정 보 보 호 학 회 지
제34권 제2호, 2024. 4

NIST PQC Additional Digital Signature Scheme 최신 동향

심 민 주*, 송 경 주*, 이 민 우**, 서 화 정***

요 약

양자컴퓨터의 급속한 발전으로 인해 현재 사용되는 암호화 알고리즘들은 위협에 직면해 있다. 이를 대비하여 양자컴퓨터로부터 안전한 양자내성암호 알고리즘을 개발하기 위해 미국 NIST에서는 양자내성암호 표준화 공모전을 개최하여 최근 4개의 표준화 알고리즘이 선정되었다. NIST는 다양성을 위해 다른 기반 문제를 갖는 알고리즘 선정을 위해서 현재 4라운드를 진행하고 있다. 하지만 4라운드 후보군 알고리즘은 모두 공개키 알고리즘이 선정되어 전자서명 알고리즘에 대한 후보군 알고리즘은 존재하지 않아 NIST는 2023년 PQC 전자서명 추가 공모전을 개최하였다. 따라서 본 논문에서는 NIST PQC 전자서명 추가 공모전에 대해 소개하고, 1라운드에 진출한 알고리즘의 특징과 최신 동향을 살펴본다.

Ⅰ. 서 론

양자컴퓨터의 발전에 따라 Legacy 암호화 체계가 많은 위협을 받고 있다. 1994년 Peter Shor가 제안한 알고리즘은 이산로그, 인수분해 등 기존 공개키 암호의 기반 문제를 이론적으로 해결할 수 있으며, 1996년 Lov Grover가 제안한 알고리즘은 대칭키 암호에 대한 무작위 공격을 가속화 할 수 있다[1, 2]. 이에 따라 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 양자컴퓨터 상에서의 암호화 시스템에 대한 위협에 대응하기 위해 양자 내성암호를 선정하기 위한 공모전을 개최하였다. 2022년 4개의 표준화 알고리즘이 선정되었고, 현재 표준화로 선정된 알고리즘과는 다른 기반 문제를 갖는 공개키 암호 알고리즘들을 대상으로 4라운드가 진행되고 있다. 하지만 전자 서명 알고리즘에 대한 후보군 알고리즘은 존재하지 않아 NIST는 2023년 NIST PQC 전자서명 추가 공모전을 진행하고 있다.

본 논문에서는 NIST PQC 전자서명 추가 공모전에 대한 최신 동향을 살펴본다. 본 논문의 구성은 다음과 같다. 2장에서 NIST 양자내성암호 표준화 공모전에 대해서 살펴보고 3장에서 NIST 양자내성암호 전자서명 표준화 추가 공모전과 1라운드 후보군 알고리즘 특징에 대해 소개한다. 4장에서는 양자내성암호 전자서명 표준화 추가 공모전 1라운드에 진출한 알고리즘에 대해 ARM Cortex-M4 상에서의 적합성과 성능을 분석한 연구 동향을 확인한다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

Ⅱ. NIST 양자내성암호 표준화 공모전

2016년 NIST는 양자 컴퓨터 시대에 대비하여 양자내성암호 표준화 공모전에 대한 소개를 진행했다[3]. 이 공모전은 기존의 이산대수 문제가 아닌 새로운 수학적 난제를 바탕으로 한 암호화 방법을 찾는 것을 목표로 한다[4]. 공모전의 주요 요구사항 중 하나는 최소 보안 레벨이 exhaustive key search 관점에서 AES-128, AES-192, AES-256의 보안성을 만족시켜야 하는 것이다. SHA-256 또는 SHA-384에서의 collision search 관점에서의 보안성도 충족해야 한다.

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 정보통신기술진흥-센터의 지원을 받아 수행된 연구임 (No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천기술 연구, 50%).

* 한성대학교 정보컴퓨터공학과 (대학원생, minjoos9797@gmail.com, thdrudwn98@gmail.com)
** 한성대학교 융합보안학과 (대학원생, minunejip@gmail.com)
*** 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

또한 고성능 양자내성 알고리즘은 연산 속도나 메모리 요구사항이 높아질 수 있으므로, 구현 비용과 성능 최적화도 중요한 평가 기준이 된다.

NIST는 안전하면서도 실용적인 구현을 요구했다. 이는 각 플랫폼마다 제공하는 컴퓨팅 자원량이 다르기 때문이다. 컴퓨팅 자원을 많이 요구하는 알고리즘은 자원이 부족한 플랫폼에서 실행이 불가능할 수 있다. 알고리즘의 확장성도 중요하다. 플랫폼 의존성 없이 효율적으로 실행될 수 있는 알고리즘이 필요하며, 특정 명령어 집합을 사용하는 알고리즘은 일부 플랫폼에서 실행 불가능할 수 있다.

NIST의 양자내성암호 공모전 추진 경과는 다음과 같다. 2017년 1차 후보로 69개 알고리즘을 선정하고, 이후 보안, 비용, 성능, 특성, 확장성을 기준으로 평가했다. 2019년에는 26개 알고리즘을 2차 후보로 발표했으며, 여기에는 공개키 알고리즘 17개와 전자서명 알고리즘 9개가 포함됐다. 이 알고리즘들은 이전 단계의 취약점을 개선해 제출됐다. 2020년 3차에서는 최종적으로 7개 알고리즘을 선정했고, 추가 후보로 8개 알고리즘을 포함했다.

2022년 6월, NIST는 양자 내성 암호 표준의 최종 선정 결과를 공개했다[5]. 공개키 부문에서 CRYSTALS-KYBER가 선택되었고, 전자서명 분야에서는 CRYSTALS-Dilithium, FALCON, SPHINCS+가 선정되었다. 수학적 기반이 부족한 공개키 알고리즘을 개선하기 위해 4차 라운드가 진행 중이며, BIKE, Classic McEliece, HQC가 후보로 올라 있다. SIKE는 4차 라운드에 올랐으나 보안상의 문제가 발견되어 탈락했다[6].

2023년 8월 24일, NIST는 양자 내성 암호 표준 초안을 발표했다. 실제 선정된 양자내성암호 표준은 총 4종이지만, NIST는 연방 정보 처리 표준(Federal Information Processing Standards, FIPS) 초안 3종을 우선 공개했다. 초안에는 PKE/KEM(Public Key Encapsulation/Key Encapsulation Mechanisms)인 Crystals-Kyber와 전자서명 알고리즘인 Crystals-Dilithium 및 SPHINCS+가 포함된다. 표준 초안은 FIPS 문서로 통합되며, Crystals-Kyber, Crystals-Dilithium, SPHINCS+가 각각 FIPS-203, FIPS-204, FIPS-205에 해당한다. 이 문서들은 알고리즘의 구조, 모듈, 매개변수 등에 대해 설명하고, 암호화 및 서명 과정의 의사코드를 포함한다. FIPS 표준은 호환성을 보장하며, NIST는 이 초안을 바탕으로 지속적인 개선을 예정하고 있다.

Ⅲ. NIST 양자내성암호 전자서명 표준화 추가 공모전

3.1. NIST 양자내성암호 전자서명 표준화 추가 공모전

2022년 9월, NIST는 양자내성암호 전자서명 표준화 추가 공모전을 소개하였다[7]. 2023년 6월에 50개의 서명 알고리즘이 제출되었고, 2023년 7월 40개의 후보군 알고리즘이 1라운드에 진출하였다[8]. 격자 기반 알고리즘이 아닌 다양한 기반 알고리즘이 채택되었고, CRYSTALS-Dilithium과 FALCON보다 성능이 우수하고 높은 보안성을 갖는 격자 기반 알고리즘도 선정되었다.

3.2. Code-based Signatures

Code-based Signature 로는 1라운드에 총 6개의 알고리즘 CROSS[9], Enhanced pqsigRM[10], FuLeeca[11], LESS[12], MEDS[13], Wave[14]가 진출하였다.

- CROSS: Restricted Syndrome Decoding Problem (R-SDP)를 기반으로 한다. Fiat-Shamir 변환을 사용하여 interactive zero-knowledge Identification 프로토콜을 서명 체계로 변환하였다. 서명이 간결하고 공개키가 크기가 작다.
- Enhanced pqsigRM: NIST PQC 표준화 공모전에 제출된 알고리즘인 pqsigRM[15]을 개선한 modified Reed-Muller(RM) 코드 기반 서명 알고리즘이다. 작은 서명 크기를 지니고 있고 검증이 빠르다.
- FuLeeca: quasi-cyclic Lee-Metric 코드를 기반으로 한다. FALCON 보다는 성능이 뛰어나고 공개키+서명의 크기는 FALCON보다 조금 크고 Dilithium과 SPHINCS+보다는 작다.
- LESS: Zero-Knowledge identification에 Fiat-Shamir 변환을 적용하였고, Linear Equivalence Problem (LEP)을 기반으로 하는 Sigma 프로토콜을 사용한다. 공개키 크기와 서명 크기가 작다.

- MEDS: 서로 다른 2개의 동등한 matrix rank-metric 코드 간에 isometry를 찾는 Matrix Code Equivalence(MCE) 문제의 어려움에 기반한다 [16]. 공개키와 서명 크기를 유연하게 조절할 수 있는 매개변수를 제공한다.
- Wave: Gentry, Perikert, Vaikuntanathan의 프레임워크[17]를 이론적 기반으로 한다. 보안은 Decoding Problem(DP)의 어려움에 서명 길이는 짧고 검증 속도는 빠르지만, 공개키 크기는 크다.

3.3. Isogeny Signature

Isogeny Signature 로는 1라운드에 총 1개의 알고리즘 SQIsign[18]이 제출되었다.

- SQlsign: PQC 표준 서명 방식 중 공개 키 및 서명 크기의 합이 가장 작으며 검증이 빠르지만 서명 속도가 느리다.

3.4. Lattice-based Signatures

Lattice-based Signature 로는 1라운드에 총 7개의 알고리즘 EagleSign[19], EHTv3 and EHTv4[20], HAETAE[21], HAWK[22], HuFu[23], Raccoon[24], SQUIRRELS[25]이 제출되었다.

- EagleSign: MLWE 및 MNTRU 문제를 기반으로 하여 빠르고 심플하게 구현된 격자기반 알고리즘으로 두 가지 변형 알고리즘을 가진다. Dilithium 보다 서명이 최대 2배 빠르고 키 생성이 최대 1.5배 빠르다.
- EHTv3 and EHTv4: EHTv3, EHTv4 모두 보안 수준을 높이기 위한 매개변수 선택이 유연하며 서명 길이가 짧다. 하지만 EHTv4와 달리 EHTv3의 공개키 크기가 크다.
- HAETAE: LWE 및 SIS를 기반으로하며 서명 크기가 Dilithium 보다 30~40% 작고 검증 키 크기가 20~25% 작다. 전체 서명 프로세스는 고정 소수점 연산으로 구현할 수 있다.
- HAWK: isomorphism problem (LIP) 기반으로하여 서명 생성 및 검증이 빠르며 키 크기 및 서명 크기가 다소 작으며 메모리 공간이 작다. 부동 소수점 연산이 포함되지 않아 FPU 장치 없이 동작이 가능하다.
- HuFu: SIS 및 LWE 문제를 기반으로하여 비용이 많이 드는 서명 작업을 오프라인 단계에서 수행할 수 있으며 온라인에서 진행할 작업은 모두 정수로 이뤄져 간단하고 빠르다. 서명 크기는 Dilithium과 비슷하지만 서명 및 검증이 보다 빠르다.
- Raccoon: Fiat-Shamir paradigm을 기반으로 한 격자 기반 서명체계이다. 마스킹이 용이하며 균일 분포 기반의 오류 분포를 가지면서 모듈러스가 쉽게 분할되어 이식성이 좋다. 하지만 서명 크기가 Dilithium 보다 상당히 크며 검증 키 크기는 유사하다.
- SQUIRRELS: Unstructured co-cyclic lattice를 기반으로 한다. Falcon 및 Dilithium과 유사한 서명 크기를 가지며 서명 생성 및 검증 측면에서 높은 효율성을 보인다. 서명 검증에서 해시 연산과 단일 선형 방정식의 검증으로 구성되어 검증 절차를 간소화 한다.

3.5. MPC-in-the-head Signatures

Multi-Party Computation-in-the-Head (MPCitH) Signatures 로는 1라운드에 총 7개의 알고리즘 Bitcuit[26], MIRA[27], MiRitH[28], MQOM[29], PERK[30], RYDE[31], SDitH[32]가 진출하였다.

- Bitcuit: NIST PQC 표준화 공모전에 제출된 알고리즘인 MQDSS[33]와 Picnic[34]과 연관되어 있고, PowAff2라는 정의한 문제를 기반으로 한다. 특히 Picnic의 MPC 기술을 접근 방식으로 채용하였다. EUF-CMA 보안을 달성하며, SPINCS+보다 작고 Dilithium과 비교 가능한 공개키와 서명 크기를 갖는다.
- MIRA: MinRank 문제와 MPCitH에 기반한 서명 프로토콜로 대칭 함수와 zero-knowledge 증명을 기초로 한다. [35]의 hypercube 구조 기법과 [36]의 linearized polynomial을 사용하는 MPC 프로토콜을 활용한다. 공개키 크기가 작아 NIST 보안 레벨 1 일 때 공개키+서명의 크기는 Dilithium보다 2배 작다.

- MiRitH: MinRank 문제의 난이도를 기반으로 하고 Fiat-Shamir 변환을 통한 ZKPoK(Zero-Knowledge Proof of Knowledge)에서 구성된다. 유한체 상의 작은 행렬에 대한 선형대수 계산을 사용하기 때문에 최적화 하기 쉽다. 서명 크기가 작고 Ring 서명 스킴으로 쉽게 확장이 가능하다.
- MQOM: MPCitH를 MQ(Multivariate Quadratic) 문제에 적용하여 설계되었고, Seed trees[37]와 hypercube를 사용하여 MPCitH 변환을 개선하였다. 공개키 크기가 작고 서명의 크기도 상대적으로 작다.
- PERK: 변형된 Permuted Kernel Problem(PKP)을 기반으로 하는 zero-knowledge 시스템을 기반으로 구축되었다. 공개키와 비밀키 크기가 매우 작고 PKP와 r-PKP 공격에 Resilience를 갖는다.
- RYDE: 대칭 함수에 기반으로 하며, 서명의 보안은 Rank Syndrome Decoding 문제에 기반한다. 공개키+서명의 크기가 작으며 Rank-SD 공격에 대해 Resilience를 갖는다.
- SDitH: 유한체 상의 임의의 linear codes에 대한 Syndrome Decoding(SD) 문제에 기반한다. 높은 보안성을 제공하고 매개변수 조절이 유연하다. 서명, 공개키, 개인키의 크기가 작다.

3.6. Multivariate Signatures

Multivariate Signature 로는 1라운드에 총 10개의 알고리즘 3WISE[38], DME-Sign[39], HPPC[40], MAYO[41], PROV[42], QR-UOV[43], SNOVA[44], TUOV[45], UOV[46], VOX[47]가 제출되었다.

- 3WISE: 벡터의 각 요소에 대해 세제곱 곱셈 연산을 수행하고, 이를 기반으로 보안성을 제공한다. 그러나 NIST는 해당 방식이 MinRank 공격에 취약한 문제가 있다고 밝혔다[48].
- DME-Sign: 결정론적 트랩도어 순열을 핵심으로 하는 알고리즘으로, 공개키 암호 시스템인 DME[49]에 기반한다. 서명 크기가 32~64bytes로 매우 작은 특징을 보인다.
- HPPC: 고차 대수방정식을 기반으로 하는 HFE를 사용하며, 큰 차수의 개인 다항식을 사용하여 보안성을 제공한다. 서명 크기는 21~33bytes로 매우 작으나, 공개키 및 개인키의 크기가 Dilithium보다 매우 큰 특징을 보인다.
- MAYO: Oil and Vinegar 스킴의 변형으로, 공개키 크기를 줄이는데 주력했다. Dilithium보다 15~25% 작은 공개키 크기를 보인다.
- PROV: UOV(Unbalanced Oil and Vinegar) 스킴을 기반으로 한다. 공개키 크기가 매우 크나, 비밀키과 서명의 크기가 작으며, 비밀키의 경우 SPHINCS+의 절반의 크기를 지닌다.
- QR-UOV: UOV 스킴을 기반으로 하며, 대수 구조를 활용하여 공개키의 크기를 줄이는데 집중하였다. 타 UOV 기반 알고리즘보다 공개키의 크기가 작은 경향을 보이나, Dilithium보다는 매우 큰 크기를 지닌다.
- SNOVA: noncommutative-ring을 기반으로 하며, NOVA[50]의 간소화된 버전이다. 공개키의 크기를 줄이는데 집중하였으며, 보안레벨 5에서 UOV 기반 알고리즘 중 가장 작은 공개키 크기를 지닌다.
- TUOV: UOV 스킴을 기반으로 한다. 보안 레벨 1에서 Dilithium 및 FALCON보다 서명 크기가 작고, 서명 생성 속도와 검증 속도 또한 빠르다. 그러나 타 UOV 기반 알고리즘보다 공개키의 크기가 큰 특징을 보인다.
- UOV: 1999년에 처음 제안된 알고리즘으로, 다변수 이차 방정식 시스템에 트랩도어를 포함시켜 보안성을 제공한다. 서명 생성과 검증 속도가 빠르나, 공개키의 크기가 매우 커 일반적인 용도로 사용하기는 부적합한 특징을 보인다.
- VOX: UOV 스킴을 기반으로 하며, 공개키의 크기를 줄이는데 집중하였다. 타 UOV 기반 알고리즘들 보다 보안레벨 1,3에서 가장 작은 공개키 크기를 지닌다.

3.7. Symmetric-based Signatures

Symmetric-based Signature 로는 1라운드에 총 4개의 알고리즘 AIMer[51], Ascon-Sign[52], FAEST[53], SPHINCS-alpha[54] 가 제출되었다.

- AIMer: MPCitH 기반 알고리즘으로, BN++ 시스템에 적용 가능한 단방향 함수 AIM과 영지식 증

명 시스템으로 구성된다. 작은 공개키와 비밀키 크기를 지니나, 상대적으로 큰 서명 크기와 서명 생성 및 검증 시간을 지닌다.

- Ascon-Sign: ASCON[55]을 사용하여 SPHINCS+를 변형하였다. AEAD와 해싱 기능을 제공하며, 리소스가 제한된 환경을 타겟으로 한다.
- FAEST: 영지식 증명 시스템인 VOLEitH와 정보이론적 증명 시스템인 QuickSilver를 통합하였고, Fiat-Shamir 변환을 사용한다. SPHINCS+보다 50~70% 작은 서명 크기를 지니나, 검증 속도가 약간 느린 경향을 보인다.
- SPHINCS-alpha: SPHINCS+를 기반으로 하였으며, 매개 변수를 재조절하여 서명 크기를 줄였다. SPHINCS+에 비해 서명 크기가 8~12% 감소하였고, 성능을 2~16% 향상시켰다.

3.8. Other Signatures

Other Signature 들은 다양한 기반 문제를 바탕으로 하는 알고리즘들을 의미하며 1라운드에 총 5개의 알고리즘 ALTEQ[56], eMLE-Sig 2.0[57], KAZ-SIGN[58], Preon[59], Xifrat1-Sign.I[60]이 제출되었다.

- ALTEQ: ATFE(Alternating Trilinear Form Equivalence) 문제를 기반으로 하는 서명 알고리즘이다. 격자기반 알고리즘에 비해 느린 속도를 가지며 공개 키 및 서명 크기가 크다.
- eMLE-Sig 2.0: Embedded Multilayer Equations (eMLE) 문제의 새로운 버전을 기반으로 하며 공개 키와 서명 크기의 합이 NIST 표준 서명 체계보다 작다.
- KAZ-SIGN: 2-DLP (Second Order Discrete Logarithm Problem) 문제를 기반으로 하며 키 크기가 작고 속도가 빠르다.
- Preon: zk-SNARK 기반 서명 체계이며 범용 증명 시스템을 통해 그룹 서명, 속성과 같은 체계를 최소 비용으로 구축할 수 있다. Dilithium과 비교하여 속도가 빠르며 서명 및 공개 키, 개인 키 사이즈가 작다.
- Xifrat1-Sign.I: 무작위로 생성된 16개 요소의 abelian quasigroup을 기반으로 하며 서명 크기 및 공개 키, 개인 키 크기가 작고 핵심 연산이 상수 시간 내에 수행된다.

Ⅳ. NIST 양자내성암호 전자서명 표준화 추가 공모전 최신 동향

2024년 Matthias et al.은 NIST PQC 전자서명 알고리즘 추가 공모전 후보 알고리즘들에 대해 ARM Cortex-M4 마이크로컨트롤러에서의 적합성과 성능을 분석한 논문을 발표하였다[61]. 논문에서 수행한 분석에서 사용한 타겟 보드는 640-KiByte RAM을 가지는 STM32L4R5ZI이다. 해당 보드는 2017년에 출시된 STM32L4+ Series 중 하나이며 2-MByte Flash memory, 최대 120MHz 주파수, 암호화 가속기 엔진(AES, HASH)을 제공한다. pqm4 벤치마킹 프레임워크에 15개의 reference 구현과 5개의 M4 최적화 구현을 하였고, STM32L4R5ZI에서의 성능 평가를 제시하였다. NIST PQC 전자서명 알고리즘 추가 공모전 후보 알고리즘은 총 40개의 알고리즘이 1라운드 후보군 알고리즘으로 선정되었지만 15개의 알고리즘에 대해서만 구현을 진행한 이유는 공개적으로 심각한 취약점이 발견되거나 공개키의 크기가 타겟 보드의 RAM 사이즈인 640KB 이상의 메모리를 사용하는 경우, 또는 Cortex-M4에 포팅하기 어려운 코드를 사용하거나 Cortex-M4와 호환되지 않는 외부 종속성 및 동적 메모리 할당을 사용한 경우의 알고리즘 등이 제외되었다. [표 1]은 pqm4에서 측정한 Nucleo-L4R5ZI 상에 포팅된 알고리즘(clean ver)에서 가장 작은 파라미터 기준 성능을 보여준다.

〔표 1〕 pqm4 측정 성능(unit :thousands of cycles)

Scheme	KeyGen	Verify	Sign
aimer-l1 -param1	393	31,112	32,386
perk-128 -fast-3	698	96,371	217,643
cross-sha3-r -sdp-1-fast	968	30,641	58,864
biscuit128f	1,055	254,371	274,072
mirith_Ia_fast	1,304	276,068	296,733
dilithium2	1,874	2,062	7,283
cross-sha2-r -sdp-1-fast	5,615	142,974	216,566
mqom_cat1 _gf251_fast	7,790	136,748	149,074

Scheme	KeyGen	Verify	Sign
mayo1	7,977	6,294	18,005
haetae2	9,265	1,154	32,068
hawk256	16,846	628	1,116
snova-24-5 -16-4-esk	24,841	88,454	139,248
sphincs-a -sha2-128f	30,279	35,696	382,271
meds13220	47,801	1,766,410	1,773,022
ascon-sign -128f-simple	69,377	96,768	1,629,111
ov-Ip	350,784	1,301	6,479

Ⅴ. 결 론

양자 컴퓨터 시대를 대비하여 양자컴퓨터에서도 안전한 양자내성암호에 대한 표준을 선정하기 위해 NIST에서는 꾸준히 공모전을 진행해오고 있다. 현재 4개의 표준화 알고리즘이 선정되었으며, 다양성을 위해 다른 기반 문제의 알고리즘들을 대상으로 NIST PQC 표준화 4라운드가 진행되고 있다. 하지만 4라운드 후보군 알고리즘에 전자서명 알고리즘은 제외되었다. 이에 따라 NIST는 PQC 전자서명 표준화 추가 공모전을 개최하였다. 따라서 본 논문에서는 NIST PQC 전자서명 표준화 추가 공모전에 대해 소개하고, 1라운드 선정된 알고리즘의 특징에 대해 살펴보았다. 그리고 양자내성암호 전자서명 표준화 추가 공모전 1라운드에 진출한 알고리즘에 대해 ARM Cortex-M4 상에서의 적합성과 성능을 분석한 연구를 확인하였다. 결과적으로 현재 양자내성암호 표준화 알고리즘이나 4라운드 후보군 알고리즘에 대한 연구가 활발히 이뤄지고 있는 것처럼 전자서명 표준화 추가 공모전 후보군 알고리즘에 대해서도 많은 연구가 필요하다.

참 고 문 헌

[1] Shor, P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM review, 41(2), pp. 303-332, 1999.

[2] Grover, L. K., "A fast quantum mechanical algorithm for database search," In Proceedings of the twenty- eighth annual ACM symposium on Theory of computing, pp. 212-219, 1996.

[3] K. B. Jang, and H. J. Seo, “Quantum Computer and Standardization trend of NIST Post-Quantum Cryptography,” Proceedings of the Korea Information Processing Society Conference, 26(1), pp. 129-132, 2019.

[4] H. D. Kwon, M. J. Sim, K. J. Song.M. W. Lee, and H. J. Seo, “NIST PQC 벤치마크 플랫폼 최신 동향,” 정보보호학회지, 33(2), 69-77, 2023.

[5] NIST, “Selected Algorithms 2022,” Online: https://csrc.nist.gov/Project s/post-quantum-cryptography/selected-algorithms-2022, 2022

[6] NIST, “Round 4 Submissions,” Online: https://csrc.nist.gov/Project s/post-quantum-cryptography/round-4-submissions, 2022.

[7] NIST, “Request for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process ,” Online: https://csrc.nist.gov/News/2022/request-additional-pqc-digital-signature-schemes, 2022

[8] NIST, “Round 1 Submissions,” Online : https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures, 2023

[9] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/ Projects/pqc-dig-sig/documents/round-1/spec-files/CROSS-spec-web.pdf, 2023

[10] J.K. Cho, J.S. No, Y.W. Lee, Y.S. Kim, and Z.H. Koo, “Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature and FastVerification for Post-Quantum Cryptography,” Cryptology ePrint Archive, 2022.

[11] S. Ritterhoff, G. Maringer, S. Bitzer, V. Weger, P. Karl, T. Schamberger, J. Schupp, and A. Wachter-Zeh, “FuLeeca: A-Lee-based Signatures Scheme,” Cryptology ePrint Archive, 2023.

[12] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/me dia/Projects/pqc-dig-sig/documents/round-1/spec-files/less-spec-web.pdf, 2023

[13] MEDS-PQC, “Matrix Equivalence Digital Signature,” Online: https://www .meds-pqc.org/spec/M EDS-2023-07-26.pdf, 2023.

[14] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/r

ound-1/spec-files/wave-spec-web.pdf, 2023.

[15] W. Lee, Y. S. Kim, Y. W. Lee, and J. S. No, ”Post quantum signature scheme based on modified Reed‐Muller code pqsigRM,” in First Round Submission to the NIST Postquantum Cryptography Call, Nov. 2017.

[16] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska, “Take yourMEDS: Digital Signatures from Matrix Code Equivalence,” In AFRICACRYPT 2023,LNCS.

[17] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and newcryptographic constructions. In Proceedings of the fortieth annual ACM symposium on Theoryof computing, pages 197‐206. ACM, 2008.

[18] Chavez-Saab, J., Santos, M.C.R., De Feo, L., Eriksen, J.K., Hess, B., Kohel, D., Leroux, A., Longa, P., Meyer, M., Panny, L. and Patranabis, S., “SQIsign algorithm specifications and supporting documentation”. Project Homepage, Jun 2023.

[19] Hounkpevi, Abiodoun Clement, Sidoine Djimnaibeye, and Michel Seck. "Eaglesign: A new post-quantum elgamal-like signature over lattices." Submission to the NIST’s post-quantum cryptography standardization process 2023.

[20] Semaev, Igor, Auxiliary Submitter, and Martin Feussner. “DIGITAL SIGNATURE ALGORITHMS EHTV3 AND EHTV4” SUBMISSION TO NIST PQC.

[21] Chen, Cong, Oussama Danba, Jeffrey Hoffstein, Andreas Hülsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, and Zhenfei Zhang. "Algorithm specifications and supporting documentation." Brown University and Onboard security company, Wilmington USA Mar, 2019.

[22] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles and Wessel van Woerden, “HAWK version 1.0”,

[23] Yu, Yang, Huiwen Jia, Leibo Li, Delong Ran, Zhiyuan Qiu, Shiduo Zhang, Xiuhan Lin, and Xiaoyun Wang. "HuFu: Hash-and-Sign Signatures From Powerful Gadgets."

[24] del Pino, Rafael, Thomas Espitau, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, Mélissa Rossi, and Markku-Juhani Saarinen. "A Side-Channel Secure Signature Scheme." , 2023.

[25] Espitau, Thomas, Guilhem Niot, Chao Sun, and Mehdi Tibouchi. "Square Unstructured Integer Euclidean Lattice Signature," Submission to the NIST’s post-quantum cryptography standardization process, 2023.

[26] Luk Bettale, Delaram Kahrobaei, Ludovic Perret, and Javier Verbel, “Biscuit: Shorter MPC-based Signature from PoSSo, ” Online: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/ documents/round-1/spec-files/Biscuit-spec-web.pdf, 2023.

[27] Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez,Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu,Matthieu Rivain, and Jean-Pierre Tillich, “MIRA Specifications,” 2023.

[28] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/MiRitH_spec-web.pdf, 2023.

[29] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/MQOM-spec-web.pdf, 2023.

[30] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/PERK-spec-web.pdf, 2023.

[31] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ryde-spec-web.pdf, 2023.

[32] NIST, “Round 1 Submissions,” Online:https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SDitH-spec-web.pdf, 2023.

[33] Ming-Shing Chen, Andreas H¨ulsing, Joost Rijneveld, Simona Samardjiska, and Peter

Schwabe.From 5-pass MQ -based identification to MQ -based signatures. In Jung Hee Cheon andTsuyoshi Takagi, editors, Advances in Cryptology - ASIACRYPT 2016 - 22nd InternationalConference on the Theory and Application of Cryptology and Information Security, Hanoi,Vietnam, December 4-8, 2016, Proceedings, Part II, volume 10032 of Lecture Notes in Computer Science, pages 135 – 165, 2016.

[34] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Bhavani Thuraisingham, David Evans, Tal Malkin,and Dongyan Xu, editors, Proceedings of the 2017 ACM SIGSAC Conference on Computerand Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017,pages 1825 – 1842. ACM, 2017.

[35] Carlos Aguilar-Melchor, Nicolas Gama, James Howe, Andreas Hülsing, David Joseph, and Dongze Yue. “The Return of the SDitH,“ Cryptology ePrint Archive, Paper 2022/1645, 2022. https:// eprint.iacr .org /2022/1645

[36] Thibauld Feneuil. Building MPCitH-baseds Signatures from MQ, MinRank, Rank SD andPKP. Cryptology ePrint Archive, Paper 2022/1512, 2022. https://eprint.iacr.org/2022/1512.

[37] J. Katz, V. Kolesnikov, and X. Wang. Improved non-interactive zero knowledgewith applications to post-quantum signatures. In D. Lie, M. Mannan, M. Backes,and X. Wang, editors, ACM CCS 2018, pages 525 – 537. ACM Press, 2018.

[38] Rodrıguez, Borja Gómez. "3WISE: Cubic Element-Wise trapdoor based MPKC cryptosystem", 2023.

[39] LUENGO, IGNACIO, and MARTÍN AVENDANO. "DME: MULTIVARIATE SIGNATURE PUBLIC KEY SCHEME." SUBMISSION TO NIST PQC, 2023.

[40] Rodrıguez, Borja Gómez. "HPPC: Hidden Product of Polynomial Composition Submission.", 2023

[41] Ward Beullens Fabio Campos Sofia Celi Basil Hess Matthias J. Kannwischer. Nibbling MAYO: Optimized implementations for AVX2 and Cortex-M4. Cryptology ePrint Archive, 2023.

[42] Louis Goubin Benoît Cogliati Jean-Charles Faugère Pierre-Alain Fouque Robin Larrieu Gilles Macario-Rat Brice Minaud Jacques Patarin. *“PROV: PRovable unbalanced Oil and Vinegar Specification v1”,* 2023.

[43] Hiroki Furue Yasuhiko Ikematsu Fumitaka Hoshino Tsuyoshi Takagi Kan Yasuda Toshiyuki Miyazawa Tsunekazu Saito Akira Nagai. QR-UOV. 2023.

[44] Lih-Chung Wang, Chun-Yen Chou Jintai Ding Yen-Liang Kuan Ming-Siou Li Bo-Shu Tseng Po-En Tseng Chia-Chun Wang. A Simple Noncommutative UOV Scheme. Cryptology ePrint Archive, 2022.

[45] Boru Gong, Hao Guo, Xiaoou He, Yi Jin, Yuansheng Pan, Dieter Schmidt, Chengdong Tao, Danli Xie, Bo-Yin Yang, Ziyu Zhao. TUOV: Triangular Unbalanced Oil and Vinegar. 2023.

[46] Ward Beullens Ming-Shing Chen Jintai Ding Boru Gong Matthias J. Kannwischer Jacques Patarin Bo-Yuan Peng Dieter Schmidt Cheng-Jhih Shih Chengdong Tao Bo-Yin Yang. Unbalanced Oil and Vinegar. NIST Round, 1: 61, 2023.

[47] Jacques Patarin Benoît Cogliati Jean-Charles Faugère Pierre-Alain Fouque Louis Goubin Robin Larrieu Gilles Macario-Rat Brice Minaud. Principal submitter: Jacques Patarin, 2023

[48] SMITH-TONE, Daniel. A total break of the 3wise digital signature scheme. Cryptology ePrint Archive, 2023.

[49] LUENGO, Ignacio; AVENDAÑO, Martín; COSCOJUELA, Pilar. *“DME: a full encryption, signature and KEM multivariate public key cryptosystem,”* International Conference on Post-Quantum Cryptography. Cham: Springer Nature Switzerland, 2023.

[50] Lin-Chung Wang, Po-En Tseng, Yen-Liang Kuan, Chun-Yen Chou, “NOVA, a Noncommutative-ring

Based Unbalanced Oil and Vinegar Signature Scheme with Key-randomness Alignment," Cryptology ePrint Archive, 2022.

[51] Seongkwang Kim Jihoon Cho Mingyu Cho Jincheol Ha Jihoon Kwon Byeonghak Lee Joohee Lee Jooyoung Lee Sangyub Lee Dukjae Moon Mincheol Son Hyojin Yoon. *"The AIMer Signature Scheme,"* 2023.

[52] Vikas Srivastava Naina Gupta Arpan Jati Anubhab Baksi Jakub Breier Anupam Chattopadhyay Sumit Kumar Debnath Xiaolu Hou. Ascon-sign. NIST PQC Additional Round, 2023.

[53] Carsten Baum Lennart Braun Cyprien Delpech de Saint Guilhem Michael Klooß Christian Majenz Shibam Mukherjee Emmanuela Orsini Sebastian Ramacher Christian Rechberger Lawrence Roy Peter Scholl. "*FAEST: Algorithm Specifications*," 2023.

[54] Yu Yu Hongrui Cui Kaiyi Zhang. SPHINCS-$\alpha $: A Compact Stateless Hash-Based Signature Scheme. Cryptology ePrint Archive, 2022.

[55] DOBRAUNIG, Christoph, et al. Ascon v1. 2: Lightweight authenticated encryption and hashing. Journal of Cryptology, 2021.

[56] Bläser, Markus, Dung Hoang Duong, Anand Kumar Narayanan, Thomas Plantard, Youming Qiao, Arnaud Sipasseuth, and Gang Tang. *"The ALTEQ Signature Scheme: Algorithm Specifications and Supporting Documentation."* NIST PQC Submission, 2023.

[57] Liu, Dongxi, and Raymond K. Zhao. *"eMLE-Sig 2.0: A Signature Scheme based on Embedded Multilayer Equations with Heavy Layer Randomization."*, 2023.

[58] Muhammad Rezal Kamel Ariffin, Nur Azman Abu, Terry Lau Shue Chien, Zahari Mahad, Liaw Man Cheon, Amir Hamzah Abd Ghafar, Nurul Amiera Sakinah Abdul Jamal, *"Kriptografi Atasi Zarah Digital Signature (KAZ-SIGN)"*,2023.

[59] Chen, M.S., Chen, Y.S., Cheng, C.M., Fu, S., Hong, W.C., Hsiang, J.H., Hu, S.T., Kuo, P.C., Lee, W.B., Liu, F.H. and Thaler, J., *"Preon: zk-SNARK based Signature Scheme"*, May 2023.

[60] *Jianfang "Danny" Niu, Daniel Enrique Náger Piazuelo "NIST Submission: Xifrat1-Sign.I DSS"*

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

〈저 자 소 개〉

심 민 주 (Min-Joo Sim)

학생회원

2021년 2월 : 한성대학교 IT융합공학부 졸업

2023년 2월 : 한성대학교 IT융합공학부 석사

2023년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정

<관심분야> 정보보안, 암호구현

송 경 주 (Gyeong-Ju Song)

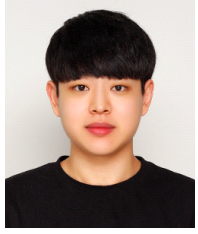
학생회원

2021년 2월 : 한성대학교 IT융합공학부 졸업

2023년 2월 : 한성대학교 IT융합공학부 석사

2023년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정

<관심분야> 양자컴퓨팅, 암호구현, 정보보안



이 민 우 (Min-Woo Lee)

2023년 2월 : 한성대학교 IT융합공학부 졸업

2023년 3월~현재 : 한성대학교 융합보안학과 석사과정

<관심분야> 정보보안, 암호구현

서 화 정 (Hwa-Jeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 졸업

2012년 2월 : 부산대학교 컴퓨터공학과 석사

2016년 2월 : 부산대학교 컴퓨터공학과 박사

2017년 4월~2023년 2월 : 한성대학교 IT융합공학부 조교수

2023년 3월~현재 : 한성대학교 융합보안학과 부교수

<관심분야> 정보보안, 암호구현