Hashlet

for version 0.1.0, 30 December 2013

Josh Datko (support@cryptotronix.com)

This manual is for Hashlet (version 0.1.0, 30 December 2013), which is a command line application for the Cryptotronix Hashlet.

Table of Contents

Preface

Welcome to the Cryptotronix Hashlet Manual! This manual is meant for end users of the Hashlet, an authentication device designed for the BBB (BeagleBone Black). It is expected that readers of this manual have some familiarity with the BBB and installing and running software on GNU/Linux platforms.

1 Hardware Overview

The Hashlet device as shipped from Cryptotronix, is fully assembled and does not require any end-user assembly. The mini-cape (capelet) is designed to sit on the P9 header of the BBB. See Figure 1.1. It uses pins P9_19 and P9_20 for the I2C protocol. I2C test points are available on the Hashlet for convenient access and debugging.

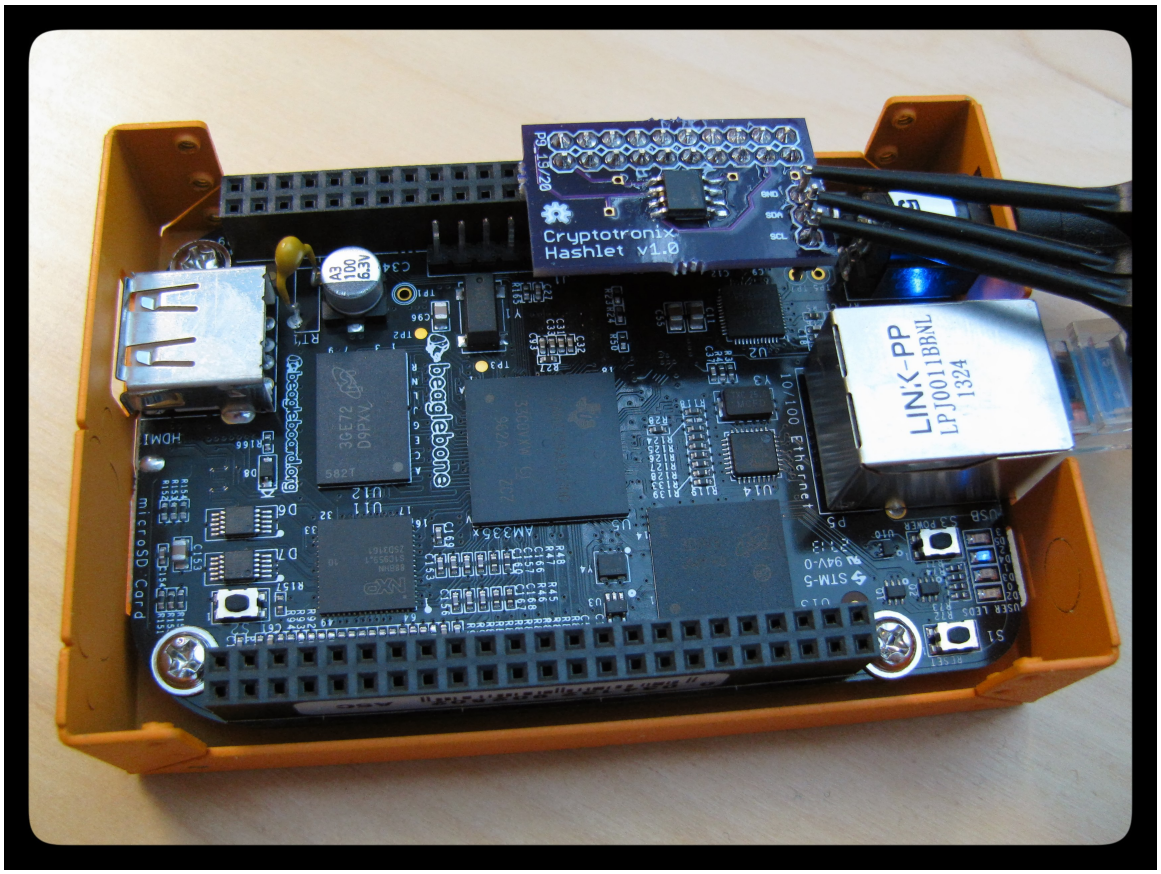

Figure 1.1: Hashlet installed on a BBB using optional test points

The IC (Integrated Circuit) on the Hashlet is the Atmel ATSHA204[1]. The key features of the ATSHA204 used by the Hashlet are:

- Hardware random number generator.
- Lockable configuration, OTP (One Time Programmable), and Data zones
- Slots for 16 keys (14 of which are user keys, 2 are test keys)
- Hardware MAC (Message Authentication Code) using SHA256 and internal data unique to the device.
- Hardware verification of MACs generated on the device.

[1] ATSHA204 Datasheet: http://www.atmel.com/Images/Atmel-8740-CryptoAuth-ATSHA204-Datasheet.pdf

The Hashlet, while designed for a BBB, is 5 Volt compatible and can be used on other platforms like a Raspberry Pi or Arduino. However, the Hashlet software requires a GNU/Linux compatible operating system.

1.1 Schematic

The Hashlet requires only four supply lines. See Figure 1.2. On a BeagleBone Black, the P9 header supplies all the necessary inputs. In their default configuration, pins P9_19 and P9_20 provide I2C data and clock, therefore no extra device tree files are needed to configure the pins.

I2C test points are conveniently brought out to jumper J3 which provides access to the SDA, SCL, and GND lines.

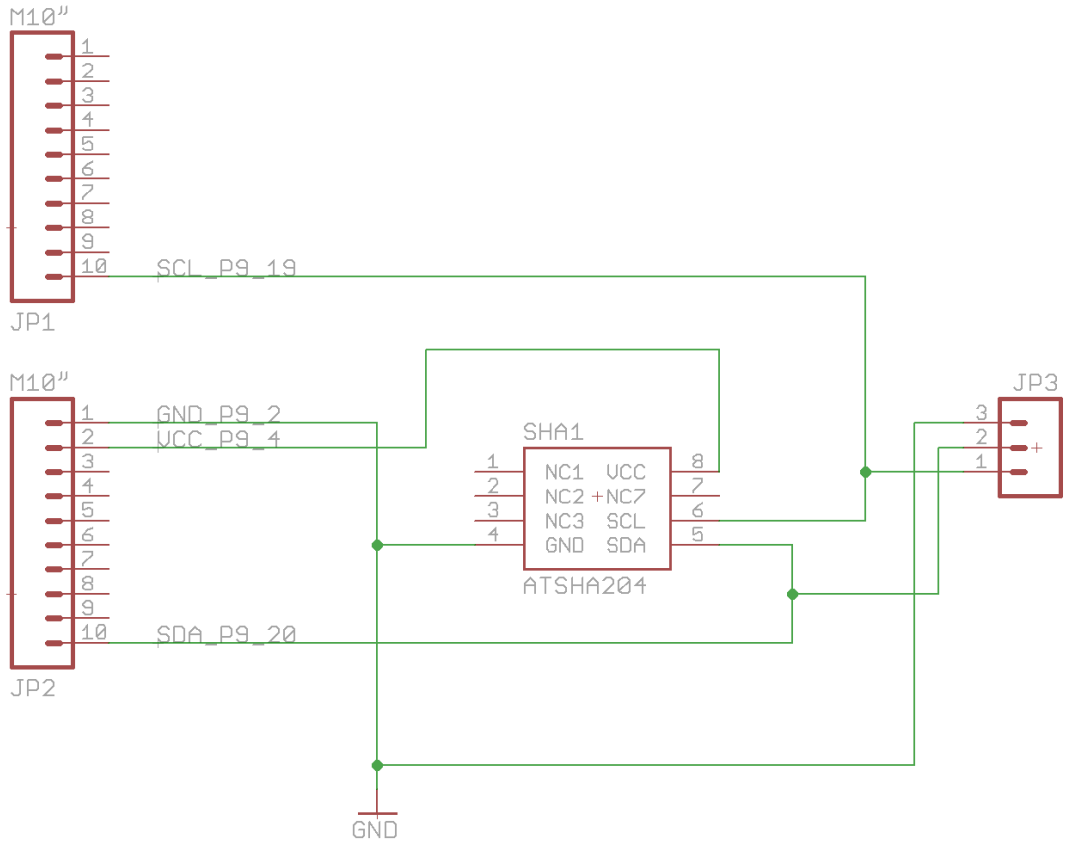

Figure 1.2: Hashlet electrical schematic

2 Installation

2.1 Hardware Installation

The Hashlet ships fully assembled and tested. Remove the device from the static-free bag and attached it to the P9 header of the BeagleBone Black. See Figure 1.1. Once attached, the device is ready for use.

2.2 Software Installation

The latest release for the software is available at `http://download.savannah.gnu.org/releases/hashlet/`. The software was signed with a GPG key with a fingerprint of `0xB5919B1AC7135905F4669C847BFA5031BD2EDEA6`, which you can download from a key server or from Savannah.[1]

After verification, run the typical commands, `./configure` and `make` to build the software. However, to enable all of the features, you should fist install `libgcrypt`. Consult your operating system's package manager for documentation. For Debian, one can install `libgcrypt` as follows: *`sudo apt-get install libgcrypt11-dev`*. If `libgcrypt` is not installed, `configure` will produce a warning. See Listing 2.1.

```
-------------------------------------------------
Unable to find gcrypt.h on this system.
Some features are disabled, install libgcrypt and
rebuild to enable them.
-------------------------------------------------
```

Listing 2.1: Warning messages users can expect if `ibgcrypt` is not installed

Once the software is built, one can install the software with *`sudo make install`*. The default install location is `/usr/local/bin/hashlet`. The hashlet is shipped in a *factory* state. This means that unique keys have not yet been loaded and the device is not ready for cryptographic operation.

Prior to running commands, you should add your user to the `i2c` group, otherwise you will need to run the commands as '`root`', which is not recommended. The first command you should run to ensure that the device is working and is in the correct state is *`hashlet /dev/i2c-1 state`*. The response to this command should be `Factory`. If it's not, contact Cryptotronix support[2].

The next command one should run is *`hashlet /dev/i2c-1 personalize`*. This will configure the hashlet by populating the key slot configuration. See Appendix A [Key Slot Configuration], page 8. It will also fill in random keys in key slots 0-13 and test keys in 14-15. The test keys should not be used for production use. Upon successful personalization, a backup of all keys will be written to `~/.hashlet` in un-encrypted form. The command will silently complete on success, but if you want to ensure that it completed succesfuly, you can verify the exit code is 0 with *`echo $?`*.

[1] `https://savannah.nongnu.org/people/viewgpg.php?user_id=93382`.

[2] `support@cryptotronix.com`

With a device now in the *personalized* state, the output of the `state` command should now be `Personalized`. Also, if you return to the build directory, the `make check` target will now test the cryptographic operation of the device.

Congratulations, you now have a personalized Hashlet!

3 Invoking hashlet

The command `hashlet` requires two positional arguments, `bus` and `command`. The `bus` argument refers to the I2C bus on which the hashlet communications. For offline commands, where the device is not used, this argument should be `/dev/null`. The second command is the command to run. Optional arguments may be supplied and may be relevant depending on the command.

On a BeagleBone Black, the default I2C bus is `/dev/i2c-1`.

3.1 Online Commands

The following list of commands require the Hashlet to be physically attached to the bus in order to succeed.

`state` [Command]

The `state` command returns the state of the device. The three possible results of this command are `Factory`, `Initialized`, and `Personalized`.

- `Factory` This is the device's initial state. Unique keys have not yet been written to the device.
- `Initialized` This is an intermediate state that should not be encountered by users. The meaning of this state is that the configuration zone in the device has been locked, but the data and *One Time Programmable Zone*, has not. Thus, key material in the device my be overwritten in this state.
- `Personalized` This is the final state and indicates that the device is ready for cryptographic operation. The configuration and OTP zones may not be written to and the data slots may be accessed according to the configuration parameters. See Appendix A [Key Slot Configuration], page 8.

`serial-num` [Command]

This command returns the device's serial number. Each device has a non-configurable serial number which is unique. The serial number is always readable in any device state.

`random --update-seed` [Command]

This command returns 32 bytes of random data from the device. Until the device is in the Personalized state, it will return a fixed pattern. The option, `--update-seed`, is available for this command. When supplied, this command will also update the internal random seed on the device. This need not be done frequently.

`mac --key-slot --file` [Command]

This command calculates a SHA256 hash with external and internal data to produce a Message Authentication Code (MAC). See Listing 3.1. The option, `--key-slot`, or `-k`, specifies which key to use in the calculation. The input can either be provided by `stdin` or can be specified with the option, `--file`, or `-f`. In either case, the input is hashed with SHA256 to produce a fixed 32 byte *challenge* to the device. This calculation is performed in software by `libgcrypt`.

```
'SHA256 (Key | SHA256 (Input) | 0x08 | Mode Byte | Param2 | 00000000 |
000 | SN[8] | 0000 | SN[0:1] | SN[2:3])'
```

Listing 3.1: MAC calculation in Hashlet 0.1.0

The response to this command, upon success, will be the following:

```
mac       : C3466ABB8640B50938B260E17D86489D0EBB3F9C8009024683CB225FFFD3B4E4
challenge : 9F0751C90770E6B40E34BA8E06EFE453FAA46B5FB26925FFBD664FAF951D000A
meta      : 08000000000000000000000000
```

The '`mac`' is the result of the calculation. '`Challenge`' is the SHA256 output of the input and '`meta`' is associated meta data that must accompany the data. The meta data is required as input into the `check-mac` operation.[1]

This entire response must be saved in order to verify the mac with the `check-mac` command.

If `--key-slot` is not specified, key slot 0 is used.

`check-mac --challenge-response --challenge --meta-data` [Command]

`check-mac` sends data to the device to test if `--challenge-response` was produced by `--challenge` and `--meta-data`. The short versions of these options are `-r`, `-c`, and `-r` respectively. For this command, these options are *required*. These strings are the output from the `mac` command.

Upon success, the command will exit silently with an exit code of 0. Otherwise, it will display an error and exit with 1.

3.2 Offline commands

The following commands may be run without the Hashlet physically present.

`offline-verify --challenge-response --challenge --key-slot` [Command]

`offline-verify` verifies a MAC produced by the Hashlet. If `--key-slot` is not specified, key slot 0 is used. The options, `--challenge-response` and `--challenge` are *required*.

For this command to work, the backup key file must be located in `~/.hashlet`. However, only the key slot used in the calculation need be included in that file, other key slot entries can be deleted. This calculation works using the fixed values from the `mac` command. See Listing 3.1. In future versions, more sophisticated options will be enabled.

Upon success, the command will exit silently with an exit code of 0. Otherwise, it will display an error and exit with 1.

[1] See the `get_check_mac_meta_data` function for how the meta data is calculated

Appendix A Key Slot Configuration

During the personalization process, the key usage fields are set in the configuration zone. For each of the 16 data slots, there is a corresponding slot configuration that describes how that data slot is used. There are several attributes that control various aspects about the data slot. See Table A.1.

'`ReadKey`' The corresponding slot that is used for encrypted reads.

'`CheckOnly`'
: If set, this slot can only be used in CheckMac operations.

'`SingleUse`'
: If set, this key slot has a limited amount of uses

'`EncryptedRead`'
: If set, encrypted reads are required for this slot

'`IsSecret`'
: If set, encrypted reads and writes are required for this slot

'`WriteKey`'
: The slot of the key used for encrypted writes.

'`DeriveKey`'
: If set, this slot may be written to with the Derive Key command

'`WriteAlways`'
: If set, non-encrypted writes are always allowed

'`WriteNever`'
: If set, writes are never permitted once the Data zone is locked

'`WriteEncrypt`'
: If set, only encrypted writes are permitted.

Table A.1

If '`IsSecret`' is set and '`EncryptedRead`' is not, the slot can never be read. Likewise, if '`WriteNever`' is set, the data slot can not be written.

To alleviate the burden of the user from deciding how to configure their devices, Cryptotronix has picked the following defaults. See Table A.2. These settings are set during personalization. If a property is mentioned, it is set, otherwise it is off (not set).

Keys 0-7 can be used for keyed hashing applications. Keys 8-11 are reserved for password checking features. Slots 12 and 13 allow write and read access and therefore are available for data storage. Key storage in these slots is not recommended. Key slots 14 and 15 are used as fixed test keys and can be read but not written after personalization.

'Data Slot 0'	'IsSecret', 'WriteNever'
'Data Slot 1'	'IsSecret', 'WriteNever', 'DeriveKey'
'Data Slot 2'	'IsSecret', 'WriteNever'
'Data Slot 3'	'IsSecret', 'WriteNever', 'DeriveKey'
'Data Slot 4'	'IsSecret', 'WriteNever'
'Data Slot 5'	'IsSecret', 'WriteNever', 'DeriveKey'
'Data Slot 6'	'IsSecret', 'WriteNever'
'Data Slot 7'	'IsSecret', 'WriteNever', 'DeriveKey'
'Data Slot 8'	'IsSecret', 'WriteNever'
'Data Slot 9'	'IsSecret', 'WriteNever'
'Data Slot 10'	'IsSecret', 'WriteNever'
'Data Slot 11'	'IsSecret', 'WriteNever'
'Data Slot 12'	'WriteAlways'
'Data Slot 13'	'WriteAlways'
'Data Slot 14'	'WriteNever'
'Data Slot 15'	'WriteNever'

Table A.2

Appendix B GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released

under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

   If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

   If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

   If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

   It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

   You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

   A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any,

be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their

titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

   You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

   The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

   In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

   You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

   You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

   A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

   If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

   Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

   If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

   You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

   However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

   Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

   Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

    The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

    Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

    "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

    "CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

    "Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

    An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

    The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  year  your name.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts.  A copy of the license is included in the section entitled ``GNU
Free Documentation License''.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with. . . Texts." line with this:

```
with the Invariant Sections being list their titles, with
the Front-Cover Texts being list, and with the Back-Cover Texts
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Index