정 보 보 호 학 회 지
제 33 권 제1호, 2023. 2

코드 기반 암호와 아이소제니 기반 암호의 공격 사례

양 유 진*, 오 유 진**, 장 경 배*, 서 화 정***

요 약

차세대 컴퓨터인 양자 컴퓨터는 현재 정보화시스템에서 널리 사용되고 있는 공개키 암호 시스템인 RSA와 Elliptic Curve Cryptography (ECC)의 안전성을 위협하고 있다. 특히 양자 알고리즘인 Shor 알고리즘은 RSA와 ECC가 기반하고 있는 수학적 난제들을 다항 시간 내에 해결할 수 있기 때문에 NIST에서는 양자컴퓨터 상에서 내성을 가진 공개키 암호 표준화 공모전을 개최하였다. 2022년도에 NIST에서는 4개의 3라운드 최종 표준화 알고리즘을 발표하였다. 이와 동시에, 4라운드 표준화 알고리즘을 진행함으로써, 공개키 분야에서 코드 기반 또는 아이소제니 기반의 새로운 암호 알고리즘을 추가로 표준화할 예정이다. 이에 본 논문에서는 NIST 양자 내성 암호 표준화 공모전 4라운드의 후보 알고리즘인 코드 기반 암호 Classic McEliece, BIKE, HQC와 아이소제니 기반 암호 SIKE의 최신 동향에 대해 확인해본다. 추가적으로, 해당 암호 알고리즘에 대한 분석 기법과 공격 사례에 대해 살펴보고록 한다.

Ⅰ. 서 론

특정 문제를 효율적으로 모델링하고 해결할 수 있는 차세대 컴퓨팅 능력을 보유한 양자 컴퓨터의 개발에 전 세계의 관심이 주목되고 있다. 다른 차원의 문제 해결 능력을 가지는 양자 컴퓨터는 현재 암호 알고리즘들에서 기반하고 있는 안전성 문제들을 효과적으로 해결할 수 있다.

대칭키 암호의 경우, 양자 검색 알고리즘인 Grover 알고리즘을 사용하면 고전 컴퓨터를 대상으로 주장하던 보안 강도가 제곱근으로 감소하게 된다. 예를 들어, n-bit 키를 사용하는 암호 알고리즘에 대한 고전적인 전수 조사 복잡도인 $O(2^n)$일 때, Grover 알고리즘을 사용한 전수 조사 복잡도는 $\sqrt{2^n}$으로 감소한다. 다행히도, 이러한 보안성 감소는 키 길이를 두 배로 증가시킴으로써 대응할 수 있다.

반면, 현재 널리 사용되고 있는 공개키 암호의 경우 보안성이 완전히 무너지게 된다. RSA와 Elliptic Curve Cryptography (ECC)는 소인수 분해와 이산 대수 문제의 어려움에 안전성을 기반하고 있지만, 양자 푸리에 변환과 양자 위상 추정을 사용하는 Shor 알고리즘은 소인수 분해와 이산 대수의 내부 문제를 다항 시간 내에 해결할 수 있다. 따라서 보안 파라미터의 증가와는 상관없이 고성능의 양자 컴퓨터가 개발될 경우, 해당 암호화 알고리즘의 안정성은 붕괴된다. 즉, 대칭키 암호의 상황과는 다르게 양자 컴퓨터의 계산 능력에 내성을 가지는 새로운 양자 내성 암호가 요구되고 있다. NIST에서는 양자 내성 암호 공모전을 주최하였으며, 현재 1개의 공개키 암호 알고리즘 KYBER (격자 기반 암호) 3개의 전자 서명 알고리즘 DILITHIUM, FALCON (격자기반), SPHINCS+ (해시기반)이 표준화 알고리즘으로 선정되었다.

NIST는 격자 기반 암호만이 공개키 분야의 최종 알고리즘으로 선정된 현 상황에서, 다른 문제에 기반하는 암호 알고리즘을 추가로 선정할 계획이다. 이에 후보 알고리즘으로는 코드 기반 암호인 Classic McEliece, BIKE, HQC과 아이소제니 기반 암호인 SIKE가 있다.

어떠한 암호 알고리즘이 추가적으로 표준화될 것인지 전 세계의 관심이 집중되고 있다. 본 논문에서는 4라운드의 후보 암호 알고리즘들에 대해 살펴보고, 그에 따른 암호 분석 기법과 몇 가지 공격 사례에 대해 살펴보고자 한다.

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 100%).
* 한성대학교 IT융합공학과 (대학원생, yujin.yang34@gmail.com, 학부생, oyj0922@gmail.com, 대학원생, starj1023@gmail.com)
** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)

Ⅱ. 코드 기반 암호

코드 기반 암호는 NP-complete로 알려진 신드롬 디코딩 문제의 어려움을 기반으로 하는 양자 내성 암호 중 하나이다. 신드롬 디코딩 문제는 행렬 $H \in \mathbb{F}_2^{(n-k)\times n}$와 특정 hamming weight를 조건으로 가지는 비밀 벡터 $e \in \mathbb{F}_2^n$와의 곱셈을 통해 벡터 $s \in \mathbb{F}_2^{n-k}$가 생성된다 ($s = He^T$). 그리고 이 때, H와 s가 알려져 있다 해도, 비밀 벡터 e를 찾는 것은 매우 어렵다는 수학적 기반을 전제로 하고 있다.

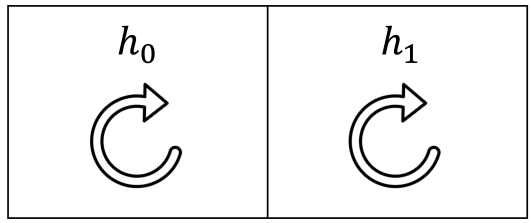
현재 Classic McEliece, BIKE, 그리고 HQC가 4 라운드의 후보 알고리즘으로 남아 있다.

2.1. Classic McEliece

Classic McEliece는 패리티 체크 행렬이 공개키로 사용되는 Niederreiter 시스템을 사용하고 있으며, 오랜 역사를 가진 Goppa 코드가 사용된다. Goppa 코드를 채택함으로써의 단점은 공개키로 사용되는 패리티 체크 행렬이 매우 크다는 것이다. 장점으로는, 비록 비효율적일 수 있지만 오랜 역사 동안 우수한 보안 강도를 제공해온 Goppa 코드를 그대로 사용한다는 것이다. Classic McEliece의 가장 작은 파라미터인 mceliece348864는 (768 × 3488) 크기의 패리티 체크 행렬이 생성되어 암호화에 사용된다. 암호화에서는 낮은 hamming weight (mceliece348864의 경우 64)를 조건으로 가지는 무작위 벡터가 생성되어 패리티 체크 행렬과 곱해지고 이로 인해 생성된 벡터가 암호문 역할을 수행한다. Classic McEliece에서는 큰 공개키 크기를 줄이기 위해 패리티 체크 행렬에 대한 가우스 소거를 수행하여 구분되는 항등 행렬 (mceliece348864의 경우 768 × 768)을 제외한 나머지 행렬 (768×2720)만을 공개키로 저장하는 기법이 활용된다.

2.2. BIKE

BIKE는 하나의 행만으로 전체 행렬을 표현할 수 있는 Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) 코드를 사용하는 효율적인 코드 기반 암호이다. 첫 번째 행만으로 큰 크기의 행렬이 표현될 수 있기 때문에 키 크기를 줄이는데 효율적이며 BIKE는 4라운드의 코드 기반 암호 중 가장 우수한 성능을 제공한다. hamming weight가 낮은 희소 벡터 h_1, h_2가 생성되어 개인키로 사용되며, [그림 1]과 같이 순환 이동에 닫혀 있음으로써, 행렬 H_1, H_2를 표현할 수 있다.



〔그림 1〕 Quasi Cyclic code

공개키 생성 시, 이진 필드 상에서의 벡터 곱셈이 수행되어 $h = h_0 \bullet h_1^{-1}$가 공개키로 사용되며 이 또한 행렬 H를 표현할 수 있다.

복호화 시, Black-Gray-Flip (BGP) 디코더가 사용되며 디코딩 실패 확률이 존재한다. 평균 디코딩 실패 확률이 높을수록, 이로 인한 부채널 분석이 용이해진다. BIKE에서 사용되는 BGP 디코더는 부채널 분석에 사용되기 부족한 평균 디코딩 실패 확률을 제공한다. 하지만 [1]에서는, BIKE에 대한 광범위한 실험을 수행하였다. 해당 실험에서 특정 약한 비밀 키를 사용하는 경우 디코딩 실패 확률이 높아지는 것을 확인하였으며, 이로 인한 잠재적 보안 위협을 보여주었다. 현재 BIKE 암호 팀은 디코딩 실패 확률에 대한 약한 키의 영향력을 완전히 분석하지 못했기 때문에 보안 주장이 완벽하다고 할 수 없다 BIKE는 높은 성능을 보여주긴 하지만, 4 라운드에서 표준화되기 위해서는 이러한 디코딩 실패율에 대한 철저한 분석이 추가되어야 할 것으로 사료된다.

2.3. HQC

HQC는 BIKE와 같은 QC-MDPC 코드를 사용하는 코드 기반 암호이다. HQC의 경우, 부채널 공격에 취약했던 이력이 있다. [2]에서는 HQC에 대한 부채널 분석을 통해 복호화 내부, 디코딩에서 사용되는 BCH 디코더가 선택된 암호문의 오류를 수정하는지에 대한 여부를 출력하는 오라클을 구축하였다. HQC의 복호화에 적용된 해당 오라클의 출력을 기반으로 비밀키의 많은 부분을 복구할 수 있도록 하였다. 복구되지 않은 키의 나머지 부분은 선형 대수학을 기반으로 하는 알고리즘에 의해 해결됨을 보임으로써, HQC에 대한 강

력한 부채널 분석을 제시한 첫 번째 사례이다. 현재 HQC 암호 팀은 constant 구현을 제시함으로써 [2]의 부채널 분석 기법에 대한 보완을 마친 상황이다.

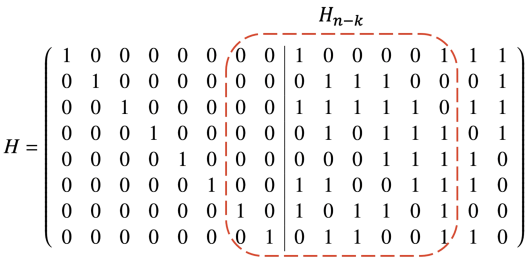
HQC 또한 BIKE와 동일하게 디코딩에 대한 실패 확률이 존재한다. 하지만 HQC의 경우, 무시 가능할 정도의 낮은 실패 확률을 제공하며 이와 관련한 안전성에 대해 철저한 분석을 제시하고 있다. 따라서 HQC는 BIKE 보다 높은 보안성을 제공한다고 평가되고 있다. 하지만 암호 알고리즘의 성능은 BIKE보다 낮은 편에 속한다.

2.4. Information Set Decoding

Information Set Decoding (ISD)은 현재, 코드 기반 암호에 대한 최적의 암호 분석 알고리즘이다. ISD는 개인키를 복구하는 것이 아닌, 공개키와 암호문만을 사용하여 비밀 벡터를 복구하는 것을 목표로 한다. n-bit 비밀 벡터 전체를 대상으로 전수 조사하는 것이 아닌 부분 벡터를 대상으로 함으로써 검색 복잡도를 줄이는 것을 목표로 한다.

초기 Prange의 ISD 알고리즘을 기반으로 하여, 다양한 ISD 알고리즘들이 제시되고 있으며, 공격 대상으로 하는 Infromation Set에 대한 접근을 달리함으로써 복잡도를 감소시킨다. 하지만 획기적인 성능 향상을 제공하지는 못하며, 암호의 보안 파라미터가 증가될 경우, 최신 ISD 알고리즘들의 공격 성능은 크게 감소한다.

신드롬 디코딩 문제 $s = He^T$ ($H \in \mathbb{F}_2^{(n-k)\times n}$, $e \in \mathbb{F}_2^n$, $s \in \mathbb{F}_2^{n-k}$)가 주어졌을 때, 일반 전수 조사는 암호문 s를 만족하는 특정 hamming weight를 가지는 n-bit 벡터에 대한 검색을 수행한다. 반면 ISD 알고리즘은 $H \in \mathbb{F}_2^{(n-k)\times n}$로부터 Information Set 행렬인 $H_{(n-k)} \in \mathbb{F}_2^{(n-k)\times(n-k)}$를 [그림 2]와 같이 재구성한 뒤, 축소된 검색 공간에서의 전수 조사를 수행한다. $(n-k)$개의 열을 선택은 반드시 순차적일 필요 없으며, 중복은 불가능하다.



〔그림 2〕 Information Set 구성 예시

이후 재구성한 Information Set 행렬 $H_{(n-k)}$에 가우스 소거를 수행함으로써 $H_{(n-k)}$의 역행렬 $H_{(n-k)}^{-1}$을 계산한다. 만약 재구성한 $H_{(n-k)}$가 invertible 하지 않을 경우, $H_{(n-k)}$를 다시 재구성해야 한다. $H_{(n-k)}^{-1}$를 계산했다면, 암호문과의 곱셈 $H_{(n-k)} \cdot s^T$을 통해 결과 벡터를 계산하며 [그림 3]과 같다.

(Information Set 행렬의 역행렬 × 암호문)의 결과 벡터의 hamming weight가 벡터 e의 hamming weight와 동일할 경우, 공격은 성공이며 이 때의 결과 벡터는 비밀 벡터 e에서 비트 값이 1인 위치 (오류)에 대한 정보를 포함한다. ISD 알고리즘은 Information Set 행렬 $H_{(n-k)}$를 재구성할 때, 비밀 벡터의 비트 값이 1에 해당하는 열들을 모두 선택했을 경우 성공한다.

결과 벡터가 Hamming weight를 만족했다는 것은, Information Set 행렬 구성 시, 오류 위치에 해당하는 열들을 모두 선택했음을 의미한다. 따라서 Information Set 행렬 구성 시 선택한 $(n-k)$에서 결과 벡터의 값이 1인 곳을 동일하게 1로 설정함으로써 비밀 벡터 e를 복구할 수 있다.

$$\begin{pmatrix} 1\,1\,0\,1\,1\,0\,1\,0 \\ 1\,1\,0\,1\,0\,1\,0\,1 \\ 1\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,0 \\ 1\,0\,1\,1\,0\,0\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0\,0 \\ 1\,0\,0\,1\,1\,1\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$(H_{n-k})^{-1}$ $\quad$ s^T

〔그림 3〕 Information Set^{-1} × 암호문 계산

2.5. Quantum Information Set Decoding

n-bit의 데이터 집합에 대한 검색은 $O(2^n)$의 검색 복잡도를 가지는 반면, 양자 알고리즘인 Grover 검색 알고리즘은 n-qubit을 대상으로 하며, 제곱근으로 감

소 된 $\sqrt{2^n}$의 복잡도를 가진다.

ISD 알고리즘은 기본적으로, 전수 조사를 기반으로 하기 때문에 Grover 알고리즘을 통한 가속화가 가능하다. 하지만 [3]에서 R. Overbeck과 N. Sendrier은 Grover 알고리즘을 사용한 ISD 알고리즘의 가속화는 온전히 고전 복잡도를 제곱근으로 감소시킬 수 없다고 주장하였다. 분할 정복 방식을 택하는 ISD 알고리즘은 Information Set을 재구성하는 첫 번째 단계와 가우스 소거를 수행하는 두 번째 단계로 구성된다. 이때, 두 번째 단계인 가우스 소거가 첫 번째 단계에 의존함으로써 Grover 알고리즘의 반복 적용이 분할 정복 방식을 효과적으로 가속화할 수 없다는 것이다.

하지만 곧이어 [4]에서 D. J. Bernstein은 양자 ISD에 대한 새로운 분석을 제시하였다. [3]의 분석은 Grover 알고리즘에 대한 저자들의 잘못된 오해일 것이며, 완전한 가속화가 달성될 수 있음을 제시하였다. n개의 열 중에서 $(n-k)$개의 열들을 선택하는 것에 있어, $(n-k)$의 hamming weight를 만족하는 중첩 상태의 n-qubit를 준비함으로써 Information Set 행렬 $H_{(n-k)}$의 재구성과 가우스 소거를 한 단계로 통합시키는 것이 가능해졌기 때문이다.

[4]를 시작으로, 고전 ISD 알고리즘에 Grover 알고리즘을 적용함으로써, 복잡도를 제곱근으로 감소시키는 연구들이 발표되고 있다. 하지만 이때 주목해야 할 것은 양자 구현 비용이다. 이에 대해서는 이미 [4]에서 언급된 바 있다. 현재, 다양한 ISD 알고리즘들이 존재하지만, 복잡도의 개선이 크지는 않다. 하지만 이 다양한 ISD 알고리즘들이 양자 컴퓨터상에서 구현되기 위한 양자 비용의 차이는 유의미하다. Stern의 ISD [5]의 경우, 고전적으로 Prange의 ISD를 개선했지만, hamming weight의 확인이 두 번 수행된다. 하지만 hamming weight를 확인하는 작업은 양자 컴퓨터에서 비교적 높은 비용을 차지하기 때문에 조금의 복잡도 개선을 위해 높은 양자 비용을 소모하는 것은 오히려 비효율적이다. 따라서 양자 버전의 최적화 된 ISD 알고리즘 구현이 중요하며 가장 단순한 Prange의 ISD알고리즘이 비교적 양자 컴퓨터상에서 효율적으로 구현될 수 있다.

Information Set 행렬 $H_{(n-k)}$이 양자 상태로 준비되었다면, 이에 대한 양자 가우스 소거가 구현되어야 한다. [7]에서는 양자 컴퓨터상에서 가우스 소거를 수행하는 데 있어 Grover 알고리즘을 사용하였다. 이러한 양자 가우스 소거가 양자 ISD에서 수행될 경우, Grover 알고리즘이 이중으로 동작하기 때문에 [3]의 상황과 같기 때문에 복잡도의 감소가 완전히 이루어지지 않는다.

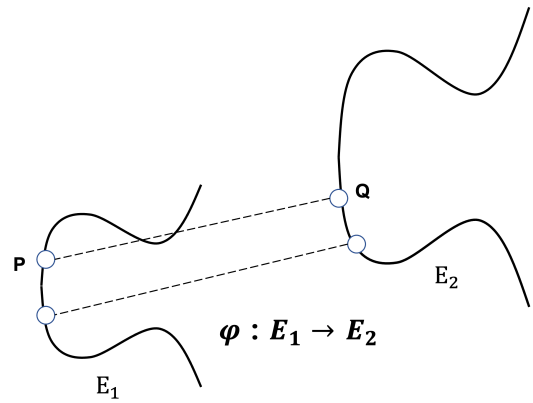
반면 [8]에서는 양자 가우스 소거를 수행하는 데 있어, Grover 알고리즘이 아닌 고전 가우스 소거 연산을 양자 회로상에서 구현하였다. 따라서 [8]의 양자 가우스 소거가 양자 ISD에서 구현되는 경우, 완전한 제곱근으로의 복잡도 감소가 달성될 수 있다.

ISD의 양자화에서 중요한 것은 공격에 사용되는 양자 자원들을 최소화하는 것이다. 이러한 측면에 있어 Classic McEliece은 공격에 요구되는 양자 자원량이 매우 높다. 왜냐하면 공격 대상이 되는 공개키 행렬의 크기가 매우 크기 때문이다. 행렬을 양자 컴퓨터상에 세팅하기 위한 큐비트 수가 매우 높고, 행렬 크기가 크기 때문에 양자 연산 또한 비용이 증가하게 된다. Classic McEliece의 단점인 공개키 크기가 오히려 양자 컴퓨터의 공격을 어렵게 만드는 요인이 되는 것이다.

아직 ISD의 양자화에 관한 연구는 더 많이 필요한 상황이며, 4라운드 후보 암호 4개 중 3개가 코드 기반 암호인 시점에서, 더욱 관심이 주목될 것으로 사료된다.

Ⅲ. 아이소제니 기반 암호

2000년대에 등장한 아이소제니 기반 암호는 타원 곡선 암호 (ECC)에서 파생되었다. 타원 곡선을 1개만 사용하는 ECC와 달리 아이소제니 기반 암호는 타원 곡선을 2개 사용한다. [그림 4]는 아이소제니 기반 암호에 사용되는 아이소제니에 대한 설명을 나타낸 것으로 타원곡선 E_1와 E_2가 있을 때, 아이소제니



〔그림 4〕 아이소제니 타원 곡선

$\phi: E_1 \rightarrow E_2$는 E_1과 E_2를 연결하는 모든 경로를 의미한다. 그림의 $E_1(P)$과 $E_2(Q)$를 연결한 선은 ϕ에 속하는 아이소제니 중 하나라고 볼 수 있다. 아이소제니 기반 암호는 아이소제니 기반 암호는 아이소제니를 찾는 어려움에 기반하며 SIDH, SIKE, 그리고 CSIDH가 대표적이다. 이 중 SIKE만이 NIST 표준화 공모전에 제출되었으며 현재 4라운드의 후보 알고리즘으로 남아 있는 상태이다.

3.1. SIDH

SIDH(Supersingular Isogeny Diffie-Hellman)는 2011년 Jao와 De Feo에 의해 제안된 아이소제니 기반 암호로, 초특이 타원 곡선 (Supersingular Elliptic Curve)을 사용하는 Diffie-Hellman 형태의 키 교환 알고리즘이다[9]. SIDH의 이전 연구인 CRS는 ordinary 곡선을 사용하여 endomorphism ring이 가환적이라 하지수 시간 공격 (sub-exponential attack)이 존재할 뿐만 아니라 속도가 비효율적이라는 문제가 존재한다. SIDH는 F_{p^2}상에서 초특이 타원 곡선 (Supersingular Elliptic Curve)을 선택하여 endomorphism ring을 비가환적으로 만들어 이러한 문제를 해결하였다. 이러한 비가환적인 특성으로 인해 Alice와 Bob이 연산한 값이 완전히 일치하지 않기 때문에 키 교환 시 j-불변수 (j-invariant)를 사용한다. SIDH의 안전성은 유한체 위에 정의된 두 개의 초특이 타원 곡선 사이의 아이소제니를 찾는 어려움에 기반한다 [10]. 두 개의 초특이 타원 곡선 사이에 알려지지 않은 높은 차수의 아이소제니를 찾는 일은 양자컴퓨터 환경에서도 어려운 문제로 여겨진다.

[11]에서 Maino와 Martindale은 SIDH의 비밀키에 해당하는 secret isogeny $\phi_A: E_0 \rightarrow E_A$ (A는 서로소 정수)를 적절한 시간에 복구할 수 있는 공격 알고리즘을 제안하였다. 해당 알고리즘에는 SSI-T (Supersingular Isogeny with Torsion) 문제가 사용된다. SSI-T 문제는 서로소 정수 A, B 일 때, 유한체 위에 정의된 초특이 타원 곡선 E_0, E 가 알 수 없는 A-차수의 isogeny $\phi_A: E_0 \rightarrow E$로 연결되고, isogeny ϕ가 시작 곡선 E_0의 비틀림 지점 (torsion point) $\phi(B)$로 제한된 경우, 이 조건에 일치하는 isogeny ϕ를 구하는 문제이다. SSI-T 문제를 이용한 해당 공격 알고리즘의 핵심은 타원 곡선 E 와 선택된 isogeny $\phi_f: E \rightarrow E_0$, 그리고 아벨 곡선(abelian surface) $E \times E_A$에서 발생하는 polarized isogeny Φ를 구성하여 이 구성 요소 중 하나로 dual secret isogeny $\phi_A: E_0 \rightarrow E_A$를 구하는 것이다. 공격은 모든 시작 곡선 E_0에 적용되며 이를 통해 SIDH의 비밀키를 복구할 수 있다.

3.2. SIKE

Jao et al.에 의해 제안된 SIKE (Supersingular Isogeny Key Encapsulation)는 SIDH 기반으로 만들어진 키 캡슐화 매커니즘이다 [12]. NIST 양자 내성 암호 표준화 공모전에 제출하기 위하여 개발된 암호 알고리즘으로, 암호문과 키 사이즈가 다른 암호 후보들보다 작다는 장점으로 주목을 받았다. 그러나 22년 취약점이 발견됨에 따라 최종 표준화에 오르지 못하고 4라운드 대체 후보군으로 진출하였다. 최근 22년 12월 공개된 NIST 양자 내성 암호 표준화 공모전 컨퍼런스에서 SIKE팀은 해당 암호가 더 이상 안전하지 않음을 인정하였고 아이소제니 기반의 암호시스템과 관련하여 더 많은 연구가 필요함을 주장하였다[13].

Castryck와 Decru가 제안한 논문 [14]이 위에서 언급한 SIKE의 취약점에 대해 다루고 있는 논문이다. [14]에서는 Kani가 제안한 'glue-and-split' 정리에 기반한 키 복구 공격을 통해 SIKE의 비밀키를 다항 시간 안에 복구하였다. 해당 공격은 SIKE의 기반이 되는 SIDH에 보조 비틀림 지점 (auxiliary torsion points)이 존재하고, 시작 타원 곡선에 non-scalar endomorphism 존재하여 최종적으로 secret isogeny를 획득할 수 있다는 취약점을 이용한 공격이다. 공격에는 Magma로 작성된 코드와 Intel Xeon CPU E5-2630v2, 2.60GHz 싱글코어가 사용되었다. SIKE 파라미터 중 양자 보안 레벨 1을 충족한 SIKEp434의 키는 약 1시간 2분 만에 복구되었고 그 밖의 파라미터

〔표 1〕 SIKE 파라미터별 키 복구 공격 수행 시간

Parameter (Security Level)	Execution time
SIKEp434 (Level 1)	1h 2m
SIKEp503 (Level 2)	2h 19m
SIKEp610 (Level 3)	8h 15m
SIKEp751 (Level 5)	20h 37m

의 키 복구 공격에 걸린 시간은 [표 1]에 나와있다.

3.3. CSIDH

CSIDH (Commutative SIDH)는 2018년 Castryck, Lange에 의해 제안된 아이소제니 기반 암호 알고리즘으로 CRS를 개선한 알고리즘이다 [15]. CSIDH는 CRS를 기반으로 하지만 ordinary 곡선이 아닌 SIDH에서 사용하는 초특이 타원 곡선에서 파라미터를 선택하여 CRS의 비효율적인 속도 문제를 개선했다. CSIDH의 안전성은 아이디얼 유군(ideal class group) $Cl(O)$에서 선택한 임의의 $[a]$와 F_p에서 정의된 타원 곡선 중 endomophism이 O 인 임의의 타원곡선 E를 군의 작용 (group action) 연산하는 것이 어렵다는 점에 기반한다. 또한 CSIDH는 F_{p^2}를 사용하는 SIDH와 달리 F_p에서 정의된 초특이 타원 곡선을 사용하고 F_p에 국한되어있기 때문에 가환성을 가진다. SIDH는 타원 곡선 (E) 뿐만 아니라 자신의 아이소제니로 상대의 공개키를 연산한 결과도 교환한 반면, CSIDH는 가환적인 성질 때문에 타원 곡선 타원 곡선 (E)만 교환한다. 또한 키 교환 시 동일한 타원 곡선을 얻을 수 있다.

[16]에서 Campos et al은 고의로 일시적인 오류를 유발하여 알고리즘이 오류를 발생 여부에 따라 1-비트의 정보를 유출할 수 있는 '안전 오류 공격 (Safe-Error attack)'에 대한 SIKE와 CSIDH의 취약성을 분석하였다. 안전 오류 공격은 크게 명령 건너뛰기 등을 통해 계산 자체를 방해하는 '전산 안전 오류 (C safe-error) 공격'과 공격자가 메모리를 수정하는 '메모리 안전 오류 (M safe-error) 공격'이 있다. SIKE와 CSIDH 공격을 위해서 공격자가 오류 주입을 통해 변수를 무작위하거나 명령을 건너뛰는 것이 가능하고, 미리 계산된 동일한 개인키를 사용하여 공유 비밀 (shared secret)의 계산을 여러 번 트리거하고 공격할 수 있다고 가정해야 한다. SIKE의 경우 성공적인 공격을 위해 공격자가 높은 정확도로 결함을 주입하였을 때 개인키의 1-비트를 드러내는 공격 루프 내의 중요한 지점을 알고 있다고 가정해야 한다. 이런 환경에서 218-비트인 개인키의 각 비트에 5개씩 총 1,090개를 주입하면 99% 이상의 전체키 복구 성공률을 달성할 수 있다. CSIDH의 목표는 실제 아이소제니와 더미 아이소제니를 구별하는 것이다. 그런데 CSIDH는 실제 구현에서 런타임이 상대적으로 길기 때문에 최대 실행 수를 미리 계산하고 그에 따른 추가 공격 매개변수를 결정해야 한다. 더미 기반 상수 시간 구현을 의미하는 MCR 구현을 공격할 때 개인 키 벡터에 양수 값만 허용이 되기 때문에 99% 이상의 성공률을 달성하기 위해서는 전체키 복구를 위해 최소 296×4= 1,184 개의 주입이 필요하다. 결론적으로 두 가지 암호 모두 제한된 실험 환경에서 안전 오류 공격을 통해 전체 키 복구가 가능함을 보였다.

SDIH, SIKE와 달리 CSIDH는 아직 치명적인 취약성이 발견되지 않았다. 이러한 이유로 양자 공격 분석 연구가 진행되고 있다 [17,18]. CSIDH가 CRS를 기반으로 하기 때문에 양자 공격은 endomorphism ring이 가환적이라는 특성을 이용한다. 이러한 특성을 이용하여 CSIDH에 Kuperberg가 제안한 hidden shift 문제를 해결하는 알고리즘 [19]을 적용하는 공격이 가장 효율적이라 여겨진다 [20].

Ⅳ. 결 론

다가오는 양자 컴퓨터 시대에 대비하여 NIST에서 진행 중인 양자 내성 암호 표준화 공모전에 세계적 관심이 주목되고 있다. 특히 공개키 분야에 있어 NIST는 격자 기반이 아닌 새로운 문제에 기반하는 암호 알고리즘을 4라운드에서 표준화할 계획이다. 이에 본 논문에서는 4라운드의 후보 알고리즘인 Classic McEliece, BIKE, HQC, 그리고 SIKE에 대한 암호 분석 기법과 몇 가지 공격 사례들을 살펴보았다. 양자 내성 암호 표준화 4라운드가 진행됨에 따라 해당 암호들에 대한 공격과 안전성 분석 연구가 더욱 활발하게 이뤄질 것으로 사료된다.

참 고 문 헌

[1] M. R. Nosouhi, S. W. Shah, L. Pan, Y. Zolotavkin, A. Nanda, P. Gauravaram, R. Doss, R, "Weak-Key Analysis for BIKE Post-Quantum Key Encapsulation Mechanism," *arXiv preprint arXiv:2204.13885*, 2022.

[2] T, Schamberger, J. Renner, G. Sigl, A. Wachter-Zeh, "A power side-channel attack on the CCA2-secure HQC KEM," *Cryptology ePrint Archive*, 2020.

[3] R. Overbeck, N. Sendrier, N,“Code-based cryptography,“ *In Post-quantum cryptography*, Springer, Berlin, Heidelberg, pp. 95-145, 2009.

[4] D. J. Bernstein, “Grover vs. mceliece,” *In International Workshop on Post-Quantum Cryptography,* Springer, Berlin, Heidelberg, pp. 73-80, 2010.

[5] J. Stern, “A method for finding codewords of small weight,” *In International colloquium on coding theory and applications,* pp. 106-113, Springer, Berlin, Heidelberg. 1989.

[6] E. Prange. “The use of information sets in decoding cyclic codes,” *IRE Transactions on Information Theory*, 8(5), pp. 5-9, 1962.

[7] D. N.Diep, D. H. Giang, N. Van Minh, “Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers,” *International Journal of Theoretical Physics*, 56(6), pp. 1948-1960. 2017.

[8] K. Jang, H. Kim, H. Seo, “Quantum Gauss-Jordan Elimination for Code in Quantum,” *In 2022 International Conference on Platform Technology and Service (PlatCon)* , pp. 44-47, 2022.

[9] D. Jao, L. De Feo. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” *in: PQCrypto, Lecture Notes in Comput. Sci. 7071, Springer*, pp. 19-34, 2011.

[10] L. De Feo, D. Jao, J. Plût. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” *Journal of Mathematical Cryptology,* 8(3), pp. 209-247, 2014 June.

[11] L. Maino, C. Martindale. “An attack on SIDH with arbitrary starting curve,” *Cryptology ePrint Archive,* 25 Aug 2022.

[12] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalili, B. Koziel, B. LaMacchia, P. Longa, et al. “SIKE: Supersingular isogeny key encapsulation”, 2017 Nov.

[13] NIST Fourth PQC Standardization Conference, https://csrc.nist.gov/csrc/media/Presentations/2022/sike-update/images-media/session-4-jao-sike-pqc2022.pdf

[14] W. Castryck, T. Decru, “An efficient key recovery attack on SIDH (preliminary version),” *Cryptology ePrint Archive*, Paper 2022/975, 2022 Aug.

[15] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, “CSIDH: An efficient post-quantum commutaitve group action,” ASIACRYPT, LNCS 11274, pp. 395-427, 2018 Dec.

[16] F. Campos, J. Krämer, M. Müller,“Safe-error attacks on SIKE and CSIDH,” *International Conference on Security, Privacy, and Applied Cryptography Engineering*, Springer, Cham, pp. 104-125, 2021 Dec.

[17] D. J. Bernstein, T. Lange, C. Martindale, L. Panny, “Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies,” *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Cham, pp. 409-441, 2019, May.

[18] X. Bonnetain, A. Schrottenloher, “Quantum security analysis of CSIDH,” *In Annual International Conference on the Theory and Applications of Cryptographic Techniques* Springer, Cham. pp. 493-522, 2020, May.

[19] G. Kuperberg, “A subexponential-time quantum algorithm for the dihedral hidden subgroup problem,” *SIAM Journal of Computing*, vol 35, no. 1, pp. 170-188, 2005.

[20] 김수리, "Isogeny 기반 암호의 최신 연구 동향," *정보보호학회지* 32, 1, pp. 19-29, 2022.

〈저 자 소 개〉

양 유 진 (Yujin Yang)

학생회원

2022년 2월 : 한성대학교 IT융합공학부 졸업
2022년 3월~현재 : 한성대학교 IT융합공학과 석사과정
<관심분야> 양자컴퓨터, 정보보안

장 경 배 (Kyungbae Jang)

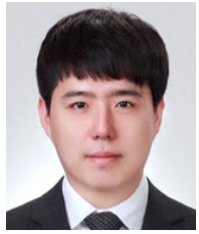
학생회원

2019년 2월 : 한성대학교 IT응용시스템공학과 공학 학사
2021년 2월 : 한성대학교 IT융합공학과 석사과정
2021년 3월~현재 : 한성대학교 IT융합공학과 박사과정
<관심분야> 양자 컴퓨터, 정보보안

오 유 진 (Yujin Oh)

학생회원

2019년 3월~현재 : 한성대학교 IT융합공학부 학사
<관심분야> 양자 컴퓨터, 암호구현



서 화 정 (Hwajeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 학사
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2016년 1월 : 부산대학교 컴퓨터공학과 박사
2016년 1월~2017년 3월 : 싱가포르 과학기술청
2017년 4월~현재 : 한성대학교 IT 융합공학부 조교수
<관심분야> 암호구현