정 보 보 호 학 회 지
제28권 제5호, 2018. 10

양자내성암호 표준화, 연구 동향 및 전망

박 태 환*, 김 호 원**

요 약

최근 양자 컴퓨팅 환경에서도 안전한 양자내성암호에 대한 많은 연구가 진행되고 있으며, 이에 따라 미국 국립표준기술연구소에서는 2017년 11월 30일부터 양자내성암호에 대한 연방 표준화 사업을 진행하고 있다. 현재 표준화 1라운드가 진행되고 있으며, 제출된 양자내성암호들에 대한 안전성 분석이 진행되고 있다. 또한 CHES와 같은 세계 유수의 학회에서도 이러한 양자내성암호에 대한 많은 연구결과들이 발표되고 있으며, 본 논문에서는 양자내성암호 표준화와 연구의 최신 동향을 살펴보며, 이에 따른 향후 연구 전망을 제시하고자 한다.

Ⅰ. 서 론

최근 양자 컴퓨팅 기술의 발전과 더불어 PQCrypto, CHES 등 다양한 세계 유수의 학회에서 양자 컴퓨팅 환경에 안전한 양자내성암호(Post-Quantum Cryptography)에 대한 많은 연구가 이루어지고 있으며, 이러한 연구 흐름에 맞추어 미국 국립표준기술연구소 (NIST, National Institute of Standards and Technology)에서는 PQCrypto 2016에서 양자내성암호에 대한 미국 연방 표준 사업 계획을 발표하였다. 이후 작년 11월 30일까지 양자내성암호 표준 후보군에 대한 접수를 받은 후, 올해 4월에는 PQCrypto 학회와 같이 표준 공모전 워크샵을 개최하였으며, 현재 표준화 1라운드가 진행되고 있다. 이러한 상황에서 양자내성암호 표준 공모전에 제안된 기법들을 중심으로 안전성 분석, 소프트웨어/하드웨어 최적화 구현 등 다양한 연구 관점에 연구가 활발히 이루어지고 있으며, 이에 따른 표준화 진행에도 변화가 있었다. 본 논문에서는 미국 NIST 양자내성암호 표준화 사업과 양자내성암호에 대한 소프트웨어/하드웨어 구현 연구, 안전성 분석 연구 분야에 대한 최신 동향을 살펴보며, 이를 통해, 향후 연구 전망을 제시하고자 한다.

Ⅱ. 미국 NIST 양자내성암호 표준화 동향

미국 NIST 양자내성암호 표준화 사업에는 총 69개의 양자내성암호 기법들이 제안되었으며, 이후, 5개의 양자내성암호 기법이 취소를 하여 현재 총 64개의 양자내성암호 기법들에 대한 표준화 1라운드가 진행되고 있다. 이러한 양자내성암호의 유형으로는 격자 기반 (Lattice-based), 코드 기반 (Code-based), 다변수 기반 (Multivariate-based), 해시 기반 (Hash-based), Isogeny 기반 및 기타로 나누어 질 수 있다. 그리고 제안 기법의 경우, 전자 서명, KEM (Key Encapsulation Mechanism), 암호화 방식으로 나누어 질 수 있다. 격자 기반 양자내성암호의 경우, 총 26개 제안되었으며, 이 중 5개는 전자서명 방식이며, 나머지 21개는 KEM 혹은 암호화 방식으로 확인되었다. 코드 기반의 경우, 총 18개가 제안되었으며, 2개의 전자서명 기법과 16개의 KEM/암호화 방식으로 제안되었다. 다 변수 기반의 경우는 총 9개 (7개의 전자서명과 2개의 KEM/암호화)가 제출되었다. 해시 기반의 경우, 3개가 제출되었으며, 해시 기반 특성으로 인해 모두 전자서명 기법으로 제안되었다. Isogeny 기반의 경우, SIKE [1]라는 KEM 방식이 제안되었으며, 기타 유형으로 Post-quantum RSA-Signature/Encryption 등이 있다. 이러한 미국 NIST 양자내성암호 표준 공모 사업에 제출된 여러 기법들에 대

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구)
* 부산대학교 전기전자컴퓨터공학과 (pth5804@pusan.ac.kr)
** (교신 저자) 부산대학교 전기전자컴퓨터공학과 howonkim@pusan.ac.kr

해 NIST PQC 포럼을 통해, 전 세계 다양한 연구자들과 NIST 간의 의견 교환을 통해, 표준화 사업이 진행되고 있다.

표준화 사업에 있어서, 미국 NIST에서는 소프트웨어용 API만 제시하였으며, 제출된 대다수의 양자내성암호 기법들이 하드웨어 구현 결과물을 제시되어 있지 않고, 제안된 기법들의 경우, 서로 다른 FPGA 하드웨어 환경 상에서의 성능을 제시하고 있는 문제점이 있었다. 이를 해결하기 위해, 미국 조지 메이슨 대학교의 Kris Gaj 교수 연구진에서는 미국 NIST 양자내성암호 공모전을 위한 하드웨어 API를 제안하였다 [2]. 표준화 사업에 제출된 기법들에 대한 대표적인 안전성 공격 사례는 코드 기반 KEM 방식인 DAGS에 대해 partial brute-force search 기반의 공격과 Grobner bases를 가지는 bilinear system의 resolution을 활용한 공격에 대해 취약성 및 공격 성공 연구가 발표되었다 [3]. 이로 인해, 현재 DAGS는 해당 공격에 안전한 파라미터 선정 연구 및 관련 구현 연구가 진행되고 있다. 표준 공모전 후보군들에 대한 소프트웨어 성능 평가의 경우, SUPERCOP[4]에서 미국 NIST 표준 공모전에 제출된 KEM과 전자서명 기법 중 일부에 대해 titan0 (Intel Haswell) 환경 상에서의 소프트웨어 성능 평가 결과를 제시하고 있다. 그리고 표준 공모전 후보군 통합의 경우, 최근 10월 22일부로 미국 NIST 표준 공모전에 제출되었던 Post-Quantum RSA Encryption과 Post-Quantum RSA Signature 기법이 Post-Quantum RSA로 통합되어 표준 공모전이 진행 중에 있다.

Ⅲ. 양자내성암호 소프트웨어 구현 연구 동향

최근 CHES 2018에서는 양자내성암호에 대한 다양한 연구결과들이 발표되었으며, 그 중 양자내성암호 소프트웨어 구현 연구 동향에 대해 살펴본다.

Oder et al. [5]는 Adaptive chosen-ciphertext attack과 같은 active attack과 부채널 공격에 강인한 ring-LWE 암호화 방식을 제안하였으며, ARM Cortex-M4F 환경 상에서의 Frodo KEM에 제안 기법을 적용한 소프트웨어 성능 결과를 제시하고 있으며, Frodo KEM encapsulation에는 4,176,684 cycle이 소요되었으며, masking과 hiding 기법이 적용된 decapsulation의 경우, 25,640,830 cycle이 소요되었다.

Ducas et al. [6]은 미국 NIST 양자내성암호 표준 공모전에 제출된 CRYSTAL (Cryptographic Suite for Algebraic Lattices)의 격자 기반 서명 기법인 Dilithium에 대한 AVX2 (Advanced Vector eXtension 2) SIMD (Single Instruction Multiple Data) 기반의 소프트웨어 최적화 구현 결과를 제시하고 있다. 해당 소프트웨어 구현물에 대한 타이밍 공격 대응 방안으로 Montgomery reduction을 사용하였으며, branch-free 알고리즘 기반으로 구현 되었다. 그리고 성능 향상 측면에서는 NTT (Number Theoretic Transform)을 사용하였고, SHAKE 해시 함수에 대해서는 AVX2 기반의 벡터화 구현을 적용하였다.

Seo et al. [7]은 32비트 ARMv7-A 프로세서와 64비트 ARMv8 프로세서 환경 상에서 Isogeny 기반의 SIDH (Supersingular Isogeny Diffie-Hellman) 키 교환 프로토콜과 SIKE Supersingular Isogeny Key Encapsulation)에 대한 ARM 어셈블리어와 NEON 어셈블리어 기반의 속도 최적화 소프트웨어 구현 결과를 제시하고 있다. 해당 구현물은 성능 향상을 위해, Hybrid-scanning 방식을 사용하는 Montgomery Reduction과 Multi-precision multiplication을 구현 적용하였다. 그리고 해당 구현물의 가장 큰 특징은 constant-time 수행을 보장함으로써 타이밍 공격과 캐시 공격에 대한 안전성을 제공한다.

Karmakar et al. [8]은 ARM Cortex-M 계열의 환경 상에서 미국 NIST 양자내성암호 표준 공모전에 제출된 CCA-secure 격자 기반 KEM인 Saber에 대한 소프트웨어 최적 구현 결과를 제시하고 있다. 그들은 성능 향상을 위해, 디지털 신호 처리 명령을 사용하였으며, 메모리에 대한 효율적인 접근을 위해, NTT 기반의 다항식 곱셈 고속화를 적용 하였다. 그리고 메모리 접근 효율성을 강화한 Karatsuba 곱셈기 및 just-in-time 방식을 적용하여 메모리 접근 효율성을 강화하였다. 고속 최적화 구현 결과물은 ARM Cortex-M4 환경 상에서 키 생성, encapsulation, decapsulation 과정에 각각 1.147K, 1,444K, 1,543K clock cycle이 소요되었으며, 메모리 최적화 구현물은 ARM Cotex-M0 환경 상에서 4,786K, 6,328K, 7,509K clock cycles의 속도와 6.2KB의 메모리를 소모하는 것으로 확인되었다.

Howe, James, et al. [9]은 미국 NIST 양자내성암호 표준 공모전에 제출된 Frodo KEM에 대해 ARM

Cortex-M4F 환경 상에서의 소프트웨어 최적화 구현 결과를 제시하고 있다. 제한적 메모리를 가지는 타겟 보드 환경의 특성으로 인해, 메모리 사용 최적화 구현에 맞추어 구현되었으며, 이를 위해, 에러 값에 대한 On-The-Fly 방식의 생성을 적용하였으며, 이를 기반 한 LWE 연산을 수행하는 구조에 대해 ARM 어셈블리어 기반으로 개발되었다. ARM Cotex-M4F 환경 상에서의 해당 최적화 구현 결과물은 Frodo KEM-976-AES의 키 생성 과정, Encapsulation, Decapsulation 과정에 있어 각각 35,484-byte, 63,484-byte, 63,628-byte의 메모리를 소모하였으며, 전체 수행에 있어서 315,600,317 cycle의 시간이 소요되었다. 부채널 공 공격 대응 관점에서 타이밍 공격에 대한 안전성 제공을 위해, constant-time 내에 수행되는 cSHAKE 해시함수를 사용하였으며, AES의 경우, 타겟 보드 상의 하드웨어 가속기를 사용하였다. 그리고 캐시 타이밍 공격에 대한 안전성 제공을 위해, FLASH_ACR 레지스터의 9, 10번 비트를 0으로 처리함으로써 cache 사용을 막는 형태로 구현 적용되었다.

Ⅳ. 양자내성암호 하드웨어 구현 연구 동향

양자내성암호 하드웨어 구현 연구 동향과 관련하여 CHES 2018에서 발표된 양자내성암호 하드웨어 구현에 대한 연구 결과에 대해 살펴본다.

Howe, James, et al. [9]에서는 격자 기반 Key Encapsulation 방식인 Frodo KEM에 대해 FPGA 하드웨어 구현 결과를 제시하고 있다. 해당 논문에서는 Frodo KEM의 Decapsulation 과정에 대해 FPGA 하드웨어 구현을 진행하였으며, 7,220 LUTs, 3,549 FFs와 1개의 DSP, 16개의 block RAM 모듈이 사용되었다. 논문에서의 최대 동작주파수는 162MHz이며, Decapsulation 과정에 20.7ms 시간이 소요된다. 해당 논문에서의 FPGA 설계 중점은 면적 사용률과 throughput 성능의 밸런스를 맞추는데 있으며, 하나의 multiplexer 모듈의 제한적 사용과 최소한의 메모리 사용에 중점을 두고 있다. LWE 곱셈 코어의 경우, 병렬화 처리를 하였으며, 재사용이 가능하도록 설계하였다. 하지만 해당 LWE 곱셈 코어가 설계에 있어 critical path를 생성하는 문제를 가지지만, 수행 시간은 입력의 개수에 의존성을 가지며, 이는 모든 설계 내용이 constant time 내에 수행되는 것을 의미한다. 대부분의 하드웨어 설계 결과는 2000 FPGA slice 이하를 사용하였으며, main parameter set에 대해 초당 51회의 연산(20ms)이 가능하며, higher parameter set에 대해 초당 22회의 연산(45ms)이 가능한 것으로 확인되었다.

Amiet et al. [10]에서는 Kintex-7 Xilinx FPGA 보드 환경 상에 SPHINCS-256 해시 기반 서명 기법을 구현하였으며, 19,000 LUTs, 38,000 FFs, 36 BRAMs을 사용하며, 서명 생성 과정에 1.53ms, 서명 검증 과정에 65μs를 소요하였다. Area와 Throughput 측면에서 기존 RSA 기반의 서명 방식에 비해 월등한 성능을 보이고 있다.

Ⅴ. 양자내성암호 안전성 분석 연구 동향

다음으로는 CHES 2018에서 발표된 양자내성암호에 대한 부채널 공격 및 안전성 분석 연구 동향에 대해 살펴본다.

Park et al.[11]에서는 Rainbow에 대해 서명 과정에서 matrix-vector product 생성에 사용되는 secret affine map S와 T 상에서의 비밀 정보 누출 취약성을 분석하였으며, 이를 바탕으로 Rainbow와 UOV (Unbalanced Oil and Vinegar)에 대해 8비트 AVR 환경 상에서 CPA (Correlation Power Analysis)를 통한 키 복구 공격 성공 사례를 제시하고 있다.

Albrecht et al. [12]에서는 ring-LWE와 module-LWE에 기반 한 격자 기반 양자내성암호에 대해 메모리에 다항식 계수 정보를 저장하는 인코딩 방식과 키를 저장하기 전 NTT를 수행하는 방식에 대한 cold boot attack에 대한 취약성 분석 결과를 제시하고 있으며, Kyber KEM에 대해 해당 공격을 시도하였을 경우, 첫 번째 인코딩 방식에서는 2^{43}회의 수행이 필요하며, 두 번째 인코딩 방식에서는 2^{70}회의 수행을 통한 공격이 가능하다는 것을 제시하고 있다. 이를 통해, ring-LWE 기반의 KEM 방식인 New Hope에서도 유사한 공격 난이도를 가지는 것을 제시하고 있다.

Groot method [13]에서는 결정론적 격자 기반 서명 기법인 Dilitium과 qTESLA에 대해 차분 오류 주입 공격에 대한 취약성 및 공격 성공 사례를 제시하고 있다. 해당 공격은 ARM Cortex-M4 환경 상에서 clock glitch 주입을 통한 차분 오류 주입 공격을 수행하였으

며, Dilithium의 수행시간 중 65.2%가 unprofiled 공격에 취약한 것으로 확인되었으며, 이를 통한 키 복구에 성공하였다.

Ⅵ. 양자내성암호 연구 전망

앞서 살펴본 바와 같이 최근 양자내성암호에 대해 소프트웨어/하드웨어 최적화 구현 및 부채널 공격/안전성 분석에 관한 연구가 활발히 이루어지고 있다. 특히, 미국 NIST 양자내성암호 표준 공모전에 제출된 후보군들에 대한 연구에 초점이 맞춰져있다. 하지만, 아직 많은 후보군들에 대한 구현 및 안전성 분석 연구가 필요할 것으로 보이며, 특히 미국 양자내성암호 표준 공모전 2라운드가 진행될 경우, 다양한 환경 상에서의 구현 연구의 필요성이 더 커질 것으로 예상 된다.그리고 안전성 분석의 경우, 암호 설계적 관점에서의 안전성 분석뿐만 아니라 다양한 부채널 공격에 대한 취약성 및 안전성 분석이 필요할 것으로 예상된다. 이러한 연구를 통해, 안전성과 구현성이 높은 후보군에 대한 응용 서비스 및 프로토콜에 대한 적용 연구도 활발해질 것으로 예상된다.

Ⅶ. 결 론

본 논문에서는 최신 양자내성암호 표준화 및 연구 동향에 대해 살펴보았다. 이를 통해, 많은 연구들이 미국 NIST 양자내성암호 표준 공모전의 후보군들에 초점이 맞춰 이루어지고 있으며, 향후 다양한 후보군들에 대한 구현 및 안전성분석 연구가 활발히 이루어질 것으로 보이며, 이러한 연구를 통해, 안전성과 구현 측면에서 검증된 기법들에 대한 응용 및 적용 연구 또한 활발히 이루어질 것으로 예상된다.

참 고 문 헌

[1] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. H. A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, Sike, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[2] Kris Gaj, “PQC Hardware API & Fair Benchmarking of PQC”, PQCrypt 2018 Recent Result Session, 2018

[3] Barelli, Elise, and Alain Couvreur. "An efficient structural attack on NIST submission DAGS." arXiv preprint arXiv:1805.05429 (2018).

[4] SUPERCOP (System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives), available at https://bench.cr.yp.to/supercop.html

[5] T. Oder, T. Schneider, T. Pöppelmann, and T. Güneysu, “Practical cca2-secure and masked ring-lwe implementation,” IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2018, no. 1, pp. 142 – 174, 2018.

[6] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, “Crystals-dilithium: a lattice-based digital signature scheme,” IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2018, no. 1, pp. 238 – 268, 2018.

[7] H. Seo, Z. Liu, P. Longa, and Z. Hu, “Sidh on arm: Faster modular multiplications for faster post-quantum supersingular isogeny key exchange,” IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 1 – 20, 2018.

[8] A. Karmakar, J. M. B. Mera, S. S. Roy, and I. Verbauwhede, “Saber on arm,” IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 243 – 266, 2018.

[9] J. Howe, T. Oder, M. Krausz, and T. Gneysu, “Standard lattice-based key encapsulation on embedded devices,” IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 372 – 393, 2018.

[10] Amiet, Dorian, Andreas Curiger, and Paul Zbinden. "FPGA-based Accelerator for Post-Quantum Signature Scheme SPHINCS-256." IACR Transactions on Cryptographic Hardware and Embedded Systems 2018.1 (2018): 18-39.

[11] Park, A., Shim, K.-A., Koo, N., & Han, D.-G.

(2018). Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3), 500-523. https://doi.org/10.13154/tches.v2018.i3.500-523

[12] Albrecht, M., Deo, A., & Paterson, K. (2018). Cold Boot Attacks on Ring and Module LWE Keys Under the NTT. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3), 173-213. https://doi.org/10.13154/tches.v2018.i3.173-213

[13] Groot Bruinderink, L., & Pessl, P. (2018). Differential Fault Attacks on Deterministic Lattice Signatures. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3), 21-43. https://doi.org/10.13154/tches.v2018.i3.21-43

〈저 자 소 개〉

박 태 환 (Taehwan Park)

학생회원

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

김 호 원 (Howon Kim)

종신회원

1993년 2월 : 경북대학교 전자공학과 (공학사)
1995년 2월 : 포항공과대학교 전자전기공학과 (공학석사)
1999년 2월 : 포항공과대학교 전자전기공학과 (공학박사)
2008년~현재 : 부산대학교 정보컴퓨터공학부 교수
2015년~현재 : 부산대학교 정보컴퓨터공학부 교수
관심분야 : IoT, 블록체인, 강화학습, 디지털트윈, 플랫폼 보안, 암호 프로세서 등