Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.1, Feb. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.1.1

Sparse 구조의 다변수 이차식 기반 서명에 대한 안전성 분석*

조 성 민,[1†] 서 승 현[2‡]
[1,2]한양대학교 (대학원생, 교수)

Security Analysis on Multivariate Quadratic Based Digital Signatures Using Sparse Matrices*

Seong-Min Cho,[1†] Seung-Hyun Seo[2‡]
[1,2]Hanyang University (Graduate student, Professor)

요 약

다변수 이차식 기반 전자서명 알고리즘은 구현의 용이성과 작은 서명 크기를 장점으로 갖는 양자내성암호 후보군이다. 이러한 다변수 이차식 기반 전자서명의 효율성을 높이기 위해 희소 행렬을 사용한 전자서명 기법들이 제시되었으며, 이 중 HiMQ는 국내 정보통신단체 표준으로 제정되었다. 그러나 HiMQ는 2022년 제안된 MinRank 공격에 의해 깨진 대표적 다변수 이차식 기반 전자서명인 Rainbow와 유사한 키 구조를 갖는다. HiMQ는 국내 정보통신단체 표준으로 제정되면서 권고 파라미터를 제시하였는데, 이는 2020년 기준의 암호 분석에 기반한 파라미터로 최근 공격 기법들이 고려되지 않았다. 이에 본 논문에서는 HiMQ에 적용 가능한 다변수 이차식 기반 전자서명에 대한 공격 기법들을 살펴보고 이에 대한 안전성 분석을 수행하였다. HiMQ에 가장 효과적인 공격은 2022년 제안된 개선된 MinRank 공격인 combined attack이며, 세 개의 권고 파라미터 모두 기준 보안강도를 만족하지 못하였다. 또한 HiMQ-128과 HiMQ-160은 최소 보안강도인 128-bit 비도도 만족하지 못하였다.

ABSTRACT

Multivariate Quadratic (MQ)-based digital signature schemes have advantages such as ease of implementation and small signature sizes, making them promising candidates for post-quantum cryptography. To enhance the efficiency of such MQ-based digital signature schemes, utilizing sparse matrices have been proposed, including HiMQ, which has been standardized by Korean Telecommunications Technology Association standard. However, HiMQ shares a similar key structure with Rainbow, which is a representative MQ-based digital signature scheme and was broken by the MinRank attack proposed in 2022. While HiMQ was standardized by a TTA and recommended parameters were provided, these parameters were based on cryptanalysis as of 2020, without considering recent attacks. In this paper, we examine attacks applicable to MQ-based digital signatures, specifically targeting HiMQ, and perform a security analysis. The most effective attack against HiMQ is the combined attack, an improved version of the MinRank attack proposed in 2022, and none of the three recommended parameters satisfy the desired security strength. Furthermore, HiMQ-128 and HiMQ-160 do not meet the minimum security strength requirement of 128-bit security level.

Keywords: Post-Quantum Cryptography, MQ-based signature, Cryptanalysis

Received(08. 14. 2023), Modified(12. 18. 2023), Accepted(12. 19. 2023)

* 본 논문은 2023년도 정보보호학회 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임.

* 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2023-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발).

* 본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2021R1A2C1095591).

† 주저자, smcho3315@hanyang.ac.kr

‡ 교신저자, seosh77@hanyang.ac.kr(Corresponding author)

I. 서 론

다변수 이차식(MQ, Multivariate Quadratic) 기반 전자서명 알고리즘은 다변수 이차식 문제와 다항식의 확장 동형(EIP, Extended Isomorphism of Polynomials) 문제의 어려움에 기반한 서명 기법이다. 이중 다변수 이차식 문제는 NP-난해(NP-hard)이며, 양자 컴퓨터를 이용한 공격에도 평균적으로 지수적 어려움을 갖는다고 알려져 있다. 대표적인 다변수 이차식 기반 전자서명으로는 NIST 양자내성암호 표준화 프로젝트 3라운드의 최종 후보(finalist)였던 Rainbow[1]가 있다. Rainbow는 또 다른 다변수 이차식 기반 전자서명인 UOV (Unbalanced Oil and Vinegar) 서명 기법을 2계층 구조로 변형하여 키와 서명 크기를 줄이고 빠른 서명 생성을 가능하도록 하였다.

MQ 기반 전자서명의 효율성을 높이기 위한 또다른 방안은 희소 행렬 구조의 중앙맵을 사용하는 것이다. 희소 행렬을 사용하게 되면 키의 길이를 줄일 수 있을 뿐 아니라 서명 생성 속도를 높일 수 있다. 이러한 시도 중 하나가 NIST 양자내성암호 표준화 프로젝트의 1라운드 후보였던 HiMQ-3다. HiMQ-3는 Rainbow와 유사한 키 구조 및 서명 과정을 거치지만 개인키인 중앙맵을 희소 행렬 구조로 설정하여 효율성을 개선하였다. 이러한 HiMQ-3를 개선한 HiMQ[2]는 2020년 6월 국내 정보통신단체표준(TTA 표준) 양자내성암호로 제정되었다. HiMQ는 Rainbow와 유사한 키 구조를 가지며 2계층으로 구성되어 있다. 그러나 HiMQ나 Rainbow와 같이 2계층 구조의 다변수 이차식 기반 전자서명 기법의 안전성은 추가적으로 MinRank 문제의 어려움에 의존한다. 이러한 MinRank 문제를 풂으로써 개인키를 복원하는 것이 MinRank 공격 기법이며, 최근 Rainbow에 대한 효과적인 MinRank 공격들이 제안되었다. Ward Beullens는 2021년과 2022년 Rainbow에 대한 개선된 MinRank 공격 기법을 제안하면서 Rainbow의 파라미터들이 해당 보안강도를 만족하지 못함을 보였다[3, 4]. 특히 2022년 제안된 공격의 경우, 2라운드 Rainbow의 파라미터 I에 대해 53시간 만에 키를 복원하는 데 성공하였다. 이처럼 Rainbow에 대한 실질적인 키 복원 공격이 제안되면서 Rainbow는 NIST 양자내성암호 표준에 선정되지 못하였다.

2계층 구조의 다변수 이차식 기반 전자서명이 MinRank 공격을 통한 키 복원 공격에 취약함을 보이면서, 다시금 UOV와 같은 1계층 구조의 다변수 이차식 기반 전자서명이 주목받고 있다. Ward Beullens는 2021년 seed를 통해 키를 확장하는 방식으로 전체 키 크기를 줄인 UOV의 변형 전자서명 기법인 MAYO를 제안하였다. 국내에서는 UOV 기반에 HiMQ와 같은 희소 행렬을 중앙맵에 적용하여 키 크기와 서명 생성 성능을 개선한 MQ-Sign이 KpqC 공모전에 제안되었다. 그러나 2023년, Thomas Aulbach 등이 MQ-Sign의 희소 행렬 구조를 이용한 키 복원 공격을 제안하고[5], Yasuhiko Ikematsu 등이 개선된 서명 위조 공격을 제안[6]하면서 MQ-Sign의 안전성에 대한 의문이 제기되었다.

국내 정보통신단체 표준인 HiMQ는 Rainbow와 유사한 키 구조를 가지며 2계층 구조로 구성되어 있기에 MinRank 공격에 취약할 것으로 예상된다. 또한 MQ-Sign과 같이 중앙맵이 희소 행렬로 구성되어 있기에, MQ-Sign에 대한 키 복원 공격 및 서명 위조 공격에 대한 보안 분석이 필요하다. 이에 본 논문에서는 [5]와 [6]의 희소 행렬 구조 활용 공격에 대한 HiMQ 적용 가능성을 검토하고, [4]에서 제안한 키 복원 공격을 HiMQ에 적용하였을 때의 공격 비용을 추정해본다. 또한 이를 기반으로 HiMQ가 TTA 표준으로 제정될 시 제안하였던 권고 파라미터들의 보안 강도를 검증한다. 본 논문의 분석 결과에 의하면 [4]의 공격에 의해 HiMQ의 TTA 표준 문서에서 제안된 세 개의 권고 파라미터 중 두 개의 보안강도가 128-bits 이하로 떨어졌으며, 가장 높은 보안강도를 제공하는 파라미터가 192-bits 보안강도를 만족하지 못함을 보였다.

II. HiMQ

HiMQ[2]는 다변수 이차식 기반 전자서명 알고리즘으로, 2020년 6월 17일 국내 정보통신단체표준(TTA표준)으로 제정되었다. 국가수리과학연구소에서 NIST 양자내성암호 표준화 프로젝트에 제출한 HiMQ-3를 계승하였으며, 3계층 구조를 갖는 HiMQ-3와 달리 HiMQ는 Rainbow와 같은 2계층 구조를 갖는다. HiMQ의 개인키인 중앙 맵이 희소 행렬 구조를 갖는다는 것을 제외하고는 전체적인 키 생성, 서명 생성 및 검증 과정이 Rainbow와 유사하게 진행된다.

2.1 파라미터

HiMQ는 표수가 2인 유한체 $\mathbb{F}_q$ 상의 다변수 이차식 문제의 어려움에 기반하고 있으며, 다변수 이차식 문제는 총 n개의 변수(v개의 vinegar 변수 및 o_1+o_2개의 oil 변수, $n=v+o_1+o_2$)와 m개의 방정식 ($m=o_1+o_2$)으로 구성된다. 보안강도별 HiMQ의 권고 파라미터는 Table 1.과 같다.

Table 1. The recommended parameter sets of HiMQ (λ: the security length)

	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

2.2 키 생성

HiMQ는 역변환이 가능한 아핀 변환 $S:\mathbb{F}_q^m\to\mathbb{F}_q^m$와 $T:\mathbb{F}_q^n\to\mathbb{F}_q^n$의 역변환인 S^{-1}와 T^{-1}, 그리고 첫 번째와 두 번째 계층의 다변수 이차다항식으로 구성된 중앙 함수 $F=(F^{(1)},...,F^{(m)}):\mathbb{F}_q^n\to\mathbb{F}_q^m$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.

$$\begin{aligned}F^{(1)}(x_1,..,x_n)&=\Phi_1(x_1,..,x_v)+\delta_1x_{v+1}x_{v+2}\\F^{(2)}(x_1,..,x_n)&=\Phi_2(x_1,..,x_v)+\delta_2x_{v+2}x_{v+3}\\&\vdots\\F^{(o_1)}(x_1,..,x_n)&=\Phi_{o_1}(x_1,..,x_v)+\delta_{o_1}x_{v+o_1}x_{v+1}\end{aligned}\quad(1)$$

$$\Phi_i=\sum_{1\le i<j}^{v}\alpha_{i,j}x_ix_j\quad(2)$$

$$\begin{aligned}F^{(o_1+1)}(x_1,..,x_n)&=\Psi_1(x_1,..,x_{v+o_1})\\&+\Theta_1(x_1,..,x_n)+\epsilon_1x_{o_1+1}+c_1\\&\vdots\\F^{(o_1+o_2)}(x_1,..,x_n)&=\Psi_{o_2}(x_1,..,x_{v+o_1})\\&+\Theta_{o_2}(x_1,..,x_n)+\epsilon_{o_2}x_{o_1+o_2}+c_{o_2}\end{aligned}\quad(3)$$

$$\Psi_i=\sum_{j=1}^{v+o_1}\beta_{i,j}x_jx_{(i+j-1)(\mathrm{mod}\,v+o_1)+1}\quad(4)$$

$$\Theta_i=\sum_{j=1}^{v+o_1}\gamma_{i,j}x_jx_{v+o_1+1+(j-i)(\mathrm{mod}\,o_2)}\quad(5)$$

Fig. 1.은 $v=6$, $o_1=5$, $o_2=4$일 때 HiMQ의 1계층에서의 중앙맵을, Fig. 2.는 2계층에서의 중앙맵을 보여준다. Fig. 1, 2.와 같이 HiMQ는 중앙맵이 희소 행렬로 구성된다.

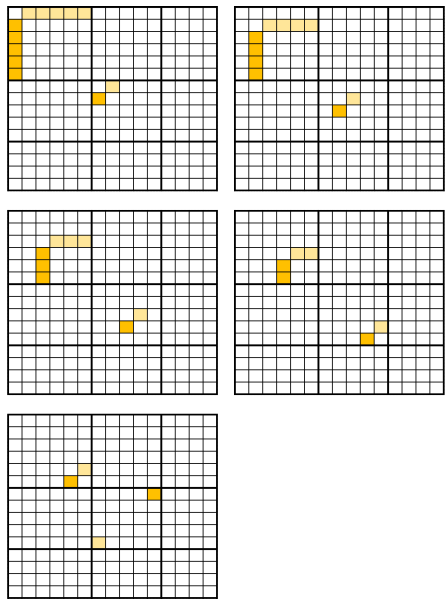

Fig. 1. The sparse central map of HiMQ's first layer when $v=6$, $o_1=5$, and $o_2=4$

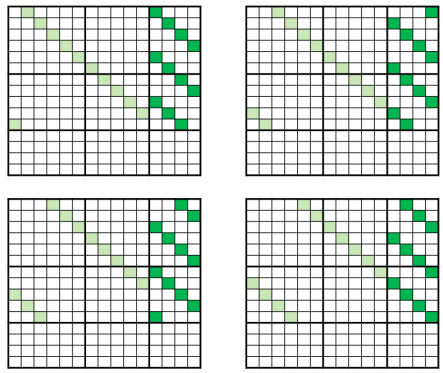

Fig. 2. The sparse central map of HiMQ's second layer when $v=6$, $o_1=5$, and $o_2=4$

2.3 서명 생성

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 $\begin{cases}\delta_1 x_{v+1}x_{v+2}=\zeta_1-\Phi_1(s_v)\\ \vdots\\ \delta_{o_1}x_{v+o_1}x_{v+1}=\zeta_{o_1}-\Phi_{o_1}(s_v)\end{cases}$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

2.4 서명 검증

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

III. HiMQ 적용 가능 공격

HiMQ는 2계층 구조로 구성되며 공개키가 두 개의 아핀 변환과 중앙맵의 합성으로 구성된다는 점에서 Rainbow와 유사한 키 구조를 갖는다. 따라서 [4]에서 제안한 공격을 적용할 수 있으며, 이에 대한 안전성 분석이 필요하다. 또한 개인키인 중앙맵이 MQ-Sign과 같은 희소 행렬로 구성되기 때문에 [5]과 [6]의 희소 행렬 구조 특성 기반 공격에 대한 적용 가능성을 검토할 필요가 있다. 본 장에서는 [4], [5], [6]에서 제안된 공격에 대한 HiMQ 적용 가능성을 검토한다.

3.1 Simple Attack

O_1'을 첫 $n-m$개의 원소가 0인 $\mathbb{F}_q^n$ 상의 벡터 부분 공간이고, O_2'를 첫 $n-o_2$개의 원소가 0인 $\mathbb{F}_q^n$ 상의 벡터 부분 공간, W'를 첫 o_1개의 원소가 0인 $\mathbb{F}_q^m$ 상의 벡터 부분 공간이라 하자. 이들 부분 공간과 개인키 S와 T로 구성된 선형 부분 공간 $O_1=T^{-1}O_1'$, $O_2=T^{-1}O_2'$, $W=S^{-1}W'$는 공개키 P에 대해 Fig. 3.과 같은 매핑 관계를 갖는다. 이때 simple attack은 O_2를 W로 매핑하는 D_{x}를 추정한다.

$$D_{\mathrm{x}}=\mathbb{F}_q^n\to\mathbb{F}_q^m:\mathrm{y}\mapsto P'(\mathrm{x},\mathrm{y}) \tag{6}$$

이때 $\mathrm{x}\in\mathbb{F}_q^n$는 임의의 벡터이며, $\mathrm{o}_2\in O_2$이다. $\dim(O_2)=\dim(W)=o_2$이므로, D_{x}가 O_2에서 커널 벡터를 가지는 확률은 $\mathbb{F}_q$ 상의 임의의 $o_2\times o_2$ 행렬이 특이(singular)일 확률과 동일하다. 행렬은 첫 번째 행이 비영(non-zero)인 경우 비특이(non-singular)이며, 각각의 $i<o_2$에 대해 $i+1$번째 행이 처음 i개의 행의 span에 존재하지 않는다. 이에 대한 확률은 q^{i-1-o_2}이다. 따라서 충분히 큰 q의 경우에는 o_2와 무관하게 $1/q$에 가까워진다.

$$1-\prod_{i=0}^{o_2-1}\left(1-q^{i-o_2}\right) \tag{7}$$

[4]에서 제안한 공격은 단순히 임의의 비영인 x를 선택하고 이때 D_{x}의 커널과 O_2가 자명하지 않게

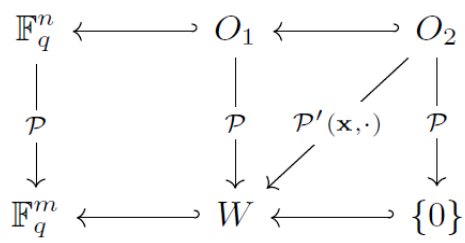

Fig. 3. The structure of HiMQ private keys

(non-trivial) 교차(intersect)한다면, 이 교차점에서 벡터 o를 찾게 된다. 이때 모든 $o \in O_2$에 대해 $P(o)=0$이므로, 다음 시스템을 해결한다.

$$\begin{cases} D_x o = 0 \\ P(o) = 0 \end{cases} \tag{8}$$

시스템 (8)은 o개의 변수에 대한 m개의 동차(homogeneous) 선형 방정식과 m개의 동차 이차 방정식으로 구성된다. 이때 m개의 선형 방정식을 풀게 되면, m개의 변수에 대한 해를 구할 수 있으며, 이차 방정식은 $n-m$개의 변수에 대한 m개의 동차 방정식으로 이루어진 시스템이 된다. 열들이 D_x의 커널의 기저로부터 형성된 행렬 $B \in \mathbb{F}_q^{n-m}$에 대해, $\tilde{P}(y) := P(By)$이며, $\tilde{P}(y)$의 해 $y \in \mathbb{F}_q^{n-m}$를 찾음으로써 개인키를 복원할 수 있다.

3.2 Combined Attack

Simple attack은 vinegar 변수의 개수가 작은 파라미터에 대해서는 효율적이지만, Rainbow의 파라미터 세트 III($v_1=68, o_1=32, o_2=48$)과 V($v_1=96, o_1=36, o_2=64$)와 같이 vinegar 변수의 개수가 크다면 rectangular MinRank 공격보다 효율적이지 않다. 이에 rectangular MinRank 공격에 simple attack의 D_x 추정 기법을 결합하여 공격의 효율성을 높인 combined attack이 제안되었다. 좋은 D_x를 추정함으로써 MinRank 문제의 instance를 $n-m$개의 $(n-1)\times m$ 행렬로 축소시킬 수 있으며, 이러한 MinRank 문제를 풀게 되면, 개인키를 효율적으로 복원할 수 있다. 본 논문의 분석 결과에 따르면 각각 66, 68개의 vinegar 변수를 갖는 HiMQ-160과 HiMQ-192 역시 combined attack에 취약한 것으로 나타났다.

3.3 Aulbach 등의 MQ-Sign 키 복원 공격

Aulbach 등은 MQ-Sign에 대한 다항 시간 내의 키 복원 공격을 제안하였다[5]. 그들이 제안한 공격은 MQ-Sign의 중앙맵 중 vinegar-oil 부분(F_{OV})이 희소 행렬 구조일 때 개인키를 감추는 기반 문제인 다항식의 확장 동형성(EIP) 문제를 다항 시간 내에 풂으로써 개인키 T를 복원한다. 그러나 이 공격은 비밀 값인 중앙맵 F가 희소행렬로 구성되고, 아핀 맵 T가 [7]에서 제안된 것과 같이 효율성을 위한 동등한 키 변형 구조(수식 (9))일 때, 이 특성에 기반한 공격이다. 따라서 랜덤한 아핀맵을 사용하는 HiMQ에는 적용이 힘들다. MQ-Sign 역시 효율성을 위해 구현코드에서는 동등키를 사용하였지만, 공격이 제안된 이후로 구현 코드는 랜덤 아핀 맵을 사용하도록 업데이트되었다.

$$\begin{pmatrix} P_1^{(k)} & P_2^{(k)} \\ 0 & P_4^{(k)} \end{pmatrix} = \begin{pmatrix} I & 0 \\ S_1^T & I \end{pmatrix} \begin{pmatrix} F_1^{(k)} & F_2^{(k)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} I & S_1 \\ 0 & I \end{pmatrix} \tag{9}$$

3.4 Ikematsu 등의 MQ-Sign 서명 위조 공격

간단한 구조의 개인키 S를 갖는 MQ-Sign-RS와 MQ-Sign-SS에 대한 키 복원 공격을 제안한 [5]와 달리, Yasuhiko Ikematsu 등은 일반적인 개인키 S에도 적용 가능한 서명 위조 공격을 제안하였다.

그들은 MQ-Sign의 중앙맵이 희소 행렬 구조의 특성을 활용한 서명 위조 공격을 시도하였다. 그들의 공격은 아핀 맵 T와 중앙맵 F의 합성으로 이루어진 공개키 P에 대해 $Px=0$을 만족하는 해를 찾음으로써 서명을 위조한다. 이때 중앙맵 F가 희소행렬로 구성됨에 따라 x를 빠르게 찾을 수 있으며, 이로 인해 희소 행렬로 구성된 중앙맵의 사용이 안전성에 문제가 있을 수 있음을 제기하였다. 그러나 MQ-Sign의 중앙맵 P가 F와 T 두 행렬의 합성으로 이루어진 것과 달리 HiMQ는 F, S, T 세 개의 행렬의 합성으로 이루어지며, i번째 중앙맵 F_i가 공개키 전체에 영향을 미치기 때문에 [6]의 공격은 HiMQ에 직접 적용하는데에 한계가 있다.

IV. HiMQ 보안강도 분석

HiMQ는 중앙맵을 희소 행렬로 구성하는 부분을 제외하고 Rainbow와 키 구조가 거의 유사하다.

HiMQ는 중앙맵이 희소 행렬임을 제외하고 Rainbow와 키 구조 및 생성 방법이 거의 유사하다. 따라서 HiMQ 또한 Rainbow에 대한 combined attack이 적용될 수 있으며, 이에 취약할 것으로 예상된다. 또한 TTA에 제출된 HiMQ의 권고 파라미터는 2020년의 안전성 분석에 기반하여 설정되었기 때문에, 이러한 개선된 MinRank 공격

에 대한 보안 강도 분석을 통해 파라미터 안전성 검증을 수행하고 보안강도를 검증하는 것이 시급하다. 본 장에서는 HiMQ에 combined attack을 적용할 때 소요되는 공격 비용을 분석하고, 이를 기반으로 HiMQ 권고 파라미터의 보안강도를 검증한다. HiMQ의 유한체 크기를 q, 전체 변수의 개수를 n, oil 변수의 개수를 m이라 할 때, simple attack과 combined attack 각각의 공격 비용은 Table 2.와 같다.

Table 2. The cost for the simple attack and combined attack against HiMQ

parameter set	Simple attack	Combined attack
HiMQ-128	97	95
HiMQ-160	194	124
HiMQ-192	187	131

4.1 Simple Attack

HiMQ의 유한체 크기를 q, 전체 변수의 개수를 n, oil 변수 개수를 m, 두 번째 레이어의 oil 변수 개수를 o_2라 할 때, HiMQ에 대한 simple attack의 전체적인 공격 비용 산출 방법은 Fig. 4.의 알고리즘과 같다.

HiMQ에 대한 simple attack은 공개키에 대한 차분 선형 사상 D_{x}를 추정한 후, XL 알고리즘을 통해 이차 시스템을 해결하여 개인키를 복원한다. 이때 선형 사상 D_{x}의 추정 확률 $p_{D_{\mathrm{x}}}$는 수식 10과 같다.

Algorithm 1 Calculation of simple attack cost for HiMQ

Input: q, n, m, o_2

Output: Simple attack cost c for HiMQ

1: Probability $p_{D_{\mathrm{x}}}$ of estimating the linear mapping D_{x}

$$p_{D_{\mathrm{x}}} = 1 - \prod_{i=0}^{o_2-1}\left(1 - q^{i-o_2}\right)$$

2: Solving quadratic systems using the XL algorithm

- For the degree D of non-positive smallest integer term in the power series expansion of $\frac{(1-t^2)^{m-1}}{(1-t)^{n-m-1}}$

$$ec_{XL} = 3\binom{(n-m-1)-1+D}{D}^2\binom{(n-m-1)+1}{2}$$

3: Cost $gates_M$ of multiplication over $\mathbb{F}_q$

$$gates_M = 2\left((\log_2 q)^2 + \log_2 q\right)$$

4: Return the total attack cost $c = ec_{XL} \times gates_M / p_{D_{\mathrm{x}}}$

Fig. 4. The algorithm for calculating simple attack cost for HiMQ

$$p_{D_{\mathrm{x}}} = 1 - \prod_{i=0}^{o_2-1}\left(1 - q^{i-o_2}\right) \tag{10}$$

고정된 비영인 x에 대해, O_2로 제한된 $D_{\mathrm{x}}|O_2$는 O_2에서 W로의 균일한 무작위 선형 맵이다. 이때 $\dim(O_2) = \dim(W) = o_2$이며, D_{x}가 O_2에서 커널 벡터를 가지는 확률은 $\mathbb{F}_q$ 상의 임의의 o_2-by-o_2 행렬이 특이(singular)일 확률과 동일하다. 행렬은 첫 번째 행이 비영인 경우 비특이(non-singular)이며, 각각의 $i < o_2$에 대해 $i+1$번째 행이 처음 i개의 행이 span에 존재하지 않을 확률이 q^{i-1-o_2}이다. 따라서 특이일 확률은 수식 (10)과 같다. 충분히 큰 q의 경우에는 o_2와 무관하게 $1/q$에 가까워진다.

이를 통해 $n-m$개의 변수에 대한 m개의 동차 선형 방정식으로 이루어진 시스템으로 줄게 되고, 이 시스템을 XL 알고리즘[8]으로 푸는 복잡도가 다음과 같다.

$$3\binom{(n-m-1)-1+D}{D}^2\binom{(n-m-1)+1}{2} \tag{11}$$

이때 D는 XL의 operating degree로, $n-m$개의 변수에 대한 m개의 선형 방정식에 대해 $\frac{(1-t^2)^{m-1}}{(1-t)^{n-m-1}}$의 멱급수 전개(power series expansion)에서 계수가 양수가 아닌 가장 작은 정수인 항의 차수(t^D)이다.

HiMQ에 대한 simple attack의 비용은 (XL 알고리즘을 통한 시스템을 푸는데 필요한 곱셈 횟수) $\times$ ($\mathbb{F}_q$ 상에서의 곱셈 비용 $gates_M$)/(D_{x} 추정 확률 $p_{D_{\mathrm{x}}}$)이다. 이러한 분석에 기반한 HiMQ 파라미터별 키 복원 공격의 전체 비용은 Table 3.과 같다.

Table 3. The cost for the simple attacks against HiMQ parameters

parameter set	(q, n, m, o_2)	total cost $(\log_2)$
HiMQ-128	(256, 82, 45, 24)	97
HiMQ-160	(256, 134, 68, 33)	194
HiMQ-192	(512, 140, 72, 35)	188

4.2 Combined Attack

HiMQ의 유한체 크기를 q, 전체 변수의 개수를 n, oil 변수 개수를 m, 두 번째 레이어의 oil 변수 개수를 o_2라 할 때, HiMQ에 대한 combined attack의 전체적인 공격 비용 산출 방법은 Fig. 5.의 알고리즘과 같다.

HiMQ에 대한 combined attack의 공격 비용을 추정하기 위해서 먼저 개인키 부분 공간 $O_2 \subset \mathbb{F}_q^n$를 $W \subset \mathbb{F}_q^m$로 매핑하는 선형 사상 D_{x}를 성공적으로 추정할 확률 $p_{D_{\mathrm{x}}}$은 다음과 같다.

$$p_{D_{\mathrm{x}}} = 1 - \prod_{i=0}^{o_2-1}\left(1 - q^{i-o_2}\right) \tag{12}$$

D_{x}를 추정한 후, HiMQ에 대한 MinRank 문제의 instance는 $n-m$개의 $(n-1)\times m$ 행렬로 축소되며, 이때 이 행렬들의 선형결합의 랭크 r이 최대 o_2가 되도록 하는 벡터를 찾게 된다. 이는 [3]에서의 rectangular MinRank 공격 대비 적은 복잡도 만으로 공격이 가능하게 한다.

이러한 MinRank 문제는 Magali Bardet 등이 2020년 제안한 support-minors 알고리즘[9]을 활용하여 가장 효율적으로 풀 수 있다. support-minors 알고리즘은 동작 차수 b(본 논문의 경우, $1 \le b \le 4$로 제한)에 대하여 다음 부등식을 만족하는 가장 작은 m값 m'을 찾는다.

$$\binom{m}{r}\binom{n-m+b-2}{b} - 1 \le \sum_{i=1}^{b}(-1)^{i+1}\binom{m}{r+i}\binom{n+i-1}{i}\binom{n-m+b-i-2}{b-i}$$

이때 MinRank instance 행렬의 크기는 $(n-1)\times m'$으로 다시 한번 축소될 수 있으며, 가능한 m'의 범위가 $r+1$에서 m까지로 제한되기 때문에 위 부등식을 만족하는 가장 작은 m'을 찾는 복잡도는 negligible하다. 결과적으로 MinRank 문제를 푸는 비용은 ec_{MR}번의 $\mathbb{F}_q$ 상의 곱셈 비용과 같다.

$$ec_{MR} = 3(n-m-1)(r+1)\binom{m'}{r}^2\binom{n-m+b-2}{b}^2$$

본 논문에서는 $1 \le b \le 4$에 대해 각각의 경우에 해당하는 m'을 찾은 후, ec_{MR}을 최소로 하는 (b, m') 쌍을 선택하였다. Table 4.는 HiMQ 파라미터 별 선택한 (b, m') 쌍과 이에 대한 MinRank 공격 비용을 보여준다.

MinRank 문제를 푸는 비용은 $\mathbb{F}_q$ 상의 곱셈 비용으로 표현되며, 이는 사용되는 게이트 수로 계산이 가능하다. 본 논문에서는 [3]에서와 같이 $\mathbb{F}_q$ 상의 곱셈의 비용을 $gates_M = 2\left((\log_2 q)^2 + \log_2 q\right)$로 추정하는 모델을 기준으로 분석한다.

최종적으로 HiMQ의 키를 복원하는데 필요한 비용은 (MinRank 공격시 곱셈 횟수 ec_{MR})×($\mathbb{F}_q$ 상에서의 곱셈 비용 $gates_M$)/(D_{x} 추정 확률 $p_{D_{\mathrm{x}}}$)이

Algorithm 2 Calculation of combined attack cost for HiMQ

Input: q, n, m, o_2

Output: Combined attack cost c for HiMQ

1: Probability $p_{D_{\mathrm{x}}}$ of estimating the linear mapping D_{x}

$$p_{D_{\mathrm{x}}} = 1 - \prod_{i=0}^{o_2-1}\left(1 - q^{i-o_2}\right)$$

2: Performing MinRank attack using the support-minors algorithm

- For $1 \le b \le 4$, searching for the minimum value of m, denoted as m', that satisfies the following inequality.

$$\binom{m}{r}\binom{n-m+b-2}{b} - 1 \le \sum_{i=1}^{b}(-1)^{i+1}\binom{m}{r+i}\binom{n+i-1}{i}\binom{n-m+b-i-2}{b-i}$$

- Deriving the pair (b, m') that minimizes the MinRank attack cost ec_{MR}

$$ec_{MR} = 3(n-m-1)(r+1)\binom{m'}{r}^2\binom{n-m+b-2}{b}^2$$

3: Cost $gates_M$ of multiplication over $\mathbb{F}_q$

$$gates_M = 2\left((\log_2 q)^2 + \log_2 q\right)$$

4: Return the total attack cost $c = ec_{MR} \times gates_M / p_{D_{\mathrm{x}}}$

Fig. 5. The algorithm for calculating combined attack cost for HiMQ

Table 4. The attack parameters and cost for the support-minors algorithms against HiMQ

parameter sets	b	m'	cost $(\log_2)$
HiMQ-128	3	31	80.1
HiMQ-160	3	44	109.5
HiMQ-192	2	49	113.7

Table 5. The total cost for the key recovery attacks against HiMQ parameters

parameter set	(q, n, m, o_2)	total cost $(\log_2)$
HiMQ-128	(256, 82, 45, 24)	95.1
HiMQ-160	(256, 134, 68, 33)	124.5
HiMQ-192	(512, 140, 72, 35)	130.7

다. 이러한 분석에 기반한 HiMQ 파라미터별 키 복원 공격의 전체 비용은 Table 5.와 같다.

4.3 HiMQ 보안강도

simple attack은 $n-m$이 작은 경우에 효율적인 공격이다. 따라서 [4]에서도 Rainbow 파라미터 I일 때는 combined attack보다 simple attack이 더 효율적이다. 그러나 본 논문의 분석 결과에 따르면 HiMQ의 경우 모든 파라미터 세트에서 combined attack이 효과적일 뿐 아니라, HiMQ-160의 공격 비용이 HiMQ-192의 공격 비용보다 많이 소요되는 것을 확인하였다. 이는 HiMQ-160의 경우 $n-m$이 66일 때 m이 68로 두 값의 차이가 크지 않기 때문이다. 실제로 동일한 $n-m$ 값에 대해서 m 값이 작아질수록 복잡도가 증가한다. 또한 파라미터 I에서 simple attack이 효율적이었던 Rainbow와 달리 HiMQ는 파라미터 I에서도 combined attack이 효율적이었다. 이는 공격 파라미터인 D가 Rainbow에서는 6, 7인 반면 HiMQ는 12로 상당히 큰 값으로 인한 결과이다. 추가적으로 비슷한 $n-m$에 대해 HiMQ가 훨씬 작은 m을 갖는다.

V. 결 론

본 논문에서는 sparse 행렬로 구성된 중앙맵을 사용하는 MQ 기반 전자서명인 HiMQ에 대해 적용 가능한 공격 기법들을 검토하고, 적용 가능성 및 공격 복잡도를 분석하였다. HiMQ의 경우, [4]의 combined attack이 가장 효율적인 공격이었으며, 모든 파라미터가 기준 보안강도를 만족하지 못함을 보였다.

References

[1] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," International Conference on Applied Cryptography and Network Security (ACNS), pp. 164-175, June 2005.

[2] Korea Telecommunications Technology Association, "Post Quantum Cryptography based on Multivariate Quadratic Equations - Part 2: HiMQ, Digital Signature Algorithm with Appendix," TTAK.KO-12.0348-Part2, June 2020.

[3] W. Beullens, "Improved cryptanalysis of UOV and Rainbow," Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 348-373, Oct. 2021.

[4] W. Beullens, "Breaking rainbow takes a weekend on a laptop," Annual International Cryptology Conference (CRYPTO), pp. 484-479, Aug. 2022.

[5] T. Aulbach, S. Samardjiska, and M. Trimoska, "Practical key-recovery attack on MQ-Sign," Cryptology ePrint 2023/432, 2023.

[6] Y. Ikematsu, H. Jo, and T. Yasuda, "A security analysis on MQ-Sign," Cryptology ePrint 2023/581, 2023.

[7] A. Petzoldt, "Selecting and Reducing Key Sizes for Multivariate Cryptography," Ph.D. Thesis, Darmstadt University of Technology, Germany, July 2013.

[8] C-M. Cheng, T. Chou, R. Niederhagen, and B-Y. Yang, "Solving Quadratic Equations with XL on Parallel Architectures," International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp. 356-373, Sep. 2012.

[9] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J-P. Tillich, and J. Verbel,

"Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems," International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 507-536, Dec. 2020.

〈저자소개〉

조 성 민 (Seong-Min Cho) 학생회원
2019년 2월: 한양대학교 ERICA 캠퍼스 전자공학부 졸업
2019년 3월~현재: 한양대학교 전자공학과 석박사통합과정
〈관심분야〉 IoT 보안, 임베디드 시스템 보안, 양자 내성 암호

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