Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.533

다변수 이차식 기반 서명 기법 Rainbow의 공격 기법 및 보안강도 분석*

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

Analysis of Attacks and Security Level for Multivariate Quadratic Based Signature Scheme Rainbow*

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

요 약

양자적 특성을 활용한 Shor 알고리즘은 인수분해 및 이산대수 문제를 효율적으로 풀 수 있다. 이로 인해 RSA, 타원곡선(ECC: Elliptic Curve Cryptography) 등 인수분해와 이산대수 문제의 어려움에 기반하고 있는 기존 공개키 암호 시스템이 위협받고 있다. 이에 미국 국립표준기술연구소(NIST)에서는 양자 컴퓨터의 강력한 연산 능력에도 안전한 새로운 공개키 암호 체계의 표준인 양자 내성 암호(PQC: Post Quantum Cryptography)를 선정하는 공모를 진행하고 있다. 양자 내성 암호 후보군 중 다변수 이차식 기반 서명 기법은 짧은 서명 길이와 빠른 서명 및 검증으로 인해 사물인터넷(IoT) 등 제한된 자원을 갖는 기기에 적합하다. 이에 본 논문에서는 다변수 이차식 기반 서명 중 유일하게 3 라운드까지 최종 선정된 Rainbow에 대한 클래식 공격 기법과 양자적 특성을 이용한 공격 기법들을 분석하고, 현재 3라운드에 제시된 레인보우 파라미터에 대한 공격 복잡도를 계산하여 양자 내성 암호 표준화 후보 알고리즘인 레인보우 서명기법이 제공하는 보안 강도를 분석한다.

ABSTRACT

Using Shor algorithm, factoring and discrete logarithm problem can be solved effectively. The public key cryptography, such as RSA and ECC, based on factoring and discrete logarithm problem can be broken in polynomial time using Shor algorithm. NIST has been conducting a PQC(Post Quantum Cryptography) standardization process to select quantum-resistant public key cryptography. The multivariate quadratic based signature scheme, which is one of the PQC candidates, is suitable for IoT devices with limited resources due to its short signature and fast sign and verify process. We analyzes classic attacks and quantum attacks for Rainbow which is the only multivatiate quadratic based signature scheme to be finalized up to the round 3. Also we compute the attack complexity for the round 3 Rainbow parameters, and analyzes the security level of Rainbow, one of the PQC standardization candidates.

Keywords: Post Qquantum Cryptography, Multivariate Quadratic based signature scheme, Security level

Received(04. 30. 2021), Modified(05. 27. 2021), Accepted(05. 27. 2021)

* 본 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발).

† 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2021-2018-0-01417)

† 주저자, smcho3315@hanyang.ac.kr

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

I. 서 론

1980년대 초반, Richard Feynman은 양자 중첩을 활용한 양자 컴퓨터를 제안하였다[1]. 고전 컴퓨터가 0 또는 1의 값을 갖는 비트를 정보 처리의 기본 단위로 사용하는 반면, 양자 컴퓨터는 0과 1의 상태가 확률적 중첩 상태로 동시에 존재하는 큐비트를 사용한다.

현재 IBM, Google, D-Wave Systems 등 전 세계적으로 우수한 여러 IT 기업들이 양자 컴퓨터 개발에 뛰어들고 있다. Google은 2019년 현존하는 최고 성능의 슈퍼컴퓨터로 1만년이 걸릴 문제를 200초 만에 풀어낸 양자 프로세서 'Sycamore'를 개발하여 Nature지에 발표하였으며[2], D-WAVE Systems는 2020년에 양자 어닐링 기법을 이용한 5000 큐비트 양자 컴퓨터를 개발하였다.

양자 컴퓨터는 중첩 상태를 갖는 큐비트의 성질을 이용하여 정보 단위를 더 고차원적인 형태로 표현할 수 있기 때문에, 적은 수의 큐비트로도 굉장히 많은 경우의 수를 동시에 표현할 수 있다. 양자 역학 원리와 양자 현상에 의해 작동하는 양자 컴퓨터는 중첩과 얽힘과 같은 양자적 특성을 활용하여 기존 컴퓨터로 다루기 힘든 문제를 효율적으로 풀 수 있다. 이러한 양자 컴퓨터의 이점을 사용하여 기존의 어려운 문제들을 풀기 위한 다양한 양자 알고리즘들이 제안되었다. 1985년, David Deutsch는 최초의 지수적 성능 향상을 이룬 Deutsch 알고리즘[3]를 제안하였으며, 1996년에는 비정형 탐색 문제에 대해 2차 속도 향상을 이룬 그로버(Grover) 알고리즘[4]이 Lov Grover에 의해 제안되었다.

1994년, Peter Shor가 제안한 쇼어(Shor) 알고리즘[5]는 인수분해와 이산로그 문제를 다항 시간 안에 풀 수 있다. 그에 따라 인수분해 및 이산대수 문제의 어려움에 기반하여 설계된 기존 RSA 및 타원곡선(ECC: Elliptic Curve Cryptography) 등의 공개키 암호가 대용량 큐비트 계산이 가능한 양자 컴퓨터의 등장으로 보안에 취약해질 수 있다.

따라서 양자 컴퓨터의 연산 능력에도 안전한 새로운 암호 알고리즘의 필요성이 대두되었고, 미국 국립표준기술연구소 (NIST, National Institute of Standards and Technology)는 2016년 초 양자 내성 암호(PQC, Post Quantum Cryptography) 공개 모집 공고하였다. 현재 3 라운드를 거치며 총 7개의 공개키 암호 알고리즘들이 후보로 남아있다.

3라운드 양자 내성 암호 표준 알고리즘 후보군들 중에서 상대적으로 짧은 서명 길이로 빠른 서명 및 검증 알고리즘을 장점으로 갖는 다변수 이차식 기반 서명 기법은 사물인터넷(IoT)이나 드론 등 제한된 자원을 갖는 기기에서 효율적으로 사용될 것으로 기대된다.

현재 3 라운드 양자 내성 암호 후보로 선정된 Rainbow[6] 기법을 비롯한 다변수 이차식 기반 서명 기법에 대한 클래식 공격 기법들과 양자적 특성을 이용한 공격기법들이 다수 발표되었다. NIST의 양자 내성 암호 공모가 최종 라운드까지 진행되었고, 2022~2024년 정도에 새로운 양자 내성 암호 표준의 초안 발표를 앞두고 있는 만큼, Rainbow 표준 문서에서 제시하고 있는 안전성 파라미터들에 대한 보안강도가 어느 정도인지 그 수준을 분석하고 검증할 필요성이 있다.

본 논문에서는 다변수 이차식 기반 서명 기법 중 NIST 양자 내성 암호 표준화 최종 3라운드 후보로 남아있는 Rainbow 서명 기법에 대한 클래식 공격 기법들과 양자적 특성을 활용하여 Rainbow의 서명을 위조하는 공격기법들에 대해 소개한다. 또한 Rainbow 표준 문서에서 제공하는 안전성 파라미터들을 실제 공격 기법들의 복잡도에 대입하여 계산함으로써 현재 3 라운드 Rainbow의 보안강도 수준을 평가한다.

본 논문은 다음과 같이 구성되어 있다; 2장에서 양자 내성 암호와 다변수 이차식 기반 서명 기법에 대해 살펴본 후, 3장에서 Rainbow 서명 기법에 대해 설명한다. 4장에서는 Rainbow 서명 기법에 대한 공격들에 대해 살펴보고, 5장에서 공격 기법들에 대해 서술한 뒤, NIST의 보안강도에 대해 3 라운드 Rainbow가 제공하는 보안강도 수준을 분석한다.

II. Preliminaries

2.1 양자 내성 암호

현재 사용되고 있는 대부분의 보안 프로토콜들은 디피-헬만(Diffie-Hellman) 키 교환, RSA(Rivest-Shamir-Adleman) 암호, 타원 곡선 암호를 이용하여 구현되며, 이들은 모두 인수 분해와 이산 로그 문제의 수학적 어려움에 기반을 둔다. 그러나 1994년 Bell 연구소의 Peter Shor는

기존 컴퓨터로는 풀기 어려운 인수 분해 및 이산 로그 문제를 양자 컴퓨터를 이용하면 효율적으로 풀 수 있음을 보였다[5]. 따라서 대용량 큐비트를 계산할 수 있는 양자 컴퓨터가 개발되면 인수분해 문제나 이산대수 문제의 어려움에 기반하여 설계된 공개키 암호 기법들을 더 이상 사용할 수 없게 된다. 또한 1996년 Lov Grover에 의해 제안된 양자 탐색 알고리즘은 비정형 탐색 문제에 대해 2차 속도 향상을 제공한다[4]. 기존 컴퓨터 대비 빠른 탐색이 가능한 양자 컴퓨터의 특성은 대칭키 암호가 더 큰 키 사이즈를 사용하도록 요구한다. 이로 인해 일부 전문가들은 향후 20년 이내에 양자 컴퓨터가 현재 사용 중인 모든 공개키 기법을 깰 수 있을 것이라고 예측하기도 한다[7].

따라서 양자 컴퓨터의 개발에도 안전한 공개키 암호 체계를 구축할 필요성이 대두되었으며, 이를 양자 내성 암호라 명명하고 이에 대한 연구가 활발히 진행되고 있다. 이에 NIST는 2016년 2월 양자 내성 암호에 대한 컨퍼런스인 PQCrypto에서 양자 내성 암호의 표준을 정하기 위한 공모를 시작하였다. 양자 내성 암호 표준은 공개키 암호 및 키 설정 기법과 전자 서명 기법 2가지 분야에 대해 공모를 진행하였다. 2017년 12월 1라운드 양자 내성 암호 후보들이 공개되었으며, 2019년 1월 2라운드 후보들을 거쳐 2020년 7월 3라운드 양자 내성 암호 후보들이 공개되었다. Table 1.은 3라운드 양자 내성 암호 후보들에 대한 요약을 보여준다.

Table 1. Round 3 Candidates for Post Quantum Cryptography Standardization

	algorithm	base problem
Public-key Encryption and Key-establishment Algorithms	Round 3 Finalists	
	Classic McEliece	Code-based
	CRYSTALS-KYBER	Lattice-based
	NTRU	Lattice-based
	SABER	Lattice-based
	Alternate Candidates	
	BIKE	Code-based
	FrodoKEM	Lattice-based
	HQC	Code-based
	NTRU Prime	Lattice-based
	SIKE	
Digital Signature Algorithms	Round 3 Finalists	
	CRYSTALS-DILITHIUM	Lattice-based
	FALCON	Lattice-based
	Rainbow	MQ-based
	Alternate Candidates	
	GeMSS	MQ-based
	Picnic	Symmetric-based
	SPHINCS+	Symmetric-based

2.2 다변수 이차식 기반 서명 기법

다변수 이차식 기반 서명 기법은 다변수 이차식 문제(Multivariate Quadratic problem)와 다항식의 확장 동형(EIP: Extended Isomorphism of Polynomials) 문제의 어려움에 기반한 서명 기법이다. 이 중 대표적인 것이 NIST 양자 내성 암호 표준 공모의 3 라운드 후보에 올라있는 Rainbow 서명 기법이다.

n을 변수 $x=(x_1,\dots,x_n)$의 개수, m을 방정식의 개수라 할 때 F_q 상의 다변수 이차식 함수 $MQ(n,m,\mathrm{F}_q)$는 일반적으로 다음과 같이 표현할 수 있다.

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

이때, 주어진 $v\in\mathrm{F}_q^m$에 대해, $F(x)=v$를 n개의 변수에 대한 m개의 이차 방정식 시스템이라 하며, 이를 만족하는 변수 벡터 x를 찾는 것을 다변수 이차식 문제라고 한다. 다변수 이차식 문제는 NP-완전(NP-complete)으로 알려져 있으며, 양자 컴퓨터에서도 아주 다루기 힘들다고 알려져 있다[8].

다항식의 확장 동형 문제란 공개키 pk가 $P=S\circ F\circ T$를 만족하는 P의 계수의 집합이고, 이 공개키 pk가 주어졌을 때, $P=S\circ F\circ T$로부터 F와 S, T를 각각 찾는 문제이다. 다항식의 확장 동형 문제는 NP-완전으로 증명되지는 않았지만, 현재까지 풀기 어려운 문제로 알려져 있으며, 이 문제의 어려운 정도는 다변수 이차다항식 F의 구조에 의

존한다.

III. Rainbow

Rainbow는 다변수 이차식 기반 서명 기법 중 하나로 미국 NIST 양자 내성 암호 공모전 3 라운드 후보로 선정된 서명 알고리즘이다[9]. 유오브이(UOV: Unbalanced Oil-Vinegar) 문제에 기반을 둔 Rainbow 서명은 상대적으로 짧은 서명 길이로 빠른 서명 및 검증 알고리즘을 장점으로 한다. 본 장에서는 Rainbow 서명 알고리즘의 키 생성과 서명 생성 및 검증 방법에 대해 서술한다.

3.1 파라미터 선택

Rainbow에서는 NIST 보안 카테고리 5개를 3개로 묶어 나타내며, Rainbow에서 사용되는 파라미터는 다음과 같다.

I : $\mathrm{F}=GF(16)$, $(v_1,o_1,o_2)=(36,32,32)$
NIST 보안강도 레벨 Ⅰ, Ⅱ에 해당
III : $\mathrm{F}=GF(256)$, $(v_1,o_1,o_2)=(68,32,48)$
NIST 보안강도 레벨 Ⅲ, Ⅳ에 해당
V : $\mathrm{F}=GF(256)$, $(v_1,o_1,o_2)=(96,36,64)$
NIST 보안강도 레벨 Ⅴ에 해당

Rainbow에서 사용하는 총 변수의 개수가 n개일 때, $n=v_1+o_1+o_2$이다. v_1은 첫 번째 레이어의 비네가 변수의 개수이고, o_1, o_2는 각각 첫 번째와 두 번째 레이어의 오일 변수의 개수를 나타낸다.

3.2 키 생성

3.2.1 개인키

Rainbow의 개인키는 역행렬이 존재하는 아핀 맵 $S:\mathrm{F}^m\to\mathrm{F}^m$, $T:\mathrm{F}^n\to\mathrm{F}^n$와 중앙 맵 $F:\mathrm{F}^n\to\mathrm{F}^n$로 이루어져 있다. 중앙 맵 F는 m개($m=n-v_1$)의 다변수 다항식 $f^{(v_1+1)},\ldots,f^{(o_1)}$로 이루어진다. $k\in v_1+1,\ldots,n$일 때, $f^{(k)}$는 다음과 같으며, Fig. 1.은 중앙 맵 F의 구성을 보여준다.

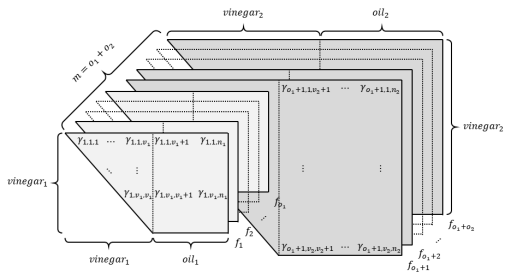

Fig. 1. Central map of Rainbow

$$f^{(k)}(x_1,\ldots,x_n)=\sum_{i,j\in V_l}^{i\le j}\alpha_{ij}^{(k)}x_ix_j+\sum_{i\in V_l,\,j\in O_l}\beta_{ij}^{(k)}x_ix_j+\sum_{i,\in V_l\cup O_l}\gamma_i^{(k)}x_i+\delta^{(k)}$$

3.2.2 공개키

공개키 P는 S, F, T의 합성이다.

$$P=S\circ F\circ T:\mathrm{F}^n\to\mathrm{F}^m$$

3.3 서명 생성

서명할 메시지가 d, 해쉬 함수가 $H:\{0,1\}\to\mathrm{F}^m$, 서명이 $\mathrm{z}\in\mathrm{F}^n$일 때, 서명 생성 방법은 다음과 같다.

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

3.4 서명 검증

메시지 d와 서명 z가 주어졌을 때, 서명 검증은 다음과 같이 이루어진다.

1) 해쉬 함수를 통해 $\mathrm{h}=H(d)\in\mathrm{F}^m$를 계산한다.
2) 공개키를 이용하여 $\mathrm{h}'=P(\mathrm{z})\in\mathrm{F}^m$를 계산한다.
3) $\mathrm{h}=\mathrm{h}'$이면 서명 z가 검증된다.

IV. Rainbow에 대한 공격 기법

Rainbow에 대한 공격은 기존 클래식 공격 기법과 양자적 특성을 활용한 공격 기법 2가지로 나눌 수 있다. 본 장에서는 NIST 양자 내성 암호 표준 공모 3 라운드에 올라 있는 Rainbow 서명 기법에 대한 공격 기법에 대해 설명한다.

4.1 클래식 공격 기법

Rainbow에 대한 기존 클래식 공격 기법은 서명을 위조하는 공격과 키를 복원하는 공격 2가지가 존재한다. 서명 위조 공격에는 다이렉트(direct) 공격이 있으며, 키 복원 공격에는 유오브이(UOV) 공격과 민랭크(MinRank) 공격, 하이랭크(HighRank) 공격, 충돌(collision) 공격이 있다.

4.1.1 다이렉트 공격

다이렉트 공격은 공개키를 이용하여 서명을 검증하는 공개키 시스템 $P(\mathrm{z})=\mathrm{h}$를 풀어서 서명 값인 z를 알아냄으로써 서명을 위조하는 공격이다. 공개키 시스템은 변수의 개수가 방정식의 개수보다 많은 결정되지 않은(underdetermined) 시스템이다. 따라서 이 시스템을 풀기 위해서는 $n-m$(변수의 개수 - 방정식의 개수)개의 변수들을 수정하거나 추정하여 변수의 개수와 방정식의 개수가 같은 결정된(determined) 시스템으로 만들어야 한다. 그 후, XL 알고리즘[10] 혹은 F_4/F_5와 같은 그로브너 베이시스(Grobner Basis) 알고리즘[11]을 적용하여 시스템의 해를 구하고, 이를 서명으로 사용할 수 있다. NIST 양자 내성 암호 3라운드의 Rainbow 문서에 따르면 현재 결정된 시스템을 푸는 가장 효율적인 알고리즘은 XL 와이드만(Wiedemann) 알고리즘이다[12]. XL 알고리즘은 결정된 시스템에 대한 d차 매컬리(Macaulay) 행렬을 구하고, 이 매컬리 행렬을 이용하여 효율적으로 시스템의 해를 구하는 알고리즘이다. 이때, 매컬리 행렬은 희소 행렬의 형태를 띄고, 희소 행렬로 이루어진 시스템을 와이드만 알고리즘으로 푸는 방식이 XL 와이드만 알고리즘이다.

4.1.2 유오브이 공격

Rainbow 서명은 UOV 서명 기법에서 확장된 것으로 조화(reconciliation) 공격[13]이나 오일 부분 공간(oil subspace) 공격[14] 등의 UOV 서명 공격 기법들을 사용할 수 있다. 그 중 Aviad Kipnis와 Adi Shamir가 제안한 오일 부분 공간 공격은 조화 공격에 비해 효율적이라고 알려져 있다. 오일 부분 공간 공격은 Rainbow의 비네가 변수의 개수 $v=v_1+o_1$, 오일 변수의 개수 $o=o_2$로 설정함으로써 Rainbow를 UOV의 형태로 만든 후, 비네가 변수들을 모두 0으로 설정하고, 이들의 아핀 변환 T에 대한 역상을 찾는 것이다. 이를 통해 비네가 변수들로부터 오일 변수들을 분리할 수 있고, 최종적으로 비밀키를 복원할 수 있다.

4.1.3 민랭크 공격

민랭크 문제는 m개의 $n\times n$ 행렬들 $Q_1,\dots,Q_m$이 주어졌을 때, 특정 랭크 r보다 작은 랭크를 갖는 선형결합 $Q=\sum_{i=1}^{m}\lambda_i Q_i$를 찾는 문제이다. 민랭크 공격은 이러한 민랭크 문제를 풀어서 Rainbow의 중앙 맵 F를 찾는 공격이다. Rainbow의 경우, 두 번째 레이어의 비네가 변수 개수인 v_2의 랭크를 갖는 공개키들의 선형 결합이 첫 번째 레이어의 중앙 맵들의 선형결합에 대응된다. 이러한 선형 결합을 첫 번째 레이어의 오일 변수 개수인 o_1개 찾음으로써 첫 번째 레이어의 중앙 맵을 복원할 수 있고, 이로 인해 Rainbow의 비밀키를 찾을 수 있다.

Magali Bardet 등은 2020년 민랭크 문제를 푸는 가장 효율적인 방법을 제안하였다[15]. 작은 랭크를 갖는 행렬 Q를 다음 식과 같이 각각 Q의 열공간을 나타내는 $n\times r$ 행렬 S와 $r\times n$행렬 C로 분해한다.

$$Q=S\bullet C$$

그 다음, $C_j'=\begin{pmatrix} r_j \\ C \end{pmatrix}$로 정의된 행렬의 $r+1$-Minors를 0으로 세팅한다. 그 결과로 나오는 시스템이 변수의 개수보다 방정식의 개수가 더 많으므로, 와이드만 알고리즘[16]을 이용한 선형화를 통해 시스템을 풀 수 있다.

4.1.4 하이랭크 공격

하이랭크 공격[17]은 중앙 맵 F에서 가장 적게 나오는 수를 찾는 것을 시작으로 중앙 맵 F를 찾아가는 공격이다. 마지막 레이어의 오일 변수 $x_{v_u+1},...,x_n$은 마지막 레이어의 중앙 맵 $f^{(v_u+1)},...,f^{(n)}$에서만 나타난다. 이에 마지막 레이어의 오일 변수를 찾아냄으로써 마지막 레이어의 중앙 맵을 복원할 수 있고, 이로 인해 Rainbow의 비밀키를 찾을 수 있다.

4.1.5 충돌 공격

충돌 저항성(Collision resistance)이란 사용된 해쉬 함수에 대해 해쉬 값이 같은 서로 다른 입력 쌍을 찾는 것이 계산적으로 불가능해야 하는 성질이다. Rainbow는 해쉬 값을 서명하는 방식으로, 동일한 서명 값을 갖는 서로 다른 해쉬 값을 찾음으로써 서명을 위조할 수 있다.

4.2 양자적 특성을 이용한 공격 기법

Rainbow에 대한 양자적 특성을 이용한 공격 기법은 서명을 위조하는 공격만 존재하며, 그로버 알고리즘을 이용한 공격 기법들이 존재한다.

4.2.1 그로버 알고리즘

그로버 알고리즘은 양자적 특성을 이용하여 비정형 데이터에 대한 탐색을 기존 클래식 컴퓨터를 사용한 방법 대비 2차 속도 향상을 가진 기법으로, 1996년 Lov Grover에 의해 제안되었다[4]. Fig. 2.는 그로버 알고리즘의 전체 회로도를 나타낸다.

그로버 알고리즘은 $|0>^{\otimes n}$으로 초기화된 n 큐비트의 입력 $|x>$에 대해 0부터 2^n-1까지의 중첩 상태 $\frac{1}{\sqrt{2^n}}\sum_{z=0}^{2^n-1}|z>$에 오라클(Oracle) 회로 $O_f^{\pm}$와 그로버 디퓨전(Diffusion) 회로 D를 반복 수행하여 찾고자 하는 결과가 관측될 확률을 높인다. 오라클 회로는 입력이 풀고자 하는 문제의 해 $|x^*>$일 경우에만 $|b>$ 큐비트에 NOT 게이트를 취하도록 설계되어야 한다. Fig. 3.은 오라클 회로의 동작을 나타낸다.

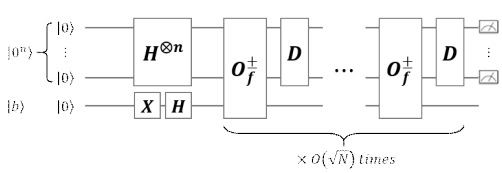

Fig. 2. Overall circuit of Grover algorithm

디퓨전 회로는 문제의 해 $|x^*>$가 관측될 확률을 높이는 역할을 수행한다.

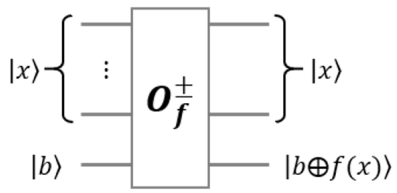

Fig. 3. Grover Oracle circuit $O_f^{\pm}$

4.2.2 그로버 알고리즘을 이용한 이진 다변수 이차식 풀이(binary MQ solver)

Peter Schwabe와 Bas Westerbaan은 2016년 그로버 알고리즘을 이용하여 F_2 상의 다변수 이차식 문제를 푸는 방법을 제안하였다[18]. [18]에서는 비트간 연산의 +1 역할을 하는 NOT 게이트와 덧셈 역할을 하는 CNOT 게이트, 곱셈 역할을 하는 토폴리(Toffoli) 게이트를 이용하여 F_2 상의 다변수 이차식 $Ax=b$의 Ax부분을 오라클 회로로 구현하였다. Fig. 4.는 [18]에서 F_2 상의 다변수 이차식을 양자 회로로 구현한 예시이다.

오라클 회로는 Ax의 결과가 b일 경우에만 $|b>$ 큐비트를 반전하도록 설계하였다. 최종적으로 오라클

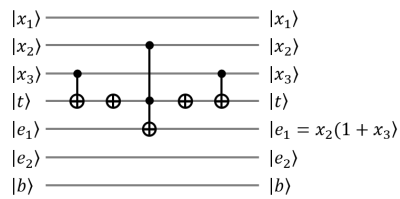

Fig. 4. Oracle circuit for multivariate quadratic equation over F_2: $x_2(1+x_3)$

회로와 디퓨전 회로 쌍을 $O(\sqrt{2^n})$번 반복 진행하면 높은 확률로 F_2 상의 다변수 이차식 문제의 해를 찾을 수 있다.

4.2.3 그로버XL 알고리즘

Daniel J. Bernstein과 Bo-Yin Yang은 2016년 그로버 알고리즘에 XL 알고리즘을 접목하여 Rainbow의 서명을 위조하는 방법을 제안하였다[19].

XL(Extenced Linearization) 알고리즘[10]은 유한체 F_q 상의 다변수 이차식 문제를 풀기 위해 1981년 Lazard에 의해 처음 제안되었다. XL 알고리즘은 다변수 이차식 문제를 d차 매컬리 행렬로 만든 다음 가우시안(Gaussian) 소거법 등을 통해 해를 찾는 방법이다. [19]에서는 이러한 XL 알고리즘을 그로버 오라클로 구현하여 다변수 이차식 기반 서명 기법의 서명을 찾는 개념을 제안하였으나, 실제 오라클 회로를 어떻게 구성해야 하는지는 제안하지 못하였다.

V. Rainbow 파라미터에 대한 보안강도 분석

본 장에서는 4장에서 설명한 클래식 공격기법과 양자적 특성을 이용한 Rainbow 기법에 대한 공격 기법의 복잡도를 분석하고, 3 라운드 Rainbow 표준문서에서 제시하고 있는 안전성 파라미터를 사용했을 때 Rainbow 기법의 보안강도를 평가한다.

5.1 클래식 공격 기법

Rainbow의 파라미터에 따른 클래식 공격 기법의 복잡도가 NIST의 보안 레벨을 만족하지 못한다면, Rainbow는 안전하지 못하다. 따라서 각각의 클래식 공격 기법의 복잡도를 파악하고, 이러한 공격들에 안전하도록 파라미터를 설정해야 한다.

5.1.1 다이렉트 공격

현재 가장 효율적인 다이렉트 공격 방법은 XL 알고리즘[10]으로 시스템의 해를 찾는 것이다. 이때 XL 알고리즘에서 가장 많은 연산을 차지하는 것이 매컬리 행렬로 이루어진 시스템의 해를 찾는 것이다. 매컬리 행렬은 희소 행렬의 형태를 띄며, 희소 행렬로 이루어진 시스템의 해를 가장 효율적으로 찾는 기법이 와이드만 알고리즘[12]이다. XL 알고리즘에 와이드만 기법을 적용하여 Rainbow에 대한 다이렉트 공격을 수행하는 복잡도는 다음과 같다.

$$Compl_{Direct} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right)$$

이때, d_{reg}는 해를 찾을 수 있는 매컬리 행렬의 차수이며, d_{reg}의 상한은 비네가 변수의 개수와 오일 변수의 개수 중 작은 값에 1을 더한 값이다[20]. 따라서 다이렉트 공격은 Rainbow 파라미터 I에 대해 $k=62$일 때 최소 2^{268} 정도의 복잡도를 가지며, 파라미터 III에 대해서는 $k=69$일 때 최소 2^{636} 정도, 파라미터 V에 대해서는 $k=98$일 때 최소 2^{808} 정도의 복잡도를 갖는다.

5.1.2 유오브이 공격

랜덤 백터 $\lambda \in F^{o_u}$를 통해 공개키의 선형결합 $W=\sum_{i=1}^{o_u} \lambda_i \cdot P^{(i)}$을 계산한다. 여기서 $P^{(k)}$는 역행렬이 존재한다. 이에 $\left(P^{(k)}\right)^{-1} \cdot W$는 $T^{-1}(O)$의 부분공간인 불변 부분 공간을 갖는다. 중앙 맵 F를 구하기 위해 총 o개의 선형 독립 벡터 $v_1, \ldots, v_o \in T^{-1}(O)$가 필요하다. $T^{-1}(O)$에 속하는 한 개의 0이 아닌 벡터를 구하는데 $q^{v_u - o_u - 1} = q^{n-2o_2-1}$번의 복잡도를 갖는다. 총 o개의 선형독립 벡터를 찾은 후 행렬 M^T를 재구성하여 동치키를 찾는데 있어 총 $q^{n-2o_2-1} \cdot o_2^4$의 복잡도를 갖는다.

$$Compl_{UOV} = q^{n-2o_2-1} \cdot o_2^4$$

Rainbow 파라미터 I에 대해 유오브이 공격은 2^{168}의 복잡도를 가지며, 파라미터 III에 대해 2^{430}, 파라미터 V에 대해서는 2^{560}의 복잡도를 갖는다.

5.1.3 민랭크 공격

민랭크 공격을 통해 구한 시스템은 변수의 개수보

다 방정식의 개수가 많다. 따라서 와이드만 알고리즘을 통해 선형화하여 시스템을 풀 수 있다. 와이드만 알고리즘을 통해 시스템을 선형화하고 해를 찾는 복잡도는 다음과 같다.

$$Compl_{MinRank} = 3 \cdot \left(\left((o_2 + 1) \cdot \binom{n'}{r} \right)^2 \cdot (r+1) \cdot (o_2 + 1) \right)$$

Rainbow 파라미터 I에 대해 민랭크 공격은 2^{170} 정도의 복잡도를 가지며, 파라미터 III에 대해서는 2^{244}, 파라미터 V에 대해서는 2^{311}의 복잡도를 갖는다.

5.1.4 하이랭크 공격

$O_i = \{ x \in F^n : x_1 = \cdots = x_{v_i} = 0 \}$일 때, 임의의 $\alpha \in F^k$에 대해 $O_u \subset \ker \sum_{k=v_1+1}^{v_u} \alpha_k \cdot F^{(k)}$를 얻을 수 있고 이는 $T^{-1}(O_u)$가 공개키 $P^{(k)}$의 특정 선형결합의 커널에 놓여있다고 볼 수 있다. q^{o_u}의 확률로 해당 커널 $V \subset T^{-1}(O_u)$을 구할 수 있고 $T^{-1}(O_u)$ 전체를 구하는데 있어 $q^{o_u} \cdot \frac{n^3}{6}$의 복잡도를 갖는다.

$$Compl_{HighRank} = q^{o_u} \cdot \frac{n^3}{6}$$

Rainbow 파라미터 I에 대해 하이랭크 공격은 2^{145} 정도의 복잡도를 가지며, 파라미터 III에 대해서는 2^{403}, 파라미터 V에 대해서는 2^{532}의 복잡도를 갖는다.

5.1.5 충돌 공격

Rainbow에서 사용하는 해쉬 함수의 크기는 오일 변수의 개수인 m이다. 이때 크기가 m인 해쉬 값을 무작위로 선택하여 서명을 생성했을 때, 원하는 서명 값이 나올 확률은 $\frac{1}{q^m}$이다.

$$Compl_{Collision} = q^m$$

Rainbow 파라미터 I에 대해 충돌 공격은 2^{256}의 복잡도를 가지며, 파라미터 III에 대해 2^{640}, 파라미터 V에 대해 2^{800}의 복잡도를 갖는다.

5.2 양자적 특성을 이용한 공격 기법

다변수 이차식 기반 서명 기법에 대한 양자적 특성을 이용한 공격 기법은 양자 컴퓨터 개발 정도에 따른 실현 가능성을 따져봐야 한다. 특히 공격을 위해 필요한 양자 큐비트 정도가 중요한 파라미터 중 하나이다. IBM은 2023년까지 1000 큐비트의 양자 컴퓨터를 개발하겠다는 목표를 세웠고, D-WAVE는 현재 2000 큐비트의 양자 컴퓨터를 개발하여 실제 주식 수익률을 계산하는 등 실제 응용에 활용하고 있다. 다변수 이차식 기반 서명 기법의 파라미터들은 실현 가능한 양자 큐비트에 대해 안전하도록 설정되어야 한다.

5.2.1 그로버 알고리즘을 이용한 이진 다변수 이차식 풀이

그로버 알고리즘을 이용하여 F_2 상의 다변수 이차식 문제를 푸는 방법은 80 비트 정도의 보안강도를 갖는 85개의 방정식과 81개의 변수를 갖는 F_2 상의 다변수 이차식 문제에 대해 오라클 회로는 91개의 큐비트와 55,080개의 양자 NOT 게이트와 2,206,260개의 양자 CNOT 게이트, 27,710개의 토폴리 게이트가 필요하다. 이러한 오라클 회로에 대해 2^{40}번의 오라클 회로와 디퓨전 회로 쌍의 반복이 필요하다. 이때 실제 양자 컴퓨터 상에서 토폴리 게이트는 Fig. 5.와 같이 T 게이트, CNOT 게이트, 아다마르(Hadamard) 게이트를 조합하여 구현된다.

T 게이트는 다른 게이트들에 비해 구현 비용이 크기 때문에, 전체 양자 회로에서 사용된 T 게이트 개수와 회로 깊이(depth)는 양자 회로의 복잡도를 분석할 때 중요한 정보 중 하나이다. Table 2.는 그로버 알고리즘을 이용하여 80 비트 보안강도를 갖는

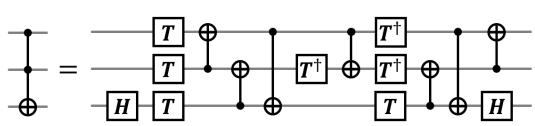

Fig. 5. Decomposition of Toffoli gate

Table 2. Quantum resources of binary MQ solver at 80-bits security

quantum resources	binary MQ solver
qubits	91
NOT	2^{56}
CNOT	2^{61}
Toffoli	2^{55}
Number of T gate	2^{58}
T-depth	2^{20}

F_2 상의 다변수 이차식 문제를 푸는 이진 다변수 이차식 문제 풀이에 필요한 양자 자원 수를 나타낸다.

그러나 이 공격 기법은 $GF(2)$ 상에서의 다변수 이차식 문제에 대한 공격을 실제 Rainbow는 $GF(16)$과 $GF(256)$을 유한체로 사용하기 때문에, 덧셈 및 곱셈을 단순히 NOT, CNOT, 토폴리 게이트만 사용할 수 없고, $GF(q)$에 대한 덧셈기 및 곱셈기를 사용하여야 한다. 이로 인해 실제 Rainbow를 공격하기 위해서는 굉장히 많은 양자 자원이 필요하다. 따라서 $GF(q)$ 상에서의 다변수 이차식 문제를 풀기 위한 양자 알고리즘에 대한 연구가 필요하며, 이때 필요한 양자 자원에 대한 분석 또한 이루어져야 한다.

5.2.2 그로버XL 알고리즘

그로버 알고리즘에 XL 알고리즘을 접목하여 다변수 이차식 문제를 푸는 그로버XL 알고리즘은 그로버 알고리즘의 오라클 게이트를 설계하는 방법을 제시하지 못하고, 컨셉만 제시하였으며, 필요한 양자 자원에 대한 분석도 이루어지지 않았다.

5.3 Rainbow 보안강도 평가

암호 알고리즘은 일정 수준의 보안강도를 만족하여야 하며, 이에 대해서 NIST에서는 암호 알고리즘의 안전성 수준을 평가할 수 있도록 암호 알고리즘 및 키 길이에 대한 가이드라인을 제공한다[21].

NIST는 보안강도를 5가지 레벨로 분류하여 제공하고 있다. NIST에서 제공하는 보안강도는 Table 3.과 같다.

보안강도 레벨 Ⅰ, Ⅲ, Ⅴ는 대칭키 암호 시스템인 AES에 대해 전사적 공격을 시행했을 때 깨지는 정도의 계산 복잡도로서 제공하고 있으며, 보안강도 레벨 Ⅱ, Ⅳ는 해쉬 함수에 대해 충돌 공격을 시행했을 때 깨지는 정도의 계산 복잡도로 제공하고 있다.

Table 3. Security level of NIST

level	Security Description	complexity
Ⅰ	hard to break AES128	2^{128}
Ⅱ	hard to break SHA256	2^{128}
Ⅲ	hard to break AES192	2^{192}
Ⅳ	hard to break SHA384	2^{192}
Ⅴ	hard to break AES256	2^{256}

앞서 계산한 클래식 공격들에 대해서 3 라운드 Rainbow의 파라미터에 따라 제공하는 안전성 수준은 Table 4.와 같다.

3라운드 Rainbow는 파라미터 Ⅰ에 대해 최소 NIST 보안강도 Ⅰ을 만족하고 있으며, 파라미터 Ⅲ에서는 민랭크 공격을 제외한 나머지 공격들에 대해 NIST 보안강도 Ⅴ를 만족하고 있다. 현재 Rainbow에 대한 클래식 공격 중 가장 효율적인 기법은 민랭크 공격이며, 이에 대해서도 모두 NIST 보안강도를 만족하여 현재 수준에서 암호 안전성 수준을 만족하고 있다.

한편 양자적 특성을 이용하여 다변수 이차식 문제를 푸는 기법들 또한 제안되고 있지만, F_2 상의 다변수 이차식 문제를 푸는 양자 회로만 제안하거나 F_q 상의 다변수 이차식 문제를 풀 수 있는 개념 정도만 제시하고 실제 이를 구현하기 위한 양자 회로는 제안하지 못하는 등 아직 한계가 존재한다. 따라서 다변수 이차식 문제에 대한 양자적 공격이 이루어지기 위해서는 F_q 상에서의 다변수 이차식 문제를 풀 수 있는 양자 알고리즘을 제안하고 이에 필요한 양자

Table 4. Security level of Rainbow against attacks

attacks	Round 3 parameters of Rainbow		
	Ⅰ	Ⅲ	Ⅴ
Direct attack	Ⅲ(2^{268})	Ⅴ(2^{636})	Ⅴ(2^{808})
UOV attack	Ⅰ(2^{168})	Ⅴ(2^{430})	Ⅴ(2^{560})
MinRank attack	Ⅰ(2^{170})	Ⅲ(2^{244})	Ⅴ(2^{311})
HighRank attack	Ⅰ(2^{145})	Ⅴ(2^{403})	Ⅴ(2^{532})
Collision attack	Ⅴ(2^{256})	Ⅴ(2^{640})	Ⅴ(2^{800})

자원에 대한 분석이 이루어져야 한다. 이때, 필요한 양자 자원이 현실적으로 구현이 가능하게 되면 다변수 이차식 기반 서명 기법 또한 위협받을 수 있기 때문에 양자적 공격에도 안전하도록 안전성 파라미터를 수정할 필요가 있다.

VI. 결론 및 향후 연구과제

양자 컴퓨터에 대한 개념이 등장하고, 양자적 특성을 활용한 쇼어 알고리즘이 인수분해와 이산로그 문제를 효율적으로 풀 수 있게 되면서, 인수분해와 이산로그 문제의 어려움에 기반한 기존 공개키 암호 시스템이 양자 컴퓨터에 의해 깨질 수 있다. 이에 현재 NIST에서는 양자 내성 암호를 공모 중에 있으며, 현재 3라운드의 후보까지 선정이 완료되었다. 2022~2024년 최종 표준 초안 발표를 앞두고 양자 내성 암호 후보군들에 대한 안전성 분석이 활발하게 이루어지고 있으며, 본 논문에서는 이 중 다변수 이차식 기반 서명 기법 중 유일하게 3 라운드를 통과한 Rainbow에 대한 공격 기법들을 살펴보고, 제공하고 있는 안전성 수준을 분석하였다.

Rainbow에 대한 클래식 공격 기법들에 대해서 3라운드에서 제시한 파라미터들은 최소 NIST 보안강도 I 이상을 만족하고 있으며, 특히 Rainbow 파라미터 III 이상부터는 민랭크 공격을 제외한 모든 공격들에 대해 NIST 보안강도 V를 만족하고 있다. 이처럼 Rainbow는 클래식 공격 기법들에 대한 안전성 분석을 통해 파라미터를 수정하면서 클래식 공격 기법들에 대해 안전하도록 설계되었다.

그러나 그로버 알고리즘 등의 양자 알고리즘을 이용한 Rainbow 공격 기법들은 현재까지 F_2 상의 다변수 이차식 문제만을 타겟으로 하는 등 실제 Rainbow 표준 파라미터에 맞게 설계된 양자 회로들이 제안되지 않고 있다. 따라서 Rainbow 표준 파라미터에 맞춰 설계된 양자 회로를 구성하고 이에 대한 양자 자원을 계산하여 Rainbow의 안전성을 분석하는 연구가 필요가 있다. 이를 위해 우리는 향후 양자적 특성을 이용한 기존의 공격 기법들을 Rainbow 표준 파라미터에 맞게 변환한 양자 회로를 설계하고 이에 대한 Rainbow의 양자적 안전성을 분석할 계획이다. 또한 클래식 공격 기법들에 양자 알고리즘을 적용할 수 있는 부분들을 검토하고 이를 양자 회로로 설계하여 Rainbow의 안전성을 분석하는 연구를 수행할 계획이다.

References

[1] R. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, pp. 467-488, Jun. 1982.

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J.C. Bardin, R. Barends, R. Biswas, S. Bioxo, et al. and J.M. Martinis, "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 779, pp. 505-510, Oct. 2019.

[3] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, vol. 400, no. 1818, pp. 97-117, Jul. 1985.

[4] 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, Jul. 1996.

[5] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, Nov. 1994.

[6] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," Applied Cryptography and Network Security, LNCS 3531, pp. 164-175, 2005.

[7] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, Oct. 2018.

[8] 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.

[9] J. Ding, M-S. Chen, M. Kannwischer, J.

Patarin, A. Petzoldt, D. Schmidt, and B-Y. Yang, "Rainbow - round 3," Round 3 submission for NIST Post Quantum Cryptography Standardization, 2020.

[10] D. Lazard, "Resolution des systemes d'equations algebriques," Theoretical Computer Science, vol. 15, no. 1, pp. 77-110, 1981.

[11] J-C. Faugere, "A new efficient algorithm for computing grobner bases (F4)," Journal of Pure and Applied Algebra, vol. 139, no. 1-3, pp. 61-88, Jun. 1999.

[12] C-M. Cheng, T. Chou, R. Niederhagen, and B-Y. Yang, "Solving quadratic equations with xl on parallel architectures," Cryptographic Hardware and Embedded Systems, CHES 2012, LNCS 7428, pp. 356-373, 2012.

[13] J. Ding, B-Y. Yang, C-H. O. Chen, M-S. Chen, and C-M. Cheng, "New differential-algebraic attacks and reparametrization of Rainbow," Applied Cryptography and Network Security, ACNS 2008, LNCS 5037, pp. 242-257, 2008.

[14] A. Kipnis and A. Shamir, "Cryptanalysis of the oil and vinegar signature scheme," Advances in Cryptology, CRYPTO '98, LNCS 1462, pp. 257-266. 1998.

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

[16] D. Wiedemann, "Solving sparse linear equations over finite fields," IEEE Transactions on Information Theory, vol. 32, no. 1, pp. 54-62, Jan. 1986.

[17] P. Czypek, S. Heyse, and E. Thomae, "Efficient implementations of mqpks on constrained devices," Cryptographic Hardware and Embedded Systems, CHES 2012, LNCS 7428, pp. 374-389, 2012.

[18] P. Schwabe and B. Westerbaan, "Solving binary mq with grover's algorithm," International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2016, LNCS 10076, pp. 303-322, 2016.

[19] D.J. Berstein and B-Y Yang, "Asymptotically faster quantum algorithms to solve multivariate quadratic equations," Post-Quantum Cryptography, PQCrypto 2018, LNCS 10786, pp. 487-5016, 2018.

[20] J-C. Faugere, M.S.E. Din, and P-J. Spaenlehauer, "Grobner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): algorithms and complexity," Journal of Symbolic Computation, vol. 46, no. 4, pp. 406-437, Apr. 2011.

[21] KISA, "The guide to using cryptographic algorithm and key sizes," KISA-GD-2018-0034, Korea Internet & Security Agency, 2018.

〈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

김 제 인 (Jane Kim) 학생회원
2021년 2월: 한양대학교 ERICA 캠퍼스 전자공학부 졸업
2021년 3월~현재: 한양대학교 전자공학과 석사과정
〈관심분야〉 스마트그리드 보안, 양자 내성 암호, 블록체인 보안

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