CC32xx SHA-MD5 Demo Application

Overview

The SHA/MD5 module provides hardware-accelerated hash functions and can run:

- MD5 message digest algorithm developed by Ron Rivest in 1991
- SHA-1 algorithm compliant with the FIPS 180-3 standard
- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) algorithm compliant with the FIPS 180-3 standard
- The algorithms produce a condensed representation of a message or a data file, called digest or signature, which can then be used to verify the message integrity.
- Hashing of 0 to 233 2 bytes of data (of which 232 1 bytes are in one pass) using the MD5, SHA-1, SHA-224, or SHA-256 hash algorithm (byte granularity only, no support for bit granularity)
- Automatic HMAC key preprocessing for HMAC keys up to 64 bytes
- Host-assisted HMAC key preprocessing for HMAC keys larger than 64 bytes
- HMAC from precomputes (inner/outer digest) for improved performance on small blocks
- Support of μDMA operation for data and context in/result out transfers
- Support of interrupt to read the digest (signature)

Application details

The application is a reference to usage of DES DriverLib functions on CC3200. Developer/User can refer to this simple application and re-use the functions in their applications. This application can be used with our without "Uart Terminal".

If the user wishes to use "Uart Terminal" to give some inputs and follow the execution path prints, then they might do so by defining "USER-INPUT" in the des_main.c file.

- hash: This command allows the user to excercise the hashing (SHAMD5) functionality on CC3200. The command needs a parameter, shamd5_mode.
 - shamd5_mode is the Hashing algorithm that user can choose, the value can be MD5 or SHA1 or SHA224 or SHA256 or HMAC_MD5 or HMAC_SHA1 or HMAC_SHA224 or HMAC_SHA256.

Further, user will be prompted for more inputs

Not defining or un-defining the USER-INPUT will allow the user to follow the execution path on the IAR or CCS IDE, in the "debugging" mode and no input is needed to be given by the user.

Source Files briefly explained

• main.c - The main file that contians the core-logic for encryption and decryption. The functions in the file uses DriverLib calls to perform encryption and decryption.

Supporting files

- **shamd5_userinput.c** This file is used in the USER-INPUT mode. The function in the file reads the input from the user, parses the input string and feed the core-logic functions in the shamd5_main.c
- pinmux.c Generated by the PinMUX utility. UART0 pins are brought out in this file.
- startup_ccs.c CCS related functions
- **startup_ewarm.c** IAR related functions
- uart_if.c Functions to display information on UART

Usage

1. Setup a serial communication application (HyperTerminal/TeraTerm). For detail info visit Terminal setup On the host PC, open a hyperterminal, with the following settings

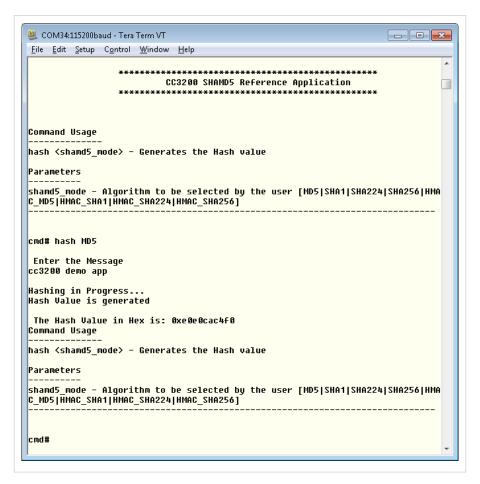
• Port: Enumerated COM port

• Baud rate: 115200

Data: 8 bit Parity: None Stop: 1 bit

• Flow control: None

- 2. Run the reference application.
 - · Flash the bin or
 - Open the project in IAR/CCS.Build and download the application to the board
- 3. On the Hyperterminal, a prompt appears
 - The SHA-MD5 commands need to be issued and the results can be seen



Limitations/Known Issues

None.

Article Sources and Contributors

CC32xx SHA-MD5 Demo Application Source: http://processors.wiki.ti.com/index.php?oldid=178390 Contributors: Codycooke, Jitgupta, Malokyle

Image Sources, Licenses and Contributors

Image:CC3200 shamd5 runScreen.png Source: http://processors.wiki.ti.com/index.php?title=File:CC3200_shamd5_runScreen.png License: unknown Contributors: Codycooke

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

License

1. Definitions

- "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in included in its entirety in unmodified form and or or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License. "Creative Commons Compatible Licenses" means a license that is listed at http://creative/commons.org/compatible/cinesses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and (ii) explicitly permits the relicensing of adaptations of works made available under that license under that license under that license under this License or a Creative Commons jurisdiction license with the same License Elements of this License."

 "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.

 "License Elements" means the following high-level license attributes as selected by Licensors and indicated in the office of this License.

 "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale

2. Fair Dealing Rights

tended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other

to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated

- to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections; to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified."; to Distribute and Publicly Perform the Work including as incorporated in Collections; and, to Distribute and Publicly Perform Adaptations.

 For the avoidance of doubt:

i. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;
ii. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,
iii. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. RestrictionsThe license granted in Section 3 above is expressly made subject to and limited by the following restrictions

- Restrictions

 ileases granted in Section 3 above is expressly made subject to and limited by the following restrictions:

 You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URD) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. Work you must keep intent all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform. When You impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Adaptation on you must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.

 You may Distribute or Publicly Perform an Adaptation on you under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons Compatible License. If you tiense the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that License. If you tiense the Adaptation on the terms of any of the licenses with every copy of each Adaptation on the recipient of the Adaptation on the rems of any of the Recipient of the Adaptation on the rems of the Applicable License with the rems of the Applicable Licenses. If you tiense the Adaptation on the terms of the Adaptation to exercise the rights granted to the terms of the Applicable Licen

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFERINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability
EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE
OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

- This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Seatons 1, 2, 5, 6, 7, and 8 will survive any termination of this License. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will force and effect unless terminated as stated above.

License

8. Miscellaneous

- Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License. Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License. If any provision of this License is invalid or unenforceable land; in the line of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent. This License seconstitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License were drafted utilizing the terminology of the Berne Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Copyright Treaty of 1996, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonagers Treaty of 1996 and the Universal Copyright Convention of as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright Tleaving the support of the parties with the support of the parties of the parties with the license is not intended to restrict the license of any rights under applicable law.