Supersingular Isogeny Diffie-Hellman

Michael Naehrig
Microsoft Research

Real World Cryptography Conference
New York, 4 January 2017

Elliptic curves in cryptography

- Factoring (ECM), Primality proving (ECPP)
- Simple and fast key exchange
- Digital signatures
- Small parameters, only generic attacks
- Pairings: ID-based encryption, short signatures, ABE,…

Elliptic curves in cryptography

Some prominent curves:

- NIST: P-256, P-384, P-521
- IRTF/CFRG: Curve25519, Curve448

Widely used: TLS, OpenSSL, OpenSSH, Signal,…

Here is a quite different curve…

$$p = 2^{372} \cdot 3^{239} - 1$$

$$E/\mathbb{F}_{p^2} : y^2 = x^3 + x$$

$$\#E(\mathbb{F}_{p^2}) = (2^{372} \cdot 3^{239})^2$$

…that's really bad for traditional ECC

It is supersingular and has smooth group order:

- Can solve DLP in any subgroup easily via Pohlig-Hellman
- Weil pairing maps DLP to finite field group, where it becomes even easier

$$p = 2^{372} \cdot 3^{239} - 1$$

$$E/\mathbb{F}_{p^2} : y^2 = x^3 + x$$

$$\#E(\mathbb{F}_{p^2}) = (2^{372} \cdot 3^{239})^2$$

$$e : E[2^{372} \cdot 3^{239}] \times E[2^{372} \cdot 3^{239}] \to \mathbb{F}_{p^2}^*$$

Subgroups as secrets

- There is a large number of cyclic subgroups of maximal 2-power order.

$$E[2^{372}] \cong \mathbb{Z}_{2^{372}} \times \mathbb{Z}_{2^{372}}$$

$$E[2^{372}] = \langle P_A, Q_A \rangle \subset E(\mathbb{F}_{p^2})$$

$$G = \langle R_A \rangle = \langle [m_A]P_A + [n_A]Q_A \rangle$$

$$\#\{\langle R_A \rangle \mid \mathrm{ord}(R_A) = 2^{372}\} = 3 \cdot 2^{371}$$

Subgroups as secrets

- There is a large number of cyclic subgroups of maximal 3-power order.

$$E[3^{239}] \cong \mathbb{Z}_{3^{239}} \times \mathbb{Z}_{3^{239}} \qquad E[3^{239}] = \langle P_B, Q_B \rangle \subset E(\mathbb{F}_{p^2})$$

$$H = \langle R_B \rangle = \langle [m_B]P_B + [n_B]Q_B \rangle$$

$$\#\{\langle R_B \rangle \mid \mathrm{ord}(R_B) = 3^{239}\} = 4 \cdot 3^{238}$$

Isogenies correspond to subgroups

- Isogeny: (non-constant) rational map that is a group homomorphism

$$\phi : E_1 \to E_2$$
$$\phi(\mathcal{O}_{E_1}) \to \mathcal{O}_{E_2}$$

- A finite subgroup corresponds to a unique (up to isomorphism) curve and isogeny with that kernel

$$G \subseteq E_1$$
$$\phi : E_1 \to E_2$$
$$\ker(\phi) = G$$
$$E_2 = \phi(E_1) = E_1/G$$

- Degree of (separable) isogeny is number of elements in its kernel, same as its degree as a rational map

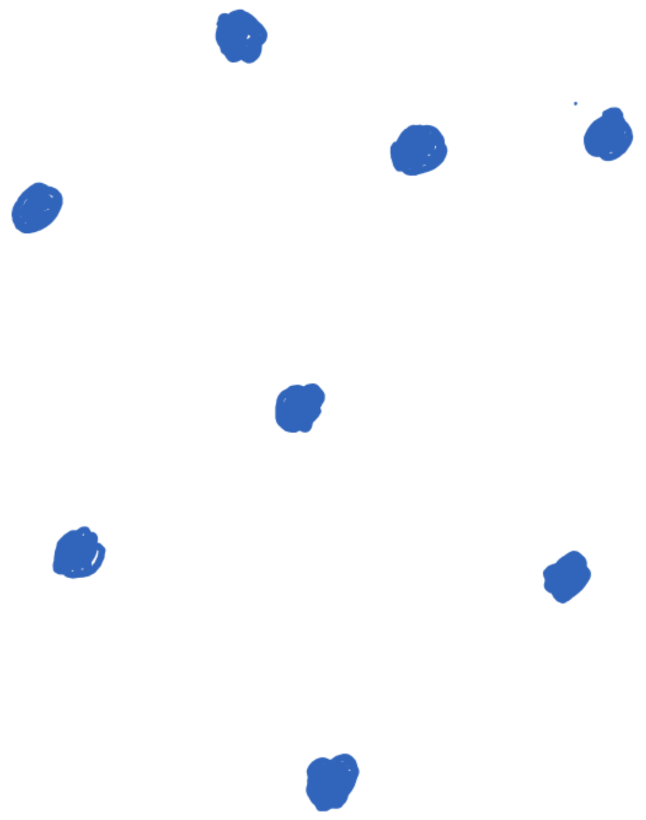
$$\deg(\phi) = |G|$$

Supersingular isogeny graphs

- Vertices: all isogenous elliptic curves over $\mathbb{F}_{p^2}$
  There are about $\lfloor p/12 \rfloor$ of them,
  all have the same order.
- Edges: isogenies of a fixed prime degree ℓ (here $\ell = 2$ or $\ell = 3$)
  Get a connected, (ℓ+1)-regular graph.

Supersingular isogeny graphs

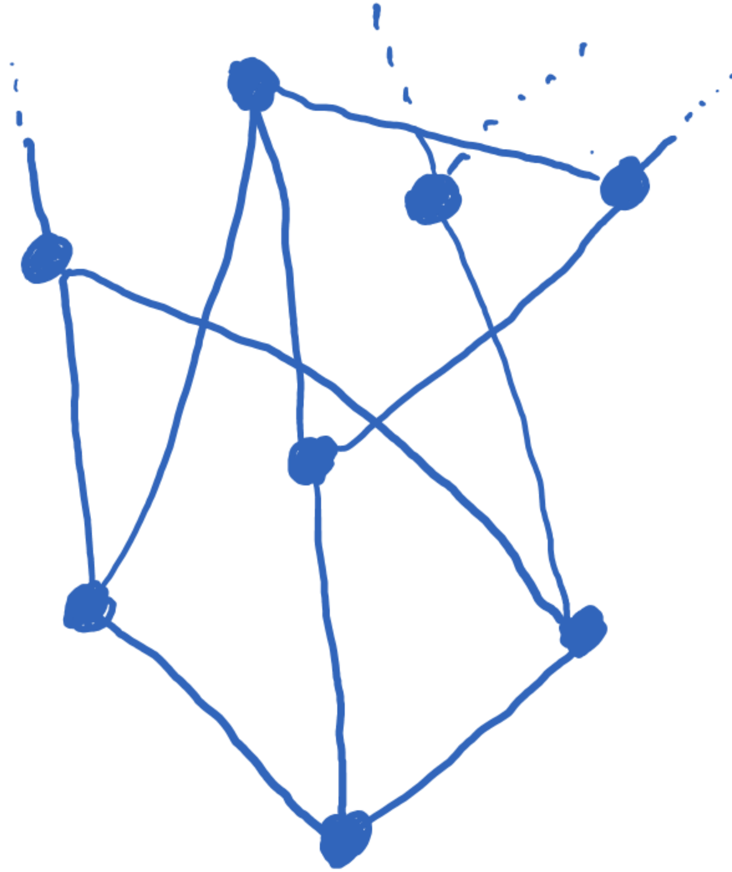
- Vertices: all isogenous elliptic curves over $\mathbb{F}_{p^2}$
  There are about $\lfloor p/12 \rfloor$ of them,
  all have the same order.
- Edges: isogenies of a fixed prime degree ℓ (here $\ell = 2$ or $\ell = 3$)
  Get a connected, (ℓ+1)-regular graph.



Supersingular isogeny graphs

- Vertices: all isogenous elliptic curves over $\mathbb{F}_{p^2}$
  There are about $\lfloor p/12 \rfloor$ of them, all have the same order.

- Edges: isogenies of a fixed prime degree ℓ (here $\ell = 2$ or $\ell = 3$)
  Get a connected, (ℓ+1)-regular graph.

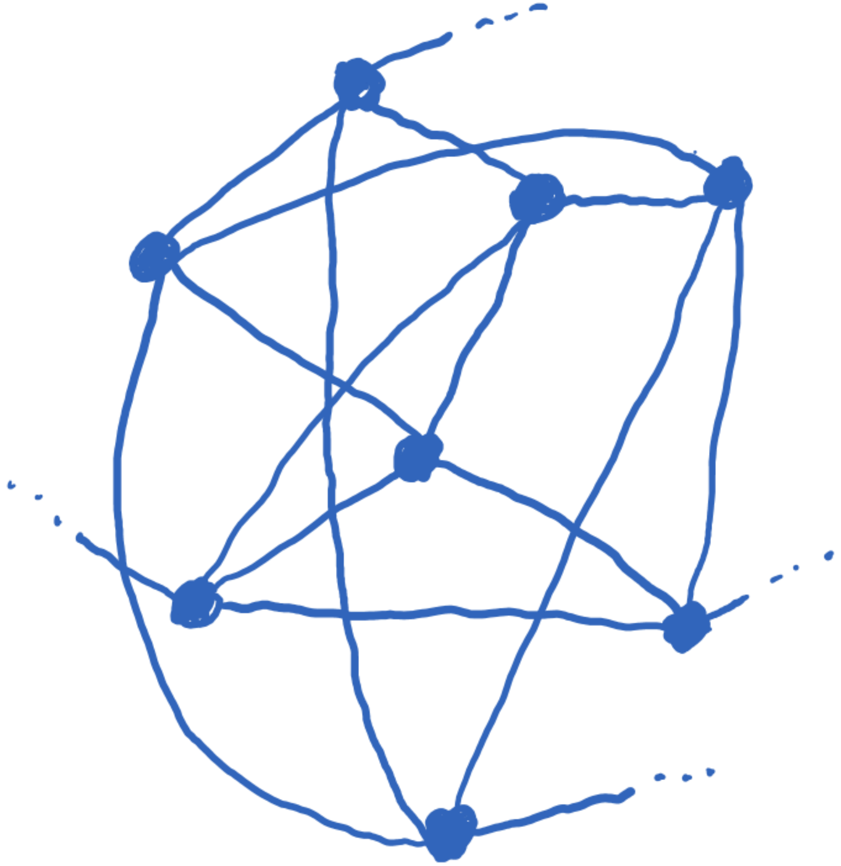


$\ell = 2$

Supersingular isogeny graphs

- Vertices: all isogenous elliptic curves over $\mathbb{F}_{p^2}$
  There are about $\lfloor p/12 \rfloor$ of them, all have the same order.

- Edges: isogenies of a fixed prime degree ℓ (here $\ell = 2$ or $\ell = 3$)
  Get a connected, (ℓ+1)-regular graph.



$\ell = 3$

Evaluating smooth-degree isogenies

- Can compute isogenies of prime degree ℓ via Vélu's formulas at cost $\mathcal{O}(\ell)$ field operations

- Can only compute large-degree isogenies if smooth

- For example: $\phi : E \to E/\langle R_0 \rangle, \ \mathrm{ord}(R_0) = 2^{372}$
  Decompose into 2-isogenies

$$\phi = \phi_{371} \circ \phi_{370} \circ \cdots \circ \phi_1 \circ \phi_0$$

$$\phi_0 : E_0 \to E_1 = E_0/\langle [2^{371}] R_0 \rangle, R_1 = \phi_0(R_0)$$

Analogues between DH instantiations

	DH	ECDH	SIDH
elements	Integers g modulo prime	points P in curve group	curves E in isogeny class
secrets	exponents x	scalars k	isogenies ϕ
computations	$(g, x) \mapsto g^x$	$(P, k) \mapsto [k]P$	$(E, \phi) \mapsto \phi(E)$
hard problem	given g, g^x find x	given $P, [k]P$ find k	given $E, \phi(E)$ find ϕ

Supersingular Isogeny Diffie-Hellman

Alice (secret)
Bob (secret)
Public

$$S = [m_A]P_A + [n_A]Q_A$$

$$R = [m_B]P_B + [n_B]Q_B$$

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E/\langle S \rangle \\ E/\langle R \rangle & \end{tikzcd}$$

Supersingular Isogeny Diffie-Hellman

Alice (secret)
Bob (secret)
Public

$$S = [m_A]P_A + [n_A]Q_A \qquad \{\phi_A(P_B), \phi_A(Q_B)\}$$

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E/\langle S \rangle \\
E/\langle R \rangle &
\end{tikzcd}$$

$$R = [m_B]P_B + [n_B]Q_B$$

$$\{\phi_B(P_A), \phi_B(Q_A)\}$$

Supersingular Isogeny Diffie-Hellman

Alice (secret)
Bob (secret)
Public

$$S = [m_A]P_A + [n_A]Q_A \qquad \{\phi_A(P_B), \phi_A(Q_B)\}$$

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "R = [m_B]P_B + [n_B]Q_B \quad \phi_B"'] & E/\langle S \rangle \arrow[d, "\phi_A(R) = [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B)"] \\
E/\langle R \rangle \arrow[r, "\phi_B(S)"] & E/\langle R, S \rangle
\end{tikzcd}$$

$$\{\phi_B(P_A), \phi_B(Q_A)\}$$

Supersingular Isogeny Diffie-Hellman

Alice (secret)
Bob (secret)
Public

$$\left.\begin{array}{c}\{\phi_A(P_B), \phi_A(Q_B)\}\\ E/\langle S\rangle\end{array}\right\}\ 564\text{B}$$

$$\begin{tikzcd}
E \arrow[r, "\phi_A", "S"'] \arrow[d, "\phi_B"', "R"] & E/\langle S\rangle \arrow[d, "\phi_A(R)"] \\
E/\langle R\rangle \arrow[r, "\phi_B(S)"] & E/\langle R, S\rangle
\end{tikzcd}$$

$$564\text{B}\ \left\{\begin{array}{c}E/\langle R\rangle\\ \{\phi_B(P_A), \phi_B(Q_A)\}\end{array}\right.$$

SIDH performance

SIDH operation	Time
Alice key generation	46
Bob key generation	52
Alice shared secret	44
Bob shared secret	50
Total	192

Table: millions of clock cycles for DH operations on Intel core i7-4770 (3.4GHz) Haswell

https://www.microsoft.com/en-us/research/project/sidh-library/

*includes full protection against timing and cache attacks

Supersingular Isogeny Problem

For a large prime p, supersingular $E_1/\mathbb{F}_{p^2}$, $E_2/\mathbb{F}_{p^2}$, an isogeny $\phi : E_1 \to E_2$ with fixed, smooth, public degree:

Given $E_1, E_2,\ P_1, Q_1 \in E_1,\ \phi(P_1), \phi(Q_1) \in E_2,$

compute ϕ !

- **Best (known) attacks:** classical $\mathcal{O}(p^{1/4})$, quantum $\mathcal{O}(p^{1/6})$ via generic claw finding algorithms
- Post-quantum security roughly 125 bits

Public key compression

Represent points not by coordinates, but by scalars w.r.t. a deterministically computed torsion basis.

- Scalars are shorter representation than coordinates

$E_A[2^{372}] = \langle R_1, R_2 \rangle$ $\phi_B(P_A) = \alpha_P R_1 + \beta_P R_2$ $\alpha_P, \beta_P \in \mathbb{Z}_{2^{372}}$

Original public key

$(E_B, \phi_B(P_A), \phi_B(Q_A))$

$6\log(p) \leftrightarrow 564\mathrm{B}$

Compressed public key

$(E_B, \alpha_P^{-1}\beta_P, \alpha_P^{-1}\alpha_Q, \alpha_P^{-1}\beta_Q)$

$\approx \frac{7}{2}\log(p) \leftrightarrow 330\mathrm{B}$

Public key compression

- Deterministically, compute a basis of the torsion group
- Map DLPs to field via pairing computation
- Solve DLPs with (nested) Pohlig-Hellman algorithm
- Cost: about the same as one full key exchange

$$E_A[2^{372}] = \langle R_1, R_2 \rangle$$

$$e_0 = e\left(R_1, R_2\right) \in \mathbb{F}_{p^2}^*$$
$$e_1 = e\left(R_1, P\right) = e_0^{\beta_P}$$
$$e_2 = e\left(R_1, Q\right) = e_0^{\beta_Q}$$
$$e_3 = e\left(R_2, P\right) = e_0^{-\alpha_P}$$
$$e_4 = e\left(R_2, Q\right) = e_0^{-\alpha_Q}$$

Ephemeral vs. static keys

Assume Alice uses a static key $S = P_A + [n_A]Q_A$

- Bob sends his "public key"

$$\left(E_B, \phi_B(P_A), \phi_B(Q_A) + [2^{371}]\phi_B(P_A)\right)$$

- Honestly computes the shared secret and uses Alice as an oracle:

$$\left\langle \phi_B(P_A) + [n_A]\phi_B(Q_A) \right\rangle = \left\langle \phi_B(P_A) + [n_A]\left(\phi_B(Q_A) + [2^{371}]\phi_B(P_A)\right) \right\rangle$$

if and only if $n_A \equiv 0 \mod 2$

Ephemeral vs. static keys

- This let’s Bob determine the LSB of Alice’s secret
- Proceed similarly for the other bits
- Can determine Alice’s public key bit by bit

One-sided static keys can only be used with a costly validation procedure.

Otherwise, use ephemeral key exchange only!

Call for help!

Take another look at isogeny-based crypto!

Break it: try to find efficient (classical/quantum) algorithms for solving isogeny problems

Speed it up: find better algorithms for isogeny evaluation/computation, write fast implementations (on different platforms)

Solve open problems: public key validation, efficient signatures

References

L. DeFeo, D. Jao, J. Plut: **Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies**. J. Math. Crypt. 8(3), 2014.

C. Costello, P. Longa, M. Naehrig: **Efficient Algorithms for Supersingular Isogeny Diffie-Hellman**. CRYPTO 2016.

R. Azarderaksh, D. Jao, K. Kalach, B. Koziel, C. Leonardi: **Key compression for Isogeny-Based Cryptosystems**. AsiaPKC 2016.

C. Costello, D. Jao, P. Longa, M. Naehrig, J. Renes, D. Urbanik: **Efficient compression of SIDH public keys**. http://eprint.iacr.org/2016/963.

S. D. Galbraith, C. Petit, B. Shani, Y. B. Ti: **On the Security of Supersingular Isogeny Cryptosystems**. ASIACRYPT 2016.

Thank you!

$$\begin{tikzcd} E \arrow[r] \arrow[d] & E/\langle S\rangle \arrow[d] \\ E/\langle R\rangle \arrow[r] & E/\langle R, S\rangle \end{tikzcd}$$