approximations and hide many relationships between parameters which we discuss in future sections. As one can see from the table the main divergence in estimates is in the selection of the size $\ell(N)$ of the RSA modulus.

Table 4.1: Key Size Comparisons in Literature. An entry marked with a $\star$ indicates an inferred comparison induced from the web site `http://www.keylength.com`. Where a range is given by the source we present the minimum values. In the columns k is the symmetric key size, $\ell(N)$ is the RSA modulus size (or finite field size for finite field discrete logarithms) and $\ell(q)$ is the subgroup size for finite field and elliptic curve discrete logarithms.

k	$\ell(N)$	$\ell(q)$	k	$\ell(N)$	$\ell(q)$	k	$\ell(N)$	$\ell(q)$	k	$\ell(N)$	$\ell(q)$	k	$\ell(N)$	$\ell(q)$
Lenstra–Verheul 2000 [369] $\star$														
80	1184	142	112	3808	200	128	5888	230	192	20160	350	256	46752	474
Lenstra 2004 [366] $\star$														
80	1329	160	112	3154	224	128	4440	256	192	12548	384	256	26268	512
IETF 2004 [444] $\star$														
80	1233	148	112	2448	210	128	3253	242	192	7976	367	256	15489	494
SECG 2009 [520]														
80	1024	160	112	2048	224	128	3072	256	192	7680	384	256	15360	512
NIST 2012 [437]														
80	1024	160	112	2048	224	128	3072	256	192	7680	384	256	15360	512
ECRYPT2 2012 [187]														
80	1248	160	112	2432	224	128	3248	256	192	7936	384	256	15424	512

As one can see, as the symmetric key size increases the size of the associated RSA moduli

needs to become prohibitively large. Ignoring such large value RSA moduli we see that there is surprising agreement in the associated size of the discrete logarithm subgroup q, which we assume to be an elliptic curve group order.

Our implicit assumption is that the above key sizes are for (essentially) single use applications. As a key is used over and over again its security degrades, due to various time-memory tradeoffs. There are often protocol and scheme level procedures to address this issue; for example salting in password hashing or the use of short lived session keys. The same holds true in other situations, for example in [94], it is shown that AES-128 has only 85-bit security if 2^{43} encryptions of an arbitrary fixed text under different keys are available to the attacker.

Very little literature discusses the equivalent block length for block ciphers or the output length of hash functions or MAC functions; since this is very much scheme/protocol specific. A good rule of thumb for hash function outputs is that they should correspond in length to $2 \cdot k$, since often hash functions need to be collision resistant. However, if only preimage or second-preimage resistance is needed then output sizes of k can be tolerated.

The standard [434] implicitly recommends that the MAC key and MAC output size should be equal to the underlying symmetric key size k. However, the work of Preneel and van Oorschot [475, 476], implies attacks on MAC functions requiring $2^{n/2}$ operations, where n is the key size, or the size of the MAC functions internal memory. Their recommendation is that for a MAC function with an n-bit internal memory, a k-bit key and an s-bit output size one should require that $k \geq s$, $k \geq n$, and $n/2 \leq s \leq n$ and with as preferred option $k = n$ and $s = n/2$. The value of s should be selected to make an on-line forgery (that requires many verification attempts) infeasible and the value of k should be chosen to make exhaustive key search (that requires only a few text-MAC pairs but many calculations) infeasible. The value of n should be chosen to put an on-line attack that requires $2^{n/2}$ text-MAC pairs out of reach. For a block cipher with a 128-bit block and a 256-bit key, one has $n = 128$, $k = 256$ and the recommendation is $s = 64 \ldots 128$. For higher security levels, block ciphers with 256 bits would be required; unfortunately no such schemes have been standardized so far. Thus choice of the MAC output size can be very much scheme, protocol, or even system, dependent.

4.2 Block Ciphers

By a block cipher we mean (essentially) a keyed pseudo-random permutation on a block of data of a given length. A block cipher is *not* an encryption scheme, it is a component (in our terminology *primitive*) which goes into making such a scheme; often this is done via a mode of operation. In this section we consider whether a given block cipher construction is secure, in the sense that it seems to act like a pseudo-random permutation. Such a security consideration can never be proven, it is a mathematical assumption, akin to the statement that factoring 3072-bit moduli is hard. The schemes we present in Chapter 5, that use block ciphers, are often built on the assumption that the block cipher is secure in the above sense.

Some cryptanalysists include the resistance against related-key attacks in the security evaluation of a block cipher. We include these results for completeness. Note however that the existence of a related-key attack on a given block cipher does *not* contradict the assumption that the block cipher acts as a pseudo-random permutation. Furthermore, the soundness of security models allowing for related-key attacks is still under investigation.

Generally speaking we feel the minimum key size for a block cipher should be 128 bits; the minimum for the block size depends on the precise application but in many applications (for

example construction of MAC functions) a 128-bit block size should now be considered the minimum. We also consider that the maximum amount of data which should be encrypted under the same key should be substantially smallerthan $2^{n/2}$ blocks, However, as indicated before some short lived cryptograms may warrant smaller block and key sizes in their constructions; but for general applications we advise a minimum of 128 bits.[1] Again, for each primitive we give a short description of state of the art with respect to known attacks, we then give guidelines for minimum parameter sizes for future and legacy use. For convenience these guidelines are summarised in Table 4.2.

Table 4.2: Block Cipher Summary

	Classification	
Primitive	Legacy	Future
AES	✓	✓
Camellia	✓	✓
Serpent	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
Blowfish$^{\geq 80}$-bit keys	✓	✗
DES	✗	✗

4.2.1 Future Use Block Ciphers

AES

The Advanced Encryption Standard, or AES, is the block cipher of choice for future applications [160, 202]. AES is called 128-EIA 2 in LTE. AES has a block length of 128 bits and supports 3 key lengths: 128, 192 and 256 bits. The versions with longer key lengths use more rounds and are hence slower (by 20, respectively 40%).

OBSERVATION: The strong algebraic structure of the AES cipher has led some researchers to suggest that it might be susceptible to algebraic attacks [157, 409]. However, such attacks have not been shown to be effective [146, 372].

For the 192- and 256-bit key versions there are related key attacks [92, 93]. For AES-256 this attack, using four related keys, requires time equivalent to $2^{99.5}$ encryptions and data complexity $2^{99.5}$. The attack works due to the way the key schedule is implemented for the 192- and 256-bit keys (due to the mismatch in block and key size), and does not affect the security of the 128-bit variant. Related key attacks can clearly be avoided by always selecting cryptographic keys independently at random.

A bi-clique technique can be applied to the cipher to reduce the complexity of exhaustive key search. For example in [103] it is shown that one can break AES-128 with $2^{126.2}$ encryption operations and 2^{88} chosen plaintexts. For AES-192 and AES-256 these numbers become $2^{189.7}/2^{40}$ and $2^{254.4}/2^{80}$ respectively.

[1] What substantially means depends on the success probability of the adversary, that is typically about ϵ^2 when $\epsilon \cdot 2^{n/2}$ data blocks are encrypted, where n is the block size in bits; for $\epsilon = 2^{-16}$ one has a probability of 2^{-32}.

Camellia

The Camellia block cipher is used as one of the possible cipher suites in TLS, and unlike AES is of a Feistel cipher design. Camellia has a block length of 128 bits and supports 3 key lengths: 128, 192 and 256 bits [385]. The versions with a 192- or a 256-bit key are 33% slower than the versions with a 128-bit key.

OBSERVATION: Just as for AES there is a relatively simple set of algebraic equations which define the Camellia transform; this might leave it open to algebraic attacks. However, just like AES such attacks have not been shown to be effective.

The applicability of the bi-clique technique to Camellia has been investigated in [102].

Serpent

Serpent [86] was one of the AES finalist candidates. It is one of the ciphers standardised for SSH [57]. The eSTREAM portfolio stream cipher SOSEMANUK re-uses parts of Serpent in its design. Serpent has been seen to be used in various TLS ciphersuited deployed; but its' use is very limited.

Serpent has a 128-bit block size and supports 128, 192, and 256-bit key lengths. The best attack on Serpent is a key recovery attack that breaks up to 11 of 32 rounds [420]. Owing to the large security margin relative to known cryptanalysis techniques, Serpent was considered to be a conservative choice during the AES competition. However, the large number of rounds also means that software performance is markedly slower than AES.

textOBSERVATION: Due to its 4-bit S-boxes, Serpent has a very simple algebraic representation, more so than AES and Camellia. However, despite speculation to the contrary, algebraic attacks have not shown to be effective against Serpent.

4.2.2 Legacy Block Ciphers

3DES

Comes in two variants; a two key version with a 112-bit key and a three key version with a 168-bit key [438]. The effective key length of three key 3DES is 112 bits and not 168 bits as one would expect. The small block length (64-bits) is a problem in some applications.

OBSERVATION: Due to meet-in-the-middle attacks the security is not as strong as the key length would suggest. For the two key variant the security is $\min(2^{120-t}, 2^{112})$ where 2^t plaintext/ciphertext pairs are obtained [548]. For the three key variant the security is reduced to 2^{112}.

OBSERVATION: For both variants, related-key attacks with complexity 2^{88} are published [462]. For the three-key variant, a trivial related-key attack for the related keys $k_1\|k_2\|k_3$ and $\overline{k_1}\|\overline{k_2}\|k_3$, where $\overline{k}$ is the bitwise complement of k, with complexity of 2^{56} is described in [329].

Kasumi

This cipher [200], a variant of MISTY-1, has a 128-bit key and 64-bit block size. Kasumi is used in 3GPP and called UIA1 in UMTS and A5/3 in GSM.

OBSERVATION: Whilst some provable security against linear and differential cryptanalysis has been established [320], the cipher suffers from a number of problems. A related key attack [88] requiring 2^{76} operations and 2^{54} plaintext/ciphertext pairs has been presented. In [178] a more

efficient related key attack is given which requires 2^{32} time and 2^{26} plaintext/ciphertext pairs. These attacks *do not affect* the practical use of Kasumi in applications such as 3GPP, however given them we do not advise to use Kasumi in further applications.

OBSERVATION: In 2016 an attack with data complexity 2^{64} (the complete codebook) and with a time complexity of 2^{70} has been published on MISTY-1 [46]; it seems not obvious to extend this attack to KASUMI, but this demonstrates that further progress is being made for this type of block cipher.

Blowfish

This cipher [518] has a 64-bit block size, which is too small for some applications and the reason we only advise it for legacy use. It also has a key size ranging from 32- to 448-bits, which we clearly only endorse using at 80-bits and above for legacy applications. The Blowfish block cipher is used in some IPsec configurations.

OBSERVATION: There have been a number of attacks on reduced round versions [321, 486, 551] but no attacks on the full cipher.

4.2.3 Historical (non-endorsed) Block Ciphers

DES

DES has a 56-bit key and 64-bit block size and so is not considered secure by today's standards as exhaustive key search is feasible. The cipher is susceptible to linear [89] and differential cryptanalysis [386].

4.3 Hash Functions

Hash function outputs should be, in our opinion, a minimum of 160 bits in length for legacy applications and 256 bits in length for all new applications. Hash functions are probably the area of cryptography which has had the most attention in the past decade. This is due to the spectacular improvements in the cryptanalysis of hash functions, as well as the subsequent SHA-3 competition to design a replacement for our existing set of functions. Most existing hash functions are in the Merkle–Damgård family, and derive much of their design philosophy from the MD4 hash function; such hash functions are said to be in the MD-X family. This family includes MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1 and SHA-2. Hash functions built from block ciphers, as considered in [276] are not considered in this report.

4.3.1 Future Use Hash Functions

SHA-2

SHA-2 is actually a family of seven algorithms, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256. SHA-224 (resp. SHA-384) is a variant itself of SHA-256 (resp. SHA-512), but just uses a different IV and then truncates the output. SHA 512/224 (resp. SHA512/256(is a variant of SHA-512 that uses a different IV and then truncates the output. Due to our decision of symmetric security lengths of less than 128 being only suitable for legacy applications we denote SHA-224 and SHA412/224 as in the legacy only division of our analysis.

Table 4.3: Hash Function Summary

Primitive	Output Length	Classification Legacy	Future
SHA-2	256, 384, 512, 512/256	✓	✓
SHA-3	256, 384, 512	✓	✓
SHA-3	SHAKE128, SHAKE256	✓	✓
Whirlpool	512	✓	✓
BLAKE	256, 384, 512	✓	✓
RIPEMD-160	160	✓	✗
SHA-2	224, 512/224	✓	✗
SHA-3	224	✓	✗
MD5	128	✗	✗
RIPEMD-128	128	✗	✗
SHA-1	160	✗	✗

Observation: For SHA-224/SHA-256 (resp. SHA-384/SHA-512) reduced round collision attacks 31 out of 64 (resp. 24 out of 80) have been reported [273, 396, 510]. In addition reduced round variants 43 (resp. 46) have also been attacked for preimage resistance [36, 233].

SHA3

The competition organised by NIST to find an algorithm for SHA3 ended on October 2nd, 2012, with the selection of Keccak [217]. In August 2015 the standard FIPS 202 describing SHA3 was released [203]. It contains 4 hash functions: SHA3-224, SHA3-256, SHA3-384 and SHA3-512 as well as the extendable output functions SHAKE128 and SHAKE256. A further standard is planned to describe different uses of SHA-3 beyond simple hashing, for example its use as a MAC function or an authenticated encryption mode. Unlike SHA-1, SHA-2 etc the construcion of SHA-3 is not based on the Merkle-Damgård methodology; instead it is based on the sponge methodology.

Observation: Reduced round collision attacks (4 out of 24) have been reported [171]. For applications that use a secret key as part of the input of a hash function, cube attacks with practical complexity have been shown for up to 6 rounds of Keccak [172].

Whirlpool

Whirlpool produces a 512-bit hash output and is not in the MD-X family; being built from AES style methods, thus it is a good alternative to use to ensure algorithm diversity.

Observation: Preimage attacks on 5 (out of 10) rounds have been given [511], as well as collisions on 5.5 rounds [357], with complexity 2^{120}. In [514] this is extended to 6 rounds, with 2^{481} computation cost. Collision attacks are also given in [514] where eight rounds are attacked with complexity 2^{120}.

4.3.2 BLAKE and BLAKE2

BLAKE [42] was a SHA-3 finalist candidate, proposed in 2008. Its design is based on the ChaCha stream cipher [76], and follows the HAIFA construction. The BLAKE family consists of 4 variants, producing 224, 256, 384 or 512 digest sizes.

BLAKE2 [43] is a tweaked version of BLAKE, proposed in 2012, and is defined in RFC 7693 [504]. It exists in two variants, BLAKE2b (optimized for 64-bit platforms) and BLAKE2s (optimised for 8 to 32-bit platforms), and produces digests of any size between 1-64 bytes and 1-32 bytes respectively. BLAKE2 is known for having very high software performance on many platforms, even compared to deprecated algorithms such as MD5.

BLAKE has seen significant cryptanalysis as part of the SHA-3 contest, and the changes made in BLAKE2 have also been analysed. The best known attacks on BLAKE and BLAKE2 break up to 2.75 (out of 10 or more) rounds of the algorithm [198, 232].

BLAKE2 has seen rapid adoption as an independent alternative to SHA2 and SHA3. It is supported by crypto libraries such as OpenSSL, and is used internally by the Argon2 [91] password-based key derivation algorithm.

4.3.3 Legacy Hash Functions

RIPEMD-160

RIPEMD-160 is classified a legacy hash function as its output length is too small to offer 128-bits of security against birthday collision attacks. More efficient collision attacks have been found on 36 rounds (out of 80) [395] which was later extended to 42 rounds in [397].

4.3.4 Historical (non-endorsed) Hash Functions

MD5

Despite being widely deployed the MD5 hash function should not be considered secure. Collisions can be found within milliseconds on a modern desktop computer. The literature on the collision weakness of MD5 and its impact in various scenarios is wide [371, 513, 537–539]. Preimage resistance can also be broken in time $2^{124.4}$ [512].

RIPEMD-128

Given an output size of 128-bits, collisions can be found in RIPEMD-128 in time 2^{64} using generic attacks, thus RIPEMD-128 can no longer be considered secure in a modern environment irrespective of any cryptanalysis which reduces the overall complexity. Practical collisions for a 3-round variant were reported in 2006, [398]. In [358] further cryptanalytic results were presented which lead one to conclude that RIPEMD-128 is not to be considered secure.

SHA-1

SHA-1 is still in widespread use and was designed to provide protection against collision finding of 2^{80}, it was standardized in NIST-180-4 [422]. However, several authors claim that collisions can be found with a computational effort that is significantly lower [399, 559, 560].

The current best analysis is that of 2^{61} operations[2], reported in [535]. On the other hand explicit collisions for the full SHA-1 have not yet been found, despite collisions for a reduced round variant (75 rounds out of 80) being found [13]. The most recent update on collision search for the SHA-1 compression function can be found in [536].

We no longer recommend SHA-1 even for legacy use. Therefore it is recommended that parties take immediate steps to stop using SHA-1 in legacy applications.

OBSERVATION: The literature also contains preimage attacks on a variant reduced to 45-48 rounds [37, 133].

4.4 Stream Ciphers

Generally speaking stream ciphers should be used with a distinct IV for each message, unless the key is used in a one-time manner (as for example in a DEM construction). Again, for each cipher we give a short description of state of the art with respect to known attacks, we then give guidelines for minimum parameter sizes for future and legacy use. For convenience these guidelines are summarised in Table 4.4. Dedicated stream ciphers offer performance advantages over AES in CTR mode, but historically the science of stream cipher design lags that of block cipher and mode of operation design. Hence, we recommend to use a block cipher in CTR mode (or similar) instead of a dedicated stream cipher where possible.

Table 4.4: Stream Cipher Summary

	Classification	
Primitive	Legacy	Future
HC-128	✓	✓
Salsa20/20	✓	✓
ChaCha	✓	✓
SNOW 2.0	✓	✓
SNOW 3G	✓	✓
SOSEMANUK	✓	✓
Grain 128a	✓	✓
Grain	✓	✗
Mickey 2.0	✓	✗
Trivium	✓	✗
Rabbit	✓	✗
A5/1	✗	✗
A5/2	✗	✗
E0	✗	✗
RC4	✗	✗

[2]The cost has not yet been fully verified experimentally.

4.4.1 Future Use Stream Ciphers

Grain 128a

Grain refers to a family of stream ciphers. The original version was an entrant to the eSTREAM competition [252]; see later for more details under legacy stream ciphers. An updated version of Grain, called Grain 128a, was proposed in [15] and it is this version that we recommend for future use.

HC-128

HC-128 was an entrant to the eSTREAM competition and included in the final eSTREAM portfolio as promising for software implementations [567]. HC-128 uses a 128-bit key together with a 128-bit initialisation vector.

HC-256 uses 256-bit keys and initialisation vectors, is older than HC-128, but was not submitted to the eSTREAM evaluation [566]. We make no recommendation for HC-256 due to the paucity of analysis.

Salsa20/20 and ChaCha

Salsa20/r was an entrant to the eSTREAM competition [79]. It supports key lengths of 128 and 256 bits. The parameter r refers to the number of rounds used. Salsa20/12 was included in the final eSTREAM portfolio as promising for software implementations. The author of Salsa20 recommends to use the full 20 rounds.

The ChaCha stream cipher is a variant on the Salsa20 family. It modifies the Salsa design to obtain a better performance and increased diffusion. The ChaCha stream cipher forms the basis of the finalist BLAKE to the SHA-3 hash function competition. The ChaCha cipher is used within the web browser Chrome.

Observation: Aumasson et al. report an attack on Salsa20/8 requiring 2^{251} encryptions and 2^{31} chosen IVs [41]. This also applies to the ChaCha family but with a higher cost.

SNOW 2.0

SNOW 2.0 comes in 128 and 256-bit key variants. The cipher is included in ISO/IEC 18033-4 [285]

Observation: A distinguishing attack against SNOW 2.0 is theoretically possible [441], but it requires 2^{174} bits of key-stream and work. A related-key attack exists on SNOW 2.0 with 256-bit key [337].

SNOW 3G

SNOW 3G is an enhanced version of SNOW 2.0, the main change being the addition of a second S-Box as a protection against future advances in algebraic cryptanalysis. It uses a 128-bit key and a 128-bit IV. The cipher is the core of the algorithms UEA2 and UIA2 of the 3GPP UMTS system, which are identical to the algorithms 128-EIA1 and 128-EEA1 in LTE.

SOSEMANUK

SOSEMANUK was an entrant to the eSTREAM competition and included in the final eSTREAM portfolio as promising for software implementations [74]. SOSEMANUK supports key lengths from 128 to 256 bits together with a 128-bit initialisation vector. The designers of SOSEMANUK do not claim more than 128 bits of security for any key length.

The literature contains several attacks on SOSEMANUK, none breaking the claim of 128-bit security. An attack requiring only a few words of key stream and with time complexity 2^{176} was shown in [204]. An attack requiring 2^{138} words of key stream and with time complexity 2^{138} was shown in [145, 365].

4.4.2 Legacy Stream Ciphers

Grain v1

After cryptanalysis [75], the first version of Grain was revised to Grain v1 [251]. The Grain v1 version supporting an 80-bit key and a 64-bit initialisation vector was included in the final eSTREAM portfolio as promising for hardware implementations. Grain 128, which is the version of Grain v1 with 128-bit key and 80-bit initialisation vector, is not endorsed. Another 128 bit version called Grain 128a is available.

Mickey 2.0

Mickey 2.0 was evaluated by the eSTREAM competition and included in the final eSTREAM portfolio as promising for hardware implementations [44]. It uses an 80-bit key and an 80-bit initialisation vector. There exists also a scaled-up version Mickey-128 using 128-bit keys and initialisation values, but this version has not been officially evaluated by eSTREAM [44].

Rabbit

Rabbit was an entrant to the eSTREAM competition and included in the final eSTREAM portfolio as promising for software implementations. Rabbit uses a 128-bit key together with a 64-bit IV. Rabbit is described in RFC 4503 and is included in ISO/IEC 18033-4 [285]. In [163] a distinguishing attack on Rabbit is described. The effect of this attack in practice has yet to be quantified, nonetheless we downgraded Rabbit from suitable for future use to only suitable for legacy use.

Trivium

Trivium was an entrant to the eSTREAM competition and included in the final eSTREAM portfolio as promising for hardware implementations. It has been included in ISO/IEC 29192-3 on lightweight stream ciphers [288]. Trivium uses an 80-bit key together with an 80-bit IV.

OBSERVATION: There has been a number of papers on the cryptanalysis of Trivium and there currently exists no attack against full Trivium. Aumasson et al. [40] present a distinguishing attack with complexity 2^{30} on a variant of Trivium with the initialisation phase reduced to 790 rounds (out of 1152). Maximov and Biryukov [389] present a state recovery attack with time complexity around $2^{83.5}$. This attack shows that Trivium with keys longer than 80 bits provides no more security than Trivium with an 80-bit key. It is an open problem to modify

Trivium so as to obtain 128-bit security in the light of this attack; several proposals are being reviewed in the CAESAR competition.

4.4.3 Historical (non-endorsed) Stream Ciphers

A5/1

A5/1 was originally designed for use in the GSM protocol. It is initialised using a 64-bit key and a publicly known 22-bit frame number. The design of A5/1 was initially kept secret until 1994 when the general design was leaked and has since been fully reverse engineered. The cipher has been subject to a number of attacks. The best attack was shown to allow for real-time decryption of GSM mobile phone conversations [53]. As result this cipher is *not* considered to be secure.

A5/2

A5/2 is a weakened version of A5/1 to allow for (historic) export restrictions to certain countries. It is therefore *not* considered to be secure.

E0

The E0 stream cipher is used to encrypt data in Bluetooth systems. It uses a 128-bit key and no IV. The best attack recovers the key using the first 24 bits of 2^{24} frames and 2^{38} computations [376]. This cipher is therefore *not* considered to be secure.

RC4

RC4 comes in various key sizes. Despite widespread deployment the RC4 cipher has for many years been known to suffer from a number of weaknesses. There are various distinguishing attacks [381], and state recovery attacks [390]. (An efficient technique to recover the secret key from an internal state is described in [87].)

An important shortcoming of RC4 is that it was designed without an IV input. Some applications, notably WEP and WPA "fix" this by declaring some bytes of the key as IV, thereby effectively enabling related-key attacks. This has led to key-recovery attacks on RC4 in WEP [556]. When initialised the first 512 output bytes of the cipher should be discarded due to statistical biases. If this step is omitted, then key-recovery attacks can be accelerated, e.g. those on WEP and WPA [523].

Despite statistical biases being known since 1995, SSL/TLS does not discard any of the output bytes of RC4; this results in recent attacks by AlFardan et al. [19] and Isobe et al. [275]. Improved atttacks on RC4 in WPA-TKIP and TLS have been developed by Vanhoef and Piessens [550].

4.5 Public Key Primitives

For each primitive we give a short description of state of the art with respect to known attacks, we then give guidelines for minimum parameter sizes for future and legacy use. For convenience these guidelines are summarised in Table 4.5. In the table we let $\ell(\cdot)$ to denote

the logarithm to base two of a number; a $\star$ denotes some conditions which also need to be tested which are explained in the text.

Table 4.5: Public Key Summary

Primitive	Parameters	Legacy System Minimum	Future System Minimum
RSA Problem	N, e, d	$\ell(n) \geq 1024$, $e \geq 3$ or 65537, $d \geq N^{1/2}$	$\ell(n) \geq 3072$ $e \geq 65537$, $d \geq N^{1/2}$
Finite Field DLP	p, q, n	$\ell(p^n) \geq 1024$ $\ell(p), \ell(q) > 160$	$\ell(p^n) \geq 3072$ $\ell(p), \ell(q) > 256$
ECDLP	p, q, n	$\ell(q) \geq 160$, $\star$	$\ell(q) > 256$, $\star$
Pairing	p, q, n, d, k	$\ell(p^{k \cdot n}) \geq 1024$ $\ell(p), \ell(q) > 160$	$\ell(p^{k \cdot n}) \geq 6144$ if $k = 1, 2$ $\ell(p^{k \cdot n}) \geq 6144$ if $k \geq 3$ $\ell(p), \ell(q) > 256$

4.5.1 Factoring

Factoring is the underlying hard problem behind all *schemes* in the RSA family. In this section we discuss what is known about the *mathematical* problem of factoring, we then specialise to the *mathematical* understanding of the RSA Problem. The RSA Problem is the underlying cryptographic primitive, we are not considering the RSA encryption or signature algorithm at this point. In fact vanilla RSA should *never* be used as an encryption or signature algorithm, the RSA primitive (i.e. the RSA Problem) should only be used in combination with one of the well defined schemes from Chapter 5.

Since the mid-1990s the state of the art in factoring numbers of general form has been determined by the factorisation of the RSA-challenge numbers. In the last decade this has progressed at the following rate RSA-576 (2003) [211], RSA-640 (2005) [212], RSA-768 (2009) [341]. These records have all been set with the Number Field Sieve algorithm [368]. It would seem prudent that only legacy applications should use a 1024-bit RSA modulus going forward, and that future systems should use RSA keys with a minimum size of 3072 bits.

Since composite moduli for cryptography are usually chosen to be the product of two large primes $N = p \cdot q$, to ensure they are hard to factor it is important that p and q are chosen of the same bit-length, but not too close together. In particular

- If $\ell(p) \ll \ell(q)$ then factoring can be made easier by using the small value of p (via the ECM method [315]). Thus selecting p and q such that $0.1 < |\ell(p) - \ell(q)| \leq 20$, is a good choice.
- On the other hand if $|p - q|$ is less than $N^{1/4}$ then factoring can be accomplished by Coppersmith's method [149].

Selecting p and q to be random primes of bit-length $\ell(N)/2$ will, with overwhelming probably, ensure that N is hard to factor with both these techniques.

RSA Problem

Cryptosystems based on factoring are actually usually based not on the difficulty of factoring but on the difficulty of solving the RSA problem. The RSA Problem is defined to be that of

given an RSA modulus $N = p \cdot q$, an integer value e such that $\gcd(e, (p-1) \cdot (q-1)) = 1$, and a value $y \in \mathbb{Z}/N\mathbb{Z}$, find the value $x \in \mathbb{Z}/N\mathbb{Z}$ such that $x^e = y \pmod N$.

If e is too small such a problem can be easily solved, assuming some side information, using Coppersmith's lattice based techniques [147, 148, 150]. Thus for RSA based encryption schemes it is common to select $e \geq 65537$. For RSA based signature schemes such low values of e do not seem to be a problem, thus it is common to select $e \geq 3$. For efficiency one often takes e to be as small a prime as the above results would imply; thus it is very common to find choices of $e = 65537$ for encryption and $e = 3$ for signatures in use. In keeping with the conservative nature of the suggestions in this report we suggest using $e = 65537$ for future systems using RSA signatures.

The RSA private key is given by $d = 1/e \pmod{(p-1) \cdot (q-1)}$. Some implementers may be tempted to choose d "small" and then select e so as to optimise the private key operations. Clearly, just from naive analysis d cannot be too small. However, lattice attacks can also be applied to choices of d less than $N^{0.292}$ [109, 563]. Lattice attacks in this area have also looked at situations in which some of the secret key leaks in some way, see for example [197, 255]. We therefore advise that d is chosen such that $d > N^{1/2}$, this will happen with overwhelming probability if the user selects e first and then finds d. Indeed, if standard practice is followed and e is selected first then d will be of approximately the same size as N with overwhelming probability.

4.5.2 Discrete Logarithms

The discrete logarithm problem can be defined in any finite abelian group. The basic construction is to take a finite abelian group of large prime order q generated by an element g. The discrete logarithm problem is to recover $x \in \mathbb{Z}/q\mathbb{Z}$ from the value $h = g^x$. It is common for the group and generator to be used by a set of users; in this case the tuple $\{\langle g \rangle, q\}$ is called a set of *Domain Parameters*.

Whilst the DLP is the underlying number theoretic problem in schemes based on the discrete logarithm problem, actual cryptographic schemes base their security on (usually) one of three related problems; this is similar to how factoring based schemes are usually based on the RSA problem and not factoring per se. The three related problems are:

- Computational Diffie–Hellman problem: Given g^x and g^y for hidden x and y compute $g^{x \cdot y}$.
- Decision Diffie–Hellman problem: Given g^x, g^y and g^z for hidden x, y and z decide if $z = x \cdot y$.
- Gap Diffie–Hellman problem: Given g^x and g^y for hidden x and y compute $g^{x \cdot y}$, given an oracle which allows solution of the Decision Diffie–Hellman problem.

Clearly the ability to solve the DLP will also give one the ability to solve the above three problems, but the converse is not known to hold in general (although it is in many systems widely believed to be the case).

Finite Field DLP

The discrete logarithm problem in finite fields (which we shall refer to simply as DLP), and hence the Diffie–Hellman problem, Decision Diffie–Hellman problem and gap Diffie–Hellman

problem, is parametrised by the finite field $\mathbb{F}_{p^n}$ and the subgroup size q, which should be prime. In particular this means that q divides $p^n - 1$. To avoid "generic attacks" the value q should be at least 160 bits in length for legacy applications and at least 256 bits in length for new deployments.

For the case of small prime characteristic, i.e. $p = 2, 3$ a new algorithm was presented early 2013 by Joux [312], which runs in time $L(1/4 + o(1))$, for when the extension degree n is composite (which are of relevance to pairing based cryptography). This algorithm was quickly supplanted by an algorithm which runs in quasi-polynomial time by Barbulescu and others [50]. Also in 2013 a series of record breaking calculations were performed by a French team and an Irish team for characteristic two fields, resulting in the records of $\mathbb{F}_{2^{6120}}$ [230] and $\mathbb{F}_{2^{6168}}$ [310]. For characteristic three the record is $\mathbb{F}_{3^{582}}$ [547]. For prime values of n the best result is a discrete logarithm calculation in the field $\mathbb{F}_{2^{809}}$ [114]. All of these results make use of special modification to the function field sieve algorithm [14]. In light of these results no system should be deployed relying on the hardness of the DLP in small characteristic fields. It is for this reason that we impose the condition $\ell(p) > 256$ (resp. $\ell(p) > 160$ for legacy systems) in Table 4.5.

For large prime fields, i.e. $n = 1$, the algorithm of choice is a variant of the Number Field Sieve [227]. The record here is for a finite field $\mathbb{F}_p$ with p a 530-bit prime [340] set in 2007. In light of the "equivalence" between the number field sieve for factoring and that for discrete logarithms our advise is in this case that legacy applications should use a 1024-bit p, and new systems should use a minimum p of 3072 bits.

There has been some work on the case of so-called medium prime fields; fields with p larger than 100 and $1 < n < 100$, see for example [311, 313]. The last few years has seen considerable progress in this aspect of the discrete logarithm problem [49,51,336]. This means that for pairing based systems (see Section 4.5.3), which use such medium prime fields, we now recommend using a bit-size for the finite field which is twice that of what one would choose for the prime field case when a value of n is used which is greater than two.

ECDLP

Standard elliptic curve cryptography (i.e. ECC not using pairings) comes in two flavours in practice, either systems are based on elliptic curves over a large prime field $E(\mathbb{F}_p)$, or they are based on elliptic curves over a field of characteristic two $E(\mathbb{F}_{2^n})$. We denote the field size by p^n in what follows, so when writing p^n we implicitly assume either $p = 2$ or $n = 1$. We let q denote the largest prime factor of the group order and let h denote the "cofactor", so $h \cdot q = \#E(\mathbb{F}_{p^n})$. To avoid known attacks one selects these parameters so that

- The smallest t such that q divides $p^{t \cdot n} - 1$ is such that extracting discrete logarithms in the finite field of size $p^{t \cdot n}$ is hard. This is the so-called MOV condition [400].
- If $n = 1$ then we should not have $p = q$. These are the so-called anomalous curves for which there is a polynomial time attack [515, 522, 531].
- If $p = 2$ then n should be prime. This is to avoid so-called Weil descent attacks [219].

The above three conditions are denoted by $\star$ in Table 4.5. It is common, to avoid small subgroup attacks, for the curve to be chosen such that $h = 1$ in the case of $n = 1$ and $h = 2$ or 4 in the case of $p = 2$. To avoid implementation mistakes in protocols we *strongly* advise

that curves are selected with $h = 1$. Some fast implementations can be obtained when $h = 4$, but when using these protection against small subgroup attacks need to be also implemented.

There are a subclass of curves called *Koblitz curves* in the case of $p = 2$ which offer some performance advantages, but we do not consider the benefit to outweigh the cost for modern processors thus our discussion focuses on general curves only. Some standards, e.g. [199] stipulate that the class number of the associated endomorphism ring must be larger than some constant (e.g. 200). We see *no cryptographic reason* for making this recommendation, since no weakness is known for such curves. If curves are selected at random it is over whelmingly likely that the curve has a large endomorphism ring in any case.

The largest ECDLP records have been set for the case of $n = 1$ with a p of size 109-bits [113], and for $p = 2$ with $n = 109$ [138]. These record setting achievements are all performed with the method of distinguished points [549], which is itself based on Pollard's rho method [470]. To avoid such "generic attacks" the value q should be at least 160 bits in length for legacy applications and at least 256 bits in length for new deployments.

Various standards, e.g. [32, 33, 521] specify a set of recommended curves; many of which also occur in other standards and specifications, e.g. in TLS [98]. Due to issues of interoperability the authors feel that using a curve specified in a standard is best practice. Thus the main choice for an implementer is between curves in characteristic two and large prime characteristic.

Some people have called into question the wisdom of using the curves specified in the standards [32, 33, 521] as they were generated with the help of the NSA. These people make claims that such curves *could* have been *backdoored* in some way. We see no scientific reason to back up such claims, and hence would still recommend the curves in [32, 33, 521] for both legacy and future use. There are however a large number of other curves which have been recommended in the past few years with a number of special properties which implementors may want to consider.

4.5.3 Pairings

Pairing based systems take two elliptic curves $E(\mathbb{F}_{p^n})$ and $\hat{E}(\mathbb{F}_{p^{n \cdot d}})$, each containing a subgroup of order q. We denote the subgroup of order q in each of these elliptic curves by $\mathbb{G}_1$ and $\mathbb{G}_2$. Pairing based systems also utilise a finite field $\mathbb{F}_{p^{k \cdot n}}$, where q divides $p^{k \cdot n} - 1$. These three structures are linked via a bilinear mapping $\hat{t} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, where G_T is the multiplicative subgroup of $\mathbb{F}_{p^{k \cdot n}}$ of order q. The value k is called the embedding degree, and we always have $1 \leq d \leq k$. Whilst there are many hard problems on which pairing based cryptography is based, the most efficient attack is almost always the extraction of discrete logarithms in either one of the elliptic curves or the finite field (although care needs to be taken with some schemes due to the additional information the scheme makes available).

Given our previous discussion on the finite field DLP and the ECDLP the parameter choices for legacy and new systems are immediate. In addition, note that the conditions in Table 4.5 for pairings immediately imply all the special conditions for elliptic curve based systems indicated by a $\star$ in the ECDLP row. This explains the lack of a $\star$ in the pairing row of Table 4.5.

4.6 Key Size Analysis

Providing key sizes for long term use is somewhat of a hit-and-miss affair, for a start it assumes that the algorithm you are selecting a key size for is not broken in the mean time. So in providing key sizes for specific application domains we make an *implicit* assumption that the primitive, scheme or protocol which utilises this key size is not broken in the near future. All primitives and schemes marked as suitable for future use in this document we have confidence will remain secure for a significant period of time.

Making this assumption still implies a degree of choice as to key size however. The AES block cipher may remain secure for the next fifty years, but one is likely to want to use a larger key size for data which one wishes to secure for fifty years as opposed to, say, five years. Thus in providing key size guidelines we make two distinct cases for schemes relevant for future use. The first case is for security which you want to ensure for *at least* ten years (which we call *near term*), and secondly for security for thirty to fifty years (which we call *long term*). Again we reiterate these are purely key size guidelines and they do not guarantee security, nor do they guarantee against attacks on the underlying mathematical primitives.

In Table 4.6 we present our explicit key size guidelines. The reader will see that we have essentially followed the NIST equivalence [437] between the different key sizes. However, these key sizes equivalences need to be understood to apply only to the "best in class" algorithm for block ciphers, hash function, RSA parameters, etc. It is clearly possible for a block cipher of 128-bits security to not offer 128-bit security due to cryptanalytic attacks.

We have focused on 128-bit security in this document for future use guidelines; clearly this offers a good long term security guarantee. It is plausible that similar advise could be made at (say) the 112-bit security level (which would correspond to roughly 2048-bit RSA keys). The line has to be drawn somewhere and there is general agreement this should be above the 100-bit level; whether one selects 112 bits or 128 bits as the correct level is a matter of taste. Due to the need to protect long term data we have taken the conservative choice and settled on 128 bits; with a higher level for very long term use.

Table 4.6: Key Size Analysis. A * notes the value could be smaller due to specific protocol or system reasons, the value given is for general purposes.

			Future System Use	
	Parameter	Legacy	Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size*	m	80	128	256
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(p^{k \cdot n}) \geq$	1024	6144	15360
	$\ell(p), \ell(q) \geq$	160	256	512

Note, in the case of MAC output size the value given is one needed to protect against a brute force preimage finding. However, in many applications MACs are short lived authen-

tication tokens, and thus one only needs to protect against a much less powerful adversary, or even only to a statistical level of security. Thus in many applications a MAC output size of 48 bits (say) suffices. See Section 5.3.1 for a more detailed discussion of the use of small output sizes in MACs.

As key sizes are not a good measure of security on their own, and because the underlying performance costs of larger keys, at the time of writing the *guidelines for future use* can be summarised in the following simple choices:

1. Block Ciphers: For near term use we advise AES-128 and for long term use AES-256.
2. Hash Functions: For near term use we advise SHA-256 and for long term use SHA-512 and SHA-3 with a 512-bit result.
3. Public Key Primitive: For near term use we advise 256-bit elliptic curves, and for long term use 512-bit elliptic curves.

Note, that all of our guidelines need to be read given the aspects described in Section 2.4 which we do not cover in this report.

4.6.1 Post-Quantum Security

We note that the guidelines above, and indeed all analysis in this document, is on the basis that there is no breakthrough in the construction of quantum computers. If the development of quantum computers became imminent, then all this document's guidelines would need to be seriously reassessed.

In the case of symmetric primitives the usual rule of thumb would be to double the key length, i.e. instead of using 128-bit AES use 256-bit AES, due to Grovers' algorithm. However, this is overly symplistic. This rule of thumb assumes that one could build a quantum computer with sufficiently large depth. In practice early quantum computers are likely to be of limited depth, and hence a direct application of Grovers' algorithm to symmetric key search is likely to be infeasible.

It is often said that most number theoretic primitives (RSA, ECC) will also be rendered instantly insecure. Here the circuits required to break these primitives may be far too large for early quantum computers should they ever be built. In [491] the authors estimate the number of Q-bits and quantum Toffoli gates needed to break RSA and ECC at different key sizes. In terms of our recommendations for near and long term use these numbers are:

Scheme	Key Size	# Qubits	# Toffoli Gates
RSA	3072	6146	$5.2 \cdot 10^{12}$
ECC	256	2330	$1.26 \cdot 10^{10}$
RSA	15360	30722	$2.87 \cdot 10^{15}$
ECC	521	4719	$1.14 \cdot 10^{12}$

Hence we see that it *may* be the case that RSA is more secure than ECC in the early days of quantum computing, especially if large Qubit computers with large numbers of Toffoli gates are not immediately viable.

Chapter 5

Basic Cryptographic Schemes

As mentioned previously, a cryptographic scheme usually comes with an associated security proof. This is most often an algorithm which takes an adversary against the scheme in some well-defined model, and turns the adversary into one which breaks some property of the underlying primitive (or primitives) out of which the scheme is constructed. If one then believes the primitive to be secure, one has a strong guarantee that the scheme is well designed. Of course other weaknesses may exist, but the security proof validates the basic design of the scheme. In modern cryptography all schemes should come with a security proof.

The above clean explanation however comes with some caveats. In theoretical cryptography a distinction is made between schemes which have proofs in the *standard model* of computation, and those which have proofs in the *random oracle model*. The random oracle model is a model in which hash functions are assumed to be idealised objects. A similar issue occurs with proofs using idealised groups (the so-called *generic group model*), or idealised ciphers (a.k.a. the *ideal cipher model*). In this document we take a pragmatic view: a scheme with a proof in the random oracle model is better than one with no proof, and the use of random oracles and other idealised objects can be justified if they produce schemes that have performance advantages over schemes which have proofs in the standard model.

In Tables 5.1, 5.2, 5.4 and 5.5 we present our summary of the various symmetric and asymmetric schemes considered in this document. In each scheme we assume the parameters and building blocks have been chosen so that the guidelines of Chapter 4 apply.

5.1 Key Seperation

It is sometimes tempting for an implementer to use the same key for different purposes. For example, a symmetric AES key might be used as both the key to an application of AES in an encryption scheme, and also for the use of AES within a MAC scheme, or within different modes of operation [223]. As another example one can imagine using an RSA private key both as a decryption key and as a key to generate RSA signatures; indeed this latter use-case is permitted in the EMV chip-and-pin system [165]. Another example would be to use the same encryption key on a symmetric channel between Alice and Bob for two-way communication, i.e. using one bidirectional key as opposed to two unidirectional keys. Such usage can often lead to unexpected system behaviour, thus it is good security practice to design into systems explicit *key separation*.

Key separation means we can isolate the systems dependence on each key and its usages;

indeed, many security proofs implicitly assume that key separation is being adopted. However, in some *specific* instances one can show, for specific pairs of cryptographic schemes, that key separation is not necessary. We do not discuss this further in this document but refer the reader to [26, 165, 454], and simply warn the reader to violate the key separation principle with extreme caution. In general key separation is a good design principle in systems, which can help to avoid logical errors in other system components. If key separation is not adopted then we advise this is only done following a rigorous analysis, and associated security proofs.

5.2 Block Cipher Basic Modes of Operation

In this section we detail the main modes of operation for using a block cipher as a symmetric encryption scheme. Note that we leave a discussion of schemes which are secure against chosen-ciphertext attacks (IND-CCA) until Section 5.4; this section is about chosen-plaintext secure (IND-CPA) schemes only. As such *all* schemes in this section need to be used with extreme care in an application, and are recommended only for legacy applications. If used within a new application, then justification must be provided as to why an authenticated encryption scheme is not suitable. Further technical discussion and comparison on the majority of modes stated here can be found in [496].

Many modes make use of either a nonce or a random IV. A *nonce* is a non-repeating value which is not necessarily random, such as a non-repeating sequence number. In contrast, a random IV must be generated independently and uniformly at random, and be unpredictable to the adversary.

Table 5.1: Symmetric Key Encryption Summary Table

Scheme	Legacy	Future	Notes
Block Cipher Modes of Operation			
OFB	✓	✗	No padding required
CFB	✓	✗	No padding required
CTR	✓	✗	No padding required
CBC	✓	✗	
ECB	✗	✗	
XTS	✓	✗	
EME	✓	✓	
FFX	✓	✓	
Authenticated Encryption			
Generic Composition	✓	✗	Encrypt-then-MAC, and other variants
CCM	✓	✗	Superseded by EAX
CWC	✓	✗	Superseded by GCM
OCB	✓	✓	
EAX	✓	✓	
GCM	✓	✓	
ChaCha20+Poly1305	✓	✓	

5.2.1 ECB

Electronic Code Book (ECB) mode [428] should only be used to encrypt messages with length at most that of the underlying block size. Keys must be used in a one-time manner, unless the messages are guaranteed to be unique for every encryption, for example via the use of a nonce. Without such restrictions ECB mode provides few security guarantees.

5.2.2 CBC

Cipher Block Chaining (CBC) mode [428] is the most widely used mode of operation. Unless used with a one-time key, an unpredictable and random IV *must* be used for each message; with such a usage the mode can be shown to be IND-CPA secure [61], if the underlying block cipher is secure. With a non-random or predictable IV, CBC mode is insecure. In particular using a nonce as the IV leads to attacks.

The mode is not IND-CCA secure. Adding simple integrity checks does not improve security, and can lead to padding oracle attacks [456, 553, 568]. Applications requiring IND-CCA security must use an authenticated encryption mode. For further details see Section 5.4.

5.2.3 OFB

Output Feedback (OFB) mode [428] produces a stream cipher from a block cipher primitive, using an IV as the initial input to the block cipher and then feeding the resulting output back into the blockcipher to create a stream of blocks. To reduce the latency the stream can be precomputed.

The mode is IND-CPA secure when the IV is random (this follows from the security result for CBC mode). If the IV is a nonce then IND-CPA security is not satisfied. The mode is not IND-CCA secure as ciphertext integrity is not ensured. Applications requiring IND-CCA security must use an authenticated encryption mode (cf. Section 5.4).

5.2.4 CFB

Cipher Feedback (CFB) mode [428] produces a self-synchronising stream cipher from a block cipher. Unless used with a one-time key, an independent and random IV*must* be used for each message; with such a usage the mode can be shown to be IND-CPA secure [21], if the underlying block cipher is secure.

The mode is not IND-CCA secure as ciphertext integrity is not ensured. For applications requiring IND-CCA security an authenticated encryption mode is to be used (cf. Section 5.4).

5.2.5 CTR

Counter (CTR) mode [428] produces a stream cipher from a block cipher primitive, using a counter as the input message to the block cipher and then taking the resulting output as the key stream. The counter (or IV) should be a nonce to achieve IND-CPA security [61]. The scheme is rendered insecure if the counter is repeated.

The mode is not IND-CCA secure as ciphertext integrity is not ensured. For applications requiring IND-CCA security an authenticated encryption mode is to be used (cf. Section 5.4).

5.2.6 XTS

XTS mode [431] is short for *XEX Tweakable Block Cipher with Ciphertext Stealing* and is based on the XEX tweakable block cipher [494] (using two keys instead of one). A tweakable block cipher is a block cipher that accepts an additiona public input string, the tweak; the goal is that for every value of the tweak a new 'independent' block cipher is obtained. The mode was specifically designed for encrypted data storage using fixed-length data units, and was used in the TrueCrypt system.

Due to the specific application of disc encryption the standard notion of IND-CPA security is not appropriate for this setting. It is mentioned in [431] that the mode should provide slightly more protection against data manipulation than standard confidentiality-only modes. The exact notion remains unclear and as a result XTS mode does not have a proof of security. Further technical discussion on this matter can be found in [496, Chapter 6] and [375]. The underlying tweakable block cipher XEX is proved secure as a strong pseudo-random permutation [494].

Due to its "narrow-block" design, XTS mode offers significant efficiency benefits over "wide-block" schemes.

5.2.7 EME

ECB-mask-ECB (EME) mode was designed by Halevi and Rogaway [238] and has been improved further by Halevi [236]. EME mode is designed for the encrypted data storage setting and is proved secure as a strong tweakable pseudo-random permutation. Due to its wide block design it will be half the speed of XTS mode but in return does offer greater security. EME is patented and its use is therefore restricted.

5.2.8 FPE

Format-preserving encryption mode currently covers two submodes, FF1 and FF3 [433]. FF1 (submitted to NIST under the name FFX) was designed by Bellare, Rogaway and Spies as a refinement to the previous FFSEM mode proposed by Spies. FF3 (submitted to NIST under the name BPS) was degigned by Brier, Peyrin, and Stern. These modes are format-preserving, meaning that the cipher maps a string with a specified length and alphabet onto a string within that same format. These modes are tweakable. They use 8-12 invocations of the underlying cipher, so are typically not used for bulk data encryption, but have found application for encryption of structured identifying information, such as payment card or tax id numbers. Parts of FF1 and FF3 are patented.

5.3 Message Authentication Codes

Message Authentication Codes (MAC) are symmetric-key cryptosystems that aim to provide message integrity. The most commonly used designs fall in one of three categories: block-cipher based schemes (detailed in Section 5.3.1), hash function based schemes (Section 5.3.2), and those based on universal hash functions (Section 5.3.3). Before looking at specific constructions we note that a MAC function with security level 2^s should have a key size of at least s bits and an output size of at least s bits; and for a well designed MAC function the output size should be exactly s bits. If we truncate a MAC output length from s to $\epsilon \cdot s$, then the security drops to $2^{\epsilon \cdot s}$ for a well designed MAC function.

Table 5.2: Symmetric Key Based Authentication Summary Table. When instantiating the primitives they should be selected according to our division into legacy and future use to provide the MAC function with the same level of security.

	Classification		
Scheme	Legacy	Future	Building Block
CMAC	✓	✓	Any block cipher as a PRP
EMAC	✓	✓	Any block cipher as a PRP
AMAC	✓	✓	Any block cipher
HMAC	✓	✓	Any hash function as a PRF
UMAC	✓	✓	An internal universal hash function
GMAC	✓	✗	Finite field operations
Poly1305	✓	✗	Finite field operations

5.3.1 Block Cipher Based MACs

Almost all block cipher based MACs are based on CBC-MAC. The essential differences in application arise due to the padding method employed, how the final iteration is performed and the post-processing method needed to produce the final output. The final iteration and post-processing methods impact on the number of keys required by the MAC function. The ISO 9797-1 standard [291] defines four padding methods, three final iteration methods and three post-processing methods, and from these it defines six CBC-MAC algorithms which can be utilised with any cipher; one of which uses a non-standard processing of the first block. Table 5.3 summarises these six algorithms, where H_q is the output of the final iteration, H_{q-1} is the output of the penultimate iteration, D_i is the i padded message block, and K is the block cipher key used for iterations $1, \ldots, q-1$. In schemes that use extra keys K', K'', all keys are derived from a single key in a way specified by the standard. Usually there is no corresponding increase in security if these keys are generated independently.

Table 5.3: The MAC functions defined in ISO 9797-1

ISO 9797-1 Number	First Iteration	Final Iteration	Post Processing	a.k.a
1	$H_1 = E_K(D_1)$	$H_q = E_K(D_q \oplus H_{q-1})$	$G = H_q$	CBC-MAC
2	$H_1 = E_K(D_1)$	$H_q = E_K(D_q \oplus H_{q-1})$	$G = E_{K'}(H_q)$	EMAC
3	$H_1 = E_K(D_1)$	$H_q = E_K(D_q \oplus H_{q-1})$	$G = E_K(D_{K'}(H_q))$	AMAC
4	$H_1 = E_{K''}(E_K(D_1))$	$H_q = E_K(D_q \oplus H_{q-1})$	$G = E_{K'}(H_q)$	-
5	$H_1 = E_K(D_1)$	$H_q = E_K(D_q \oplus H_{q-1} \oplus K')$	$G = H_q$	CMAC
6	$H_1 = E_K(D_1)$	$H_q = E_{K'}(D_q \oplus H_{q-1})$	$G = H_q$	LMAC

We treat here EMAC, AMAC and CMAC, being the most utilised variants. Note that vanilla CBC-MAC is on its own not considered secure, except in very limited circumstances; for example where the message length is pre-pended to the message before applying the MAC function. The choice of keysizes, output sizes and internal memory for a MAC algorithm is a delicate task. The key size k should be determined by the security level, similar to the case

of a block cipher. The output size s is determined by the number of on-line MAC verification attempts that can be made. For a well-designed MAC algorithm the success probability of one attempt is 2^{-s}. This number of attempts is limited by the lifetime of the system, the time it takes to verify a MAC value, the value of a successful attempt and the total number of users (note that it does not depend on the lifetime of the key). One can take specific measures (e.g. an exponential backoff algorithm) to limit the number of verifications. Most iterated MAC functions (including all those described in this section) are vulnerable to an internal collision attack [475,476], that requires $2^{n/2}$ known input-output pairs and about 2^{n-s} chosen input-output pairs, with n the number of internal memory bits (for the CBC-MAC variants described in this section n is the block length of the block cipher). The required value of n depends on how many input-output pairs are generated with a single key. For a security level of k bits, the key size should ideally be chosen equal to k bits, the internal memory $n = 2k$ bits and the output size $s = k$. But with some restrictions in place on the number of text-MAC pairs generated with a single key and with restrictions on the number of MAC verficiation attempts, one could also accept $n = k/2$ and $s = k/2$ or even $3k/8$. For example with AES-256 one could accept $k = 256$, $n = 128$ and $s = 96$: one would authenticate with a single key up to 2^{48} messages and one would verify up to 2^{64} text-MAC pairs, each with a success probability of 2^{-96}. In both cases the success probability of the attack per user is limited to 2^{-32}. If a higher security level would be required, a block cipher with a larger block length (192 or 256 bits) would be needed; no such block cipher has been standardized so far.

EMAC

The Algorithm was introduced in [460] and is specified as Algorithm 2 in ISO-9797-1 [291]. As with all block cipher modes of operation, there are known attacks against the scheme that require $2^{n/2}$ MAC operations, where n is the block size. For a variant of the scheme that uses two independent keys, provable security guarantees have been derived in [460,464]. Note however that the security of the scheme is bounded by 2^k, where k is the length of a single key. There are no known guarantees for the version where the two keys are derived from a single key in the way specified by the standard. The function LMAC obtains the same security bounds as EMAC but uses one fewer encryption operation; the proof for EMAC is also valid for LMAC.

AMAC

The algorithm was introduced in [28] and is specified as Algorithm 3 in ISO 9797-1 [291]. The algorithm is known as ANSI Retail MAC, or just AMAC for short, and is deployed in banking applications with DES as the underlying block cipher. As with all block cipher modes of operation, there are known attacks against the scheme that require $2^{n/2}$ MAC operations, where n is the block size. A disadvantage of AMAC is that an internal collision not only leads to forging a MAC but also to efficient key recovery.

CMAC

The CMAC scheme was introduced in [299] and standardized as Algorithm 5 in [291]. It enjoys provable security guarantees under the assumption that the underlying block-cipher is a PRP [411]. In particular this requires frequent rekeying; for example when instantiated with AES-128 existing standards recommend that the scheme should be used for at most 2^{48}

messages. After 2^{48} messages, the probability of an internal collision is 2^{-32}; if such a collision is found an internal key is recovered and forgeries become possible. Furthermore, the scheme should only be used in applications where no party learns the enciphering of the all-0 string under the block-cipher underlying the MAC scheme. (This is a problem if Key Check Values as defined in ANSI X9.24-1:2009 [29] are used.)

5.3.2 Hash Function Based MACs

HMAC

The HMAC scheme[1] was introduced in [128] and standardized in [292, 349, 424]. The construction is based on an underlying hash function which, itself, needs to have an iterative design of the Merkle–Damgård form [162, 401]. Provable security results for HMAC aim to establish that HMAC behaves like a PRF [128]. A proof that relies on the pseudo-randomness of the underlying compression-function and does not require collision-resistance requires however a non-uniform model [58]; the value of such a proof is criticised in [139] as this requires much stronger assumptions than what is typically verified by cryptanalysts. It remains an open problem whether instantiations of HMAC with compression functions that are not collision-resistant are stll reasonably secure, provided that the collision attacks do not yield distinguishing attacks against the pseudo-randomness of the underlying compression function. HMAC-MD4 should therefore not be used while HMAC-SHA1, HMAC-MD5 are still choices for which forgeries cannot be made. However, we do not propose usage with MD5 even for legacy applications and use with SHA-1 is proposed with the usual caveats mentioned before. Conservative instantiations should consider HMAC-SHA-2 and HMAC-SHA-3. New and more efficient MAC functions derived from SHA-3 are under development.

5.3.3 MACs Based on Universal Hash functions

A universal hash function is actually a family of hash functions [136]. The properties of a universal hash function are defined over the distribution of all hash functions in the family. This means that it becomes possible to define a property like *collision probability* in a mathematically meaningful way: The probability that two inputs give a collision is defined as the fraction of functions in the family for which two inputs result in the same output.

Universal hash functions can be used in MAC constructions with provable security properties. A hash function from the family is fixed, and then on each invocation of the hash function a one-time (or pseudo-random) pad is added to the output. This effectively means that on each invocation, a new hash function is defined in a way that is unpredictable by the attacker. In cryptographic applications, this is typically achieved by a combination of a secret key (defining the element of the family) and a non-repeating value or nonce (defining the pad). For some constructions, re-use of the same nonce leads to recovery of the secret key. Many constructions reuse the key of the universal hash function; secret key recovery problems as mentioned above can be avoided by selecting a new hash function key for each message.

[1] The standard ISO 9797-2 specifies three closely related schemes that can be seen as instantiations of NMAC with different parameters.

UMAC

UMAC was introduced in [97] and specified in [354]. The scheme has provable security guarantees [97]. The scheme uses internally a universal hash function for which the computation can be paralellized, which in turn allows for efficient implementations with high throughput. The scheme requires a nonce for each application. One should ensure that the input nonces do not repeat. Rekeying should occur after 2^{64} applications. Due to analysis by Handschuh and Preneel [241], the 32-bit output version results in a full key recovery after a few chosen texts and 2^{40} verifications. This implies one also needs to limit the number of verifications, irrespective of nonce reuse. MAC tags of 64-bits in length should be used in all cases.

GMAC

GMAC is the MAC function underlying the authenticated encryption mode GCM. It makes use of polynomials over the finite field $GF(2^{128})$, and evaluates a message-dependent function at a fixed value. This can lead to some weaknesses, indeed in uses of SNOW 3G in LTE the fixed value is altered at each invocation in a highly similar construction. Without this fix, there is a growing body of work examining weaknesses of the construction, e.g. [241,478,505]. Due to these potential issues we leave the use of GMAC outside of GCM mode in the legacy only division. See the entry on GCM mode below for further comments.

Poly1305

Poly1305 was introduced in [78] as a polynomial-based Wegman-Carter MAC and is used in the authenticated encryption scheme ChaCha20+Poly1305. Since it is a polynomial-based MAC, attacks similar to GMAC can be used [241, 478, 505]. However, the authenticated encryption scheme ChaCha20+Poly1305 rekeys the MAC for every encryption, thereby making the scheme more robust against possible vulnerabilities. Still, unless Poly1305 is rekeyed as done in ChaCha20+Poly1305, we recommend Poly1305 only for legacy use.

5.4 Authenticated Encryption (with Associated Data)

An authenticated encryption (AE) scheme aims to provide both chosen-ciphertext confidentiality (IND-CCA) and ciphertext integrity (INT-CTXT). An authenticated encryption scheme which is for one-time use only is often called a Data Encapsulation Mechanism (DEM).

Authentication Encryption with Associated Data (AEAD) [493] is an extension of AE which allows one to input data which is to be authenticated, but not encrypted, such as header data. All of the modes described in this section are AEAD schemes, with the exception of the generic composition which depends on the exact construction. We first describe generic composition modes, which typically use two independent keys, one for encryption and one for the MAC function. AEAD schemes have a single key for both operations.

5.4.1 Generic Composition (Encrypt-then-MAC)

Generic composition considers how to combine an encryption scheme with a MAC to create an AE scheme. Various ways of combining the two were discussed in [64], including Encrypt-then-MAC. Their conclusion is that Encrypt-then-MAC is the only way one can confidently

combine an encryption scheme with a MAC and achieve security. However, they use syntax which does not align with how encryption schemes and MACs are defined in practice, resulting in the conclusion of the paper occasionally being misinterpreted.

The result of [64] says the Encrypt-then-MAC method is secure if the encryption scheme is a *probabilistic* IND-CPA scheme and the MAC function is UF-CMA secure. The ISO 19772 standard builds an Encrypt-then-MAC scheme from a nonce-based encryption scheme (one which is not IND-CPA) and then appeals to [64] to claim security. The key difference is that (say when using CBC or CTR mode) the IV is not authenticated. This was pointed out in [410], and changes are being made to the ISO standard to correct this bug.

Other related constructions, such as Encrypt-and-MAC or MAC-then-Encrypt, in general *should not* be used as various real world attacks have been implemented on systems that use these insecure variants; for example SSL/TLS uses MAC-then-Encrypt and in such a configuration suffers from an attack [20]. Methods such as MAC-then-Encrypt can be shown to be secure in specific environments and with specific components (i.e. specific underlying IND-CPA encryption scheme and specific underlying MAC), see [350]. However, the probability of an error being made in the choice, implementation or application is too large to enable safe usage. For these reasons, we keep generic composition and all its variants in the legacy category.

Further details on how IV and nonce-based constructions of this type may be composed securely can be found in the paper by Namprempre et al. [410].

5.4.2 OCB

Offset Codebook (OCB) mode [287] was proposed by Rogaway et al. [498]. The mode's design is based on Jutla's authenticated encryption mode, IAPM. OCB mode is provably secure assuming the underlying block cipher is secure. OCB mode is a one-pass mode of operation making it highly efficient. Only one block cipher call is necessary for each plaintext block, with an additional two calls needed to complete the whole encryption process.

The adoption of OCB mode has been hindered due to two U.S. patents. As of January 2013, one of the designers has stated that OCB mode is free for software usage under a GNU General Public License, and for other non-open-source software under a non-military license [497].

5.4.3 CCM

CCM mode standardized by NIST [429] was proposed in [562] and essentially combines CTR mode with CBC-MAC, using the same block cipher and key. The mode is defined only for 128-bit block ciphers and is adopted in the 802.11i standard. A proof of security was given in [307], and a critique was given in [500].

The main drawback of CCM mode comes from its inefficiency. Each plaintext block implies two block cipher calls; the CTR mode allows for parallelization, but the CBC-MAC mode does not. Secondly, the mode is not "online", as a result the whole plaintext must be known before encryption can be performed. An online scheme allows encryption to be performed on-the-fly as and when plaintext blocks are available. For this reason (amongst others) EAX mode is now preferred over CCM mode, and we recommend CCM only for legacy applications.

5.4.4 EAX

EAX mode [287] was presented in [68], where an associated proof of security was also given. It is very similar to CCM mode, also being a two-pass method based on CTR mode and CBC-MAC but with the advantage that both encryption and decryption can be performed in an online manner.

5.4.5 CWC

Carter-Wegman + Counter (CWC) mode was designed by Kohno, Viega and Whiting [347]. As the name suggests it combines a Carter-Wegman MAC, to achieve authenticity, with CTR mode encryption, to achieve privacy. It is provably secure assuming the IV is a nonce and the underlying block cipher is secure. Care should be taken to ensure that IVs are never repeated otherwise forgery attacks may be possible. When considering whether to standardise CWC mode or GCM, NIST ultimately chose GCM. As a result GCM is much more widely used and studied, and we recommend CWC only for legacy applications.

5.4.6 GCM

Galois/Counter Mode (GCM) [430] was designed by McGrew and Viega [393, 394] as an improvement to CWC mode. It again combines Counter mode with a Carter-Wegman MAC (the GMAC algorithm), whose underlying hash function is based on polynomials over the finite field $GF(2^{128})$. This operation is supported by modern processors (e.g., the PCLMULQDQ instruction on Intel processors). GCM is widely used and is recommended as an option in the IETF RFCs for IPsec, SSH and TLS. The mode is online, is fully parallelisable and its design facilitates efficient implementations in hardware.

Iwata et al. show that the original security proof of the GCM scheme is flawed [300]; they provide a corrected proof assuming that the IV is a nonce and the underlying block cipher is secure; note that the results in quantitatively weaker security guarantees. Repeating IVs lead to key recovery attacks [241, 309]. Joux [309] also demonstrated a problem in the NIST specification of GCM when non-default length IVs are used. Ferguson's [308] critique highlights a security weakness when short authentication tags are used. To prevent attacks based on short tags it is wise to insist that authentication tags have length at least 96 bits. Furthermore it is wise to also insist that the length of nonces is fixed at 96 bits. Weak keys of GCM have been identified by Handschuh and Preneel [241], Saarinen [505], and Procter and Cid [478]. The latter work discusses the significance of weak key attacks: they state that although it is highly undesirable for almost every subset of the keyspace to be a weak key class, for many schemes (GCM included) this will not reduce the security to an unacceptable level. Abdelraheem et al. [8] use twisted polynomials to extend this work and present improved forgery attacks.

The conclusion is that GCM is a rather brittle scheme, in the sense that wrong parameter choices or small implementation mistakes can have very strong implications: when deploying GCM, one should carefully check the parameters and implementation details; in particular, one should verify that all the conditions in the annex of [430] are met.

5.4.7 ChaCha20+Poly1305

ChaCha20+Poly1305 is the combination of the stream cipher ChaCha20 with the universal hash function Poly1305 in an Encrypt-then-MAC style, much like GCM mode, with the difference being that the authentication key is changed with every encryption. It is described in RFC 7905 [359] and the composition is analyzed in [477]. Because its authentication key is updated with every encryption, it manages to avoid many potential vulnerabilities that are present with GCM.

5.5 Key Derivation Functions

Key Derivation Functions (KDFs) are used to derive cryptographic keys from a source of keying material, such as a shared random strings (in the case of key agreement protocols) or from an entropy source (in the case of key generation). For example they are used to derive keys for use in authenticated encryption schemes from a secret shared random string obtained via some public key encapsulation mechanism. Often they take additional input of a shared info field, which is not necessarily secret.

The idea is that the input keying material to the KDF may reveal some partial information, may not be uniformly generated, may have some statistical bias, etc. The KDF takes such an input and outputs a pseudo-random key. An additional usage is to expand a given cryptographically strong key into multiple keys. Thus KDFs act both as a randomness extractor as well as an expander. See [351] for a extensive discussion on the extract-then-expand approach to KDF design; and HKDF in particular.

In security proofs KDFs are often modelled as random oracles. We emphasise that simply instantiating these random oracles with vanilla hash, as often suggested in academic papers, should be avoided. In practice KDFs are specifically designed, each of which is built upon a specific primitive such as a keyed PRF or a hash function. Naturally, when instantiating such a KDF design, the underlying primitive (PRF or hash function) needs to be secure. We summarize the constructions in Table 5.4, where the column "Building Block" refers to the underlying primitive used to create the KDF primitive.

Table 5.4: Key Derivation Function Summary Table. When instantiating the primitives they should be selected according to our division into legacy and future use to provide the PRF function with the same level of security.

Primitive	Classification		Building Block
	Legacy	Future	
NIST-800-108-KDF(all modes)	✓	✓	A PRF
X9.63-KDF	✓	✓	Any hash function
NIST-800-56-KDF-A/B	✓	✓	Any hash function
NIST-800-56-KDF-C	✓	✓	A MAC function
HKDF	✓	✓	HMAC based PRF
IKE-v2-KDF	✓	✓	HMAC based PRF
TLS-v1.2-KDF	✓	✓	HMAC (SHA-2) based PRF
IKE-v1-KDF	✓	✗	HMAC based PRF
TLS-v1.1-KDF	✓	✗	HMAC (MD-5 and SHA-1) based PRF

5.5.1 NIST-800-108-KDF

NIST-SP800-108 [425] defines a family of KDFs based on pseudo-random-functions (PRFs). While PRFs are stronger primitives than MAC functions, most MAC functions have been shown to be PRFs. These KDFs can produce arbitrary length output obtained by repeated application of the PRF. One variant (Counter mode) applies the PRF with the input secret string as key, to an input consisting of a counter and auxiliary data; one variant (Feedback mode) does the same but also takes as input in each round the output of the previous round. The final double pipelined mode uses two iterations of the same PRF (with the same key in each iteration), but the output of the first iteration (working in a feedback mode) is passed as input into the second iteration; with the second iteration forming the output. The standard does not define how any key material is turned into a key for the PRF, but this is addressed in NIST-SP800-56C [436].

5.5.2 X9.63-KDF

This KDF is defined in the ANSI standard X9.63 [33] and was specifically slated for use with elliptic curve derived keys; although this is not important for its application. The KDF works by repeatedly hashing the concatenation of the shared random string, a counter and the shared info. The KDF is secure in the random oracle model, however there are now better designs for KDF's than this one. We still include it for future use however, as there are no reasons (bar the existence of better schemes) to degrade it to legacy only.

5.5.3 NIST-800-56-KDFs

A variant of the X9.63-KDF is defined in NIST-SP800-56A/B, [434,435]. The main distinction is that the hash function is repeatedly applied to the concatenation of the counter, the shared random string and the shared info (i.e. a different order is used). Similar comments apply to its use for future and legacy systems as that made for X9.63-KDF above.

In NIST-SP800-56C [436] a different KDF is defined which uses a MAC function application to obtain the derived key, with a publicly known parameter (or salt value) used as the key to the MAC. This KDF has stronger security guarantees than the hash function based KDFs (in particular it has a security proof that avoids the use of the random oracle model). However, the output length is limited to the output length of the underlying MAC, which can be problematic when deriving secret keys for use in authenticated encryption schemes (e.g. Encrypt-then-MAC) – as these schemes require double length keys. For this reason the standard also specifies a key expansion methodology based on NIST-800-108 [425], which takes the same MAC function used in the KDF, and then uses the output of the KDF as the key to the MAC function to define a PRF.

5.5.4 HKDF, IKE-v1-KDF and IKE-v2-KDF

HKDF, presented in [351] and [352] is a KDF based on the HMAC function. It is the basis of the design of the KDFs specified in [246] and [325] for the IKE sub-protocol of IPsec. In all variants HMAC is first used to extract randomness from the shared random value (i.e. a Diffie–Hellman secret), and then HMAC is used again to derive the actual key material. The IETF considers the Version 1 of the KDF (IKE-v1-KDF) to be obsolete. We can find no public explanation of this decision but we expect this is due to the analysis in [144].

5.5.5 TLS-KDF

This is the KDF defined for use in TLS; it is defined in [168] and [98]. In versions v1.0 and v1.1 of TLS the KDF function is constructed from HMAC-SHA1 and HMAC-MD5: these are used as key derivation functions and their output is exclusive-or'd together. The resulting construction is a PRF sometimes called *HMAC-MD5/HMAC-SHA1*. In TLS v1.2 this PRF is simply HMAC instantiated with SHA-2. In both cases the underlying PRF is used to both extract randomness and for key expansion.

5.6 Generalities on Public Key Schemes

Before using a public key scheme there are some basic operations which need to be performed. We recap on these here as an aide-mémoire for the reader, but do not discuss them in much extra detail.

- **Certification:** Public keys almost always need to be certified in some way; i.e. a cryptographic binding needs to be established between the public key and the identity of the user who owns that key. Such certification usually comes in the form of a digital certificate, produced using a proposed signing algorithm. This is not needed for the identity based schemes which we discuss later.
- **Domain Parameter Validation:** Some schemes, such as those based on discrete logarithms, share a set of a parameters across a number of users; these are often called Domain Parameters. Before using such a set of domain parameters a user needs to validate them to be secure, i.e. to meet the security level that the user is expecting. To ease this concern it is common to select domain parameters which have been specified in a well respected standards document.
- **Public Key Validation:** In many schemes and protocols long term or ephemeral public keys need to be validated. By this we mean that the data being received actually corresponds to a potentially valid public key (and not a potentially weak key). For example this could consist of checking whether a received elliptic curve point actually is a point on the given curve and/or does not lie in a small subgroup. These checks are very important for security but often are skipped in descriptions of protocols and academic treatments.

5.7 Public Key Encryption

Public key encryption schemes are rarely used to actually encrypt messages, they are typically used to encrypt a symmetric key for future bulk encryption. Of the schemes considered below only RSA-PKCS# 1 v1.5 and RSA-OAEP can be considered as traditional public key encryption algorithms. Most public key encryption schemes either deployed or in standards follow the KEM/DEM hybrid encryption paradigm (see Section 5.8). Non-KEM based applications should only be used when encrypting small amounts of data, and in this case only RSA-OAEP is secure.

Table 5.5: Public Key Based Scheme Summary Table

Scheme	Classification Legacy	Future	Notes
Public Key Encryption/Key Encapsulation			
RSA-OAEP	✓	✓	See text
RSA-KEM	✓	✓	See text
PSEC-KEM	✓	✓	See text
ECIES-KEM	✓	✓	See text
RSA-PKCS# 1 v1.5	✗	✗	
Public Key Signature Schemes			
RSA-PSS	✓	✓	See text
ISO-9796-2 RSA-DS2	✓	✓	Message recovery variant of RSA-PSS
PV Signatures	✓	✓	ISO 14888-3 only defines these for a finite field
(EC)Schnorr	✓	✓	See text
(EC)KDSA	✓	✓	See text
XMSS	✓	✓	See text
RSA-PKCS# 1 v1.5	✓	✗	No security proof
RSA-FDH	✓	✗	Issues in instantiating the required hash function
ISO-9796-2 RSA-DS3	✓	✗	Similar to RSA-FDH
(EC)DSA,(EC)GDSA	✓	✗	Weak provable security guarantees
(EC)RDSA	✓	✗	Weak provable security guarantees
ISO-9796-2 RSA-DS1	✗	✗	Attack exists (see notes)

5.7.1 RSA-PKCS# 1 v1.5

This encryption method defined in [466,467] has no modern security proof, although it is used extensively in the SSL/TLS protocol. The scheme is vulnerable to a chosen ciphertext reaction attack[2] [100]. In SSL/TLS the scheme has been modified to mitigate against this specific attack. The weak form of padding can also be exploited in other attacks if related messages and/or a low public exponent are used [150, 153, 249]. Attacks on various cryptographic devices which use this encryption scheme have also been reported [52]. This method of encryption should not be used for any applications, bar the specific use (for legacy reasons) in SSL/TLS. The specific use within modern versions of SSL/TLS has been shown to be provably secure [353], however this usage is *not* forward secure so even usage in SSL/TLS should be phased out as soon as possible. The current draft of the forthcoming TLS 1.3 standards does not include any RSA based key-exchange mode.

5.7.2 RSA-OAEP

Defined in [467], and first presented in [67], this is the preferred method of using the RSA primitive to encrypt a *small* message. The scheme is secure in the random oracle model, i.e. under the assumption that the hash functions used in the scheme behave as random oracles. The proof has also been verified in the Coq theorem proving system [54]. A decryption

[2] A type of chosen ciphertext attack in which the attacker obtains valid/in-valid ciphertext signals as opposed to full decryptions for his chosen ciphertexts.

failure oracle attack is possible [382] if implementations are not careful in uniform error reporting/constant timing. It is good practice to ensure that the hash functions used in the scheme be implemented with SHA-1 for legacy applications and SHA-2/SHA-3 for future applications.

5.8 Hybrid Encryption

The combination of a Key Encapsulation Mechanism (KEM) with a Data Encryption Mechanism (DEM) (both secure in the sense of IND-CCA) results in a secure (i.e. IND-CCA) public key encryption algorithm; and is referred to as a hybrid cipher. This is the preferred method for performing public key encryption of data, and is often called the KEM-DEM paradigm.

Various standards specify the precise DEM to be used with a specific KEM. So for example ECIES can refer to a standardized scheme in which a specific choice of DEM is mandated for use with ECIES-KEM. In this document we allow *any* DEM to be used with *any* KEM, the exact choice is left to the user. Our analysis depends on the security level (legacy or future) we ascribe to the DEM and its constituent parts as well as the particular instantiation of the underlying public key primitive.

5.8.1 RSA-KEM

Defined in [284], this Key Encapsulation Method takes a random element $m \in \mathbb{Z}/N\mathbb{Z}$ and encrypts it using the RSA function. The resulting ciphertext is the encapsulation of a key. The output key is given by applying a KDF to m, so as to obtain a key in $\{0,1\}^k$. The scheme is secure in the random oracle model (modelling the KDF as a random oracle), with very good security guarantees [250, 526]. We assume that the KDF used in the scheme be one of the secure instances overviewed in Section 5.5.

5.8.2 PSEC-KEM

This scheme is defined in [284] and is based on elliptic curves. Under the assumption that the underlying KDF is a random oracle, this scheme is provably secure, assuming the computational Diffie–Hellman problem is hard in the group where the scheme is instantiated. Whilst this gives a stronger security guarantee than ECIES-KEM described below, in that security is not based on gap Diffie–Hellman, the latter scheme is often preferred due to performance considerations. Again it we assume that the KDF used in the scheme be one of the good ones from Section 5.5.

5.8.3 ECIES-KEM

This is the discrete logarithm based encryption scheme of choice. Defined in [33, 284, 520], the scheme is secure assuming the KDF is modelled as a random oracle and if the gap Diffie–Hellman problem is hard (this assumption holds in general elliptic curve groups but sometimes trivially fails in pairing groups). Earlier versions of standards defining ECIES had issues related to how the KDF was applied, producing a form of *benign malleability*, which although not a practical security weakness did provide unwelcome features of the scheme. In instantiations, we assume that the KDF used is a secure one (i.e. one of those described in Section 5.5).

5.9 Public Key Signatures

5.9.1 RSA-PKCS# 1 v1.5

Defined in [466, 467] this scheme has no security proof, nor any advantages over other RSA based schemes such as RSA-PSS below, however it is widely deployed. As such we do not propose that it is used anywhere but in legacy systems.

5.9.2 RSA-PSS

This scheme, defined in [467], can be shown to be UF-CMA secure in the random oracle model [306]. It is used in a number of application, including e-passports.

5.9.3 RSA-FDH

The RSA-FDH scheme hashes the message to the group $\mathbb{Z}/N\mathbb{Z}$ and then applies the RSA (decryption) function to the output. The scheme has strong provable security guarantees [151, 152, 317], but is not wise to use in practice due to the difficulty of defining a suitably strong hash function with codomain the group $\mathbb{Z}/N\mathbb{Z}$. Thus whilst conceptually simple and appealing the scheme is not practically deployable.

One way to instantiate the hash function for an $\ell(N)$ bit modulus would be to use a hash function with an output length of more than $2 \cdot \ell(N)$ bits, and then take the output of this hash function modulo N so as to obtain the pre-signature. This means the full domain of the RSA function will be utilised with very little statistical bias in the distribution obtained. This should be compared with ISO's DS3 below.

5.9.4 ISO 9796-2 RSA Based Mechanisms

ISO 9796-2 [290] defined three different RSA signature padding schemes called Digital Signature 1, Digital Signature 2 and Digital Signature 3. Each scheme supports either full or partial message recovery (depending of course on the length of the message). We shall refer to these as DS1, DS2 and DS3.

Variant DS1 essentially uses the RSA function to encrypt a padded version of the message along with a hash of the message. This variant has been attacked by Coron et al. [154, 155] who show how to carry an attack using a substantial number of chosen text-signature pairs but only to 2^{61} operations rather than 2^{80} operations as desired (the hash function used in the attack is SHA-1, which has a 160-bit result). Using a number of implementation tricks the authors of [155] manage to produce forgeries in a matter of days utilising a small number of machines. Thus this variant should no longer be considered secure.

Variant DS2 is a variation of RSA-PSS which allows partial message recovery. All comments associated to RSA-PSS apply to variant DS2.

Variant DS3 is defined by taking DS2 and reducing the randomisation parameter to length zero. This results in a deterministic signatures scheme which is "very close" to RSA-FDH, but for which the full RSA domain is not used to produce signatures. The fact that a hash image is not taken into the full group $\mathbb{Z}/N\mathbb{Z}$ means the security proof for RSA-FDH does not apply. We therefore do not propose the use of DS3 for future applications.

5.9.5 (EC)DSA

The Digital Signature Algorithm (DSA) and its elliptic curve variant (ECDSA) is widely standardized [32, 423, 520]; and there exists a number of variants including the German DSA (GDSA) [256, 281], the Korean DSA (KDSA) [281, 546] and the Russian DSA (RDSA) [228, 282]. The basic construct is to produce an ephemeral public key (the first part of the signature component), then hash the message to an element in $\mathbb{Z}/q\mathbb{Z}$, and finally to combine the hashed message, the static secret and the long term secret in a "signing equation" to produce the second part of the signature.

All (EC)DSA variants (bar KDSA) have weak provable security guarantees; whilst some proofs do exist, they are in less well understood models (such as the generic group), for example [122]. The reason for this is that the hash function is only applied to the message and not the combination of the message and the ephemeral public key.

The KDSA algorithm uses a hash function to compute the r-component of the signature, a full proof in the random oracle model can be given for this variant [120]. Thus KDSA falls into our category of suitable for future use. KDSA also has a simpler signing equation than DSA, it does not require a modular inversion, however the extra hash function invocation is likely to counterbalance this benefit.

All (EC)DSA variants also suffer from lattice attacks against poor ephemeral secret generation [263, 418, 419]. A method to mitigate against these attacks was officially suggested in [487] (but which was known to be "folklore"), is to derive the ephemeral secret key by applying a PRF (with a default key) to a message containing the static secret key and the message to be signed. This technique needs to be used with extreme caution as the use of a deterministic emphemeral key derivation technique could lead to an implementation open to side-channel analysis.

5.9.6 PV Signatures

ISO 14888-3 [281] defined a variant of DSA signatures (exactly the same signing equation as for DSA), but with the hash function computed on the message and the ephemeral key. This scheme is due to Pointcheval and Vaudeney [469], and the scheme is often denoted as the PV signature scheme[3]. The PV signature scheme can be shown to be provably secure in the random oracle model, and so have much of the benefits of Schnorr signatures. However Schnorr signatures have a simpler to implement signing equation which avoids the use of modular inversions. Whilst only defined in the finite field setting in ISO 14888-3, the signatures can trivially be extended to the elliptic curve setting.

Similarly to (EC)DSA signatures, PV signatures suffer from issues related to poor randomness in the ephemeral secret key. Thus the defences proposed for (EC)DSA signatures should also be applied to PV signatures.

5.9.7 (EC)Schnorr

Schnorr signatures [519], standardized in [282], are like (EC)DSA signatures with two key differences; firstly the signing equation is simpler (allowing for some optimisations) and secondly the hash function is applied to the concatenation of the message and the ephemeral key. This

[3]There is another PV signature scheme which this should not be confused with, due to Pintsov and Vanstone [465], which is a signature scheme with message recovery originally used to secure electronic postal franks.

last property means that Schnorr signatures can be proved UF-CMA secure in the random oracle model [468]. There is also a proof in the generic group model [417]. In addition the signature size can be made shorter than that of DSA. We believe Schnorr signatures are to be preferred over DSA style signatures for future applications.

Just like (EC)DSA signatures, Schnorr signatures suffer from issues related to poor randomness in the ephemeral secret key. Thus the defences proposed for (EC)DSA signatures should also be applied to Schnorr signatures.

5.9.8 XMSS

The eXtended Merkle Signature Scheme (XMSS) is a hash-based signature scheme. Hash-based signatures are constructed solely using a cryptographic hash function. I.e., in contrast to all other schemes mentioned in this section, there is no additional number theoretic assumption involved like factoring or computing discrete logarithms. Hence, if a hash function is chosen that resists attacks using quantum-computers, these schemes are secure even against quantum attacks.

There exist several versions of XMSS. At the time of writing an Internet Draft [265] exists that is supposed to become an RFC soon. It is suggested to use the version of XMSS described in this Draft with the parameters proposed there. The scheme has a tight security reduction [266] from the security properties of the underlying hash function properties.

The proposed parameters in [265] lead to 128-bit quantum and 256-bit classical security for the 256-bit hash functions SHA2-256 and SHAKE128, and 256-bit quantum and 512-bit classical security for the 512-bit hash functions SHA2-512 and SHAKE256. All parameter sets are endorsed for future use.

One important aspect that needs to be mentioned is that XMSS is a stateful signature scheme: the secret signing key changes after every signature. If a secret key state is used twice, XMSS becomes insecure, immediately. We therefore caution that developers have to make sure that reuse of a secret key state never occurs.

Chapter 6

Advanced Cryptographic Schemes

In this chapter we discuss more esoteric or specialised schemes. These include password based key derivation, password based encryption, key-wrap algorithms and identity based encryption. We summarize our conclusions in Table 6.1.

Table 6.1: Advanced Scheme Summary Table

Scheme	Categorisation		Notes
	Legacy	Future	
Password Based Key Derivation			
PBKDF2	✓	?	See text
bcrypt	✓	?	See text
scrypt	✓	?	See text
Key Wrap Algorithms			
KW	✓	✗	No security proof; no associated data
TKW	✓	✗	No security proof; no associated data
KWP	✓	✗	No security proof; no associated data
AESKW	✓	✗	No security proof; inefficient
TDKW	✓	✗	No security proof; inefficient
AKW1	✓	✗	No security proof; no associated data
AKW2	✗	✗	Not fully secure
SIV	✓	✓	See text
Identity Based Encryption			
BB	✓	✓	See text
SK	✓	✓	See text
BF	✓	✗	See text

6.1 Password-Based Key Derivation

Section 5.5 provides details on algorithms to derive cryptographic keys from a secret random string. In many situations the only secret that may be present is a password but due to their low entropy and possibly poor randomness they need to be used with special care and must

not be used directly as cryptographic keys. As a result a special key-derivation function should be used which is designed for this case. Password-Based Key Derivation functions are a very important topic since passwords are still the main mechanism by which humans interact with cryptographic services. There exists some standardisation of these functions by NIST [427], and ISO is currently writing the ISO/IEC 11770-6 standard [280]. Standardization work in this area has also started in the IRTF; the schemes considered there include Argon2 [91] and Balloon [108] (cf. infra).

From 2013 to 2015 the Password Hashing Competition (PHC)[1] has run as an open competition. In addition to (second) preimage resistance and collision resistance, the main security goal is that these hash functions are 'memory hard', that is, it is difficult to speed them up with dedicated hardware. The winner of the PHC is Argon2 [91]. Recent research by Alwen and Blocki [23] has shown that many designs (including Argon2 and Balloon) are asymptotically suboptimal; moreover, there are indications that this result can be extended to fixed memory sizes [24]; it remains an open problem whether it is indeed possible to build faster ASICs and whether better constructions can be found.

As this research is rather recent, we restrict ourselves to older schemes. For all the algorithms we detail below there exists no formal security analysis and so we only give classifications for legacy use at this time. As they are very slow, it is highly unlikely that it is possible to find (second) preimages. While there exists no known vulnerabilities in any of the schemes we do not make any statements as to their future use until more formal provable security results are known.

Given a password derived key a password based encryption algorithm can be obtained by applying a block cipher with the associated key, see [318] for an example of this.

6.1.1 PBKDF2

NIST SP 800-132 [427] standardises the PBKDF2 function, which was first defined in RFC 2898 [318]. PBKDF is based on any secure PRF; in [318] it is defined with HMAC using SHA-1. Additionally, PBKDF2 is defined by an iteration count which specifies the number of times the PRF is iterated. The iteration count is used to increase the workload of dictionary attacks and should be as large as possible whilst ensuring the compute time is not unnecessarily long. A minimum of 1000 iterations was initially proposed, although this is now recommended to be 40000 or higher.

The input to the key-derivation function is the password, a salt and the desired key length. The salt is used to generate a large set of keys for each password. It should be generated with a secure random number generator (cf. Section 3.2) and be at least 128 bits long. The key length should be at least 112 bits.

Despite the ability to adjust the number of iterations it is still possibly to implement dictionary attacks relatively cheaply on ASICs or GPUs. The bcrypt function and scrypt functions provide progressively greater resistance to such attacks due to the respective attacks increasing need for additional RAM.

6.1.2 bcrypt

bcrypt was designed by Provos and Mazières [480]. It is based on the blockcipher Blowfish (cf. Section 4.2.2). bcrypt is more resistant to dictionary attacks than PBKDF2.

[1] `https://password-hashing.net/`

6.1.3 scrypt

scrypt [458] was designed by Percival to create a key derivation function which was much more resistant to dictionary attacks than bcrypt. The scheme was introduced in 2009, and is thus more recent than other schemes. This means that it has not been subject to as much usage and analysis. An asymptotic analysis has been performed by Alwen et al. [25].

6.2 Key Wrap Algorithms

In this section we discuss the main modes of operation for using a block cipher to wrap other keys. This functionality is particularly important for the storage and transmission of symmetric keys. An important consideration when using key wrap, is that the security level of the key wrap is bound by the key length of the key that is used to encrypt. For instance, wrapping an AES-256 key under an AES 128-bit key will reduce the security of the AES-256 key to 128 bits (or less).

The accepted security notion for key wrap is deterministic authenticated encryption. It is related to authenticated encryption (Section 5.4), in particular there is an important (practically relevant) notion of binding associated data with the encrypted key (for example key usage information). The majority of modes for key wrap lack formal analysis. For a detailed discussion of the key wrap security notion and a critique of several key wrap modes, refer to [499].

6.2.1 KW and TKW

The two schemes AES Key Wrap, abbreviated KW, and Triple DEA Key Wrap, abbreviated TKW, are specified in NIST Special Publication 800-38F [432]. RFC 3394 [516] and ISO/IEC 19772 [286] both contain an equivalent specification of AES Key Wrap. The schemes KW and TKW do not natively support associated data.

Both KW and TKW are constructed using two transformations. The first transformation creates a variable input length cipher from the block cipher. The input lengths of the cipher is measured in semi-blocks (with a minimum of three semi-blocks). Thus for key wrap based on AES strings with bit-length a multiple of 64 can be encrypted, whereas for 3DES the input length needs to be a multiple of 32 bits. To encrypt n semi-blocks, $6(n-1)$ blockcipher calls are needed, which is a relatively high overhead. There are no formal results regarding the security of the variable input length cipher.

The second stage is the use of the variable input length cipher to create a deterministic authenticated encryption scheme. For both schemes this is achieved by padding the message with a fixed integrity check value, that is checked upon decryption. This method is has a security reduction proof [499].

Since 3DES should be considered legacy only, so should TKW. KW can be still be used in scenarios where there is no associated data.

6.2.2 KWP

The scheme AES Key Wrap with Padding, abbreviated KWP, is specified in [432] and RFC 5649 [262]. It shares the variable input length cipher from KW, but due to the use of an explicit padding scheme, inputs of any number of bytes are allowed.

6.2.3 AESKW and TDKW

The two key wrap schemes AESKW and TDKW are specified in [27]. They share the variable input length ciphers from KW and TKW, respectively. The padding scheme allows key data of arbitrary bit length. Additionally, the padding scheme natively supports associated data to be authenticated, but it should be noted that for authentication, this data is encrypted it along with the actual payload.

6.2.4 AKW1

The scheme AKW1 is specified in ANSI X9.102 [27] and consists essentially of a SHA1 based padding scheme, followed by two layers of CBC encryption, one with a random IV and one with a fixed IV, where the underlying blockcipher is 3DES. The random IV makes the scheme probabilistic, making classification as an authenticated encryption scheme (without associated data) more accurate than as a key wrap scheme. Even when instantiated with a modern block cipher instead of 3DES, AKW1 should be considered a legacy only construction.

6.2.5 AKW2

The scheme AKW2 is specified in ANSI X9.102 [27] and corresponds to an Encrypt-then-MAC scheme using related keys. For the encryption, CBC mode using TDEA is stipulated, whereas for authentication CBC-MAC is used. The scheme supports associated data and indeed, the first block of associated data is used as initialisation vector for the CBC mode. AKW2 is demonstrably not a secure key wrap scheme [499] and we believe it should not be used.

6.2.6 SIV

Synthetic Initialisation Vector (SIV) authenticated encryption was introduced by Rogaway and Shrimpton [499]. It is a 2-pass mode based on using an IV-based encryption scheme with a pseudo-random function. The pseudo-random function is used to compute a tag that is used both for authentication purposes and as IV to the encryption scheme. SIV is captured by RFC 5297 [245], combining CMAC with AES in counter mode. SIV is provably secure and relatively efficient.

6.3 Identity Based Encryption/KEMs

6.3.1 BF

An identity based encryption (IBE) scheme allows a user to encrypt to a public key consisting of an arbitrary string. This string can be an identity, identifier or more generally any string meaningful to the user. To enable decryption a trusted authority issues decryption keys associated to the strings to users. As such identity based encryption provides a key escrow service by default. The “gold” standard for security is that a scheme should be indistinguishable against an adversary who can request secret keys for arbitrary identities (bar the target one), and can also request decryptions of arbitrary ciphertexts with respect to any identity (bar the target identity). This is the ID-IND-CCA security model.

A lot of advanced encryption functionalities can be built from these ideas; e.g. hierarchical IBE, functional encryption. Many of the more academic schemes are based on the idea of a Water's Hash, which first appeared in [561]. In this paper an IBE scheme which is secure in the standard model is given. No standardized scheme however uses this latter construction.

The Boneh–Franklin IBE scheme [110, 111] is known to be ID-IND-CCA secure in the random oracle model and is presented in the IEEE 1363.3 standard [271]. The scheme is not as efficient as the following two schemes, and it does not scale well with increased security parameters; thus it we only categorise it for legacy use. The underlying construction can also be used in a KEM mode.

6.3.2 BB

The Boneh–Boyen IBE scheme [107] is secure in the standard model under the decision Bilinear Diffie–Hellman assumption, but only in a weak model of selective ID security. However, the scheme, as presented in the IEEE 1363.3 standard [271], hashes the identities before executing the main BB scheme. The resulting scheme is therefore fully secure in the random oracle model. The scheme is efficient, including at high security levels, and has a number of (technical) advantages when compared to other schemes.

6.3.3 SK

The Sakai–Kasahara key construction is known to be fully secure in the random oracle model, and at the same curve/field size outperforms the prior two schemes. The constructions comes as an encryption scheme [141] and a KEM construction [142], and is also defined in the IEEE 1363.3 standard [271]. The main concern on using this scheme is due to the underlying hard problem (the q-bilinear Diffie–Hellman inversion problem) not being as hard as the underlying hard problem of the other schemes. This concern arises from a series of results, initiating with those of Cheon [143], on q-style assumptions.

Part III

Cryptographic Protocols

Chapter 7

General Protocols

In this section we detail some protocol classes, which on their own have been specified in standards but for which we know of no *concrete* implementation. Thus we call them *general* protocols as they essentially specify classes of protocols; some of which are then instantiated in Chapter 8 on Specific Protocols.

For each protocol class we specify a general description, standardization efforts, limitations and then we give technical details.

7.1 Key Establishment

General Description: A key establishment protocol allows two parties to establish shared secret key. There are various properties which may hold in a protocol; for example, one or both parties may end up being authenticated to the other, the protocol may guarantee a random key is output even if one party is compromised, and so on. Authentication of parties is generally obtained by parties holding a *static* public/private key pair, which are used in multiple sessions. Any key pairs used in a specific session are called *ephemeral* keys. An important distinction is between *key transport* where one party generates a key and sends it to the other, and *key agreement* where neither party has full control over the key.

We first discuss key establishment, since this is the one areas in which there has been a rigorous analysis of protocols; with concrete security definitions being given. Despite this, the situation in relation to how these security definitions map onto real world protocols and their usages is still in a state of flux.

Standardization Efforts: The NIST standard [434] (resp. [435]) and the ANSI standards [30,33] (resp. [31]) define methods for general key establishment using discrete logarithm based systems (resp. factoring based systems). The standard [434] introduces a nice taxonomy for such schemes with the notation $C(a, b)$, where $a, b \in \{0, 1, 2\}$. The number a refers to how many of the two parties contribute ephemeral keys to the calculation and the number b refers to how many of the two parties are authenticated by long term public/private key pairs. For example, traditional non-authenticated Diffie–Hellman is of type $C(2, 0)$, where as traditional MQV [363] is of type $C(2, 2)$. The standards also provide various mechanisms for key confirmation.

There are a sequence of standards in the ISO/IEC 11770 series, which mirror the ISO/IEC 9798 series discussed below. The main set (ISO/IEC 11770-2,-3, and -4) detail mechanisms

involving symmetric encipherment techniques [277], public key techniques [278], and weak secrets (such as passwords) [279].

LIMITATIONS: The standards on key establishment mentioned above are very general. It would not be possible to develop interoperable implementations based solely on these standards. The reader should refer to the TLS, IPsec, etc. discussions in Chapter 8 for examples of such protocols in more detail.

TECHNICAL DETAILS: The security of key establishment schemes is somewhat complicated. The traditional security models of Bellare, Rogaway, et al. base security on indistinguishablity of keys [65, 66, 99, 132]. This property is often not satisfied by real world protocols, and in particular by protocols using key confirmation. This issue has started to be treated in a number of works focusing on the TLS protocol (see below). Also discussion of the notion of one-sided authentication in key agreement protocols has only recently been considered in the academic literature [125, 353]. Thus many of the options in these standards cannot be said to have fully elaborated proofs of security which are applicable in general situations. The precise choice of which key agreement scheme to use is therefore highly dictated by the underlying application.

Finally, a crucial requirement which is becoming more important in the real world is that of of *forward secrecy*. A key agreement scheme is said to be forward secure if the compromise of the long term static private key of a party does not compromise the confidentiality of the agreed key for sessions which occurred prior to the compromise of the key. Thus we are ensured that the key agreed now will be secure against any *future* compromise of the static keys.

7.2 Identification and Authentication Protocols

GENERAL DESCRIPTION: Identification protocols enable a party to establish in an online protocol that they are both "live" and the claimed person at the other end of the communication. As such parties have *static* secret or private key whose possession is being verified. This static key may either be associated to the known static public key, or may be a shared secret held between the person verifying their identify and the person proving their identity.

In this work we make no distinction between identification and user authentication; however in some applications (for example those based on biometrics) the distinction is important. In general, in an authentication protocol we are aiming to verify the person against a known *claimed* identity, in an identification protocol the verifier is not given the claimed identity[1] and needs to also output this value. Thus, *identification* means a way of determining who someone is from a given population, whereas *user authentication* means confirming a claimed identity.

Identification and user authentication are closely related to the topic of key establishment. Indeed in the academic key agreement literature these are often treated at the same time, see for example [132]. The reason for this linkage is that key establishment without user identification achieves relatively little; similarly, remote user identification without key establishment is not very useful. In addition, often keys are agreed for the primary purpose of authenticating a subsequent communication without the need to perform expensive public

[1] They know however, for example, that the identifying party claims to have an identity in some given database.

key operations on each communication. However, in terms of applications the usage of identification and authentication techniques have wider impact; for example in access to resources and/or physical settings.

Standardization Efforts: The main standards in this area are the ISO/IEC 9798 series [293–298]. The main set (ISO/IEC 9798-2,-3, and -4) detail mechanisms involving symmetric encipherment (i.e. encrypting a challenge under a secret key as a means of authentication) [294], those involving a cryptographic check function (i.e. applying a MAC function to a challenge as a means of authentication) [295], and those involving a digital signature (i.e. signing a given challenge as a means of authentication) [296].

Limitations: The standards in the ISO/IEC 9798 series are mainly "folklore" and as such their analysis has only recently been performed in the academic literature. Work in the provable security tradition was first performed as early as 2001 [62], despite this the original standards contained numerous problems which were identified in 2011 [55, 56] using the symbolic tradition. See below for an extensive discussion on this point.

Technical Details: The problems identified in [55, 56] were identified using a tool called SCYTHER, which found the weaknesses and determined whether proposed fixes were correct. A related tool called SCYTHER-PROOF was used to produce proof scripts which were then machine-checked using the Isabelle/HOL theorem prover. Various problems were identified including role-mixup attacks, type flaws, and reflection attacks; most of the flaws resulted from poor specification of message formats or crucial missing fields. Thus data intended for one person could be routed to another, or data elements could be interpreted in different ways. The standards have since been revised to take into account the problems identified, but the analysis is a lesson in the importance of applying modern scientific techniques to protocol design as opposed to relying on folklore.

As mentioned the analysis in [55, 56] is purely in the symbolic tradition. Thus we obtain guarantees of correctness and the identification of logical weaknesses. To our knowledge no systematic analysis has been done in the computational tradition; nor has an analysis been conducted as to whether computational soundness results can be applied to the existing symbolic analysis. Clearly some of the protocols in ISO/IEC 9798-2, -3, and -4 have been analysed in the academic literature in a computational manner but this is not documented well, and there is always the issue of problems related to idealisation between the definition in the standard and the definition used in the academic literature.

The standard ISO/IEC 9798-5 [297] details protocols based on zero-knowledge techniques. Due to the difficulty of dealing with these using symbolic methods, these are not analysed in [55, 56]. However, all of the protocols in this standard have appeared in the academic literature with computational proofs of security. All of the basic techniques are based on the ideas behind the Fiat–Shamir identification[2] scheme [208], and the closely related Guillou–Quisquater scheme [231]. In these protocols a user is identified by showing knowledge of some secret value which has been committed in their identifying information (e.g. by showing knowledge of a private key associated to a public key). As well as these "classic" methods the standard also contains the schemes of Girault, Poupard and Stern [221, 473], Girault and Paillés [222], Brandt et al [116] and Mitchell and Yuan [403]. The technique of Girault, Poupard and Stern [221, 473] also appears in ISO/IEC 29192-4 [289], which focuses on lightweight cryptographic techniques..

[2]Note that in this paper the term 'identification' corresponds to what has been defined as 'user authentication' in this chapter.

Despite being based on provably secure protocols there has been (to our knowledge) no analysis as to whether the idealisation process between the specification and the prior analysed protocols is correct, nor whether the protocols as specified are subject to type attacks (since the standardised protocols introduce many fields for various application specific reasons).

Standard ISO 9798-6 [298] examines mechanisms which utilise the need of a human operator to manually transfer a short data string from one device to another, or to manually verify that two short data strings are identical. The standard makes no reference to academic literature, although there is an extensive literature in this space, [45, 224, 316, 360–362, 383, 384, 412, 413, 447, 448, 485, 533, 554].

7.3 Password Authenticated Key Exchange Protocols

General Description: Just like in key-agreement, password-based key exchange protocols (PAKEs) allow two parties to share a key. The difference is that the authentication of the entities involved in the exchange relies on passwords shared between clients and servers (thus reducing the dependence on a PKI). The challenge is to design protocols that are secure against off-line dictionary attacks – attacks where adversaries infer information about the password only from the transcripts of protocol executions. The guarantee one wants is that an adversary cannot impersonate a user except if he successfully guesses a password.

Standardization Efforts: Their has been some standardization of PAKE protocols. But these are usually relatively limited in terms of application areas, being tied to a specific application, or have limited (if any) take up.

Limitations: Despite their intuitive usefulness their has been little take up in the real world of PAKE protocols. One reason, which is often cited for this, is the existence of a general patent on the EKE protocol. It may be useful to note that the patent on the EKE protocol expired in 2011

Technical Details: Syntactically, PAKE protocols fall in two classes, balanced and augmented. In balanced PAKEs the server and the users share passwords, whereas in augmented PAKEs (or verifier-based PAKEs) the server has only a one-way function of the passwords (e.g. a hash of the passwords). The latter are preferable as they offer some degree of security even in face of a complete server breach.

Two types of models are used in the security analysis of these protocols. The model proposed by Bellare, Pointcheval, and Rogaway (henceforth the BPR model) [65] is an indistinguishablity based model that builds on the ideas in [66]. There are two types of simulation based models, one due to Boyko, MacKenzie and Patel (henceforth the BMP model) [115], which in turn build on those of Bellare, Canetti, and Krawczyk [60] and Shoup [526], and one due to Canetti et al. (henceforth the CHKLM model) [131], which builds on the Universal Composability framework [129]. We start with an overview of existent efficient protocols in the Random Oracle Model, with Figure 7.1 summarising the discussion.

The seminal protocol in this area is the Encrypted Key Exchange (EKE) protocol of Bellovin and Merritt [71], followed by an augmented version [72]. The security of the protocol had been first analysed by Bellare et al. [65] but the analysis relies on the strong ideal cipher model. Slight variations that aim to preserve the efficiency of the protocol but reduce the assumptions needed in the proof have later been provided [118, 119]. The most efficient protocol that resulted from this line of work is the SPAKE protocol due to Abdalla and

Pointcheval [6]; the protocol has a security analysis in the random oracle model.

The SPEKE and B-SPEKE protocols proposed by David Jablon [301, 302] were two of the first proposed protocols following the publication of EKE. MacKenzie provides an analysis of SPEKE in a restricted variant of the BPR model [378] (the mBPR model). In a similar vein Boyko, MacKenzie and Patel [115] proposed PAK and prove it secure in the BMP model assuming the random oracle. They also provide an augmented version called PAK-X.

In contrast to the above protocols, the PACE protocol is one which was designed for a specific application. It was proposed by the German Federal Office for Information Security, and is intended for deployment in machine readable travel documents, and protocol is fully specified in standards, e.g. in [349]. The protocol has a security proof with respect to (a variant) of the BPR model. The proof assumes both random oracles and ideal ciphers [73].

Some other protocols that have gain some traction recently (mainly as IP free alternatives) are J-PAKE [243] and Dragonfly [244]. Claims of security for these protocols are however not supported by fully worked-out proofs.

Figure 7.1: Summary of PAKE in the Random Oracle Model (ROM) and in the Ideal Cipher Model (ICM)

Protocol	Augmented /Balanced	Security Model/Proof	References
EKE	balanced	BPR/ICM	[65, 71]
SPEKE	balanced	mBMP/ROM	[302]
B-SPEKE	augmented	none	[301]
PAK	balanced	BMP/ROM	[115]
SPAKE	balanced	BPR/ROM	[6]
PACE	balanced	mBPR/ROM	[73, 355]
J-PAKE	both	See text	[242, 243]
Dragonfly	balanced	none	[247]

Just like for any other primitive/protocol PAKE protocols secure in the standard model, i.e. ones not using random oracles, are not very efficient; to the point where they are not really practical. A series of works starting with the protocol of Katz, Ostrovsky and Yung [324] and the more general framework of Goldreich and Lindell [226] propose PAKEs that are secure in the standard model. These protocols which include those in [5, 7, 47] but are significantly less efficient than those discussed above.

Chapter 8

Specific Protocols

In this section we detail relatively general protocols for accomplishing various tasks, which can be used, and are, used in multiple application scenarios. Whilst the protocols here were designed for *specific* tasks (for example TLS was designed to secure communication between a browser and a web site) they can, and are, used for other applications.

8.1 TLS

General Description: The TLS protocol (the current version being v1.2) is primarily aimed at securing traffic between an unauthenticated web browser and an authenticated web site, although the protocol is now often used in other applications due in part to the availability (and ease of use) of a variety of libraries implementing TLS. The TLS protocol suite aims to provide a confidential channel rather than simply a key agreement protocol as discussed before in Section 7.1. The protocol is broken up into two phases: A handshake (or key agreement) phase and a record layer encryption phase.

Standardization Efforts: The protocol has been standardised by the IETF in various standards, of which we list just some [98,168–170,391,509]. The genesis of the protocol dates back to SSL v1.0, in 1993, and its current complex state is a symptom of both issues related to backward compatibility and mission creep. The protocol is currently undergoing a major revision so as to produce TLS v1.3.

A complete list of ciphersuites for TLS is listed at the website `http://www.iana.org/assignments/tls-parameters/tls-parameters.xml`. If following the recommendations of this document, the restrictions on the ciphersuites to conform to our future recommendations means this large list becomes relatively small. We provide recommendations on specific ciphersuites, for both the handshake and record layer transport phases, below.

Limitations: Due to the non-systematic development process, the protocol is hard to analyse and easily prone to implementation weaknesses. Below we summarise the latest knowledge in this regard. Care must be taken in long term key generation as a number of TLS implementations have been shown to be weak due to poor random number generation, see [253] and Section 3.2.

Technical Details: The handshake/key agreement phase has now been fairly thoroughly analysed in a variety of works [124, 303, 304, 353, 407]. A major issue in these analyses is the use of the derived key during key confirmation via the `FINISHED` messages.

The handshake/key agreement phase runs in one of essentially two main modes: either RSA-based key transport or Diffie–Hellman key exchange (an option also exists for pre-shared keys). The RSA key transport methodology uses RSA-PKCS#1 v1.5, which as discussed in Section 5.7.1 is not considered secure in a modern sense. However, the use of this key transport methodology has been specifically patched in TLS to avoid the attack described in [100], and a formal security analysis supporting this approach in the TLS context can be found in [353]. This latter analysis shows that key transport in TLS can be made secure (but not forward secure) under a sufficiently strong number theoretic assumption and in the Random Oracle Model. The Diffie–Hellman based key agreement mode is considered much more secure, and offers the benefit of perfect forward secrecy of the agreed key. In both modes the output of the key agreement phase is a so-called pre-master secret.

For the handshake part of the protocol the principle issue is that the RSA signing algorithm in TLS 1.2 is RSA-PKCS# 1 v1.5. Since most certificates issued are certificates on RSA keys, this means that RSA-PKCS# 1 v1.5 is the *default* signing algorithm for use in TLS. As explained in Section 5.9.1 we do not recommend the use of this signature scheme in future systems.

Considering the discrete logarithm or elliptic curve signature variants, one finds that the situation is a little better. The required signature algorithm here is (EC)DSA, which also has no proof of security, bar in the generic group model for the elliptic curve variant. See Section 5.9.5 for more details. Thus for the key negotiation phase one is left to rely on cryptographic schemes which we only recommend for legacy use.

Given these caveats, we recommend the following key exchange methods for legacy use in TLS as they provide forward secrecy

- `TLS_DHE_DSS_WITH_`$\star$,
- `TLS_DHE_RSA_WITH_`$\star$,
- `TLS_ECDHE_ECDSA_WITH_`$\star$,
- `TLS_ECDHE_RSA_WITH_`$\star$,

where $\star$ suffix denotes an underlying record layer encryption method. The only thing which stops us recommending any key exchange methods for future use is the lack of a provably secure public key signature algorithm within the available choices. Of the four choices `TLS_ECDHE_ECDSA_WITH_`$\star$ is probably to be preferred as ECDSA signatures are more likely to be secure in the long run than the RSA method.

In TLS 1.3 it is proposed to remove the key transport (i.e. RSA variant) and only have forward secure key agreement phases. In particular this would mean that long term public keys are only used to provide key authentication and are not used to provide key confidentiality. This change, as well as being good security practice, has been accelerated since summer 2013 due to the Snowden revelations.

During the handshake phase the key to use in the transport layer is derived from the agreed pre-master secret. This derivation occurs in one of two ways, depending on whether TLS 1.2 [170] is used or whether an earlier standard is used (TLS 1.0 [169] and TLS 1.1 [169]). As discussed in Section 5.5.5, the use of TLS-v1.1-KDF should only be used for legacy applications, with the TLS-v1.2-KDF variant being considered suitable for future applications.

The record layer, i.e. the layer in which actual encrypted messages are sent and received, has received extensive analysis. In TLS 1.0 and TLS 1.1 the two choices are either MAC-then-Encode-then-Encrypt using a block cipher in CBC mode or the use of MAC-then-Encrypt using the RC4 stream cipher. Both these forms of the record layer have been shown to be problematic [19, 20, 135, 452, 553]. The main problems here are that the MAC-then-Encode-then-Encrypt construction used in TLS is difficult to implement securely (and hard to provide positive security results about), and that RC4 is, by modern standards, a weak stream cipher. These issues are partially corrected in TLS 1.2 [170] by adding support for Authenticated Encryption, and with GCM mode and CCM mode for TLS being specified in [509] and [391], respectively. Other recent attacks include those by Duong and Rizzo, known as BEAST [179] and CRIME [180]. BEAST exploits the use of chained IVs in CBC mode in TLS 1.0, and CRIME takes advantage of information leakage from the optional use of data compression in TLS. In TLS 1.3 it is proposed that only AEAD methods are used to secure the record layer.

Looking at the record layer protocol (i.e. the algorithms to encrypt the actual data), we see that only the use of Camellia and AES, within a mode such as GCM or CCM, are compatible with the recommendations in earlier chapters. This means at the time of writing we would only recommend the following cipher suites, for the record layer for future (and legacy) use within TLS

- ⋆_WITH_Camellia_128_GCM_SHA256,
- ⋆_WITH_AES_128_GCM_SHA256,
- ⋆_WITH_Camellia_256_GCM_SHA384,
- ⋆_WITH_AES_256_GCM_SHA384,
- ⋆_WITH_AES_128_CCM,
- ⋆_WITH_AES_128_CCM_8,
- ⋆_WITH_AES_256_CCM,
- ⋆_WITH_AES_256_CCM_8.

where the ⋆ prefix denotes an underlying key exchange method.

Given the above discussion it is hard to recommend that TLS 1.0 and TLS 1.1 be used in any new application, and phasing out their use in legacy applications is recommended. It would appear that TLS 1.2 is sufficient for future applications. There is now widespread support for TLS 1.2 in browsers and web servers. All mainstream libraries support it. It is not so widely used in email and other applications.

8.2 SSH

General Description: Secure Shell (SSH) was originally designed as a replacement for insecure remote shell protocols such as telnet. It has now become a more general purpose tool that is used to provide a secure channel between two networked computers for applications such as secure file transfer. In general the host one is connecting to is authenticated, whereas the client is not (although some corporations do insist on client side authentication for SSH usage).

Standardization Efforts: SSHv2 was standardised in a collection of RFCs [570–572] in 2006, other relevant standards are [57, 84, 159, 272, 374, 374]. The original version, SSHv1 has several design flaws and should no longer be used. OpenSSH [443] is one of the most widely used implementations of the protocol. In 2008 it accounted for more than 80% of all implementations, but currently it is not so popular anymore [17]. The transport layer of SSH [572] is responsible for the initial key-exchange, server authentication and, confidentiality and integrity of messages sent on the channel.

Limitations: The main issue with SSH, much like TLS above, is that most of the standard encryption algorithms for the transport layer are not sufficient to ensure complete security. They possess a number of cryptographic weaknesses, which would not exist if the protocol choices had been made more recently. See the following section for a technical discussion on these matters, as well as recommendations going forward.

Technical Details: The key-exchange protocol is based on Diffie–Hellman and host authentication is provided by combining this with a signature. Client authentication is also possible but defined in a separate RFC [570]. Methods for authenticating the client are either using a password, public-key cryptography (DSA, RSA, X.509), an "interactive-keyboard" challenge-response method [159] or the GSSAPI [374] which allows the use of external mechanisms such as Kerberos. Support for the key-exchange methods, `diffie-hellman-group1-sha1` and `diffie-hellman-group14-sha1` is mandated by the RFC [572]. These methods use the Oakley Group 1 (1024-bit prime field) and Oakley Group 14 (2048-bit prime field) [339]. RFC4419 [215] describes a key-exchange method for SSH that allows the server to propose new groups on which to perform the Diffie–Hellman key exchange with the client. RFC4432 [248] specifies a key-transport method for SSH based on 1024-bit and 2048-bit RSA. RFC5656 [534] defines introduces support for Elliptic-Curve Cryptography; detailing support for ECDH and ECMQV.

Williams [565] has performed an analysis of the key-exchange methods in SSH. This work showed that the six application keys (two IV keys, two encryption keys and two integrity keys) generated by the protocol and passed to the next stage of the SSH protocol are indistinguishable from random. The analysis assumes the server's public key is validated through a certificate from some secure public-key infrastructure. The author of [565] notes that if no such certificate is used, then the protocol is vulnerable to attack, unless the client has some other method of verifying the authenticity of a server's public key.

Once keys are established all message are then sent encrypted over the channel using the Binary-Packet Protocol (BPP) [572, Section 6]. This specifies an encryption scheme based on an Encode-then-Encrypt-and-MAC construction using a block cipher in CBC mode or the stream cipher RC4. The encode function specifies two length fields which must be prepended to messages prior to encryption and a padding scheme (for the case of CBC mode). The first length field specifies the total length of the packet and the second gives the total length of padding used. The specification recommends using CBC mode with chained IVs (the last block of the previous ciphertext becomes the IV of the following ciphertext). This has been shown to be insecure by Dai [161] and Rogaway [492]. Albrecht et al. [18] were able to perform plaintext-recovery attacks against SSH (when using CBC mode) by exploiting the use of encrypted length fields. As a result of these attacks we state that CBC mode *should not* be used, even though the CBC scheme in SSH can be patched to resist the attacks. We note that OpenSSH Version 6.2 [443] supports a non-standard version of the BPP for use with CBC mode in an Encrypt-then-MAC construction where length fields are *not* encrypted

but still authenticated. This style of construction would be secure against the Albrecht et al. attack of [18]. This was recently formerly proven in Albrecht et al. [17].

A first formal security analysis of the SSH-BPP was performed by Bellare et al. [63]. As a result of the Albrecht et al. attacks this security analysis was proved to be incomplete and a further security analysis, which more closely matched actual implementations of SSH, was performed by Paterson and Watson [455]. They proved that the Encode-then-Encrypt-and-MAC construction utilising counter mode encryption is secure against a large class of attacks including those of Albrecht et al. We recommend counter mode as the best choice of available cipher in the Encode-then-Encrypt-and-MAC construction when combined with a secure MAC algorithm. The original choice of MAC algorithms specified in RFC4253 was limited to HMAC with either SHA-1 or MD5. We recommend neither of these hash functions for current use. RFC6668 [84] details the use of SHA-2 for HMAC. In addition to the Encode-then-Encrypt-and-MAC construction confidentiality and integrity in SSH may also be provided by GCM encryption as specified in RFC5647 [272]. OpenSSH also has support for ChaCha20 in combination with the Poly1305 MAC algorithm; this is the default algorithm since OpenSSH v6.9. All of the modes available in OpenSSH, except for CTR mode, are analyzed in Albrecht et al. [17]; CTR mode was already analyzed in Paterson and Watson [455].

A complete list of ciphersuites for SSH is listed at the website

`http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xml`.

Based on the recommendations of this document we would only recommend the following encryption and MAC algorithms, for future use within SSH:

- `aes128-ctr` with `hmac-sha2-256` or `hmac-sha2-512`
- `aes192-ctr` with `hmac-sha2-256` or `hmac-sha2-512`
- `aes256-ctr` with `hmac-sha2-256` or `hmac-sha2-512`
- `AEAD_AES_128_GCM`
- `AEAD_AES_256_GCM`

8.3 IPsec

General Description: IPsec is designed to provide security at the IP network layer of the TCP/IP protocol stack. This differs from protocols such as TLS and SSH, above, which provide security at higher layers such as the application layer. This is advantageous since no re-engineering of the applications is required to benefit from the security IPsec provides. The main use of IPsec has been to create virtual private networks (VPNs) which facilitates secure communication over an untrusted network such as the Internet.

The IPsec protocols can be deployed in two basic modes: tunnel and transport. In tunnel mode cryptographic protection is provided for entire IP packets. In essence, a whole packet (plus security fields) is treated as the new payload of an outer IP packet, with its own header, called the outer header. The original, or inner, IP packet is said to be encapsulated within the outer IP packet. In tunnel mode, IPsec processing is typically performed at security gateways

(e.g. perimeter firewalls or routers) on behalf of endpoint hosts. By contrast, in transport mode, the header of the original packet itself is preserved, some security fields are inserted, and the payload together with some header fields undergo cryptographic processing. Transport mode is typically used when end-to-end security services are needed, and provides protection mostly for the packet payload. In either mode, one can think of the IPsec implementation as intercepting normal IP packets and performing processing on them before passing them on (to the network interface layer in the case of outbound processing, or to the upper layers in the case of inbound processing).

Standardization Efforts: The protocol was originally standardised in a collection of RFCs in 1995 and their third incarnation can be found in RFCs 4301–4309 [182, 258, 261, 325, 331–334, 517]. For a more complete description of the cryptography in the IPsec standards we refer the reader to the survey by Paterson [449].

Limitations: The key agreement phase of IPsec, called IKE, is well studied and well defined. As for TLS and SSH the payload encryption algorithms have had a number of issues over the years, related to poor acceptance of the need for AEAD/IND-CCA encryption algorithms. More details are provided in the technical section below.

Technical Details: Each IPsec implementation contains a Security Policy Database (SPD), each entry of which defines processing rules for certain types of traffic. Each entry in the SPD points to one or more Security Associations (SAs) (or the need to establish new SAs). The SAs contain (amongst other information) cryptographic keys, initialisation vectors and anti-replay counters, all of which must be initialised and shared between appropriate parties securely. This can be solved manually, and such an approach works well for small-scale deployments for testing purposes. However, for larger scale and more robust use of IPsec, an automated method is needed. The Internet Key Exchange (IKE) Protocol provides the preferred method for SA negotiation and associated cryptographic parameter establishment. The latest version of IKE, named IKEv2 [326], provides a flexible set of methods for authentication and establishment of keys and other parameters, supporting both asymmetric and symmetric cryptographic methods. There were initially two Diffie–Hellman Groups defined for use in IKEv2 [326, Appendix B], one with a 768-bit modulus the other with 1024-bit modulus. Further DH groups are defined in RFC3526 [339] of sizes 1536, 2048, 3072, 4096, 6144 and 8192 bits. Elliptic Curve groups are defined in RFC 5903 [216] with sizes of 256, 384 and 521 bits. RFC5114 [370] defines an additional 8 groups. Based on Section 4.5 we recommend for future use a group size of at least 3072 bits, and 256 bits in the case of elliptic curve groups. For key derivation, as discussed in Section 5.5.4, the use of IKE-v1-KDF should only be used for legacy applications, with the IKE-v2-KDF variant being considered suitable for future applications.

There are two main IPsec protocols which specify the actual cryptographic processing applied to packets. These are called Authentication Header (AH) and Encapsulating Security Payload (ESP).

AH provides integrity protection, data origin authentication and anti-replay services for packets through the application of MAC algorithms and the inclusion of sequence numbers in packets. There are a number of MAC algorithms defined for use with IPsec. These include HMAC (with MD5 [379], SHA-1 [380] or SHA-2 [327]), GMAC [392] and XCBC (a CBC-MAC variant) [214]. Based on earlier chapters we only recommend HMAC with SHA-2 for future use.

ESP provides similar services to AH (though the coverage of its optional integrity protec-

tion feature is more limited) and in addition provides confidentiality and traffic flow confidentiality services through symmetric key encryption and variable length padding of packets. ESP allows both encryption-only and authenticated encryption modes. The attacks we shall mention in the following paragraph demonstrate the encryption-only modes should *not* be used. ESP must therefore always be configured with some form of integrity protection. The encryption algorithms on offer are CBC mode (with either 3DES [459], AES [213] or Camellia [323]), CTR mode (with either AES [260] or Camellia [323]). Of these algorithms we would only recommend CTR mode and stress it must be combined with a MAC algorithm. Further options for authentication encryption are provided by the combined algorithms CCM (with either AES [261] or Camellia [323]) and GCM with AES [261].

An initial analysis of the IPsec standards was performed by Ferguson and Schneier [206]. This was followed by Bellovin [70] who found a number of attacks against encryption-only ESP. Practical attacks were demonstrated by Paterson and Yau [457] against the Linux implementation of IPsec where encryption-only ESP was operating in tunnel mode. By adapting the padding oracle attack of Vaudenay [553], Degabriele and Paterson were then able to break standards-compliant implementations of IPsec [166] with practical complexities. These attacks were against encryption-only ESP using CBC mode and operating in either tunnel or transport mode. From these attacks, the need to use some form of integrity protection in IPsec is evident. It is therefore recommended that encryption-only ESP *not* be used. A further set of attacks by Degabriele and Paterson [167] breaks IPsec when it is implemented in any MAC-then-Encrypt configuration (for example, if AH in transport mode is used prior to encryption-only ESP in tunnel mode). On the other hand, no attacks are known if ESP is followed by AH, or if ESP's innate integrity protection feature is used. To conclude, we reiterate that ESP should always be used with some form of integrity protection, and that care is needed to ensure an appropriate form of integrity protection is provided.

A close to complete list of ciphersuites for IPsec is listed at the website

`http://www.iana.org/assignments/isakmp-registry/isakmp-registry.xml`.

Based on the recommendations in earlier chapters we would only recommend the following algorithms for future use within IPsec:

- If only authentication is required then either AH or ESP may be used with one of the following MAC algorithms as defined in RFC4868 [327].
  - `HMAC-SHA2-256`,
  - `HMAC-SHA2-384`,
  - `HMAC-SHA2-512`,
- If confidentiality is required then ESP should be used by combining one of the following encryption algorithms with one of the MAC algorithms described above.
  - `AES-CTR`,
  - `CAMELLIA-CTR`,
- Alternatively one of the following combined authenticated encryption modes may be used:
  - `AES-CCM_`$\star$,

- CAMELLIA-CCM_⋆,
- AES-GCM_⋆,

Here ⋆ denotes the size (in bytes) of the integrity check value (ICV) and we recommend choosing either 12 or 16.

8.4 Kerberos

General Description: Kerberos is an authentication service which allows a client to authenticate his or herself to multiple services e.g. a file server or a printer. The system uses a trusted authentication server which will grant tickets to participating parties allowing them to prove their identity to each other. It is primarily based on symmetric-key primitives; the specific construction being derived from the Needham-Schroeder Protocol [415]. Public-key primitives, namely RSA signatures, may also be used during the initial authentication phase [574].

Standardization Efforts: Kerberos was designed as part of project Athena at MIT during the 1980s [402]; the first three versions were not released publicly; Version 4 can therefore be viewed as the "original" release. The current version, Version 5 [416], fixed a number of security deficiencies present in its predecessor [69]. Version 4 required the use of DES; Version 5 expanded the possible ciphers and AES is now supported [482].

Limitations: Again there are issues related to the usage of strong encryption schemes (i.e. AEAD/IND-CCA schemes) due to the age of the documents defining the protocol.

Technical Details: Version 4 made use of a non-standard version of CBC mode called PCBC which has been shown to be insecure [346]. The encryption scheme used by Version 5 has been formally analysed by Boldyreva and Kumar [104], who first show that the Encode-then-Checksum-then-Encrypt construction defined in RFC3961 [483] does not meet the INT-CTXT definition of security. If a secure MAC algorithm is used for the checksum then this construction will be secure. Additionally, Boldyreva and Kumar analyse the Encode-then-Encrypt-and-MAC construction given in RFC3962 [482] and show this to be secure assuming the underlying primitives meet standard definitions of security. The encryption scheme specified for use in Version 5 is CBC mode with ciphertext stealing using either DES, 3DES [483], AES [482] or Camellia [264] as the underlying blockcipher.

A complete list of ciphersuites for Kerberos is listed at the website `http://www.iana.org/assignments/kerberos-parameters/kerberos-parameters.xml`. At the time of writing we recommend the following ciphersuites for future use within Kerberos:

- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`
- `camellia128-cts-cmac`
- `camellia256-cts-cmac`

Chapter 9

Application Specific Protocols

In this chapter we present a quick overview of protocols which are used in relatively restricted application areas; for example wireless, mobile communications or banking.

9.1 WEP/WPA

General Description: The WEP/WPA protocols are used to protect communication in wireless networks; for example in securing the communication between a laptop and the wireless router (a.k.a access point) to which it connects. The key design requirement is to ensure that an eavesdropper is unable to break the confidentiality of the messages being sent. We discuss their use in the setting where the device and the access point to which it connects have a shared key.

Standardization Efforts: WEP (Wired Equivalent Privacy) is specified in the IEEE 802.11 standard [267]. The protocol is intended to offer confidential and authenticated communication. The protocol is symmetric key based (it uses either 40 bit, 104 bit, or 232 bit keys) and employs RC4 for confidentiality and CRC32 for authentication. WPA (Wi-Fi Protected Access) is a successor of WEP. It employs the Temporal Key Integrity Protocol (TKIP) a stronger set of encryption and authentication algorithms; but TKIP has been deprecated by the IEEE. The WPA2 is the latest version of the protocol suite which is described in [268].

Limitations: Practical key-recovery attacks against the WEP protocols have been devised [96, 210, 541] and the protocol is considered completely broken. The use of this protocol should be avoided. WEP has been deprecated by the IEEE. The TKIP protocol was intended as a temporary replacement for WPA, and is capable of running on legacy hardware. The protocol fixes some of the design problems in WEP, but some attacks against TKIP have been found [239, 404, 406, 524, 540, 543]. A recent attack, [451], based on prior analysis of RC4 [19] in TLS, breaks the basic WPA protocol, and thus users should move to WPA2 as a matter of urgency.

Technical Details: The protocol WPA2 uses stronger primitives. It employs the Counter Cipher mode with Message Authentication Code Protocol (CCMP), an encryption scheme that uses AES in CCM mode (see Section 5.4.3) and offers both message confidentiality and message authentication. While some weaknesses in settings where WPA2 is used exist, no serious attacks are known against the protocol itself.

9.2 UMTS/LTE

General Description: The GSM, UMTS and LTE protocols are designed to secure communications between a mobile phone and the operators base station. The goal being to provide confidentiality services for the user and authentication services for the mobile phone operator. The protocols also define what happens when a user "roams" to another service providers network, by for example travelling to another country. In addition the protocols provide a limited form of anonymization of the user, by preventing a passive eavesdropper from linking one communication with another from the same phone.

Standardization Efforts: The Universal Mobile Telecommunication System (UMTS) and its latest version called Long-Term Evolution (LTE) are standards for wireless communication in mobile phones and data terminals. The standard is developed by the 3rd Generation Partnership Project (3GPP) and is now at version 10. The protocol is intended as a replacement for GSM. All technical specification documents referenced in this section are available at `www.3gpp.org`.

Limitations: There are known minor weaknesses in the cryptographic components used in LTE, in particular Kasumi [88] and SNOW 3G [95, 338], but these do not seem to translate into attacks against the secure channel that they implement.

Technical Details: Very roughly, the protocol works in two phases, a key-establishment and authentication phase, and a data transmission phase. Unlike the TLS and IPSec protocols discussed earlier the key establishment and authentication are obtained via symmetric as opposed to public key techniques.

UMTS/LTE replaces the one-way authentication protocol used in GSM (which authenticates the mobile but not the network) with a stronger protocol called Authentication and Key Agreement (AKA). This is a three party protocol that involves a mobile station (MS) a serving network (SN) and the home environment (HE). Upon a succcesful execution of the protocol MS and SN have confirmed that they communicate with valid partners and establish a shared key. An additional design goal for the protocol is to protect the identity of the mobile station: an eavesdropper should not be able to determine weather the same mobile station was involved in two different runs of the protocol.

The key shared between MS and SN is used to implement a bi-directional secure channel between the two parties. Integrity and confidentiality are implemented (respectively) via algorithms UIA1 and UEA1 (in UMTS) [1] and UIA2 and UEA2 (in LTE) [2]. The algorithms have the same structure; the difference is determined by the underlying primitive: the Kasumi blockcipher [4] in UMTS and SNOW 3G streamcipher [3] in LTE.

There are no provable security guarantees for the protocol. The few published analyses for the protocol are mainly concerned with the anonymity guarantees [38, 348] and indicate that the protocol is susceptible to a number of attacks against mobile station confidentiality. Security of the channel established via UMTS/LTE had not been thoroughly analysed.

9.3 Bluetooth

General Description: Bluetooth is technology for exchanging data, securely, over short-distances between up to seven devices. It is often used to connect devices on a body (for example a mobile phone and a headset) or within a vehicle (for example a mobile phone and

the vehicles audio system).

Standardization Efforts: The protocol stack for Bluetooth was originally standardised as IEEE802.15.1 standard, which is no longer maintained. The current development is over seen by the Bluetooth Special Interest Group. We discuss the cryptographic features of Bluetooth 2.1; the later versions (the latest is Bluetooth 4.0) are mainly concerned with improved bandwidth and power efficiency with little changes to the underlying cryptography.

Limitations: See below for issues related to the pairing of devices.

Technical Details: Operating takes place in two stages. In the "pairing" stage, two Bluetooth devices agree on a pair of keys, an initialisation key used for mutual authentication via a challenge response protocol based on HMAC-SHA-256; after authentication succeeds, the devices also agree on a link key for encrypting the traffic. Since Bluetooth 2.1 this stage is implemented with Elliptic Curve Diffie-Hellman (ECDH); depending on the capabilities of the devices involved, several mechanisms for providing protection against man-in-the-middle can be used. Data is encrypted in Bluetooth using streamcipher E0. Each packet is XORed with a keystream obtained by running the E0 algorithm on several inputs, one of which is the key link and another is a unique identifier.

The main weakness of Bluetooth is the pairing phase. Although stronger than in Bluetooth 1.0-2.0, pairing is still open to Man-In-The-Middle attacks for devices without user input/output capabilities or other out-of-band communication means, or in configurations where a predefined PIN is used. As far as confidentiality of the communication goes, the few known theoretical attacks against E0 [209, 254] do not seem to impact confidentiality of messages. Message integrity protection is implemented with a cyclic redundancy code and is therefore minimal.

9.4 ZigBee

General Description: ZigBee is a radio communication standard which can be considered to operate mainly at lower power and ranges than Bluetooth. The key idea is to provide extended ranges by utilising mesh networks of ZigBee connected devices.

Standardization Efforts: The ZigBee protocol suite is defined by the ZigBee Alliance `http://www.zigbee.org/`.

Limitations: There are no known issues with the Zigbee protocols, although we know of no formal analysis of the protocols.

Technical Details: Bulk data encryption and authentication is based on the symmetric key mechanisms of IEEE 802.15.4 [269], and key management is implemented either by active key management with ZigBee-specific uses of ECDSA/ECDH or by predistribution of symmetric keys.

The main confidentiality algorithms are AES in CTR mode, an AES based CBC-MAC algorithm outputting either a 32-bit, 64-bit or 128-bit MAC value, or for combined authenticated encryption the use of AES in CCM mode, or a variant of CCM mode called CCM*. TLS support is provided with two mandatory cipher suites

`TLS_PSK_WITH_AES_128_CCM_8` and `TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8`,

these derive keying material either via symmetric preshared keys or via a elliptic curve Diffie–

Hellman key exchange authenticated with ECDSA respectively. An optional suite of

`TLS_DHE_RSA_WITH_AES_128_CCM_8`

prepares the shared keying material via a finite field Diffie–Hellman exchange authenticated with RSA signatures.

9.5 EMV

General Description: The EMV system defines a "platform" for enabling a chip card to be used in banking applications. Generally this platform is used to implement the chip-and-pin system deployed across much of the world. It is also used in some countries to provide online banking services via the use of a cheap chip-card reader. The EMV system is slated to be rolled out world wide with the adoption in the United States in the next couple of years.

Standardization Efforts: The chip-and-pin bank/credit card system follows a specification defined by EMVCo. Since this report is mainly focused on cryptographic aspects, we will restrict our discussion to the cryptographic components only; which are defined in "EMV Book 2" [192]. A new system is currently in the process of being standardised.

Limitations: There are a number of systems security level issues observed by the Cambridge security group [11, 12, 105, 176, 408].

Technical Details: Much of the existing EMV specification dates from before the advent of provable security; thus many of the mechanisms would not be considered cryptographically suitable for a new system. For example, the RSA based digital signature is DS1 from the standard ISO 9796-2 [290]; in a message recovery mode. As already explained in Section 5.9.4, this scheme suffers from a number of weaknesses, although none have been exploited to any significant effect in the EMV system.

As a second example, the RSA encryption method (used to encrypt PIN blocks in some countries) is bespoke and offers no security guarantees. The only known analysis of this algorithm is in [532], which presents a Bleichenbacher-style attack against this specific usage.

Another issue is that the card is allowed to use the same RSA private key for signing and encryption. This is exploited in [165] via another Bleichenbacher-style attack which converts the decryption oracle provided by the Bleichenbacher-style attack into a signing oracle; in turn, this can be used to forge EMV transaction certificates. It should be stated that none of the above attacks has been shown to be exploitable "in the wild". Rather, they highlight potential problems with the current algorithm choices.

The symmetric key encryption schemes used in EMV are also slightly old fashioned. Two block ciphers are supported Triple DES and AES, with the underlying encryption method being CBC mode. The standard supports two MAC functions, AMAC for use with single DES and CMAC for use with AES.

EMVCo is currently engaged in the process of renewing their cryptographic specifications to bring them up to date. There has been a lot of work on defining elliptic curve based schemes for use in EMV. Some work has been done on analysing the specific protocols and schemes being considered for use in the new specifications. For example [125] presents a detailed security analysis of the key agreement and secure channel protocol which is proposed to be used to secure the communication between the chip card and the merchants terminal.

Bibliography

[1] Technical Specification Group Services 3rd Generation Parternship Project and 3G Security System Aspects. Confidentiality and integrity algorithms UEA1 & UIA1. Document 1: UEA1 and UIA1 specifications.

[2] Technical Specification Group Services 3rd Generation Parternship Project and 3G Security System Aspects. Confidentiality and integrity algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 specifications.

[3] Technical Specification Group Services 3rd Generation Parternship Project and 3G Security System Aspects. Confidentiality and integrity algorithms UEA2 & UIA2. Document 2: SNOW 3G specification.

[4] Technical Specification Group Services 3rd Generation Parternship Project and 3G Security System Aspects. Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification, v.3.1.1.

[5] Michel Abdalla, Olivier Chevassut, and David Pointcheval. One-time verifier-based encrypted key exchange. In Serge Vaudenay, editor, *Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 47–64. Springer, 2005.

[6] Michel Abdalla and David Pointcheval. Simple password-based encrypted key exchange protocols. In Alfred Menezes, editor, *CT-RSA*, volume 3376 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2005.

[7] Michel Abdalla and David Pointcheval. A scalable password-based group key exchange protocol in the standard model. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 332–347. Springer, 2006.

[8] Mohamed Ahmed Abdelraheem, Peter Beelen, Andrey Bogdanov, and Elmar Tischhauser. Twisted polynomials and forgery attacks on GCM. In Oswald and Fischlin [445], pages 762–786.

[9] Masayuki Abe, editor. *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, volume 6477 of *Lecture Notes in Computer Science*. Springer, 2010.

[10] Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors. *Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers*, volume 4876 of *Lecture Notes in Computer Science*. Springer, 2007.

[11] Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ross J. Anderson, and Ronald L. Rivest. On the security of the EMV secure messaging API (extended abstract). In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols Workshop*, volume 5964 of *Lecture Notes in Computer Science*, pages 147–149. Springer, 2007.

[12] Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven J. Murdoch, Ross J. Anderson, and Ronald L. Rivest. Phish and chips. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols Workshop*, volume 5087 of *Lecture Notes in Computer Science*, pages 40–48. Springer, 2006.

[13] Andrew V. Adinetz and Evgeny A. Grechnikov. Building a collision for 75-round reduced SHA-1 using GPU clusters. In Christos Kaklamanis, Theodore S. Papatheodorou, and Paul G. Spirakis, editors, *Euro-Par 2012*, volume 7484 of *Lecture Notes in Computer Science*, pages 933–944. Springer, 2012.

[14] Leonard M. Adleman. The function field sieve. In Leonard M. Adleman and Ming-Deh A. Huang, editors, *ANTS*, volume 877 of *Lecture Notes in Computer Science*, pages 108–121. Springer, 1994.

[15] Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: a new version of Grain-128 with optional authentication. *IJWMC*, 5(1):48–59, 2011.

[16] Mehdi-Laurent Akkar and Christophe Giraud. An implementation of DES and AES, secure against some attacks. In Çetin Kaya Koç et al. [137], pages 309–318.

[17] Martin R. Albrecht, Jean Paul Degabriele, Torben Brandt Hansen, and Kenneth G. Paterson. A surfeit of SSH cipher suites. In *ACM Conference on Computer and Communications Security*, 2016. To appear.

[18] Martin R. Albrecht, Kenneth G. Paterson, and Gaven J. Watson. Plaintext recovery attacks against SSH. In *IEEE Symposium on Security and Privacy*, pages 16–26. IEEE Computer Society, 2009.

[19] Nadhem J. AlFardan, Daniel J. Bernstein, Kenneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt. On the security of RC4 in TLS. In Samuel T. King, editor, *USENIX Security*, pages 305–320. USENIX Association, 2013.

[20] Nadhem J. AlFardan and Kenneth G. Paterson. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2013.

[21] Ammar Alkassar, Alexander Geraldy, Birgit Pfitzmann, and Ahmad-Reza Sadeghi. Optimized self-synchronizing mode of operation. In Mitsuru Matsui, editor, *FSE*, volume 2355 of *Lecture Notes in Computer Science*, pages 78–91. Springer, 2001.

[22] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - a new hope. *IACR Cryptology ePrint Archive*, 2015:1092, 2015.

[23] Joël Alwen and Jeremiah Blocki. Efficiently computing data-independent memory-hard functions. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO II*, volume 9815 of *Lecture Notes in Computer Science*, pages 241–271. Springer, 2016.

[24] Joël Alwen and Jeremiah Blocki. Towards practical attacks on Argon2i and Balloon hashing. Cryptology ePrint Archive, Report 2016/759, 2016. `http://eprint.iacr.org/2016/759`.

[25] Joël Alwen, Binyi Chen, Chethan Kamath, Vladimir Kolmogorov, Krzysztof Pietrzak, and Stefano Tessaro. On the complexity of scrypt and proofs of space in the parallel random oracle model. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT II*, volume 9666 of *Lecture Notes in Computer Science*, pages 358–387. Springer, 2016.

[26] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In Knudsen [342], pages 83–107.

[27] ANSI X9.102. Symmetric key cryptography for the financial services industry - wrapping of keys and associated data. American National Standard Institute, 2008.

[28] ANSI X9.19. Financial institution retail message authentication. American National Standard Institute, 1996.

[29] ANSI X9.24. Retail financial services symmetric key management part 1: Using symmetric techniques. American National Standard Institute, 2009.

[30] ANSI X9.42. Agreement of symmetric keys using discrete logarithm cryptography. American National Standard Institute, 2005.

[31] ANSI X9.42. Key agreement and key transport using factoring-based cryptography. American National Standard Institute, 2005.

[32] ANSI X9.62. Public key cryptography for the financial services industry – The elliptic curve digital signature algorithm (ECDSA). American National Standard Institute, 2005.

[33] ANSI X9.63. Public key cryptography for the financial services industry – Key agreement and key transport using elliptic curve cryptography. American National Standard Institute, 2011.

[34] ANSI X9.82. Random number generation part 1: Overview and basic principles. American National Standard Institute, 2006.

[35] ANSSI. Référentiel Général de Sécurité, Annexe B1 Mécanismes cryptographiques : Régles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 1.20 du 26 janvier 2010. `http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf`, 2010.

[36] Kazumaro Aoki, Jian Guo, Krystian Matusiewicz, Yu Sasaki, and Lei Wang. Preimages for step-reduced SHA-2. In Matsui [387], pages 578–597.

[37] Kazumaro Aoki and Yu Sasaki. Meet-in-the-middle preimage attacks against reduced SHA-0 and SHA-1. In Halevi [237], pages 70–89.

[38] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Ryan. Formal analysis of UMTS privacy. *CoRR*, abs/1109.2066, 2011.

[39] Dmitri Asonov and Rakesh Agrawal. Keyboard acoustic emanations. In *IEEE Symposium on Security and Privacy*, pages 3–11. IEEE Computer Society, 2004.

[40] Jean-Philippe Aumasson, Itai Dinur, Willi Meier, and Adi Shamir. Cube testers and key recovery attacks on reduced-round MD6 and Trivium. In Orr Dunkelman, editor, *FSE*, volume 5665 of *Lecture Notes in Computer Science*, pages 1–22. Springer, 2009.

[41] Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger. New features of latin dances: Analysis of Salsa, ChaCha, and Rumba. In Nyberg [440], pages 470–488.

[42] Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan, and Luca Henzen. *The Hash Function BLAKE*. Information Security and Cryptography. Springer, 2014.

[43] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. BLAKE2: simpler, smaller, fast as MD5. In Michael J. Jacobson Jr., Michael E. Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *Applied Cryptography and Network Security - 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings*, volume 7954 of *Lecture Notes in Computer Science*, pages 119–135. Springer, 2013.

[44] Steve Babbage and Matthew Dodd. The mickey stream ciphers. In Robshaw and Billet [490], pages 191–209.

[45] Dirk Balfanz, Diana K. Smetters, Paul Stewart, and H. Chi Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *NDSS*. The Internet Society, 2002.

[46] Achiya Bar-On and Nathan Keller. A 2^70 attack on the full MISTY1. In Robshaw and Katz [488], pages 435–456.

[47] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. *J. Cryptology*, 24(4):720–760, 2011.

[48] Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to /dev/random. In Vijay Atluri, Catherine Meadows, and Ari Juels, editors, *ACM Conference on Computer and Communications Security*, pages 203–212. ACM, 2005.

[49] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In Oswald and Fischlin [445], pages 129–155.

[50] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic, 2013.

[51] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The tower number field sieve. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 31–55. Springer, 2015.

[52] Romain Bardou, Riccardo Focardi, Yusuke Kawamoto, Lorenzo Simionato, Graham Steel, and Joe-Kai Tsay. Efficient padding oracle attacks on cryptographic hardware. In Safavi-Naini and Canetti [507], pages 608–625.

[53] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. *J. Cryptology*, 21(3):392–429, 2008.

[54] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Formal certification of code-based cryptographic proofs. In Zhong Shao and Benjamin C. Pierce, editors, *POPL*, pages 90–101. ACM, 2009.

[55] David A. Basin, Cas Cremers, and Simon Meier. Provably repairing the iso/iec 9798 standard for entity authentication. *Journal of Computer Security*, 21(6):817–846, 2013.

[56] David A. Basin, Cas J. F. Cremers, and Simon Meier. Provably repairing the iso/iec 9798 standard for entity authentication. In Pierpaolo Degano and Joshua D. Guttman, editors, *POST*, volume 7215 of *Lecture Notes in Computer Science*, pages 129–148. Springer, 2012.

[57] M. Bellare, T. Kohno, and C. Namprempre. The Secure Shell (SSH) Transport Layer Encryption Modes. RFC 4344 (Proposed Standard), January 2006.

[58] Mihir Bellare. New proofs for NMAC and HMAC: Security without collision resistance. In Dwork [181], pages 602–619.

[59] Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged public-key encryption: How to protect against bad randomness. In Matsui [387], pages 232–249.

[60] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract). In Jeffrey Scott Vitter, editor, *STOC*, pages 419–428. ACM, 1998.

[61] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *FOCS*, pages 394–403. IEEE Computer Society, 1997.

[62] Mihir Bellare, Marc Fischlin, Shafi Goldwasser, and Silvio Micali. Identification protocols secure against reset attacks. In Pfitzmann [461], pages 495–511.

[63] Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm. *ACM Trans. Inf. Syst. Secur.*, 7(2):206–241, 2004.

[64] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Tatsuaki Okamoto, editor, *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer, 2000.

[65] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In Preneel [474], pages 139–155.

[66] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In Douglas R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249. Springer, 1993.

[67] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer, 1994.

[68] Mihir Bellare, Phillip Rogaway, and David Wagner. The EAX mode of operation. In Roy and Meier [502], pages 389–407.

[69] S. M. Bellovin and M. Merritt. Limitations of the Kerberos authentication system. *SIGCOMM Comput. Commun. Rev.*, 20(5):119–132, October 1990.

[70] Steven M. Bellovin. Problem areas for the IP security protocols. In *Proceedings of the Sixth Usenix Unix Security Symposium*, pages 1–16, 1996.

[71] Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secureagainst dictionary attacks. In *Proceedings of the 1992 IEEE Symposium on Security and Privacy*, SP '92, pages 72–, Washington, DC, USA, 1992. IEEE Computer Society.

[72] Steven M. Bellovin and Michael Merritt. Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM Conference on Computer and Communications Security*, pages 244–250. ACM, 1993.

[73] Jens Bender, Marc Fischlin, and Dennis Kügler. Security analysis of the pace key-agreement protocol. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *ISC*, volume 5735 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2009.

[74] Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert. Sosemanuk, a fast software-oriented stream cipher. In Robshaw and Billet [490], pages 98–118.

[75] Côme Berbain, Henri Gilbert, and Alexander Maximov. Cryptanalysis of Grain. In Robshaw [489], pages 15–29.

[76] Dan J. Bernstein. Chacha, a variant of salsa20, 2008. `http://cr.yp.to/papers.html#chacha`.

[77] Daniel J. Bernstein. Cache-timing attacks on AES. `http://cr.yp.to/antiforgery/cachetiming-20050414.pdf`, 2005.

[78] Daniel J. Bernstein. The Poly1305-AES message-authentication code. `http://cr.yp.to/mac/poly1305-20050329.pdf`, 2005.

[79] Daniel J. Bernstein. Snuffle 2005: the Salsa20 encryption function, 2007. http://http://cr.yp.to/snuffle.html.

[80] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren. Factoring RSA keys from certified smart cards: Coppersmith in the wild. In Sako and Sarkar [508], pages 341–360.

[81] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. Mcbits: fast constant-time code-based cryptography. *IACR Cryptology ePrint Archive*, 2015:610, 2015.

[82] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU prime. *IACR Cryptology ePrint Archive*, 2016:461, 2016.

[83] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. SPHINCS: practical stateless hash-based signatures. In Oswald and Fischlin [445], pages 368–397.

[84] D. Bider and M. Baushke. SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol. RFC 6668 (Proposed Standard), July 2012.

[85] Eli Biham. A fast new DES implementation in software. In Eli Biham, editor, *FSE*, volume 1267 of *Lecture Notes in Computer Science*, pages 260–272. Springer, 1997.

[86] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A new block cipher proposal. In Vaudenay [552], pages 222–238.

[87] Eli Biham and Yaniv Carmeli. Efficient reconstruction of RC4 keys from internal states. In Nyberg [440], pages 270–288.

[88] Eli Biham, Orr Dunkelman, and Nathan Keller. A related-key rectangle attack on the full KASUMI. In Roy [501], pages 443–461.

[89] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[90] Alex Biryukov, editor. *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*. Springer, 2007.

[91] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich. Argon2: New generation of memory-hard functions for password hashing and other applications. In *IEEE EuroS&P*, pages 292–302. IEEE, 2016.

[92] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In Gilbert [220], pages 299–319.

[93] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Matsui [387], pages 1–18.

[94] Alex Biryukov, Sourav Mukhopadhyay, and Palash Sarkar. Improved time-memory trade-offs with multiple data. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 110–127. Springer, 2005.

[95] Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang. Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G $^{(+)}$. In Zhou and Yung [573], pages 139–153.

[96] Andrea Bittau, Mark Handley, and Joshua Lackey. The final nail in WEP's coffin. In *IEEE Symposium on Security and Privacy* [270], pages 386–400.

[97] John Black, Shai Halevi, Hugo Krawczyk, Ted Krovetz, and Phillip Rogaway. UMAC: Fast and secure message authentication. In Wiener [564], pages 216–233.

[98] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). RFC 4492 (Informational), May 2006. Updated by RFC 5246.

[99] Simon Blake-Wilson, Don Johnson, and Alfred Menezes. Key agreement protocols and their security analysis. In Michael Darnell, editor, *IMA Int. Conf.*, volume 1355 of *Lecture Notes in Computer Science*, pages 30–45. Springer, 1997.

[100] Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In Hugo Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 1998.

[101] Lenore Blum, Manuel Blum, and Mike Shub. A simple unpredictable pseudo-random number generator. *SIAM J. Comput.*, 15(2):364–383, 1986.

[102] Andrey Bogdanov. Security evaluation of block ciphers AES, Camellia, CLEFIA and SC2000 using two new techniques: Biclique attacks and zero-correlation linear attacks.

[103] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Lee and Wang [364], pages 344–371.

[104] Alexandra Boldyreva and Virendra Kumar. Provable-security analysis of authenticated encryption in Kerberos. *IET Information Security*, 5(4):207–219, 2011.

[105] Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei P. Skorobogatov, and Ross J. Anderson. Chip and skim: Cloning EMV cards with the pre-play attack. *CoRR*, abs/1209.2531, 2012.

[106] Dan Boneh, editor. *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*. Springer, 2003.

[107] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.

[108] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter. Balloon hashing: A memory-hard function providing provable protection against sequential attacks. Cryptology ePrint Archive, Report 2016/027, 2016. `http://eprint.iacr.org/2016/027`.

[109] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Transactions on Information Theory*, 46(4):1339–1349, 2000.

[110] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Kilian [335], pages 213–229.

[111] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[112] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. *IACR Cryptology ePrint Archive*, 2016:659, 2016.

[113] Joppe W. Bos and Marcelo E. Kaihara. Playstation 3 computing breaks 2^{60} barrier: 112-bit prime ECDLP solved. EPFL Laboratory for cryptologic algorithms - LACAL, 2009.

[114] Cyril Bouvier. Discrete logarithm in GF(2^{809}) with FFS. Post to NMBRTHRY@LISTSERV.NODAK.EDU, 2013.

[115] Victor Boyko, Philip D. MacKenzie, and Sarvar Patel. Provably secure password-authenticated key exchange using diffie-hellman. In Preneel [474], pages 156–171.

[116] Jørgen Brandt, Ivan Damgård, Peter Landrock, and Torben P. Pedersen. Zero-knowledge authentication scheme with secret key exchange (extended abstract). In Shafi Goldwasser, editor, *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 583–588. Springer, 1988.

[117] Gilles Brassard, editor. *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*. Springer, 1990.

[118] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Security proofs for an efficient password-based key exchange. In Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors, *ACM Conference on Computer and Communications Security*, pages 241–250. ACM, 2003.

[119] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. New security results on encrypted key exchange. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 145–158. Springer, 2004.

[120] Ernest F. Brickell, David Pointcheval, Serge Vaudenay, and Moti Yung. Design validations for discrete logarithm based signature schemes. In Hideki Imai and Yuliang Zheng, editors, *Public Key Cryptography*, volume 1751 of *Lecture Notes in Computer Science*, pages 276–292. Springer, 2000.

[121] Julien Brouchier, Tom Kean, Carol Marsh, and David Naccache. Temperature attacks. *IEEE Security & Privacy*, 7(2):79–82, 2009.

[122] Daniel R. L. Brown. Generic groups, collision resistance, and ECDSA. *Des. Codes Cryptography*, 35(1):119–152, 2005.

[123] Daniel R. L. Brown and Kristian Gjøsteen. A security analysis of the NIST SP 800-90 elliptic curve random number generator. In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 466–481. Springer, 2007.

[124] Christina Brzuska, Marc Fischlin, Nigel P. Smart, Bogdan Warinschi, and Stephen C. Williams. Less is more: relaxed yet composable security notions for key exchange. *Int. J. Inf. Sec.*, 12(4):267–297, 2013.

[125] Christina Brzuska, Nigel P. Smart, Bogdan Warinschi, and Gaven J. Watson. An analysis of the EMV channel establishment protocol. In Sadeghi et al. [506], pages 373–386.

[126] BSI. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102 Version 2013.2, `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.pdf?__blob=publicationFile`, 2013.

[127] Bundesnetzagentur. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung. `http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2013Algorithmenkatalog.pdf?__blob=publicationFile&v=1`, 2013.

[128] Mihir Bellare Ran Canetti and Hugo Krawczyk. Keying hash functions for message authentication. In Koblitz [343], pages 1–15.

[129] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–145. IEEE Computer Society, 2001.

[130] Ran Canetti and Juan A. Garay, editors. *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*. Springer, 2013.

[131] Ran Canetti, Shai Halevi, Jonathan Katz, Yehuda Lindell, and Philip D. MacKenzie. Universally composable password-based key exchange. In Cramer [158], pages 404–421.

[132] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In Pfitzmann [461], pages 453–474.

[133] Christophe De Cannière and Christian Rechberger. Preimages for reduced SHA-0 and SHA-1. In Wagner [558], pages 179–202.

[134] Anne Canteaut and Kapalee Viswanathan, editors. *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*. Springer, 2004.

[135] Brice Canvel, Alain P. Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a SSL/TLS channel. In Boneh [106], pages 583–599.

[136] Larry Carter and Mark N. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[137] Çetin Kaya Koç, David Naccache, and Christof Paar, editors. *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, volume 2162 of *Lecture Notes in Computer Science*. Springer, 2001.

[138] Certicom. Certicom announces elliptic curve cryptosystem (ECC) challenge winner. Certicom Press Release, 2009.

[139] Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar. Another look at tightness II: Practical issues in cryptography. *IACR Cryptology ePrint Archive*, 2016:360, 2016.

[140] Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham. On the practical exploitability of Dual EC in TLS implementations. In *USENIX Security Symposium*, 2014.

[141] Liqun Chen and Zhaohui Cheng. Security proof of Sakai-Kasahara's identity-based encryption scheme. In Nigel P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 442–459. Springer, 2005.

[142] Liqun Chen, Zhaohui Cheng, John Malone-Lee, and Nigel P. Smart. An efficient ID-KEM based on the Sakai–Kasahara key construction. *IEE Proc. Information Security*, 153:19–26, 2006.

[143] Jung Hee Cheon. Security analysis of the strong Diffie-Hellman problem. In Vaudenay [555], pages 1–11.

[144] Olivier Chevassut, Pierre-Alain Fouque, Pierrick Gaudry, and David Pointcheval. Key derivation and randomness extraction. *IACR Cryptology ePrint Archive*, 2005:61, 2005.

[145] Joo Yeon Cho and Miia Hermelin. Improved linear cryptanalysis of sosemanuk. In Donghoon Lee and Seokhie Hong, editors, *ICISC*, volume 5984 of *Lecture Notes in Computer Science*, pages 101–117. Springer, 2009.

[146] Carlos Cid and Gaëtan Leurent. An analysis of the XSL algorithm. In Roy [501], pages 333–352.

[147] Don Coppersmith. Finding a small root of a bivariate integer equation; Factoring with high bits known. In Maurer [388], pages 178–189.

[148] Don Coppersmith. Finding a small root of a univariate modular equation. In Maurer [388], pages 155–165.

[149] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptology*, 10(4):233–260, 1997.

[150] Don Coppersmith, Matthew K. Franklin, Jacques Patarin, and Michael K. Reiter. Low-exponent RSA with related messages. In Maurer [388], pages 1–9.

[151] Jean-Sébastien Coron. On the exact security of full domain hash. In Mihir Bellare, editor, *CRYPTO*, volume 1880 of *Lecture Notes in Computer Science*, pages 229–235. Springer, 2000.

[152] Jean-Sébastien Coron. Optimal security proofs for PSS and other signature schemes. In Knudsen [342], pages 272–287.

[153] Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier. New attacks on PKCS#1 v1.5 encryption. In Preneel [474], pages 369–381.

[154] Jean-Sébastien Coron, David Naccache, and Julien P. Stern. On the security of RSA padding. In Wiener [564], pages 1–18.

[155] Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi, and Ralf-Philipp Weinmann. Practical cryptanalysis of ISO/IEC 9796-2 and EMV signatures. In Halevi [237], pages 428–444.

[156] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny diffie-hellman. In Robshaw and Katz [488], pages 572–601.

[157] Nicolas Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer, 2002.

[158] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.

[159] F. Cusack and M. Forssen. Generic Message Exchange Authentication for the Secure Shell Protocol (SSH). RFC 4256 (Proposed Standard), January 2006.

[160] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.

[161] W. Dai. An attack against SSH2 protocol. E-mail to the SECSH Working Group available from `ftp://ftp.ietf.org/ietf-mail-archive/secsh/2002-02.mail`, 6th Feb. 2002.

[162] Ivan Damgård. A design principle for hash functions. In Brassard [117], pages 416–427.

[163] Nasser Ramazani Darmian. A distinguish attack on rabbit stream cipher based on multiple cube tester. *IACR Cryptology ePrint Archive*, 2013:780, 2013.

[164] Debian. Debian Security Advisory DSA-1571-1: OpenSSL – predictable random number generator, 2008. `http://www.debian.org/security/2008/dsa-1571`.

[165] Jean Paul Degabriele, Anja Lehmann, Kenneth G. Paterson, Nigel P. Smart, and Mario Strefler. On the joint security of encryption and signature in EMV. In Orr Dunkelman, editor, *CT-RSA*, volume 7178 of *Lecture Notes in Computer Science*, pages 116–135. Springer, 2012.

[166] Jean Paul Degabriele and Kenneth G. Paterson. Attacking the IPsec standards in encryption-only configurations. In *IEEE Symposium on Security and Privacy*, pages 335–349. IEEE Computer Society, 2007.

[167] Jean Paul Degabriele and Kenneth G. Paterson. On the (in)security of IPsec in MAC-then-encrypt configurations. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM Conference on Computer and Communications Security*, pages 493–504. ACM, 2010.

[168] T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard), January 1999. Obsoleted by RFC 4346, updated by RFCs 3546, 5746, 6176.

[169] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346 (Proposed Standard), April 2006. Obsoleted by RFC 5246, updated by RFCs 4366, 4680, 4681, 5746, 6176.

[170] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFCs 5746, 5878, 6176.

[171] Itai Dinur, Orr Dunkelman, and Adi Shamir. Improved practical attacks on round-reduced keccak. *J. Cryptology*, 27(2):183–209, 2014.

[172] Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michal Straus. Practical complexity cube attacks on round-reduced keccak sponge function. *IACR Cryptology ePrint Archive*, 2014:13, 2014.

[173] Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergnaud, and Daniel Wichs. Security analysis of pseudo-random number generators with input: /dev/random is not robust. In Sadeghi et al. [506], pages 647–658.

[174] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too - optimal recovery strategies for compromised rngs. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO (2)*, volume 8617 of *Lecture Notes in Computer Science*, pages 37–54. Springer, 2014.

[175] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. *ACM Trans. Inf. Syst. Secur.*, 13(1), 2009.

[176] Saar Drimer, Steven J. Murdoch, and Ross J. Anderson. Optimised to fail: Card readers for online banking. In Roger Dingledine and Philippe Golle, editors, *Financial Cryptography*, volume 5628 of *Lecture Notes in Computer Science*, pages 184–200. Springer, 2009.

[177] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In Canetti and Garay [130], pages 40–56.

[178] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Rabin [481], pages 393–410.

[179] T. Duong and J. Rizzo. Here come the $\oplus$ ninjas. Unpublished manuscript, 2011.

[180] Thai Duong and Juliano Rizzo. The CRIME attack. Presentation at ekoparty Security Conference, 2012.

[181] Cynthia Dwork, editor. *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*. Springer, 2006.

[182] D. Eastlake. Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH). RFC 4305 (Proposed Standard), December 2005. Obsoleted by RFC 4835.

[183] D. Eastlake 3rd, J. Schiller, and S. Crocker. Randomness Requirements for Security. RFC 4086 (Best Current Practice), June 2005.

[184] ECRYPT II NoE. ECRYPT II Yearly Report on Algorithms and Key Lengths (2008-2009). ECRYPT II deliverable D.SPA.7-1.0, 2009.

[185] ECRYPT II NoE. ECRYPT II Yearly Report on Algorithms and Key Lengths (2009-2010). ECRYPT II deliverable D.SPA.13-1.0, 2010.

[186] ECRYPT II NoE. ECRYPT II Yearly Report on Algorithms and Key Lengths (2010-2011). ECRYPT II deliverable D.SPA.17-1.0, 2011.

[187] ECRYPT II NoE. ECRYPT II Yearly Report on Algorithms and Key Lengths (2011-2012). ECRYPT II deliverable D.SPA.20-1.0, 2012.

[188] ECRYPT NoE. ECRYPT Yearly Report on Algorithms and Key Lengths (2004). ECRYPT deliverable D.SPA.10-1.1, 2004.

[189] ECRYPT NoE. ECRYPT Yearly Report on Algorithms and Key Lengths (2005). ECRYPT deliverable D.SPA.16-1.0, 2005.

[190] ECRYPT NoE. ECRYPT Yearly Report on Algorithms and Key Lengths (2006). ECRYPT deliverable D.SPA.21-1.0, 2006.

[191] ECRYPT NoE. ECRYPT Yearly Report on Algorithms and Key Lengths (2007-2008). ECRYPT deliverable D.SPA.28-1.0, 2008.

[192] EMV Co. Book 2 – Security and key management. EMV 4.3, 2011.

[193] ENISA. The use of cryptographic techniques in Europe. `http://www.enisa.europa.eu/activities/identity-and-trust/library/the-use-of-cryptographic-techniques-in-europe`, 2011.

[194] ENISA. Algorithms, key size and parameters report – 2013 recommendations. `http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report`, 2013.

[195] ENISA. Algorithms, key size and parameters report – 2014. `https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`, 2014.

[196] ENISA. Study on cryptographic protocols – 2014. `https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols`, 2014.

[197] Matthias Ernst, Ellen Jochemsz, Alexander May, and Benne de Weger. Partial key exposure attacks on RSA up to full size exponents. In Cramer [158], pages 371–386.

[198] Thomas Espitau, Pierre-Alain Fouque, and Pierre Karpman. Higher-order differential meet-in-the-middle preimage attacks on SHA-1 and BLAKE. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 683–701. Springer, 2015.

[199] ETSI TS 102 176-. Electronic signatures and infrastructures (ESI); Algorithms and parameters for secure electronic signatures; Part 1: Hash functions and asymmetric algorithms. European Telecommunications Standards Institute, 2007.

[200] ETSI/SAGE Specification. Specification of the 3GPP Confidentiality and Integrity Algorithms. Document 2: Kasumi Algorithm Specification. ETSI/SAGE, 2011.

[201] European Payments Council. Guidelines on algorithms usage and key management, 2013.

[202] Federal Information Processing Standards Publication 197. Advanced encryption standard (AES). National Institute of Standards and Technology, 2001.

[203] Federal Information Processing Standards Publication 202. SHA-3 standard: Permutation-based hash and extendable-output functions (draft). National Institute of Standards and Technology, 2014.

[204] Xiutao Feng, Jun Liu, Zhaocun Zhou, Chuankun Wu, and Dengguo Feng. A byte-based guess and determine attack on sosemanuk. In Abe [9], pages 146–157.

[205] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Mathematical Cryptology*, 8(3):209–247, 2014.

[206] Niels Ferguson and Bruce Schneier. A cryptographic evaluation of IPsec. Unpublished manuscript available from `http://www.schneier.com/paper-ipsec.html`, February 1999.

[207] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering — Design Principles and Practical Applications*. Wiley, 2010.

[208] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[209] Scott R. Fluhrer and Stefan Lucks. Analysis of the E_0 encryption system. In Vaudenay and Youssef [557], pages 38–48.

[210] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. In Vaudenay and Youssef [557], pages 1–24.

[211] Jens Franke. RSA576. Post to various internet discussion boards/email lists, 2003.

[212] Jens Franke. RSA576. Post to various internet discussion boards/email lists, 2005.

[213] S. Frankel, R. Glenn, and S. Kelly. The AES-CBC Cipher Algorithm and Its Use with IPsec. RFC 3602 (Proposed Standard), September 2003.

[214] S. Frankel and H. Herbert. The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec. RFC 3566 (Proposed Standard), September 2003.

[215] M. Friedl, N. Provos, and W. Simpson. Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol. RFC 4419 (Proposed Standard), March 2006.

[216] D. Fu and J. Solinas. Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2. RFC 5903 (Informational), June 2010.

[217] M Peeters G. Bertoni, J. Daemen and G. Van Assche. The Keccak sponge function family. `http://keccak.noekeon.org/`.

[218] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In Çetin Kaya Koç et al. [137], pages 251–261.

[219] Pierrick Gaudry, Florian Hess, and Nigel P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.

[220] Henri Gilbert, editor. *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*. Springer, 2010.

[221] Marc Girault. Self-certified public keys. In Donald W. Davies, editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 490–497. Springer, 1991.

[222] Marc Girault and Jean-Claude Paillés. On-line/off-line RSA-like. In *Proceedings of WCC 2003*, pages 173–184, 2003.

[223] Danilo Gligoroski, Suzana Andova, and Svein J. Knapskog. On the importance of the key separation principle for different modes of operation. In Liqun Chen, Yi Mu, and Willy Susilo, editors, *ISPEC*, volume 4991 of *Lecture Notes in Computer Science*, pages 404–418. Springer, 2008.

[224] Ian Goldberg, Atefeh Mashatan, and Douglas R. Stinson. On message recognition protocols: recoverability and explicit confirmation. *IJACT*, 2(2):100–120, 2010.

[225] Ian Goldberg and David Wagner. Randomness and the Netscape browser, 1996. `http://www.drdobbs.com/windows/184409807`.

[226] Oded Goldreich and Yehuda Lindell. Session-key generation using human passwords only. *J. Cryptology*, 19(3):241–340, 2006.

[227] Daniel M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, 1993.

[228] GOST R 34-10-2001. Information technology – Cryptography data security – Formation and verification process of [electronic] signatures. State Standard of the Russion Federation, 2001.

[229] Louis Goubin and Ange Martinelli. Protecting AES with shamir's secret sharing scheme. In Bart Preneel and Tsuyoshi Takagi, editors, *CHES*, volume 6917 of *Lecture Notes in Computer Science*, pages 79–94. Springer, 2011.

[230] Robert Granger. Discrete logarithms in GF(2^{6120}). Post to NMBRTHRY@LISTSERV.NODAK.EDU, 2013.

[231] Louis C. Guillou and Jean-Jacques Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In Christoph G. Günther, editor, *EUROCRYPT*, volume 330 of *Lecture Notes in Computer Science*, pages 123–128. Springer, 1988.

[232] Jian Guo, Pierre Karpman, Ivica Nikolic, Lei Wang, and Shuang Wu. Analysis of BLAKE2. In Josh Benaloh, editor, *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings*, volume 8366 of *Lecture Notes in Computer Science*, pages 402–423. Springer, 2014.

[233] Jian Guo, San Ling, Christian Rechberger, and Huaxiong Wang. Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. In Abe [9], pages 56–75.

[234] Peter Gutmann. Software generation of practically strong random numbers. In Aviel D. Rubin, editor, *USENIX Security*. USENIX Association, 1998.

[235] Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the linux random number generator. In *IEEE Symposium on Security and Privacy* [270], pages 371–385.

[236] Shai Halevi. EME*: Extending EME to handle arbitrary-length messages with associated data. In Canteaut and Viswanathan [134], pages 315–327.

[237] Shai Halevi, editor. *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*. Springer, 2009.

[238] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In Okamoto [442], pages 292–304.

[239] Finn Michael Halvorsen, Olav Haugen, Martin Eian, and Stig Fr. Mjølsnes. An improved attack on TKIP. In Audun Jøsang, Torleiv Maseng, and Svein J. Knapskog, editors, *NordSec*, volume 5838 of *Lecture Notes in Computer Science*, pages 120–132. Springer, 2009.

[240] Mike Hamburg, Paul Kocher, and Mark E. Marson. Analysis of Intel's Ivy Bridge digital random number generator, March 2012. `http://www.cryptography.com/public/pdf/Intel_TRNG_Report_20120312.pdf`.

[241] Helena Handschuh and Bart Preneel. Key-recovery attacks on universal hash function based MAC algorithms. In Wagner [558], pages 144–161.

[242] Feng Hao and Peter Ryan. J-pake: Authenticated key exchange without pki. *Transactions on Computational Science*, 11:192–206, 2010.

[243] Feng Hao and Peter Y. A. Ryan. Password authenticated key exchange by juggling. In Bruce Christianson, James A. Malcolm, Vashek Matyas, and Michael Roe, editors, *Security Protocols Workshop*, volume 6615 of *Lecture Notes in Computer Science*, pages 159–171. Springer, 2008.

[244] Dan Harkins. Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks. In *Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications*, SENSORCOMM '08, pages 839–844, Washington, DC, USA, 2008. IEEE Computer Society.

[245] Dan Harkins. Synthethic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). RFC 5297 (Informational), October 2008.

[246] Dan Harkins and Dave Carrel. The Internet Key Exchange (IKE). RFC 2409 (Proposed Standard), November 1998. Obsoleted by RFC 4306, updated by RFC 4109.

[247] Dan Harkins and Glen Zorn. Extensible authentication protocol (eap) authentication using only a password. RFC 5931 (Informational), 2010.

[248] Ben Harris. RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol. RFC 4432 (Proposed Standard), March 2006.

[249] Johan Håstad. Solving simultaneous modular equations of low degree. *SIAM J. Comput.*, 17(2):336–341, 1988.

[250] Johan Håstad and Mats Näslund. The security of all RSA and discrete log bits. *J. ACM*, 51(2):187–230, 2004.

[251] Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. The Grain family of stream ciphers. In Robshaw and Billet [490], pages 179–190.

[252] Martin Hell, Thomas Johansson, and Willi Meier. Grain: a stream cipher for constrained environments. *IJWMC*, 2(1):86–93, 2007.

[253] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J.Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *USENIX Security Symposium – 2012*, pages 205–220, 2012.

[254] Miia Hermelin and Kaisa Nyberg. Correlation properties of the Bluetooth combiner generator. In JooSeok Song, editor, *ICISC*, volume 1787 of *Lecture Notes in Computer Science*, pages 17–29. Springer, 1999.

[255] Mathias Herrmann and Alexander May. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 53–69. Springer, 2010.

[256] Erwin Hess, Marcus Schafheutle, and Pascale Serf. The digital signature scheme ECGDSA, 2006.

[257] Shoichi Hirose. Security analysis of DRBG using HMAC in NIST SP 800-90. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *Information Security Applications, 9th International Workshop, WISA 2008, Jeju Island, Korea, September 23-25, 2008, Revised Selected Papers*, volume 5379 of *Lecture Notes in Computer Science*, pages 278–291. Springer, 2008.

[258] P. Hoffman. Cryptographic Suites for IPsec. RFC 4308 (Proposed Standard), December 2005.

[259] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[260] R. Housley. Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP). RFC 3686 (Proposed Standard), January 2004.

[261] R. Housley. Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP). RFC 4309 (Proposed Standard), December 2005.

[262] R. Housley and M. Dworkin. Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm. RFC 5649 (Informational), August 2009.

[263] Nick Howgrave-Graham and Nigel P. Smart. Lattice attacks on digital signature schemes. *Des. Codes Cryptography*, 23(3):283–290, 2001.

[264] G. Hudson. Camellia Encryption for Kerberos 5. RFC 6803 (Informational), November 2012.

[265] Andreas Hülsing, Denis Butin, Stefan-Lukas Gazdag, and Aziz Mohaisen. XMSS: Extended hash-based signatures. Internet Draft, IETF Crypto Forum Research Group, 2015. `https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/`.

[266] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography – PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*, pages 387–416, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[267] IEEE 802.11. Wireless LAN medium access control MAC and physical layer PHY specifications. Institute of Electrical and Electronics Engineers Standard, 1999.

[268] IEEE 802.11-2012 (Revision of IEEE 802.11-2007). Wireless LAN medium access control MAC and physical layer PHY specifications. Institute of Electrical and Electronics Engineers Standard, 2012.

[269] IEEE 802.15.4 . Law rate WPAN. Institute of Electrical and Electronics Engineers Standard, 2012.

[270] IEEE Computer Society. *2006 IEEE Symposium on Security and Privacy (S&P 2006), 21-24 May 2006, Berkeley, California, USA*, 2006.

[271] IEEE P1363.3 (Draft D5). Identity-based public key cryptography using pairings. Institute of Electrical and Electronics Engineers Standard, 2012.

[272] K. Igoe and J. Solinas. AES Galois Counter Mode for the Secure Shell Transport Layer Protocol. RFC 5647 (Informational), August 2009.

[273] Sebastiaan Indesteege, Florian Mendel, Bart Preneel, and Christian Rechberger. Collisions and other non-random properties for step-reduced SHA-256. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 276–293. Springer, 2008.

[274] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Boneh [106], pages 463–481.

[275] Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii. Full plaintext recovery attack on broadcast rc4. In Moriai [405], pages 179–202.

[276] ISO/IEC 10118-2:2010. Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher. International Organization for Standardization, 2010.

[277] ISO/IEC 11770-2. Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques. International Organization for Standardization, 2008.

[278] ISO/IEC 11770-3. Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. International Organization for Standardization, 2008.

[279] ISO/IEC 11770-4. Information technology – Security techniques – Key management – Part 3: Mechanisms based on weak secrets. International Organization for Standardization, 2006.

[280] ISO/IEC 11770-6. Information technology – Security techniques – Key management – Part 6: Key derivation. International Organization for Standardization, Under Development.

[281] ISO/IEC 14888-3. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. International Organization for Standardization, 2009.

[282] ISO/IEC 14888-3. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms – Ammendment 1. International Organization for Standardization, 2009.

[283] ISO/IEC 18031. Information technology – Security techniques – Random bit generator. International Organization for Standardization, 2011.

[284] ISO/IEC 18033-2. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric Ciphers. International Organization for Standardization, 2006.

[285] ISO/IEC 18033-4. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. International Organization for Standardization, 2011.

[286] ISO/IEC 19772. Information technology – Security techniques – authenticated encryption. International Organization for Standardization, 2009.

[287] ISO/IEC 19972. Information technology – Security techniques – Authenticated encryption. International Organization for Standardization, 2009.

[288] ISO/IEC 29192-3. Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers. International Organization for Standardization, 2012.

[289] ISO/IEC 29192-4. Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques. International Organization for Standardization, 2013.

[290] ISO/IEC 9796-2. Information technology – Security techniques – Digital signatures giving message recovery – Part 2: Integer factorization based schemes. International Organization for Standardization, 2010.

[291] ISO/IEC 9797-1:2011. Information technology – Security techniques – Digital signatures giving message recovery – Part 1: Mechanisms using a block cipher. International Organization for Standardization, 2011.

[292] ISO/IEC 9797-2:2011. Information technology – Security techniques – Digital signatures giving message recovery – Part 2: Mechanisms using a dedicated hash-function. International Organization for Standardization, 2011.

[293] ISO/IEC 9798-1. Information technology – Security techniques – Entity authentication – Part 1: General. International Organization for Standardization, 2010.

[294] ISO/IEC 9798-2. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment techniques. International Organization for Standardization, 2008.

[295] ISO/IEC 9798-3. Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques. International Organization for Standardization, 1998.

[296] ISO/IEC 9798-4. Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function. International Organization for Standardization, 1999.

[297] ISO/IEC 9798-5. Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques. International Organization for Standardization, 2009.

[298] ISO/IEC 9798-6. Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer. International Organization for Standardization, 2010.

[299] Tetsu Iwata and Kaoru Kurosawa. OMAC: One-key CBC MAC. In Thomas Johansson, editor, *FSE*, volume 2887 of *Lecture Notes in Computer Science*, pages 129–153. Springer, 2003.

[300] Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu. Breaking and repairing GCM security proofs. In Safavi-Naini and Canetti [507], pages 31–49.

[301] David P. Jablon. Extended password key exchange protocols immune to dictionary attacks. In *WETICE*, pages 248–255. IEEE Computer Society, 1997.

[302] David P. Jablon and Westboro Ma. Strong password-only authenticated key exchange. *ACM Computer Communications Review*, 26:5–26, 1996.

[303] Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk. On the security of TLS-DHE in the standard model. In Safavi-Naini and Canetti [507], pages 273–293.

[304] Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk. On the security of TLS-DHE in the standard model. In Safavi-Naini and Canetti [507], pages 273–293.

[305] Thomas Johansson and Phong Q. Nguyen, editors. *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*. Springer, 2013.

[306] Jakob Jonsson. Security proofs for the RSA-PSS signature scheme and its variants. Cryptology ePrint Archive, Report 2001/053, 2001. `http://eprint.iacr.org/`.

[307] Jakob Jonsson. On the security of CTR + CBC-MAC. In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 76–93. Springer, 2002.

[308] Antoine Joux. Comments on the choice between CWC or GCM – authentication weaknesses in GCM. `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf`.

[309] Antoine Joux. Comments on the draft GCM specification – authentication failures in NIST version of GCM. `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/800-38_Series-Drafts/GCM/Joux_comments.pdf`.

[310] Antoine Joux. Discrete logarithms in GF(2^{6168}). Post to NMBRTHRY@LISTSERV.NODAK.EDU, 2013.

[311] Antoine Joux. Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields. In Johansson and Nguyen [305], pages 177–193.

[312] Antoine Joux. A new index calculus algorithm with complexity $$l(1/4+o(1))$$ in small characteristic. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography*, volume 8282 of *Lecture Notes in Computer Science*, pages 355–379. Springer, 2013.

[313] Antoine Joux, Reynald Lercier, Nigel P. Smart, and Frederik Vercauteren. The number field sieve in the medium prime case. In Dwork [181], pages 326–344.

[314] Marc Joye and Sung-Ming Yen. The montgomery powering ladder. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *CHES*, volume 2523 of *Lecture Notes in Computer Science*, pages 291–302. Springer, 2002.

[315] Hendrik W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987.

[316] Ronald Kainda, Ivan Flechais, and A. W. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In Lorrie Faith Cranor, editor, *SOUPS*, ACM International Conference Proceeding Series. ACM, 2009.

[317] Saqib A. Kakvi and Eike Kiltz. Optimal security proofs for full domain hash, revisited. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 537–553. Springer, 2012.

[318] B. Kaliski. PKCS #5: Password-Based Cryptography Specification Version 2.0. RFC 2898 (Informational), September 2000.

[319] Seny Kamara and Jonathan Katz. How to encrypt with a malicious random number generator. In Nyberg [440], pages 303–315.

[320] Ju-Sung Kang, Sang Uk Shin, Dowon Hong, and Okyeon Yi. Provable security of KASUMI and 3GPP encryption mode f8. In Colin Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 255–271. Springer, 2001.

[321] Orhun Kara and Cevat Manap. A new class of weak keys for Blowfish. In Biryukov [90], pages 167–180.

[322] Emilia Käsper and Peter Schwabe. Faster and timing-attack resistant AES-GCM. In Christophe Clavier and Kris Gaj, editors, *CHES*, volume 5747 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2009.

[323] A. Kato, M. Kanda, and S. Kanno. Modes of Operation for Camellia for Use with IPsec. RFC 5529 (Proposed Standard), April 2009.

[324] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient and secure authenticated key exchange using weak passwords. *J. ACM*, 57(1), 2009.

[325] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), December 2005. Obsoleted by RFC 5996, updated by RFC 5282.

[326] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 5996 (Proposed Standard), September 2010. Updated by RFC 5998.

[327] S. Kelly and S. Frankel. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. RFC 4868 (Proposed Standard), May 2007.

[328] John Kelsey, Bruce Schneier, and Niels Ferguson. Yarrow-160: Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 13–33. Springer, 1999.

[329] John Kelsey, Bruce Schneier, and David Wagner. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In Koblitz [343], pages 237–251.

[330] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. In Vaudenay [552], pages 168–188.

[331] S. Kent. Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP). RFC 4304 (Proposed Standard), December 2005.

[332] S. Kent. IP Authentication Header. RFC 4302 (Proposed Standard), December 2005.

[333] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303 (Proposed Standard), December 2005.

[334] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), December 2005. Updated by RFC 6040.

[335] Joe Kilian, editor. *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.

[336] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In Robshaw and Katz [488], pages 543–571.

[337] A. Kircanski and A. M. Youssef. On the sliding property of SNOW 3G and SNOW 2.0. *IET Inf. Secur.*, 5(4):199–206, 2011.

[338] Aleksandar Kircanski and Amr M. Youssef. On the sliding property of SNOW 3G and SNOW 2.0. *IET Information Security*, 5(4):199–206, 2011.

[339] T. Kivinen and M. Kojo. More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). RFC 3526 (Proposed Standard), May 2003.

[340] Thorsten Kleinjung. Discrete logarithms in GF(p) — 160 digits. Post to NMBRTHRY@LISTSERV.NODAK.EDU, 2007.

[341] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman J. J. te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA modulus. In Rabin [481], pages 333–350.

[342] Lars R. Knudsen, editor. *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*. Springer, 2002.

[343] Neal Koblitz, editor. *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*. Springer, 1996.

[344] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Koblitz [343], pages 104–113.

[345] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Wiener [564], pages 388–397.

[346] John T. Kohl. The use of encryption in Kerberos for network authentication. In Brassard [117], pages 35–43.

[347] Tadayoshi Kohno, John Viega, and Doug Whiting. CWC: A high-performance conventional authenticated encryption mode. In Roy and Meier [502], pages 408–426.

[348] Geir M. Køien and Vladimir A. Oleshchuk. Location privacy for cellular systems; analysis and solution. In George Danezis and David Martin, editors, *Privacy Enhancing Technologies*, volume 3856 of *Lecture Notes in Computer Science*, pages 40–58. Springer, 2005.

[349] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Best Current Practice), February 1997.

[350] Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is SSL?). In Kilian [335], pages 310–331.

[351] Hugo Krawczyk. Cryptographic extraction and key derivation: The HKDF scheme. In Rabin [481], pages 631–648.

[352] Hugo Krawczyk. Hmac-based extract-and-expand key derivation function (hkdf). RFC 5869 (Informational), 2010.

[353] Hugo Krawczyk, Kenneth G. Paterson, and Hoeteck Wee. On the security of the TLS protocol: A systematic analysis. In Canetti and Garay [130], pages 429–448.

[354] T. Krovetz. UMAC: Message Authentication Code using Universal Hashing. RFC 4418 (Best Current Practice), March 2006.

[355] D. Kuegler and Y. Sheffer. Password authenticated connection establishment with the internet key exchange protocol version 2 (ikev2). RFC 2104 (Best Current Practice), 2012.

[356] Patrick Lacharme, Andrea Röck, Vincent Strubel, and Marion Videau. The linux pseudorandom number generator revisited. *IACR Cryptology ePrint Archive*, 2012:251, 2012.

[357] Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, and Martin Schläffer. Rebound distinguishers: Results on the full Whirlpool compression function. In Matsui [387], pages 126–143.

[358] Franck Landelle and Thomas Peyrin. Cryptanalysis of full RIPEMD-128. In Johansson and Nguyen [305], pages 228–244.

[359] A. Langley, N. Mavrogiannopoulos, J. Strombergson, and S. Josefsson. ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS). RFC 7905 (Proposed Standard), June 2016.

[360] Sven Laur and Kaisa Nyberg. Efficient mutual data authentication using manually authenticated strings. In David Pointcheval, Yi Mu, and Kefei Chen, editors, *CANS*, volume 4301 of *Lecture Notes in Computer Science*, pages 90–107. Springer, 2006.

[361] Sven Laur and Sylvain Pasini. Sas-based group authentication and key agreement protocols. In Ronald Cramer, editor, *Public Key Cryptography*, volume 4939 of *Lecture Notes in Computer Science*, pages 197–213. Springer, 2008.

[362] Sven Laur and Sylvain Pasini. User-aided data authentication. *IJSN*, 4(1/2):69–86, 2009.

[363] Laurie Law, Alfred Menezes, Minghua Qu, Jerome A. Solinas, and Scott A. Vanstone. An efficient protocol for authenticated key agreement. *Des. Codes Cryptography*, 28(2):119–134, 2003.

[364] Dong Hoon Lee and Xiaoyun Wang, editors. *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*. Springer, 2011.

[365] Jung-Keun Lee, Dong Hoon Lee, and Sangwoo Park. Cryptanalysis of sosemanuk and snow 2.0 using linear masks. In Josef Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 524–538. Springer, 2008.

[366] Arjen Lenstra. Key lengths. In Hossein Bidgoli, editor, *Handbook of Information Security: Volume II: Information Warfare; Social Legal, and International Issues; and Security Foundations*, pages 617–635. Wiley, 2004.

[367] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Public keys. In Safavi-Naini and Canetti [507], pages 626–642.

[368] Arjen K. Lenstra and Hendrik W. Lenstra. *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer, 1993.

[369] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Datenschutz und Datensicherheit*, 24(3), 2000.

[370] M. Lepinski and S. Kent. Additional Diffie-Hellman Groups for Use with IETF Standards. RFC 5114 (Informational), January 2008.

[371] Gaëtan Leurent. Message freedom in MD4 and MD5 collisions: Application to APOP. In Biryukov [90], pages 309–328.

[372] Chu-Wee Lim and Khoongming Khoo. An analysis of XSL applied to BES. In Biryukov [90], pages 242–253.

[373] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In Aggelos Kiayias, editor, *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer, 2011.

[374] J. Linn. Generic Security Service Application Program Interface Version 2, Update 1. RFC 2743 (Proposed Standard), January 2000. Updated by RFC 5554.

[375] Moses Liskov and Kazuhiko Minematsu. Comments on the proposal to approve XTS-AES – Comments on XTS-AES. `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/XTS/XTS_comments-Liskov_Minematsu.pdf`.

[376] Yi Lu, Willi Meier, and Serge Vaudenay. The conditional correlation attack: A practical attack on Bluetooth encryption. In Shoup [527], pages 97–117.

[377] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43, 2013.

[378] Philip MacKenzie. On the security of the SPEKE password-authenticated key exchange protocol. *IACR Cryptology ePrint Archive*, 2001:19, 2001.

[379] C. Madson and R. Glenn. The Use of HMAC-MD5-96 within ESP and AH. RFC 2403 (Proposed Standard), November 1998.

[380] C. Madson and R. Glenn. The Use of HMAC-SHA-1-96 within ESP and AH. RFC 2404 (Proposed Standard), November 1998.

[381] Subhamoy Maitra and Goutam Paul. New form of permutation bias and secret key leakage in keystream bytes of RC4. In Nyberg [440], pages 253–269.

[382] James Manger. A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0. In Kilian [335], pages 230–238.

[383] Atefeh Mashatan and Douglas R. Stinson. Practical unconditionally secure two-channel message authentication. *Des. Codes Cryptography*, 55(2-3):169–188, 2010.

[384] Atefeh Mashatan and Serge Vaudenay. A message recognition protocol based on standard assumptions. In Zhou and Yung [573], pages 384–401.

[385] M. Matsui, J. Nakajima, and S. Moriai. A Description of the Camellia Encryption Algorithm. RFC 3713 (Informational), April 2004.

[386] Mitsuru Matsui. Linear cryptoanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[387] Mitsuru Matsui, editor. *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*. Springer, 2009.

[388] Ueli M. Maurer, editor. *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*. Springer, 1996.

[389] Alexander Maximov and Alex Biryukov. Two trivial attacks on Trivium. In Adams et al. [10], pages 36–55.

[390] Alexander Maximov and Dmitry Khovratovich. New state recovery attack on RC4. In Wagner [558], pages 297–316.

[391] D. McGrew and D. Bailey. AES-CCM Cipher Suites for Transport Layer Security (TLS). RFC 6655 (Best Current Practice), July 2012.

[392] D. McGrew and J. Viega. The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH. RFC 4543 (Proposed Standard), May 2006.

[393] David A. McGrew. Efficient authentication of large, dynamic data sets using Galois/Counter mode (GCM). In *IEEE Security in Storage Workshop*, pages 89–94. IEEE Computer Society, 2005.

[394] David A. McGrew and John Viega. The security and performance of the Galois/Counter mode (GCM) of operation. In Canteaut and Viswanathan [134], pages 343–355.

[395] Florian Mendel, Tomislav Nad, Stefan Scherz, and Martin Schläffer. Differential attacks on reduced ripemd-160. In Dieter Gollmann and Felix C. Freiling, editors, *ISC*, volume 7483 of *Lecture Notes in Computer Science*, pages 23–38. Springer, 2012.

[396] Florian Mendel, Tomislav Nad, and Martin Schläffer. Improving local collisions: New attacks on reduced SHA-256. In Johansson and Nguyen [305], pages 262–278.

[397] Florian Mendel, Thomas Peyrin, Martin Schläffer, Lei Wang, and Shuang Wu. Improved cryptanalysis of reduced ripemd-160. In Sako and Sarkar [508], pages 484–503.

[398] Florian Mendel, Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen. On the collision resistance of RIPEMD-160. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 101–116. Springer, 2006.

[399] Florian Mendel, Christian Rechberger, and Martin Schläffer. Update on SHA-1. Presented at Rump Session of Crypto 2007, 2007.

[400] Alfred Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.

[401] Ralph C. Merkle. A certified digital signature. In Brassard [117], pages 218–238.

[402] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer. Kerberos authentication and authorization system. In *In Project Athena Technical Plan*, 1987.

[403] Chris J. Mitchell and Chan Yeob Yeun. Fixing a problem in the helsinki protocol. *Operating Systems Review*, 32(4):21–24, 1998.

[404] Vebjørn Moen, Håvard Raddum, and Kjell Jørgen Hole. Weaknesses in the temporal key hash of WPA. *Mobile Computing and Communications Review*, 8(2):76–83, 2004.

[405] Shiho Moriai, editor. *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*. Springer, 2014.

[406] Masakatu Morii and Yosuke Todo. Cryptanalysis for RC4 and breaking WEP/WPA-TKIP. *IEICE Transactions*, 94-D(11):2087–2094, 2011.

[407] Paul Morrissey, Nigel P. Smart, and Bogdan Warinschi. The TLS handshake protocol: A modular analysis. *J. Cryptology*, 23(2):187–223, 2010.

[408] Steven J. Murdoch, Saar Drimer, Ross J. Anderson, and Mike Bond. Chip and pin is broken. In *IEEE Symposium on Security and Privacy*, pages 433–446. IEEE Computer Society, 2010.

[409] Sean Murphy and Matthew J. B. Robshaw. Essential algebraic structure within the AES. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2002.

[410] Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton. Reconsidering generic composition. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT*, volume 8441 of *Lecture Notes in Computer Science*, pages 257–274. Springer, 2014.

[411] Mridul Nandi. A unified method for improving PRF bounds for a class of blockcipher based MACs. In Seokhie Hong and Tetsu Iwata, editors, *FSE*, volume 6147 of *Lecture Notes in Computer Science*, pages 212–229. Springer, 2010.

[412] Moni Naor, Gil Segev, and Adam Smith. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. In Dwork [181], pages 214–231.

[413] Moni Naor, Gil Segev, and Adam Smith. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. *IEEE Transactions on Information Theory*, 54(6):2408–2425, 2008.

[414] National Security Agency. Suite b cryptography. `http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml`, 2009.

[415] Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Commun. ACM*, 21(12):993–999, 1978.

[416] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The Kerberos Network Authentication Service (V5). RFC 4120 (Proposed Standard), July 2005. Updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113, 6649, 6806.

[417] Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Hash function requirements for Schnorr signatures. *J. Mathematical Cryptology*, 3(1):69–87, 2009.

[418] Phong Q. Nguyen and Igor Shparlinski. The insecurity of the digital signature algorithm with partially known nonces. *J. Cryptology*, 15(3):151–176, 2002.

[419] Phong Q. Nguyen and Igor Shparlinski. The insecurity of the elliptic curve digital signature algorithm with partially known nonces. *Des. Codes Cryptography*, 30(2):201–217, 2003.

[420] Phuong Ha Nguyen, Hongjun Wu, and Huaxiong Wang. Improving the algorithm 2 in multidimensional linear cryptanalysis. In Udaya Parampalli and Philip Hawkes, editors, *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, volume 6812 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 2011.

[421] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *J. Cryptology*, 24(2):292–321, 2011.

[422] NIST Special Publication 180-4. Secure hash standard (SHS). National Institute of Standards and Technology, 2012.

[423] NIST Special Publication 186-4. Digital signature standard (DSS). National Institute of Standards and Technology, 2013.

[424] NIST Special Publication 198-1. The keyed-hash message authentication code (HMAC). National Institute of Standards and Technology, 2008.

[425] NIST Special Publication 800-108. Recommendation for key derivation using pseudo-random functions. National Institute of Standards and Technology, 2009.

[426] NIST Special Publication 800-130. A framework for designing cryptographic key management systems. National Institute of Standards and Technology, 2013.

[427] NIST Special Publication 800-132. Recommendation for password-based key derivation – Part 1: Storage applications. National Institute of Standards and Technology, 2010.

[428] NIST Special Publication 800-38A. Recommendation for block cipher modes of operation – Modes and techniques. National Institute of Standards and Technology, 2001.

[429] NIST Special Publication 800-38C. Recommendation for block cipher modes of operation – The CCM mode for authentication and confidentiality. National Institute of Standards and Technology, 2004.

[430] NIST Special Publication 800-38D. Recommendation for block cipher modes of operation – Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology, 2007.

[431] NIST Special Publication 800-38E. Recommendation for block cipher modes of operation – The XTS-AES mode for confidentiality on storage devices. National Institute of Standards and Technology, 2010.

[432] NIST Special Publication 800-38F. Recommendation for block cipher modes of operation – Methods for Key Wrapping. National Institute of Standards and Technology, 2012.

[433] NIST Special Publication 800-38G. Recommendation for block cipher modes of operation: Methods for format-preserving encryption. National Institute of Standards and Technology, 2016.

[434] NIST Special Publication 800-56A. Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. National Institute of Standards and Technology, 2007.

[435] NIST Special Publication 800-56B. Recommendation for pair-wise key establishment schemes using integer factorization cryptography. National Institute of Standards and Technology, 2009.

[436] NIST Special Publication 800-56C. Recommendation for key derivation through extraction-then-expansion. National Institute of Standards and Technology, 2009.

[437] NIST Special Publication 800-57. Recommendation for key management – Part 1: General (Revision 3). National Institute of Standards and Technology, 2012.

[438] NIST Special Publication 800-67-Rev1. Recommendation for the triple data encryption standard algorithm (tdea) block cipher. National Institute of Standards and Technology, 2012.

[439] NIST Special Publication 800-90A. Recommendation for random number generation using deterministic random bit generators. National Institute of Standards and Technology, 2012.

[440] Kaisa Nyberg, editor. *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*. Springer, 2008.

[441] Kaisa Nyberg and Johan Wallén. Improved linear distinguishers for SNOW 2.0. In Robshaw [489], pages 144–162.

[442] Tatsuaki Okamoto, editor. *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, volume 2964 of *Lecture Notes in Computer Science*. Springer, 2004.

[443] Open SSH Project. OpenSSH project. `http://www.openssh.org/`.

[444] H. Orman and P. Hoffman. Determining Strengths For Public Keys Used For Exchanging Symmetric Keys. RFC 3766 (Best Current Practice), April 2004.

[445] Elisabeth Oswald and Marc Fischlin, editors. *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*. Springer, 2015.

[446] Christof Paar and J. Pelzl. *Understanding cryptography: A textbook for students and practitioners*. Springer, 2009.

[447] Sylvain Pasini and Serge Vaudenay. An optimal non-interactive message authentication protocol. In David Pointcheval, editor, *CT-RSA*, volume 3860 of *Lecture Notes in Computer Science*, pages 280–294. Springer, 2006.

[448] Sylvain Pasini and Serge Vaudenay. Sas-based authenticated key agreement. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 395–409. Springer, 2006.

[449] Kenneth G. Paterson. A cryptographic tour of the IPsec standards. Cryptology ePrint Archive, Report 2006/097, 2006. `http://eprint.iacr.org/`.

[450] Kenneth G. Paterson, editor. *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*. Springer, 2011.

[451] Kenneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt. Plaintext recovery attacks against WPA/TKIP. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 325–349. Springer, 2014.

[452] Kenneth G. Paterson, Thomas Ristenpart, and Thomas Shrimpton. Tag size does matter: Attacks and proofs for the TLS record protocol. In Lee and Wang [364], pages 372–389.

[453] Kenneth G. Paterson, Jacob C. N. Schuldt, and Dale L. Sibborn. Related randomness attacks for public key encryption. In Hugo Krawczyk, editor, *Public Key Cryptography*, volume 8383 of *Lecture Notes in Computer Science*, pages 465–482. Springer, 2014.

[454] Kenneth G. Paterson, Jacob C. N. Schuldt, Martijn Stam, and Susan Thomson. On the joint security of encryption and signature, revisited. In Lee and Wang [364], pages 161–178.

[455] Kenneth G. Paterson and Gaven J. Watson. Plaintext-dependent decryption: A formal security treatment of SSH-CTR. In Gilbert [220], pages 345–361.

[456] Kenneth G. Paterson and Arnold K. L. Yau. Padding Oracle Attacks on the ISO CBC Mode Encryption Standard. In Okamoto [442], pages 305–323.

[457] Kenneth G. Paterson and Arnold K. L. Yau. Cryptography in theory and practice: The case of encryption in IPsec. In Vaudenay [555], pages 12–29.

[458] C. Percival and S. Josefsson. The scrypt Password-Based Key Derivation Function draft-josefsson-scrypt-kdf-01. Internet-Draft (Informational), September 2012.

[459] R. Pereira and R. Adams. The ESP CBC-Mode Cipher Algorithms. RFC 2451 (Proposed Standard), November 1998.

[460] Erez Petrank and Charles Rackoff. CBC MAC for real-time data sources. *J. Cryptology*, 13(3):315–338, 2000.

[461] Birgit Pfitzmann, editor. *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*. Springer, 2001.

[462] Raphael Chung-Wei Phan. Related-key attacks on triple-DES and DESX variants. In Okamoto [442], pages 15–24.

[463] Josef Pieprzyk, editor. *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, volume 5985 of *Lecture Notes in Computer Science*. Springer, 2010.

[464] Krzysztof Pietrzak. A tight bound for EMAC. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 168–179. Springer, 2006.

[465] Leon A. Pintsov and Scott A. Vanstone. Postal revenue collection in the digital age. In Yair Frankel, editor, *Financial Cryptography, 4th International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings*, volume 1962 of *Lecture Notes in Computer Science*, pages 105–120. Springer, 2000.

[466] PKCS #1 v1.5. RSA cryptography standard. RSA Laboratories, 1993.

[467] PKCS #1 v2.1. RSA cryptography standard. RSA Laboratories, 2002.

[468] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3):361–396, 2000.

[469] David Pointcheval and Serge Vaudenay. On provable security for digital signature algorithms. Technical Report LIENS-96-17, 1996.

[470] John M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comput.*, 32(143):918–924, 1978.

[471] Thomas Popp and Stefan Mangard. Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints. In Josyula R. Rao and Berk Sunar, editors, *CHES*, volume 3659 of *Lecture Notes in Computer Science*, pages 172–186. Springer, 2005.

[472] Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-channel resistant crypto for less than 2, 300 ge. *J. Cryptology*, 24(2):322–345, 2011.

[473] Guillaume Poupard and Jacques Stern. Security analysis of a practical "on the fly" authentication and signature generation. In Kaisa Nyberg, editor, *EUROCRYPT*, volume 1403 of *Lecture Notes in Computer Science*, pages 422–436. Springer, 1998.

[474] Bart Preneel, editor. *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*. Springer, 2000.

[475] Bart Preneel and Paul C. van Oorschot. MDx-MAC and building fast MACs from hash functions. In Don Coppersmith, editor, *CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 1995.

[476] Bart Preneel and Paul C. van Oorschot. On the security of iterated message authentication codes. *IEEE Transactions on Information Theory*, 45(1):188–199, 1999.

[477] Gordon Procter. A security analysis of the composition of chacha20 and poly1305. Cryptology ePrint Archive, Report 2014/613, 2014. `http://eprint.iacr.org/2014/613`.

[478] Gordon Procter and Carlos Cid. On weak keys and forgery attacks against polynomial-based mac schemes. In Moriai [405], pages 287–304.

[479] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Johansson and Nguyen [305], pages 142–159.

[480] Niels Provos and David Mazières. A future-adaptable password scheme. In *USENIX Annual Technical Conference, FREENIX Track*, pages 81–91. USENIX, 1999.

[481] Tal Rabin, editor. *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*. Springer, 2010.

[482] K. Raeburn. Advanced Encryption Standard (AES) Encryption for Kerberos 5. RFC 3962 (Proposed Standard), February 2005.

[483] K. Raeburn. Encryption and Checksum Specifications for Kerberos 5. RFC 3961 (Proposed Standard), February 2005.

[484] Ananth Raghunathan, Gil Segev, and Salil P. Vadhan. Deterministic public-key encryption for adaptively chosen plaintext distributions. In Johansson and Nguyen [305], pages 93–110.

[485] Mohammad Reza Reyhanitabar, Shuhong Wang, and Reihaneh Safavi-Naini. Non-interactive manual channel message authentication based on etcr hash functions. In Josef Pieprzyk, Hossein Ghodosi, and Ed Dawson, editors, *ACISP*, volume 4586 of *Lecture Notes in Computer Science*, pages 385–399. Springer, 2007.

[486] Vincent Rijmen. *Cryptanalysis and design of iterated block ciphers*. PhD thesis, Katholieke Universiteit Leuven, 1997.

[487] Thomas Ristenpart and Scott Yilek. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In *NDSS*. The Internet Society, 2010.

[488] Matthew Robshaw and Jonathan Katz, editors. *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*. Springer, 2016.

[489] Matthew J. B. Robshaw, editor. *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*. Springer, 2006.

[490] Matthew J. B. Robshaw and Olivier Billet, editors. *New Stream Cipher Designs - The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*. Springer, 2008.

[491] Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin E. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. *IACR Cryptology ePrint Archive*, 2017:598, 2017.

[492] P. Rogaway. Problems with proposed IP cryptography. Available at `http://www.cs.ucdavis.edu/~rogaway/papers/draft-rogaway-ipsec-comments-00.txt`, 61995.

[493] Phillip Rogaway. Authenticated-encryption with associated-data. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security*, pages 98–107. ACM, 2002.

[494] Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[495] Phillip Rogaway. Nonce-based symmetric encryption. In Roy and Meier [502], pages 348–359.

[496] Phillip Rogaway. Evaluation of some blockcipher modes of operation. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, 2011.

[497] Phillip Rogaway. Free OCB licenses. `http://www.cs.ucdavis.edu/~rogaway/ocb/license.htm`, 2013.

[498] Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, 2003.

[499] Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In Vaudenay [555], pages 373–390.

[500] Phillip Rogaway and David Wagner. A critique of CCM. Cryptology ePrint Archive, Report 2003/070, 2003. `http://eprint.iacr.org/`.

[501] Bimal K. Roy, editor. *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*, volume 3788 of *Lecture Notes in Computer Science*. Springer, 2005.

[502] Bimal K. Roy and Willi Meier, editors. *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*. Springer, 2004.

[503] Markku-Juhani O. Saarinen. Weakness of the OpenSSL PRNG in versions up to OpenSSL 0.9.6a, 2001. `http://mjos.fi/doc/secadv_prng.txt`.

[504] Markku-Juhani O. Saarinen and Jean-Philippe Aumasson. The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). RFC 7693 (Proposed Standard), 2015.

[505] Markku-Juhani Olavi Saarinen. Cycling attacks on GCM, GHASH and other polynomial MACs and hashes. In Anne Canteaut, editor, *FSE*, volume 7549 of *Lecture Notes in Computer Science*, pages 216–225. Springer, 2012.

[506] Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors. *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*. ACM, 2013.

[507] Reihaneh Safavi-Naini and Ran Canetti, editors. *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*. Springer, 2012.

[508] Kazue Sako and Palash Sarkar, editors. *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, volume 8270 of *Lecture Notes in Computer Science*. Springer, 2013.

[509] J. Salowey, A. Choudhury, and D. McGrew. AES Galois Counter Mode (GCM) Cipher Suites for TLS. RFC 5288 (Proposed Standard), August 2008.

[510] Somitra Kumar Sanadhya and Palash Sarkar. New collision attacks against up to 24-step SHA-2. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT*, volume 5365 of *Lecture Notes in Computer Science*, pages 91–103. Springer, 2008.

[511] Yu Sasaki. Meet-in-the-middle preimage attacks on AES hashing modes and an application to Whirlpool. In Antoine Joux, editor, *FSE*, volume 6733 of *Lecture Notes in Computer Science*, pages 378–396. Springer, 2011.

[512] Yu Sasaki and Kazumaro Aoki. Finding preimages in full MD5 faster than exhaustive search. In Antoine Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 134–152. Springer, 2009.

[513] Yu Sasaki, Lei Wang, Kazuo Ohta, and Noboru Kunihiro. Security of MD5 challenge and response: Extension of APOP password recovery attack. In Tal Malkin, editor, *CT-RSA*, volume 4964 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2008.

[514] Yu Sasaki, Lei Wang, Shuang Wu, and Wenling Wu. Investigating fundamental security requirements on whirlpool: Improved preimage and collision attacks. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT*, volume 7658 of *Lecture Notes in Computer Science*, pages 562–579. Springer, 2012.

[515] Takakazu Satoh and Kiyomichi Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Math. Univ. St. Pauli*, 47:81–92, 1998.

[516] J. Schaad and R. Housley. Advanced Encryption Standard (AES) Key Wrap Algorithm. RFC 3394 (Informational), September 2002.

[517] J. Schiller. Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2). RFC 4307 (Proposed Standard), December 2005.

[518] Bruce Schneier. Description of a new variable-length key, 64-bit block cipher (Blowfish). In Ross J. Anderson, editor, *FSE*, volume 809 of *Lecture Notes in Computer Science*, pages 191–204. Springer, 1993.

[519] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In Brassard [117], pages 239–252.

[520] SEC 1. Elliptic curve cryptography – version 2.0. Standards for Efficient Cryptography Group, 2009.

[521] SEC 2. Recommended elliptic curve domain parameters – version 2.0. Standards for Efficient Cryptography Group, 2010.

[522] Igor A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comput.*, 67(221):353–356, 1998.

[523] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Statistical attack on RC4 - distinguishing WPA. In Paterson [450], pages 343–363.

[524] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Statistical attack on rc4 - distinguishing wpa. In Paterson [450], pages 343–363.

[525] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[526] Victor Shoup. A proposal for an ISO standard for public key encryption. Cryptology ePrint Archive, Report 2001/112, 2001. `http://eprint.iacr.org/`.

[527] Victor Shoup, editor. *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*. Springer, 2005.

[528] Thomas Shrimpton and R. Seth Terashima. A provable-security analysis of intel's secure key RNG. In Oswald and Fischlin [445], pages 77–100.

[529] Dan Shumov and Nils Ferguson. On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng, August 2007. Rump session presentation at Crypto 2007, `http://rump2007.cr.yp.to/15-shumow.pdf`.

[530] Sergei P. Skorobogatov. Using optical emission analysis for estimating contribution to power analysis. In Luca Breveglieri, Israel Koren, David Naccache, Elisabeth Oswald, and Jean-Pierre Seifert, editors, *FDTC*, pages 111–119. IEEE Computer Society, 2009.

[531] Nigel P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

[532] Nigel P. Smart. Errors matter: Breaking RSA-based PIN encryption with thirty ciphertext validity queries. In Pieprzyk [463], pages 15–25.

[533] Frank Stajano and Ross J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols Workshop*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–194. Springer, 1999.

[534] D. Stebila and J. Green. Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer. RFC 5656 (Proposed Standard), December 2009.

[535] Marc Stevens. New collision attacks on SHA-1 based on optimal joint local-collision analysis. In Johansson and Nguyen [305], pages 245–261.

[536] Marc Stevens, Pierre Karpman, and Thomas Peyrin. Freestart collision for full SHA-1. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT I*, volume 9665 of *Lecture Notes in Computer Science*, pages 459–483. Springer, 2016.

[537] Marc Stevens, Arjen K. Lenstra, and Benne de Weger. Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. In Moni Naor, editor, *EUROCRYPT*, volume 4515 of *Lecture Notes in Computer Science*, pages 1–22. Springer, 2007.

[538] Marc Stevens, Arjen K. Lenstra, and Benne de Weger. Chosen-prefix collisions for MD5 and applications. *IJACT*, 2(4):322–359, 2012.

[539] Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen K. Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. In Halevi [237], pages 55–69.

[540] Erik Tews and Martin Beck. Practical attacks against wep and wpa. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *WISEC*, pages 79–86. ACM, 2009.

[541] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit WEP in less than 60 seconds. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *WISA*, volume 4867 of *Lecture Notes in Computer Science*, pages 188–202. Springer, 2007.

[542] Kris Tiri and Ingrid Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *DATE*, pages 246–251. IEEE Computer Society, 2004.

[543] Yosuke Todo, Yuki Ozawa, Toshihiro Ohigashi, and Masakatu Morii. Falsification attacks against WPA-TKIP in a realistic environment. *IEICE Transactions*, 95-D(2):588–595, 2012.

[544] Elena Trichina, Tymur Korkishko, and Kyung-Hee Lee. Small size, low power, side channel-immune AES coprocessor: Design and synthesis results. In Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors, *AES Conference*, volume 3373 of *Lecture Notes in Computer Science*, pages 113–127. Springer, 2004.

[545] Eran Tromer, Dag Arne Osvik, and Adi Shamir. Efficient cache attacks on AES, and countermeasures. *J. Cryptology*, 23(1):37–71, 2010.

[546] TTA.KO-12.0001/R1. Digital signature scheme with appendix – Part 2: Certificate-based digital signature algorithm. Korean Telecommunications Technology Association, 2000.

[547] Kyushu University, NICT, and Fujitsu Laboratories. Achieve world record cryptanalysis of next-generation cryptography. `http://www.nict.go.jp/en/press/2012/06/PDF-att/20120618en.pdf`, 2012.

[548] Paul C. van Oorschot and Michael J. Wiener. A known plaintext attack on two-key triple encryption. In Ivan Damgård, editor, *EUROCRYPT*, volume 473 of *Lecture Notes in Computer Science*, pages 318–325. Springer, 1990.

[549] Paul C. van Oorschot and Michael J. Wiener. Parallel collision search with cryptanalytic applications. *J. Cryptology*, 12(1):1–28, 1999.

[550] Mathy Vanhoef and Frank Piessens. All your biases belong to us: Breaking RC4 in WPA-TKIP and TLS. In Ajay Gulati and Hakim Weatherspoon, editors, *USENIX*. USENIX Association, 2016.

[551] Serge Vaudenay. On the weak keys of Blowfish. In Dieter Gollmann, editor, *FSE*, volume 1039 of *Lecture Notes in Computer Science*, pages 27–32. Springer, 1996.

[552] Serge Vaudenay, editor. *Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings*, volume 1372 of *Lecture Notes in Computer Science*. Springer, 1998.

[553] Serge Vaudenay. Security flaws induced by CBC padding - Applications to SSL, IPSEC, WTLS ... In Knudsen [342], pages 534–546.

[554] Serge Vaudenay. Secure communications over insecure channels based on short authenticated strings. In Shoup [527], pages 309–326.

[555] Serge Vaudenay, editor. *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*. Springer, 2006.

[556] Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on RC4. In Adams et al. [10], pages 344–359.

[557] Serge Vaudenay and Amr M. Youssef, editors. *Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers*, volume 2259 of *Lecture Notes in Computer Science*. Springer, 2001.

[558] David Wagner, editor. *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*. Springer, 2008.

[559] Xiaoyun Wang. New collision search for SHA-1. Presented at Rump Session of Crypto 2005, 2005.

[560] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [527], pages 17–36.

[561] Brent Waters. Efficient identity-based encryption without random oracles. In Cramer [158], pages 114–127.

[562] Doug Whiting, Russ Housley, and Neils Ferguson. Submission to NIST: Counter with CBC-MAC (CCM) – AES mode of operation. `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/ccm.pdf`.

[563] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990.

[564] Michael J. Wiener, editor. *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*. Springer, 1999.

[565] Stephen C. Williams. Analysis of the SSH key exchange protocol. In Liqun Chen, editor, *IMA Int. Conf.*, volume 7089 of *Lecture Notes in Computer Science*, pages 356–374. Springer, 2011.

[566] Hongjun Wu. A new stream cipher hc-256. In Roy and Meier [502], pages 226–244.

[567] Hongjun Wu. The stream cipher hc-128. In Robshaw and Billet [490], pages 39–47.

[568] Arnold K. L. Yau, Kenneth G. Paterson, and Chris J. Mitchell. Padding oracle attacks on CBC-mode encryption with secret and random IVs. In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *Lecture Notes in Computer Science*, pages 299–319. Springer, 2005.

[569] Scott Yilek. Resettable public-key encryption: How to encrypt on a virtual machine. In Pieprzyk [463], pages 41–56.

[570] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Authentication Protocol. RFC 4252 (Proposed Standard), January 2006.

[571] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Protocol Architecture. RFC 4251 (Proposed Standard), January 2006.

[572] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Transport Layer Protocol. RFC 4253 (Proposed Standard), January 2006. Updated by RFC 6668.

[573] Jianying Zhou and Moti Yung, editors. *Applied Cryptography and Network Security, 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010. Proceedings*, volume 6123 of *Lecture Notes in Computer Science*, 2010.

[574] L. Zhu and B. Tung. Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). RFC 4556 (Proposed Standard), June 2006. Updated by RFC 6112.

Index