정 보 보 호 학 회 지
제34권 제2호, 2024. 4

KpqC 공모전 2라운드 암호 소개 및 동향

엄 시 우*, 송 민 호**, 김 상 원**, 서 화 정***

요 약

2022년 KpqC 공모전을 통해 국내에서 자체적인 양자 컴퓨터에 대한 내성을 갖는 양자 내성 암호 개발을 진행하고 있다. 2022년 16개의 알고리즘이 1라운드를 진행하여, 2023년 12월 1라운드를 통과한 8개의 알고리즘이 현재 2라운드를 진행하고 있다. 본 논문에서는 1라운드를 통과한 2라운드 후보 알고리즘에 대해서 소개하고 1라운드 이후 2라운드 후보 알고리즘의 최신 개발 동향에 대해서 소개한다.

Ⅰ. 서 론

RSA 암호의 안전성은 대규모 소인수분해의 계산적 어려움에 기반을 두고 있다. 그러나, 피터 쇼어(Peter Shor)에 의해 개발된 알고리즘은 양자 컴퓨터를 이용하여 소인수분해 문제를 효율적으로 해결할 수 있음을 보여준다[1]. 이는 양자 컴퓨터의 실현 가능성이 점차 현실화됨에 따라, 현재 널리 사용되는 암호 체계의 보안성에 심각한 위협을 가하고 있으며, 양자 컴퓨터 시대에 대비한 새로운 암호 기술의 필요성을 촉구하고 있다.

이에 대응하여, 미국 국립표준기술연구소(NIST)는 양자 컴퓨터에 대한 내성을 갖는 암호화 기술, 즉 양자 내성 암호(Post-Quantum Cryptography, PQC)의 표준화를 진행하였다. 이 공모전을 통해 다양한 양자 내성 암호 알고리즘들이 제안되었으며, CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon 그리고 SPHINCS+가 최종 라운드에 선정되었다. 현재는 추가적인 전자 서명 표준화를 위해 추가적인 전자서명 PQC 공모전이 진행중이다.

국내에서도 2022년부터 KpqC(Korea Post-Quantum Cryptography) 공모전을 통해 국내의 자체적인 PQC 알고리즘 개발을 진행하고 있다. 2022년 16개의 알고리즘이 1라운드를 진행하였으며, 2023년 12월 1라운드를 통과한 알고리즘들이 발표되어 현재 8개의 알고리즘이 2라운드 진행 중에 있다.

본 논문은 국내에서 진행 중인 KpqC 공모전의 2라운드에 진출한 2라운드 후보 알고리즘들을 소개하고, 해당 알고리즘들의 최신 동향을 소개한다.

Ⅱ. KpqC 2라운드 후보 알고리즘 소개(Digital Signature, PKE/KEM)

2.1. 격자 기반 PKE/KEM

격자 기반 암호는 격자 위에서 계산하는 문제의 어려움을 기반으로 한다. NP-hard라는 수학 문제를 기반으로 두고 있기 때문에 안전성에 강점이 있으며 계산 효율성이 높다. NP-hard는 다항시간 내에 풀 수 없는 문제를 의미하며 다항식 대신에 지수식으로 풀 수 있는 문제를 뜻한다[2].

격자 기반 암호의 가장 큰 특징 중 하나는 인수분해와 같은 어려운 수학적 문제를 사용하는 것이 아닌 행렬처럼 쉬운 문제를 기반으로 한다는 것이다. 쉬운 문제에 잡음을 주어 답을 조금씩 다르게 한다면 수학적으로 어려운 문제로 만들 수 있으며 200차원의 격

본 연구는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 50%) 그리고 본 연구는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천기술 연구, 50%).

* 한성대학교 정보시스템공학과 (대학원생, shuraatum@gmail.com)
** 한성대학교 융합보안학과 (대학원생, smino0906@gmail.com, kim3875@gmail.com)
*** 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

차를 사용하기 때문에 답을 찾기 어렵다.

오늘날에는 격자 기반이 암호화, 복호화, 전자서명 뿐만 아니라 동형암호, 함수암호 등 여러 분야에서 연구가 진행되고 있다. 대표적으로는 NTRU, BLISS 등이 있으며 NIST PQC 공모전에 최종 선정된 FALCON, CRYSTALS-Kyber/Dilithium이 존재한다.

2.1.1. NTRU+

NTRU는 다항식 기반 환(Ring)의 격자에 구축된 실용적인 공개 키 암호화 체계이며 지난 수십 년 동안 암호 분석 공격으로부터 안전한 것으로 간주되었다[3]. 그러나 NTRU는 다른 격자 기반 암호에 비해 상대적으로 느리며 최악의 정확성 오류를 달성하기 어렵다는 단점을 가지고 있다. 이러한 단점을 가진 NTRU의 성능을 거의 모두 극복한 KEM 체계가 NTRU+이다.

NTRU+는 FO⊥(Fujisaki-Okamoto 변형) 및 ACWC2라는 변환 기법으로 구성된다[4]. FO⊥는 재암호화 없이 선택된 암호문 보안을 달성하는데 사용되며 ACWC2는 최악의 정확성 오류를 쉽게 달성하기 위해 사용된다.

다항식 차수에 따라 NTRU+576, NTRU+768, NTRU+864, NTRU+1152로 분류가 가능하며 각각의 모듈러스 및 크기는 (표 1)과 같다.

〔표 1〕 Sizes of NTRU+ (n: polynomial degree of the ring. q: modulus)

	n	q	Sizes (bytes)	
NTRU+ 576	576	3,457	pk	864
			ct	864
			sk	1,728
NTRU+ 768	768	3,457	pk	1,152
			ct	1,152
			sk	2,304
NTRU+ 864	864	3,457	pk	1,296
			ct	1,296
			sk	2,592
NTRU+ 1152	1,152	3,457	pk	1,728
			ct	1,728
			sk	3,456

2.1.2. SMAUG-T

SMAUG-T는 KpqC 공모전 1라운드에 제출되었던 SMAUG와 TiGER가 병합된 암호이다. SMAUGT-T.PKE의 IND-CPA 보안은 MLWE(Module Learning With Errors) 문제와 MLWR(Module Learning With Rounding) 문제의 견고성에 의존하며 이는 SMAUG-T.KEM의 IND-CCA2 보안을 의미한다[5]. MLWE 문제 강도를 기반으로 비밀 키에 대한 보안을 보장하며 MLWR 문제 강도에 의존하여 공유 키를 보호한다. SMAUG-T.KEM의 체계는 최근 양자 내성 KEM의 구성 방식인 Lizard[6] 및 RLizard[7]을 따른다. SMAUG-T는 PKE 체계 SMAUGT-T.PKE로 구성되며 FO(Fujisaki-Okamoto) 변환을 통해 SMAUGT-T.KEM으로 전환된다.

SMAUG-T는 경량 디바이스에 적합하도록 설계되었으며 빠른 성능, 작은 메모리 크기, 짧은 키 길이, 부채널 공격에 대한 저항성을 가진다. 크기에 따라 SMAUG-T128, SMAUG-T192, SMAUG-T256으로 구분하며 각각 NIST 보안 레벨 1, 3, 5에 해당한다. IoT를 위해 새로 제안된 TiMER는 보안 레벨 1에 해당한다. 각각의 크기와 성능은 (표 2)와 같다.

〔표 2〕 Sizes and Performance of SMAUG-T on Intel Core i7-10700k (3.80GHz)

	Sizes (bytes)		Cycles (med)	
TiMER (for IoT)	sk	136	keygen	70,348
	pk	672	encap	71,748
	ctxt	608	decap	90,978
SMAUG-T128	sk	176	keygen	70,398
	pk	672	encap	75,082
	ctxt	672	decap	97,368
SMAUG-T192	sk	236	keygen	136,436
	pk	1,088	encap	126,114
	ctxt	1,024	decap	160,354
SMAUG-T256	sk	218	keygen	231,824
	pk	1,792	encap	232,854
	ctxt	1,472	decap	271,794

2.2. 코드 기반 PKE/KEM

코드 기반 PKE/KEM(Public Key Encryption/Key Encapsulation Mechanism)은 암호화 알고리즘의 일종으로, 특정 오류 수정 코드를 복호화 문제의 어려움에 기반하는 공개 키 암호화의 한 형태이다. 코드 기반 암호 설계의 주요 아이디어는 메시지에 의도적으로 오류를 주입해서 오류를 정확히 알고 있는 사용자만 메시지를 복원할 수 있도록 만드는 것이다. 코드 기반은 양자내성암호 중에서도 가장 오래된 분야이며, 가장 초기이자 가장 잘 알려진 코드 기반 암호 시스템 중 하나는 1978년 Robert McEliece가 제안한 McEliece 이다[8]. McEliece는 특정 오류 수정 코드의 일종인 Goppa 코드를 기반으로 한다.

코드 기반 암호화는 행렬 연산이기 때문에 암호화 연산 속도가 빠르다는 장점이 있으나, 복호화가 암호화보다 연산 속도가 느리고 키 크기가 크다는 단점이 있다.

2.2.1. REDOG

NIST PQC에 제안됐던 McNie는 McEliece와 Niederreiter 암호 시스템의 특징을 모두 가지고 있으며 코드 기반 암호화 시스템에 대한 Known Structural Attack으로부터 안전하도록 설계되었다. 하지만 [9]에서 Gaborit이 제안한 메시지 복원 공격(Message Recovery Attack)에 의해 보안강도가 약해졌고 이를 보완하기 위해 McNie의 수정본[10]인 Dual-Ouroboros가 제안되었다.

이는 LRPC(Low Rank Parity Check codes) 복호화를 사용하는데, LRPC 복호화는 확률적 복호화 알고리즘으로서 복호화 실패 확률을 가진다. 이를 해결하기위해 LRPC 코드를 Gabidulin 코드로 대체한 변형된 형태의 Dual-Ouruboros(DO.Gab-PKE)[11]가 제안되었다. Gabidulin 코드는 복호화 실패확률이 0이며 더욱 향상되고 빠른 복호화 연산 복잡성을 갖는다. 게다가 Gabidulin 코드를 사용하는 DO.Gab-PKE는 Overbeck's attack을 포함하여 기지 평문 복구 공격에 대해 훨씬 더 강력한 보안을 제공한다. 하지만 이후에 가역행렬 S를 선택하는 제한조건이 없는 경우에 암호 알고리즘이 안전하지 않다는 것이 밝혀져, 이를 보안한게 REinforced modified Dual-Ouroboros based on Gabidulin codes 줄여서 REDOG이라고 한다[12].

REDOG에서는 비밀키 선택을 위해 F_{q^m}의 서브필드 λ-디멘션 상의 가역행렬을 사용하였고 공개키는 r-Frobenius weak code 사용을 피해서 Frobenius weak attack을 미연에 방지하도록 하였다. REDOG은 기존 Do.Gab-PKE의 많은 부분을 개선하였지만, 비밀키, 공개키의 안전을 위한 기법으로 인해 키 크기가 커지는 단점이 존재한다.

2.2.2. PALOMA

PALOMA는 이진 분리 가능한 Goppa code를 사용하는 NP-Hard 신드롬복호화(SDP) 기반 트랩도어와 ROM과 QROM 모두에서 IND-CCA2 보안을 보장하는 FO(Fujisaki-Okamoto) 변환을 결합하여 설계된 키 캡슐화 메커니즘(KEM)이다[13].

SDP는 random binary parity-check matrix와 syndrome에 대해 특정 해밍 웨이트를 가지는 preimage vector를 찾는 문제이다. SDP의 트랩도어 구조는 McEliece와 Niederreiter 암호 알고리즘에도 적용되어 있다. PALOMA의 단점은 공개키 크기가 크고 키 생성이 느리다는 것이다. 이는 SDP의 특성에 기인하는데, SDP는 랜덤 매트릭스에서 공개키가 도출되기 때문이다. 다만 PALOMA는 SDP를 완전하게 도입하는 트랩도어 구조만을 차용하였고 binary separable Goppa code와 FO 변환을 사용하여 IND-CCA2 보안 요구사항을 보장하였다.

PALOMA의 특성상 서버-클라이언트간 일시적인 키 생성에 활용하기 유리하며, E2EE (end-to-end encryption)과 같은 클라이언트-클라이언트간에는 고정 키를 사용하는 것을 추천하고 있다.

2.3. 다변수 기반 전자서명: MQ-Sign

다변수 이차식(Multivariate Quadratic:MQ) 기반 전자서명은 다변수 이차식의 시스템의 해를 구하는 것이 어렵다는 문제를 기반으로 한다. MQ-Sign은 짧은 서명, 짧은 비밀키 길이와 빠른 성능을 목표로 UOV(Unbalanced Oil-and-Vinegar) 구조를 이용하여 설계되었다. UOV는 1999년 Aviad Kipnis et al.이 제안한 단일 레이어를 갖는 MQ-기반 전자서명이다[14]. MQ-Sign은 희소 다항식(Sparse Polynomials:S)

과 무작위 다항식(Random Polynomials:R)을 사용하여 SS,SR,RS,RR 네 가지 유형의 비밀키를 제공한다. 네 가지 유형의 서로 다른 키 생성 방식에도 불구하고, 동일한 서명과 검증 알고리즘으로 동작 가능하다[15].

MQ-Sign은 절반 크기 부분 행렬과 슈어 보수 행렬(Schur complement matrix)의 역행렬을 활용하는 Block Inversion Method(BMI)를 이용하여 더 빠른 서명 생성이 가능하다. 또한, 서명 생성에서 계산의 대부분을 차지하는 선형 시스템의 해를 구하기 위한 부분 행렬 간의 연산을 사전 계산할 수 있도록 설계되어 굉장히 빠른 온라인 서명이 가능하다. 결과적으로 사전 계산이 포함된 MQ-Sign은 사전 계산이 없는 방식보다 안전도 1, 3, 5에서 4.6~6.3배 빠르다.

2.4. 영지식 기반 전자서명: AIMer

AIMer는 단방향 함수를 위한 Preimage Knowledge에 대한 영지식증명(Zero-Knowledge Proof, ZPK)을 기반으로 한 전자서명이다. ZKP는 사용자가 특정 계산의 결과를 알고 있다는 것을 증명하는 방식으로 동작한다.

AIMer 전자 서명은 MPC-in-the-Head 패러다임[16]을 사용하여 원방향 함수의 시뮬레이션을 통해 ZKP 시스템을 구축한다. MPCitH 패러다임에 기반한 시스템 중에서 BN++ 증명 시스템[17]을 사용하여 구성되며, 이 시스템은 복잡한 필드 연산을 효율적으로 처리하고 증명하는 데 특화되어 있다. BN++은 NIZPoK(Non-Interactive Zero-Knowledge Proof of Knowledge) 시스템의 하나로, 대규모 필드에서의 산술 연산을 증명하기 위해 다자간 계산(Multi-Party Computation, MPC)을 가상으로 실현한다. AIMer는 이러한 패러다임을 활용하여 원방향 함수의 작동을 시뮬레이션하고 그 결과를 제로 지식 증명으로 구성함으로써 보안성 있는 디지털 서명을 생성한다.

MPCitH를 기반으로 하는 전자 서명의 특징은 원방향 함수의 일방향성을 통한 보안을 제공하고 시간과 크기 사이의 트레이드 오프가 있어 작은 공개키와 작은 개인키로 동작 가능하지만 서명과 검증 시간이 오래 걸리고 큰 서명값을 갖는 문제도 있다.

2.5. 격자 기반 전자서명: HAETAE

HAETAE[18]은 최신 격자 기반 전자서명 체계로, 높은 안전성과 효율성을 제공한다. 이 체계는 "Fiat-Shamir with Aborts" 패러다임[19, 20]를 기반으로 한다. HAETAE는 CRYSTALS-Dilithium[21]과 유사하지만, 이보다 더 짧은 서명 및 검증 키 크기를 사용하도록 설계됨으로써 공간 제한적인 환경에서도 사용 가능한 설계를 목표로 하였다. 격자 기반 문제(LWE와 SIS)의 어려움에 기반하여 안전성이 보장되며, CRYSTALS-Dilithium과의 두 가지 주요 차별점은 하이퍼볼 균일 분포의 사용과 바이모달 분포를 통한 Rejection 샘플링이다. 이러한 접근 방식은 서명의 크기를 줄이고, 공격에 대한 저항성을 향상시킨다.

HAETAE의 설계는 높은 수준의 보안을 유지하면서도, 서명 및 검증 키 크기를 대폭 축소하였다. 예를 들어, 서명 및 검증 키 크기는 각각 Dilithium 대비 최대 39% 및 25%까지 줄일 수 있다. 이는 TCP나 UDP 데이터그램에 서명을 쉽게 포함시킬 수 있음을 의미한다.

2.6. 격자 기반 전자서명: NCC-Sign

NCC-Sign Non-cyclotomic은 비순환 다항식을 사용하는 새로운 격자 기반 서명 알고리즘으로, 현존하는 2의 멱승의 순환 다항식 기반 구조의 보안 우려를 해결하기 위해 제안되었다[22]. 기존의 순환 다항식을 사용하는 방식과는 달리, NCC-Sign은 $X^p - X + 1$ 형태의 비순환 다항식을 이용하며, 이는 가장 큰 갈루아 그룹에 해당하는 S_p와 동형인 대수적 구조를 제거함으로써 강한 안전성을 제공한다. 그러나 비순환 다항식을 사용하는 NCC-Sign은 잠재적인 위협에 대해 보다 강한 안전성을 보장하지만, 2의 멱승의 순환 다항식 기반 알고리즘의 최적화된 구현 방법을 사용할 수 없어 효율성이 떨어진다는 단점이 있다. 이 문제를 해결하기 위해, 강한 안전성 제공과 효율성을 충족시킬 수 있도록, 차수가 $n = 2^a \cdot 3^b$인 다항식 $X^n - X^{n/2} + 1$을 사용하는 NCC-Sign Trinomial을 제안하였다. NCC-Sign은 2의 멱승의 순환 다항식을 이용한 RLWE와 MLWE 기반 암호에서 발생하는 파라미터 점프가 없어 원하는 복잡도의 파라미터를 유연하게 선택할 수 있다는 장점이 있다. 결과적으로,

NCC-Sign의 파라미터의 고전적인 Core-SVP 추정치가 보안 수준인 1, 3, 5에서 각각 128, 192, 256비트와 거의 동일하거나 이를 초과한다. 이는 Core-SVP 추정치가 각 보안수준에서 123, 182, 252인 Dilithium에 비하여 더 높은 복잡도와 강한 안전성을 제공한다. 이는 현재 진화하는 다양한 공격에 대한 대응의 관점에서 충분한 안전성 마진을 확보하고 있다고 볼 수 있다.

Ⅲ. 암호 알고리즘 별 개발 동향

본 장에서는 KpqC 2라운드 후보 알고리즘에 대해 KpqC 1라운드 이후에 알고리즘의 성능적인 부분 또는 변경 사항과 같은 후보 알고리즘의 동향을 소개한다. KpqC 공모전에서는 1라운드를 통과한 2라운드 후보 알고리즘에 대해 알고리즘의 상세 설명과 현재 개발 현황을 공유하기 위한 2024 Winter Camp를 개최하였으며, 해당 세미나에서 2라운드 후보 알고리즘의 자세한 진행 현황을 발표하였다. 본 논문에서는 2024 Winter Camp에서 공개된 자료를 포함한 2라운드 후보 알고리즘에 대한 동향을 소개한다[23]. 다만 1라운드 이후 알고리즘의 큰 변경 사항 또는 발표된 자료가 없는 알고리즘의 경우 제외하고 소개한다.

3.1. NTRU+ 알고리즘 동향

NTRU+는 초기에 다중 대상 공격에 대한 보안을 고려하도록 설계되지 않았다. 보안성을 높이기 위해 NTRU+는 $FO\perp$ 변환을 적용할 때 공개 키의 해시 값 $F(pk)$을 $(r,K)=H(m,F(pk))$와 같은 해싱에 추가하는 방법을 선택했다. 이에 따라 비밀 키도 $sk=(f,h^{-1},F(pk))$로 변경되었으며 전체적으로 크기가 32바이트씩 늘어났다. 변경을 통해 보안성은 높아졌지만 KeyGen, Encap, Decap 과정의 cycle 수가 늘어났으며 전체적인 성능이 떨어졌다.

NTRU+는 NTRU+PKE라는 새로운 NTRU 기반의 IND-CCA 보안 PKE를 제안했다. NTRU+PKE는 $\overline{FO}^{\perp}_{KEM}$이라고 하는 $FO^{\perp}_{PKE}$의 변형을 CPA-NTRU+에 적용하여 만들어진다. 여기서 $FO^{\perp}_{PKE}$는 Fujisaki et al.이 [24]에서 제안한 변환을 의미하며 IND-CPA 보안 PKE에서 IND-CCA 보안 PKE로 변환한다. 기존의 NTRU+와 NTRU+PKE 관련 혼동을 방지하기 위해 기존의 NTRU+는 NTRU+KEM이라 명칭하였다.

3.2. SMAUG-T 알고리즘 동향

SMAUG-T는 부채널 공격의 종류 중 하나인 타이밍 공격에 대비하기 위해 상수시간 구현인 $dGaussian_{\sigma}$을 사용한다. 그러나 $dGaussian_{\sigma}$에 대한 전력/EM 기반 부채널 공격 문제가 KpqC 1라운드에서 발생했다. 이 공격이 SMAUG-T에 실질적인 취약점이 될 수 있음이 나타났기에 $dGaussian_{\sigma}$에 대응책을 적용하여 이를 방지하고자 했다. 공개키 생성 과정에서 $dGaussian_{\sigma}$ 함수는 가우시안 오류 발생시 [-3, 3] 범위 내의 정수 중간 값을 생성한다. 양수 값과 음수 값 사이의 상당한 해밍 웨이트 차이로 인해 이러한 값이 두 세트로 구분된다. 이러한 구별과 선형 대수적 접근 방식을 사용하면 비밀 키를 복구하거나 후보를 줄일 수 있는 가능성이 있다.

이러한 공격을 방지하기 위한 대응책은 첫 번째로 마스킹 기법이 존재한다. 그러나 비선형 비트 연산이 있는 상황에서 효율적인 마스킹 기법을 설계하는 것은 어려울 수 있으며 상당한 오버헤드가 발생할 수 있다. 또 다른 대응책으로는 하이딩 기법이 있다. 현재 발견된 공격에는 키 생성 과정에서 계수를 분류하는 논리가 존재한다. 이는 어떤 계수가 어떤 세트에 속하는지 구별하기 어렵게 한다. 따라서 하이딩 기법이 마스킹 기법보다 효과적이며 SMAUG-T는 Fisher-Yates 셔플 알고리즘을 적용했다.

대응책을 적용했을 때의 오버헤드는 (표 3)과 같다. 오버헤드는 암호화 및 복호화 과정에서는 발생하지 않고 키 생성 과정에서만 발생한다. TLS와 같은 환경에서의 키 생성은 일반적으로 암호화보다 빈도가 낮

〔표 3〕 Results of the application of the countermeasure to clustering SCA in the $dGaussian_{\sigma}$ - Median cycle counts of 1000 executions.

Schemes	TiMER	SMAUG-T128	SMAUG-T192	SMAUG-T256
Original	70,348	70,398	136,436	231,824
Countermeasure	122,258	124,426	241,444	491,184
Overhead	76.7%	76.9%	111.8%	73.7%

으므로 이 대응책의 오버헤드는 암호화 과정에서 최소한의 영향을 미친다.

3.3. REDOG 알고리즘 동향

최근 진행된 2024 KpqC 윈터캠프 발표 자료에 따르면 T. Lange et al.는 메시지 복구 공격을 통해 REDOG의 보안이 알려진 것 보다 취약하다는 걸 입증 했다[25]. 이들은 REDOG의 부정확한 추정치가 부정확한 복호화를 야기한다고 했고, Hamming metric 기법을 이용해 메시지 복구 공격을 수행할 수 있음을 보였다. 이에 대한 해결 방법으로 떳떳 행렬 P^{-1}이 선택되는 공간을 변경하는 것을 제시하였다. 이후 떳떳 파라미터 값에 변화가 있었다. t값의 경우는 t값에서 t1과 t2로 분리 되었다.

〔표 4〕 REDOG 파라미터 변경점

Scheme	REDOG1	REDOG2	REDOG3
n	44 → 30	58 → 44	72 → 58
k	8 → 6	10 → 8	12 → 10
l	37 → 25	49 → 37	61 → 49
q	2	2	2
m	83 → 59	109 → 83	135 → 109
r	18 → 12	24 → 18	30 → 24
λ	3	3	3
t	6	8	10
t1	6	12	15
t2	2	2	3
Public Key (KB)	14.25 → 4.17	32.84 → 13.66	62.98 → 31.87
Secret Key (KB)	1.45 → 0.6	2.52 → 1.43	3.89 → 2.50
Ciphertext (KB)	0.83 → 0.38	1.44 → 0.82	2.23 → 1.44

3.4. MQ-Sign 알고리즘 동향

MQ-Sign는 네 가지 변형, SS, RS, SR, RR의 방법으로 비밀키를 선택하여 사용할 수 있도록 설계되어 있다. S는 Sparse 다항식을 R은 랜덤한 다항식을 나타내는 것으로 [26]에서 SS, RS에서 동치키를 사용하는 경우 비밀키를 복구할 수 있는 키 복구 공격이 발표되었다.

2라운드에서는 sparse 다항식 기반 키생성에 제안된 공격과 잠재적인 공격에 대응하기 위해 최종적으로 RR과 LR의 키생성 방법으로 수정되었다. MQ-Sign-LR은 F_V를 v개의 라인과 변수의 선형 조합으로 비밀키를 생성하여 F_V를 순환 행렬-벡터 곱으로 표현할 수 있게 된다. 이 구조로 LR의 비밀키는 RR에 비해 약 37% 줄어든다. 또한, LR은 서명 생성에서 시간이 많이 소요되는 F_V에 랜덤한 Vinegar 값의 대입하는 과정을 단 한 번의 순환 행렬-벡터 곱의 계산할 수 있도록 설계되어 LR의 키생성과 서명 생성 성능이 RR보다 약 30%에서 50%까지 향상된다. (표 5)는 MQ-Sign의 키길이와 서명 길이를 정리한 표이고, (표 6)은 AVX2 최적 구현에서 개선된 성능을 정리한 표이다.

MQ-Sign-RR에서 추가된 사항은 은 서명에 공개

〔표 5〕 Key, signature size of MQ-Sign (Unit: bytes)

Security level	1	3	5
MQ-Sign-RR			
Public key	328,505	1,238,825	2,893,025
Secret key	276,649	1,044,385	2,436,769
Signature	150	216	276
MQ-Sign-LR			
Public key	328,505	1,238,825	2,893,025
Secret key	160,881	601,249	1,400,113
Signature	150	216	276

〔표 6〕 Performance measurement result of MQ-Sign (Unit: clock cycles, median values)

Security level	1	3	5
MQ-Sign-RR AVX2-optimized			
KeyGen	9,454,708	40,250,626	102,775,550
Sign	90,480	268,866	524,030
Verify	50,460	185,086	363,611
MQ-Sign-LR AVX2-optimized			
KeyGen	5,451,597	25,605,484	67,485,424
Sign	65,300	168,684	360,636
Verify	51,744	191,986	381,019

키와 메시지를 묶어줄 수 있는 바인딩 기술을 사용하여 잠재적인 공격에 대한 안전성을 보장해 준다. 바인딩 방법은 서명 생성과 검증에서 H(M||r) 대신 H(M||r||H(P))을 사용하는 것이다.

3.5. AIMer 알고리즘 동향

최근 연구에서 [27, 28] AIM에 특정 대수적 취약점이 발견되었다. 가장 큰 공격은 Liu et. al.이 제시한 a Fast exhaustive search attack으로 AIM이 중간 수준의 Bool 변수에서 낮은 차수의 다항식 체계를 허용하는 것을 이용한 공격이다. 이를 통해 기존의 AIM의 완전 탐색 복잡도 분석과 비교하였을 때 최대 12bit까지의 잠재적인 보안 감소를 보여준다[29, 30].

이러한 공격을 완화하기 위해 새로운 AIM2를 제안하였다. AIM2는 기존의 AIM과 유사한 구조를 가지고 있지만, 더 높은 지수를 가진 역 Mersenne S-box 사용함으로써 중간 수준의 Bool 변수를 가진 낮은 차수의 다항식 체계를 구축하기 어렵게 만든다. 또한 각 S-box의 입력에 고유한 상수를 추가하여 모든 S-box에 공통 변수를 사용하는 다항식 체계를 구축하기 어렵게 하였다.

결과적으로 기존의 AIM 보다 성능에 영향 없이 최근에 AIM에 대한 공격에 대해서 더 강력한 보안을 제공하는 AIM2를 제안하였다.

3.6. HAETAE 알고리즘 동향

HAETAE 알고리즘은 KpqC 공모전뿐만 아니라 NIST(National Institute of Standards and Technology)에서 진행하고 있는 추가적인 PQC 전자서명 표준화 과정도 진행하고 있다. 추가 서명 PQC 표준화 과정은 2023년 7월 1라운드 암호 40개를 소개하였으며, HAETAE 알고리즘도 40개에 포함되어 표준화 과정에 참여하고 있다.

pqm4[1] 프로젝트는 위처럼 PQC 표준화 과정을 진행하고 있는 알고리즘을 포함하는 PQCRYPTO 프로젝트이다. pqm4 프로젝트는 ARM Cortex-M4를 대상으로 하는 PQC KEM 또는 전자서명 알고리즘 구현을 포함한 라이브러리, 벤치마킹 및 테스팅을 제공한다.

1) https://github.com/mupq/pqm4

pqm4는 구현된 암호 알고리즘에 대해서 벤치마킹을 통한 성능 결과를 공개하고 있다[31]. 공개된 성능 결과에는 HAETAE 알고리즘과 같은 격자 기반의 Dilithium과 HAWK 알고리즘더 포함되어 있다. HAETAE는 Dilithium에 비해 키 생성과 서명 과정의 속도가 느린 것을 확인할 수 있다. 하지만 Dilithium에 비해서 빠른 속도로 검증이 가능하다. 같은 추가 PQC 전자서명 표준화 과정에 1라운드를 진행하고 있는 HAWK 알고리즘과 비교하였을 때, HAETAE 알고리즘이 서명 과정에 약 9배 느린 성능을 보여주지만 키 생성과 검증 과정에서 약 11배, 1.2배 더 빠른 성능 결과를 보여준다.

3.7. NCC-Sign 알고리즘 동향

NCC-Sign은 2라운드에서 Non-cyclotomic 버전은 LWE 문제와 SIS문제의 복잡도의 균형을 맞춘 새로운 파라미터를 제시하였고, Trinomial 버전은 기존의 모듈러스를 2의 멱승으로 사용하는 파라미터를 NTT 연산을 사용할 수 있는 파라미터로 변경하였다.

Non-cyclotomic 버전은 NTT를 이용할 수 없지만 NTT를 사용할 수 있는 큰 다항식 링으로 임베딩을 시켜 NTT를 수행하는 방법으로 구현하였고, Trinomial 버전은 NTT 연산을 이용하여 Non-cyclotomic 버전 보다 효율적이다. Trinomial 버전은 강한 안전성 확보를 위해 Dilithium보다 더 큰 파라미터를 사용하고 있지만, 참조 구현은 Dilithium 보다 빠른 결과를 보였다. 그러나, AVX2 최적 구현은 Dilithium보다 느린 상황이다. Dilithium은 AVX2 최적 구현에서 모듈 구조를 이용한 SHAKE 최적화와

〔표 7〕 Performance measurement result of NCC-Sign Trinomial (Unit: clock cycles, median values)

Security level	1	3	5
NCC-Sign Trinomial Reference			
KeyGen	240,496	324,140	488,168
Sign	616,746	1,245,144	1,781,784
Verify	339,698	460,808	722,320
NCC-Sign Trinomial AVX2-optimized			
KeyGen	175,692	235,426	353,822
Sign	304,684	590,212	885,536
Verify	176,644	226,734	365,292

NTT 연산의 최적화로 크게 속도가 향상되었지만, 그 최적화 기법이 NCC-Sign에는 적용하기 어려운 구조이다. 그렇지만 AVX2 최적 구현, 특히 NTT 최적화의 경우에는 개선의 여지가 있다고 판단되고 있다. (표 7)은 NCC-Sign Trinomial의 레퍼런스 구현과 AVX2 최적 구현에서 개선된 성능을 정리한 표이다.

Ⅳ. 결 론

본 논문에서는 국내에서 진행중인 KpqC 공모전의 2라운드 후보 알고리즘에 대해 살펴보았다. 현재 2라운드에서는 격자, 코드, 다항식 그리고 영지식과 같은 다양한 기반의 알고리즘이 선정되어 2라운드를 진행하고 있다. 알고리즘의 개발 과정에서 발견된 취약점을 빠르게 보완하고 알고리즘의 수정을 통해 효율적이고 안전한 알고리즘이 개발되고 있으며, NIST PQC에서 선정된 Kyber, Dilithium과 같은 효율적이고 안전한 알고리즘과 비교하였을 때에도 성능적인 부분과 효율성 측면에서 비슷한 수준을 보여주는 알고리즘도 개발되고 있는 것을 확인할 수 있다. 현재 KpqC 공모전은 2라운드를 진행하고 있으며, 최종 선정 알고리즘은 2024년 말에 공개될 예정이다.

참 고 문 헌

[1] Shor, Peter W. “Algorithms for quantum computation: discrete logarithms and factoring.” Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994.

[2] Knuth, Donald E. “Postscript about NP-hard problems”, ACM SIGACT News 6.2. 15-16, 1974.

[3] Hoffstein, Jeffery. “NTRU: a new high speed public key cryptosystem”, presented at the rump session of Crypto 96, 1996.

[4] J. H. Kim, and J. H. Park. “NTRU+: compact construction of NTRU using simple encoding method”, IEEE Transactions on Information Forensics and Security, 2023.

[5] 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

[6] J. H. Cheon, et al. “Lizard: Cut off the tail! A practical post-quantum public-key encryption from LWE and LWR” International Conference on Security and Cryptography for Networks. Cham: Springer International Publishing, pp. 160-177, 2018.

[7] J. H. Lee, et al. “RLizard: Post-quantum key encapsulation mechanism for IoT devices”, IEEE Access 7, 2080-2091, 2018.

[8] McEliece, Robert J. “A public-key cryptosystem based on algebraic.” Coding Thv 4244 (1978): 114-116. 1978.

[9] Official Comments-McNie, read official comments on McNie dated Dec 24, 2017 and (Dec. 26, 2017). available at: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/McNie-official-comment.pdf

[10] P. Gaborit, L. Galvez, A. Hauteville, J. L. Kim, M.J. Kim, Y. S. Kim, “Dual-Ouroboros: an improvement of the McNie scheme.” Adv. Math. Commun. 2019.

[11] J. L. Kim, et al. “A modified Dual-Ouroboros public-key encryption using Gabidulin codes.” Applicable Algebra in Engineering, Communication and Computing 32.2 (2021): 147-156. 2021.

[12] J. L. Kim, et al. “REDOG and its performance analysis.” Cryptology ePrint Archive(2022).

[13] D. C. Kim, et al. “PALOMA: binary separable Goppa-based KEM.” Code-Based Cryptography Workshop. Cham: Springer Nature Switzerland, 2023.

[14] A. Kipnis, J. Patarin, and L. Goubin. “Unbalanced Oil and Vinegar signature schemes”, Advances in Cryptology, CRYPTO'99, LNCS 1592, pp. 206-222, 1999.

[15] 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.

[16] I. Yuval, K. Eyal, O. Rafail and S. Amit. "Zero-knowledge from secure Multiparty Computation", In ACM STOC 2007, pp. 21-30, 2007.

[17] K. Daniel and Z Greg. "Efficient Lifting for Shorter Zero-Knowledge Proofs and Post-Quantum Signatures", Cryptology ePrintArchive, Paper 2022/588, 2022. https://eprint.iacr.org/2022/588.

[18] 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

[19] L. Vadim. "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures" In Mitsuru Matsui, editor, ASIACRYPT 2009, volume 5912 of LNCS, pages 598-616. Springer, Heidelberg, December 2009. doi:10.1007/978-3-642-10366-7_35.

[20] L. Vadim. "Lattice Signatures without Trapdoors" In David Pointcheval and Thomas Johansson, editors, EUROCRYPT 2012, volume 7237 of LNCS, pages 738-755. Springer, Heidelberg, April 2012. doi: 10.1007/978-3-642-29011-4_43.

[21] L. Ducas, et al. "Crystals-dilithium: A lattice-based digital signature scheme", IACR Transactions on Cryptographic Hardware and Embedded Systems(2018): 238-268, 2018. doi: https://doi.org/10.13154/tches.v2018.i1.238-268

[22] 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).

[23] 2024 KpqC Winter Camp, 2024. available at: https://kpqc.or.kr/contents/02_notice/board.html?board_id=board_notice&mode=view&no=58&cate=%EA%B5%90%EC%9C%A1

[24] Fujisaki, Eiichiro, and T. Okamoto. "How to enhance the security of public-key encryption at minimum cost." International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 53-68, 1999.

[25] Lange, Tanja, Alex Pellegrini, and Alberto Ravagnani. "On the security of REDOG." Cryptology ePrint Archive (2023).

[26] Aulbach, Thomas, Simona Samardjiska, and Monika Trimoska. "Practical key-recovery attack on MQ-Sign." Cryptology ePrint Archive(2023).

[28] F. K. Liu, M. Mahzoun, M. Øygarden, and W. Meier. "Algebraic Attacks on RAIN and AIM Using Equivalent Representa- tions", IACR Transactions on Symmetric Cryptology, 2023(4):166-186, Dec. 2023.

[29] K. Zhang, Q. Wang, Y. Yu, C. Guo, and H. Cui. "Algebraic Attacks on Round-Reduced Rain and Full AIM-III. In Jian Guo and Ron Steinfeld", editors, ASIACRYPT 2023, pages 285-310. Springer, 2023.

[30] S. K. Kim, J. C. Ha, M. C. Son, and B. H. Lee. "Efficacy and Mitigation of the Cryptanalysis on AIM", Cryptology ePrint Archive, Paper 2023/1474, 2024. https://eprint.iacr.org/2023/1474.

[31] J. Y Lee, et al. "The AIMer Signature Scheme-Submission to the KpqC Competition Version 2.0", Submission to KpqC Competition Round 2, 2024. available at https://aimer-signature.org/docs/AIMer-specification-v2.0.pdf

[32] Kannwischer, Matthias J., et al. "pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers" Cryptology ePrint Archive, 2024.

〈저자소개〉

엄 시 우 (Si-Woo Eum)

학생회원

2021년 2월 : 한성대학교 IT융합공학부 학사 졸업
2023년 2월 : 한성대학교 IT융합공학부 석사 졸업
2023년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 암호구현, 정보보안

송 민 호 (Min-Ho Song)

학생회원

2023년 2월 : 한성대학교 IT융합공학부 졸업
2023년 3월~현재 : 한성대학교 융합보안학과 석사과정
<관심분야> 암호구현, 정보보안

김 상 원 (Sang-Won Kim)

학생회원

2023년 8월 : 한성대학교 컴퓨터공학부 졸업
2023년 9월~현재 : 한성대학교 융합보안학과 석사과정
<관심분야> 암호구현, 정보보안

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
2017년 4월~2023년 2월 : 한성대학교 IT융합공학부 조교수
2023년 3월~현재 : 한성대학교 융합보안학과 부교수
<관심분야> 정보보안, 암호구현