정 보 보 호 학 회 지
제27권 제6호, 2017. 12

양자 내성 암호 최신 소프트웨어 구현 동향

박 태 환*, 서 화 정**, 이 가 람*, 김 호 원*+

요 약

최근 양자 컴퓨터 기술의 발전에 따라 기존에 많이 사용하고 있는 대칭키 암호와 공개키 암호의 보안 위험성이 고려되어야하며, 이에 따라 양자 컴퓨터 환경에서도 보안성을 제공할 수 있는 암호 알고리즘인 양자 내성 암호에 대한 연구가 활발히 이루어지고 있으며, 이와 관련하여 미국 NIST의 양자 내성 암호 표준 공모전이 진행중에 있다. 본 논문에서는 양자 내성 암호별 다양한 플랫폼/디바이스 환경 및 언어 기반의 최신 소프트웨어 구현 동향을 살펴본다.

Ⅰ. 서 론

최근 양자 컴퓨터 기술의 급속한 발전으로 인해 구글, IBM, MS, D-Wave 등 국외의 많은 기업들에서 양자 컴퓨터 개발이 이루어지고 있다. 이러한 양자 컴퓨터 기술의 발전에 따라 양자 컴퓨터 환경 상에서의 Shor 양자 알고리즘 적용을 통한 이산 대수 기반의 공개키 암호 안전성의 위협과 Grover 양자 알고리즘 적용에 따른 대칭키 암호와 해시함수의 안전성의 위협에 따른 대칭키 암호의 키 길이 증가 및 해시함수의 출력 길이 증가가 필요한 상황이다. 이러한 상황에서 세계 각국의 연구자들에 의해 양자 컴퓨터 환경에서도 안전한 양자 내성 암호 (Post-Quantum Cryptography)에 대한 연구가 활발히 이루어지고 있으며, PQCrypto와 같은 학회를 개최하고 있으며, 이를 통해, 안전성과 최적화 구현 등의 관점에서 많은 연구가 진행되고 있다. 양자 내성 암호는 격자 기반, 코드 기반, 다변수 기반, Isogeny 기반, 해시 기반 등의 카테고리로 나누어 질 수 있으며, 특히 양자 내성 암호에 대한 표준화와 관련하여 미국 NIST에서는 올해 11월 30일까지 양자 내성 암호 표준 공모전 접수를 진행하였으며, 이를 통한 보다 활발한 연구가 진행되고 있다. 본 논문에서는 각 양자 내성 암호별 다양한 환경 상에서의 소프트웨어 최적화 구현 동향에 대해 살펴본다.

Ⅱ. 양자 내성 암호 최신 소프트웨어 최적화 구현 동향

본 절에서는 양자 내성 암호별 최신 소프트웨어 최적화 구현 동향에 대해 살펴본다.

2.1. 격자 기반 양자 내성 암호 최신 소프트웨어 최적화 구현 동향

격자 기반 양자 내성 암호의 최신 소프트웨어 최적화 구현 동향은 다음과 같다.

Cheon et al.[1]은 sparse secret 정보와 Learning with Errors(LWE)를 접목 시킨 spLWE 기반의 PKE를 제안하였으며, IND-CPA 및 IND-CCA에 대해 C++ 기반의 소프트웨어 최적 구현을 통해, Intel Core i5급과 Intel Core 2 Duo 환경 상에서의 구현 성능을 제시하고 있다. 그리고 Cheon et al.[2]에서는 기존의 LWE 기반 문제와 Learnig with Rounding(LWR) 기반 문제를 적용한 Lizard, Ring-Lizard와 IND-CPA, IND-CCA 및 Additive Homomorphic Encryption을 제안하였으며, AVX-2 기반의 최적화 구현 결과에 대해 Intel Core i5급 환경 상에서의 성능을 제시하고 있다. Bos, Joppe, et al.[3]에서는 미국 NIST 양자 내성 암호 표준에 제출한 CRYSTAL의 일부분인 Kyber와 이와 관련된

본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2012-0-00265, 개방형 고성능 표준 IoT 디바이스 및 지능형 SW 개발)
* 부산대학교 전기전자컴퓨터공학과 ({pth5804, rkfka4370, howonkim}@pusan.ac.kr)
** 한성대학교 IT융합공학부 (hwajeong@hansung.ac.kr)

Key-Encapsulation Mechanism(KEM), CPA-secure, CCA-secure 버전에 대한 제시와 Number Theoretical Transform(NTT)에 대한 최적화 구현 적용 및 AVX-2 적용 결과에 대해 Intel Core i7급 환경에서의 성능을 제시하고 있으며, BCNS, NewHope, FRODO에 비해 KEM 버전이 높은 성능을 보이는 것으로 확인되었으며, CCA-secure KEM의 경우, NTRU Prime, spLWE-KEM보다 높은 성능을 보였으며, CCA-secure Public Key Encryption의 경우, NTRU Encrypt ees742ep1과 Lizard보다 높은 성능을 보이고 있다. 최근 CHES 2017에서는 NTRU 기반의 Key encapsulation에 대해 AVX-2 적용과 Polynomial 곱셈 및 Inversion에 대해 고속화 구현 결과물에 대해 Intel Core i7(Haswell)환경 상에서의 구현 성능을 제시하고 있다[4].

임베디드 디바이스 환경 상에서의 최적화 구현 연구의 경우, Guillen et al.[5]에서 NTRU 암호 알고리즘에 대해 기본 모델, Product-form 곱셈 모델, Time-independent 모델, 패턴 곱셈 모델 등을 적용하여 Cortex-M0와 ARMv7 32-bit 환경과 ATmega128 8-bit 프로세서 환경 상에서의 최적화 구현 성능을 제시하고 있다. Order et al.[6]에서는 32-bit ARM Cortex-M4F 환경 상에서 BLISS에 대한 최적화 구현 성능을 제시하고 있으며, De Clercq et al.[7]에서는 32비트 ARM 프로세서 환경 상에서의 32비트 레지스터 활용성을 높이는 방향으로 Ring-LWE 최적화 구현한 성능을 제시하고 있다. LATINCRYPT'15에서는 8비트 ATxmega128 프로세서 환경 상에서의 Ring-LWE와 BLISS의 최적화 구현 결과[8]를 제시하고 있으며, CHES'15에서는 Ring-LWE에 대해 모듈러 곱셈과 NTT 계산의 효율적 방안과 적은 메모리 사용과 메모리 접근 횟수를 최소화하는 방안을 적용한 최적화 성능 결과를 제시하고 있다[9]. 앞선 연구 결과와 동일한 환경에서 Timing 공격에 안전한 Ring-LWE와 BLISS 서명기법에 대한 제시와 Montgomery Reduction 최적화 기법을 적용한 구현 결과를 제시하고 있다[10]. Ring-LWE에 대해 32-bit ARM Cortex-A 환경에서 ARM-NEON을 적용한 병렬 최적화 구현 결과[11]와 16비트 MSP430 환경 상에서의 최적화 구현 연구 결과가 나와 있다[12]. 가장 최근인 ICISC'16에서는 8비트 AVR 프로세서 환경 상에서 Timing 공격에 안전한 NTT 최적화 구현 방안과 Ring-LWE에 적용한 성능 결과를 제시하고 있다[13].

〔표 1〕 격자 기반 양자내성암호 구현 환경별 최적화 구현 여부

성능 평가 환경	최적화 구현 여부
Intel x64환경(C)	○
Intel x64환경(AVX-2)	○
8비트 AVR 프로세서 환경	○
16비트 MSP430 프로세서 환경	○
32비트 ARM 프로세서 환경	○
32비트 ARM 프로세서 환경 (ARM-NEON)	○

아래의 표는 격자 기반 양자 내성 암호 최신 소프트웨어 구현 동향에 대해 성능 평가 환경을 기준으로 간략히 정리한 표이다.

2.2. 코드 기반 양자 내성 암호 최신 소프트웨어 최적화 구현 동향

양자 내성 암호 중 코드 기반 양자 내성 암호에 대한 최신 소프트웨어 최적화 구현 동향은 다음과 같다.

CHES 2013[14]에서는 Timing 공격에 강인한 McBits라는 코드 기반 양자 내성 암호를 제안하였으며, Bitslicing과 external parallelism을 적용하였으며, additive FFT와 cache-timing 공격 방지를 위한 sorting network를 활용하여 Intel Ivy Bridge 코어 환경에서의 최적화 구현 성능을 제시하고 있다. Misoczki, Rafael, et al.[15]에서는 기존 코드 기반 양자 내성 암호 중 하나인 McEliece에 대해 Moderate Density Parity-Check Code(MDPC)를 적용하여 기존 대비 공개키의 크기를 줄인 새로운 McEliece 코드 기반 양자 내성 암호를 제안함과 동시에 제안된 기법에 대해 Intel Xeon CPU 환경에서 C++기반의 코드의 성능을 제시하고 있다. 해당 연구 이후, 같은 해에 QC-MDPC (Quasi-Cyclic MDPC)에 대해 Decode 부분에 대한 최적화 기법을 제안함과 동시에 제안 기법을 적용한 QC-MDPC에 대해 8비트 AVR 마이크로프로세서 환경과 Xilinx Virtex-6 FPGA 상에서의 성능을 제안하고 있으며, 특히 8비트 AVR 마이크로프로세서 환경 상에서의 코드 및 메모리 크기 최적화 구현을 통해, 기존 연구보다 적은 수의 SRAM과 flash 메모리를 사용한 성능 제시하고 있다[16]. PQCrypto 2014[17]에서는

ARM Cortex-M4 마이크로프로세서 상에서의 QC-MDPC 최적화 구현 기법 제안 및 성능을 제시하고 있으며, 2015년 ACM TECS(Transactions on Embedded Computing Systems)[18]에서는 QC-MDPC에 대해 ARM Cortex-M4 마이크로프로세서 환경 상에서 decoding iteration 횟수 감소 및 decoding failure 확률을 낮추는 기법을 제안하였으며, 이에 대한 성능을 제시하고 있다. PQCrypto 2016[19]에서는 기존의 QC-MDPC를 활용하여 constant-time 수행이 가능하여 Timing 공격에 대해 강인성을 가지며, 작은 키 크기를 가지고 Bitslicing 기법을 적용한 QcBits라는 코드 기반 양자 내성 암호를 제안하였으며, Intel Haswell 아키텍처 기반의 프로세서 환경과 ARM Cortex-M4 마이크로프로세서 환경 상에서의 최적화 구현 성능을 제안하고 있다. Barreto, Paulo SLM, et al.[20]에서는 기존의 QC-MDPC McEliece 암호화 기법을 활용한 KEM(Key Encapsulation Mechanism)인 CAKE (Code-based Algorithm for Key Encapsulation)을 제안하고 있다. 해당 KEM은 MDPC decoding에 있어서 reaction 공격에 대응 하기 위해 ephemeral key 사용과 효율적인 키 생성 기법을 제안하였으며, CAKE 기반의 인증 키 교환 프로토콜 또한 제안하였다. 제안된 CAKE에 대한 최적화 구현 및 성능 평가는 Intel AVX512 기반의 SIMD(Single Instruction Multiple Data) 최적화 구현 및 성능 평가를 제시하고 있다. CHES 2017[21]에서는 기존의 McBits[14]의 복호화 부분에 대해 internal parallelism을 적용하여 Intel IvyBridge와 Haswell 환경 상에서의 최적화된 성능을 제시하고 있다.

아래의 표는 코드 기반 양자 내성 암호 최신 소프트웨어 구현 동향에 대해 성능 평가 환경을 기준으로 간략히 정리한 표이다.

〔표 2〕 코드 기반 양자내성암호 구현 환경별 최적화 구현 여부

성능 평가 환경	최적화 구현 여부
Intel x64환경(C/C++)	○
Intel x64환경 (AVX, AVX512)	○
8비트 AVR 프로세서 환경	○
16비트 MSP430 프로세서 환경	X
32비트 ARM 프로세서 환경 (Cortex-M4)	○
32비트 ARM 프로세서 환경 (ARM-NEON)	X

2.3. 다변수 기반 양자 내성 암호 최신 소프트웨어 최적화 구현 동향

다변수 기반 양자 내성 암호의 최신 소프트웨어 최적화 구현 동향은 다음과 같다.

CHES 2015[22]에서는 다변수 기반 스킴인 Hidden Field Equations(HFE)에 대해 보안성이 강화된 서명 기법을 제안하고 있으며, carry-less 곱셈을 위해, PCMULQDQ 명령어를 적용하여 최적화 구현을 진행하였으며, GCD 연산의 최적화 기법 제안 및 적용을 통해 AMD Opteron 6212(Bulldozer), Intel Xeon E5-2620, Intel Xeon E3-1245 환경 상에서의 최적화 구현 성능을 제시하고 있다. ICISC 2016[23]에서는 기존의 Cubic UOV 서명 기법에 대한 공격 사례로 인해, 해당 공격에 안전하며 기존의 CUOV와 UOV보다 효율적인 2개의 새로운 다변수 서명 기법인 CSSv와 SVSv2를 제안하며, Intel Core i5-4300U 환경 상에서 linear system solving과 uni-variate quadratic equation solving을 위한 MAGMA의 IsConsistent()와 Factorization()함수를 적용한 성능을 제시하고 있다. Petzoldt et al.[24]에서는 기존의 Rainbow multi-variate 서명기법을 blind 서명 기법으로 변환 방식에 대한 transform 방식을 제안하였으며, Intel Quad-core 환경 상에서 Sage 기반으로 최적화 구현된 성능을 제시하고 있다. Chen, Ming-Shing, et al.[25]에서는 128비트의 보안 강도를 가지는 안전한 Multi-variate Public Key Cryptosystems (MPKC)을 제안하였으며, additive Fast Fourier Transform과 constant time linear solver기반의 multi-variate polynomials와 곱셈을 적용하였으며, AVX-2 SIMD와 AES-NI 기반의 최적화 구현을 진행하였으며, Intel Xeon E3-1245 v3 환경 상에서의 최적화 성능을 제시하고 있다. 그리고 해당 논문에서는 Intel x86 플랫폼 상에서 AVX-2 명령어 기반의 구현을 통해 부채널 공격에 대한 강인성을 가지도록 구현 개발 되었다. Peng et al.[26]에서는 기존 Rainbow 서명 기법의 단점인 큰 키 사이즈를 해결하기 위해, Rainbow 서명 과정의 고속화를 위해, 비밀키의 일부분에 대한 rotating relation 기법과 이를 통한 비밀키 크기를 45% 감소시키는

〔표 3〕 다변수 기반 양자내성암호 구현 환경별 최적화 구현 여부

성능 평가 환경	최적화 구현 여부
Intel x64환경(MAGMA, Sage)	○
Intel x64환경(AVX-2)	○
8비트 AVR 프로세서 환경	X
16비트 MSP430 프로세서 환경	X
32비트 ARM 프로세서 환경	X
32비트 ARM 프로세서 환경 (ARM-NEON)	X

Circulant Rainbow를 제안하였으며, 제안된 기법에 대해 AVX-2 기반의 최적화 구현을 통해, Intel Core i7-4790 환경 상에서의 최적화 성능을 제시하고 있다.

아래의 표는 다변수 기반 양자 내성 암호 최신 소프트웨어 구현 동향에 대해 성능 평가 환경을 기준으로 간략히 정리한 표이다.

2.4. Isogeny 기반 양자 내성 암호 최신 소프트웨어 최적화 구현 동향

Isogeny 기반 양자 내성 암호의 최신 소프트웨어 최적화 구현 동향은 다음과 같다.

PQCrypto 2011[27]에서는 기존의 ordinary curve를 사용하는 isogeny 기반 양자 내성 암호보다 효율적인 supersingular elliptic curve 간의 isogeny 특성 기반의 암호 프로토콜을 제시하며, 이에 대해 Sage, C/Cython을 같이 활용하며, GMP 라이브러리를 활용하여 2.4GHz Opetron 프로세서 환경 상에서 최적화 결과를 제시하고 있다. CRYTO 2016[28]에서는 supersingular isogeny 특성을 활용한 Diffie-Hellman 프로토콜의 효율적인 구현 결과를 제시하고 있으며, F_{p^2} 상에서의 연산 고속화 기법과 Projective isogenies를 적용하여 isogeny 연산 상에서 inversion 연산을 제거하였고, 사용된 파라미터에 맞춰 Montgomery reduction 최적화를 적용하여 Intel Core i7-2600 Sandy Bridge 프로세서와 Intel Core i7-4770 Haswell 프로세서 환경 상에서 C와 Assembly 언어 기반의 최적화 성능(Intel TurboBoost 비활성화)을 제시하고 있다. AsiaPKC 2016[30]에서는 Isogeny 기반 양자 내성 암호에서의 공개키 정보에 대한 Key compression의 효율적인 기법을 제시하며, 효율성을 위해, 기존의 Montgomery Curve를 short Weierstrass curve로 변환하는 최적화 방식을 적용한 제안 기법에 대해 C와 GMP 라이브러리와 OpenSSL을 사용하여 Intel i7-4790K Haswell 프로세서 환경과 NVIDIA Jetson TK1(ARM Cortex-A15) 환경 상에서의 최적화 성능을 제시하고 있다. Koziel, Brian, et al.[30]에서는 CRYTO 2016[28]에서 제안된 isogeny 기반의 키 교환 프로토콜에 대해 finite field 연산을 constant 시간 내에 수행 할 수 있는 새로운 prime 제시와 isogeny 연산 최적화 및 GMP 라이브러리 기반의 Montgomery 곱셈과 reduction 최적화를 적용하여 C 기반의 구현 결과물과 ARM Assembly 및 NEON 기반의 SIMD 적용 구현 결과물에 대해 BeagleBoard Black(ARMv7 Cortex-A8 프로세서) 환경과 Jetson TK1 환경 상에서의 성능을 제시하고 있다. Yoo, Youngho method[31]의 경우, supersingular isogeny 특성을 활용한 디지털 서명 기법을 제안하였으며, 작은 키 사이즈를 가진다는 장점을 지니고 있다. 해당 논문에서는 Intel Xeon E5-2637 Haswell 프로세서 환경과 ARM Cortex-A57 프로세서 환경 상에서 C와 ARM Assembly를 적용하여 최적화 구현을 진행하였으며, ZKP 프로토콜 및 라운드에 대해 오프라인으로 pre-compute를 진행하여 효율성을 높인 성능을 제시하고 있다. Costello, Craig, et al.[31]에서는 SIDH 기법에서의 공개키에 대한 효율적인 Compression 방식을 제안하고 있으며, 제안 기법을 통해 공개키를 기존 대비 약 25% 감소시키는 결과를 제시하고 있다. 해당 논문에서는 Montgomery inversion sharing trick에 대한 최적화 및 Pohlig-Hellman 알고리즘에 대한 최적화 구현을 적용하여 Intel Core i7-4770 Haswell 프로세서 환경 상에서의 최적화 성능을 제시하고 있다.

아래의 표는 Isogeny 기반 양자 내성 암호 최신 소프

〔표 4〕 Isogeny 기반 양자내성암호 구현 환경별 최적화 구현 여부

성능 평가 환경	최적화 구현 여부
Intel x64환경(Sage, C)	○
Intel x64환경(AVX-2)	X
8비트 AVR 프로세서 환경	X
16비트 MSP430 프로세서 환경	X
32비트 ARM 프로세서 환경	○
32비트 ARM 프로세서 환경 (ARM-NEON)	○

트웨어 구현 동향에 대해 성능 평가 환경을 기준으로 간략히 정리한 표이다.

2.5. 해시 기반 양자 내성 서명 기법 최신 소프트웨어 최적화 구현 동향

해시 기반 양자 내성 서명 기법의 최신 소프트웨어 최적화 구현 동향은 다음과 같다.

Bernstein, Daniel J., et al.[33]에서는 기존의 해시 기반 양자 내성 서명 기법에서의 단점 중 하나인 Stateful이라는 문제에 대해 MSS-SPR 트리 구조와 WOTS+ 기반의 OTS와 HORST 기반의 FTS를 적용하여 State 없이 동작되는 해시 기반 양자 내성 서명 기법인 SPHINCS-256을 제안하였다. 해당 논문에서는 효율성을 위해, BLAKE-512 기반의 해시함수와 ChaCha12를 PRG로 사용하였으며, 이를 통한 0.041MB 사이즈의 서명과 0.001MB 크기의 공개키 및 개인키를 가지는 특징이 있으며, 서명 크기의 경우, 기존의 Goldreich 기법보다 15배가 작은 특징을 가진다. 제안 기법에 대한 최적화를 위해 AVX-2를 적용하였으며, 8개의 해시 연산에 대한 병렬화 및 벡터처리를 하였으며, Intel Haswell 프로세서 환경 상에서의 최적화 성능을 제시하고 있다. 이후 SPHINCS와 관련하여 Hülsing, Andreas et al.[34]에서는 ARM Cortex-M3 보드 환경 상에서 16KB RAM 상에서 41KB 크기의 서명 값을 처리할 수 있는 SPHINCS-256을 제안하였으며, 이를 위해, 연산 별로 나누어 메모리 소비를 줄이도록 구현을 하였고, 전체 트리 구조를 저장하는 것이 아닌 root 값을 저장하는 형태로 구현된 최적화 성능을 제시하고 있다. Gueron et al.[35]에서는 SPHINC에 대해SIMPIRA cryptographic permutation을 적용한 최적화 결과를 제시하고 있다. 해당 논문에서는 Intel 환경 상에서 SIMPIRA 최적화 구현을 위해, AES-NI를 적용하였으며, Intel Skylake 프로세서 환경 상에서의 최적화 구현 성능을 제시하고 있다. Kolbl, Stefan method[36]에서는 Intel, AMD와 ARM 프로세서 환경 상에서 서로 다른 해시함수를 사용하는 SPHINCS에 대한 최적화 구현 결과를 제시하고 있다. 최적화 구현을 위해, SHA-256, KECCAK, SIMPIRA, HARAKA와 CHACHA에 대해 벡터 기반 병렬화 최적 구현(AVX-2, ARM NEON)을 적용하였으며, Intel Haswell, Intel Skylake, AMD Ryzen, ARM Cortex A57과 A72 환경 상에서의 최적화 성능을 제시하고 있다.

〔표 5〕 해시 기반 양자내성 서명 기법 구현 환경별 최적화 구현 여부

성능 평가 환경	최적화 구현 여부
Intel x64환경(C/C++)	O
Intel x64환경(AVX-2)	O
8비트 AVR 프로세서 환경	X
16비트 MSP430 프로세서 환경	X
32비트 ARM 프로세서 환경 (C/ASM)	O
32비트 ARM 프로세서 환경 (ARM-NEON)	O

Ⅲ. 결 론

본 논문에서는 최근 활발히 연구가 되고 있는 격자 기반, 코드 기반, Isogeny 기반, Multi-variate 기반, 해시 기반의 양자 내성 암호/서명 기법별 소프트웨어 구현 최신 동향에 살펴보았다. 각 양자 내성 암호별 소프트웨어 구현 연구가 활발히 이루어지고 있으며, 8비트, 16비트 등 경량 임베디드 프로세서 환경에 대한 최적화 구현 연구 및 ARM-NEON과 같은 32비트 프로세서 환경 상에서의 병렬 최적화 연구가 활발히 진행될 것으로 보인다.

참 고 문 헌

[1] Son, Yongha. “A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE.” Information Security and Cryptology--ICISC 2016: 19th International Conference, Seoul, South Korea, November 30--December 2, 2016, Revised Selected Papers. Vol. 10157. Springer, 2017.

[2] Cheon, J. H., Kim, D., Lee, J., & Song, Y. S. “Lizard: Cut off the Tail!//Practical Post-Quantum Public-Key Encryption from LWE and LWR.” IACR Cryptology ePrint Archive 2016 (2016): 1126.

[3] Bos, Joppe, et al. “CRYSTALS‐Kyber: a

CCA-secure module-lattice-based KEM." IACR Cryptology ePrint Archive 2017 (2017): 634.

[4] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., & Stehlé, D. "High-speed key encapsulation from NTRU." International Conference on Cryptographic Hardware and Embedded Systems, pp. 232-252. Springer, Cham, 2017.

[5] Guillen, O. M., Poppelmann, T., Mera, J. M. B., Bongenaar, E. F., Sigl, G., Sepulveda, J. (2017). "Towards post-quantum security for IoT endpoints with NTRU", In 2017 Design, Automation & Test in Europe Conference & Exhibition(DATE), IEEE, pp. 698-703.

[6] T. Oder, T. Poppelmann, and T. Guneysu. "Beyond ECDSA and RSA: Lattice-based Digital Signatures on Constrained Devices", 51st Annual Design Automation Conference(DAC), pp. 1-6, 2014.

[7] R. De Clercq, S. S. Roy, F. Vercauteren, and I. Verbauwhede, "Efficient Software Implementation of Ring-LWE Encryption", 18th Design, Automation & Test in Europe Conference & Exhibition, pp. 339-344, 2015.

[8] T. Pöppelmann, T. Oder, and T. Guneysu, "High-performance ideal lattice-based cryptography on 8-bit ATxmega microcontrollers", In International Conference on Cryptology and Information Security in Latin America, pages 346-365. Springer, 2015.

[9] Z. Liu, H. Seo, S. S. Roy, J. GroBschadl, H. Kim, and I. Verbauwhede, "Efficient Ring-LWE encryption on 8-bit AVR processors", In International Workshop on Cryptographic Hardware and Embedded Systems, pages 663-682. Springer, 2015.

[10] Z. Liu, T. Poppelmann, T. Oder, H. Seo, S. S. Roy, T. Guneysu, J. Groschadl, H. Kim, and I. Verbauwhede, "High-performance ideal lattice-based cryptography on 8-bit AVR microcontrollers", ACM Transactions on Embedded Computing Systems (TECS), 16(4):117, pp. 1-20, 2017.

[11] Z. Liu, R. Azarderakhsh, H. Kim, and H. Seo, "Efficient software implementation of Ring-LWE encryption on IoT processors", IEEE Transactions on Computers, pp. 1-11, 2017.

[12] Z. Liu, H. Seo, J. GroBschadl, and H. Kim, "Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes", IEEE Transactions on Information Forensics and Security, 11(7), pp. 1385-1397, 2016.

[13] Hwajung Seo, Zhe Liu, Taehwan Park, Hyeokchan Kwon, Sokjoon Lee, and Howon Kim, "Secure Number Theoretic Transform and Speed Record for Ring-LWE Encryption on Embedded Processors", International Conference on Information Security and Cryptology. Springer, Cham, pp. 1-14, 2017.

[14] Bernstein, Daniel J., Tung Chou, and Peter Schwabe. "McBits: fast constant-time code-based cryptography." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, pp. 250-272, 2013.

[15] Misoczki, R., Tillich, J. P., Sendrier, N., & Barreto, P. S. "MDPC-McEliece: New McEliece variants from moderate density parity-check codes." Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on. IEEE, pp. 2069-2073, 2013.

[16] Heyse, Stefan, Ingo Von Maurich, and Tim Guneysu. "Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, pp.273-292, 2013.

[17] Von Maurich, Ingo, and Tim Güneysu. "Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices." PQCrypto 2014, pp. 266-282, 2014

[18] Maurich, Ingo Von, Tobias Oder, and Tim Guneysu. “Implementing QC-MDPC McEliece Encryption.“ ACM Transactions on Embedded Computing Systems (TECS) 14.3 (2015): 44., pp. 1-25, 2015

[19] Chou, Tung. “QcBits: constant-time small-key code-based cryptography.” International Conference on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2016.(0), pp. 280-300, 2016

[20] Barreto, P. S., Gueron, S., Güneysu, T., Misoczki, R., Persichetti, E., Sendrier, N., & Tillich, J. P. “CAKE: Code-Based Algorithm for Key Encapsulation.” IMA International Conference on Cryptography and Coding. Springer, Cham, 2017.(0), pp. 207-226, 2017

[21] Chou, Tung. “McBits revisited.” International Conference on Cryptographic Hardware and Embedded Systems. Springer, Cham, pp. 213-231, 2017.

[22] A. Petzoldt, M-S Chen, B-Y Yang, C. Tao, and J. Ding, “Design Principles for HFEv- based Multivariate Signature Schemes”, Advances in Cryptology: ASIACRYPT2015, LNCS 9452, pp. 311-334, 2015.

[23] D. H. Duong, T. Yasuda, A. Petzoldt, Y. Wang and T. Takagi, “Revisiting the Cubic UOV Signature Scheme”, ICISC 2016, LNCS 10157, pp. 223-238, 2016.

[24] Petzoldt, Albrecht, Alan Szepieniec, and Mohamed Saied Emam Mohamed. “A Practical Multivariate Blind Signature Scheme.” IACR Cryptology ePrint Archive 2017 (2017): 131., pp. 1-21, 2017

[25] Chen, M. S., Li, W. D., Peng, B. Y., Yang, B. Y., & Cheng, C. M. “Implementing 128-bit Secure MPKC Signatures.” Cryptology ePrint Archive, Report 2017/636, pp. 1-32, 2017.

[26] Peng, Zhiniang, and Shaohua Tang. “Circulant Rainbow: A New Rainbow Variant With Shorter Private Key and Faster Signature Generation.” IEEE Access 5 (2017), pp. 11877-11886., 2017

[27] De Feo, L., Jao, D., Plut, J., “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.”, Journal of Mathematical Cryptology 8(3), pp. 209-247, September 2014

[28] Costello, C., Longa, P., Naehrig, M., “Efficient Algorithms for Supersingular Isogeny Diffie-Hellman”, Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I. Springer Berlin Heidelberg, Berlin, Heidelberg (2016), pp. 572-601, 2016

[29] Azarderakhsh, R., Jao, D., Kalach, K., Koziel, B., Leonardi, C., “Key compression for isogeny-based cryptosystems.”, Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography. AsiaPKC '16, New York, NY, USA, ACM, pp. 1-10, 2016

[30] Koziel, B., Jalali, A., Azarderakhsh, R., Jao, D., & Mozaffari-Kermani, M. “NEON-SIDH: efficient implementation of supersingular isogeny Diffie-Hellman key exchange protocol on ARM.” International Conference on Cryptology and Network Security. Springer International Publishing, pp. 88-103, 2016

[31] Yoo, Y., Azarderakhsh, R., Jalali, A., Jao, D., & Soukharev, V. “A Post-Quantum Digital Signature Scheme Based on Supersingular Isogenies.” IACR Cryptology ePrint Archive 2017 (2017): 186., pp. 1-18, 2017

[32] Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., & Urbanik, D. “Efficient compression of SIDH public keys.” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, pp. 279-706, 2017.

[33] Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., & Wilcox-O’Hearn, Z. “SPHINCS: practical stateless hash-based signatures.” Annual International Conference on the Theory and

Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, pp. 368-397, 2015.
[34] Hülsing, Andreas, Joost Rijneveld, and Peter Schwabe. “ARMed SPHINCS.” Public-Key Cryptography – PKC 2016. Springer Berlin Heidelberg, 2016, pp. 446-470, 2016
[35] Gueron, Shay, and Nicky Mouha. “SPHINCS-Simpira: Fast Stateless Hash-based Signatures with Post-quantum Security.” Cryptology ePrint Archive, Report 2017/645, pp. 1-12, 2017
[36] Kolbl, Stefan. “Putting Wings on SPHINCS.” PQCrypto 2017, pp. 1-20, 2017

〈저 자 소 개〉

박 태 환 (Tae-hwan Park)
학생회원

2013년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2013년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석, 박사 통합과정
관심분야 : 암호화 구현, IoT 디바이스 보안, 양자 내성 암호

서 화 정 (Hwa-jeong Seo)
종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사 졸업
2016년 2월 : 부산대학교 컴퓨터공학과 박사 졸업
2015년 4월~5월 : 싱가포르 난양공대 인턴쉽
2016년 1월~2017년 3월 : 싱가포르 과학기술청 연구원
2017년 4월~현재 : 한성대학교 조교수
관심분야 : 정보보호, 암호화 구현, IoT

이 가 람 (Ga-ram Lee)
학생회원

2016년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2016년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석사과정
관심분야 : SW 암호 최적화 구현, IoT 보안, 역공학, 임베디드 보안, 머신러닝

김 호 원 (Ho-won Kim)
종신회원

1993년 2월 : 경북대학교 전자공학과 학사 졸업
1995년 2월 : 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월 : 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월 : 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재 : 부산대학교 전기컴퓨터공학부 정교수
관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT