An introduction to supersingular isogeny-based cryptography

Craig Costello

Summer School on Real-World Crypto and Privacy
June 8, 2017
Šibenik, Croatia
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies

LUCA DE FEO, DAVID JAO, JÉRÔME PLÛT


Full version of Crypto’16 paper
(joint with P. Longa and M. Naehrig)
http://eprint.iacr.org/2016/413

Full version of Eurocrypt’17 paper
(joint with D. Jao, P. Longa, M. Naehrig, D. Urbanik, J. Renes)
http://eprint.iacr.org/2016/963

Preprint of recent work on flexible SIDH
(joint with H. Hisil)
http://eprint.iacr.org/2017/504

SIDH library v2.0
https://www.microsoft.com/en-us/research/project/sidh-library/
Part 1: Motivation

Part 2: Preliminaries

Part 3: SIDH
Quantum computers ↔ Cryptopocalypse

- Quantum computers break elliptic curves, finite fields, factoring, everything currently used for PKC
- Aug 2015: NSA announces plans to transition to quantum-resistant algorithms
Post-quantum key exchange

Which hard problem(s) to use now???

This talk: supersingular isogenies
# Diffie-Hellman(ish) instantiations

<table>
<thead>
<tr>
<th></th>
<th>DH</th>
<th>ECDH</th>
<th>R-LWE</th>
<th>LWE</th>
<th>SIDH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>elements</strong></td>
<td>integers $g$ modulo prime</td>
<td>points $P$ in curve group</td>
<td>elements $a$ in ring $R = \mathbb{Z}_q[x]/\langle \Phi_n(x) \rangle$</td>
<td>matrices $A$ in $\mathbb{Z}_q^{n \times n}$</td>
<td>curves $E$ in isogeny class</td>
</tr>
<tr>
<td><strong>secrets</strong></td>
<td>exponents $x$</td>
<td>scalars $k$</td>
<td>small errors $s, e \in R$</td>
<td>small $s, e \in \mathbb{Z}_q^n$</td>
<td>isogenies $\phi$</td>
</tr>
<tr>
<td><strong>computation</strong></td>
<td>$g, x \mapsto g^x$</td>
<td>$k, P \mapsto [k]P$</td>
<td>$a, s, e \mapsto as + e$</td>
<td>$A, s, e \mapsto As + e$</td>
<td>$\phi, E \mapsto \phi(E)$</td>
</tr>
<tr>
<td><strong>hard problem</strong></td>
<td>given $g, g^x$ find $x$</td>
<td>given $P, [k]P$ find $k$</td>
<td>given $a, as + e$ find $s$</td>
<td>given $A, As + e$ find $s$</td>
<td>given $E, \phi(E)$ find $\phi$</td>
</tr>
</tbody>
</table>
Part 1: Motivation
Part 2: Preliminaries
Part 3: SIDH
Extension fields

To construct degree $n$ extension field $\mathbb{F}_{q^n}$ of a finite field $\mathbb{F}_q$, take $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ where $f(\alpha) = 0$ and $f(x)$ is irreducible of degree $n$ in $\mathbb{F}_q[x]$.

Example: for any prime $p \equiv 3 \mod 4$, can take $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 + 1 = 0$
Recall that every elliptic curve $E$ over a field $K$ with $\text{char}(K) > 3$ can be defined by

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in K$, $4a^3 + 27b^2 \neq 0$.

For any extension $K'/K$, the set of $K'$-rational points forms a group with identity.

The $j$-invariant $j(E) = j(a, b) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2}$ determines isomorphism class over $\overline{K}$.

E.g., $E' : y^2 = x^3 + au^2x + bu^3$ is isomorphic to $E$ for all $u \in K^*$.

Recover a curve from $j$: e.g., set $a = -3c$ and $b = 2c$ with $c = j/(j - 1728)$.
Example

Over $\mathbb{F}_{13}$, the curves

\[ E_1 : y^2 = x^3 + 9x + 8 \]

and

\[ E_2 : y^2 = x^3 + 3x + 5 \]

are isomorphic, since

\[ j(E_1) = 1728 \cdot \frac{4 \cdot 9^3}{4 \cdot 9^3 + 27 \cdot 8^2} = 3 = 1728 \cdot \frac{4 \cdot 3^3}{4 \cdot 3^3 + 27 \cdot 5^2} = j(E_2) \]

An isomorphism is given by

\[ \psi : E_1 \rightarrow E_2, \quad (x, y) \mapsto (10x, 5y), \]

\[ \psi^{-1} : E_2 \rightarrow E_1, \quad (x, y) \mapsto (4x, 8y), \]

noting that $\psi(\infty_1) = \infty_2$
Torsion subgroups

• The multiplication-by-\( n \) map:
  \[ n : E \to E, \quad P \mapsto [n]P \]

• The \( n \)-torsion subgroup is the kernel of \( [n] \):
  \[ E[n] = \{ P \in E(\overline{K}) : [n]P = \infty \} \]

• Found as the roots of the \( n^{th} \) division polynomial \( \psi_n \)

• If \( \text{char}(K) \) doesn’t divide \( n \), then
  \[ E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n \]
Example \((n = 3)\)

- Consider \(E/F_{11} : y^2 = x^3 + 4\) with \(\#E(F_{11}) = 12\)

- 3-division polynomial \(\psi_3(x) = 3x^4 + 4x\) partially splits as \(\psi_3(x) = x(x + 3)(x^2 + 8x + 9)\)

- Thus, \(x = 0\) and \(x = -3\) give 3-torsion points. The points \((0,2)\) and \((0,9)\) are in \(E(F_{11})\), but the rest lie in \(E(F_{11^2})\)

- Write \(F_{11^2} = F_{11}(i)\) with \(i^2 + 1 = 0\). \(\psi_3(x)\) splits over \(F_{11^2}\) as \(\psi_3(x) = x(x + 3)(x + 9i + 4)(x + 2i + 4)\)

- Observe \(E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3\), i.e., 4 cyclic subgroups of order 3
Subgroup isogenies

• **Isogeny**: morphism (rational map)
  \[ \phi : E_1 \to E_2 \]
  that preserves identity, i.e. \( \phi(\infty_1) = \infty_2 \)

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

• Given finite subgroup \( G \in E_1 \), there is a unique curve \( E_2 \) and isogeny \( \phi : E_1 \to E_2 \) (up to isomorphism) having kernel \( G \). Write \( E_2 = \phi(E_1) = E_1/\langle G \rangle \).
Subgroup isogenies: special cases

• Isomorphisms are a special case of isogenies where the kernel is trivial
  \[ \phi : E_1 \to E_2, \quad \ker(\phi) = \infty_1 \]

• Endomorphisms are a special case of isogenies where the domain and co-domain are the same curve
  \[ \phi : E_1 \to E_1, \quad \ker(\phi) = G, \quad |G| > 1 \]

• Perhaps think of isogenies as a generalization of either/both: isogenies allow non-trivial kernel and allow different domain/co-domain

• Isogenies are *almost* isomorphisms
Velu’s formulas

Given any finite subgroup of $G$ of $E$, we may form a quotient isogeny

$$\phi: E \to E' = E/G$$

with kernel $G$ using Velu’s formulas

Example: $E : y^2 = (x^2 + b_1x + b_0)(x - a)$. The point $(a, 0)$ has order 2; the quotient of $E$ by $\langle (a, 0) \rangle$ gives an isogeny

$$\phi : E \to E' = E/\langle (a, 0) \rangle,$$

where

$$E' : y^2 = x^3 + (-(4a + 2b_1))x^2 + (b_1^2 - 4b_0)x$$

And where $\phi$ maps $(x, y)$ to

$$\left( \frac{x^3-(a-b_1)x^2-(b_1a-b_0)x-b_0a}{x-a}, \frac{x^2-(2a)x-(b_1a+b_0)}{(x-a)^2} \right)$$
Velu’s formulas

Given curve coefficients \(a, b\) for \(E\), and all of the \(x\)-coordinates \(x_i\) of the subgroup \(G \in E\), Velu’s formulas output \(a', b'\) for \(E'\), and the map

\[
\phi : \ E \rightarrow E',
\]

\[
(x, y) \mapsto \left( \frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)} \right)
\]
Example, cont.

- Recall $E/F_{11} : y^2 = x^3 + 4$ with $\#E(F_{11}) = 12$

- Consider $[3] : E \rightarrow E$, the multiplication-by-3 endomorphism

- $G = \ker([3])$, which is not cyclic

- Conversely, given the subgroup $G$, the unique isogeny $\phi$ with $\ker(\phi) = G$ turns out to be the endomorphism $\phi = [3]$

- But what happens if we instead take $G$ as one of the cyclic subgroups of order 3?
Example, cont. \( E/\mathbb{F}_{11}: y^2 = x^3 + 4 \)

\[ E_1/\mathbb{F}_{11}: y^2 = x^3 + 2 \]

\[ E_2/\mathbb{F}_{11}: y^2 = x^3 + 5x \]

\[ E_3/\mathbb{F}_{11^2}: y^2 = x^3 + (7i + 3)x \]

\[ E_4/\mathbb{F}_{11^2}: y^2 = x^3 + (4i + 3)x \]

\( E_1, E_2, E_3, E_4 \) all 3-isogenous to \( E \), but what’s the relation to each other?
Isomorphisms and isogenies

- Fact 1: $E_1$ and $E_2$ isomorphic iff $j(E_1) = j(E_2)$
- Fact 2: $E_1$ and $E_2$ isogenous iff $\#E_1 = \#E_2$ (Tate)
- Fact 3: $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$ (Hasse)

Upshot for fixed $q$

$O(\sqrt{q})$ isogeny classes

$O(q)$ isomorphism classes
Supersingular curves

- $E / \mathbb{F}_q$ with $q = p^n$ supersingular iff $E[p] = \{\infty\}$
- Fact: all supersingular curves can be defined over $\mathbb{F}_p^2$
- Let $S_{p^2}$ be the set of supersingular $j$-invariants

Theorem: $\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + b, \quad b \in \{0,1,2\}$
The supersingular isogeny graph

- We are interested in the set of supersingular curves (up to isomorphism) over a specific field.

- Thm (Mestre): all supersingular curves over $\mathbb{F}_{p^2}$ in same isogeny class.

- Fact (see previous slides): for every prime $\ell$ not dividing $p$, there exists $\ell + 1$ isogenies of degree $\ell$ originating from any supersingular curve.

Upshot: immediately leads to $(\ell + 1)$ directed regular graph $X(S_{p^2}, \ell)$. 

E.g. a supersingular isogeny graph

- Let $p = 241$, $\mathbb{F}_{p^2} = \mathbb{F}_p[w] = \mathbb{F}_p[x]/(x^2 - 3x + 7)$

- $\#S_{p^2} = 20$

- $S_{p^2} = \{93, 51w + 30, 190w + 183, 240, 216, 45w + 211, 196w + 105, 64, 155w + 3, 74w + 50, 86w + 227, 167w + 31, 175w + 237, 66w + 39, 8, 23w + 193, 218w + 21, 28, 49w + 112, 192w + 18\}$

Credit to Fre Vercauteren for example and pictures...
Supersingular isogeny graph for $\ell = 2$: $X(S_{241^2}, 2)$
Supersingular isogeny graph for $\ell = 3$: $X(S_{241^2}, 3)$
Supersingular isogeny graphs are Ramanujan graphs

**Rapid mixing property:** Let $S$ be any subset of the vertices of the graph $G$, and $x$ be any vertex in $G$. A “long enough” random walk will land in $S$ with probability at least $\frac{|S|}{2|G|}$.

See De Feo, Jao, Plut (Prop 2.1) for precise formula describing what’s “long enough.”
Part 1: Motivation
Part 2: Preliminaries
Part 3: SIDH
SIDH: history

• **1999**: Couveignes gives talk “Hard homogenous spaces” ([eprint.iacr.org/2006/291](eprint.iacr.org/2006/291))

• **2006 (OIDH)**: Rostovsev and Stolbunov propose ordinary isogeny DH

• **2010 (OIDH break)**: Childs-Jao-Soukharev give quantum subexponential alg.

• **2011 (SIDH)**: Jao and De Feo fix by choosing supersingular curves

**Crucial difference**: supersingular (i.e., non-ordinary) endomorphism ring is not commutative (resists above attack)
WARNING

DO NOT BE DETERRED
BY THE WORD
SUPERSINGULAR
W. Castryck (GIF): “Elliptic curves are dead: long live elliptic curves”  
SIDH: in a nutshell

\[ E_0 \phi_A = E_A = E_0 / \langle A \rangle \]

\[ E_0 / \langle B \rangle = E_B \phi_A' \phi_B = E_{AB} = E_0 / \langle A, B \rangle \]

\( E_0 \)'s are isogenous curves
\( P \)'s, \( Q \)'s, \( R \)'s, \( S \)'s are points
SIDH: in a nutshell

\[ E_0 = \frac{E_0}{\langle P_A + [s_A]Q_A \rangle} \]
\[ (R_A, S_A) = (\phi_A(P_B), \phi_A(Q_B)) \]
\[ E_A = \frac{E_0}{\langle P_A + [s_A]Q_A \rangle} \]
\[ E_{AB} = \frac{E_0}{\langle A, B \rangle} \]

\[ E_0/\langle P_B + [s_B]Q_B \rangle = E_B \]
\[ (\phi_B(P_A), \phi_B(Q_A)) = (R_B, S_B) \]

**Key:** Alice sends her isogeny evaluated at Bob’s generators, and vice versa

\[ E_A/\langle R_A + [s_B]S_A \rangle \cong E_0/\langle P_A + [s_A]Q_A, P_B + [s_B]Q_B \rangle \cong E_B/\langle R_B + [s_A]S_B \rangle \]

**params** public private

\( E \)'s are isogenous curves
\( P \)'s, \( Q \)'s, \( R \)'s, \( S \)'s are points
• Why $E' = E/\langle P + [s]Q \rangle$, etc?

• Why not just $E' = E/\langle [s]Q \rangle$?...
because here $E'$ is $\approx$ independent of $s$

• Need two-dimensional basis to span two-dimensional torsion

• Every different $s$ now gives a different order $n$ subgroup, i.e., kernel, i.e. isogeny

• Composite same thing, just uglier picture

\[ E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n \]

($n$ prime depicted below)

$n + 1$ cyclic subgroups order $n$
• Why $E' = E/\langle P + [s]Q \rangle$, etc?

• Why not just $E' = E/\langle [s]Q \rangle$?...
because here $E'$ is $\approx$ independent of $s$

• Need two-dimensional basis to span two-dimensional torsion

• Every different $s$ now gives a different order $n$ subgroup, i.e., kernel, i.e. isogeny

• Composite same thing, just uglier picture
• Why $E' = E / \langle P + [s]Q \rangle$, etc?

• Why not just $E' = E / \langle [s]Q \rangle$?... because here $E'$ is $\approx$ independent of $s$

• Need two-dimensional basis to span two-dimensional torsion

• Every different $s$ now gives a different order $n$ subgroup, i.e., kernel, i.e. isogeny

• Composite same thing, just uglier picture

$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$

($n$ prime depicted below)

$n + 1$ cyclic subgroups order $n$
• Why \( E' = E / \langle P + [s]Q \rangle \), etc?

• Why not just \( E' = E / \langle [s]Q \rangle \) ?... because here \( E' \) is \( \approx \) independent of \( s \)

• Need two-dimensional basis to span two-dimensional torsion

• Every different \( s \) now gives a different order \( n \) subgroup, i.e., kernel, i.e. isogeny

• Composite same thing, just uglier picture

\[ E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n \]

\((n \text{ prime depicted below})\)

\(n + 1\) cyclic subgroups order \( n \)
Exploiting smooth degree isogenies

• Computing isogenies of prime degree $\ell$ at least $O(\ell)$, e.g., Velu’s formulas need the whole kernel specified

• We (obviously) need exp. set of kernels, meaning exp. sized isogenies, which we can’t compute unless they’re smooth

• Here (for efficiency/ease) we will only use isogenies of degree $\ell^e$ for $\ell \in \{2,3\}$
Exploiting smooth degree isogenies

• Suppose our secret point $R_0$ has order $\ell^5$ with, e.g., $\ell \in \{2,3\}$, we need $\phi : E \rightarrow E/\langle R_0 \rangle$

• Could compute all $\ell^5$ elements in kernel (but only because exp is 5)

• Better to factor $\phi = \phi_4 \phi_3 \phi_2 \phi_1 \phi_0$, where all $\phi_i$ have degree $\ell$, and

\[
\phi_0 = E_0 \rightarrow E_0/\langle [\ell^4]R_0 \rangle, \quad R_1 = \phi_0(R_0);
\]
\[
\phi_1 = E_1 \rightarrow E_1/\langle [\ell^3]R_1 \rangle, \quad R_2 = \phi_1(R_1);
\]
\[
\phi_2 = E_2 \rightarrow E_2/\langle [\ell^2]R_2 \rangle, \quad R_3 = \phi_2(R_2);
\]
\[
\phi_3 = E_3 \rightarrow E_3/\langle [\ell^1]R_3 \rangle, \quad R_4 = \phi_3(R_3);
\]
\[
\phi_4 = E_4 \rightarrow E_4/\langle R_4 \rangle.
\]

(credit DJP'14 for picture, and for a much better way to traverse the tree)
SIDH: security

• **Setting:** supersingular elliptic curves $E / \mathbb{F}_p^2$ where $p$ is a large prime

• **Hard problem:** Given $P, Q \in E$ and $\phi(P), \phi(Q) \in \phi(E)$, compute $\phi$ (where $\phi$ has fixed, smooth, public degree)

• **Best (known) attacks:** classical $O(p^{1/4})$ and quantum $O(p^{1/6})$

• **Confidence:** above complexities are optimal for (above generic) claw attack
(Our) parameters

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

\( p \approx 2^{768} \) gives \( \approx 192 \) bits classical and \( 128 \) bits quantum security against best known attacks.

\[ E_0 / \mathbb{F}_{p^2} : y^2 = x^3 + x \]

\[ \#E_0 = (p + 1)^2 = (2^{372} \cdot 3^{239})^2 \]

\( P_A, P_B \in E_0(\mathbb{F}_p), Q_A = \tau(P_A), Q_B = \tau(P_B) \)

\( S_A, S_B \in \mathbb{Z} \)

\[ \text{PK} = [x(P), x(Q), x(Q - P)] \in (\mathbb{F}_{p^2})^3 \]

\( j(E_{AB}) \in \mathbb{F}_{p^2} \)

- params: 564 bytes
- public: 376 bytes
- private: 188 bytes

- 48 bytes
Point and isogeny arithmetic in $\mathbb{P}^1$

ECDH: move around different points on a fixed curve.
SIDH: move around different points and different curves

\[ E_{a,b} : \quad by^2 = x^3 + ax^2 + x \]

\[(x, y) \leftrightarrow (X : Y : Z) \quad \quad (a, b) \leftrightarrow (A : B : C) \]

\[ E_{(A:B:C)} : \quad BY^2Z = CX^3 + AX^2Z + CXZ^2 \]

$\mathbb{P}^1$ point arithmetic (Montgomery): \((X : Z) \leftrightarrow (X' : Z')\)

$\mathbb{P}^1$ isogeny arithmetic (this work): \((A : C) \leftrightarrow (A' : C')\)

The Montgomery $B$ coefficient only fixes the quadratic twist. Can ignore it in SIDH since $j(E) = j(E')$
Performance

<table>
<thead>
<tr>
<th>comparison</th>
<th>uncompressed</th>
<th>compressed</th>
<th>uncompressed</th>
<th>compressed</th>
<th>uncompressed</th>
<th>compressed</th>
<th>uncompressed</th>
<th>compressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>public key size (bytes)</td>
<td>564</td>
<td>330</td>
<td>768</td>
<td>385</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>uncompressed speed (cc x 10^6)</td>
<td>Alice total</td>
<td>90</td>
<td>267</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>compressed speed (cc x 10^6)</td>
<td>Bob total</td>
<td>102</td>
<td>274</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alice total</td>
<td>239</td>
<td>263</td>
<td>6887</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob total</td>
<td>8514</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(see papers for references and benchmarking details)
## SIDH vs. lattice “DH” primitives

<table>
<thead>
<tr>
<th>Name</th>
<th>Primitive</th>
<th>Full DH (ms)</th>
<th>PK size (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frodo</td>
<td>LWE</td>
<td>2.600</td>
<td>11,300</td>
</tr>
<tr>
<td>NewHope</td>
<td>R-LWE</td>
<td>0.310</td>
<td>1,792</td>
</tr>
<tr>
<td>NTRU</td>
<td>NTRU</td>
<td>2.429</td>
<td>1,024</td>
</tr>
<tr>
<td>SIDH</td>
<td>Supersingular Isogeny</td>
<td>900</td>
<td>564</td>
</tr>
</tbody>
</table>

*Table*: ms for full DH round (Alice + Bob) on 2.6GHz Intel Xeon i5 (Sandy Bridge). See “Frodo” for benchmarking details.

All numbers above are for plain C implementations (e.g., SIDH w. assembly optimizations is 56ms)
## Compressed SIDH vs. lattice “DH” primitives

<table>
<thead>
<tr>
<th>Name</th>
<th>Primitive</th>
<th>Full DH (ms)</th>
<th>PK size (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frodo</td>
<td>LWE</td>
<td>2.600</td>
<td>11,300</td>
</tr>
<tr>
<td>NewHope</td>
<td>R-LWE</td>
<td>0.310</td>
<td>1,792</td>
</tr>
<tr>
<td>NTRU</td>
<td>NTRU</td>
<td>2.429</td>
<td>1,024</td>
</tr>
<tr>
<td>SIDH</td>
<td>Supersingular Isogeny</td>
<td>$\approx 2390$</td>
<td>330</td>
</tr>
</tbody>
</table>

Compressed SIDH roughly 2-3 slower than uncompressed SIDH.
Further topics and recent work...
Validating public keys

• Issues regarding public key validation: Asiacrypt2016 paper by Galbraith-Petit-Shani-Ti

• NSA countermeasure: “Failure is not an option: standardization issues for PQ key agreement”

• Thus, library currently supports ephemeral DH only

• But all PQ key establishment (codes, lattice) suffer from this
BigMont: a strong SIDH+ECDH hybrid

- No clear frontrunner for PQ key exchange
- Hybrid particularly good idea for (relatively young) SIDH
- Hybrid particularly easy for SIDH

There are exponentially many $A$ such that $E_A / \mathbb{F}_{p^2}: y^2 = x^3 + Ax^2 + x$ is in the supersingular isogeny class. These are all unsuitable for ECDH.

There are also exponentially many $A$ such that $E_A / \mathbb{F}_{p^2}: y^2 = x^3 + Ax^2 + x$ is suitable for ECDH, e.g. $A = 624450$. 
### SIDH vs. SIDH+ECDH hybrid

<table>
<thead>
<tr>
<th>comparison</th>
<th>SIDH</th>
<th>SIDH+ECDH</th>
</tr>
</thead>
<tbody>
<tr>
<td>bit security (hard problem)</td>
<td>classical</td>
<td>192 (SSDDH)</td>
</tr>
<tr>
<td></td>
<td>quantum</td>
<td>128 (SSDDH)</td>
</tr>
<tr>
<td>public key size (bytes)</td>
<td></td>
<td>564</td>
</tr>
<tr>
<td>Speed (cc x 10^6)</td>
<td></td>
<td>46</td>
</tr>
<tr>
<td>Alice key gen.</td>
<td>52</td>
<td>58</td>
</tr>
<tr>
<td>Bob key gen.</td>
<td>44</td>
<td>50</td>
</tr>
<tr>
<td>Alice shared sec.</td>
<td>50</td>
<td>57</td>
</tr>
<tr>
<td>Bob shared sec.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Colossal amount of classical security almost-for-free (≈ no more code)
Simple, compact, (relatively) efficient isogenies of arbitrary degree

C-Hisil: For odd order $\ell = 2d + 1$ point $P$ on Montgomery curve $E$, map

$\phi : E \to E', \quad (x, y) \mapsto (\phi_x(x), y \cdot \phi'_x(x))$

with

$\phi_x(x) = x \cdot \prod_{1 \leq i \leq d} \left( \frac{x \cdot x[i]P - 1}{x - x[i]P} \right)^2$

is $\ell$-isogeny with $\ker(\phi) = \langle P \rangle$, and moreover, $E'$ is Montgomery curve.
Arbitrary degree isogenies

Need not have \( p = 2^i3^j - 1 \), can easily implement

\[
p = \left( \prod q_i^{m_i} \right) \cdot \left( \prod r_j^{n_j} \right) - 1
\]

with \( \gcd(\prod q_i, \prod r_j) = 1 \)
Questions?