KpqC 암호 최적화 구현 동향

Trends in Optimized Implementation of KpqC Cryptography

송민호* ,엄시우*, 김상원* , 서화정**
* 한성대학교 (대학원생), **한성대학교 (교수)

요약

양자 컴퓨터의 발전은 현재 사용 중인 공개키 암호 알고리즘의 보안을 위협하고 있다. 이에 대한 대안으로 양자내성암호가 존재한다. 국내에서 자체적인 양자내성암호 개발 및 연구를 위해 2022년 KpqC 공모전을 개최하였고 2023년 12월 2라운드에 8개의 알고리즘이 선정되었다. 그러나 양자내성암호는 기존의 암호 알고리즘보다 많은 연산 시간 및 메모리 크기를 필요로 하여 최적화 연구가 중요하다. 따라서, 본 논문에서는 KpqC 공모전 2라운드에 진출한 암호들의 최적 구현에 대한 동향을 알아본다.

서론

양자 컴퓨터의 발전과 피터 쇼어(Peter Shor)의 알고리즘은 기존의 공개키 암호 알고리즘의 보안을 위협한다. 쇼어 알고리즘은 인수분해, 이산로그 등의 수학적 문제에 기반하는 공개키 암호 알고리즘을 다항 시간 내에 해독할 수 있는 알고리즘이다[1]. 이러한 양자 컴퓨터 환경에서 안전할 수 있는 새로운 공개키 암호가 필요한데 이를 양자내성암호라고 한다. 그러나 양자 내성암호는 기존에 사용하는 암호 알고리즘보다 연산시간이 오래 소요되며 필요한 메모리 크기도 크다. 이러한 특징으로 인해 성능 향상을 위한 최적화 연구가 필요하다.
따라서 본 논문에서는 KpqC(Korea Post Quantum Cryptography) 공모전 2라운드에 진출한 암호 알고리즘에 대해 살펴보며 최적 구현에 대한 동향을 알아본다.

KpqC

국내에서 자체적인 양자내성암호를 개발하고자 KpqC 공모전을 개최하였다. 2022년 양자내성암호연구단에서 개최한 KpqC 공모전을 통해 연구가 진행되고 있으며 총 16개의 알고리즘이 공모전 1라운드를 진행하였다. 이후 2023년 12월 8개의 알고리즘이 선정되었으며 2라운드에 진출했다.
2라운드 진행 중인 KpqC는 PKE/KEM 및 Digital Signature로 나뉘어진다. NTRU+, PALOMA, REDOG, SMAUG-T 4개는 PKE/KEM 알고리즘이며 AIMER, HATAE, MQ-Sign, NCC-sign 4개는 Digital Signature 알고리즘이다.
NTRU+, SMAUG-T는 격자 기반 PKE/KEM에 해당한다. NTRU+는 기존에 존재하는 NTRU의 단점을 극복하여 만들어진 공개키 알고리즘이다. NTRU는 다항식 기반 환의 격자에 구축된 실용적인 공개키 암호이며 NTRU+는 다항식 차수에 따라 NTRU+576, NTRU+768, NTRU+864, NTRU+1152로 나누어진다[2]. SMAUG-T는 KpqC 공모전 1라운드에 제출되었던 SMAUG와 TiGER가 병합된 암호이다. MLWE(Module Learning With Errors)와 MLWR(Module Learning with Round)에 기반하며 크기에 따라 TiMER, SMAUG-T128, SMAUG-T192, SMAUG-T256로 나누어진다[3].
REDOG, PALOMA는 코드 기반 PKE/KEM에 해당한다. REDOG은 Gabidulin 코드를 기반으로 하며 안전성에 따라 REDOG-1, REDOG-2, REDOG-3으로 나누어진다[4]. PALOMA는 NP-hard SDP 기반 트랩도어와 이진 분리 가능한 Goppa code 및 FO(Fujisaki-Okamoto) 변환을 결합하여 설계된 KEM이다. 안전성에 따라 PALOMA-128, PALOMA-192, PALOMA-256으로 나누어진다[5].
MQ-Sign은 다변수 기반 전자서명이다. MQ-Sign은 다변수 이차식(Multivariate Quadratic)을 기반으로 하며 이는 다변수 이차식의 해를 구하는 것이 어렵다는 문제를 기반으로 한다. 키 생성 방법에 따라 MQ-Sign-RR, MQ-Sign-LR로 나누어진다[6].
AIMER는 영지식 기반 전자서명이다. 단방향 함수를 위한 Preimage Knowledge에 대한 영지식증명을 기반으로 한다. 키와 서명 사이즈에 따라 aimer128f, aimer128s, aimer192f, aimer192s, aimer256f, aimer256s로 나누어진다[7].
HATAE, NCC-Sign은 격자 기반 전자서명이다. HATAE는 CRYSTALS-Dilithium 알고리즘과 같은 Fiat-Shamir with Aborts 패러다임을 기반으로 한다. 안전성에 따라 HATAE-120, HATAE-180, HATAE-260으로 나누어진다[8]. NCC-Sign은 비순환 다항식을 사용하며 RLWE를 기반으로 한다. 안전성에 따라 NCC-Sign1, NCC-Sign3, NCC-Sign5로 나누어진다[9].

KpqC 최적 구현 동향

SMAUG-T

J. H. Cheon, et al.[3]은 AVX2 환경에서 AVX 벡터화를 통한 최적화된 구현과 symmetric primitives를 위한 90s 최적화 구현을 제공한다. AVX2 내장 함수를 사용하여 최적화를 진행하였으며 약 1.7배에서 1.8배의 성능 향상을 보여주었다. 90s 구현은 내부 알고리즘 대신 AES, SHA2를 활용하여 최적화된 성능을 보여주기 위한 벤치마크 역할을 한다. 해시 함수 G, H, 확장 가능한 출력 함수 XOF, 의사 난수 함수 PRF를 교체한다. G는 SHA2-512로 H는 SHA2-256으로 XOF와 PRF는 모두 AES를 사용하게 된다. 이를 통한 90s 최적화 구현은 약 2.5배에서 3배의 성능 향상을 보여주었다.

AIMER

Lee, Minwoo, et al.[10]는 Symmetric primitive AIM에 대한 고속 구현 기법을 통해 AIMER 최적화 구현을 진행하였다. 해당 구현에서는 Mer 연산 최적화 기법과 선형 레이어 연산 단순화를 사용한다. AIM-1 암호화 연산의 경우 동일한 입력 값을 복사하여 Mer3 및 Mer27 연산을 수행한다. 그러나 제안된 Combined Mer 연산은 각각의 연산을 수행하지 않고 결합하여 한 번의 Mer 연산을 진행한다. 제안된 연산은 Mer27 연산을 한 번 진행하는 것과 동일한 복잡성을 갖는다. AIM의 선형 레이어 연산은 총 4번의 행렬 벡터 곱셈을 수행하며 암호화할 때 마다 새로운 행렬을 생산한다. 하지만 해당 연구는 룩업 테이블을 사용하여 필요한 행렬을 미리 생성한 후 암호화를 진행한다. 이를 통해 최적화를 진행하였다. 해당 연구를 통해 전체적인 성능은 [표 1]과 같으며 기존 레퍼런스 코드에 비해 97.9%의 성능 향상을 보여줬다.

HATAE

H. C. Jung, et al.[8]는 AVX2 명령어를 사용하여 최적화된 구현을 제공한다. HATAE의 계산 시간을 크게 결정짓는 요소로 Keccak, NTT, 하이퍼볼 샘플링이 존재한다. Keccak 및 NTT는 기존에 존재하는 최적화된 코드를 사용하였고 본 연구는 하이퍼볼 샘플링을 AVX2 명령어를 사용하여 효율적으로 구현하는 방법을 보여준다. 하이퍼볼 샘플링을 병렬화하기 위해 4개의 서로 다른 다항식을 병렬로 샘플링하는 방식을 선택했다. 샘플링 과정이 복잡하기 때문에 내부 메모리 상태를 여러 번 전달하는 절차를 가진다. 병렬화된 Keccak의 속도는 레퍼런스에 비해 5~7배 빨라졌으며 Dilithium에서 가져온 최적화된 NTT는 약 19배 빨라졌다. 종합적으로 봤을 때 최적화된 구현은 기존보다 서명 생성 과정에서 약 5배 빨라졌으며 서명 검증의 경우 3~4배 빨라졌다.

NCC-Sign

K. A. Shim, et al.[11]는 SampleInBall이라는 알고리즘을 통해 최적화 구현을 제안한다. SampleInBall은 두 개의 서로 다른 다항식을 사용하는 서명 및 검증 알고리즘에서 challenge 다항식을 선택하기 위해 최적화된 알고리즘이다. 이를 통해 Rejection Sampling의 반복 횟수를 줄여 효율적인 연산을 가능하게 한다. 본 연구에서는 SampleInBall 알고리즘이 Rejection Sampling 과정에서 9%~15%의 속도 향상을 보여줬다.

<표 1> AIMER Performance result

	Ref	Combined Mer	Linear Layer	Combined Mer + Linear Layer
Ms	38482	38171	1268	1181
Imprv(%)	0	0.91	97.6	97.9

결론

본 논문에서는 KpqC 공모전 2라운드에 진출한 양자내성암호의 최신 최적 구현 동향에 대해 알아보았다. AVX2 명령어를 통한 최적화 구현이나 내부 함수 최적화를 통해 속도 향상을 진행하는 연구를 확인할 수 있었다. 현재 PQC에 비해 KpqC는 다양한 최적화 연구가 진행되고 있지 않다. 이는 KpqC 공모전을 시작한지 얼마 안되었으며 최신에 2라운드 후보자가 선정되었기 때문으로 보인다. 현재 다양한 최적화 연구가 진행되고 있는 PQC의 연구 내용을 KpqC에 적용하면 다방면으로 성능 향상이 될 것으로 보인다. 또한 KpqC에서만 사용하는 내부 함수들의 성능 향상을 위한 최적화 연구가 필요할 것으로 보인다.

Reference

[1] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.
[2] J. H. Kim, and J. H. Park. “NTRU+: compact construction of NTRU using simple encoding method”, IEEE Transactions on Information Forensics and Security, 2023.
[3] J. H. Cheon, et al. “SMAUG-T: the Key Exchange Algorithm based on Module-LWE and Module-LWR”, Algorithm Specifications Version 3.0, 2024. available at: https://github.com/hmchoe0528/SMAUG-T_public/blob/9a97c39459b4a757db123c9ffe23c6d32047b8b5/supporting_documentation/SMAUG-T_spec_24.02_v3.0.pdf
[4] J. L. Kim, et al. “REDOG and its performance analysis.” Cryptology ePrint Archive(2022).
[5] D. C. Kim, et al. “PALOMA: binary separable Goppa-based KEM.” Code-Based Cryptography Workshop. Cham: Springer Nature Switzerland, 2023.
[6] K.A. Shim, J. Kim, and Y. An. “MQ-Sign: A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster”, KpqC Round 1, 2022, https://www.kpqc.or.kr/images/pdf/MQ-Sign.pdf.
[7] J. Y. Lee, et al. “The AIMer Signature Scheme ”, KpqC Competition 2nd Round Submission (v2.0), 2024, available at:https://kpqc.or.kr/images/pdf/AIMer_Document.pdf
[8] H. C. Jung, H. M. Choe, D. Julien, G. Tim, D. Y. Hong, K. Markus, L. Georg, M. Marc, J. B. Shin, S. Damien and M. J. Yi. “HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures”, Algorithm Specifications Version 2.1, 2024. available at https://kpqc.cryptolab.co.kr/haetae
[9] K. A. Shim, J. S. Kim, and Y. J. An, “NCC-Sign: A New Lattice-based Signature Scheme using Non-Cyclotomic Polynomials.” Submission to the KpqC 1 (2022).
[10] Lee, Minwoo, et al. "High-speed Implementation of AIM symmetric primitives within AIMer digital signature." Cryptology ePrint Archive (2023).
[11] Shim, Kyung-Ah, Jeongsu Kim, and Hyeokdong Kwon. "NCC-Sign: A New Lattice-based Signature Scheme using Non-Cyclotomic Polynomials and Trinomials.“