# 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

dock -	FSM	Memory_Map	
reset →	WMM	Single-port RAM (210x64-bit)	
iWrite →	WMM_ALU	OP_reg	→oDat
iData →	WMM_Ctrl	Mem_control	

- DF-ECC core was designed to support eight elliptic curves (ECs) over GF(p), and twelve over GF(2<sup>m</sup>) of ECs defined in the standard document SEC2.
- It offers four point operations over EC and five modular operations based on wordbased 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



**DEC** Chip Design Contest

- 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

#### 2.5 FSTR-TRNG

byte-aligned such as ASCII



- 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

BF010052065013000600100006F01000000	ConfutNate - little	ear Co	- x
000000000000000000000000000000000000000	Put Certs	Quarter	
000000000000000000000000000000000000000	Desix (DMT	8 1 2 3 4 5 4 7 8 8 A 8 1 3 5 F Sec. OU	DHED
00000007301300275013005A3030000890	Saddt 11010 -	364	
3000003030000303000077310000770100	100301	[] enoneutoconte	E AND E See
00770100007701000077010000770100007	810 Mt 2	7 - 1600	T AKE ( See
72100007721000077210000770100007701	Avir ters -	The second secon	Carre Dawn
00007755000077050000770500007705000	Inclusion Count	1	D'atte Class
67791900077010000770100007704000077	Bud Particle Status	N	10000000
21080077010800770100087701000877019	Cets	<u></u>	L AGE LI SHE
000170100001701000017010000	Com.	<u></u>	L 402 L 944
DOPOLYBODPOLEPBOCAD DC BDEBL/4152/L1	- 12 I	9	D AKB D Seve
SA2406/15A54654465046ACA2010100FLS	-5	0	1 482 1 Set
ETAL ALBORIT AND COMPANY TO COMPANY AND THE	lippers force	Sed Rubpe   1/1   3tensi   38 mi   0	.06
4/00/239/879/144/95/2020/2020/28/0/10	Tool & Grann	ho	
15504800560340300000230024025005	Cite Intended 52	Colorade SUP Charles OUS _ Hereite COLD (Start Debun)	453 04
103A010378C1F80#5207000330C1000548	80 Cau	Reading the standard sector of the standard sector and an a sector of the standard sector sec	hereferent
90794/114514901051080004000491346FF	Post Cost		
117/1100F0/5000F0/59/8038411-1/2/1038	These Device Manager		
THE THE THE THE TAKEN AND A CARDINET			
300799630000° 1/00700F0000520F0100520			
100000206000020470180040094563429			
PB02880701050280801009070704	1.00		
1002908D0C30702000275401C4918022904	Yon		
03830702050280801C8916E3E700226EF700	000		
UNITE STATE AND AND AND	$\sim$		

## 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.

