정 보 보 호 학 회 지
제25권 제2호, 2015. 4

사물인터넷 디바이스 상의 암호기법 구현 기술 동향 및 전망

박 태 환*, 서 화 정*, 김 지 현*, 최 종 석*, 김 호 원*

요 약

본 논문에서는 최근 각광받고 있는 사물인터넷 기술 중 디바이스 상의 암호기법 구현 기술의 최신 동향과 앞으로의 전망을 알아보고자 한다. 이를 위해, 사물인터넷 디바이스에 대해 프로세서 기반으로 분류를 하여, 각각의 사물인터넷 디바이스의 특징과 각 디바이스에 대한 암호기법 구현 기술 현황 분석을 통해, 현재 사물인터넷 디바이스 상의 암호기법 구현 기술의 문제점과 앞으로의 사물인터넷 환경에서의 디바이스에 대한 암호기법 구현의 전망을 살펴본다.

Ⅰ. 서 론

최근 사물인터넷 기술의 발달로 인해, 많은 사물인터넷 기반의 서비스와 연구가 이루어지고 있다. 전 세계 사물인터넷 디바이스 시장은 2013년에는 1,888억 달러에서 2022년에 4,450억 달러의 규모로 성장할 것으로 예측되고 있다[1]. 특히, 사물인터넷 통신모듈과 단말기의 경우, 평균 18.3%와 8.8%의 평균 성장률을 가질 것으로 예상되고 있다[1]. 이러한 시장규모와 성장률을 가지는 사물인터넷 디바이스 시장은 4-, 8-, 16-, 32-bit 기반의 다양한 프로세서를 사용하고 있으며, Atmel 사, ARM 사, TI사, EPSON 등 다양한 기업에서 사물인터넷 디바이스 기술을 확보하고 있다. 본 논문에서는 앞서 설명한 다양한 사물인터넷 디바이스의 특성 분석과 사물인터넷 디바이스 상의 암호기법 기법 구현 기술 동향 및 앞으로의 전망에 대해 알아보고자 한다. 논문의 구성은 2장에서 현재 사용되고 있는 다양한 사물인터넷 디바이스 별 특성과 동향에 대해 알아보고, 3장에서는 2장에서 설명한 사물인터넷 디바이스 별 암호기법 구현 기술 동향에 대해 알아보며, 4장에서는 사물인터넷 디바이스 상의 암호기법 구현 기술 비교 분석 및 앞으로의 전망에 대해 알아보며, 5장의 결론으로 구성된다.

Ⅱ. 사물인터넷 디바이스 동향

본 장에서는 현재 사용되어지는 다양한 사물인터넷 디바이스에 대해, 각 디바이스에서 사용 중인 프로세서 별로 분류하여 각 디바이스의 특성에 대해 알아보고자 한다.

2.1. 4-bit 프로세서 기반 사물인터넷 디바이스

본 절에서는 사물인터넷 디바이스 중, 초경량(4-bit) 사물인터넷 디바이스에 해당하는 Atmel사의 MARC4 프로세서와 EPSON의 S1C63 계열 프로세서에 대해 알아본다.

2.1.1. Atmel MARC4 프로세서

Atmel사의 MARC4 프로세의 특징은 기존의 8, 16, 32-bit 기반의 프로세서와 달리, Stack Machine 기반의 프로세서 구조를 가지며, 16kHz, 500kHz 혹은 2MHz로 동작하며, 저장 공간의 경우, EEPROM(4kBytes), RAM (4way-256bytes), 1mA의 저전력의 전력소모(active mode) 특징이 있으며, 온도 -40~125 상에서 동작이 가능하다. 전원의 경우, 1.8V~6.5V사이의 전원으로 동작이 가능하며, 주 응용 분야는 리모컨, 인터넷 뱅

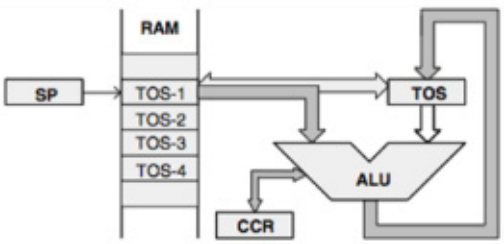
본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1017)

* 부산대학교 전기컴퓨터공학부 (pth5804@pusan.ac.kr, hwajeong84@gmail.com, jihyunkim@pusan.ac.kr, js.choi85@gmail.com, howonkim@pusan.ac.kr)

킹 토큰, 자동차 키 등에 사용되고 있다.

Atmel MARC4 프로세서의 Stack 기반의 연산은 아래의 블록도와 같이 Stack의 TOS레지스터를 이용하여 2개의 피연산사를 ALU로 가지고와서 연산을 처리하게 된다.

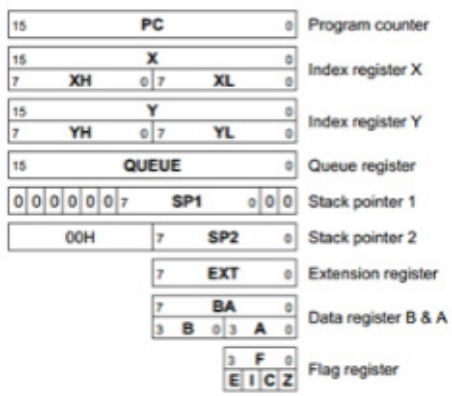
Atmel MARC4 프로세서는 직접(Direct), 간접(Indirect), Stack Pointer(SP)를 이용한 방식(8-bit단위), 6-bit short, 12-bit long 주소 형식을 지원한다. 레지스터의 경우, 8-bit RAM 주소 레지스터 X, Y와 8-bit RAM 주소 레지스터 X, Y와 8-bit Expression Stack Pointer(SP), Return Stack Pointer(RP, 12-bit), 상태 정보 저장을 위한 Conditional Code Register(CCR), 프로그램 수행순서 확인을 위한 Program Counter(PC, 12bit), Top Of Stack(TOS) 레지스터, 6개의 programmable 레지스터로 구성된다.



〔그림 1〕 Atmel MARC4 Stack기반의 연산 블록도

2.1.2. EPSON S1C63 계열 프로세서

EPSON의 S1C63계열 프로세서는 앞서 설명한 Atmel의 MARC4 프로세서와 동일하게 4-bit 프로세서 기반이며, Stack Machine기반의 구조를 가진다, 주소 방식은 직접(Direct), 간접(Indirect, 2개), Stack Pointer (SP)를 이용한 방식을 제공하고 있다. 저장 공간의 경우, 26kB code ROM(16k*13bits), 1kB data ROM (2k*4bits), 2kB ROM(4k*4bits)를 지원한다. EPSON S1C63C는 2개의 4-bit 데이터 레지스터 A, B, 4-bit 플래그 레지스터 F(확장 E, 인터럽트 I, 캐리 C 그리고 제로 플래그 Z로 구성), 2개의 16bit 인덱스 레지스터 X, Y (post-increment 명령어 지원), 2개의 8bit stack pointers SP1(주소 용), SP2(데이터 용)을 지원하고 있으며, stack pointer에 대해 주소용과 데이터용으로 나누어 사용한다는 점에서 앞서 설명한 Atmel의 MARC4와의 차이가 있다. EPSON S1C63C 계열 레지스터의 구성은 아래의 그림과 같다.



〔그림 2〕 EPSON S1C63 family 레지스터 구성

2.2. 8-bit 프로세서 기반 사물인터넷 디바이스

본 절에서는 경량 사물인터넷 디바이스에 해당되는 8-bit 프로세서 기반의 사물인터넷 디바이스의 특성에 대해 설명한다. 대표적인 8-bit 프로세서 기반의 사물인터넷 디바이스로는 Atmel 사의 Atmega128이 있다. Atmega128은 앞서 설명한 4-bit 프로세서 기반의 초경량 사물인터넷 디바이스에 비해 높은 동작 주파수와 많은 명령어 셋을 가진다는 점에서 차이가 있다.

Atmel 사의 Atmega128의 명령어 셋(instruction Set)의 특징은 133개의 명령어을 지원하며, 대부분의 명령어를 1사이클에 수행되며, 1MHz의 클록으로 1MIPS 성능을 얻을 수 있다는 특징을 가지고 있다.

Atmel 사의 Atmega128의 주소방식은 I/O Direct, Data Direct/Indirect(with Displacement, Pre-decrement, Post-Increment), Program Memory Constant Addressing로 구성된다.

저장공간의 경우, 4KBytes EEPROM을 지원하며, 128KBytes ISP(In System Programming)이 가능하며, 4KBytes의 내부 SRAM은 최대 64KBytes 까지 확장이 가능하다.

Atmega128의 레지스터는 Status Register(SREG), X, Y, Z: Indirect Address Register(X=R27:R26, Y=R29:R28, Z=R31:R30)(16bit), Stack Pointer, 32개의 8-bit 범용 레지스터, RAM Page Z 선택 레지스터로 구성된다.

2.3. 16-bit 프로세서 기반 사물인터넷 디바이스

본 절에서는 16-bit 프로세서 기반의 대표적인 경량 사물인터넷 디바이스인 TI사의 MSP430의 특성에 대해 알아본다.

TI사의 MSP430의 명령어 셋(Instruction Set)은 27개의 명령어 셋로 구성되어 있으며, Register Mode, Indexed Mode, Symbolic Mode, Absolute Mode, Indirect Register Mode, Immediate Mode로 총 6가지의 주소방식을 지원한다. 저장 공간의 경우, 60kB flash program memory, 256bytes flash information memory, 2kB RAM으로 구성되어 있다. MSP430의 레지스터는 16개의 16-bit 레지스터(R0~R15), R0(program counter), R1(stack pointer), R2(status), R3(constant generator) 와 범용 레지스터:R4~R15로 구성된다.

2.4. 32-bit 프로세서 기반 사물인터넷 디바이스

본 절에서는 32-bit 기반의 고성능 사물 인터넷(IoT) 디바이스 중 대표적인 ARM-Cortex A9 32-bit 마이크로컨트롤러의 특성에 대해 설명한다. ARM-Cortex-A9는 ARMv7 기반이며, 멀티코어, 쿼드코어 지원, NEON SIMD강화, 비순차적 명령어처리 지원을 통해, 명령 실행 효율을 높이는 특징이 있다. 이러한 Cortex-A9에는 NEON 미디어 처리 엔진(MPE)를 통한 연산 효율을 높이고 있다. NEON 미디어 처리 엔진(MPE)는 쿼드-MAC, 매 주기 별 8, 16, 32-bit 정수와 32-bit 부동 소수 데이터 관련 SIMD 운영세트 지원하며, 64-bit 및 128-bit 레지스터 세트 제공과 FPU에서 이용할 수 있는 레지스터 파일 확대 기능이 있으며, unsigned, signed integer 연산, single bit coefficient polynomial, single-precision floating-point value를 지원하는 특징을 가지고 있다. 고성능의 연산을 위해, ARM Cortex-A9은 32개 32-bit 레지스터 S, 32개 64-bit 레지스터 D, 16개 128-bit 레지스터 Q, 벡터 소수점 연산(Vector Floating Point, VFP)을 제공하는 FPSID 레지스터, FPU 제어를 위한 FPSCR 레지스터, advanced NEON, VFP 확장을 위한 FPEXC 레지스터로 구성되어 있다.

Ⅲ. 사물인터넷 디바이스 상의 암호기법 구현 기술 및 연구 동향

본 장에서는 앞서 2장에서 살펴본 4, 8, 16, 32-bit 프로세서 기반의 사물인터넷 디바이스 상에서의 암호화 구현 연구 및 최신 동향에 대해 알아본다.

3.1. 4-bit 프로세서 기반 사물인터넷 디바이스 상의 암호기법 구현 기술 및 연구 동향

본 절에서는 4-bit 마이크로프로세서 기반의 초경량 사물인터넷 디바이스인 Atmel MARC4와 EPSON S1C63 계열 프로세서 상에서의 암호 구현 연구 사례에 대해 알아본다.

3.1.1. Atmel MARC4 프로세서 상의 암호기법 구현 연구 사례

본 절에서는 Atmel MARC4 프로세서 상에서의 암호 기법 구현 연구 사례에 대해 알아본다. PRESENT 암호 기법의 경우, 4x4 S-Box를 사용한다는 점에서 4-bit 프로세서에 매우 적합하며, PRESENT-80(key size:80-bit, block size: 64-bit) 암호 기법을 MARC4프로세서에 구현 하여, 1,250byte의 코드 크기와 6,967 cycle/byte의 성능을 나타내는 것으로 확인되었다[2].

AES 암호기법의 경우, 4-bit 프로세서 기반 환경에서의 구현은 Atmel MARC4프로세서에 가장 먼저 구현이 되었으며, 4-bit 환경에 맞게 분기문 삭제와 S-Box와 Shiftrow연산을 결합하여 구현하였으며, AES-128에 대하여 23,828bytes의 코드 크기와 1,489cycle/byte 그리고 15,848byte의 코드 크기와 991cycle/byte의 성능을 나타내었다[3].

PRINTcipher의 경우, Block의 크기가 48-, 96-bit이며, 키 스케쥴이 필요하지 않은 장점을 가지며, S-Box가 3-bit단위로 구성되어 4-bit 프로세서의 구현에 있어서 장점을 가진다. 이러한 PRINTcipher의 성능은 PRINTcipher48에 대하여, 각각 490/10,415, 1,250/5,013, 2,788/2,819(코드사이즈(Byte)/키생성+암호화(Cycle/byte))의 성능을 나타내었다[4].

Hummingbird 암호기법의 경우, 16-bit의 Block 크기와 4-bit 기반의 S-Box로 구성되어 4-bit환경에 적합

한 장점을 가지며, 키 크기가 256-bit인 경우에 대해, 1,532byte의 코드 크기와 2,877Cycle/byte의 성능을 나타내었다[5].

3.1.2. EPSON S1C63 계열 프로세서 상의 암호기법 구현 연구 사례

본 절에서는 EPSON의 S1C63계열 프로세서 상의 암호기법 구현 연구사례에 대해 알아본다.

EPSON의 S1C63계열 프로세서는 앞서 설명한 Atmel의 MARC4 프로세서와 동일하게 4-bit 프로세서 구조를 가지며, Atmel MARC4의 경우와 달리 대칭키 암호기법뿐만 아니라 공개키 암호기법에 대한 구현 연구가 진행되었으며, 이에 대해 설명한다.

3.1.2.1. EPSON S1C63 계열 프로세서 상의 대칭키 암호기법 및 해쉬 함수 구현 연구 사례

EPSON S1C63계열 프로세서 상에서도 앞서 설명한 Atmel MARC4에서 구현된 AES가 구현되었으며, MixColumns, Key Expansion, AddRoundKey 부분을 통합하여 구현하였으며, Loop unrollilng과 in-line기법을 적용하여 AES-128의 경우, 메모리 최적화 기법 적용 시, 1,294bytes의 코드 크기와 17,347Cycles의 성능을 보였으며, 속도 최적화의 경우, 2,645bytes의 코드 크기와 13,749cycles의 성능을 나타내었다[6]. 앞서 설명한 속도 최적화 기법 적용을 통해, Atmel MARC4에서의 구현 결과 보다 속도를 향상 시켰다.

SHA-1 해쉬 함수에 대하여, 30-bit left rotation 연산을 2-bit right rotation연산으로 대치하였으며, Loop-unrolling과 in-line기법 적용을 통한 속도 향상이 있었으며, Round 함수의 재사용을 통해, 코드 크기를 최소화하였으며, 코드 크기 최적화의 경우, 2,038bytes의 코드 크기와 108,666 Cycles/block의 성능을 보였으며, 속도 최적화의 경우, 2,324bytes의 코드 크기와 87,788 Cycles/block의 성능을 보였다[6].

3.1.2.2. EPSON S1C63 계열 프로세서 상의 공개키 암호기법 구현 연구 사례

본 절에서는 EPSON의 S1C63계열 프로세서 상의 공개키 암호기법 구현 연구사례에 대해 알아본다.

RSA와 DSA에서와 같은 공개키 암호에서는 모듈러 연산이 많이 사용된다. 이러한 모듈러 연산은 Montgomery 곱셈을 가장 많이 사용되고 있으며, EPSON S1C63 계열 프로세서의 환경에 맞게 재구성하여 구현되었으며, 512-bit에 대한 Montgomery 곱셈은 260bytes 코드 크기와 0.243 Cycles(million)의 성능을 보였으며, 1,024-bit 곱셈에 대해서는 0.961 Cycles(million)의 성능을 보였다[7].

타원 곡선 암호(Elliptic Curve Cryptosystem)의 경우, 연산 속도 향상을 위해, Row-wise multiplication을 사용하였으며, 효율적인 Point Arithmetic연산을 위해, Jacobian projective 좌표계를 이용하였으며, 기존의 Non-Adjacent Form(NAF)방식의 Scalar multiplication을 Left-to-right방식으로 변형하여 on-the-fly방식의 Scalar multiplication을 구현하였다. secp160r1 곡선기반으로 구현하였으며, 10,616bytes의 코드 사이즈를 가지며, Point Multiplication의 경우, 30.39 Cycles, Field Multiplication의 경우, 1,690 Cycles의 성능을 나타내었다[6].

3.2. 8-bit 프로세서 기반 사물인터넷 디바이스 상의 암호기법 구현 기술 및 연구 동향

본 절에서는 8-bit 마이크로프로세서 기반의 경량 사물인터넷 디바이스인 Atmel사의 Atmega128 프로세서 상에서의 암호 구현 연구 사례에 대해 알아본다.

대칭키 암호 구현의 경우, 대표적인 사례로는 AES와 LEA가 있으며, 각각의 구현 연구의 내용은 아래와 같다.

AES 대칭키 암호화의 경우, 8-bit 프로세서에 맞춰 개발되었기 때문에 사전 테이블 방식을 사용하지 않고 구현되었으며, MixColumn연산에 대해 조건 분기문과 XOR연산을 조합하여 구현하였으며, 키 생성과 암호화 과정에 대해 171 Cycle/byte의 성능을 보였다[8].

LEA 대칭키 암호화의 경우, 32-bit 프로세서에 맞게 설계 및 개발되었기 때문에 8-bit 단위로 나누어 연산을 수행하였다. 암호화과정에 대해 190 Cycle/byte의 성능을 보였다[9].

공개키 암호 구현의 경우, RSA와 ECC가 있으며, RSA 구현의 경우, Product-scanning방식과 Operand-scanning기법 활용을 통한 속도 향상이 있었으며, 제곱연산에 대하여 Sliding Block Doubling기법을 적용하

여 성능향상을 도출하였다. 해당 구현의 성능은 RSA 수행에 0.11초의 수행 속도를 가진다[10].

ECC의 경우, Subtractive Karatsuba 곱셈과 Karatsuba 제곱연산을 활용하여 구현되었으며, 160-bit ECDH에 대해 1.48초의 수행속도를 가진다[11].

3.3. 16-bit 프로세서 기반 사물인터넷 디바이스 상의 암호기법 구현 기술 및 연구 동향

본 절에서는 16-bit 마이크로프로세서 기반의 경량 사물인터넷 디바이스인 TI사의 MSP430 프로세서 상에서의 암호 구현 연구 사례에 대해 알아본다.

대칭키 암호 기법 구현의 경우, 앞서 살펴본 8-bit 프로세서 기반의 Atmel Atmega128상에서 구현된 것과 같이 AES와 LEA가 구현 가능하다. AES의 경우, 16-bit 단위의 XOR연산과 SubByte, ShiftRow, MixColumn을 결합한 사전 테이블 방식으로 구현되었으며, 339 Cycle/byte의 성능을 나타내었다[12].

LEA 대칭키 암호화 기법의 경우, 8-bit의 경우와 마찬가지로 16-bit 단위로 32-bit를 나누어 연산하는 것이 가능하다. 현재까지 이에 대한 구현 결과는 제시되지 않고 있지만 동일한 기법을 통해 쉽게 구현 가능하다.

공개키 암호화 기법 구현에 대해서는 ECC의 경우, 하드웨어 기반의 곱셈기 활용과 Product-Scanning기법을 적용하여 구현되었다. 성능은 192-bit기준으로 약 0.5초안에 ECDH가 수행이 가능하며, ECDSA의 경우, 1초 안에 수행이 가능할 것으로 예상된다[13].

3.4. 32-bit 프로세서 기반 사물인터넷 디바이스 상의 암호기법 구현 기술 및 연구 동향

본 절에서는 32-bit 마이크로프로세서 기반의 고성능 사물인터넷 디바이스인 ARM Cortex-A9 프로세서 상에서의 암호 구현 연구 사례에 대해 알아본다.

대칭키 암호화 기법 구현의 경우, 대표적인 사례로는 AES와 LEA가 있다.

AES의 경우, 8-bit 결과 값인 T-table을 전체 Round에 대하여 4번의 사전테이블에 저장하여 이용하는 방식으로 구현되었으며, 34Cycle/byte의 성능을 나타내었다[8].

LEA의 경우, 32-bit 프로세서를 타겟으로 설계되었으며 모든 연산이 하나의 명령어 셋으로 수행 가능한 장점을 가진다 [9]. 이는 암호화 시 20.1 cycle/byte로 연산 가능한 장점을 가진다.

공개키 암호화 기법 중 RSA 1024가 구현되었으며, 성능은 0.000191초의 성능 속도를 가지며, 2,048-bit의 경우, 0.000624초의 성능을 가진다[14]. 즉, 1초에 2048-bit RSA를 2,000번을 수행할 수 있다.

ECC의 경우, 1초에 256-bit field상에서 4,000을 수행할 수 있는 성능을 가지고 있다[15].

Ⅳ. 사물인터넷 디바이스 상의 암호기법 구현 기술 비교 분석

앞서 살펴본 다양한 사물인터넷 디바이스 상의 암호기법 구현 기술에 대해 알아보았다. 4, 8, 16, 32-bit 프로세서 기반의 사물인터넷 디바이스 별 암호기법 구현 연구 사례는 아래의 표와 같다.

	4-bit	8-bit	16-bit	32-bit
대칭키 암호	AES PRESENT	AES	AES	AES
공개키 암호	ECDSA RSA ECC	ECDSA RSA ECC	ECDSA ECC	ECDSA RSA ECC

Ⅴ. 결 론

사물 인터넷(IoT) 디바이스에서의 경량 암호 구현과 관련하여, 기존의 디바이스 상에서의 경량 암호 구현은 8-bit, 16-bit CPU 기반의 경량 디바이스 혹은 ARM과 같은 32-bit CPU 기반의 고성능 디바이스에서만 이루어졌으며, 기존의 TPM쪽에서의 보안에 대해 이루어졌다. 하지만, 사물 인터넷(IoT) 서비스의 궁극적인 목표인 언제 어디서나 서비스 이용에 있어서, 향후 사물 인터넷(IoT) 디바이스는 스마트 더스트 급과 같은 극단적인 환경에 노출되어 저 전력으로 오랜 시간 원하는 기능을 수행 할 수 있어야한다고 전망되며, 이러한 스마트 더스트 급의 디바이스로는 Atmel 사의 MARC4와 EPSON 사의 S1C63 family와 같은 4-bit CPU 기반의 초저전력 초경량 디바이스가 있다. 기존의 많은 대칭키 경량 암호 알고리즘과 공개키 암호 알고리즘 구현은 8-bit~32-bit 프로세서를 기반으로 한 디바이스에서 수행이 많이 되어 있으며, 스마트 더스트 급 초경량 디바

이스에 대한 구현이 많이 이루어지지 않은 것을 확인할 수 있었다. 이를 통해, 앞으로의 사물인터넷 디바이스 상에서의 암호기법 연구는 스마트 더스트 급에서의 구현이 필요할 것으로 보이며, 이를 통해 스마트 더스트 급 사물인터넷 디바이스의 보안성 확보가 가능할 것으로 보인다.

참 고 문 헌

[1] 한국수출입은행, “사물인터넷 시장 현황과 전망”, 2014.08

[2] Vogt, Markus, Axel Poschmann, and Christof Paar. "Cryptography is feasible on 4-bit micro-controllers-a proof of concept." In RFID, 2009 IEEE International Conference on, pp. 241-248. IEEE, 2009

[3] Kaufmann, Tino, and Axel Poschmann. "Enabling standardized cryptography on ultra-constrained 4-bit microcontrollers." In RFID (RFID), 2012 IEEE International Conference on, pp. 32-39. IEEE, 2012.

[4] Kaufmann, Tino, and Axel Poschmann. "Enabling standardized cryptography on ultra-constrained 4-bit microcontrollers." In RFID (RFID), 2012 IEEE International Conference on, pp. 32-39. IEEE, 2012

[5] Fan, Xinxin, Honggang Hu, Guang Gong, Eric M. Smith, and Daniel Engels. "Lightweight implementation of Hummingbird cryptographic algorithm on 4-bit microcontrollers." In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for, pp. 1-7. IEEE, 2009.

[6] Jacob, Nisha, Sirote Saetang, Chien-Ning Chen, Sebastian Kutzner, San Ling, and Axel Poschmann. "Feasibility and practicability of standardized cryptography on 4-bit micro controllers." In Selected Areas in Cryptography, pp. 184-201. Springer Berlin Heidelberg, 2013.

[7] Chen, Chien-Ning, et al. "Standardized Signature Algorithms on Ultra-constrained 4-Bit MCU." Advances in Information and Computer Security. Springer Berlin Heidelberg, 2012. 37-50.

[8] D. A. Osvik, J. W. Bos, D. Stefan, and D. Canright. Fast software aes encryption. In Fast Software Encryption, pages 75{93. Springer, 2010.

[9] K. H. Ryu and D.-G. Lee. Lea: A 128-bit block cipher for fast encryption on common processors. Information Security Applications, page 3.

[10] Zhe Liu, Hwajeong Seo, Howon Kim and Johann Großschädl, "Reverse Product-Scanning Multiplication on 8-bit AVR Processors: Tradeoffs between Performance, Code Size and Scalability", ICICS2014, 2014. 12

[11] Zhe Liu, Hwajeong Seo, Johann Grobschadl, Howon Kim, "Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for Sensor Nodes," ICICS'13, 2013. 11

[12] Texas Instruments. Institute for Applied Information Processing and Communication: Crypto software for microcontrollers. Available for download at http://jce.iaik.tugraz.at/sic/Products/Crypto_Software_for_Microcontrollers/Texas_Instruments_MSP430_Microcontrollers, 2012.

[13] Zhe Liu, Hwajeong Seo, Zhi Hu, Xinyi Huang and Johann Großschädl, "High-Speed MoTE ECDH Implementation on Sensor Nodes using MSP430 Microcontrollers," AsiaCCS'15, APR. 2015.

[14] Hwajeong Seo, Zhe Liu, Jongseok Choi, Johann Groszschaedl, Howon Kim, "Montgomery Modular Multiplication on ARM-NEON Revisited," ICISC2014. 2014. 12.

[15] BERNSTEIN, Daniel J., et al. Kummer strikes back: new DH speed records. In: Advances in Cryptology–ASIACRYPT 2014. Springer Berlin Heidelberg, 2014. p. 317-337.

〈저 자 소 개〉

박 태 환 (Taehwan Park)
학생회원

2013년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2013년 3월~현재 : 부산대학교 컴퓨터공학과 석, 박사 통합 과정
관심분야 : 정보보호, 암호화 SW구현, IoT

서 화 정 (Hwajeong Seo)
종신회원

2010년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 박사과정
관심분야 : 정보보호, 암호화 구현, IoT

김 지 현(Jihyun Kim)
학생회원

2010년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2012년 8월 : 부산대학교 전기전자컴퓨터공학과 석사 졸업
2013년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 박사과정
관심분야 : 정보보호, 컴퓨터보안, 데이터마이닝, IoT

최 종 석(Jongseok Choi)
학생회원

2011년 2월 : 동명대학교 정보보호학과 학사 졸업
2013년 2월 : 부산대학교 전기전자컴퓨터공학과 석사 졸업
2013년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 박사과정
관심분야 : 정보보호, 컴퓨터보안, IoT 보안

김 호 원(Howon Kim)
종신회원

1999년 2월 : POSTECH 전자전기공학과 박사
1998년12월~2003년 6월 : ETRI 정보보호연구본부 선임연구원
2003년 7월~2004년 6월 : 독일 보훔대학교 Post Doc.
2004년 7월~2008년2월 : ETRI 정보보호연구단 팀장
2008년3월~현재 : 부산대학교 정보컴퓨터공학부 교수
관심분야 : 사물인터넷, 정보보호/해킹 대응, 암호, 지능형 시스템/머신러닝