03

Supersingular Isogeny Diffie-Hellman (SIDH)

목차

1

아이소제니 기반 암호

Introduction to Isogeny-based cryptography

History

- 아이소제니 기반 암호는 2006년 Couveignes, Rostovtsev, Stolbunov 에 의해 처음으로 제안 (CRS)
- Ordinary curve를 사용한 DH 기반 암호
- 하지만 ordinary curve의 endomorphism ring의 commutative 한 성질을 활용한 Childs 등에 공격으로 subexponential complexity를 가지게 됨
- 또한 매우 느린 속도로 효율성이 저하됨

Introduction to Isogeny-based cryptography

History

- 2011년 De Feo와 Jao의 supersingular를 사용한 DH 기반 키 교환 프로토콜로 다시 주목을 받음
  - Supersingular isogeny Diffie-Hellman (SIDH)
- Supersingular curve는 endomorphism ring이 noncommutative 하기 때문에 Childs 등의 공격에 안전

Introduction to Isogeny-based cryptography

History

ordinary curves
- subexponential,
- inefficient

2006
CRS Scheme

2011
SIDH
Jao, De Feo supersingular curves
- exponential

Costello et al. Practical implementation

2016
SIDH Library

2017
SIKE
NIST PQC Submission Round 3 alternative candidate

Castryck et al. CRS using supersingular curve

2018
CSIDH

Introduction to Isogeny-based cryptography

Security base

- Isogeny problem
  - Let E_1, E_2 be elliptic curves over $F_q, \#(E_1) = \#(E_2)$
  - Find an isogeny ϕ such that $\phi: E_1 \rightarrow E_2$

- Ramanujan Graph
  - Spectral gap 이 최대인 regular graph

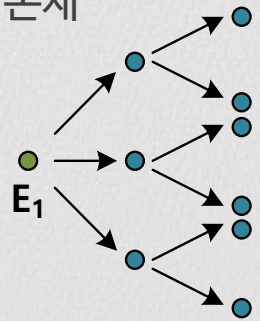
그래프의 모든 vertex가 동일한 degree

Introduction to Isogeny-based cryptography

Security base

- Isogeny problem
  - Let E_1, E_2 be elliptic curves over $F_q, \#(E_1) = \#(E_2)$
  - Find an isogeny ϕ such that $\phi: E_1 \rightarrow E_2$

- Ramanujan Graph
  - Isogeny graph는 Ramanujan graph의 한 종류 ➔ 가장 많이 퍼지는 그래프
  - 연속된 ℓ-isogeny ➔ $\ell + 1$ 가지 neighbor 존재
  - Example : 연속된 2-isogeny



Introduction to Isogeny-based cryptography

특징

- Velu formula : 타원곡선과 subgroup 이 주어지면 isogeny 연산 가능
  - 공개정보 : 두 타원곡선
  - 비밀정보 : Kernel (subgroup) (isogeny)
  - 비밀정보를 가진 사용자는 Velu의 공식으로 isogeny 연산 가능

Introduction to Isogeny-based cryptography

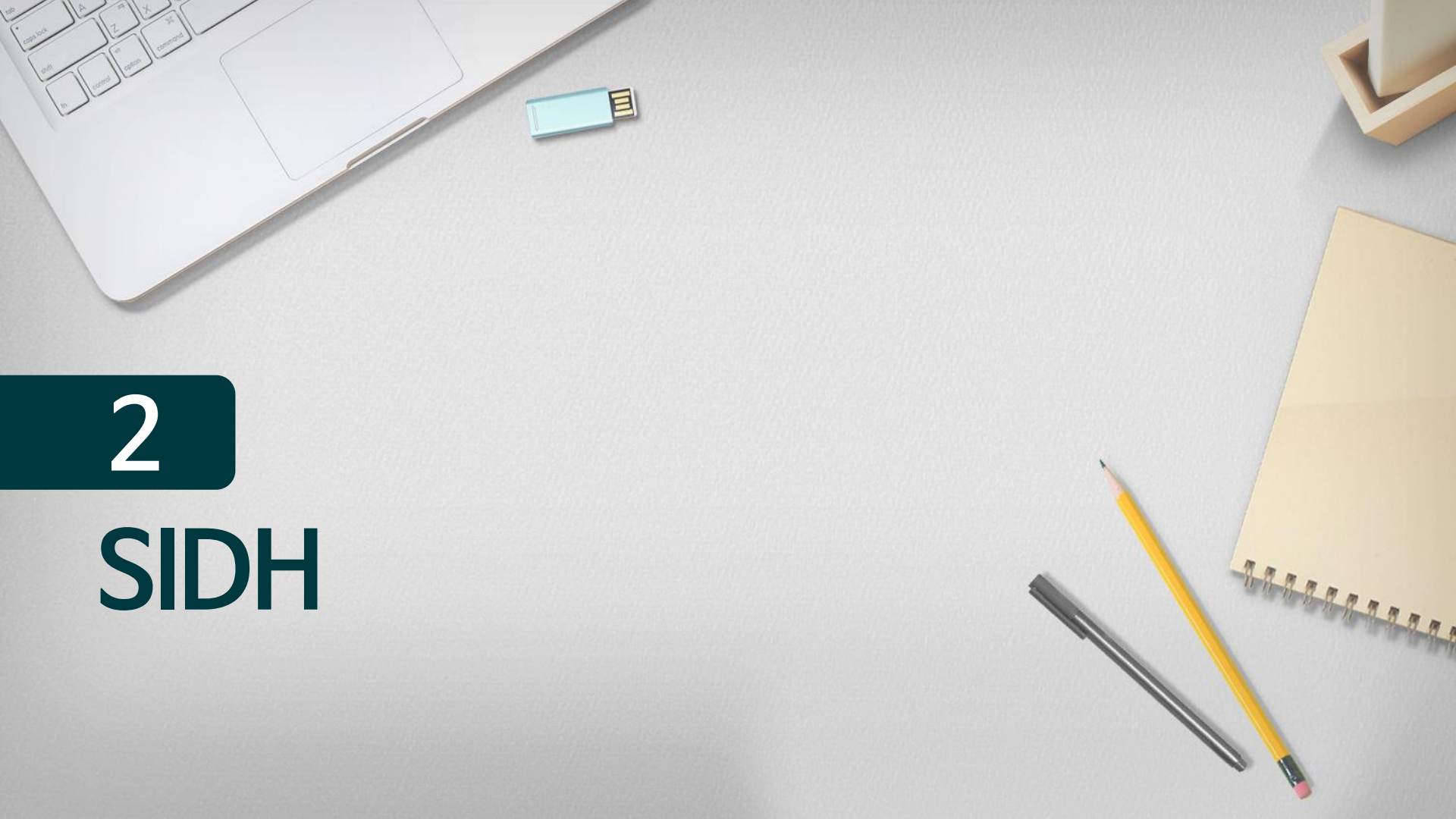
기존 ECC와 차이점

- Supersingular elliptic curves E over F_p
  - $E[p] \cong \{O\}$
  - Endomorphism ring ≅ Quaternion algebra
  - j-invariant 는 F_{p^2} $(or\ F_p)$ 에 존재

	SIDH	ECC
Prime	$p = 2^{e_A}3^{e_B} - 1$	$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} + 1$
Field	F_{p^2}	F_p
Curve	Supersingular elliptic curve	Ordinary curve
Order of a curve	$(2^{e_A}3^{e_B})^2$	Near prime
Security	Hardness of finding isogeny between given two elliptic curve	Hardness of solving ECDLP
Private key	Isogeny (kernel)	d

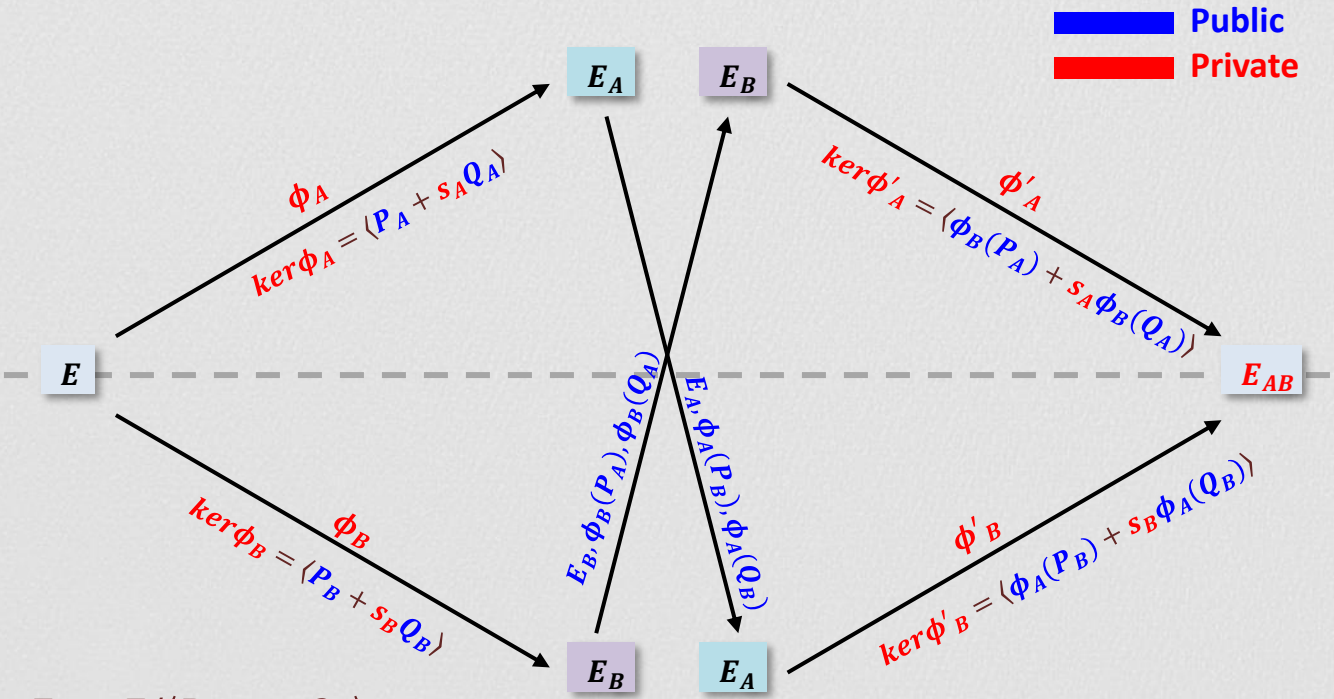
2

SIDH



SIDH

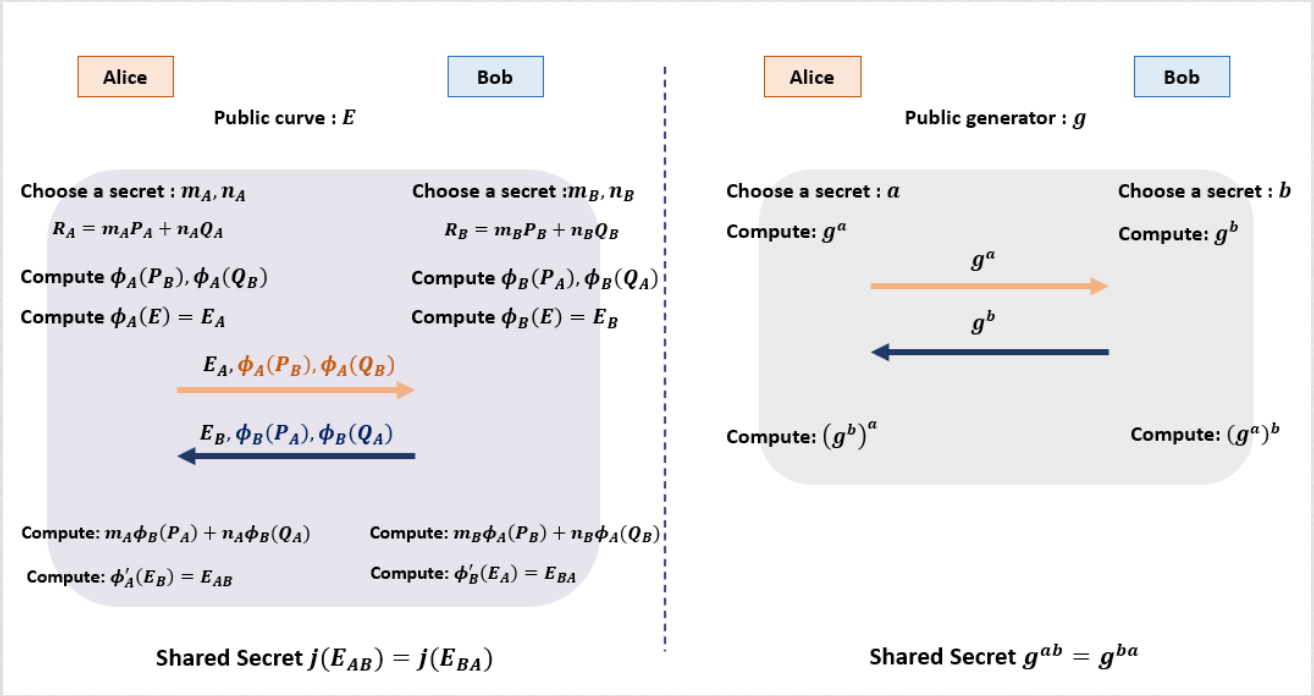
Protocol Outline



$$E_A = E/\langle P_A + s_A Q_A \rangle$$
$$E_B = E/\langle P_B + s_B Q_B \rangle$$

SIDH

Diffie-Hellman 과의 비교



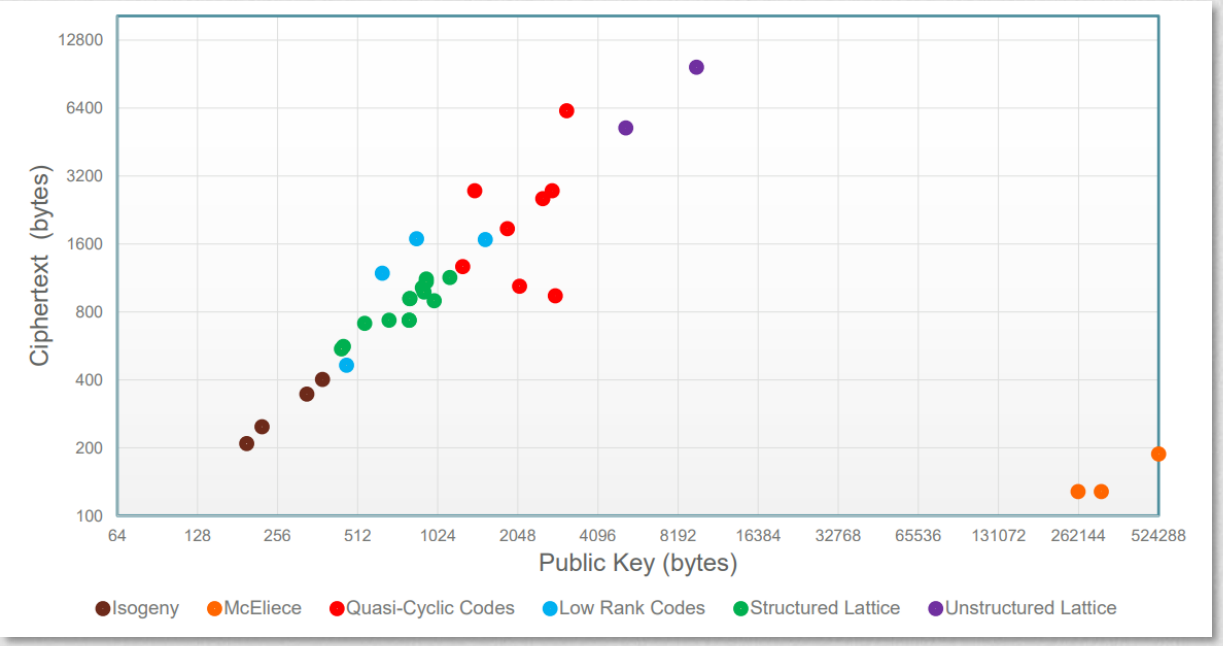
SIDH

장단점

- 장점
  - 다른 PQC 암호에 비해 키 사이즈가 작다
- 단점
  - 다른 PQC 암호에 비해 느리다

SIDH

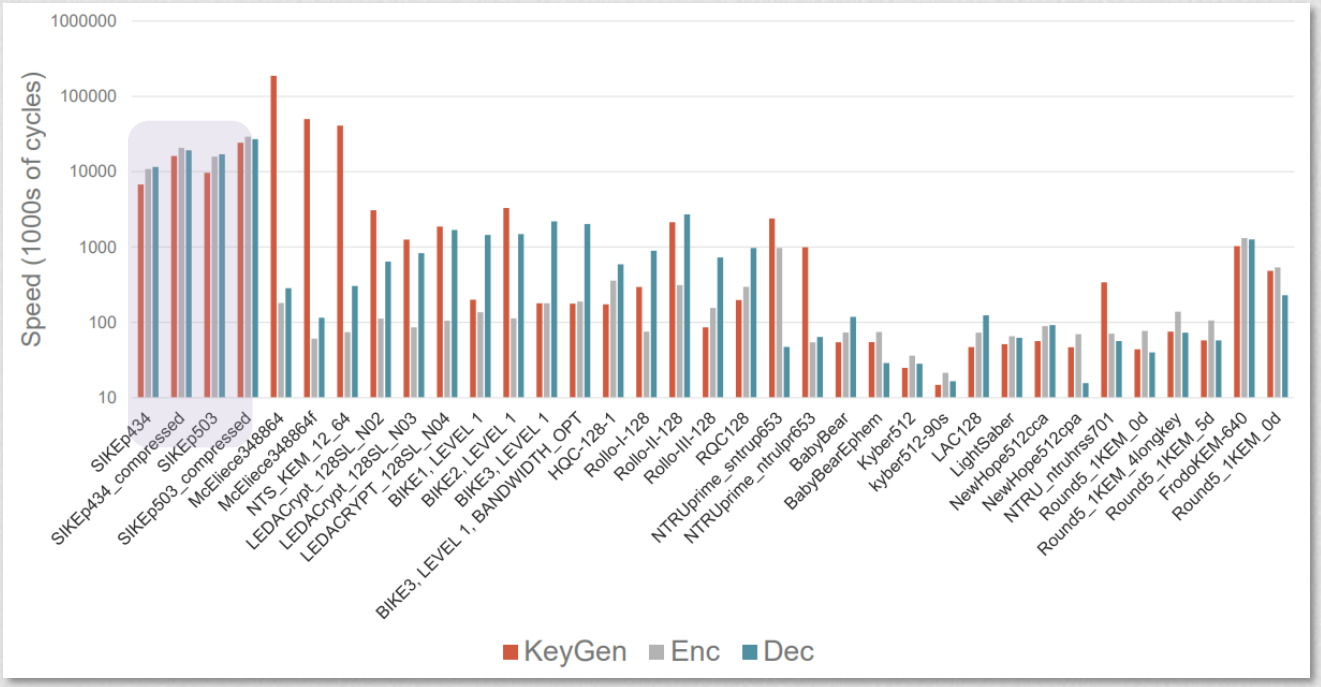
Performance



Opening Remarks PQC 2019, csrc.nist.gov

SIDH

Performance



Opening Remarks PQC 2019, csrc.nist.gov