정 보 보 호 학 회 지
제 33 권 제1호, 2023. 2

다변수 이차식 기반 전자서명 기법의 연구 동향

조 성 민*, 차 정 현**, 서 승 현***

요 약

다변수 이차식 기반 전자서명은 양자내성암호 중 짧은 서명 길이와 빠른 서명 생성 및 검증으로 인해 자원이 제한된 기기에 적합할 것으로 예상된다. SFLASH는 NESSIE 표준으로 선정되었으며, NIST 양자내성암호 표준 공모에 다수의 다변수 이차식 기반 서명이 제출되었다. 또한 HiMQ는 국내 TTA 표준으로 선정되었다. 이러한 다변수 이차식 기반 전자서명의 장점으로 인해 NSIT 양자내성암호 표준의 추가 전자서명 공모에도 다변수 이차식 기반 전자서명이 제출될 것으로 예상되며, 국내 양자내성암호 국가공모전에는 MQ-Sign이 1라운드 후보로 공개되었다. 본 논문에서는 대표적인 다변수 이차식 기반 전자서명에 대해서 살펴보고, 다변수 이차식 기반 전자서명의 표준화 동향에 대해 살펴본다.

Ⅰ. 서 론

Richard Feynman이 1982년 양자 중첩과 얽힘 현상을 활용한 양자 컴퓨터를 제안한 이후로 [RF82], 양자 컴퓨터 개발이 급속한 발전을 이루고 있다. 양자 컴퓨터의 개발은 IBM, Google, D-Wave Systems 등 세계적인 IT 기업들이 주도하고 있다. Google은 2019년 53-큐비트 양자 프로세서인 ‘Sycamore’를 공개하면서 최초로 양자 우위에 도달했다고 발표했으며 [AANM19], IBM은 2022년 433-큐비트 양자 프로세서인 ‘Osprey’를 발표하였다[IBM22].

양자적 성질에 기반하여 설계된 양자 컴퓨터는 기존 컴퓨터로는 풀기 어려운 문제를 빠르게 풀 수 있다. 이러한 양자 컴퓨터를 활용하여 기존의 어려운 문제를 효율적으로 푸는 양자 알고리즘들이 제안되었다. Peter Shor가 1994년 제안한 쇼어(Shor) 알고리즘[PS94]은 인수분해 및 이산로그 문제를 다항 시간 안에 풀 수 있으며, 1996년 Lov Grover가 제안한 그로버(Grover) 알고리즘[LG96]은 비정형 탐색 문제 풀이에 2차 속도 향상을 가져왔다.

특히, 인수분해 및 이산로그 문제는 기존 공개키 암호인 RSA 및 타원곡선 암호(ECC: Elliptic Curve Cryptography)가 기반하고 있는 문제로 대용량 양자 컴퓨팅 환경에서 보안에 취약해질 것으로 예상된다. 미국 국립표준기술연구소인 NIST(National Institute of Standards and Technology)는 빠르면 2026년에 4096 큐비트의 양자 컴퓨터 상에서 쇼어 알고리즘을 통해 2048-비트 RSA가 깨질 것으로 추정하고 있다. 이에 NIST는 양자 컴퓨터에도 안전한 새로운 암호 알고리즘인 양자내성암호(PQC: Post Quantum Cryptography)를 2016년 공개 모집하였다. 2022년 7월, NIST는 키 캡슐화 메커니즘(KEM: Key Encapsulation Mechanism)인 CRYSTALS-Kyber와 전자서명 알고리즘인 CRYSTALS-Dilithium, Falcon, SPHINCS+를 양자내성암호 표준으로 발표하였다. NIST는 추가적인 키 캡슐화 메커니즘 표준을 정하기 위해 4라운드를 진행하고 있으며, 격자 기반 알고리즘이 대부분인 전자서명 표준 외에 다른 문제에 기반하고 있는 전자서명을 추가로 모집 중에 있다. 국내에서도 국가보안기술연구소에서 양자내성암호연구단(KpqC)를 발족하여 양자내성암호 국가공모전을 진행 중이다. 2022년 12월, 공모전 1라운드 알고리즘(KEM 7종, 전자서명 9종)이 공개되어 이들에 대한 공개검증이 시작되었다.

본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2019-0-00033-005. 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발)
본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2021R1A2C1095591)
* 한양대학교 전자공학과 (대학원생, smcho3315@hanyang.ac.kr)
** 한양대학교 ERICA 전자공학부 (학부생, jhcha0822@hanyang.ac.kr)
*** 한양대학교 ERICA 전자공학부 (교수, seosh77@hanyang.ac.kr)

양자내성암호 중 다변수 이차식(MQ: Multivariate Quadratic) 기반 전자서명 기법은 타 알고리즘 대비 짧은 서명 길이를 가지며 서명 생성 및 검증이 빠르다는 장점을 갖고 있어 제한된 자원을 갖는 IoT 디바이스 등에서의 구현이 용이할 것으로 기대되고 있다[KS21].

양자 컴퓨팅 시대를 대비하기 위해 새로운 공개키 암호인 양자내성암호에 대한 제안 및 검토가 활발하게 진행되고 있는 현 시점에서, 본 논문에서는 다양한 양자내성암호 중 다변수 이차식 기반의 전자서명 알고리즘의 현황에 대해 조사한다.

본 논문은 다음과 같이 구성되어 있다; 2장에서는 전반적인 연구 배경과 다변수 이차식 기반 전자서명의 개념에 대해서 살펴본다. 3장에서는 여러 다변수 이차식 기법을 설명한 후, 4장에서 국내외 연구 동향을 살펴본다.

Ⅱ. Preliminaries

2.1. 양자내성암호 (PQC: Post Quantum Cryptograpy)

현재까지 공개키 암호로써 널리 사용되고 있는 RSA(Rivest-Shamir-Adleman) 암호 및 타원 곡선 암호(ECC: Elliptic Curve Cryptography)는 인수분해 및 이산로그 문제의 어려움에 기반하여 설계되었다. 그러나 Peter Shor가 양자적 특성을 활용하여 인수분해 및 이산로그 문제를 다항시간 안에 풀 수 있는 양자 알고리즘[PS94]을 제안하면서, 더 이상 기존 공개키 암호가 안전하지 않다는 문제가 제기되었다. 이후 실제 RSA 및 ECC를 해독할 수 있을 만큼 양자 컴퓨터 개발 기술이 발전하면서 기존 공개키 암호에 대한 보안 위협이 가시화되고 있다[MM18].

양자 컴퓨팅 환경에서의 기존 공개키 암호에 대한 위협에 맞서기 위해, 미국 국립표준기술연구소인 NIST(National Institute of Standards and Technology)는 2016년 초부터 양자내성암호(PQC: Post Quantum Cryptography)를 공개 모집하였다. NIST는 2022년 7월 키 캡슐화 메커니즘(KEM: Key Encapsulation Mechanism) 1종과 전자서명 알고리즘 3종을 양자내성암호 표준으로 발표하였다. 현재는 4라운드를 진행하여 추가적인 KEM 표준을 정하는 과정을 진행 중이며, 격자 기반 이외의 전자서명 알고리즘에 대해서도 추가 모집을 진행하고 있다. 표 1은 NIST 양자내성암호의 표준 알고리즘 4종 및 4라운드 후보 알고리즘을 보여준다.

〔표 1〕 NIST 양자내성암호 표준 알고리즘 및 4라운드 후보 알고리즘

Standardization	KEMs	CRYSTALS-KYBER
	Digital Signatures	CRYSTALS-Dilithium
		FALCON
		SPHINCS+
Fourth Round Candidates	KEMs	BIKE
		Classic McEliece
		HQC
		SIKE*

국내에서도 양자내성암호 관련 기술의 저변 확대 및 경쟁력 고취를 위해 양자내성암호연구단(KpqC)을 발족하였으며, 양자내성암호 국가공모전을 진행하고 있다. 2022년 12월에 KEM 7종, 전자서명 9종의 양자내성암호 국가공모전 1라운드 후보 알고리즘들이 공개되어 이들에 대한 공개 검증이 시작되었다.

2.2. 다변수 이차식 기반 서명

다변수 이차식 기반 서명은 다변수 이차식(MQ: Multivariate Quadratic) 문제의 어려움에 기반한 서명 기법으로, 아직까지 다변수 이차식 문제를 효율적으로 푸는 양자 알고리즘은 등장하지 않았다.

유한체 F_q 상의 다변수 이차식 함수 $MQ(n,m,F_q)$는 n개의 변수 $x=(x_1,...,x_n)$와 m개의 방정식으로 구성되며, 일반적으로 다음과 같이 표현된다.

$$MQ(n,m,F_q)=F(x)=(f_1(x),...,f_m(x)),$$
$$f_s(x)=\sum_{i,j}\alpha_{i,j}^{(s)}x_ix_j+\sum_i\beta_i^{(s)}x_i$$

다변수 이차식 문제란 $v\in F_q^m$가 주어졌을 때, $F(x)=v$를 만족하는 n개의 변수 $x=(x_1,...,x_n)$를 찾는 문제이며, NP-완전(NP-complete)로 알려져 있다[GJ79].

대표적인 다변수 이차식 기반 서명으로는 UOV와 NIST 양자내성암호 표준 공모의 3라운드에서 탈락한 Rainbow 등이 있으며, 국내에서는 HiMQ 서명 기법이 TTA 표준으로 채택되었다. Rainbow는 NIST 양자내성암호 표준 공모 과정에서 Ward Beullens의

rectangular MinRank 공격에 의해 깨졌으며, Beullens가 새롭게 제안한 다변수 이차식 기반 서명인 MAYO와 MinRank 공격에 대해 안전한 UOV가 NIST의 추가 전자서명 공모에 제출될 것으로 예상된다. 국내 양자내성암호 국가공모전에서는 MQ-Sign이 다변수 이차식 기반으로는 유일하게 1라운드 후보 알고리즘으로 선정되었다.

다변수 이차식 기반 서명 기법은 전수론 기반 서명 대비 짧은 서명 길이와 빠른 검증 속도를 장점으로 삼기에, 사물인터넷(Internet of Things, IoT) 기기나 드론 등의 제한된 자원을 가지는 기기에서 효율적인 사용이 기대된다.

Ⅲ. 다변수 이차식 기반 전자서명 기법

본 장에서는 대표적인 다변수 이차식 기반 전자서명 기법 중 하나인 UOV(Unbalanced Oil and Vinegar)와 UOV의 2계층 버전인 Rainbow, NIST의 추가 양자내성 전자서명 공모에 제출될 것으로 예상되는 MAYO 및 국내 TTA 표준으로 선정된 HiMQ에 대해서 설명한다.

3.1. UOV

UOV(Unbalanced Oil and Vinegar)는 1999년 Aviad Kipnis 등에 의해 제안되었다[KPG99]. UOV는 1997년 Jacques Patarin에 의해 제안된 Oil and Vinegar 서명 기법[JP97]을 개선한 것으로, oil 변수와 vinegar 변수의 개수가 같은 Oil and Vinegar와 달리 vinegar 변수의 수를 oil 변수의 수보다 많게 설정하여 보안성을 높였다.

UOV의 개인키는 두 개의 맵 F와 T로 구성된다. F는 다음과 같은 m개의 다항식 $f(x)$로 구성된다.

$$f(x)=\sum_{i=1}^{v}\sum_{j=i}^{n}\alpha_{i,j}x_ix_j+\sum_{i=1}^{n}\beta_ix_i+\gamma$$

이때, $n(=v+m)$개의 변수 $x=(x_1,\ldots,x_n)$는 v개의 vinegar 변수 $x_1,\ldots,x_v$와 m개의 oil 변수 $x_{v+1},\ldots,x_n$으로 구성된다. UOV의 공개키는 두 개의 개인키 F와 T의 합성으로 이루어진 $P=F\circ T$이다.

UOV의 서명 s는 다음과 같이 메시지 d의 해시값에 대해 개인키들의 역연산으로 계산된다.

$$s=T^{-1}\circ F^{-1}(H(d))$$

개인키 F의 역연산은 다항식 $f(x)$의 해를 구함으로써 수행되며, vinegar 변수에 랜덤한 값을 대입한 후, 다항식들을 만족하는 oil 변수들을 구하는 방식으로 계산된다. oil 변수의 수가 m이므로, vinegar 변수에 랜덤한 값을 대입하게 되면, 동일한 수의 변수와 방정식을 갖는 시스템이 되며, 이로 인해 선형 방정식을 효율적으로 구할 수 있게 된다.

그러나 UOV는 v와 m의 값에 따라 안전성에 문제가 생길 수 있으며, 서명의 크기가 메시지의 크기의 두 배가 되는 문제가 존재한다.

3.2. Rainbow

2005년 Jintai Ding과 Dieter Schmidt는 위와 같은 UOV의 문제점을 해결하기 위해 UOV 구조를 여러 번 반복하는 Rainbow를 제안하였다[DS05]. 본 절에서는 NIST 양자내성암호 3라운드의 Rainbow 기준으로 설명한다.

3.2.1. 파라미터

Rainbow는 2계층 구조로, v_1개의 vinegar 변수와 o_1개의 oil 변수가 첫 번째 계층을 구성하며, 첫 번째 계층의 변수들(v_1+o_1개)이 두 번째 계층의 vinegar 변수가 되고 o_2개의 oil 변수들과 함께 두 번째 계층을 구성한다.

NIST는 보안 카테고리 5개를 통해 알고리즘의 보안 비도를 표현하도록 규정하였다. Rainbow는 파라미터 집합 3개를 정의하였다.

$F=GF(16),(v_1,o_1,o_2)=(36,32,32)$:
NIST 보안강도 레벨 I, II에 해당

$F=GF(256),(v_1,o_1,o_2)=(68,32,48)$:
NIST 보안강도 레벨 III, IV에 해당

$F = GF(256), (v_1, o_1, o_2) = (96, 36, 64)$:
NIST 보안강도 레벨 V에 해당

3.2.2 개인키 및 공개키

Rainbow의 개인키는 역행렬이 존재하는 아핀맵 S와 T, 그리고 중앙맵 F로 구성된다. 중앙맵 F를 구성하는 m개의 다항식 $f^{(v_1+1)}, ..., f^{(n)}$은 다음과 같다.

$$f^{(k)}(x_1, ..., x_n) = \sum_{i, v \in V_i} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_i, j \in O_i} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_i \cup O_i} \gamma_i^{(k)} x_i + \delta^{(k)}$$

Rainbow의 공개키 P는 UOV와 마찬가지로 개인키들의 합성을 통해 다음과 같이 계산된다.

$$P = S \circ F \circ T$$

3.2.3 서명 생성 및 검증

서명할 메시지 d에 대한 서명 $z \in F^n$는 다음과 같이 생성된다.

1. $h = H(d) \in F^m$인 해쉬 값 h를 계산한다.
2. $x = S^{-1}(h) \in F^m$인 x를 계산한다.
3. $F(y) = x$를 만족하는 $y \in F^n$를 구한다.
4. $z = T^{-1}(y) \in F^n$를 만족하는 서명 z를 계산한다.

서명 z와 메시지 d에 대하여 $h' = P(z)$과 $h = H(d)$가 동일하다면 서명이 검증되며, 그렇지 않다면 검증에 실패한다.

Rainbow는 NIST 양자내성암호 표준 공모에 제출되어 3라운드까지 살아남았다. 그러나 2021년 Ward Beullens가 Rainbow의 공개키에 polar form 변환을 적용한 뒤 MinRank 공격을 진행하는 rectangular MinRank 공격[WB21]에 의해 보안 강도를 파라미터 세트 I, III, V에 대해 각각 127-bit, 177-bit, 226-bit로 낮추었다. 이는 NIST의 보안 강도 조건을 만족하지 못하는 수치다. 또한 2022년 Beullens는 Rainbow에 대한 두가지 새로운 키 복원 공격(simple 공격 및 combined 공격)을 제시하였다[WB22]. 그는 simple 공격을 통해 파라미터 세트 I, III, V의 보안강도를 각각 69-bit, 160-bit, 257-bit로 낮추었으며, combined 공격에서는 각각 99-bit, 157-bit, 206-bit로 낮추었다. 특히 파라미터 I의 개인키를 노트북에서 이틀만에 복원하는데 성공하였다. 이러한 안전성 문제로 인해 Rainbow는 NIST 양자내성암호 표준에 선정되지 못하였다.

3.3. SFLASH

SFLASH[CGP92]는 스마트 카드를 겨냥한 다변수 이차식 기반 고속 전자서명 알고리즘이다. HFE 기법을 기반으로 하며 259 bit의 서명, 15.4 kB의 공개키와 최소 128 bit의 길이를 가지는 랜덤 시드로 생성된 2.45 kB의 개인키를 지닌다. 서명 생성에는 최대 2.7 ms, 검증에는 최대 0.8 ms, 키 생성에는 최대 1초가 소요되며 서명 생성시 RSA보다 빠른 속도를 장점으로 갖는다. 이러한 경량 시스템으로 인하여 New European Schemes for Signatures, Integrity and Encryption(NESSIE)에 표준으로 선정되었다.

3.3.1. 파라미터

SFLASH는 $K = F_{128} = F_2[X]/(X^7 + X + 1)$와 $\mathcal{L} = K[X]/(X^{37} + X^{12} + X^{10} + X^2 + 1)$ 두 개의 유한체를 사용한다. 또한 $\{0,1\}^7$과 K 간의 전단사(bijection) π, K^{37}과 $\mathcal{L}$ 간의 전단사 ϕ를 사용한다.

3.3.2. 개인키 및 공개키

SFLASH는 역행렬이 존재하는 37×37 행렬 S_L과 37×1 벡터 S_C로 구성된 아핀 비밀 전단사 s, 동일 크기의 행렬 T_L과 벡터 T_C로 구성된 아핀 비밀 전단사 t, 80-bit 스트링 Δ를 개인키로 갖는다. 공개키 G는 개인키들을 통해 다음과 같이 생성된다.

$$G(X) = \left[t(\phi^{-1}(F(\phi(s(X))))) \right]_{0 \to 181}$$

이때 F는 $\mathcal{L}$ 상의 A에 대해 다음과 같이 정의된다.

$$F(A) = A^{128^{11}+1}$$

공개키 G는 이차다항식 P_i로 구성된 이차 변환이며, 다음과 같다.

$$(Y_0, ..., Y_{25}) = G(X_0, ..., X_{36}) \equiv \begin{cases} Y_0 = P_0(X_0, ..., X_{36}) \\ \vdots \\ Y_{25} = P_{25}(X_0, ..., X_{36}) \end{cases}$$

$$P_i(X_0, ..., X_{36}) = \sum_{0 \le j < k < 37} \xi_{i,j,k} X_j X_k + \sum_{0 \le j < 37} \upsilon_{i,j} X_j + \rho_i$$

3.3.3. 서명 생성 및 검증

서명할 메시지 M에 대한 서명 S는 다음과 같이 생성된다.

1. 메시지에 대한 해쉬 값 $M_1 = SHA1(M)$ 및 $M_2 = SHA1(M_1)$를 계산한다.
2. 182-bit, 77-bit 스트링 $V = [M_1]_{0 \to 159} \mid\mid [M_2]_{0 \to 21}$ 및 $W = [SHA1(Vvertvert\Delta)]_{0 \to 76}$를 계산한다.
3. $Y = (\pi([V]_{0 \to 6}), \pi([V]_{7 \to 13}), ..., \pi([V]_{175 \to 181}))$ 및 $R = (\pi([W]_{0 \to 6}), \pi([W]_{7 \to 13}), ..., \pi([W]_{70 \to 76}))$을 계산한다.
4. $X = (X_0, ..., X_{36}) = s^{-1}(\phi^{-1}(F^{-1}(\phi(t^{-1}(Y \mid\mid R)))))$를 계산한다.
5. 서명 $S = \pi^{-1}(X_0) \mid\mid \cdots \mid\mid \pi^{-1}(X_{36})$를 계산한다.

M_1, M_2, V를 서명 생성 과정과 동일하게 구한 후, $Y = (\pi([V]_{0 \to 6}), \pi([V]_{7 \to 13}), ..., \pi([V]_{175 \to 181}))$와 $Y' = G(\pi([S]_{0 \to 6}), \pi([S]_{7 \to 13}), ..., \pi([S]_{252 \to 258}))$이 동일하다면 서명이 검증되며, 그렇지 않다면 검증에 실패한다.

〔표 2〕 보안 강도별 HiMQ 권고 파라미터

	q	v	o_1	o_2	λ
HiMQ-128	2^8	37	21	24	128
HiMQ-160	2^8	66	35	33	160
HiMQ-192	2^9	68	37	35	192

3.4. HiMQ

HiMQ는 다변수 이차식 기반 전자서명 알고리즘으로, 3 계층 구조를 갖는 HiMQ-3가 NIST 양자내성암호 표준 공모 2라운드에서 탈락하였다. 이후, HiMQ-3를 제안하였던 국가수리과학연구소는 2 계층 구조의 HiMQ를 제안하였다. HiMQ는 2020년 6월 17일 국내 정보통신단체표준 (TTA 표준)으로 제정되었다 [TTAK12].

3.4.1 파라미터

HiMQ는 표수가 2인 유한체 F_q를 사용하며, 다변수 이차식 문제는 총 n개의 변수(v개의 vinegar 변수 및 $o_1 + o_2$개의 oil 변수, $n = v + o_1 + o_2$)와 m개의 방정식($m = o_1 + o_2$)으로 구성된다. 보안 강도별 HiMQ의 권고 파라미터는 표 2와 같다.

3.4.2 개인키 및 공개키

HiMQ는 역변환이 가능한 아핀 변환 $S: F_q^m \to F_q^m$와 $T: F_q^n \to F_q^n$의 역변환인 S^{-1}와 T^{-1}, 그리고 첫 번째와 두 번째 계층의 다변수 이차다항식으로 구성된 중앙 함수 $F = (F^{(1)}, ..., F^{(m)}) : F_q^n \to F_q^m$를 서명키로 가진다. 서명키는 의사난수함수를 통해 랜덤하게 선택되며, 서명키들에 대한 합성 연산을 통해 검증키 $P = S \circ F \circ T$를 생성한다.

중앙 함수 F를 구성하는 m개의 다변수 이차다항식 $F^{(1)}, ..., F^{(m)}$은 n개의 변수 $x_1, ..., x_n$을 가지며, 다음과 같이 생성된다.

$$\begin{cases} F^{(1)}(x_1, ..., x_n) = \Phi_1(x_1, ..., x_v) + \delta_1 x_{v+1} x_{v+2} \\ F^{(2)}(x_1, ..., x_n) = \Phi_2(x_1, ..., x_v) + \delta_2 x_{v+2} x_{v+3} \\ \vdots \\ F^{(o_1)}(x_1, ..., x_n) = \Phi_{o_1}(x_1, ..., x_v) + \delta_{o_1} x_{v+o_1} x_{v+1} \end{cases} \quad (1)$$

$$\Phi_i = \sum_{1 \le i < j}^{v} \alpha_{i,j} x_i x_j$$

$$\begin{cases} F^{(o_1+1)}(x_1, ..., x_n) = \Psi_1(x_1, ..., x_{v+o_1}) \\ \quad + \Theta_1(x_1, ..., x_n) + \epsilon_1 x_{o_1+1} + c_1 \\ \quad \vdots \\ F^{(o_1+o_2)}(x_1, ..., x_n) = \Psi_{o_2}(x_1, ..., x_{v+o_1}) \\ \quad + \Theta_{o_2}(x_1, ..., x_n) + \epsilon_{o_2} x_{o_1+o_2} + c_{o_2} \end{cases} \quad (2)$$

$$\Psi_i = \sum_{j=1}^{v+o_1} \beta_{i,j} x_j x_{(i+j-1)(\mathrm{mod} v+o_1)+1}$$

$$\Theta_i = \sum_{j=1}^{v+o_1} \gamma_{i,j} x_j x_{v+o_1+1+(j-i)(\mathrm{mod} o_2)}$$

3.4.3 서명 생성 및 검증

서명 대상 메시지 M과 2λ-bit의 랜덤 값 r에 대하여 서명 값 $\tau = (\sigma, r)$는 다음과 같이 출력된다.

1. $\zeta = (\zeta_1, ..., \zeta_m) = S^{-1}(H(M, r))$ 계산
2. 임의의 랜덤 벡터 $s_v = (s_1, ..., s_v) \in F_q^v$ 선택 후, 각 다변수 이차다항식 $F^{(i)}$ $(1 \le i \le o_1)$의 $x_1, ..., x_v$에 대입
3. 연립 이차방정식 $\begin{cases} \delta_1 x_{v+1} x_{v+2} = \zeta_1 - \Phi_1(s_v) \\ \quad \vdots \\ \delta_{o_1} x_{v+o_1} x_{v+1} = \zeta_{o_1} - \Phi_{o_1}(s_v) \end{cases}$의 해 $(x_{v+1}, ..., x_{v+o_1}) = (s_{v+1}, ..., s_{v+o_1})$찾기
4. $(s_1, ..., s_{v+o_1})$를 각 $F^{(i)}$ $(o_1+1 \le i \le o_1+o_2)$에 대입하여 o_2개의 방정식과 o_2개의 변수를 갖는 연립 일차방정식 구하기
5. 가우스 소거법을 통해 연립 일차방정식의 해 $(s_{v+o_1+1}, ..., s_n)$ 찾기
6. $F(s) = \zeta$를 만족하는 $s = (s_1, ..., s_n)$에 대해 $\sigma = (\sigma_1, ..., \sigma_n) = T^{-1}(s) \in F_q^n$ 계산
7. $\tau = (\sigma, r)$를 메시지 M에 대한 서명 값으로 출력

검증키 $P = (P_1, ..., P_m)$와 메시지 M, 서명 값 $\tau = (\sigma, r)$에 대하여 서명에 대한 검증은 다음과 같이 수행된다.

1. 메시지 M에 대한 해시 값 $H(M, r)$ 계산
2. $P(\sigma) = (P_1(\sigma), ..., P_m(\sigma))$ 계산
3. $P(\sigma) = H(M, r)$이면 검증 통과, 아니면 실패

Ⅳ. 다변수 이차식 기반 전자서명 표준화 현황

다변수 이차식 기반 전자서명은 짧은 서명 길이와 빠른 서명 생성 및 검증으로 인해 제한된 자원을 갖는 소형 기기 등에 적용하기 알맞을 것으로 예상되고 있다. 본 장에서는 3장에서 살펴본 다변수 이차식 기반 전자서명 기법 외에 추가적인 다변수 이차식 기반 전자서명 기법의 표준화 현황에 대해 살펴본다.

4.1. 국내 연구 동향

국내 양자내성암호 국가공모전인 KPQC에 다변수 이차식 기반 전자서명인 MQ-Sign[SKA22]이 제출되어 현재 1라운드 후보로 공개되었다. MQ-Sign은 1계층 UOV 기법을 기반으로 하고 있다. 기존 UOV 기법과는 달리 짧은 개인키 사이즈와 빠른 서명 생성을 장점으로 갖는다. 다계층 구조를 갖는 Rainbow는 빠른 동작과 작은 키 사이즈를 갖는 반면 MinRank 공격에 취약점을 지닌다. MQ-Sign은 단계층 구조에 기반하여 MinRank 공격에 대한 내성을 갖추면서도 단계층 구조인 UOV의 큰 키 사이즈와 느린 성능의 단점을 희소 다항식을 이용하여 해결하였다.

MQ-Sign은 서명 길이로 NIST 보안 카테고리 I, III, V 레벨에 따라 각각 134, 200, 260 바이트가 요구된다. 이는 여타 양자내성암호와 비교했을 때도 작은 값이다. 작은 서명 길이는 빠른 검증으로 이어지게 된다.

4.2. 국외 연구 동향

NESSIE에는 HFE의 두 가지 변조인 HFE-와 HFEv를 합쳐 만든 HFEv-에 기반을 둔 Quartz[PCG21]도 공모에 참여하였다. 다만 SFLASH와 달리 최종 선정되지는 못하였다. 중국에서는 2018년 8월 양자내성암호 공모전을 시작하여 2019년 9월 1라운드 후보군 발표 후, 2020년 1월 최종 수상 알고리즘을 발표하였다. 이 중 다변수 이차식 기반 KEM인 Square-Free가 1라운드 후보로 발표되었으나, 최종 수상하지는 못하였다.

NIST의 양자내성암호 공모 3라운드에 다변수 이차

식 기반 전자서명 기법인 GeMSS(Great Multivariate Short Signature)가 대체 후보군으로 등록되었다 [PCG21]. GeMSS는 HFEv- 기반으로, 짧은 서명을 생성하는 기법이다. 빠른 검증의 장점과 중간/혹은 긴 공개키 사이즈를 가진다. Rainbow와 마찬가지로 NIST 양자내성암호 표준으로 선정되지는 못하였다. 다만 전자서명 표준의 대부분이 격자 문제에 기반하고 있어 NIST는 다른 문제에 기반하고 있는 전자서명 기법들에 대해 추가적인 공모를 진행 하고 있다.

Rainbow를 깬 Ward Beullens는 2021년 UOV의 변형인 MAYO[MAYO21]를 제안하였다. UOV와 Rainbow는 서명 생성 시 다변수 이차식 시스템의 해를 빠르게 찾기 위해서 oil 변수의 개수와 다항식의 개수를 같게 설정하였다. 이는 키 복원 공격에 취약하며, 공개키의 크기가 커진다는 문제가 있다. 그는 oil 변수의 개수를 다항식의 수보다 적게 설정하여 키 복원 공격에 대한 안전성을 높이고, 공개키의 크기를 줄였다. MAYO의 경우, 서명 생성 시 찾아야 하는 oil 변수의 수가 방정식의 수보다 적기 때문에 어떠한 해도 존재하지 않을 확률이 크다. 이러한 문제를 해결하기 위해 MAYO는 다변수 이차식 시스템에 whipping 변환 [MAYO21]을 적용하여 변수의 개수가 kn인 다변수 이차식 시스템으로 확장 변환한다. 이때 k는 oil 변수의 개수 o와 방정식의 개수 m에 대해 $ko \geq m$을 만족하는 수이다. whipping 변환을 통해 찾아야 하는 변수의 개수는 ko개가 되어 큰 확률로 해를 구할 수 있게 된다. MAYO는 UOV와 함께 NIST 양자내성암호 표준의 추가 전자서명 공모에 제출될 것으로 예상되고 있다.

Ⅴ. 결 론

양자 컴퓨터의 발전으로 인해 기존 공개키 암호에 대한 보안 위협이 가시화됨에 따라 국내외로 새로운 양자내성암호 표준을 정하려는 움직임이 활발히 진행되고 있다. 그 중 다변수 이차식 기반 전자서명은 서명 길이가 짧고 서명 생성 및 검증이 빠르다는 장점으로 인해 IoT 기기 등 제한된 자원을 갖는 기기에 적합할 것으로 예상된다. 이에 NIST 양자내성암호 표준의 추가 전자서명 공모에 UOV와 MAYO가 후보로 제출될 것으로 예상되며, 국내 양자내성암호 국가공모전에 MQ-Sign이 1라운드 후보로 등록되었다. 또한 SFLASH는 경량 기기에의 적용이 주목받아 NESSIE에 표준으로 선정되었다. 그러나 Rainbow가 NIST 양자내성암호 표준 공모 3라운드에서 안전성 문제가 제기되어 탈락했기에 앞으로 보안성 검증 연구가 철저히 진행될 것으로 예상된다.

참 고 문 헌

[1] [RF82] R. P. Feynman, “Simulating Physics with Computers”, International Journal of Theoretical Physics, 21(6), pp.467-488, 1982.

[2] [AANM19] F. Arute, K. Arya, R. Babbush, D. Bacon, et al., “Quantum supremacy using a programmable superconducting processor”, Nature, 574(7779), pp.505-510, 2019.

[3] [IBM22] J. Gambetta, “IBM Quantum’s mission is to bring useful quantum computing to the world”, IBM News, Nov. 2022.

[4] [PS94] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, Proceedings 35th Annual Symposium on Foundations of Computer Science, pp.124-134, 1994.

[5] [LG96] L. K. Grover, “A fast quantum mechanical algorithm for database search”, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp.212-219, 1996.

[6] [KS21] K-A. Shim, “A Survey on Post-Quantum Public Key Signature Schemes for Secure Vehicular Communications”, IEEE Transactions on Intelligent Transportation Systems, 2021.

[7] [MM18] M. Mosca, “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?”, IEEE Security & Privacy, 16(5), pp.38-41, 2018.

[8] [OSS84] H. Ong, C. P. Schnorr, and A. Shamir, “An efficient signature scheme based on quadratic equations”, Proceedings of the sixteenth annual ACM symposium on Theory of computing, pp.208-216, 1984.

[9] [PS87] J. Pollard and C. Schnorr, “An Efficient Solution of the Congruence $x^2+ky^2=m \pmod{n}$”, IEEE Transactions on

Information Theory, 33(5), pp.702-709, 1987.

[10] [MI88] T. Matsumoto and H. Imai, “Public quadratic polynomial-tuples for efficient signature-verification and message-encryption”, Advances in Cryptology-EUROCRYPT’88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, 7, Springer Berlin Heidelberg, pp.419-453, 1988.

[11] [GJ79] M. R. Garey and D. S. Johnson, “Computers and intractability: a guide to the theory of np-completeness”, W. H. Freeman and Company, Jan. 1979.

[12] [KPG99] A. Kipnis, J. Patarin, and L. Goubin, “Unbalanced Oil and Vinegar Signature Schemes”, Eurocrypt, 99, pp.206-222, 1999.

[13] [JP97] J. Patarin, “The Oil and Vinegar Signature Scheme”, Dagstuhl Workshop on Cryptography September, 1997.

[14] [DS05] J. Ding and D. Schmidt, “Rainbow, a New Multivariable Polynomial Signature Scheme”, ACNS, 5, pp.164-175, 2005.

[15] [TTAK12] TTAK.KO-12.0348-Part2, “다변수 이차식 기반 양자내성암호 - 제2부: HiMQ, 부가형 전자서명 알고리즘”, 정보통신단체표준(국문표준), 2020.

[16] [MAYO21] W. Beullens, “MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps”, Selected Areas in Cryptography: 28th International Conference, Virtual Event, September 29-October 1, 2021, Revised Selected Papers, Cham: Springer International Publishing, pp.355-376, 2022.

[17] [SKA22] 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, 2022.

[18] [CGP92] N. Courtois, L. Goubin, J. Patarin, “SFLASH, a fast asymmetric signature scheme for low-cost smartcards-Primitive specification and supporting documentation”, URL https://www.cosic.esat.kuleuven.ac.be/nessie/workshop, 1992.

[19] [PCG21] J. Patarin, N. Courtois, and L. Goubin, “Quartz, 128-Bit Long Digital Signatures”, Topics in Cryptology－CT-RSA 2001, pp. 282-297, 2021.

[20] [CFMP17] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, “GeMSS: A Great Multivariate Short Signature”, Diss. UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France; LIP6-Laboratoire d'Informatique de Paris 6, 2017

〈저자소개〉

조 성 민 (Seong-Min Cho)

2019년 2월 : 한양대학교 ERICA 캠퍼스 전자공학부 졸업
2019년 3월~현재 : 한양대학교 전자공학과 석박사통합과정
<관심분야> IoT 보안, 양자내성암호, 양자 알고리즘, 양자 키 분배

차 정 현 (Jung-Hyun Cha)

2017년 3월~현재 : 한양대학교 ERICA 캠퍼스 전자공학부 재학
<관심분야> 정보보호, 양자내성암호

서 승 현 (Seung-Hyun Seo)

종신회원

2000년 2월 : 이화여자대학교 수학과 졸업

2002년 2월 : 이화여자대학교 컴퓨터학과 공학석사

2006년 2월 : 이화여자대학교 컴퓨터학과 공학박사

2006년 5월~2006년 11월 : 고려대학교 정보보호대학원 BK21 사업단 연구전임강사

2006년 12월~2010년 2월 : 금융보안연구원 주임연구원

2010년 2월~2012년 2월 : 한국인터넷진흥원 선임연구원

2012년 2월~2014년 5월 : 미국 퍼듀대학교 컴퓨터학과 박사후연구원

2014년 6월~2015년 2월 : 고려대학교 정보보호대학원 BK21+ 사업단 연구교수

2015년 3월~2017년 2월 : 고려대학교 세종캠퍼스 수학과 조교수

2017년 3월~2020년 2월 : 한양대학교 ERICA 캠퍼스 전자공학부 부교수

2020년 3월~현재 : 한양대학교 ERICA 캠퍼스 전자공학부 교수

<관심분야> 암호프로토콜, 암호이론, IoT 보안, 블록체인 보안, 악성 코드 분석, 양자 내성 암호