정 보 보 호 학 회 지
제 32 권 제1호, 2022. 2

Isogeny 기반 암호의 최신 연구 동향

김 수 리*

요 약

2011 Jao와 De Feo에 의해 제안된 SIDH가 기존 타원곡선 사이의 isogeny를 이용한 암호보다 효율적인 성능을 제공하고, 그 후 2016년 Costello 등의 효율적인 연산 방법으로 SIDH 속도가 3배 이상 향상되면서, 타원곡선 사이의 isogeny를 이용한 암호가 양자 컴퓨팅 환경에서 RSA와 ECC를 대체할 암호로 주목을 받기 시작했다. 특히 isogeny 기반 암호는 다른 PQC 암호에 비해 작은 키 사이즈를 제공한다는 장점으로 현재까지 활발히 연구가 진행되고 있으며, SIDH를 기반으로 둔 SIKE는 NIST PQC 표준화 공모전 Round 3의 대체 후보이다. 다른 PQC 암호에 비해 속도가 느리다는 점이 isogeny 기반 암호의 단점인 만큼, isogeny 기반 암호는 처음 제안된 후 10년 동안 최적화를 중심으로 큰 발전을 이뤄왔다. 본 논문에서는 isogeny 기반 암호의 최신 연구 동향을 소개한다.

Ⅰ. 서 론

2011년에 Jao 와 De Feo에 의해 제안된 SIDH (Supersingular Isogeny Diffie-Hellman) 이후로 isogeny 기반 암호는 작은 키 사이즈를 장점으로 후 양자 암호 (Post-quantum cryptography, PQC)의 한 분야를 이루고 있다 [15]. 처음 타원곡선 사이의 isogeny를 이용한 암호는 2006년 Couveignes, Rostovtsev, Stolbunov에 의해 제안되어, 오늘날 CRS라 부르고 있다 [10, 21]. 하지만 CRS는 ordinary curve를 사용하기 때문에 ordinary curve의 endomorphism ring이 가환성을 가지는 성질을 이용한 Childs 등의 quantum subexponential 공격이 존재한다 [7]. RSA도 공격 복잡도가 expoential인 ECC (Elliptic curve cryptography)에 비해 subexponential 공격 복잡도를 가지지만 비교적 효율적인 속도로 널리 사용된 점을 보았을 때, CRS의 가장 큰 문제는 실생활에 사용하기에는 매우 느리다는 것이다.

Isogeny 기반 암호는 2011년 SIDH에 의해 다시 주목을 받게 되었다. SIDH는 supersingular curve를 사용해서 Childs 등의 공격에 대응할 수 있을 뿐만 아니라 효율적인 속도를 가진다. 특히, 2016년 Costello등이 제안한 최적화 방법은 기존 SIDH의 속도를 3배나 빠르게 해서 실제 사용을 가능하게 하였고, 이를 기반으로 둔 SIKE는 현재 NIST PQC 표준화 공모전 Round 3의 대체 후보이다.

한편, 처음 제안된 CRS는 128 비트의 보안강도에서 대략 229초 정도의 시간이 소요돼서 실제 사용하기에는 비효율적인 단점을 가지고 있으나, SIDH와 달리 non-interative 키 교환 알고리즘을 제공한다는 장점이 있다. SIDH의 경우 비가환적인 성질 때문에 연산된 결과뿐만 아니라 추가적인 정보를 전달해야 이후의 연산을 진행해서 키 교환이 이루어질 수 있다. 아직 이러한 추가적인 정보를 이용한 효율적인 공격 방법이 존재하지는 않지만, 전달해야 할 메시지의 크기가 클 뿐만 아니라, 향후 공격에 대응하는 차원에서 CRS의 non-interactive 한 성질은 매력적이다. 따라서 De Feo 등과 Castryck 등이 각각 독립적으로 CRS를 최적화하려는 연구를 진행했다 [5, 11]. 그 중 Castryck이 제안한 CSIDH (Commutative SIDH)는 CRS를 supersingular curve를 사용해 구현해서 기존 SIDH보다 느리지만 작은 키 사이즈를 제공한다 [5].

하지만, 초기 ECC 제안과 유사하게 타원곡선을 이용하는 isogeny 기반 암호도 다른 PQC 알고리즘보다 키 사이즈가 작다는 장점이 있으나, 속도가 느리다는 단점을 가지고 있다. 32 비트 내의 행렬-벡터 연산으로 구

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2021-0-00518, 블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발)
* 성신여자대학교 수리통계데이터사이언스학부 (조교수, suhrikim@sungshin.ac.kr)

성된 다른 PQC 암호보다 isogeny 기반 암호는 400 비트 이상의 기존 ECC보다도 큰 유한체를 기반으로 이차 확장체 연산과 isogeny 연산이 추가되어 몇 배나 느린 속도를 가지고 있다. 따라서 isogeny 기반 암호는 알고리즘에 대한 최적화 관점으로 연구가 많이 진행됐다. Isogeny 기반 암호의 최적화 연구 중 한 갈래는 구현 관점의 최적화이고, 다른 갈래는 스킴 변형을 통한 최적화가 있다. 구현 관점에서는 isogeny 연산 자체의 최적화로, isogeny 연산을 효율적으로 수행할 수 있는 다른 타원곡선의 형태를 확인하거나, isogeny 공식 자체의 최적화이다 [2,17,18,19,20]. 스킴 변형을 통한 최적화 방법으로는, 기존 스킴을 구현이 쉬운 환경으로 변형시키는 방법이다. [8]에서는 SIDH의 유한체 연산을 효율적으로 수행하도록 변형한 스킴인 BSIDH를 제안하였고, [4]에서는 CSIDH의 연산을 효율적으로 수행하기 위해 CSURF를 제안하였다.

위에서 살펴본 바와 같이 isogeny 기반 암호는 다른 PQC 암호보다 연구가 시작된 지 얼마 안 되었지만, 활발히 진행되고 있다. 특히 최근에는 isogeny 기반 암호에 대한 면밀한 고전 및 양자 안전성 분석이 이루어지면서 더 안전하면서 효율적인 파라미터를 설정하는 연구가 진행되고 있다. 본문에서는 이러한 isogeny 기반 암호의 최신 연구 동향을 소개한다. 본문의 구성은 다음과 같다. 먼저 2장에서는 isogeny 기반 암호를 이해하는데 필요한 기본 지식을 설명한다. 3장에서는 isogeny 기반 암호의 대표 알고리즘인 SIDH와 CSIDH에 대해 소개를 하고 간단하게 키 사이즈와 성능을 비교한다. 4장에서는 현재 isogeny 기반 암호의 연구 동향 – 최적화 및 안전성 분석 – 에 대해 소개한다. 마지막으로 5장의 결론으로 마무리한다.

Ⅱ. 배경 지식

본 장에서는 isogeny 기반 암호를 이해하는데 필요한 배경 지식을 소개한다. 먼저 타원곡선에 대한 간단한 이론을 소개하고, isogeny의 정의 그리고 isogeny를 연산하는 Velu의 공식을 소개한다.

2.1. Elliptic Curves

K를 characteristic이 2나 3이 아닌 field라 가정하자. K위에 정의된 타원곡선은 genus 1인 무한원점을 가지는 smooth, projective curve이다. 이 무한원점과 타원곡선 위의 점은 타원곡선의 덧셈 연산을 통해 그룹을 이룬다는 성질은 잘 알려져 있다. 또한, Riemann-Roch의 정의에 의해서 모든 타원곡선은 두 변수로 이루어진 3차식으로 정의될 수 있다. 예를 들어, 타원곡선은 다음과 같은 형태로 표현될 수 있다.

$$W_{\alpha,\beta} : y^2 = x^3 + \alpha x + \beta \tag{1}$$

위 식에서 $4\alpha^3 + 27\beta^2 \neq 0$을 만족한다. 이와 같은 형태로 정의된 타원곡선을 short Weierstrass curve라 한다. 또한, 타원곡선은 다음과 같은 형태로도 정의될 수 있다.

$$M_{A,B} : By^2 = x^3 + Ax^2 + x \tag{2}$$

위 식에서 $B(A^2-4) \neq 0$을 만족한다. 이와 같이 정의된 타원곡선을 Montgomery curve라 한다. Short Weierstrass curve의 j-invariant는 $j(W_{\alpha,\beta}) = 1728 \cdot 4\alpha^3/(4\alpha^3+27\beta^2)$으로 정의되고, Montgomery curve의 경우 $j(M_{A,B}) = 256(A^2-3)^3/(A^2-4)$로 정의된다. 일반적으로 K에서 정의된 두 타원곡선 E, E'에 대해서 $j(E) = j(E')$를 만족한다면 두 타원곡선은 $\overline{K}$에서 서로 isomorphic 하다.

한편, K가 characteristic 이 p인 field라 하고 E를 K 위에 정의된 타원곡선이라 하자. ℓ이 소수일 때 다음이 성립한다.

$$E[\ell] \cong \begin{cases} Z/\ell^e Z \oplus Z/\ell Z & \text{if } \ell \neq p, \\ Z/\ell^e Z \text{ or } \{O\} & \text{if } \ell = p. \end{cases} \tag{3}$$

여기에서 $E[\ell]$은 다음과 같이 정의된다.

$$E[\ell] := \{P \in E(\overline{K}) \mid \ell P = O\} \tag{4}$$

만약, E가 조건 $E[p] \cong Z/pZ$ 를 만족시키면 ordinary curve라고 하고, 조건 $E[p] \cong \{O\}$를 만족시키면 supersingular curve라고 한다.

2.2. Isogeny

두 타원곡선 E_1, E_2 사이의 isogeny 는 유한 커널을 가지는 non-constant surjective group homomorphism 을 의미한다. 두 타원곡선이 K에서 isogenous 하다는 것은 isogeny $\phi: E_1 \rightarrow E_2$ 가 존재한다는 것을 의미한다. K에서 정의된 isogeny ϕ는 일반적으로 다음과 같은 형태로 나타내어진다.

$$\phi: (x,y) \rightarrow \left(\frac{a(x)}{c(x)}, \frac{b(x)}{d(x)} y \right) \tag{5}$$

여기에서 $a(x), b(x), c(x), d(x) \in K[x]$이고 $\gcd(a(x), c(x)) = \gcd(b(x), d(x)) = 1$을 만족한다. Isogeny ϕ의 차수는 $\max(\deg(a(x)), \deg(c(x)))$로 정의되며, $\left(\frac{a(x)}{c(x)} \right)' \neq 0$을 만족하는 경우 ϕ를 separable isogeny라 한다. 또한, separable isogeny의 경우 isogeny의 차수는 커널의 원소의 개수와 같으며, ℓ차 isogeny를 ℓ-isogeny라 부른다. 모든 separable ℓ-isogeny $\phi: E_1 \rightarrow E_2$에 대해서 같은 차수를 가지는 dual isogney $\hat{\phi}$가 존재하고, 다음을 만족한다.

$$\phi \circ \hat{\phi} = [\ell]_{E_1}, \ \hat{\phi} \circ \phi = [\ell]_{E_2} \tag{6}$$

여기에서 $[\ell]_{E_1}$은 E_1에서의 multiplication-by-ℓ map을 의미하고, $[\ell]_{E_2}$는 E_2에서의 multiplication-by-ℓ map을 의미한다. ℓ이 만약 합성수 $\ell = p_0^{e_1} p_1^{e_2} \cdots p_n^{e_n}$일 경우 다음과 같이 p_i-isogeny 인 ϕ_i들로 합성하여 나타낼 수 있다.

$$\phi = \phi_1^{e_1} \circ \cdots \phi_n^{e_n} \tag{7}$$

2.3. Velu's formula

두 타원곡선 사이의 isogeny를 연산하는 방법으로는 크게 두 가지가 있다. 첫 번째 방법은 Velu의 방법으로, 타원곡선과 타원곡선의 유한 subgroup이 주어져 있을 때, 주어진 subgroup을 커널로 하는 isogeny를 계산하는 방법이다. 후에 Kohel이 kernel polynomial을 이용해서 isogeny를 계산하는 방법을 제안하였다. 현재 isogeny 기반 암호의 경우 Velu의 공식을 이용해서 isogeny를 계산하고 있으며, 따라서 본문에는 Velu의 방법을 다루도록 한다.

K위에 주어진 타원곡선 E에 대해서 Velu의 공식은 다음 변환에 기반을 둔다.

$$(x_P, y_P) \rightarrow \left(x_P + \sum_{Q \in G - \{O\}} (x_{P+Q} - x_Q), y_P + \sum_{Q \in G - \{O\}} (y_{P+Q} - y_Q) \right) \tag{8}$$

위 공식을 short Weierstrass curve에 적용한 결과는 다음과 같다. 타원곡선 $W_{\alpha,\beta}$의 유한 subgroup G가 주어져 있다고 하자. 먼저 $G - \{O\}$를 다음을 만족하는 두 집합 G^+, G^-으로 분할한다.

$$G - O = G^+ \cup G^-$$
$$Q \in G^+ \text{ 이면, } -Q \in G^-$$

커널의 각 원소 $Q \in G^+$에 대해서 다음을 연산한다.

$$g_Q^x = 3x_Q^2 + \alpha$$
$$g_Q^y = -2y_Q$$
$$v_Q = 2g_Q^x$$
$$u_Q = (g_Q^y)^2$$
$$v = \sum_{Q \in G^+} v_Q$$
$$w = \sum_{Q \in G^+} u_Q + x_Q v_Q$$

그러면 G를 커널로 하는 isogeny ϕ는 다음과 같이 정의된다.

$$\phi(x,y) \rightarrow (x', y')$$
$$x' = x + \sum_{Q \in G^+} \frac{v_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2}$$
$$y' = y - \sum_{Q \in G^+} \frac{2u_Q y}{(x - x_Q)^3} + v_Q \frac{y - y_Q - g_Q^x g_Q^y}{(x - x_Q)^2} \tag{9}$$

Isogeny ϕ의 차수는 커널 G의 원소의 개수와 같으며, image curve의 식은 다음과 같이 정의된다.

$$E' : y^2 = x^3 + (\alpha - 5v)x + (\beta - 7w) \quad (10)$$

Ⅲ. Isogeny 기반 암호

본 장에서는 isogeny 기반 암호의 대표 알고리즘인 SIDH와 CSIDH 에 대해 소개하고, 같은 고전 보안강도에서 두 알고리즘의 성능을 비교한다.

3.1. SIDH

SIDH는 2011년에 Jao와 De Feo에 의해 처음으로 제안되었다 [15]. 처음 제안된 CRS 기반 암호는 ordinary curve 사용으로 인해 Childs 등이 제안한 quantum sub-exponential 공격에 취약하다는 단점이 있으나, 그보다도 ordinary curve 사용으로 파라미터 선택이나 구현이 쉽지 않아 실제 사용하기에는 비효율적이라는 단점이 있다. Jao 와 De Feo는 이 비효율적인 문제를 supersingular curve를 사용함을 통해서 해결하였고, 추가적인 정보 전달로 supersingular curve의 non-commutative를 해결하여 Diffie-Hellman 형태의 키 교환 알고리즘을 제안하였다.

서로 소인 두 수 ℓ_A, ℓ_B에 대해서 소수 $p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1$ 을 선택한다. 여기에서 $\ell_A^{e_A} \approx \ell_B^{e_B}$를 만족하도록 e_A, e_B를 선택한다. 이러한 소수 p에 대해서 SIDH는 F_{p^2}에 정의된 supersingular elliptic curve E를 사용한다. E는 supersingular curve이기 때문에 E의 위수는 $\left(\ell_A^{e_A}\ell_B^{e_B} f\right)^2$을 만족한다. 이 경우 ℓ^e-torsion subgroup을 정의할 수 있는데, 여기에서 $\ell \in \{\ell_A, \ell_B\}$ 이고 $e \in \{e_A, e_B\}$를 의미한다. $\ell_A^{e_A}$-torsion subgroup 에 대한 기저 $\{P_A, Q_A\}$를 선택하고, $\ell_B^{e_B}$-torsion subgroup에 대한 기저 $\{P_B, Q_B\}$를 선택한다.

Alice와 Bob가 서로 키를 교환한다고 하자. Alice의 기저를 $\{P_A, Q_A\}$라 하고, Bob의 기저를 $\{P_B, Q_B\}$라 하자. 키 생성 단계에서, Alice는 개인키 m_A, n_A를 $Z/\ell_A^{e_A}Z$에서 선택을 한다. 이때, m_A, n_A가 둘 다 ℓ_A로 나누어지지 않도록 한다. 그 후, cyclic subgroup $\langle R_A \rangle = \langle [m_A]P_A + [n_A]Q_A \rangle$를 연산한다. 그리고 Velu의 공식을 이용해서 $\langle R_A \rangle$를 커널로하는 $\ell_A^{e_A}$-isogeny $\phi_A : E \rightarrow E_A = E/\langle R_A \rangle$를 연산한다. Alice는 연산된 타원곡선 E_A와 자신의 개인키 ϕ_A로 상대방의 기저를 연산한 값인 $\phi_A(P_B)$, $\phi_A(Q_B)$를 Bob에게 전달한다. Bob도 마찬가지의 과정을 거쳐서 $(E_B, \phi_B(P_A), \phi_B(Q_A))$를 Alice에게 전달한다.

키 성립 단계에서는, Alice는 Bob에게 받은 $\phi_B(P_A)$, $\phi_B(Q_A)$를 이용해서 subgroup $\langle R_A' \rangle = \langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$를 연산한다. 그리고 Velu의 공식을 이용해서 $\langle R_A' \rangle$를 커널로 하는 isogeny를 연산해서 타원곡선 $E_{AB} = E_B/\langle R_A' \rangle$를 생성한다. Bob도 동일한 과정을 거쳐서 타원곡선 $E_{BA} = E_A/\langle R_B' \rangle$를 연산한다. Alice와 Bob의 공유한 비밀키는 E_{AB}, E_{BA}의 j-invariant인 $j(E_{AB}) = j(E_{BA})$이다.

3.2. CSIDH

CSIDH는 Castryck 등에 의해 제안된 isogeny 기반 Diffie-Hellman 스타일의 키 교환 프로토콜이다 [5]. CSIDH는 유한체 F_p위에 정의된 supersingular 타원곡선에서 가환성을 가지는 group action 연산을 이용한 알고리즘이다. O를 이차 수체에서의 order라 하자. $E\ell\ell_p(O)$를 endormophism ring을 O로 하는 F_p위에 정의된 타원곡선들의 집합이라 하자. 그러면 class group $Cl(O)$가 $E\ell\ell_p(O)$에서 자유롭고 전이적으로 작용한다는 것은 잘 알려져 있다. 이러한 group action은 $[a]E$로 표현할 수 있는데, 여기서 $E \in E\ell\ell_p(O)$이고, $[a] \in Cl(O)$이다.

소수 p는 $p = 4\ell_1\ell_2 \cdots \ell_n - 1$의 형태를 가지는 소수라 정의하자. 여기에서 $\ell_1, \cdots, \ell_n$은 서로 다른 홀수인 작은 소수이다. E를 $End_p(E) = Z[\pi]$를 만족하는 F_p위에서 정의된 supersingular 타원곡선이라 하자. 여기서 $End_p(E)$는 F_p에서 정의된 E의 endomorphism ring을 의미한다. 또한, $End_p(E)$는 quaternion order $End(E)$의 가환적인 subring 이다. 따라서 Frobenious 의 trace는 0이 되고, $E(F_p) = p + 1$을 만족한다.

$\pi^2-1\equiv 0 \bmod \ell_i$를 만족하기 때문에, 아이디얼 $\ell_i O$는 $\ell_i O=\mathfrak{l}_i\bar{\mathfrak{l}}_i$의 형태로 분리될 수 있고, 여기에서 $\mathfrak{l}_i=(\ell_i,\pi-1)$, $\bar{\mathfrak{l}}_i=(\ell_i,\pi+1)$이다. 그러면 group action $[\mathfrak{l}_i]E$는 Velu의 공식을 이용해서 F_p위의 isogeny $\phi_{\mathfrak{l}_i}$로 연산될 수 있다.

Alice와 Bob가 서로 키를 교환한다고 하자. Alice는 개인 벡터 $(e_1,\cdots,e_n)\in Z^n$에서 선택하는데, 이때 각각의 e_i는 양의 정수 m에 대해서 $e_i\in[-m,m]$의 범위를 가진다. 이 벡터가 아이디얼 클래스 $[a]=[\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_n^{e_n}]$에 대해 group action과 연관된 isogeny를 나타낸다. Alice는 공개키 $E_A=[a]E$를 연산하고 E_A를 Bob에게 전달한다. Bob도 Alice와 동일한 과정을 반복한 뒤, 공개키 $E_B=[b]E$를 전달한다. Bob의 공개키를 받은 뒤, Alice는 $[a]E_B$를 연산하고, Bob도 마찬가지로 $[b]E_A$를 연산한다. 가환성에 의해 $[a]E_B=[b]E_A$를 만족하게 된다.

3.3. 성능비교

본 장에서는 SIDH와 CSIDH의 성능을 비교한다. 먼저 고전 128비트 보안강도에 대해서 SIDH와 CSIDH의 파라미터를 비교한다.

표 1에서 n은 F_{p^2}에서의 난수를 의미한다. [Table 2]에서 A는 Montgomery 타원곡선의 계수를 의미한다. 표 1과 표 2에서 확인할 수 있듯이, CSIDH는 확장체를 사용하지 않아 SIDH에 비해 더 작은 키 사이즈를 제공할 수 있다. 또한 CSIDH는 가환성을 가지기 때문에, SIDH와 달리 j-invariant를 추가로 계산할 필요가 없으며, 타원곡선의 계수 자체를 공유되는 비밀키로 사용할 수 있다.

〔표 1〕 128-bit 고전 보안강도를 만족하는 SIDH 파라미터

	Form	Size
Field	F_{p^2} $p=2^{250}3^{159}-1$	125 byte
Public key	$P\in F_p$, $Q\in F_{p^2}$ $R(=P-Q)\in F_{p^2}$	312 byte
Private key	n	125 byte
Share key	$j(E)$	125 byte

〔표 2〕 128-bit 고전 보안강도를 만족하는 CSIDH 파라미터

	Form	Size
Field	F_p $p=2^2\cdot 3\cdots 587-1$	64 byte
Public key	A	64 byte
Private key	$[a]=(e_1,\cdots,e_{74})$ $e_i\in[-5,5]$	-
Share key	A	64 byte

다음 표는 고전 128비트 보안강도에 대해 SIDH와 CSIDH의 성능을 비교한다. 실험은 3.6GHz의 동작주파수를 가지는 Intel Core i7-7700를 이용하였으며, gcc version 9.3.0을 이용해서 컴파일하여 clock cycle을 측정하였다.

위의 표에서 확인할 수 있듯이, SIDH에 비해 CSIDH가 키 사이즈는 작지만 성능은 느리다는 것을 확인할 수 있다.

〔표 3〕 128-bit 고전 보안강도에서 SIDH와 CSIDH의 성능 비교

	CSIDH-512	SIDHp503
Alice's keygen	97,651,094	6,583,388
Bob's keygen	97,513,554	7,300,580
Alice's shared key	97,504,685	5,366,237
Bob's shared key	97,536,566	6,165,835
Total	390,205,899	25,416,040

Ⅳ. Isogeny 기반 암호의 최신 연구 동향

본 장에서는 isogeny 기반 암호의 최신 연구 동향을 소개한다. Isogeny 기반 암호는 다른 PQC 암호보다 키 사이즈가 작다는 장점은 가지고 있으나, 느리다는 단점이 있어 최적화를 중심으로 연구가 진행되고 있으며, 스킴 자체의 변형을 통한 최적화, isogeny 연산 공식 최적화의 두 분야로 나누어 진행되고 있다. 마지막으로 최근 isogeny 기반 암호의 고전 및 양자 안전성 분석을 통한 파라미터 최적화를 확인해본다.

4.1. 스킴 변형을 통한 최적화

4.1.1. BSIDH

2020년에 Costello에 의해 제안된 BSIDH는 twisted torsion을 활용한 SIDH의 변형된 알고리즘이다 [8]. SIDH는 소수 p에 대해서 유한체 F_{p^2}에서 정의된 supersingular 타원곡선을 사요앟고 있다. 여기에서 소수 p는 서로 소인 두 수 ℓ_A, ℓ_B에 대해서 $p=\ell_A^{e_A}\ell_B^{e_B}\cdot f\pm 1$의 형태이다. 효율적인 유한체 감산 연산과 isogeny 연산을 위해 $\ell_A=2$, $\ell_B=3$을 사용하고 있으나, 일반 타원곡선 암호와 비교하면 효율적인 감산연산을 구현하기 힘들다. 따라서 Costello는 감산연산이 효율적인 유한체를 활용하여, client인 Alice는 2-isogeny를 활용하고, server인 Bob은 비교적 높은 차수의 isogeny를 동일하게 효율적인 유한체에서 연산하는 방법을 제안하였다.

E을 F_{p^n} 위에서 정의된 타원곡선이라 하고, t_n을 p^n-power Frobenius endomorphism의 trace라 하자. 타원곡선의 위수는 $\#E(F_{p^n})=p^n+1-t_n$ 이고, $|t_n|\le 2\sqrt{p^n}$를 만족하게 되는데, 특히 E가 supersingular curve인 경우 t_n은 p의 배수가 된다. 역으로 t_n이 p의 배수이면 E가 supersingular curve가 된다. 한편, $n=1$일 때, $|t_1|\le 2\sqrt{p}$를 만족하면서 t_1이 p의 배수가 되는 값은 $t_1=0$인 한 경우밖에 존재하지 않는다. 따라서 F_p 위에서는 E가 supersingular curve라는 것과 $\#E(F_p)=p+1$ 인 것은 동치이다. 그러나 $n=2$인 경우에 t_2가 p의 배수가 되는 경우는 많이 존재하며, 구체적으로는 $t_2\in\{-2p,-p,0,p,2p\}$가 된다. Isogeny 기반 암호의 경우 $t_2=-2p$ 혹은 $t_2=2p$인 경우를 사용한다. 특히, $t_2=-2p$를 만족하는 타원곡선은 $t_2=2p$를 만족하는 타원곡선과 quadratic twist 관계에 있다. Quadratic twist의 의미는, 두 곡선은 F_{p^4}에서 isogenous 할 뿐만 아니라 F_{p^4}에서 isomorphic 하다는 것을 의미하고, CSIDH에서처럼 isogeny 연산도 twist에서도 사용할 수 있다. 구체적으로, $t_2=-2p$인 경우 사용하는 isogeny 연산 공식과 $t_2=2p$에서 사용되는 isogeny 연산 공식이 같다. 또한, $t_2=-2p$인 경우 타원곡선의 그룹 구조는

$$E(F_{p^2})\cong Z_{p+1}\times Z_{p+1}$$

이 되고, $t_2=2p$인 경우 타원곡선의 그룹 구조는

$$E^t(F_{p^2})\cong Z_{p-1}\times Z_{p-1}$$

이 된다. 그룹 구조가 $Z_{p-1}\times Z_{p-1}$인 모든 supersingular curve는 그룹 구조가 $Z_{p+1}\times Z_{p+1}$인 supersingular curve와 quadratic twist 관계를 이룬다. 또한, $p+1$을 나누는 어느 수 r도 $E(F_{p^2})$에서 전체 rational r-torsion을 이루는 것처럼, $p-1$을 나누는 어느 수 s도 $E^t(F_{p^2})$에서 전체 rational s-torsion을 이루게 된다.

전체적으로 BSIDH 는 $(p+1)$-torsion 과 $(p-1)$-torsion을 활용하여 연산을 진행하게 되는데, quadratic twist가 존재하는 유한체 상, 모든 알고리즘 자체가 F_{p^4} 위에서 정의된다. 하지만, 결론적으로는 Montgomery 곡선을 활용해서 구현할 경우 F_{p^2}에서 정의되는 x좌표만 활용하면 되기 때문에 기존 SIDH와 동일한 연산을 사용할 수 있다.

결론적으로 BSIDH는 SIDH와 달리 Mersenne 소수나 Ridinghood 소수와 같이 2의 큰 지수승이 소수 $p+1$을 나누는 형태의 수를 사용한다. 이 소수를 사용하면, Alice는 기존과 같이 2^m-isogeny를 SIDH나 SIKE보다 더 효율적인 유한체 위에서 연산한다. 하지만, 이러한 소수들은 $p-1$이 smooth 하지 않을 확률이 높아서, Bob의 isogeny 연산은, 기존 3^n-isogeny 연산보다 더 느릴 수 있다. 아래 표는 [1]에서 Python-3을 이용해 구현된 BSIDH의 성능을 예측한 결과이다. 구현 결과는 유한체 위에서 곱셈 연산량을 측정하기 때문에, 곱셈에 드는 cycle count를 이용해서 연산을 예측하였다. 곱셈 cycle 측정은 Skylake를 이용하였으며, 특정에 사용된 파라미터는 다음과 같다. 해당 파라미터는 NIST 보안강도 기준 1을 따른다.

위 표의 결과, BSIDH는 Bob의 isogeny 차수로 인해서 동일한 보안강도에서 SIKE보다 성능이 좋지 않지

〔표 4〕 SIKE, CSIDH, BSIDH의 성능 비교〔1〕

Implementation	Instantiation	M cycles
SIKE	SIKEp434	22
Castryck et al.	CSIDH-512 unprotected	4×155
Bernstein et al.	CSIDH-512 unprotected	4×153
	CSIDH-1024 unprotected	4×760
Cervantes-Vazquez et al.	CSIDH-512 MCR style	4×339
	CSIDH-512 OAYT style	4×238
Hutchinson et al	CSIDH-512 OAYT style	4×229
Chi-Dominguezt et al.	CSIDH-512 MCR style	4×282
	CSIDH-512 MCR style	4×223
	BSIDHp253	119

만, 대부분의 CSIDH와 비교하면 성능이 좋다는 것을 알 수 있다.

4.1.2. CSURF

CSIDH는 F_p위에서 정의된 supersingular curve를 사용하여 CRS를 구현하여, 기존 CRS의 장점인 Diffie-Hellman 스타일의 non-interactive 키 교환 알고리즘을 제공하면서 효율적인 속도를 가지게 되었다. 하지만, 알고리즘 특성상 유한체 F_p 의 소수 p를 나누는 작은 홀수 소수 ℓ에 대해서 ℓ-torsion point를 선택하고, 이를 이용해 isogeny 연산을 진행해야 하는데, ℓ-torsion point를 생성하는데 실패하는 확률이 $1/\ell$로, 이는 소수가 작을수록 실패 확률이 크다는 것을 의미한다. 따라서 CSURF는 사용하는 유한체 소수를 $p \equiv 7 \bmod 8$로 변경해 2-isogeny를 활용하는 CSURF를 제안한다 [4]. 제안하는 방법은 빠른 2-isogeny를 많이 사용하고, 큰 소수에 해당하는 isogeny를 적게 사용해서 연산 효율성을 높인다. 또한, 기존 CSIDH의 경우 각 소수에 해당하는 비밀 지수를 동일한 범위 내에서 선택하게 하였다면, CSURF의 경우 실패 확률이 큰 작은 소수 차수 isogeny와 연산 복잡도가 높은 큰 소수 차수 isogeny를 줄이기 위해 이러한 소수에 해당하는 비밀 지수는 작은 범위 내에서 선택하도록 하고, 같은 보안강도를 제공하기 위해서 그 이외의 소수들은 기존보다 크거나 같은 범위 내에서 선택하게 하였다.

4.2. Isogeny 연산 최적화

Isogeny 기반 암호를 구현하는 데 있어서 핵심적인 부분은 isogeny 연산으로, isogeny 연산이 효율적이어야 전반적인 알고리즘 자체도 효율적으로 구현될 수 있다. 특히 CSIDH가 제안되면서 큰 홀수 차수의 isogeny를 효율적으로 연산하는 것이 더 중요해졌다. 이에 따라 Bernstein 등은 [2]에서 효율적인 높은 차수의 isogeny 연산 방법에 대해서 제안했다. 일반적으로 원소의 개수가 n인 타원곡선의 부분집합을 커널로 하는 isogeny는 Velu의 공식을 이용하면 $O(n)$의 연산량으로 계산이 가능하다. Bernstein 등은 이를 $O(\sqrt{n})$의 연산량으로 계산되는 방법을 제안했으며, 제안하는 방법은 100 차수 이상의 isogeny일 경우 더 효율적이다.

먼저, Velu의 공식을 이용한 isogeny 연산을 단순화시키면, 유한체 K에서 정의된 다항식의 함수값을 계산하는 것으로 볼 수 있으며, 특히 이 다항식은 cyclic group의 원소들을 근으로 가진다는 특징이 있다. G를 P로 생성된 cyclic group이라 가정하자. 그러면 Z의 유한 부분집합 S에 대해서 다음과 같이 다항식을 정의한다.

$$h_S(X) = \prod_{s \in S} (X - f([s]P))$$

여기에서 $[s]P$는 P를 s번 그룹 연산한다는 것을 의미한다. 이를 isogeny 기반 암호로 가져온다면, 타원곡선 $E(K)$에 대해서 $P \in E(K)$가 되고, P를 ℓ-torsion point라 한다면 $G = \langle P \rangle$는 ℓ-isogeny $\phi : E \rightarrow E'$ 의 커널이 되며, $f([s]P)$는 $[s]P$의 x좌표에 해당한다고 볼 수 있다.

M_a를 Montgomery curve라 하고 $P \in M_a$를 위수가 2가 아닌 소수 ℓ이라 하자. $\langle P \rangle$를 커널로 하는 isogeny $\phi : M_a \rightarrow M_{a'}$의 함수값 연산을 위의 식을 이용해 나타나면 다음과 같이 표현할 수 있다.

$$\phi(X) = \frac{X^{\ell} \cdot h_S(1/X)^2}{h_S(X)^2}$$

여기에서 $d=((a-2)/(a+2))^{\ell}\cdot(h_S(1)/h_S(-1))^8$에 대해 $a'=2(1+d)/(1-d)$를 의미한다. 따라서 $\phi(X)$가 $O(\sqrt{\ell})$의 연산량을 가진다는 것의 의미는 $h_S(X)$가 $O(\sqrt{\ell})$의 연산량을 가진다는 것과 동치이다. $h_S(X)$도 단순히 연산하면 $O(\ell)$의 연산량을 가지지만, G의 구조를 활용하면 연산량을 줄일 수 있다. 실제로 modular factorial을 연산하는 방법에서도 이를 활용하고 있다.

$h_S(X)$를 $O(\sqrt{\ell})$의 연산량으로 연산하기 위한 핵심 과정은 S를 크기가 $\sqrt{S}$과 유사하고 특정 조건을 만족하는 더 작은 집합 I,J로 나누는 것이다. []에서는 S의 대부분의 원소가 $(I+J)\cup(I-J)$로 표현되도록 I,J를 선택하고 있다. 따라서, 근이 $[s]P$로 구성된 다항식의 함수값을 계산하는 것은, $i\in I,\ j\in J$에 대해서 근이 $[i]P$, $[j]P$로 구성된 다항식의 함수값을 계산하는 것으로 생각할 수 있다. 그 뒤 이러한 다항식들의 resultant를 이용하면 h_S를 구할 수 있다. 이를 이용하기 위해서는 $i\in I,\ j\in J$에 대해서 $[i]P$, $[j]P$, $[i+j]P$, $[i-j]P$의 x좌표들 사이의 관계를 찾아야 한다. 아래 lemma는 타원곡선 E의 점 $P,Q\in E$에 대해서 $P,Q,P+Q$와 $P-Q$의 관계를 나타내는 biquadratic polyonomial의 존재성에 대해서 제시한다,

Lemma 1. q를 소수의 지수형태라 가정하자. 타원곡선 $E(F_q)$와 $O\notin\{P,Q,P+Q,P-Q\}$를 만족하는 모든 $P,Q\in E$에 대해서 다음 식을 만족하는 biquadratic polynomial F_0,F_1,F_2는 $F_q[X_1,X_2]$에 존재한다.

$$(X-x(P+Q))(X-x(P-Q))$$
$$=X^2+\frac{F_1(x(P),x(Q))}{F_0(x(P),x(Q))}X+\frac{F_2(x(P),x(Q))}{F_0(x(P),x(Q))}$$

위 식에서 $x(P)$는 P의 x좌표를 의미한다.

만약 E가 $By^2=x^3+Ax^2+x$로 주어진 Montgomery curve일 경우 F_0,F_1,F_2는 다음과 같이 정의할 수 있다.

$$F_0(X_1,X_2)=(X_1-X_2)^2$$
$$F_1(X_1,X_2)=-2((X_1X_2+1)(X_1+X_2)+2AX_1X_2)$$
$$F_2(X_1,X_2)=(X_1X_2-1)^2$$

이를 활용하여 $h_S(X)$를 구하는 알고리즘은 다음과 같다.

Algorithm 1.
Computing $h_S(\alpha)=\prod_{s\in S}(\alpha-x([s]P))$ for $P\in E(F_q)$

INPUT : $\alpha\in F_q$

OUTPUT : $h_S(\alpha)$ where $h_S(X)=\prod_{s\in S}(X-x([s]P))$

1. $h_I\leftarrow\prod_{i\in I}(Z-x([i]P))\in F_q[Z]$
2. $D_J\leftarrow\prod_{j\in J}F_0(Z,x([j]P))\in F_q[Z]$
3. $\triangle_{I,J}\leftarrow Res_Z(h_I,D_J)\in F_q$
4. $E_J\leftarrow\prod_{j\in J}(F_0(Z,x([j]P))\alpha^2$
   $+F_1(Z,x([j]P))\alpha+F_2(Z,x([j]P))\in F_q[Z]$
5. $R\leftarrow Res_Z(h_I,E_J)\in F_q$
6. $h_K\leftarrow\prod_{k\in S\setminus(I\pm J)}(\alpha-x([k]P))\in F_q$
7. return $h_K\cdot R/\triangle_{I,J}$

4.3. Isogeny 기반 암호의 안전성 분석

고전 컴퓨터에서의 안전성만 고려하면 되는 기존 공개키 암호와는 달리, PQC 암호는 고전 컴퓨터 뿐만 아니라 양자 컴퓨팅 환경에서의 안전성도 고려해야하는 특징을 가진다. 특히, PQC 암호에 관한 양자 안전성 분석이 본격적으로 수행된 지는 얼마 안 되었기 때문에, 면밀한 안전성 분석을 통해 해당 알고리즘이 안전한지 확인하고, 보안강도에 맞는 최적의 파라미터를 선택하는 것은 중요하다. 본 장에서는 최근 isogeny 기반 암호에 대한 고전 및 양자 안전성 분석 결과를 제시한다.

4.3.1. SIDH 기반 암호의 안전성 분석

SIDH 기반 암호는 유한체 위에 정의된 두 타원곡선 사이의 isogeny를 찾는 어려움에 기반을 두고 있다. 현재 알려진 가장 효율적인 고전 공격 방법은 meet-in-the-middle 기반 공격으로 1999년에 Galbraith가 제안하는 방법을 이용하면, 유한체 소수 p에 대해 $O(p^{1/4})$의 공격 복잡도를 가진다 [3]. 한편, SIDH 기반

암호에 가장 효율적인 양자 공격 방법은 Tani's claw finding 알고리즘을 이용하는 방법으로, 유한체 소수 p에 대해 $O(p^{1/6})$의 공격 복잡도를 가진다. NIST Round 1에 제출된 SIKE의 경우 이 두 공격 방법을 이용해서 파라미터 설정이 이루어졌다.

SIDH에 대한 meet-in-the-middle 공격 방법은 $O(p^{1/4})$의 메모리가 필요한데, 2018년 Aji 등은 $O(p^{1/4})$의 메모리 복잡도는 현재 기술로는 불가능한 상황으로 meet-in-the-middle 보다 시간 복잡도가 높은 대신 적은 메모리를 사용하는 van Oorchot-Wiener (vOW)의 golden collision search 방법을 isogeny 기반 암호에 사용하는 것이 가장 효율적인 공격이라는 것을 제안하였다 [6]. Aji 등의 분석 결과, NIST Round 1에 제출된 SIKE 파라미터는 목표한 고전 보안강도보다 더 강력한 안전성을 제공해주는 것을 확인하였다.

한편, 2019년 Jaques와 Schanck는 SIKE에 대한 양자 공격을 분석한 결과, 가장 효율적인 양자 분석 방법으로는 $O(p^{1/4})$의 RAM 사용량이 필요하므로, 마찬가지로 NIST에 제안된 SIKE 파라미터는 목표한 보안강도보다 더 강력한 안전성을 제공해주는 것을 확인하였으며. 해당 분석 결과 SIDH에 대한 고전 공격과 양자 공격이 복잡도에서는 큰 차이를 보이지 않음을 알 수 있다 [12].

결론적으로 고전 컴퓨팅 환경에서의 분석보다 양자 컴퓨팅 환경에서 분석이 더 효율적인 다른 PQC 암호와 달리, SIDH 기반 암호의 경우 현재 기술에서는 양자 공격보다 고전 공격이 더 효율적이다. 다음 표는 NIST Round 3 파라미터에 대한 고전 및 양자 복잡도를 비교하였으며, 단위는 비트로 표현되었다 [13].

〔표 5〕 SIKE 파라미터에 대한 양자 공격 복잡도 〔13〕

	2^{96}	2^{64}	2^{40}
SIKEp434	124	147	178
SIKEp503	134	179	234
SIKEp610	181	189	307
SIKEp751	219	274	345

〔표 6〕 SIKE 파라미터에 대한 고전 공격 복잡도 〔13〕

	2^{96}	2^{64}	2^{40}
SIKEp434	117	133	135
SIKEp503	142	158	160
SIKEp610	183	199	201
SIKEp751	235	251	253

4.3.2. CSIDH 기반 암호의 안전성 분석

CSIDH 기반 암호는 SIDH와 다르게 endomorphism ring이 가환성을 가지므로 이를 이용한 양자 공격은 하지수시간의 복잡도를 가진다. CSIDH 에 대한 가장 효율적인 양자 공격은 Kuperberg가 제안한 abelian hidden-shift problem을 해결하는 알고리즘을 이용하는 것이다 [23]. 2003년에 Kuperberg와 Regev가 제안한 hidden-shift problem에 대한 하지수 시간 양자 알고리즘을 제안한 이후, 2011년 Kuperberg는 해당 알고리즘을 더 향상한 양자 알고리즘인 collimation sieve (c-sieve)를 제안하였다 [24]. Peikert는 2020년에 Kuperberg의 c-sieve를 임의의 유한 순환군에 대해 적용할 수 있도록 확장시키고, CSIDH-512의 파라미터에 분석이 가능한 classical simulator를 제공하여 CSIDH에 대한 c-sieve 공격 복잡도를 계산하였다 [25]. 2020년 Chavez-Saab 등은 [22]에서 CSIDH에 대한 양자 공격 복잡도를 조금 더 세밀하게 분석하고, 이에 대응하여 보안 강도를 맞출 수 있는 새로운 파라미터를 제시하였다. [22]에서 제시된 파라미터는 다음과 같다.

위의 표에서 Performance는 group action을 수행하는데 필요한 giga clock cycle을 나타낸다. [Table 7]에서 확인할 수 있듯이, 양자 컴퓨팅 환경에서 적절한 보안강도를 제공하기 위해서 CSIDH에 사용하는 유한체의 크기는 기존보다 커져야 하며, 현 상황에서는 실생활에 적용하기는 어려울 것으로 보인다.

〔표 7〕 양자 공격 복잡도를 고려한 CSIDH 파라미터

NIST level	Quantum security	Prime (bits)	Performance
1	124	4096	23.2
1	135	5120	42.2
2	148	6144	74.8
3	〉160	8192	199.1
3	〉171	9216	292.4

V. 결 론

2011년 SIDH의 제안으로 본격적으로 isogeny 기반 암호에 관한 연구가 활발히 진행되었고 그 결과 현재 isogeny 기반 암호는 많은 발전을 이뤄왔다. 구체적으로는 처음 제안보다 속도가 많이 향상되어으며, 효율적인 홀수 차수 isogeny 공식과 이를 연산하는 방법, SIDH 이외 새로운 isogeny 기반 암호의 개발이 이루어졌다. 또한 고전 및 양자 분석 관점에서도 활발히 연구가 진행되었으며 특히 CSIDH의 구체적인 양자 분석은 향후 PQC 암호들에 대한 더 정확한 양자 분석의 밑거름이 될 것으로 보인다.

ECC 가 처음 제안되었을 때 RSA보다 느린 속도로 주목을 받지 못했지만, 이후 거듭된 연구로 RSA보다 안전하면서 빠른 속도를 제공한 것처럼, 많은 isogeny 암호를 연구하는 학자들은 isogeny 기반 암호도 속도가 크게 향상될 수 있을 것이라 보고 있다.

마지막으로 [13]에서 언급된 것처럼, 암호가 제안된 지 10년 동안 안전성이 크게 떨어지지 않는 암호는 isogeny 기반 암호가 처음이라고 볼 수 있다. 이렇듯 isogeny 기반 암호의 안전성은 점점 보장되었다고 볼 수 있으며, 앞으로도 발전이 기대된다.

참 고 문 헌

[1] J. J. Chi-Domiguez et al. “On new Velu’s formulae and their applications to CSIDH and BSIDH constant-time implementations,” IACR Cryptology ePrint Archive, 2020:1109, 2020

[2] D. Bernstein et al. “Faster computation of isogenies of large prime degree,” IACR Cryptology ePrint Archive, 2020:341, 2020

[3] S. Galbraith, “ Constructing isogenies between elliptic curves over finite fields,” LMS Journal of Compuration and Mathematics, vol. 2, pp. 118-138, 1999

[4] W. Castryck and T. Decru “CSIDH on the surface,” PQCrypto, LNCS 12100, pp.111-129, April, 2020

[5] W. Castryck et al. “CSIDH: An efficient post-quantum commutaitve group action,” ASIACRYPT, LNCS 11274, pp.395-427, Dec. 2018

[6] G. Adji et al. “On the cost of computing isogenies between supersigular ellitpic curves,” SAC,2018 LNCS 11349, pp. 322-343, 2019

[7] A. Childs et al. “Constructing elliptic curve isogenies in quantum subexponential time,” Journal of Mathematical Cryptology, vol. 8, no. 1, pp. 1-29, 2014

[8] C. Costello, “B-SIDH supersingular isogeny Diffie-Hellman using twisted torsion,” ASIACRYPT, LNCS 12492, pp. 440-463, Dec. 2020

[9] C. Costello and H. Hisil, “A simple and compact algorithm for SIDH with arbitrary degree isogenies,” ASIACRYPT, LNCS 10625, pp. 303-329, Dec. 2017

[10] J.M. Couveignes, “Hard homogenous spaces,” IACR Cryptology ePrint Archive, 2006:291, 2006

[11] De Feo. et al. “Towards practical key exchange from ordinary isogeny graphs,” ASIACRYPT, LNCS 11274, pp. 365-394, Dec. 2018

[12] S. Jaques and J. M. Schanck, “Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE,” CRYPTO, LNCS 11692, pp. 32-61, 2019

[13] Craig Costello, “The Case for SIKE: A decade of the supersingular isogeny problem,” IACR Cryptology ePrint Archive, 2021:543, 2021

[14] A. Jalali, “Towards optimized and constant-time CSIDH on embedded devices,” International Workshop on Constructive Side-Channel Analysis and Secure Design, pp. 215-231, 2019

[15] D. Jao, L. De Feo “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” PQCrypto, LNCS 7071, pp. 19-34, Aug. 2011

[16] T. Kawashima, “An efficient authenticated key exchange from random self-reducibility on CSIDH,” IACR Cryptology ePrint Archive, 2020:1178, 2020

[17] S. Kim et al. “New hybrid method for iso-

geny-based cryptosystems using Edwards curves," IEEE transactions on Information Theory, vol. 66, no. 3, pp. 1934-1943, 2020

[18] M. Meyer and S. Reith "A faster way to the CSIDH," INDOCRYPT, LNCS 11356, pp. 137-152, 2018

[19] M. Meyer et al. "On hybrid SIDH schemes using Edwards and Montgomery curve arithmetic," IACR Cryptology ePrint Archive, 2017:1213, 2017

[20] D. Moody and D. Shumow, "Analogues of Velu's formula for isogenies on alternate models of elliptic curves," Mathematics of Computations, vol. 85, no. 300, pp. 1929-1951, 2016

[21] A. Stolbunov, "Constructing public-key cryptographic schemes based on class group action on a set of isogenous ellitpic curves," Advances in Mathematics of Communication, vol. 4, no. 2, pp. 215-235, 2010

[22] J.J. Chi-Domiguez et al, "The SQALE of CSIDH: Square-root Velu quantum-resistant isogeny action with low exponents", IACR Cryptology ePrint Archive, 2020:1520, 2020

[23] 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

[24] G. Kuperberg, "Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem," arXiv preprint, arXiv:1112.3333, 2011

[25] C. Peikert, "He gives C-sieves on the CSIDH," EUROCRYPT, LNCS 12106, pp. 463-492, 2020

〈저자소개〉

김 수 리 (Suhri Kim)

정회원

2014년 2월 : 고려대학교 수학과 이학사

2016년 8월 : 고려대학교 정보보호대학원 공학석사

2020년 2월 : 고려대학교 정보보호대학원 공학박사

2020년 3월~2021년 2월 : 고려대학교 정보보호대학원 박사후연구원

2020년 3월~2021년 2월 : KU Leuven ESAT/COSIC 박사후연구원

2021년 3월~현재 : 성신여자대학교 수리통계데이터사이언스학부 조교수

<관심분야> 공개키 암호시스템, 후양자암호