EdSIDH: Supersingular Isogeny Diffie-Hellman on Edwards Curves

Reza Azarderakhsh[1], Elena Bakos Lang[2], David Jao[2,3], Brian Koziel[4]

[1]Florida Atlantic University, Boca Raton, Florida, United States
[2]University of Waterloo, Waterloo, Ontario, Canada
[3]evolutionQ, Waterloo, Ontario, Canada
[4]Texas Instruments, Dallas, Texas, United States

SPACE 2018

Current PKC is safe until large-scale quantum computers are available

- ECDH, ECDSA: Protected by the Elliptic curve discrete logarithm problem

Current PKC is safe until large-scale quantum computers are available

- ECDH, ECDSA: Protected by the Elliptic curve discrete logarithm problem
- RSA: Protected by the factorization and discrete logarithm problems

Current PKC is safe until large-scale quantum computers are available

- ECDH, ECDSA: Protected by the Elliptic curve discrete logarithm problem
- RSA: Protected by the factorization and discrete logarithm problems
- Large-scale quantum computers with Shor's algorithm will BREAK the security assumptions for these primitives

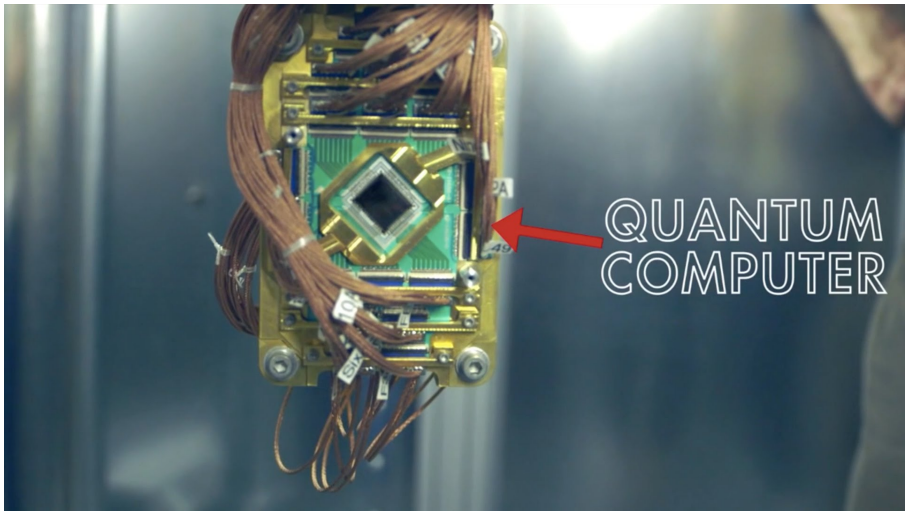


Figure: Quantum Computer (The Verge)

Primary PQC Candidates

Primary Post-Quantum Cryptography (PQC) Candidates:

- Code-Based: McEliece
- Hash-based: Lamport, Merkle Signatures
- Lattice-based: NTRU, LWE
- Multivariate: Rainbow Signature

Primary PQC Candidates

Primary Post-Quantum Cryptography (PQC) Candidates:

- Code-Based: McEliece
- Hash-based: Lamport, Merkle Signatures
- Lattice-based: NTRU, LWE
- Multivariate: Rainbow Signature
- Isogeny-based: SIDH, SIKE

Primary PQC Candidates

Primary Post-Quantum Cryptography (PQC) Candidates:

- Isogeny-based: SIDH, SIKE

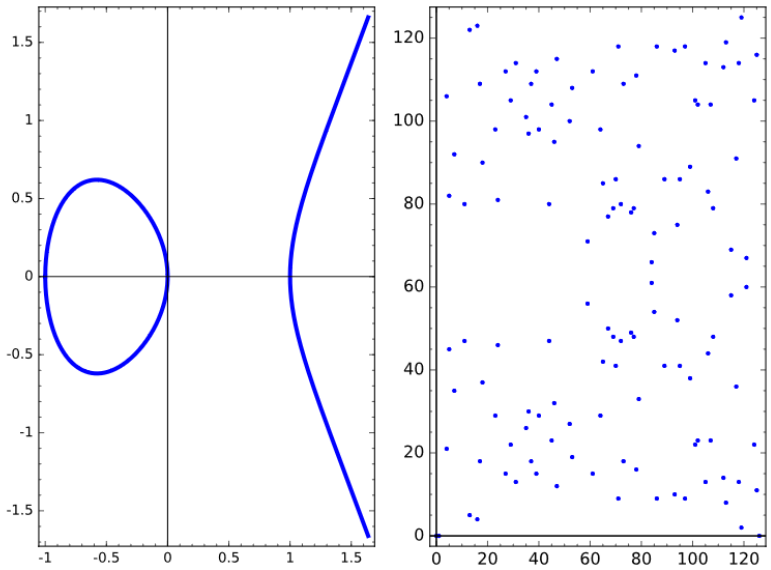


Figure: $E : y^2 = x^3 - x$ Left: $E/\mathbb{Z}$ Right: $E/\mathbb{F}_{127}$

Supersingular Isogeny-Based Cryptography Underlying Problem

- Consider two supersingular elliptic curves defined over a large prime extension field:
  $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$, where p is a large prime.
- There exists some isogeny $\phi : E_1 \rightarrow E_2$ with a fixed, smooth degree ℓ that is public which maps E_1 to E_2

Supersingular Isogeny Problem

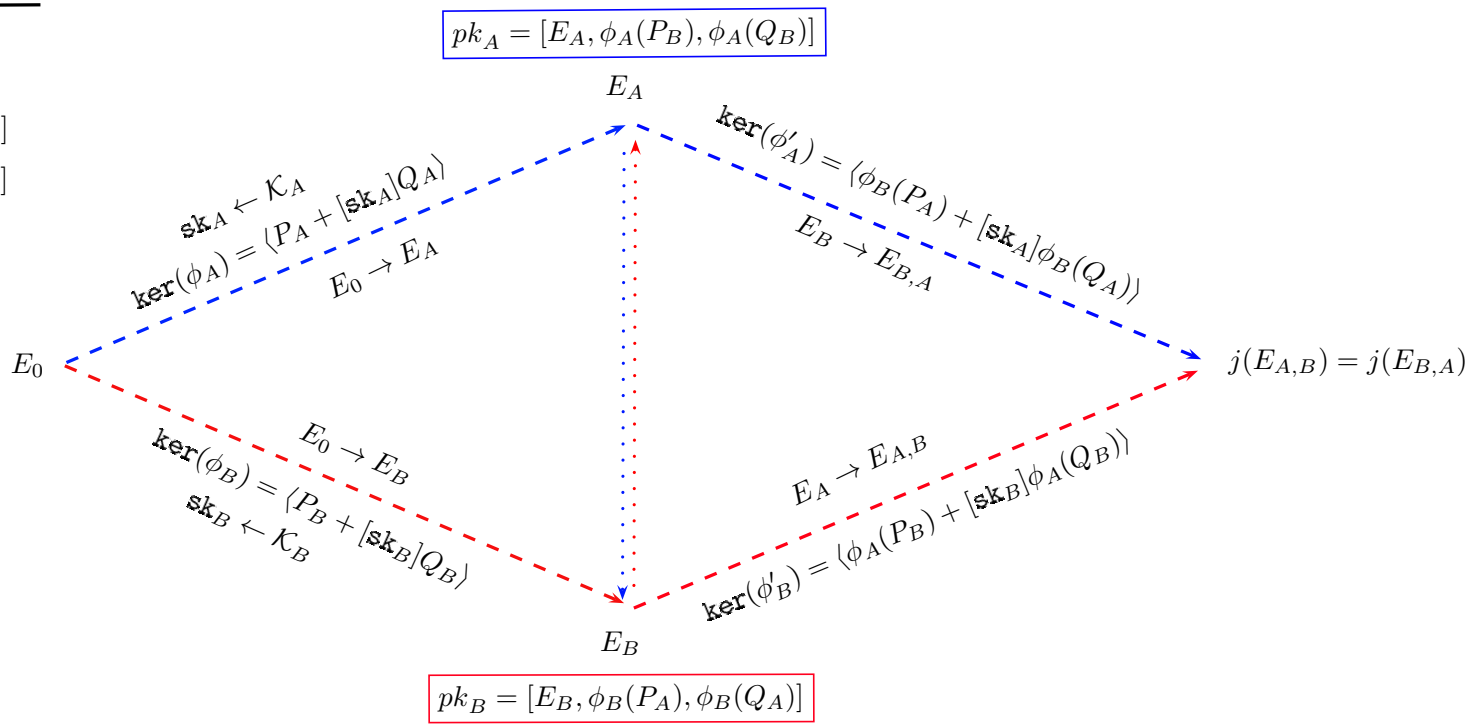
Given $P, Q \in E_1$ and $\phi(P), \phi(Q) \in E_2$, retrieve the secret isogeny map ϕ

- The best known attack is based on Claw finding algorithm
- Claw finding algorithm complexity for SIKE and SIDH:
  - $\mathcal{O}(p^{1/4})$ $\rightarrow$Classical attacks
  - $\mathcal{O}(p^{1/6})$ $\rightarrow$Quantum attacks

SIDH Key-Exchange

Public Parameters

E_0/F_{p^2}
$p = \ell_B^{e_A}\ell_B^{e_B} - 1$
$(P_A, Q_A) \in E_0[\ell_A^{e_A}]$
$(P_B, Q_B) \in E_0[\ell_B^{e_B}]$



Supersingular Isogeny-Based Cryptography Pros and Cons

- Pros
  - Very small public/private key size
  - Data-structure and implementation similar to ECC
  - Different security assumption compared to other candidates
  - No possibility of decryption error
  - No complicated error distribution, rejection sampling, etc.
  - Conservative security analysis on generic attacks
- Cons
  - Youngest PQC candidate
  - SLOW
  - Security concerns when reuse keys (handled with SIKE)
  - New schemes based on isogeny-based cryptography needs to be implemented on practical settings

Our Contributions

- We investigated implementations of SIDH/SIKE using Edwards curves;
- Derived extended Edwards curves isogeny formulas on incomplete Edwards curves (and for all possible kernels of order 2);
- Created an Edwards curves version of SIDH, which we call EdSIDH;
- Computed detailed operation counts for EdSIDH key exchange.

Edwards Form

A family of elliptic curves can be represented by an equation of the form

$$x^2 + y^2 = 1 + dx^2y^2$$

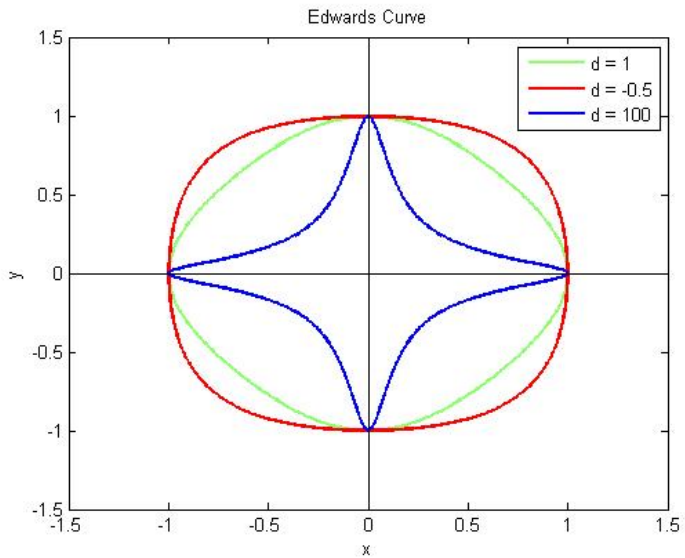
If d is not a square, Edwards curves have no points at infinity and a group law with no exceptional cases. Such curves are called complete, and otherwise are called incomplete.

The addition law for incomplete curves has exceptional cases – for some pairs P, Q we must use a different group law to compute $P + Q$.

Edwards Advantages

In classical Elliptic Curve Cryptography, Edwards curves have become widely adopted, as using a complete Edwards curve:

- Allows very fast computation of mP for a point $P \in E$;
- Removes the need for point validation in classical ECC;
- Gives better protection against side-channel attacks (no difference between formulas for ADD and DOUBLE).



Edwards Curves for SIDH

SIDH is currently defined on Montgomery curves, as they have efficient computation methods and we can use Vélu's formulas directly to compute isogenies.

Moody and Shumow (2011) presented new formulas for isogenies on (complete) Edwards curves.

Problem: We need incomplete Edwards curves for EdSIDH - complete Edwards curves only have 1 point of order 2, and curves for SIDH need to have at least 3 points of order 2.

Computing Isogenies

If an elliptic curve is in Weierstrass (or Montgomery) form, explicit equations for evaluating an isogeny with kernel F at point P given by Vélu's formulas:

$$\phi(P) = \left(x_P + \sum_{Q \in F \setminus \{\infty\}} (x_{P+Q} - x_Q), y_p + \sum_{Q \in F \setminus \{\infty\}} (y_{P+Q} - y_Q) \right)$$

Isogeny formulas equivalent to Vélu's for Edwards curves were found by Moody and Shumow (2011). They presented new formulas for odd isogenies, and composite formulas for even isogenies (with kernel $\{(0,1),(-1,0)\}$).

Computing Isogenies on Edwards Curves

Odd isogenies for (completed) Edwards curves given by:

$$\phi(P) = \left(\prod_{Q \in F} \frac{x_{P+Q}}{x_Q}, \prod_{Q \in F} \frac{y_{P+Q}}{y_Q} \right)$$

Even isogenies can be found by mapping curve to Weierstrass form, applying Vélu's formulas, and mapping back (ψ is an isomorphism between an Edwards curve and a Weierstrass one, and ϕ' is an isogeny given by Vélu's formula):

$$\phi(P) = \psi \cdot \phi' \cdot \psi^{-1}(P)$$

Odd Isogenies

We showed that Moody and Shumow's equations are still valid for incomplete Edwards curves by showing that all group operations in odd-isogeny computation use the basic group law.

An ℓ-isogeny from the curve E_d to E'_d (where $d' = \beta^8 d^3$) with kernel $F = \{(0,1), (\pm\alpha_1, \beta_1), \ldots, (\pm\alpha_s, \beta_s)\}$ is given by:

$$\psi(x,y) = \left(\frac{x}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 x^2 - \alpha_i^2 y^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 y^2 - \alpha_i^2 x^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2} \right)$$

Optimized cost (for 3-isogenies): $13M + 9S$ for $\phi(P)$ and $3S + 2M$ to compute the curve coefficent.

Even Isogenies

2-isogeny mapping the curve E_d to the curve $E_{d'}$ with $d' = 1 + 4\frac{\beta^4\alpha^2(1-d)}{\beta^2-1}$ is given by:

$$(x, y) \mapsto \left(\frac{xy}{\alpha\beta}, \frac{x(\beta^2-1)+4\beta^2(1-d)}{x(\beta^2-1)-4\beta^2(1-d)}\right)$$

Optimized cost: $23M + 2S$ for $\phi(P)$, $7M + 1I$ for the curve coefficient.

SIDH Computations

Secret Kernel Generation

- Inputs:
  - Supersingular elliptic curve $E(\mathbb{F}_{p^2})$, torsion basis $\{P, Q\}$, private keys m
- Compute $R = \langle [m]P + Q \rangle$

Large-Degree Isogeny

- Inputs:
  - Supersingular elliptic curve E, secret kernel point R
- Compute $\phi : E \rightarrow E/\langle R \rangle$ by iteratively computing isogenies

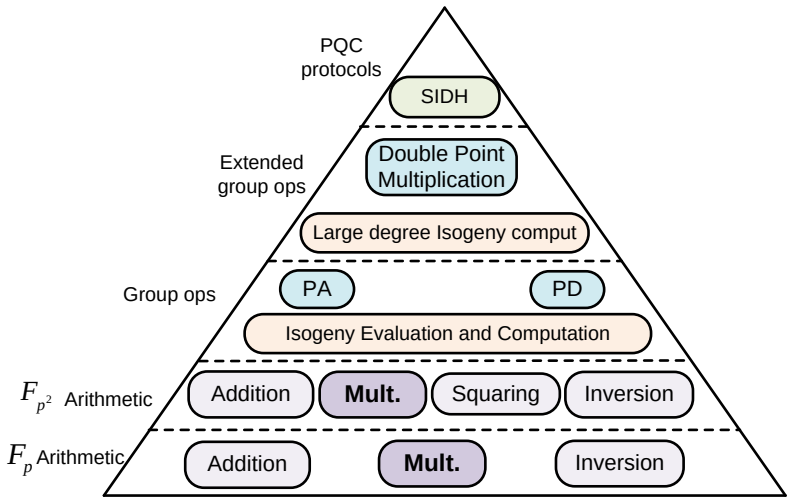


Figure: Breakdown of supersingular isogeny computations

SIDH Kernel Generation Cost

- Computing $R = \langle [m]P + Q \rangle$ can be done using a variety of ECC point multiplication techniques
- A window-based method over Edwards curves is slightly faster than Montgomery curves

Table: SIDH secret kernel generation cost per bit

Scheme	Cost per bit
Kummer Montgomery	$6M + 4S$
Edwards with Montgomery Ladder	
Projective Edwards	$13M + 5S + 1C$
Complete Edwards	$34M + 4S + 1C$
Edwards with Window Method ($k = 4$)	
Projective Edwards	$5.5M + 4.25S + 0.25C$
Complete Edwards	$12.25M + 4S + 1C$

SIDH Large-Degree Isogeny Cost

- We can compute $\phi : E \to E/\langle R \rangle$ using a sequence of point multiplications and isogeny computations
- With this work, Edwards curves appear at least twice as slow as Montgomery curves

Table: Normalized complexities for a large-degree isogeny computation for different coordinate schemes. $R = 22\lceil \log_2 p \rceil \tilde{M}$, $I = 10\tilde{M}$, $M = 3\tilde{M}$, $S = 2\tilde{M}$, and $C = 2\tilde{M}$.

Large-Degree Isogeny	Affine Mont.	Proj. Mont.	Affine Ed. (This Work)	
			Proj.	Complete
2^{250}	$27102\tilde{M}$	-	$87685\tilde{M}$	$97841\tilde{M}$
3^{159}	$29686\tilde{M}$	$28452\tilde{M}$	$65355\tilde{M}$	-
4^{125}	$22617\tilde{M}$	$24126\tilde{M}$	$181582\tilde{M}$	$191278\tilde{M}$

Conclusion

- We devised efficient formulas to implement SIDH/SIKE over Edwards curves, which may provide more security in implementations
- Currently Edwards curves with optimized formulas appear twice as slow as their Montgomery counterparts
- Our results ndicate that SIDH/SIKE may be more efficient with odd base isogeny when using Edwards formulae
- Using different representations such as y-only arithmetic may yield even faster results

References


L. De Feo, D. Jao, L. Plût, (2014), Toward Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies, Journal of Mathematical Cryptology, 8(3): 209-247.


D. Moody and D. Shumow (2011), Analogues of Vélu's formulas for Isogenies on Alternate Models of Elliptic Curves, Cryptology ePrint Archive, Report 2011/430.


C. Costello, P. Longa, M. Naehrig (2016) , Efficent Algorithms for Supersingular Isogeny DIffie-Hellman, CRYPTO 2016, Part I, pages 679-706.

Questions?