Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.73

초특이 아이소제니 Diffie-Hellman의 구현 및 모바일 보안 제품에서의 응용*

윤 기 순,[1†] 이 준 영,[1] 김 수 리,[2] 권 지 훈,[2] 박 영 호[3‡]
[1]NSHC, [2]고려대학교, [3]세종사이버대학교

An Implementation of Supersingular Isogeny Diffie-Hellman and Its Application to Mobile Security Product*

Kisoon Yoon,[1†] Jun Yeong Lee,[1] Suhri Kim,[2] Jihoon Kwon,[2] Young-Ho Park[3‡]
[1]NSHC, [2]Korea University, [3]Sejong Cyber University

요 약

미래의 양자 컴퓨팅 환경에 대응한 양자내성 암호 알고리즘의 연구 개발이 NIST를 비롯한 국내외 연구기관 및 기업들의 참여 하에 활발히 이루어지고 있다. 양자내성 암호 알고리즘으로는 다변수다항식-기반, 부호-기반, 격자-기반, 해시-기반, 그리고 아이소제니-기반 암호 알고리즘들이 연구되고 있다. 그 중에서 아이소제니-기반(isogeny-based) 암호 알고리즘은 가장 최근에 등장했으며 타원곡선 연산을 사용하고, 양자내성 암호 알고리즘들 중 가장 짧은 키 길이를 가지고 있어 주목받고 있다. 본 논문에서는 초특이 아이소제니 Diffie-Hellman (SIDH) 프로토콜을 저사양 모바일 환경에 적합하도록 파라미터를 선택하고 효율적으로 구현하였다. 파라미터로는 현재의 보안강도와 저사양 모바일 환경을 고려하여 523비트 소수 유한체 상에서 정의되는 초특이 타원곡선을 선택하였으며 그에 최적화된 아이소제니 계산 전략 트리를 생성하였다. 적용 SIDH 모듈은 32비트 환경에서 동작하도록 구현하였다.

ABSTRACT

There has been increasing interest from NIST and other companies in studying post-quantum cryptography in order to resist against quantum computers. Multivariate polynomial based, code based, lattice based, hash based digital signature, and isogeny based cryptosystems are one of the main categories in post quantum cryptography. Among these categories, isogeny based cryptosystem is known to have shortest key length. In this paper, we implemented Supersingular Isogeny Diffie-Hellman (SIDH) protocol efficiently on low-end mobile device. Considering the device's specification, we select supersingular curve on 523 bit prime field, and generate efficient isogeny computation tree. Our implementation of SIDH module is targeted for 32bit environment.

Keywords: supersingular isogeny Diffie-Hellman, isogeny-based cryptography, post-quantum cryptography

I. 서 론

현재 주로 사용되는 공개키 암호 알고리즘들은 큰 정수의 인수분해 문제나 유한체 또는 유한체 상에서 정의된 타원곡선에서의 이산로그 문제 등의 계산이 어려움에 기반하여 그 안전성이 보장되고 있다. 하지만

Received(11. 30. 2017), Modified(12. 26. 2017), Accepted(01. 05. 2018)
* "본 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임" (2017R1A2B4011599)
† 주저자, kisoon.yoon@gmail.com
‡ 교신저자, youngho@sjcu.ac.kr(Corresponding author)

양자 컴퓨터를 이용하면 Shor의 알고리즘에 의해 그러한 문제들이 다항식시간 안에 해결된다는 사실이 알려져 있으며 30년 이내에 양자 컴퓨터의 구현 가능성이 논의되고 있는 현 시점에 그 위협에 대비해야 할 필요성이 제기되고 있다 [15].

양자 컴퓨터로도 풀기 어려운 계산 문제에 기반하여 안전성을 보장하는 암호 알고리즘을 양자내성 암호 알고리즘이라 부르는데 잘 알려진 것으로 다변수 다항식-기반(multivariate polynomial-based), 부호-기반(code-based), 격자-기반(lattice-based), 해시-기반(hash-based), 그리고 아이소제니-기반(isogeny-based) 암호 알고리즘들이 있다. 그 중에서 아이소제니-기반 암호 알고리즘은 가장 최근에 등장했으며 저변이 넓은 타원곡선 연산을 사용하고 양자내성 후보 알고리즘들 중 가장 짧은 키 길이를 가지고 있어 주목받고 있다.

아이소제니-기반 암호 알고리즘은 임의의 두 타원곡선 E_1과 E_2가 주어졌을 때 둘 사이의 임의의 아이소제니 $\varphi : E_1 \to E_2$를 찾아내는 문제의 어려움을 이용하고 있는데, 이 문제를 타원곡선 아이소제니 문제라고 부른다.

타원곡선 아이소제니를 사용하는 암호 알고리즘은 A. Stolbulnov [16]에 의해 처음으로 제안되었지만 당시 제안된 일반 타원곡선 아이소제니를 사용하는 방법이 비효율적이었고 양자 알고리즘으로 하지수 시간에 해결되는 단점이 있어 실용화되지 못했다 [4].

그러나 2014년에 De Feo, Jao와 Plût에 의해 제안된 초특이 타원곡선 아이소제니 문제에 기반하는 새로운 키 교환 프로토콜인 초특이 아이소제니 Diffie-Hellman (SIDH : Supersingular Isogeny Diffie-Hellman) 은 효율적인 연산이 가능하고 안전성도 높아 주목을 받았다 [7]. 2016년에 Costello와 Reza 등에 의해 효율적 구현 방법들이 제안되면서 SIDH에 대한 관심은 더욱 증대되었고 그 후속 결과들도 많이 제시되었다 [1,5,6].

II. 타원곡선 상의 아이소제니

본 논문에서는 표수가 3보다 큰 유한체 $\mathbb{F}_q$상에서 정의되는 타원곡선을 다룰 것이며 이 경우 타원곡선은 다음과 같은 Weierstrass 방정식으로 정의되는 매끈한 (smooth) 평면곡선이다.

$$E/\mathbb{F}_q : y^2 = x^3 + Ax + B,$$
$$4A^3 + 27B^2 \neq 0,\ A, B \in \mathbb{F}_q$$

위와 같은 타원곡선 E의 j-불변량 (j-invariant)은 $j(E) = 1728\dfrac{4a^3}{4a^3+27b^2} \in \mathbb{F}_q$와 같이 정의되며 두 타원곡선 E와 E'이 동형일 때 $j(E) = j(E')$가 성립한다. 즉, 동형인 타원곡선들의 클래스는 하나의 j-불변량으로 표현될 수 있다. 또한 주어진 j-불변량을 가지는 타원곡선을 다음과 같이 구할 수 있다.

$$y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}, \quad j \neq 0, 1728 \text{ 이면}$$
$$j = 0 \text{ 이면 } y^2 = x^3 + B,$$
$$j = 1728 \text{이면 } y^2 = x^3 + Ax$$

타원곡선 상의 점들은 점의 덧셈 (point addition) 연산에 대해 군을 이루며 무한원점 (point at infinity) O를 항등원으로 한다. 두 타원곡선 E와 E' 사이의 유한체 $\mathbb{F}_q$ 상에서 정의되는 아이소제니 $\phi : E \to E'$는 $\phi(O) = O'$을 만족하는 자명하지 않은 정칙함수 (regular function)이다. 그러면 ϕ는 전사 준동형 사상 (surjective homomorphism)이 된다. 또한 ϕ가 체 $\mathbb{F}_q$ 상에서 정의되는 아이소제니라 하면 다음과 같이 표준형으로 표현된다.

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, \left(\frac{u(x)}{v(x)} \right)' y \right), u(x), v(x) \in \mathbb{F}_q[x]$$

이 때 ϕ에 대응하는 당김사상 (pullback) $\phi^* : k(E') \to k(E)$는 $\phi^* f = f \circ \phi$로 정의되며 ϕ^*가 단사이므로 함수체 확장 $\mathbb{F}_q(E)/\phi^*\mathbb{F}_q(E')$을 생각할 수 있다. 이 함수체 확장이 분리가능 (separable)이면 ϕ를 분리가능 아이소제니 (separable isogeny)라 부르며 그렇지 않은 경우 비분리적 아이소제니 (inseparable isogeny)라 부른다. 이 때 ϕ의 차수 (degree)를 $[\mathbb{F}_p(E) : \phi^*\mathbb{F}_p(E)]$로 정의하는데, 이 값은 $\max\{\deg(u), \deg(v)\}$와 일치한다. ϕ가 분리가능 아이소제니인 경우 ϕ의 차수는 $\#\ker(\phi)$와 정확히 일치한다.

타원곡선 E에서 정의되는 모든 아이소제니의 핵(kernel)은 E의 유한 부분군이며 역으로 E의 유한 부분군 G가 주어지면 다음과 같이 Vélu의 공식에 의해 G를 핵으로 가지는 아이소제니를 계산할 수 있다 [17].

$$\phi(x,y)=(x+\sum_{Q\in G\setminus\{O\}}\left(\frac{3x_Q+A}{x-x_Q}+\frac{2y_Q^2}{(x-x_Q)^2}\right)$$

$$y-\sum_{Q\in G\setminus\{O\}}\left(\frac{3x_Q+A}{(x-x_Q)^2}+\frac{2y_Q^2}{(x-x_Q)^3}\right))$$

$$A'=A-5\sum_{Q\in G\setminus\{O\}}(3x_Q^2+A),$$

$$B'=B-7\sum_{Q\in G\setminus\{O\}}(5x_Q^2+3Ax_Q+2B).$$

여기서 A,B는 위에서 정의된 타원곡선의 계수들이며 A',B'은 ϕ의 상 (image)이 되는 곡선 $E'/\mathbb{F}_q: y^2=x^3+A'x+B'$의 계수이다.

특히 n배 사상 $[n]: E\to E,\ P\to P+\cdots+P$ (n-times)은 자기준동형사상이며 그 커널은 $E[n]$로 표기하고 E의 n-torsion 부분군이라 부른다.

타원곡선 E의 자기준동형사상환 (endomorphism ring)은 $End(E)$로 표기하며 그 자기준동형사상 대수 (endomorphism algebra)는 $End^0(E)=\mathbb{Q}\otimes_{\mathbb{Z}}End(E)$로 정의된다. $End^0(E)$는 유리수체, 복소 이차체 (imaginary quadratic field), 또는 사원수 대수 (quaternion algebra) 중 하나가 된다. $End(E)\neq\mathbb{Z}$이면 E는 복소 곱셈 (complex multiplication)을 가진다고 한다.

분리가능 아이소제니 $\phi: E\to E'$의 차수가 ℓ이라 하면 항상 그에 대응하는 아이소제니 $\hat{\phi}: E'\to E$가 존재하여 $\hat{\phi}\circ\phi=[\ell]_E$을 만족시키는데 이 때 $\hat{\phi}$을 ϕ의 쌍대 아이소제니 (dual isogeny)라 한다.

표수가 p인 체 상에서 정의되는 타원곡선 E에 대해 다음의 조건들은 동치이다.

(i) $E[p]\cong\{O\}$.
(ii) 프로베니우스 대각합수 (trace of Frobenius)이 p의 배수이다.
(iii) $End^0(E)$가 사원수 대수이다.

위 조건을 만족시키는 타원곡선을 초특이 타원곡선 (supersingular eliptic curve)라고 하며 그렇지 않은 타원곡선을 일반 타원곡선 (ordinary elliptic curve)이라고 한다.

유한체 $\mathbb{F}_q$에서 정의되는 타원곡선 E에 대해 $End(E)$는 프로베니우스 자기준동형사상 $\pi_q: E\to E,\ (x,y)\mapsto(x^q,y^q)$을 포함하며 π_q는 이차 특성방정식 $\pi_q^2+t_q\pi_q+[q]=O$를 만족하는데, 이 때, 정수 t_q를 프로베니우스 대각합 (trace of Frobenius)이라 한다. Hasse의 정리에 의해 $t_q\le 2\sqrt{q}$이므로 π_q는 정수배 사상이 아니다. 따라서 유한체에서 정의되는 일반 타원곡선은 항상 복소곱셈을 가진다.

표수가 p인 체에서 정의되는 모든 초특이 타원곡선은 $\mathbb{F}_{p^2}$상에서 정의되는 초특이 타원곡선과 동형이며 그 동형류 (isomorphic class)의 개수는 (i) $p=2,\ 3$일 때 1 개, (ii) $p=1,5,7,11 \bmod 12$ 일 때 각 경우에 대해여 $\left\lfloor\frac{p}{12}\right\rfloor$, $\left\lfloor\frac{p}{12}\right\rfloor+1$, $\left\lfloor\frac{p}{12}\right\rfloor+1$, $\left\lfloor\frac{p}{12}\right\rfloor+2$ 개이다. 이 사실로부터 아이소제니 그래프는 $p>3$가 큰 경우 충분히 많은 꼭짓점을 가진다는 것을 알 수 있다.

Deuring의 올림정리 (lifting theorem)에 의해 유한체 $\mathbb{F}_q$에서 정의되는 모든 타원곡선 E는 어떤 수체 (number field) K에서 정의되는 타원곡선을 그 수체의 어떤 소아이디얼 (prime ideal)을 법으로 축소시켜 (modular reduction) 얻을 수 있다. 이 때 그 소아이디얼 아래 놓여있는 소수가 K에서 분할(splitting)되지 않는다는 것과 E가 초특이 타원곡선이라는 것은 동치이다. 주어진 위수를 가지는 유한체 상의 타원곡선을 찾기 위해 Deuring의 정리에 기초한 CM-방법 (complex multiplication method)이 널리 사용되고 있다. 특히 Bröker의 논문 [2]에 의하면 초특이 타원곡선의 경우 CM-방법의 계산복잡도가 다항식 시간인 $O(\log q^3)$로서 계산복잡도가 지수시간인 일반 타원곡선에 비해 더 효율적임을 알 수 있다.

III. 아이소제니 문제

초특이 타원곡선 (resp. 일반 타원곡선) 아이소제니를 짧게 초특이 (resp. 일반) 아이소제니라 부르기

로 하자.

Galbraith는 유한체 $\mathbb{F}_q$ 상에서 정의되는 일반 타원곡선 아이소제니 그래프 상에서 주어진 임의의 두 타원곡선 사이의 아이소제니를 찾는 문제를 복잡도 $\widetilde{O}(q^{1/4})$안에 해결하는 알고리즘을 제안하였다 [9]. Galbraith는 일반 타원곡선 그래프가 가지는 화산(volcano)형 구조를 이용하여 충돌 알고리즘을 가속화 했다. $\mathbb{F}_{q^2}$ (또는 $\overline{\mathbb{F}_q}$) 상에서 정의되는 초특이 타원곡선 아이소제니 그래프에서 같은 문제를 풀려면 복잡도 $\widetilde{O}(q^{1/2})$가 필요한데 이것은 일반적인 충돌 알고리즘의 복잡도와 같은 것이다. $\mathbb{F}_{q^2}$ 상의 초특이 타원곡선의 경우와 $\mathbb{F}_q$ 상의 일반 타원곡선의 경우 모두 아이소제니 그래프의 꼭짓점의 개수는 $O(q)$를 따른다는 것을 고려하면 일반 타원곡선의 경우 복잡도가 더 낮음을 알 수 있다. 하지만 Delfs와 Galbraith는 $\mathbb{F}_q$상에서 정의되는 초특이 타원곡선 아이소제니 그래프는 일반 타원곡선의 경우와 같은 방법으로 복잡도 $\widetilde{O}(q^{1/4})$인 알고리즘을 적용할 수 있다는 것을 보였다 [8]. 결론적으로 비양자 알고리즘을 이용하는 경우 아이소제니 문제를 푸는 알려진 알고리즘은 모두 지수 복잡도를 가진다.

Childs, Jao와 Soukharev의 양자 탐색알고리즘을 적용하면 $\mathbb{F}_q$에서 정의되는 일반 아이소제니 문제를 하지수시간인 $L_q(1/2, \sqrt{3}/2)$에 해결 가능하다 [4]. 또한 초특이 아이소제니 문제의 경우 Biasse, Jao와 Sankar의 알고리즘을 이용하면 복잡도 $\widetilde{O}(q^{1/6})$안에 해결 가능하다 [2]. 따라서 초특이 아이소제니 문제의 경우 아이소제니 문제를 푸는 알려진 알고리즘은 모두 지수 복잡도를 가진다.

IV. SIDH

이 절에서는 초특이 아이소제니 문제를 이용한 키 교환 프로토콜인 SIDH에 대해 소개한다. 프로토콜에 참여하는 두 개체를 Alice와 Bob으로 칭하자. 프로토콜의 목적은 Alice와 Bob이 안전하지 않은 채널을 통하여 비밀키를 공유하는 것이다.

4.1 도메인 파라미터 생성

다음과 같은 파라미터들을 생성하여 모든 사용자들이 사용할 수 있도록 게시한다.

- ℓ_A, ℓ_B는 작은 소수로서 차수 ℓ_A, ℓ_B를 가지는 아이소제니가 효율적으로 계산될 수 있도록 선택된다. 자연수 e_A, e_B, f는 $p = \ell_A^{e_A}\ell_B^{e_B}f \pm 1$가 소수가 되도록 선택한다. 이 때 $\ell_A^{e_A}$, $\ell_B^{e_A}$는 비슷한 크기를 가지도록 선택되는데 그 크기가 개인키의 길이가 된다.
- 초기 타원곡선 E는 $\mathbb{F}_{p^2}$상에서 정의되는 위수가 $\#E(K) = (\ell_A^{e_A}\ell_B^{e_B}f)^2$인 초특이 타원곡선이다. 그러면 $E[\ell_A^{e_A}]$, $E[\ell_B^{e_B}] \subset E(\mathbb{F}_{p^2})$가 되어 $E(\mathbb{F}_{p^2})$에서 비퇴화 페어링 (non-degenerate pairing)을 사용할 수 있다.
- $< P_A, Q_A > \geqq E[\ell_A^{e_A}]$ 와 $< P_B, Q_B > \geqq E[\ell_B^{e_B}]$를 만족하는 생성점 P_A와 Q_A, P_B와 Q_B를 뽑는다.

4.2 키쌍 생성

- Alice는 임의의 난수 $0 \leq m_A,\ n_A < \ell_A^{e_A}$를 선택하고, 순환군 $< m_A P_A + n_A Q_A >$를 핵으로 하는 아이소제니 ϕ_A를 이용하여 $E_A = \phi_A(E) \cong E/ < m_A P_A + n_A Q_A >$, $\phi_A(P_B)$, $\phi_A(Q_B)$를 계산한다.
- Bob은 임의의 난수 $0 \leq m_B,\ n_B < \ell_B^{e_B}$를 선택하고, 순환군 $< m_B P_B + n_B Q_B >$를 핵으로 하는 아이소제니 ϕ_B를 이용하여 $E_B = \phi_B(E) \cong E/ < m_B P_B + n_B Q_B >$, $\phi_B(P_A)$, $\phi_B(Q_A)$를 계산한다.

4.3 키 교환

Alice는 E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$를 Bob에게 보내고 E_B, $\phi_B(P_A)$, $\phi_B(Q_A)$를 Bob으로부터 받는다. Alice는 개인키 (m_A, n_A)를 이용하여 $E_{BA} = \phi_A(E_B) = E_B/ < m_A\phi_{B(}P_A) + n_A\phi_{B(}Q_A) >$를 계산하고 j-불변량 $j(E_{BA})$로부터 비밀 공유키를 계산한다.

- Bob은 E_B, $\phi_B(P_A)$, $\phi_B(Q_A)$를 Alice에게 보내고 E_A, $\phi_A(P_B)$, $\phi_A(Q_B)$를 Alice으로부터 받는다. Bob은 개인키 (m_B, n_B)를 이용하여 $E_{AB} = \phi_B(E_A) = E_A/ < m_B\phi_{A(}P_B) + n_B\phi_{A(}Q_B) >$

를 계산하고 j-불변량 $j(E_{AB})$로부터 비밀 공유 키를 계산한다.

V. SIDH 구현 기법

Costello 등은 2016년 SIDH 모듈을 효율적으로 구현하는 다양한 알고리즘을 소개하였다 [6]. 본 논문에서 적용하는 SIDH 모듈은 Costello의 기법들에 따라 구현 되므로 이 절에서 그 아이디어들에 대해 간략히 언급한다.

5.1 몽고메리 곡선 (Montgomery curve) 채택

몽고메리 곡선 (Montgomery curve)의 채택으로 점의 상수배 연산 시에 x좌표만을 이용한 몽고메리 사다리 (Montgomery ladder)를 이용하여 효율적 구현이 가능하게 했다. 유한체 $\mathbb{F}_{p^2}$ 상에서 정의되는 몽고메리 곡선은 방정식 $E_{(a,b)}: by^2 = x^3 + ax^2 + x$, $a,b \in \mathbb{F}_{p^2}$ 으로 주어지며 그 j-불변량은 $j(E_{(a,b)}) = \frac{256(a^2-3)^3}{a^2-4} \in \mathbb{F}_{p^2}$와 같이 계산된다. 계수 a가 같은 두 몽고메리 곡선은 서로 뒤틀린 곡선 (twisted curve)이므로 $j(E_{(a,b)})$이 계수 b에 의존하지 않는다는 것을 확인할 수 있다. 또한 몽고메리 사다리가 쿠머 다양체 (Kummer variety) $E_{(a,b)}/\langle \pm 1 \rangle \cong \mathbb{P}^1$ 상의 연산이므로 상수배 공식 또한 b에 의존하지 않음을 알 수 있다. 따라서 아이소제니 계산은 b로부터 독립적이며 이것은 효율성 향상을 가져온다.

5.2 파라미터 선택, 유한체 연산

SIDH 파라미터 선택에 있어 정수들 ℓ_A, e_A, ℓ_B, e_B, f을 잘 선택하는 것은 구현의 효율성과 안전성에 중요한 영향을 미친다. 즉, ℓ_A와 ℓ_B의 크기는 되도록 작게 잡아 아이소제니 계산을 용이하게 하고 e_A와 e_B를 충분히 크게 잡아 Vélu의 공식을 여러 번 적용함으로써 높은 안전성을 가지는 큰 차수의 아이소제니를 계산한다. 또한 $\ell_A = 2$, $\ell_B = 3$으로 선택하면 p가 $2^{e_A} \cdot 3^{e_B} \cdot f \pm 1$ 꼴인 점을 이용하여 효율적인 몽고메리 감산 (Montgomery reduction)을 구현할 수 있다. $R = 2^{768}, p' = -p^{-1} \bmod p$ 라 할 때, 입력 $a < pR$에 대하여 몽고메리 잉여계 (Montgomery residue) $c = aR^{-1} \bmod p$ 는 $c = (a + (ap' \bmod 2^{768}) \cdot p)/2^{768}$ 와 같이 나타낼 수 있다. 소수 $p = 2^{e_A} \cdot 3^{e_B} \cdot f \pm 1$임을 이용하면 $c = (a + (ap' \bmod 2^{768}) \cdot 2^{372} \cdot 3^{239} - (ap' \bmod 2^{768}))/2^{768}$ $= (a + (ap' \bmod 2^{768}) \cdot 2^{372} \cdot 3^{239}$ 와 같이 계산할 수 있다. 또한 $p' - 1$을 32비트 워드로 나타낼 경우 하위 11워드, 64비트 워드로 나타낼 경우 하위 5워드가 0임을 이용하면 효율적으로 연산할 수 있다.

아이소제니 계산의 중간 단계들에서 타원곡선이 연속적으로 불규칙하게 변화하므로 효율적인 연산이 가능한 타원곡선을 인위적으로 선택할 수는 없다.

초기 타원곡선은 도메인 파라미터의 크기를 최소화할 목적으로 부분체상의 곡선인 $E_{(1,0)}: y^2 = x^3 + x$로 선택하였다. 생성점들 역시 $P_A = (z, \sqrt{z^3 + z})$, $P_B = (w, \sqrt{w^3 + w})$ 이 $\mathbb{F}_p$-유리점들이 되도록 하고 Q_A와 Q_B는 뒤틀림 사상 (distortion map) $\tau(x,y) = (-x, iy)$을 이용하여 $Q_A = \tau(P_A)$, $Q_B = \tau(P_B)$와 같이 계산할 때마다 복원하여 쓸 수 있도록 하여 그 크기를 최소화 했다.

5.3 사영좌표계 (Projective coordinate) 채택

사영좌표계를 이용하는 경우 곡선의 방정식은 $E_{(A:B:C)}: BYZ^2 = CX^3 + AX^2Z + CXZ^2$ 와 같이 쓸 수 있고, 이 때 j-불변량은 $j(E_{(a,b)}) = \frac{256(A^2-3C^2)^3}{C^4(A^2-4C^2)}$와 같이 계산된다. 사영좌표를 이용하며 몽고메리 사다리 연산 및 아이소제니 계산에 있어 비용이 큰 역원 계산의 사용을 최소화할 수 있다.

아이소제니 계산은 곡선의 상 $E'_{(A',B')}: B'Y^2Z = C'X^3 + A'X^2Z + C'XZ^2$와 점의 상 $x(\phi(Q))$의 계산으로 이루어진다.

3^e-아이소제니는 연속되는 3-아이소제니를 이용하여 계산한다. 3-아이소제니에 의한 곡선의 상은 $(A' : C') = (Z_3^4 + 18X_3^2Z_3^2 - 27X_3^4 : 4X_3Z_3^3)$와 같이 계산할 수 있고 그 계산량은 $6M + 2S + 5a$이다. 또 점의 상은 $(X' : Z') = (X(X_3X - Z_3Z)^2 : Z(Z_3X - X_3Z)^2)$와 같이 계산할 수 있고 그 계산량은

$6M+2S+2a$이다. 여기에서 M, S, a는 각각 유한체 곱셈, 제곱, 덧셈 연산을 횟수를 나타낸다.

2^e-아이소제니는 연속되는 4-아이소제니를 이용하여 계산한다. 4-아이소제니 공식의 적용은 좀 더 복잡한데 그 이유는 아이소제니 적용 후 몽고메리 형식이 유지되지 않기 때문이다. 이것은 [7]에서 제안되는 동형사상 공식을 이용하여 해결할 수 있다. 초기 타원곡선은 부분체에 속하는 도메인 파라미터로 구성되어 있으므로 첫 단계의 4-아이소제니는 다음 공식들을 이용하여 계산한다.

$(A':C')=(2(a+6):a-2)$, 이 때 $A=a, C=1$로 정규화 되었음;

$(X':Z')=$

$=((X+Z)^2(aXZ+X^2+Z^2):(2-a)XZ(X-Z)^2)$

이 때 $(X':Y')$을 계산하는데 필요한 연산량은 각각 $4M+2S+9a$이다.

다른 단계들에서는 다음과 같이 일반적인 공식을 사용하여 4-아이소제니를 계산한다.

$(A':C')=(2(2X_4^4-Z_4^4):Z_4^4)$;

$(X':Z')=$

$=(X(2X_4Z_4Z-X(X_4^2+Z_4^2))(X_4X-Z_4Z)^2:$

$:Z(2X_4Z_4X-Z(X_4^2+Z_4^2))(Z_4X-X_4Z)^2)$

이 때 .$(A':C')$와 $(X':Y')$을 계산하는 데 필요한 연산량은 각각 $5S+7a$와 $9M+1S+6a$이다.

5.4 아이소제니 계산 전략

초특이 타원곡선 E 상의 차수 ℓ^e인 아이소제니 ϕ는 비밀 생성점 $R=mP+nQ$과 점 $Q\in E$에 대하여 기본적으로 다음과 같이 계산될 수 있다. $R_0:=R$, $Q_0:=Q$, $E_0:=E$로 놓고 순환군 $<[\ell^{e-1}]R_0>$을 핵으로 가지는 차수 ℓ인 아이소제니 ϕ_1을 계산하여 $E_1:=\phi_1 E$, $R_1:=\phi_1(R_0)$, $Q_1:=\phi_1(Q_0)\in E_1$을 구한다. 그 다음부터 $i=1,2,\cdots,e$에 대하여 차례로 E_i 상에서 순환군 $<[\ell^{e-i}]R_{i-1}>$을 핵으로 가지는 차수 ℓ인 아이소제니 ϕ_i를 계산하여 $E_i:=\phi_i E_{i-1}$, $R_i:=\phi_i(R_{i-1})$, $Q_i:=\phi_i(Q_{i-1})\in E_i$을 구해 나가서 최종적으로 $\phi(E)$와 $\phi(Q)$를 얻는다. 이렇게 거듭되는 상수배와 아이소제니 계산 과정을 e개의 계층으로 된 트리로 표현할 수 있다 [7]. 일반적으로 위에서 언급한 기본적인 방법은 가장 효율적인 방법이 아니며 상수배 계산비용과 아이소제니 계산 비용의 비율을 고려하여 계산 트리를 최적화 할 수 있다. 이것을 최적전략 (optimal strategy)이라 부른다. 최적전략은 도메인 파라미터와 같이 사전에 계산되는 것이며 모든 가능한 경우를 전수조사 하여 찾아낸다. 이것은 하나의 수열로서 표현될 수 있는데 자세한 사항은 [15]에 나타나 있다.

VI. 모바일 보안제품에 적용 사례

본 절에서는 5절에서 논한 기법들에 의해 최적화 구현된 SIDH 모듈을 국내 모바일 암호화 보안 제품에 탑재한 결과를 기술한다. 적용 대상 제품은 N사의 모바일 금융 보안 프로그램 엔필터 (nFilter)이다. 엔필터는 키 입력보안을 위한 가상 키패드 기능과 암호화 통신 기능을 가지고 있는데 타원곡선 Diffie-Hellman (ECDH) 키 교환 프로토콜을 사용하고 있어 구조가 유사한 SIDH로의 교체가 용이하다. 원래의 엔필터는 ECDH 키 교환 프로토콜과 국산 대칭키 암호 알고리즘인 SEED를 하이브리드 방식으로 사용하고 있다. 엔필터에 사용되는 타원곡선 파라미터는 NIST FIPS PUB 186-2 권장 B-233/K-233를 사용하고 있다. 다음 그림은 엔필터의 작동 및 암호화 통신 방식을 나타내고 있다.

엔필터의 암호화 통신 세션은 다음과 같다.

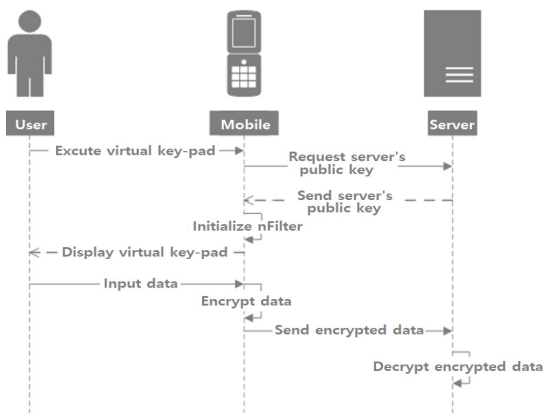


Fig. 1. cryptographic communication session of nFilter

(1) 클라이언트: 가상키패드 실행;
개인키/공개키쌍 생성;
생성된 공개키를 서버에게 전송;

(2) 서버: 개인키/공개키쌍 생성;
서버 개인키와 클라이언트
공개키로부터 비밀키 유도;
생성된 공개키를 클라이언트에게 전송;
(3) 클라이언트: 클라이언트 개인키와 서버 공개
키로부터 비밀키 유도;
가상키패드로부터 데이터 입력;
데이터를 비밀키로 암호화하여
서버에게 전송;
(4) 서버: 클라이언트로부터 수신한 암호문을
비밀키를 이용하여 복호화;

SIDH가 적용되는 구간은 (1)-(3) 구간이다. 엔필터에서는 공유된 비밀키 정보를 이용하여 가상키 위치 변환 및 암호화를 수행하므로 키 교환이 끝나고 사용자 인터페이스가 구동된다. 따라서 모바일 단말기에서의 키 교환 성능은 서비스 편의성에 적지 않은 영향을 미친다. 또한 엔필터 서버는 수많은 모바일 사용자와 키 교환을 수행해야 하므로 그 부하가 크기 때문에 서버측의 키 교환 성능이 매우 중요하다.

6.1 적용 파라미터

절에서 기술한 바와 같이 초특이 아이소제니 문제에 대한 알려진 양자 공격의 복잡도가 $\widetilde{O}(q^{1/6})$이므로 현재 권고되는 112비트 강도의 보안을 보장받으려면 소수 p를 672비트 이상이 되게 선택해야 할 것이다. 현행 보안강도를 따르기 위해서는 초특이 아이소제니 문제에 대한 비양자 공격의 복잡도가 $\widetilde{O}(q^{1/4})$임을 고려하면 소수 p가 448 비트 이상이 되게 하면 충분하다.

본 적용에서는 저사양 기기에 맞는 과도기적 적용을 목적으로 소수 p를 523비트 소수로 선택하였고 연산의 단위가 되는 워드 크기를 32비트로 제한하였다.

참고로 Costello 등의 배포 버전은 완전한 양자 컴퓨팅 환경에 대비하여 64비트 워드를 사용하고 있다.

소수 p는 다음과 같이 선택하였다.

$p = 2^{264} \cdot 3^{163} - 1 =$
17485714156904063104581295902099815603271551028000317175793233783028176625560480316047886054772352301117188983711286889932743750661121427224223633112702124031

초기 타원곡선은 다음과 같이 선택하였다.

$E: y^2 = x^3 + x;\ \#E(\mathbb{F}_{p^2}) = (2^{264} \cdot 3^{163})^2$

아이소제니를 계산하기 위한 최적의 전략은 다음과 같이 생성하였다.

Alice의 전략 : $L_A =$ 〔 0, 1, 1, 2, 2, 2, 3, 4, 4, 4, 4, 5, 5, 6, 7, 8, 8, 8, 8, 8, 9, 10, 9, 12, 11, 11, 12, 12, 13, 14, 15, 16, 16, 16, 16, 16, 17, 17, 17, 17, 17, 19, 19, 17, 18, 19, 20, 21, 22, 21, 23, 22, 24, 24, 25, 25, 27, 27, 27, 28, 30, 30, 31, 32, 32, 33, 33, 33, 33, 32, 33, 33, 33, 33, 33, 33, 33, 33, 36, 34, 35, 34, 35, 38, 37, 38, 38, 39, 38, 41, 39, 43, 38, 41, 42, 43, 43, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 48, 49, 53, 51, 51, 51, 53, 55, 56, 55, 56, 58, 58, 58, 59, 61, 61, 63, 63, 64, 64, 64, 65 〕

Bob의 전략 : $L_B =$ 〔 0, 1, 1, 2, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 7, 8, 8, 8, 8, 9, 9, 9, 9, 9, 12, 12, 12, 12, 12, 12, 12, 13, 14, 14, 15, 16, 16, 16, 16, 17, 16, 19, 17, 19, 19, 19, 20, 21, 22, 22, 22, 22, 22, 22, 22, 24, 22, 22, 24, 24, 26, 27, 27, 28, 28, 28, 30, 28, 28, 28, 28, 29, 28, 28, 28, 29, 29, 30, 33, 33, 33, 33, 34, 35, 37, 37, 37, 38, 38, 38, 37, 38, 38, 38, 38, 38, 39, 38, 44, 43, 44, 39, 40, 41, 43, 43, 43, 45, 46, 46, 46, 47, 48, 48, 49, 49, 50, 51, 51, 49, 49, 50, 51, 50, 51, 50, 50, 51, 50, 51, 51, 51, 53, 55, 55, 55, 56, 56, 56, 56, 56, 57, 58, 61, 61, 61, 63, 63, 63, 64, 65, 66, 65, 66, 66, 66, 65, 66, 66, 66, 66, 66, 68 〕

6.2 적용결과

적용 모바일 단말 환경은 다음과 같이 32비트 환경과 64비트 환경을 모두 사용하였다. 암호 모듈은

범용성을 위하여 32비트용으로 구현하였지만 참고로 64비트 환경에서의 적용 결과를 같이 실었다.

- 32비트 환경 : Galaxy note 2 / Android 4.4.2 Kitkat / 1.6GHz Exynos 4412 Quad Core / 2GB RAM.
- 64비트 환경 : Galaxy note 5 / Android 6.0.1 Marshmallow / 2.1GHz, 1.5GHz 64bit Exynos 7420 Octa Core / 4GB RAM.
- 적용 서버 : PC / Ubuntu 14.04.1 / 2.2Ghz AMD Turion(tm) II Neo N54L / 2GB RAM.

Table 1. Execution time of key generation and key exchange in mobile and server.

	Key Gen	Key Exchange
Mobile (32 bit)	2632 ms	1074 ms
Mobile (64 bit)	671 ms	276 ms
Server	800 ms	338 ms

다음은 모바일 단말기와 서버에서 프로그램 실행 결과 화면을 나타내고 있다.

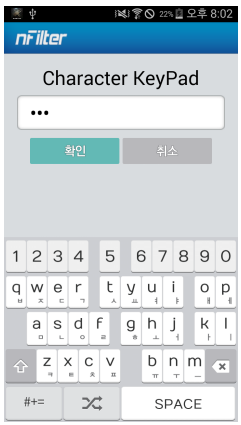


Fig. 2. Interface of mobile application

이번 적용에서 보안상 고려할 사항으로는 모바일 환경의 특성상 여러가지 형태의 해킹이 가능하다는 것이다. 개인키의 탈취와 같은 중대한 공격에 대해 시스템 레벨에서 방어하는 것 외에도 몇 가지 주의사항이 요구된다. SIDH 키가 static하게 사용되는 경우에 대한 공격 방법들 [10, 18]이 제안되었는데 해당 제품은 SIDH 키를 매번 교체하므로 여러 번에 걸쳐 공격해야 하는 [10]의 방법에는 안전하다. 하지만 [18]의 공격은 공개값인 생성점들 P_A, Q_A, P_B, Q_B의 상들 $\phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$를 연산하는 과정에서 단순히 메모리의 몇 비트를 손상시킬 수만 있으면 한번 전송되는 정보를 통해서도 개인키를 알아낼 수 있기 때문에 이에 대한 방어 설비가 고려되어야 한다. 이것은 생성점을 (x, y)와 같이 압축되지 않은 형태로 사용함으로써 해결할 수 있다.

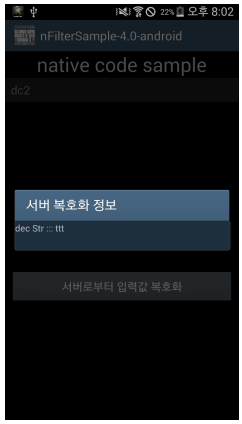


Fig. 3. Verification of the decrypted messege from server

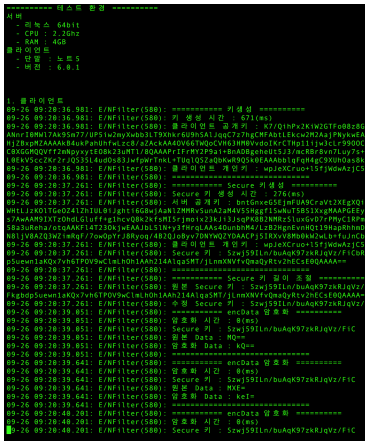


Fig. 4. Server Log

VII. 결 론

전 세계적으로 양자 컴퓨팅 환경에 대비한 양자내성 암호 알고리즘의 연구 개발이 활발히 이루어지고 있는 가운데 국외에서는 PQ Solutions Limited의 PQ-chat에 코드기반의 McEliece 암호 알고리즘, 구글사의 Canary에 격자기반 암호 알고리즘인 New Hope가 탑재되는 등 다양한 성과를 보이고 있다. 본 논문에서는 SIDH 모듈을 32비트 모바일 환경에 맞도록 구현하고 국내 최초로 상용 금융 보안 제품에 적용하여 그 활용성을 보였다. 파라미터로는 현재의 보안강도와 모바일 적용환경을 고려하여 523비트 소수 유한체 상에서 정의되는 초특이 타원곡선을 선택하였으며 그에 최적화된 아이소제니 계산 전략 트리를 생성하였다.

References

[1] R. Azarderakhsh, D. Jao, K. Kalach, and C. Leonardi, "Key compression for isogeny-based cryptosystems," Proceedings of the 3rd ACM International Workshop, pp.1-10, 2016

[2] J. Biasse, D. Jao, and A. Sankar, "A quantum algorithm for computing isogenies between supersingular elliptic curves," INDOCRYPT 2014, pp. 428-442, 2014

[3] R. Broker, "Constructing supersingular elliptic curves," J. Comb. Number Theory, pp. 269-273, 2009

[4] A. Childs, D. Jao, and V. Soukharev, "Constructing elliptic curves isogenies in quantum subexponential time," Journal of Mathematical Cryptology, vol. 8, no. 1, pp. 1-29, 2014

[5] C. Costello, D. Jao, P. Longa, M. Naehrig, J. Renes, and D. Urbanik, "Efficient compression of SIDH public keys," EUROCRYPT 2017, pp. 679-706, 2017

[6] C. Costello, P. Longa, and M. Naehrig, "Efficient algorithms for supersingular isogeny Diffie-Hellman," CRYPTO 2016, pp. 572-601, 2016

[7] L. De Feo, D. Jao, and J. Plut, "Towards quantum-resistant cryptosystems from supersingular elliptic curves isogenies," PQCrypto 2011, pp. 19-34, 2011

[8] C. Delfs and S. D. Galbraith, "Computing isogenies between supersingular elliptic curves over Fp," Des. Codes Cryptography, vol. 78, no.2, pp. 425-440, 2016

[9] S. Galbraith, "Constructing isogenies between elliptic curves over finite fields," LMS Journal of Computation and Mathematics, vol. 2, pp. 118-138, 1999

[10] S. D. Galbraith, C. Petit, and B. Shani, Y. Bo Ti, "On the security of supersingular isogeny cryptosystems," ASIACRYPT 2016, pp. 63-91, 2016

[11] S. Galbraith, C. Petit, and J. Silva, "Signature schemes based on supersingular isogeny problems," eprint, 2016

[12] A. Gelin, and B. Wesolowski, "Loop-abort faults on supersingular isogeny cryptosystems," PQCrypto 2017, pp. 93-106, 2017

[13] A. Stolbunov, "Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves," Adv. Math. Commun., vol. 4, no. 2, pp. 215 - 235, 2010

[14] T. Seiichiro, "Claw finding algorithms using quantum walk," Theoretical Computer Science, vol. 410, no. 50, pp. 5285-5297, 2009

[15] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484 - 1509, 1997

[16] A. Stolbunov, "Constructing public-key cryptographic schemes based on class

group action on a set of isogenous elliptic curves," Adv. in Math. of Comm, vol. 4, no. 2, pp. 251-235, 2010

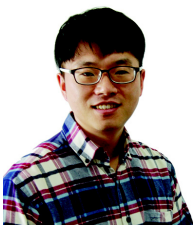
[17] J. Vélu, "Isogénies entre courbes elliptiques," C.R. Acad. Sc. Paris, Série A., vol. 273, pp. 238-241, 1971

[18] Yan Bo Ti, "Fault attack on supersingular isogeny cryptosystems," PQCrypto 2017, pp. 107-122, 2017

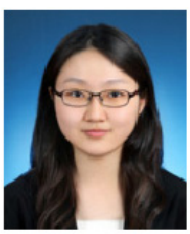
[19] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies," International Conference on Financial Cryptography and Data Security, pp. 163-181, 2017

〈저자소개〉

윤 기 순 (Kisoon Yoon) 정회원
1998년 8월: 경희대학교 수학과 이학사
2007년 8월: 고려대학교 정보보호학과 공학석사
2013년 11월: Université de Caen 수학과 이학박사
2013년 11월~현재: 엔에스에이치씨 암호기술팀 팀장
〈관심분야〉 정수론, 암호학, 정보보호



이 준 영 (Jun Yeong Lee) 정회원
2008년 2월: 명지대학교 컴퓨터소프트웨어학과 공학사
2017년 2월: 세종사이버대학교 정보보호학과 공학석사
2008년 3월~현재: 엔에스에이치씨 암호기술팀 책임연구원
〈관심분야〉 암호구현, 정보보호, 블록체인



김 수 리 (Suhri Kim) 학생회원
2014년 2월: 고려대학교 수학과 학사
2016년 2월: 고려대학교 정보보호대학원 석사
2016년 2월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 부채널 공격, 공개키 암호시스템

권 지 훈 (Jihoon Kwon) 학생회원
2010년 2월: 고려대학교 수학과 석사
2010년 3월~현재: 고려대학교 정보보호대학원 석박사 통합과정
〈관심분야〉 정보보호, 공개키 암호시스템

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 2월~현재: 세종사이버대학교 정보보호학과 교수
〈관심분야〉 공개키 암호, 암호 프로토콜, 부채널 공격, 암호안전성평가