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
- 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 SHAMD5 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) funcitonality 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

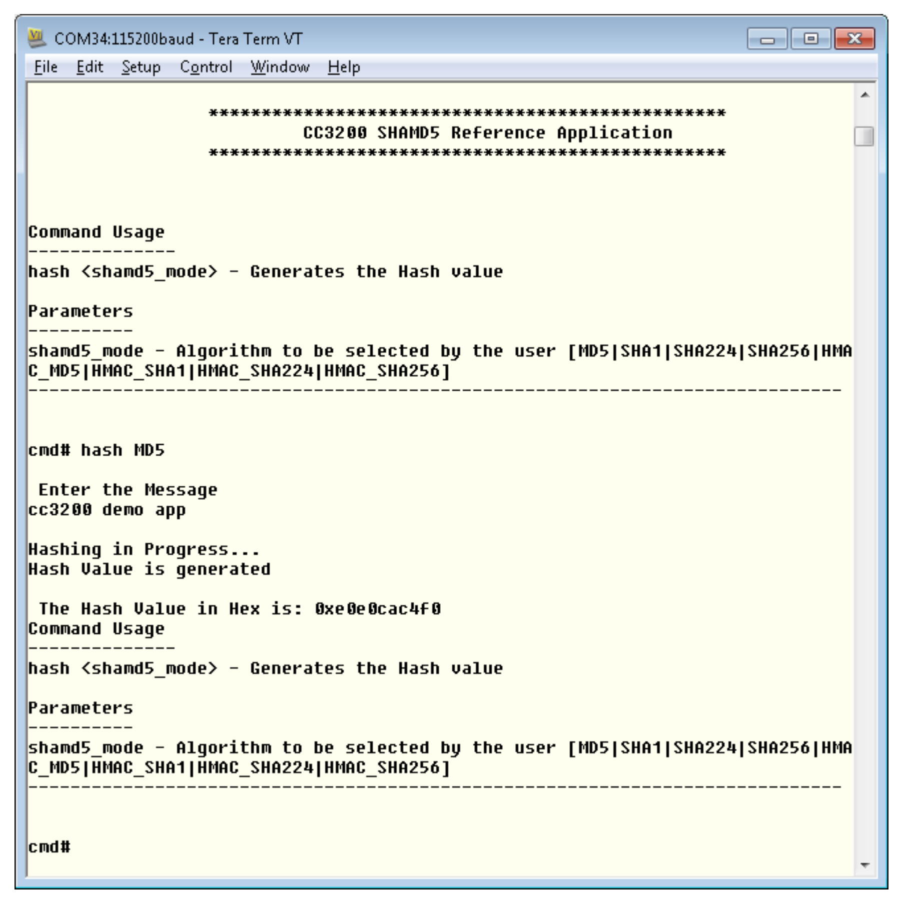
- **main.c** - The main file that contians the core-logic for encryption and decryption. The functions in the file uses DriverLib calls to perform encryption and decryption.

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


COM34:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
                 *************************************************
                          CC3200 SHAMD5 Reference Application
                 *************************************************



Command Usage
--------------
hash <shamd5_mode> - Generates the Hash value

Parameters
----------
shamd5_mode - Algorithm to be selected by the user [MD5|SHA1|SHA224|SHA256|HMA
C_MD5|HMAC_SHA1|HMAC_SHA224|HMAC_SHA256]
-----------------------------------------------------------------------------


cmd# hash MD5

 Enter the Message
cc3200 demo app

Hashing in Progress...
Hash Value is generated

 The Hash Value in Hex is: 0xe0e0cac4f0
Command Usage
--------------
hash <shamd5_mode> - Generates the Hash value

Parameters
----------
shamd5_mode - Algorithm to be selected by the user [MD5|SHA1|SHA224|SHA256|HMA
C_MD5|HMAC_SHA1|HMAC_SHA224|HMAC_SHA256]
-----------------------------------------------------------------------------


cmd#
```

Limitations/Known Issues

None.

Article Sources and Contributors

CC32xx SHA-MD5 Demo Application *Source*: http://processors.wiki.ti.com/index.php?oldid=187564 *Contributors*: Codycooke, Jitgupta, Kaushal, 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