Cryptography_TRNG_Demonstration for KIT_T2G-B-H_LITE

Customer training workshop

Q3 2024

Scope of work

- This code example demonstrates how to generate a one-time password (OTP) of eight characters in length with the True Random Number Generation (TRNG) feature using the cryptography hardware block in MCU. The generated random number consists of alphanumeric and special characters of the ASCII code. The generated OTP is then displayed on a UART terminal emulator.

- **Device**
  - The TRAVEO™ T2G CYT4BF8CDS device is used in this code example.

- **Board**
  - The TRAVEO™ T2G KIT_T2G-B-H_LITE board is used for testing.

Introduction

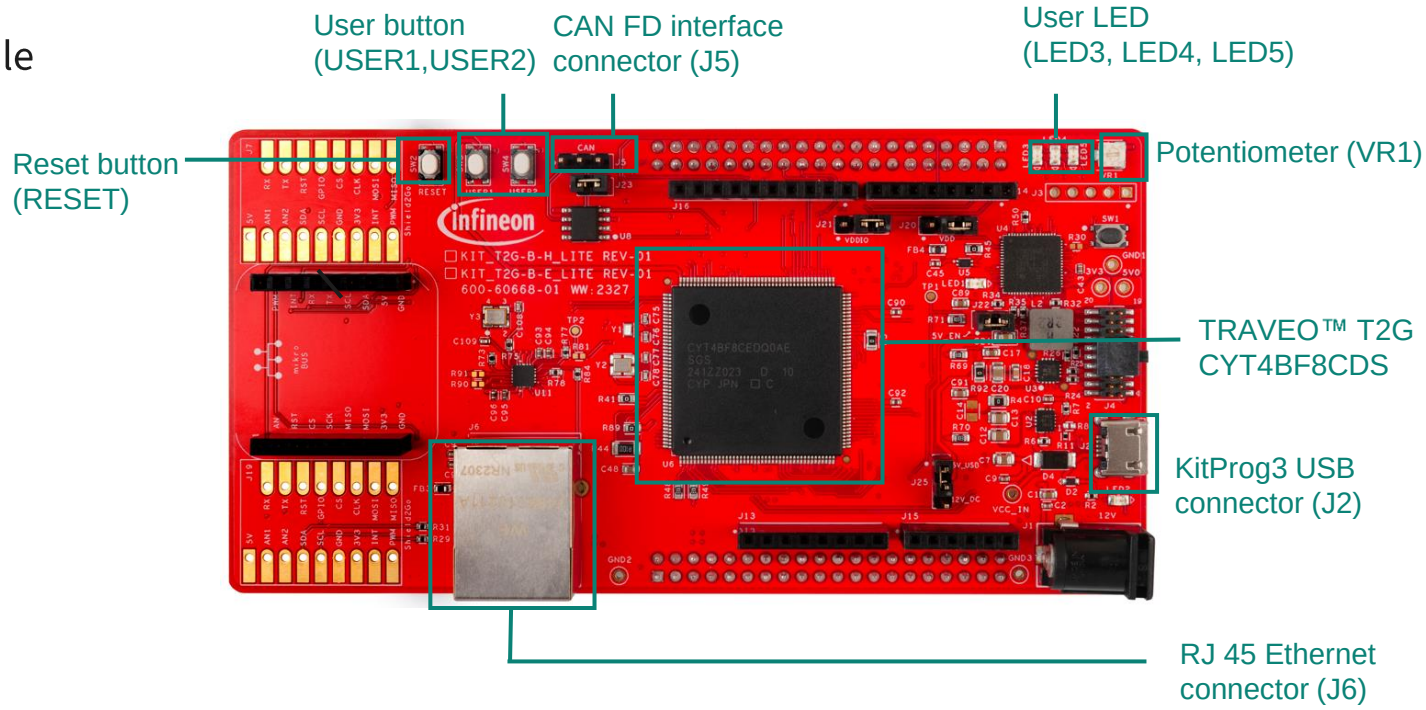
- **The cryptography block has the following features:**
  - Advanced encryption standard (AES) functionality according to FIPS 197:
    The AES component can be used to encrypt/decrypt data blocks of 128-bit length and supports programmable key length (128/192/256-bit key).
  - CHACHA20 functionality according to RFC 7539:
    CHACHA20 is a stream cipher, which produces output consisting of 512-bit random-looking bits. These random-bits can be XORed with plain-text to produce cipher-text.
  - Triple data encryption standard (TDES):
    The TDES component can be used to encrypt/decrypt data blocks of 64-bit length using a 64-bit key.
  - Secure hash algorithm (SHA) functionality according to FIPS 180-4/FIPS-202:
    This component can be used to produce a fixed-length hash (also called “message digest”) of up to 512 bits from a variable-length input data (called “message”). SHA1, SHA2, SHA3 hashes are supported.
  - Cyclic redundancy check (CRC) functionality:
    This component performs a cyclic redundancy check with a programmable polynomial of up to 32 bits.
  - String (STR) functionality:
    This component can be used for efficiently copy, set, and compare memory data.

Introduction (contd.)

- Pseudo Random Number Generator (PRNG):
  This component generates pseudo random numbers in a fixed range. This generator is based on three Linear Feedback Shift Registers (LFSRs).
- True Random Number Generator (TRNG):
  This component generates true random numbers of up to 32 bits using ring oscillators.
- Vector unit (VU):
  This component act as coprocessors to offload asymmetric key operations from the main processor.
- AHB master-interface:
  This allows to fetch operands directly from the system memory.
- Device key functionality:
  The device key usage is restricted to specific functionality; it cannot be accessed by the software that implements that functionality.
  Two independent device keys are supported.

Hardware setup

- This code example has been developed for the KIT_T2G-B-H_LITE board.
- Connect the PC to the board using the provided USB cable through the KitProg3 USB connector (J2).



Implementation

- In this example, an OTP of eight characters in length is generated. The generated OTP is then displayed on an UART terminal emulator. The firmware generates a new OTP instantly when the user press the enter key.

- **The following steps are followed to configure the code example:**
  - Configure the STDIN/STDOUT
  - Display the initial message to the terminal and check the key operation
  - Generate password

- **Configure the STDIN/STDOUT:**
  - Initialization of the GPIO for UART is done in the ***cy_retarget_io_init()*** function
    - Initialize P0.1 as UART TX, P0.0 as UART RX (these pins are connected to the KitProg3 COM port)
    - The serial port parameter changes to 8N1 and 115200 baud

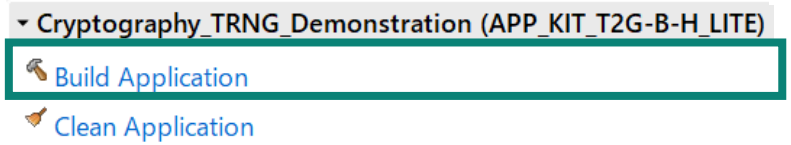
Implementation (contd.)

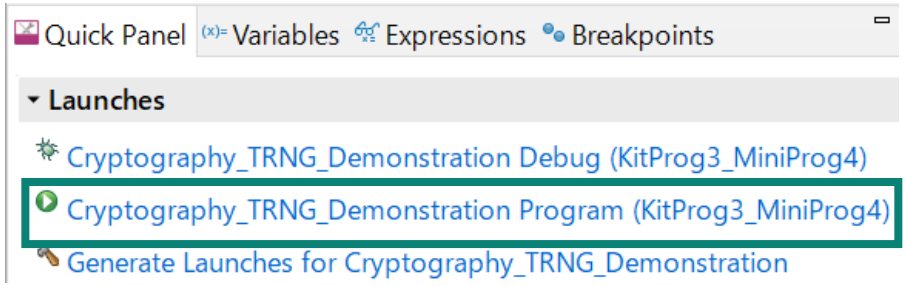
- **Display the initial message to the terminal and check key operation**
  - The terminal can be displayed by ***printf()***
    - The display data is specified as ***CLEAR_SCREEN*** and ***SCREEN_HEADER***
  - The checking of key operation is done in the ***cyhal_uart_getc()*** function
    - In this sample, it checks if the enter key was pressed

- **Generate password**
  - OTP generation of eight characters is done in the ***generate_password()*** function. This function runs the following:
    - Initialization of the cryptography TRNG block is done in the ***cyhal_trng_init()*** function
      - Generates a random number using the ***cyhal_trng_generate()*** function
        - The generated 32-bit random number is converted to an 8-character ASCII code.
        - The OTP is displayed on the terminal by ***printf()***
      - The random number generator block is released by the ***cyhal_trng_free()*** function
      - The OTP length can be changed by modifying the ***PASSWORD_LENGTH*** value

Compiling and programming

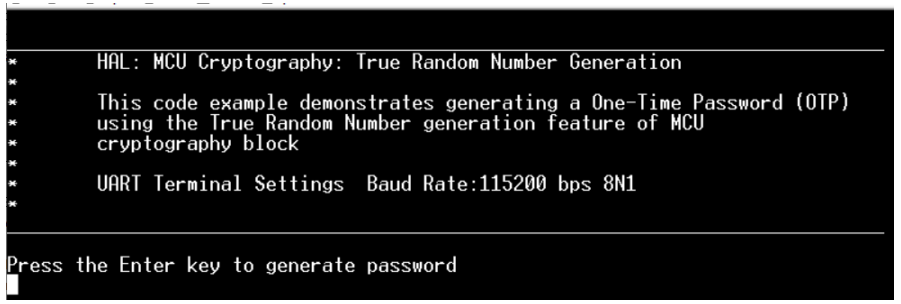
1. Connect to power and USB cable
2. Use Eclipse IDE for ModusToolbox™ software for compiling and programming
3. For compilation:
   a. Select the target application project in the Project Explorer
   b. In the Quick Panel, scroll down, and click **“Build Application”** in the Cryptography_TRNG_Demonstration (APP_KIT_T2G-B-H_LITE)
4. Open a terminal program (such as Tera Term) and select the KitProg3 COM port. Set the serial port parameters to **8N1** and **115200 baud**.
5. For programming:
   a. Select the target application project in the Project Explorer
   b. In the Quick Panel, scroll down, and **click “Cryptography_TRNG_Demonstration Program (KitProg3_MiniProg4)”** in Launches





Run and test

1. Once the programming is successfully complete, a message is displayed in the terminal window as shown in the figure.
2. When you press the enter key, an OTP is generated and displayed.
3. When you press the enter key again, another OTP is generated and displayed.



References

- Datasheet
  - CYT4BF TRAVEO™ T2G 32-bit Automotive MCU based on Arm® Cortex®-M7 dual
- Architecture reference manual
  - TRAVEO™ T2G Automotive MCU body controller high architecture reference manual
- Registers reference manual
  - TRAVEO™ T2G Automotive MCU: TVII-B-H-8M body controller high registers reference manual
- PDL/HAL
  - Peripheral driver library (PDL)
  - Hardware Abstraction Layer (HAL)
- Training
  - TRAVEO™ T2G training

Revision History

Revision	ECN	Submission Date	Description of Change
**	7782086	2022/07/05	Initial release
*A	8067465	2024/08/27	Replaced development board from KIT_T2G-B-H_EVK to KIT_T2G-B-H_LITE