*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.211

# 양자컴퓨터에 안전한 짧은 비밀키를 갖는 효율적인 다변수 이차식 기반 전자서명 알고리즘 설계*

심 경 아†‡
국가수리과학연구소 (공공기반연구본부 본부장)

# An Efficient Post-Quantum Signature Scheme Based on Multivariate-Quadratic Equations with Shorter Secret Keys*

Kyung-Ah Shim†‡
National Institute for Mathematical Sciences
(Director of Fundamental Research on Public Agenda Divison)

## 요 약

다변수 이차식 기반 암호알고리즘은 양자컴퓨터에 안전하다고 믿어지는 수학적 난제에 기반을 둔 공개키 암호알고리즘 중의 하나로 현재 사용하고 있는 공개키 암호를 대체할 수 있는 양자내성암호 중의 하나이다. NIST 양자내성암호 공모 3라운드 최종 후보 알고리즘으로 선정되었던 다변수 이차식 기반 전자서명 알고리즘 Rainbow의 다중 레이어를 사용하는 구조에 대한 진화된 공격이 대두된 후에 단일 레이어를 이용하는 UOV의 구조에 관심이 집중되고 있다. 본 논문에서는 단일 레이어를 갖는 UOV 구조를 유지하면서 일차식의 특별한 구조, 희소 다항식, 랜덤 다항식의 다양한 조합을 통해 비밀키의 길이를 대폭 줄이고, 블록 부분 행렬의 역행렬을 이용하여 선형 시스템의 해를 구하는 방법을 적용한 효율적인 다변수 이차식 기반 전자서명 알고리즘을 제안한다. 제안한 전자서명의 안전성 분석을 통해 안전한 파라미터를 설정하고 각 파라미터에서의 키길이와 서명 길이를 비교 분석한다. 제안한 다변수 이차식 기반 전자서명 알고리즘은 서명의 길이가 양자내성 전자서명 중 가장 짧고, 기존 다변수 이차식 기반 전자서명에 비해 비밀키 길이가 최대 97%의 축소 효과를 가진다.

## ABSTRACT

Multivariate quadratic equations (MQ)-based public-key cryptographic algorithms are one of promising post-quantum replacements for currently used public-key cryptography. After selecting to NIST Post-Quantum Cryptography Standardization Round 3 as one of digital signature finalists, Rainbow was cryptanalyzed by advanced algebraic attacks due to its multiple layered structure. The researches on MQ-based schemes are focusing on UOV with a single layer. In this paper, we propose a new MQ-signature scheme based on UOV using the combinations of the special structure of linear equations, spare polynomials and random polynomials to reduce the secret key size. Our scheme uses the block inversion method using half-sized block matrices to improve signing performance. We then provide security analysis, suggest secure parameters at three security levels and investigate their key sizes and signature sizes. Our scheme has the shortest signature length among post-quantum signature schemes based on other hard problems and its secret key size is reduced by up to 97% compared to UOV.

**Keywords:** Linear equation, multivariate quadratic equation, post-quantum signature, sparse polynomial, UOV

Received(02. 16. 2023), Modified(03. 13. 2023), Accepted(03. 13. 2023)

* 이 논문은 과학기술정보통신부(B23710000) 지원으로 수행하였습니다.

* This research is supported by the National Institute for Mathematical Sciences funded by Ministry of Science and ICT of Korea (B23710000).

† 주저자, hong@kashim@nims.re.kr

‡ 교신저자, kashim@nims.re.kr(Corresponding author)

## I. 서 론

양자컴퓨팅 기술의 발전으로 머지않은 미래에 양자컴퓨터의 등장이 가시화됨에 따라 현재 사용하고 있는 공개키 암호알고리즘의 붕괴를 예고하고 있다. 현재 국제표준 공개키 암호인 RSA와 ECDSA 등의 안전성은 소인수분해문제 및 이산대수문제에 기반을 두고 있는데, 큰 규모의 양자컴퓨터 개발이 완료되면 Shor 알고리즘[1]에 의해 이 난제들은 쉽게 풀리고, 국제표준 공개키 암호도 실시간 해독이 가능해져 사용할 수 없게 된다는 것이 알려져 있다. 양자내성암호 (Post-Quantum Cryptography)의 정의는 현재의 컴퓨터를 이용한 공격과 양자컴퓨터를 이용한 공격에 모두 안전한 수학적 난제의 어려움에 기반한 공개키 암호알고리즘을 의미한다. 양자내성암호는 기반이 되는 수학적 난제에 따라 다변수 이차식 기반, 격자 기반, 코드 기반, 해시 함수 기반, 아이소제니 기반으로 나누어져 활발하게 연구가 진행되고 있다.

다변수 이차식 기반 양자내성암호는 유한체에서 정의된 다변수 이차식 시스템의 해를 구하는 문제의 어려움에 기반을 둔 공개키 암호로 이차 다항식의 특성 상 일대일 함수가 아니어서 암호화 알고리즘 설계가 어려운 구조여서 주로 전자서명 알고리즘이 연구되고 있다. 가장 검증이 오래된 다변수 이차식 기반 전자서명 알고리즘은 UOV 서명으로 단일 레어어 구조를 이용하여 설계되어 있다[2] 2005년 Ding과 Schmidt은 UOV 서명을 일반화한 Rainbow를 제안하였는데, Rainbow 서명은 다중 레이어를 이용하여 키의 길이를 줄이고 서명 생성/검증 속도를 개선하였다[3]. UOV는 $P=F\circ T$의 구조를 Rainbow는 $P=S\circ F\circ T$의 구조를 사용하여 비밀키를 숨기고, 다변수 이차식의 시스템의 해를 찾아 서명을 가능하게 하는 특수한 형태의 $F$를 사용한다. $F$의 특수한 구조를 숨기기 위해 역변환이 가능한 아핀 맵 $S$와 $T$를 적용하여, $S$는 다중 레이어에서 식을 섞어주는 역할을 $T$는 변수를 섞어주는 역할을 수행하여, 결국 공개키가 랜덤한 다변수 이차식의 시스템과 구분 불가능하게 만들어 주게 된다. 이 다변수 이차식 기반 전자서명 알고리즘들은 작은 유한체를 사용하여 구현이 용이하고, 전자서명의 길이가 짧고, 서명 생성/검증 성능이 우수하다는 장점이 있지만 키길이가 크다는 단점이 있다.

Rainbow가 NIST 양자내성암호 공모 3라운드 최종 후보 알고리즘으로 선정된 이후 다중 레이어 구조를 이용한 Rainbow-Band- Separation 공격, MinRank 공격 등 진화된 공격들이 발표 되었고[4,5,6,7,8], Ward의 simple 공격으로 NIST 2라운드 제출 안전도 1의 파라미터가 랩탑에서 53 시간 만에 깨지는 결과가 발표되었다[9]. 이에, Rainbow 개발 팀은 안전도 3과 5의 파라미터를 각각 안전도 1과 3의 파라미터로 변경하겠다고 발표하였다[10], 파라미터의 변경으로 Rainbow는 안전성은 확보하였지만 단일 레이어 기반 UOV와 비교했을 때 효율성이 떨어져 장점이 사라져 UOV의 구조를 이용한 연구에 관심이 집중되고 있다.

UOV와 Rainbow의 키길이 축소에 관한 연구는 꾸준히 이루어져 왔다. 비밀키 혹은 공개키 축소를 위해 공개키의 일부 혹은 전체 비밀키를 작은 크기의 랜덤한 시드(seed)로 대체하는 CyclicUOV, Cyclic Rainbow[11], CompressedRainbow[12], 부분체 $F_2$에서 비밀키를 선택하는 Lifted UOV(LUOV)[13,12], 순환 행렬(circulant matrix) 또는 토플리츠 행렬(Toeplitz matrix)을 이용한 Circulant-UOV[14], Circulant-Rainbow[15], Block-anti-circulant UOV(BAC-UOV)[16]가 제안되었다. 이러한 전자서명 알고리즘들은 비밀키가 축소되면, 공개키 길이가 늘어나거나, 공개키를 축소하면 서명 크기가 늘어나고, 서명 혹은 검증의 성능이 크게 떨어지는 희생을 치러야했다.

이런 전자서명 알고리즘들에 대한 공격들도 발표되었다. Circulant-UOV와 Circulant-Rainbow는 순환 행렬의 특성을 이용한 Kipnis-Shamir 공격으로 완전히 깨졌고[17], LUOV는 공격이 제안되어 210분 이내에 서명을 위조가 가능하다는 것이 알려졌다[18]. Furue 등은 BAC-UOV의 구조적 공격을 제안하여 이전 공격에 비해 공격 복잡도가 감소한다는 것을 보였다[19]. 이런 전자서명 알고리즘들은 공개키의 일부 혹은 전체가 순환 행렬과 토플리츠 행렬로 구성되어 있어, 공개키 자체가 랜덤 시스템과 구별이 가능하여 랜덤 시스템과 거의 구별 불가능한 공개키를 만드는 원칙에 반하는 것이다. 결과적으로, 공개키 크기와 빠른 성능을 모두 유지하면서 비밀키 크기 축소에 성공한 결과는 거의 찾아볼 수가 없다.

본 논문에서는 단일 레이어를 갖는 UOV 구조를 유지하면서 일차식의 특별한 구조, 희소 다항식, 랜덤 다항식의 다양한 조합을 통해 비밀키의 길이를 대폭 줄이고, 블록 부분 행렬의 역행렬을 이용하여 선

형 시스템의 해를 구하는 방법을 적용한 효율적인 다변수 이차식 기반 전자서명 알고리즘을 제안한다. 제안한 전자서명의 안전성 분석을 통해 안전한 파라미터를 설정하고 각 파라미터에서의 키길이와 서명 길이를 비교 분석한다.

## II. Preliminaries

이 절에서는 가장 잘 알려진 단일 레이어 다변수 이차식 기반 전자서명 알고리즘 UOV를 소개한다[2].

먼저, 인덱스 $n$을 두 개의 집합 $V=\{1,...,v\}$와 $O=\{v+1,...,v+o\}$로 나누어, $|V|=v$, $|O|=o$, $n=v+o$을 만족하도록 $o, v$를 선택한다. 이 때, $V$를 Vinegar 변수, $O$를 Oil 변수라고 부른다. $n$개의 변수 $x_1,...,x_n$를 가지는 $o$개의 이차 다항식 $F^{(1)}, \dots, F^{(o)}$으로 이루어진 중앙 함수 $F=(F^{(1)},...,F^{(o)}) : F_q^n \rightarrow F_q^o$를 다음과 같이 생성한다.

$$F^{(k)}(x_1,...,x_n) = \sum_{i,j\in V, i\le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i\in O, j\in V} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O} \gamma_i^{(k)} x_i + c^{(k)} \quad (1)$$

이 때, $\alpha_{ij}^k, \beta_{ij}^k, \gamma_{ij}^k \ (k=1,..,o)$는 유한체 $F_q$의 임의의 원소를 선택한다. 수식 (1)은 Oil×Oil 인덱스의 이차항이 없는 구조로 Vinegar 변수에 상수를 대입하면 이차식의 시스템이 일차식의 시스템으로 전환되어 해를 찾을 수 있게 된다. 이런 다항식의 특수한 형태가 이차식의 시스템의 해를 찾는 것을 가능하게 해주는 핵심 구조가 된다.

각 이차 다항식 $F^{(k)}$는 아래의 식

$$F^{(k)} = F_V^{(k)} + F_{OV}^{(k)} + F_{L,C}^{(k)} \quad (2)$$

과 같이 표현할 수 있는데, 여기서 $F_V^{(k)}$, $F_{OV}^{(k)}$는 Vinegar×Vinegar 이차항 부분과 Vinegar×Oil 이차항 부분이고 $F_{L,C}^{(k)}$는 일차항과 상수항 부분이이다. 이차식 부분 $F_V^{(k)}, F_{OV}^{(k)}$의 선택 방법에 따라 비밀키의 크기를 줄이고 효율적인 서명 생성이 가능하다.

### 2.1 UOV 키생성 알고리즘

안전도 파라미터가 입력 값으로 주어지면 공개키와 비밀키 쌍을 출력해 주는 키생성 알고리즘은 다음과 같다.

- 비밀키 $F=(F^{(1)},...,F^{(o)})$ 생성: 중앙 함수 $F=(F^{(1)},...,F^{(o)})$를 식 (1)과 같이 생성한다.
- 비밀키 $T$ 생성: 역행렬이 존재하는 아핀 맵 $T: F_q^n \rightarrow F_q^n$를 유한체 $F_q$에서 랜덤하게 선택한다.
- 공개키 생성: $P=F\circ T$를 계산하여 공개키 $P$를 생성한다.

### 2.2 UOV 서명 생성

메시지 $M$에 대하여 비밀키 $\langle F, T\rangle$를 입력 값으로 서명을 생성하는 알고리즘은 다음과 같다.

- 메시지 $M$에 대한 해시 값 계산: $H(M)=\xi\in F_q^o$ 를 계산한다.
- Vinegar 값 선택: 임의의 랜덤 벡터 $s_V=(s_1,\cdots,s_v)\in F_q^v$를 선택해서 각 $F^{(k)}(1\le k\le o)$에 대입하면, $o$개의 식과 $o$개의 변수를 갖는 연립 일차방정식(linear system)을 얻는다.
- 연립 일차방정식의 해 계산: 가우스 소거법을 이용하여 위에서 얻은 연립 일차방정식의 해 $s_o=(s_{v+1},\cdots,s_{v+o})$를 구한다. 그러면, $s=(s_1,\cdots,s_v,s_{v+1},..,s_{v+o})$는 $F(x)=\xi$를 만족하는 해가 된다. 만약 해가 존재하지 않으면 새로운 Vinegar 값을 선택하여 다시 수행한다.
- 서명 값의 계산: $T^{-1}(s)=\sigma\in F_q^n$를 계산한 후 전자서명 값 $\sigma$을 출력 한다.

### 2.3 UOV 서명 검증 알고리즘

메시지 $M$, $M$의 서명 값 $\sigma$와 공개키 $P$를 입력 값으로 이용하여 서명을 검증하는 알고리즘은 다음과 같다.

- 메시지 $M$에 대하여 $H(M)$을 계산한다.
- $\sigma$를 공개키 $P$의 변수에 대입하여

$P(\sigma)=(P_1(\sigma),...,P_o(\sigma))$를 계산한 후 $P(\sigma)=H(M)$인지 여부를 확인한다. 식이 성립하면 유효한 서명이 된다.

## III. 효율적인 다변수 이차식 기반 전자서명 제안

이 절에서는 단일 레이어를 갖는 UOV 구조를 유지하면서 일차식을 이용한 특별한 구조, 희소 다항식, 랜덤 다항식의 다양한 조합을 통해 비밀키의 길이를 줄이고, CHES 2022[20]에서 제안된 $o\times o$ 행렬의 역행렬을 이용하는 대신 $o/2\times o/2$의 역행렬을 이용하여 효율적으로 선형 시스템의 해를 구하는 방법을 적용한 효율적인 다변수 이차식 기반 전자서명 알고리즘을 제안한다.

### 3.1 키생성 알고리즘

일차식의 특별한 구조, 희소 다항식, 랜덤 다항식의 다양한 조합을 이용한 비밀키와 공개키를 생성하는 알고리즘은 다음과 같다.

1. 비밀키 $F$ 생성: $n$개의 변수 $x_1,...,x_n$를 갖는 $o$개의 식으로 구성된 중앙 함수 $F=(F^{(1)},...,F^{(o)})$를 생성하기 위해 식 (2)에서 Vinegar×Vinegar 이차항 부분 $F_V^{(k)}$와 Vinegar×Oil 이차항 부분 $F_{OV}^{(k)}$과 일차항과 상수항 부분 $F_{L,C}^{(k)}$를 다음과 같이 선택한다.

○ 〔$F_V^{(k)}$의 선택〕 Vinegar×Vinegar 이차항 부분 $F_V^{(k)}$의 선택은 다음 두 가지로 나눌 수 있다.

- 랜덤한 $F_V^{(k)}$의 선택: 모든 Vinegar × Vinegar 이차항을 $F_q$에서 랜덤하게 선택하는 경우로 $F_V^{(k)}=F_{V,R}^{(k)}$로 표기한다.
- 일차 다항식을 이용한 $F_V^{(k)}$의 선택: $k=1,...,o$에 대해 Vinegar × Vinegar 이차항 부분 $F_V^{(k)}$를 아래의 식

$$F_{V,LE}^{(1)}=x_1L_1+x_2L_2+\cdots+x_vL_v$$
$$F_{V,LE}^{(2)}=x_vL_1+x_1L_2+\cdots+x_{v-1}L_v$$
$$\cdots,$$
$$F_{V,LE}^{(o)}=x_{v-o+2}L_1+x_{v-o+3}L_2+\cdots+x_{v-o+1}L_v$$

과 같이 선택한다. 이때, $L_i\,(i=1,...,v)$는 변수$x_1,...,x_v$와 0이 아닌 $F_q$의 임의의 계수로 구성된 일차 다항식으로 $F_V^{(k)}$의 이차항 부분에 대응되는 대칭 행렬이 전체 랭크(full rank)를 갖도록 선택한다. 이때 $v$개 변수들로 구성된 $o$개의 다항식으로 구성된 아래의 식과 같은 순환 행렬의 부분 행렬과 벡터의 곱으로 표현된다.

$$\begin{pmatrix}F_V^{(1)}\\F_V^{(2)}\\\cdots\\F_V^{(o)}\end{pmatrix}=\begin{pmatrix}F_{V,LE}^{(1)}\\F_{V,LE}^{(2)}\\\cdots\\F_{V,LE}^{(o)}\end{pmatrix}=\begin{pmatrix}x_1 & x_2 & \cdots & x_v\\ x_v & x_1 & \cdots & x_{v-1}\\ \cdots & \cdots & \cdots & \cdots\\ x_{v-o+2} & x_{v-o+3} & \cdots & x_{v-o+1}\end{pmatrix}\begin{pmatrix}L_1\\L_2\\\cdots\\L_v\end{pmatrix}$$

서명 생성에서 임의의 Vinegar 값, $(s_1,...,s_v)\in F_q^v$을 $F_V^{(k)}(k=1,...,o)$의 Vinegar ×Vinegar 이차항 부분에 대입하면 아래의 식으로 나타낼 수 있다.

$$\begin{pmatrix}s_1 & s_2 & \cdots & s_v\\ s_v & s_1 & \cdots & s_{v-1}\\ \cdots & \cdots & \cdots & \cdots\\ s_{v-o+2} & s_{v-o+3} & \cdots & s_{v-o+1}\end{pmatrix}\begin{pmatrix}L_1(s_V)\\L_2(s_V)\\\cdots\\L_v(s_V)\end{pmatrix}=M_V\bullet\eta$$

그러면, $M_V$는 순환 행렬의 부분 행렬로 FFT를 사용하면 $O(v\log v)$의 복잡도로 효율적으로 계산할 수 있다.

○ 〔$F_{OV}^{(k)}$의 선택〕의 선택은 다음 두 가지로 나눌 수 있다

- 랜덤한 $F_{OV}^{(k)}$의 선택: 모든Vinegar×Oil 이차항을 $F_q$에서 랜덤하게 선택하는 경우로 $F_{OV}^{(k)}=F_{OV,R}^{(k)}$로 표기한다.
- 희소 다항식을 이용한 $F_{OV}^{(k)}$의 선택: $k=1,...,o$에 대해 아래와 같이 희소 다항식을 선택한다.

$$F_{OV}^{(k)}=F_{OV,S}^{(k)}=\sum_{i=1}^{v}\beta_i^k x_i x_{(i+k-2\,(\mathrm{mod}\,o))+v+1}$$

이때, $i=1,...,o$와 $k=1,...,o$에 대해 $\beta_i^k$이고 0이 아닌 $F_q$의 임의의 원소이고, $F^{(k)}$의 이차식 부분에 대응되는 대칭 행렬이 전

체 랭크를 갖도록 선택한다.

○ 〔일차항과 상수항 부분 $F_{L,C}^{(k)}$의 선택〕 일차항과 상수항으로 구성된 $F_{L,C}^{(k)}$의 선택은 다음 두 가지로 나눌 수 있다.

- $F_{L,C}^{(k)}$의 모든 일차항과 상수항을 갖도록 선택하는 것으로, $F_{L,C}^{(k)} = \sum_{i \in v+1}^{o} \gamma_i^{(k)} x_i + c^{(k)}$, 여기서 $\gamma_i^k$는 $F_q$의 임의의 원소이다.
- $F_{L,C}^{(k)}$의 모든 일차항과 상수항의 계수를 0으로 선택하는 것으로, 이 경우, 공개키에도 일차항이 없어 공개키의 길이를 줄일 수 있다.

$F_V^{(k)}, F_{OV}^{(k)}, F_{L,C}^{(k)}$의 조합: 전체 비밀키는 $F_V^{(k)}$, $F_{OV}^{(k)}$, $F_{L,C}^{(k)}$의 여러 조합에 따라 결정된다. 여기서는 아래의 세 가지 조합을 제안한다.

- LER-일차식 기반 Vinegar×Vinegar+랜덤 Vinegar×Oil:

$$F^{(k)} = F_{V,LE}^{(k)} + F_{OV,R}^{(k)} + F_{L,C}^{(k)}$$

- LES-일차식 기반 Vinegar×Vinegar+희소 다항식 기반 Vinegar×Oil:

$$F^{(k)} = F_{V,LE}^{(k)} + F_{OV,S}^{(k)} + F_{L,C}^{(k)}$$

- RR-랜덤 Vinegar × Vinegar + 랜덤 Vinegar × Oil:

$$F^{(k)} = F_{V,R}^{(k)} + F_{OV,R}^{(k)}$$

의 조합 중 선택하여 사용할 수 있다.

2. 비밀키 $T$ 생성: 역행렬이 존재하는 선형 함수 $T : F_q^n \rightarrow F_q^n$를 유한체 $F_q$에서 랜덤하게 선택한 후 $T^{-1}$를 구한다.
3. 공개키 생성: $P = F \circ T$를 계산하여 공개키 $P$를 생성한다.
4. 공개키, 비밀키 쌍 출력: $(P, \langle F, T^{-1} \rangle)$를 공개키와 비밀키 쌍으로 출력한다.

### 3.2 서명 생성 알고리즘

주어진 메시지 $M$에 대하여 비밀키 $\langle F, T^{-1} \rangle$를 이용하여 서명을 생성하는 알고리즘은 다음과 같다. 먼저, 유한체 $F_q$에서 $q$는 2의 멱승이고, $o$는 짝수라고 가정한다.

- 메시지 $M$에 대한 해시 값 계산: 먼저 길이가 $l$인 랜덤한 salt 값 $r$을 선택한 후 $H(M,r) = \xi = (\xi_1, \ldots, \xi_o) \in F_q^o$를 계산한다.
- Vinegar 값 선택: 임의의 랜덤 벡터 $s_V = (s_1, \cdots, s_v) \in F_q^v$를 선택해서 각 $F^{(k)} (1 \leq k \leq o)$에 대입하면, $o$개의 식과 $o$개의 변수를 갖는 연립 일차 방정식을 얻는다. 이 연립 일차 방정식의 계수의 행렬을 $R$이라고 놓고, $R$을 4개의 부분 행렬로 구성된 블록 행렬 $R = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$로 표현한다. 여기서 $o$는 짝수이다.
- 연립 일차 방정식의 해 찾기: 〔20〕에 소개된 블록 부분 행렬의 역행렬을 이용하여 $R$의 역행렬을 구하지 않고 $R^{-1} \bullet \xi$를 직접 계산하는 방법으로, $R$의 LDU(Lower-Diagonal-Upper triangle matrix)분해를 통해 블록 부분 행렬 $A$와 $A$의 슈어 보수 행렬(Schur complement) $[D - CA^{-1}B]$의 역행렬 $A^{-1}$와 $[D - CA^{-1}B]^{-1}$를 이용하여 $R$을 계수의 행렬로 갖는 연립 일차 방정식의 해를 구한다. $R$의 아래와 같은 LDU 분해로 표현되고,

$$R = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} I & 0 \\ CA^{-1} & I \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & D - CA^{-1}B \end{pmatrix} \begin{pmatrix} I & A^{-1}B \\ 0 & I \end{pmatrix}$$

이에 따른 $R^{-1} \bullet \xi$는 아래와 같이 구할 수 있다.

$$R^{-1} \bullet \xi = \begin{pmatrix} I & -A^{-1}B \\ 0 & I \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & [D - CA^{-1}B]^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ -CA^{-1} & I \end{pmatrix} \bullet \xi$$

✓ 먼저, $A^{-1}$와 $A$의 슈어 보수 행렬의 역행렬 $[D - CA^{-1}B]^{-1}$을 구한다. 만약 $A$와 $[D - CA^{-1}B]$의 역행렬이 존재하지 않으면, 새로운 랜덤 벡터 $s_V = (s_1, \cdots, s_v) \in F_q^v$을 선택하여 다시 수행한다.

✓ $(CA^{-1})(\xi_1, \ldots, \xi_{o/2})^t = (\alpha_{o/2+1}, \ldots, \alpha_o)^t$,
$A^{-1}(\xi_1, \ldots, \xi_{o/2})^t = (\beta_1, \ldots, \beta_{o/2})$,

$$[D - CA^{-1}B]^{-1}(\alpha_{o/2+1}+\xi_{o/2+1}, ..., \alpha_o+\xi_o)^t = (\beta_{o/2+1}, ..., \beta_o)^t,$$

- ✓ $(A^{-1}B)(\beta_{o/2+1}, ..., \beta_o)^t = (\delta_1, ..., \delta_{o/2})$를 계산하면 $s_O = (\beta_1+\delta_1, ..., \beta_{o/2}+\delta_{o/2}, \beta_{o/2+1}, ..., \beta_o)$는 연립 일차 방정식의 해가 된다. 그러면 백터 $s = (s_V, s_O)$가 최종적으로 $F(x) = \xi$를 만족하는 해가 된다.
- ✓ 서명 생성의 경우 Vinegar 값을 재사용할 수 있으면 다른 메시지의 서명 값을 계산하는 경우에도 동일한 $R$을 사용할 수 있어, 효율성이 크게 향상되지만, Vinegar 값을 재사용하는 경우 서명 위조가 가능하여 안전하지 않게 되므로 서명 생성할 때마다 반드시 다른 Vinegar 값을 선택해서 사용해야 한다[20].

- 서명 값의 계산: $T^{-1}(s) = \sigma$를 계산한 후 전자서명 값 $(\sigma, r)$을 출력 한다.

### 3.3 서명 검증 알고리즘

메시지 $M$, 메시지 $M$의 서명 값$(\sigma, r)$와 공개키를 이용하여 서명을 검증하는 알고리즘은 다음과 같다.

- 메시지 $M$과 랜덤 값 $r$에 대하여 $H(M, r)$을 계산한다.
- $\sigma$를 검증키 $P$의 변수에 대입하여 $P(\sigma) = (P_1(\sigma), ..., P_o(\sigma))$를 계산한 후 $P(\sigma) = H(M, r)$인지 여부를 확인한다. 식이 성립하면 유효한 서명이 된다.

## IV. 안전성 분석

이 절에서는 제안한 다변수 이차식 기반 전자서명 알고리즘의 위조불가능성을 증명하고 알려진 대수적인 공격에 대한 안전성 분석을 제공한다.

### 4.1 위조 불가능성

제안한 다변수 이차식 기반 전자서명은 UOV의 구조를 유지하면서 특별한 형태의 비밀키와 여러 가지 효율성을 제공하는 전자서명으로 위조불가능성은 UOV 서명의 위조불가능성 (existential unforgeability against adaptive chosen-message attacks: EUF-CMA) 증명을 따른다[21]. [21]에서는 원래의 UOV 서명에서 서명 값들의 분포가 균일 분포 (uniform distribution)를 이루지 않는 것을 해결하기 위해 $H(M)$을 랜덤 salt를 이용하는 $H(M, r)$로 수정하여 균일 분포를 만들고, 그 다음 Full-Domain-Hash 스킴의 안전성 증명 방법을 이용하여 수정된 UOV의 위조불가능성을 증명한다. 제안한 다변수 이차식 기반 전자서명 또한 UOV와 동일한 Oil×Oil 이차항이 없는 구조를 따르고 랜덤 salt를 포함하는 $H(M, r)$를 이용하여 균일 분포를 이루고 있어 동일한 안전성 증명이 적용 가능하다.

### 4.2 대수적 공격에 대한 안전성 분석

다변수 이차식 기반 전자서명 알고리즘의 알려진 대수적인 공격은 기반 문제인 다변수 이차식의 시스템의 해를 구하는 문제를 풀어주는 알고리즘을 이용하는 direct 공격과 알고리즘의 대수적인 구조를 이용한 불변 부분 공간을 찾는 Kipnis-Shamir 공격, 동치키와 good key를 이용한 키복구 공격, 두 공격의 조합으로 이루어진 intersection 공격으로 이루어져 있다. 제안한 전자서명 알고리즘은 UOV의 구조를 유지하면서 특별한 비밀키의 형태를 제공하고, UOV에서처럼 공개키와 비밀키의 이차항 부분에 대응되는 대칭 행렬이 전체 랭크를 가지고 있어 안전성 분석이 UOV와 거의 유사하고, 새로운 형태로 인한 가능한 공격을 포함하여 안전성을 분석한다.

#### 4.2.1 Direct 공격

Direct Attack은 주어진 공개키로부터 유도되는 다변수 이차식 시스템의 해를 직접적으로 계산하는 공격이다. 이 공격에서는 XL 알고리즘, Buchberger 알고리즘, F4, F5 같은 Gröbner basis를 이용한 알고리즘을 활용하여 다변수 이차식 시스템의 해를 구한다. 이 공격의 복잡도는 주로 효율적인 Hybrid F5(HF5) 알고리즘[22]에 의해 결정된다. HF5 알고리즘의 핵심적인 아이디어는 F5 알고리즘을 사용하기 전에 여러 개의 변수를 예측하여 식의 개수가 변수의 개수보다 많은 시스템(overdetermined system)을 만드는 것이다. F5 알고리즘을 반복 수행하여, 유한체 $F_q$에서 $k$개의 변수를 추측하는 모든 경우의 수는 $q^k$이다. HF5 알고리즘의 경우 $F_q$에서

$n$개의 변수와 $m$개의 이차식으로 구성된 임의의 시스템의 해를 구하는 복잡도는 아래와 같이 측정된다.

$$\min_{k\geq 0} q^k \cdot O\left(\left(m \cdot \binom{n-k+d_{reg}-1}{d_{reg}}\right)^{\omega}\right),$$

이 때, $d_{reg}$는 regularity의 degree로 $S_{m,n}=\frac{(1-z^2)^m}{(1-z)^n}$의 계수 중 양이 아닌 수가 되는 가장 낮은 차수이고, $2\leq\omega\leq 3$은 일차 연립방정식의 해를 구할 때의 선형 대수 상수이다. HF5에 사용되는 내부 식은 매우 희소하므로 복잡도의 하계(lower bound) 를 얻는데 $\omega=2$가 사용되고 상계(upper bound)로 $\omega=2.8$을 사용할 수 있다[22].

#### 4.2.2 Kipnis-Shamir (UOV) 공격

처음에 제안된 Balanced Oil and Vinegar (OV) 전자서명은 Vinegar 변수의 개수와 Oil 변수의 개수를 동일하게 사용하는 것 ($v=o$)으로 설계되었는데, 이 경우는 불변 부분 공간(invariant subspace)의 존재 여부를 이용한 Kipnis-Shamir 공격에 의해 깨진다는 것이 알려졌고, 이 후 Kipnis, Patarin, Goubin이 두 개의 변수를 다르게 설정하는 Unbalanced Oil and Vinegar(UOV) 전자서명을 제안하고 OV 전자서명에 적용된 Kipnis-Shamir 공격을 $v\neq o$인 경우로 확장하였다[2].

먼저, $E: {F_q}^n \rightarrow {F_q}^n$를 아래의 형태를 갖는 $E=\begin{pmatrix} E_1 & E_2 \\ E_3 & 0_{o\times o}\end{pmatrix}$선형 변환이라 하자. 이때 $E_1$는 $v\times v$ 행렬, $E_2$는 $v\times o$ 행렬 그리고 $E_3$는 $o\times v$ 행렬이고 행렬의 원소들은 $F_q$에서 임의로 선택되었다. 먼저, ${F_q}^n$의 Oil 공간 $\mathcal{O}$와 Vinegar 공간 $\mathcal{V}$를 다음과 같이 정의한다.

$$\mathcal{O}=\{x=(x_1,..,x_n)^T\in {F_q}^n : x_1=...=x_v=0\},$$
$$\mathcal{V}=\{x=(x_1,..,x_n)^T\in {F_q}^n : x_{v+1}=...=x_{v+o}=0\}$$

그러면, $E(\mathcal{O})$는 $\mathcal{V}$의 $o$-차원 고유(proper) 부분 공간이고 $E$가 역변환이 가능하다면 $E^{-1}(\mathcal{V})$이 ${F_q}^n$의 $v$차원의 부분 공간이고 $\mathcal{O}$는 고유 부분 공간이 된다. 공개키 생성 방법에 $P^{(i)}=T^T\circ F^{(i)}\circ T$이 성립한다. 행렬 $W_1^{-1}W_2$로 생성되는 행렬의 집합을 $\Omega$라 표시하면, 역변환이 가능한 $W_1$와 $W_2$는 행렬 $\overline{Q}^{(i)}(i=1,...,o)$의 임의의 선형 결합이다. 여기서, $\overline{Q}^{(i)}$는 공개키의 이차항 부분에 대응되는 대칭 행렬이고, $\Omega$의 원소의 공통 불변 부분 공간을 찾는 것이 목적이다. $J: {F_q}^n \rightarrow {F_q}^n$는 역변환이 가능한 선형 맵으로 ${F_q}^n$에 속한 두 개의 부분 공간 $A$와 $B$가 존재하여 $J(B)\subset A$을 만족한다고 가정하자. 여기서, $A$는 차원이 $v$이고 $B$는 차원이 $o$이고 $B\subset A$를 만족하고 불변 부분 공간의 차원을 1로 제한한다. 그러므로, 만약 $J$가 자신의 곱으로 대응된다면 벡터 $\mathbf{v}\in F^n$는 불변 부분 공간 위에 속해 있게 된다. $J(B)\subset A$이기 때문에, 0이 아닌 벡터인 $\mathbf{v}\in B$이 0이 아닌 자신의 곱으로 대응될 확률은 $\frac{q-1}{q^v-1}$이다. 만약 벡터를 자신의 곱으로 대응한다면 이 벡터의 모든 곱에 대해서도 모두 동일하게 성립하기 때문에 차원이 1인 불변 부분 공간이 존재할 확률은 대략 $\frac{q^o-1}{q^v-1}\approx q^{o-v}$이 된다. 그러면, [2]에서처럼 Kipnis-Shamir 공격의 전체 과정의 복잡도는 $q^{v-o-1}\cdot o^4$이 된다.

#### 4.2.3 키복구 공격

Wolf와 Preneel이 제안한 동치키(equivalent key)는 다변수 이차식 기반 전자서명의 키복구 공격에 사용되는 핵심적인 개념이다[23]. 동치키란 합성을 하면 주어진 공개키와 동일한 공개키를 생성할 수 있고, 중앙 함수의 특별한 구조를 유지시키는 비밀키를 의미한다. 주어진 공개키에 대응하는 원래의 비밀키가 아니더라도 동치키 중 하나를 찾을 수 있으면 서명을 위조할 수 있게 된다. 다변수 이차식 기반 전자서명에서 동치키는 많이 존재한다는 것이 알려져 있으며 동치키의 정확한 정의는 다음과 같다[23].

정의 1. $T, T'\in GL_n(F_q)$ 은 역변환이 가능한 행렬이고 고정된 $1\leq k\leq m$ ($m$은 식의 개수), $I^{(k)}\subseteq\{u_iu_j|1\leq i\leq j\leq n\}$에서 다음을 만족할 때,

$$F\circ T=P=(F'\circ T')\wedge(F|_I=F'|_I),$$

즉, $F$와 $F'$이 동일한 구조를 가질 때, $(F', T')$을 $(F, T)$의 동치키라고 부른다.

$P = F \circ T$를 만족하는 주어진 $(F, T)$에 대해

$$P = F \circ T = (F \circ \Omega) \circ (\Omega^{-1} \circ T) = F' \circ T'$$

을 만족하는 변환 $\Omega \in GL_n(F_q)$가 존재하면 $(F', T')$는 $(F, T)$의 동치키가 된다. 여기서 $F' = F \circ \Omega, T' = \Omega^{-1} \circ T$이다. 이 때, $\Omega$의 형태는 블록 하삼각 행렬(lower triangular matrix)이고 $\Omega^{-1}$ 역시 동일한 형태를 갖는다. 제안한 전자서명의 경우는 UOV 서명의 Oil×Oil 이차항이 없는 구조를 유지하고 이차항 부분에 대응되는 대칭 행렬의 랭크가 유지되고 있어 UOV와 동일한 동치키를 갖는다는 것을 쉽게 보일 수 있다. 동치키의 형태는 아래 정리 1과 같다[24].

정리 1. 공개키 $P = F \circ T$가 주어져 있을 때, $F' \circ T' = P'$을 만족하는 동치키 $(F', T')$가 높은 확률로 존재하며, 이때 $T'^{-1}$는 다음과 같은 형태를 갖는다.

$$T'^{-1} = \begin{pmatrix} 1_{v\times v} & T'_{o\times v} \\ 0_{v\times o} & 1_{o\times o} \end{pmatrix}$$

이 때, $T'^{-1}$는 $T^{-1}$도 동일한 형태를 가진다. 그러면 $F \circ \Omega$은 Oli×Oil의 이차항이 없는 다항식의 형태를 가진다.

정리 1의 증명은 UOV의 경우와 동일하다.[35] 정리 1에서의 보듯이 동치키의 모양은 랜덤한 형태보다 간단하다. 이 모양을 이용하여 $F' \circ T' = P$로부터 $T'^{-1}$의 원소를 모두 구하기 위해서는 변수의 개수와 식의 개수가 아주 큰 다변수 이차식과 삼차식의 시스템을 풀어야 하므로 복잡도가 매우 높다. 물론 동치키 대신 원래의 비밀키 $T^{-1}$를 구하는 경우는 변수의 개수가 더 많은 다변수 이차식과 삼차식의 시스템 보다는 복잡도가 더 낮아지는 것은 당연한 사실이다. 이 큰 복잡도를 더 낮추기 위해 $F$의 구조 전체를 보존하는 행렬 $T'$을 찾기보다는 $F$의 일부 구조를 보존하고 $T'$의 일부분을 드러내는 행렬을 찾는 방법이 유용한데, 이것을 동치키를 일반화한 good key라고 부른다. Good key의 정의는 다음과 같다[24].

정의 2. $T \in GL_n(F_q)$은 역변환이 가능한 행렬이고 고정된 $1 \le k \le m$, $I^{(k)} \subseteq \{u_i u_j | 1 \le i \le j \le n\}$이고, 적어도 하나의 $J^{(k)} \neq \varnothing$을 만족하는 $J^{(k)} \subset I^{(k)}, J^{(k)} = I^{(k)}$가 존재할 때, $(F \circ T = F' \circ T') \wedge (F|_J = F'|_J)$를 만족하는 $T' \in GL_n(F_q)$을 good key라고 정의한다.

위의 정의를 만족하는 good key를 찾게 되면 현저하게 줄어든 변수와 식의 개수를 갖는 이차식의 시스템을 얻게 되어 동치키 $T'^{-1}$의 구성 성분을 계산할 수 있어 동치키 복구에 성공하게 된다. 제안된 전자서명 알고리즘의 경우 UOV와 동일한 동치키를 갖고 있으므로 동일한 good key를 유도하게 된다. 그에 따라 $T'^{-1}$에 대한 변수의 개수와 식의 개수가 줄어들게 되고 정확한 변수와 식의 개수는 아래 정리와 같다[24].

정리 2. 제안된 전자서명 알고리즘의 good key를 이용한 키복구 공격의 주요 복잡도는 $v$개의 변수를 갖는 $o$개의 다변수 이차식의 시스템의 해를 구하는 문제의 복잡도와 동일하다.

#### 4.2.4 Intersection 공격

Intersection 공격은 키복구 공격과 Kipnis-Shamir 공격을 결합한 공격으로 direct 공격과 함께 가장 강력한 공격으로 알려져 있다. Intersection 공격의 복잡도는 $nk-(2k-1)o$개의 변수와 $vk-o(k-1)$개의 이차식의 시스템의 해를 구하는 복잡도와 동일하다[6]. 여기서, $k < v/(v-o)$이다.

#### 4.2.5 일차식 대체 공격

마지막으로, 제안하는 일차식을 이용하여 비밀 다항식 $F = (F^{(1)}, ..., F^{(o)})$를 구성하는 경우 가능한 새로운 공격에 대해 살펴보고자 한다. $i = 1, .., v$에 대해 일차 다항식 $L_i$를 새 변수 $y_i$로 대체하여 할 수 있는 공격을 고려해 볼 수 있다. 만약 이러한 대체가

비밀 다항식의 Vinegar×Vinegar 이차항 부분에 대응되는 대칭 행렬의 랭크를 조금이라도 떨어뜨릴 수 있다면 안전성에 영향을 미쳐 복잡도가 떨어질 수 있다. 일차 다항식 $L_i$를 새 변수 $y_i$로 대체하면 비밀 다항식은 $y_1,\dots,y_v$로 표현할 수 있는데, $k=1,\dots,o$에 대해의 Vinegar×Vinegar 이차항 부분 $F_{V,LE}^{(k)}$은 다음의 식으로 표현된다.

$$F_{V,LE}^{(1)} = y_1\overline{L_1}+y_2\overline{L_2}+\cdots+y_v\overline{L_v}$$
$$\cdots,$$
$$F_{V,LE}^{(o)} = y_1\overline{L_{v-o+2}}+y_2\overline{L_{v-o+3}}+\cdots+y_v\overline{L_{v-o+1}}$$

$y_1,\dots,y_v$로 표현된 비밀 다항식 $F_{V,LE}^{(k)}$에 대한 대칭 행렬도 원래 순환 구조를 여전히 보존하여 전체 랭크의 변화를 일으키지 않으므로 안전성 영향을 미치지 않는다.

## V. 안전한 파라미터 선택

이 절에서는 IV절의 안전성 분석을 바탕으로 세 개의 안전도에서 안전한 파라미터를 설정하고 각 파라미터에서의 키길이와 서명 길이를 비교 분석한다.

### 5.1 안전한 파라미터 선택

제시된 안전성 분석에 따라 안전하고 효율적인 파라미터를 다음과 같이 선택할 수 있다.

- 유한체의 선택: 유한체는 $F_{2^8}$을 선택한다.
- 식의 개수 $o(=m)$의 선택: 우선 $o$는 블록 부분 행렬을 이용할 수 있도록 짝수로 선택하여야 한다. Direct 공격 분석에 기반 하여 안전도에 따른 복잡도 이상을 갖는 식의 개수인 $o$를 선택하기 위해 각 안전도 1, 3, 5에서 $o \geq 46, 72, 96$이 되도록 한다. 여기서 안전도 1, 3, 5는 각각 128-비트, 192-비트 안전도, 256-비트 안전도를 의미한다.
- Vinegar 변수의 개수 $v$의 선택: 식의 개수인 $o$가 선택되면, 나머지 공격의 복잡도 분석에 따라 $v$를 선택한다. intersection 공격의 복잡도에서 $v \geq 1.5o$를 만족해야 한다. 안전도 1, 3, 5에서 각각 $v = 72, 112, 148$로 선택한다.

Table 1. Suggested Parameters and Complexities of Our Scheme against Known Attacks($o$: the number of equations, $v$: the number of Vinegar values)

| Security level | 1 | 3 | 5 |
|---|---|---|---|
| $(o,v)$ | (46,72) | (72, 112) | (96,148) |
| Direct(HF5) | 135.5 | 202.4 | 262.3 |
| Intersection | 171.883 | 242.9 | 304.5 |

선택한 파라미터와 주어진 파라미터의 direct 공격과 intersection 공격의 복잡도가 Table 1에 정리되어있다.

### 5.2 키길이와 서명 길이 비교 분석

선택된 파라미터를 기준으로 제안한 전자서명 알고리즘의 키길이와 전자서명 길이를 비교한다.

#### 5.2.1 키길이 비교 분석

여기서는 제안한 전자서명 알고리즘의 키길이와 전자서명 길이를 비교를 제공한다. 제안한 다변수 이차식 기반 전자서명 RR, LER, LES는 공개키 길이와 전자서명의 길이는 동일하고, 비밀키의 크기만 차이가 난다. 여기서 RR의 이차항은 랜덤하게 선택한 것으로 UOV 서명과 이차항 부분은 동일하고 나머지 부분이 다르다.

- 랜덤한 이차식을 이용하는 RR은 Vinegar×Vinegar 부분에 일차식의 특별한 구조를 이용한 LER 보다 비밀키가 각 안전도에서 약 1.7배 크다.
- 랜덤한 이차식을 이용하는 RR은 Vinegar×Vinegar 부분에 일차식의 특별한 구조를 이용하고 Vinegar×Oil 부분에 희소 다항식을 적용한 LES 보다 비밀키가 안전도 1, 3, 5에서 각각 약 16.21배, 25배, 33,2배 크다.

세 가지 종류의 안전도에서 RR, LER, LES의 공개키, 비밀키, 전자서명의 길이는 Table 2에서 확인할 수 있다. Table 2에서 S. Size, PK, SK는 각각 전자서명의 길이, 공개키의 길이, 비밀키의 길이를 나타낸다.

Table 2. Key Sizes and Signature Sizes of Our Schemes (Bytes)

| Scheme | Security Level | 1 | 3 | 5 |
|---|---|---|---|---|
| RR | S. Size | 134 | 200 | 260 |
| | PK | 328,441 | 1,238,761 | 2,892,961 |
| | SK | 282,177 | 1,057,825 | 2,460,469 |
| LER | S. Size | 134 | 200 | 260 |
| | PK | 328,441 | 1,238,761 | 2,892,961 |
| | SK | 166,473 | 614,753 | 1,423,877 |
| LES | S. Size | 134 | 200 | 260 |
| | PK | 328,441 | 1,238,761 | 2,892,961 |
| | SK | 17,433 | 42,209 | 74,117 |

#### 5.2.2 서명 길이 비교 분석

제안한 전자서명의 서명 길이는 양자내성 전자서명 알고리즘 중 다변수 이차식 기반 전자서명 알고리즘이 가장 짧다. Table 3은 미국 NIST 양자내성암호 공모 프로젝트 4 라운드에서 표준 알고리즘으로 선정된 두 개의 전자서명 Dilithium, Falcon과 서명 길이를 비교한 것이다[25].

- Module-LWE 기반 전자서명 Dilithium은 LES 보다 안전도 1, 3, 5에서 각각 약 18배, 16배, 17.7배 크다.
- NTRU 기반 전자서명 Falcon은 LES 보다 안전도 1, 3, 5에서 각각 약 5배, 6.4배, 4.9배 크다.

Table 3. Comparison of Signature Sizes (Bytes)

| Scheme | 1 | 3 | 5 |
|---|---|---|---|
| Our Scheme | 134 | 200 | 260 |
| Dilithium | 2,420 | 3,293 | 4,595 |
| Falcon | 666 | 1,280 | |

### 5.3 효율성 비교 분석

제안한 전자서명 알고리즘에서는 키생성과 서명 생성에서 연산량이 감소하여 효율성이 향상되는데, 여기서 각 연산량을 비교한다.

- 키생성 연산량 감소
  - ✓ $F_V^{(k)}$를 랜덤하게 선택하는 경우 유한체에서 $v^2/2 \cdot o$개의 원소를 랜덤하게 생성해야 하지만 일차 다항식을 이용한 경우 $v \cdot o$개 원소생성으로 랜덤한 수 생성에서의 감소 효과가 크다.
  - ✓ $F_{OV}^{(k)}$를 랜덤하게 선택하는 경우 유한체에서 $v \cdot o^2$개의 원소를 랜덤하게 생성해야 하지만 희소 다항식을 이용한 경우 $v \cdot o$개 원소생성으로 감소한다.
- 서명 생성 연산량 감소
  - ✓ Vinegar 값 대입 연산: Vinegar×Vinegar 이차항에 상수를 대입하는 연산은 FFT의 사용으로 $O(v^3)$에서 복잡도가 $O(vlogv)$로 줄고, 비밀키의 길이가 줄어서 생기는 연산량의 감소로 효율성이 향상된다.
  - ✓ 선형 시스템의 해를 구하는 연산량 감소: $o \times o$ 행렬의 역행렬 계산에는 $3/2 \cdot o^3$개의 유한체 곱셈, $o \times o$행렬의 곱 계산에는 $o^3$개의 유한체 곱셈이 소요되고, $o/2 \times o/2$ 블록 부분 행렬의 역행렬을 이용하여 선형 시스템의 해를 구하는 경우 $2[2(o/2)^2+3/2(o/2)^3]=5/8 \cdot o^3$개의 연산량이 소요되므로 $o \times o$ 행렬의 역행렬 계산에 필요한 $3/2 \cdot o^3$개의 유한체 곱셈 보다 횟수가 줄어 효율성이 향상된다.

## VI. 결 론

본 논문에서는 단일 레이어를 갖는 UOV의 구조를 유지하면서 일차식의 특별한 구조, 희소 다항식, 랜덤 다항식의 다양한 조합을 통해 비밀키의 길이를 줄이고, 블록 행렬의 역행렬을 이용하여 선형 시스템의 해를 구하는 방법을 적용한 효율적인 다변수 이차식 기반 전자서명 알고리즘을 제안하였다. 제안한 전자서명의 위조 불가능성을 증명하고 여러 대수적인 공격에 대한 안전성 분석을 통해 안전한 파라미터를 설정하고 각 파라미터에서의 키길이와 서명 길이를 비교 분석하였다. 랜덤한 이차식을 이차항을 이용하는 RR에 비해 LES의 비밀키는 안전도 1, 3, 5에서 각각 약 6.3%, 4%, 3% 정도에 지나지 않아 최대 97%의 키길이 축소 효과를 보였으며, NIST 양자내성암호 표준화 대상 전자서명 알고리즘으로 선정된 Dilithium의 약 6%, Falcon의 20% 정도

로, 양자내성 전자서명 중에서 서명 길이가 가장 짧다는 특징을 가지고 있다. 안전성 분석 측면에서는 UOV의 안전성 분석의 핵심적인 부분 중 하나는 이차 다항식의 이차항에 대응되는 대칭 행렬의 랭크가 전체 랭크를 가지느냐 그렇지 않느냐로 결정되므로 제안된 전자서명 알고리즘은 전체 랭크를 가지도록 설계되어 알려진 공격에 대한 UOV의 안전성 분석이 그대로 적용되고 있다. 제안된 특수 구조를 이용한 새로운 대수적인 공격은 4.2.4 일차식 대체 공격이 있고, 다른 새로운 공격에 대한 유무는 계속 연구가 필요하다. 향후 새로운 형태의 대수적인 공격의 유무와 설정된 안전한 파라미터를 바탕으로 최적 구현을 수행할 계획이다.

## References


[1] W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. on Computing, pp. 1484-1509, 1997.

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

[3] J. Ding and D. Schmidt. "Rainbow, a new multivariable polynomial signature scheme", Proc. of the International Conference on Applied Cryptography and Network Security, LNCS 3531, pp. 164-175, 2005.

[4] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J-P. Tillich, "An algebraic attack on rank metric code-based cryptosystems", Advances in Cryptology, EUROCRYPT 2020, Part III, LNCS 12107, pp. 64-93, 2020.

[5] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J-P. Tillich, and J. A. Verbel, "Improvements of algebraic attacks for solving the rank decoding and MinRank problems", Advances in Cryptology, ASIACRYPT 2020, Part I, LNCS 12491, pp. 507-536, 2020.

[6] W. Beullens, "Improved cryptanalysis on UOV and Rainbow", Advances in Cryptology, EUROCRYPT 2021, Part I, LNCS 12696, pp. 348-373, 2021.

[7] D. Smith-Tone and R. Perlner, "Rainbow band separation is better than we thought", IACR ePrint 2020-702, June 2020.

[8] J. A. Verbel, J. Baena, D. Cabarcas, R. A. Perlner, and D. Smith-Tone, "On the complexity of superdetermined" minrank instances, Proc. of the International Conference on Post-Quantum Cryptography, LNCS 11505, pp. 167-186, 2019.

[9] W. Beullens, "Breaking Rainbow takes a weekend on a laptop", Advances in Cryptology, CRYPTO 2022, Part II, LNCS 13508, pp. 464-479, 2022.

[10] J. Ding, M-S. Chen, A. Petzoldt, D. Schmidt, and B-Y. Yang, "Rainbow technical report", National Institute of Standards and Technology, 2019.

[11] A. Petzoldt, S. Bulygin, and J. Buchmann, "CyclicRainbow: A multivariate signature scheme with a partially cyclic public key", Proc. of the International Conference on Cryptology in India, LNCS 6498, pp 33-48, 2010.

[12] NIST Computer Security Resource Center, "Post-quantum cryptography, round 2 submissions", https://csrc.nist.gov/ Projects/ Post-Quantum Cryptography/Round-2-Submissions, Feb. 3, 2023.

[13] W. Beullens and B. Preneel, "Field lifting for smaller UOV public keys", Proc. of the International Conference on Cryptology in India, LNCS 10698, pp. 227-246, 2017.

[14] Z. Peng and S. Tang, "Circulant UOV: a new UOV variant with shorter private key and faster signature generation", KSII Transactions on Internet and Information Systems (TIIS), vol. 12, no. 3, pp. 1376-1395, 2018.
[15] Z. Peng and S. Tang, "Circulant Rainbow: A new Rainbow variant with shorter private key and faster signature generation", IEEE Access, vol. 5, pp. 11877-11886, 2017.
[16] A. Szepieniec and B. Preneel, "Block-anti-circulant unbalanced Oil and Vinegar", Proc. of Selected Areas in Cryptography, LNCS 11959, pp. 574-588, 2020.
[17] Y. Hashimoto, "On the security of Circulant UOV/Rainbow", IACR ePrint 2018-947, Oct. 2018.
[18] J. Ding, J. Deaton, Vishakha and Bo-Yin Yang, "The nested subset differential attack: a practical direct attack against LUOV which forges a signature within 210 minutes". IACR ePrint 2020-967, Aug. 2020.
[19] H. Furue, K. Kinjo, Y. Ikematsu, Y. Wang, and T. Takagi, "A structural attack on block-anti-circulant UOV at SAC 2019", Proc. of the International Conference on Post-Quantum Cryptography, LNCS 12100, pp. 323-339, 2020.
[20] K-A. Shim, S. Lee, N. Koo, "Efficient implementations of Rainbow and UOV using AVX2", IACR Trans. Cryptogr. Hardw. Embed. Syst. vol. 2022, no. 1, pp. 245-269, 2022.
[21] K. Sakumoto, T. Shirai, H. Hiwatari: "On provable security of UOV and HFE signature schemes against chosen-message attack", Proc. of the International Conference on Post-Quantum Cryptography, LNCS 7071, pp 68-82. 2011.
[22] L. Bettale, J.-C. Faugere and L. Perret, "Hybrid approach for solving multivariate systems over finite fields", Journal of Mathematical Cryptology, vol. 3, pp. 177-197, 2009.
[23] C. Wolf and B. Preneel, "Large superfluous keys in multivariate quadratic asymmetric systems", Proc. of the International Conference on Practice and Theory of Public-Key Cryptography, LNCS 3386, pp. 275-287, 2005.
[24] E. Thomae, "About the security of multivariate quadratic public key schemes", Dissertation Thesis, RUB, June 2013.
[25] NIST Computer Security Resource Center, "Post-quantum cryptography, round 3 submissions", https://csrc.nist.gov/ Projects/ Post-Quantum Cryptography/ Round-3-Submissions, Feb. 3, 2023.

## 〈저 자 소 개〉

심 경 아 (Kyung-Ah Shim) 정회원
1992년 2월: 이화여자대학교 수학과 졸업
1994년 8월: 이화여자대학교 수학과 석사
1999년 2월: 이화여자대학교 수학과 박사
2000년 2월~2004년 2월: 한국인터넷진흥원 선임연구원
2000년 9월~2008년 8월: 이화여자대학교 연구 교수
2008년 9월~현재: 국가수리학연구소 공공기반연구본부 본부장
〈관심분야〉 암호 이론, 공개키 암호, 양자내성암호, 블록체인 보안, IoT 보안