IDEC Chip Design Contest

Design and Implementation of Security SoC Prototype Based on Cortex M0

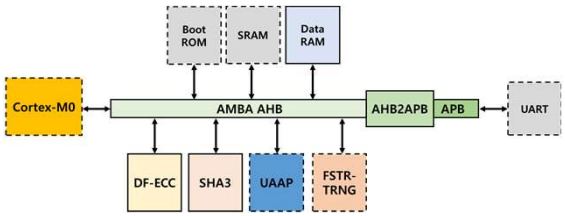
Dong-Seong Kim, Jun-Baek Choi, Jun-Yeong Choe, Kyung-Wook Shin
School of Electronic Engineering, Kumoh National Institute of Technology, Korea

1. Introduction

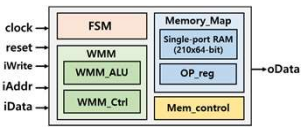
- In today's IoT era, security SoC is attracting attention to overcome the limitations of security technologies implemented by software.
- Security SoC has advantages of both hardware and software, as the crypto-cores are implemented in the hardware to increase safety and enable security protocols to be implemented in software.
- A security SoC prototype was designed using Cortex-M0 as CPU, and it integrates crypto-cores including ECC (Elliptic Curve Cryptography) core, SHA3 hash core, ARIA-AES core, and TRNG core.

2. A Design of Security SoC

2.1 Architecture of Security SoC

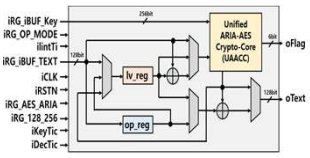


2.2 DF-ECC Core



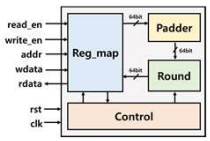
- DF-ECC core was designed to support eight elliptic curves (ECs) over GF(p), and twelve over GF(2^m) of ECs defined in the standard document SEC2.
- It offers four point operations over EC and five modular operations based on word-based Montgomery modular multiplier (WMM).
- WMM consists of two PEs which are designed with pipelined structure.

2.3 UAAP



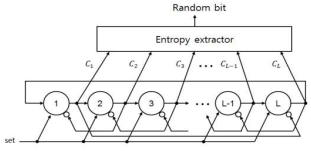
- UAAP efficiently integrates two block ciphers ARIA and AES.
- It was designed to support 128-bit and 256-bit key sizes, as well as five modes of operation including ECB, CBC, CFB, OFB, and CTR.
- Based on the common characteristics of ARIA and AES algorithms, it was optimized by sharing hardware resources in substitution layer and in diffusion layer.

2.4 SHA3 Hash Core



- It supports four different message digest sizes of 512, 384, 256, and 224 bits depending on the hash function used.
- Round block was designed with a round-iterative structure of 1600-bit data-path.
- Padder block was designed using hexadecimal form to pad messages are byte-aligned such as ASCII.

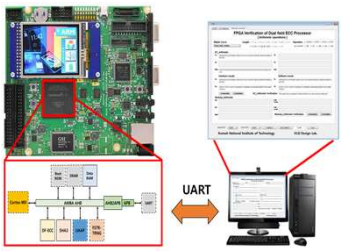
2.5 FSTR-TRNG



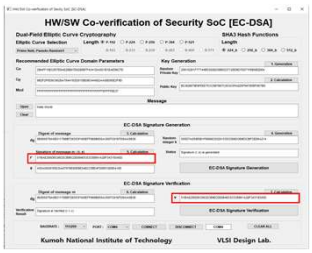
- To reduce hardware complexity of TRNG, an entropy extractor with feedback structure was proposed, which minimizes the number of ring stages.
- The number of ring stages of the FSTR-TRNG was determined to be a multiple of eleven, taking into account operating clock frequency and entropy extraction circuit.
- The tokens to bubbles ratio was determined to operate in evenly-spaced mode.

3. HW/SW Co-verification of Security SoC

3.1 HW/SW co-verification platform



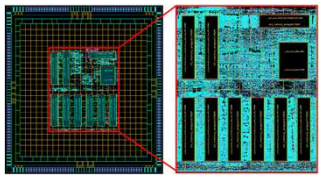
3.2 Verification results



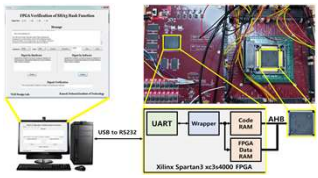
- For HW/SW co-verification, a V2M-MPS2 board equipped with a Cyclone-V FPGA was used.
- Software programmed into the Cortex-M0 controls each slave, and serial communication with PC is done through the UART port.
- Python software for GUI was used to monitor the operation of the Security SoC.
- The results of HW/SW co-verification show EC-DSA (Elliptic Curve Digital Signature Algorithm) operation with P192K1 EC and SHA3-224 modes.

4. Chip Implementation and Test

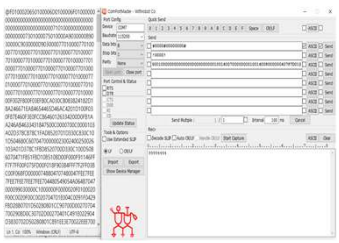
4.1 Layout design



4.2 Chip test setup



4.3 Test results of Security SoC



- The security SoC was implemented with a 65nm CMOS technology.
- Chip test was carried out using the test setup shown above with 25 MHz clock.
- According to test results, it was confirmed that read/write operations of Cortex-M0 with data RAM and some arithmetic operations worked correctly, but the operation of the entire chip was not confirmed.

5. Conclusion

- A security SoC prototype, which integrates a Cortex-M0 with crypto-cores including an ECC core, a SHA3 hash core, an ARIA-AES core, and a TRNG core, was designed, and the HW-SW co-verification was carried out using a Cyclone-V FPGA device.
- Our security SoC that has a hardware complexity of 193,312 GEs and 84 Kbits RAM was implemented with a 65nm CMOS technology, and some functions of the SoC were tested.

6. Acknowledgement

- The chip fabrication and EDA tool were supported by the IC Design Education Center(IDEC), Korea.