Supersingular Curves in Cryptography

Final Oral Defense

Gaurish Korpal

University of Arizona

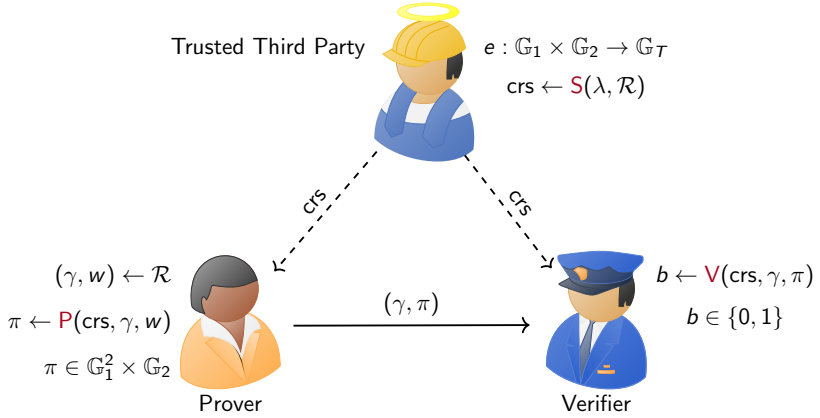
July 21, 2025

Outline

1. SNARK
   - ¬(unkind criticism)
   - Coda/Mina
   - superMNT cycle
2. NIKE
   - ¬(Greek goddess)
   - ['si:saɪd]
   - Gross lattice
3. Sigma
   - ¬(Internet slang)
   - SQIsign
   - Degree map

Succinct Non-interactive ARguments of Knowledge

A triple of probabilistic polynomial-time algorithms $(\mathsf{S}, \mathsf{P}, \mathsf{V})$ such that

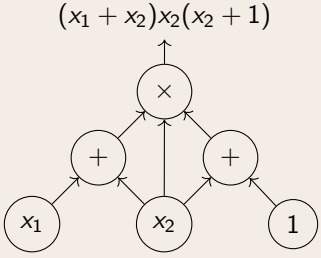


Pairing-friendly elliptic curve

1. E be an elliptic curve defined over $\mathbb{F}_p$.
2. $q \mid \#E(\mathbb{F}_p)$ and $k = \mathrm{ord}_q(p) < 50$.
3. $\mathbb{G}_1$ is an order q subgroup of $E(\mathbb{F}_p)$.
4. $\mathbb{G}_2$ is an order q subgroup of $E\left(\mathbb{F}_{p^k}\right)$.
5. $\mathbb{G}_T$ is an order q subgroup of $\mathbb{F}_{p^k}^{\times}$
6. $e([a]G_1, [b]G_2) = e(G_1, [b]G_2)^a = e([a]G_1, G_2)^b = e(G_1, G_2)^{ab} = G_T^{ab}$ with $a, b \in \mathbb{F}_q$.
7. DLP has subexponential attacks using Number Field Sieve methods.

SNARK primes

1. Prover works with $\mathbb{F}_q$-arithmetic circuits that are directed trees.



2. Verifier uses pairing and performs arithmetic in characteristic p.

Outline

1. SNARK
   - ¬(unkind criticism)
   - Coda/Mina
   - superMNT cycle
2. NIKE
   - ¬(Greek goddess)
   - ['siːsaɪd]
   - Gross lattice
3. Sigma
   - ¬(Internet slang)
   - SQIsign
   - Degree map

Unbounded recursion

- SNARKs offer fast verification, but proof generation is computationally expensive.
- Can achieve scalability via recursive proof composition: A single proof inductively attests to the correctness of a former proof or many former proofs.

Anomalous curves

Select an elliptic curve $E/\mathbb{F}_p$ with $p = \#E(\mathbb{F}_p)$. But then $k = \mathrm{ord}_p(p) = \perp$.
Furthermore, ECDLP can be solved in linear time using p-adic elliptic logarithm.

Find $E/\mathbb{F}_p$ and $\hat{E}/\mathbb{F}_q$ such that $\#E(\mathbb{F}_p) = q$ and $\#\hat{E}(\mathbb{F}_q) = p$. Here the equality is forced by Hasse interval and large primes.

Miyaji-Nakabayashi-Takano (MNT) cycle

MNT4: $E/\mathbb{F}_p$

$$p = \Phi_6(x) = x^2 - x + 1$$
$$q = \#E(\mathbb{F}_p) = \Phi_4(x) = x^2 + 1$$
$$k = \mathrm{ord}_{\Phi_4(x)}(\Phi_6(x)) = 4$$

MNT6: $\hat{E}/\mathbb{F}_q$

$$q = \Phi_4(x) = x^2 + 1$$
$$p = \#\hat{E}(\mathbb{F}_q) = \Phi_6(x) = x^2 - x + 1$$
$$k = \mathrm{ord}_{\Phi_6(x)}(\phi_4(x)) = 6$$

MNT4: $t_E = p + 1 - \#E(\mathbb{F}_p)$

1. p split into principal prime ideals in $\mathbb{Q}(\sqrt{-D})$: $4p = t_E^2 + DV^2$.
   - $DV^2 = 4p - (p + 1 - q)^2 = 3x^2 - 2x + 3$.
   - $U^2 - 3DV^2 = -8$ for $U = 3x - 1 \equiv 2 \pmod 3$.
   - Cycle through square-free $D < 10^{17}$ until we get x such that both p and q are primes.
2. Find a root of Hilbert class polynomial over $\mathbb{F}_p$: $H_D(j) \equiv 0 \pmod p$.
3. $E(j)$ is an elliptic curve defined over $\mathbb{F}_p$ with $p + 1 - t_E$ points.

Coda: Decentralized Cryptocurrency at Scale

$$D = 3\times131\times844243925531 \approx 10^{14}$$

$$x = 2046912088193309620094698681046361327832696967900119774002238984624318101029356158913071\backslash$$
$$6673677668989176697544704001 \approx 2^{376}$$

$$p = 4189849096791895340234421479124063712817070991995394907178350292102535281257110677305881\backslash$$
$$9376379033892141807097188825378611435372652958438520159160572201312646893140434794984051\backslash$$
$$4300798632774346285372062805169214126530311472168960 1 \approx 2^{753}$$

$$q = p + x$$

$$j(E) = 2949462076710896107292006556722885522651295239349323509431958561516853294269800292472951\backslash$$
$$4123962854323908600399000655248910772104868514570467069442357680336126965283413837047871\backslash$$
$$6654571796083276109533005717517663229725643589192429 8$$

$$j(\hat{E}) = 1752688993105942289627252778165192832430615020864338534954581935099618839548074240949083\backslash$$
$$6585760146854734021886348585708886463391958067458747615100977960971681648566047245426593\backslash$$
$$7296210381428415361995874222695788889582889907085 38$$

Mina: Decentralized Cryptocurrency at Scale

- E and $\hat{E}$ have too small embedding degrees 4 and 6, need to secure both of the ECDLP's in $E(\mathbb{F}_p)$ and $\hat{E}(\mathbb{F}_q)$ and both of the DLP's in $\mathbb{F}^{\times}_{p^4}$ and $\mathbb{F}^{\times}_{q^6}$.
- The 753-bits MNT cycle offers only 112-bit security as per the T-NFS attack estimates for $\#\mathbb{F}^{\times}_{p^4} \approx 2^{3012}$. Leading to highly inefficient arithmetic circuits.

On Cycles of Pairing-Friendly Elliptic Curves*

Alessandro Chiesa†, Lynn Chua†, and Matthew Weidner‡

On cycles of pairing-friendly abelian varieties

Maria Corte-Real Santos[1*], Craig Costello[2], and Michael Naehrig[2]

Abstract. One of the most promising avenues for realising scalable proof systems relies on the existence of 2-cycles of pairing-friendly elliptic curves. Such a cycle consists of two elliptic curves $\mathcal{E}/\mathbb{F}_p$ and $\mathcal{E}'/\mathbb{F}_q$ that both have a low embedding degree and also satisfy $q = \#\mathcal{E}(\mathbb{F}_p)$ and $p = \#\mathcal{E}'(\mathbb{F}_q)$. These constraints turn out to be rather restrictive; in the decade that has passed since 2-cycles were first proposed for use in proof systems, no new constructions of 2-cycles have been found.

In this paper, we generalise the notion of cycles of pairing-friendly elliptic curves to study cycles of pairing-friendly *abelian varieties*, with a view towards realising more efficient pairing-based SNARKs. We show that considering abelian varieties of dimension larger than 1 unlocks a number of interesting possibilities for finding pairing-friendly cycles, and we give several new constructions that can be instantiated at any security level.

Revisiting cycles of pairing-friendly elliptic curves

Marta Bellés–Muñoz[1,2], Jorge Jiménez Urroz[3,4], Javier Silva[1]

stract. A recent area of interest in cryptography is recursive composition of
of systems. One of the approaches to make recursive composition efficient in-
ves cycles of pairing-friendly elliptic curves of prime order. However, known
structions have very low embedding degrees. This entails large parameter sizes,
ch makes the overall system inefficient. In this paper, we explore 2-cycles com-
ed of curves from families parameterized by polynomials, and show that such
les do not exist unless a strong condition holds. As a consequence, we prove
t no 2-cycles can arise from the known families, except for those cycles already
wn. Additionally, we show some general properties about cycles, and provide
tailed computation on the density of pairing-friendly cycles among all cycles.

Outline

1. SNARK
   - ¬(unkind criticism)
   - Coda/Mina
   - superMNT cycle
2. NIKE
   - ¬(Greek goddess)
   - ['siːsaɪd]
   - Gross lattice
3. Sigma
   - ¬(Internet slang)
   - SQIsign
   - Degree map

Coda+Decrypt SNARK challenge (2019)

USD 20,000

Construct a chain of pairing-friendly curves that eventually leads into the 753-bits MNT cycle, but one for which the prime order subgroup size of the first pairing-friendly curve in the chain is closer to 224-bits, ideal case for 112-bit security.

here $p_i = \#E_{i+1}(\mathbb{F}_{p_{i+1}})$ and $\mathrm{ord}_{p_i}(p_{i+1}) = k < 50$.

Supersingular curves

- $E/\mathbb{F}_{p^n}$ with $t = p^n + 1 - \#E(\mathbb{F}_{p^n})$ and $|t| \leq 2p^{n/2}$ is supersingular if $p \mid t$.
- Supersingular curves have $\mathrm{ord}_q(p^n) \leq 6$ for any $q \mid \#E(\mathbb{F}_{p^n})$.
- The CM method used for MNT curves does not produce supersingular curves.

Bröker's algorithm

CM theory offers a simpler method for constructing supersingular curve $\mathcal{E}/\mathbb{F}_{p^n}$ with trace t:

1. Find the smallest prime $\mathcal{D} \equiv 3 \pmod 4$ such that $-\mathcal{D}$ is not a quadratic residue mod p.
2. Find a root of Hilbert class polynomial over $\mathbb{F}_p$: $H_{\mathcal{D}}(j) \equiv 0 \pmod p$.
3. $\mathcal{E}' : y^2 = x^3 + ax - a$ with $a = \frac{27j}{4(1728-j)}$ is a supersingular elliptic curve over $\mathbb{F}_p$.
4. $\mathcal{E}/\mathbb{F}_{p^n}$ is a twist of the base change of $\mathcal{E}'$ to $\mathbb{F}_{p^n}$.

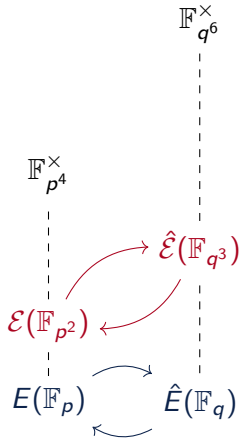
Supersingular cycle - Type 1

Costello and Korpal

Let $x \in \{6 + 12\mathbb{Z}, 10 + 12\mathbb{Z}\}$ be such that $p = x^2 - x + 1$ and $q = x^2 + 1$ are prime. Then there exist two supersingular curves $\mathcal{E}/\mathbb{F}_{p^2}$ and $\hat{\mathcal{E}}/\mathbb{F}_{q^3}$ such that

1. $\#\mathcal{E}(\mathbb{F}_{p^2}) = \Phi_4(p)$ and divisible by q.
2. $\#\hat{\mathcal{E}}(\mathbb{F}_{q^3}) = (q+1)\Phi_6(q)$ and divisible by p.
3. $\mathrm{ord}_q\left(p^2\right) = 2$
4. $\mathrm{ord}_p\left(q^3\right) = 2$

$\mathrm{ord}_p(a) = k \Longleftrightarrow p \mid \Phi_k(a)$.



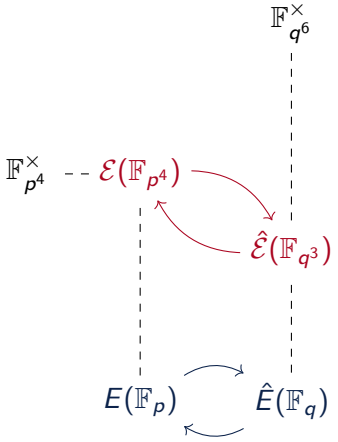
Supersingular cycle - Type 2

Costello and Korpal

Let $x \in \{12\mathbb{Z}, 4 + 12\mathbb{Z}\}$ be such that $p = x^2 - x + 1$ and $q = x^2 + 1$ are prime. Then there exist two supersingular curves $\mathcal{E}/\mathbb{F}_{p^4}$ and $\hat{\mathcal{E}}/\mathbb{F}_{q^3}$ such that

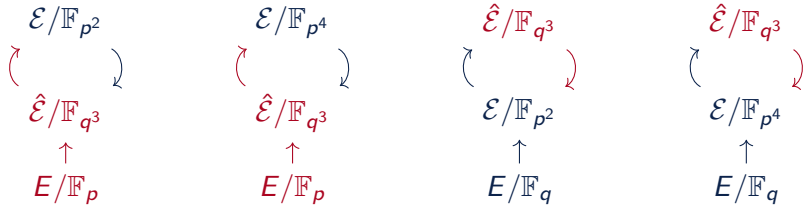
1. $\#\mathcal{E}(\mathbb{F}_{p^4}) = (\Phi_4(p))^2$ and divisible by q.
2. $\#\hat{\mathcal{E}}(\mathbb{F}_{q^3}) = (q+1)\Phi_6(q)$ and divisible by p.
3. $\mathrm{ord}_q\left(p^4\right) = 1$
4. $\mathrm{ord}_p\left(q^3\right) = 2$

$\mathrm{ord}_p(a) = k \Longleftrightarrow p \mid \Phi_k(a)$.

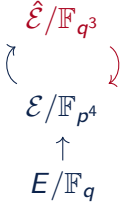


superMNT

- No known difference in the security picture of superMNT cycles and the underlying MNT cycles.
- superMNT cycles can be constructed for all values of x that give rise to p and q as primes.
- Lets us construct another pairing-friendly curve, $E/\mathbb{F}_p$ or $E/\mathbb{F}_q$, with prime $r \mid \#E$ such that the complexity of solving the ECDLP in $E[r]$ is much closer to the complexity of solving the DLP in $\mathbb{F}_{p^4}^{\times}$.



Lollipop-585-216 (near 112-bit security)



1. $\Phi_6(q) = (x^2 - x + 1)(x^2 + x + 1) = p \cdot \#E(\mathbb{F}_q)$ with $r \mid \#E(\mathbb{F}_q)$.
2. CM method: $DV^2 = 4q - t^2 = 4q - (q + 1 - \#E(\mathbb{F}_q))^2 = 3x^2 + 2x + 3$.
3. Continued fractions: $U^2 - 3DV^2 = -8$ for $U = 3x + 1 \equiv 1 \pmod 3$.
4. Bröker's algorithm: $x \equiv 0 \pmod{12}$ hence Type 2 cycle.

$D = 673 \times 1449611 \approx 10^9$

$x = 111243196646662532081433025245205554364586793578885562112631763747633323269724095686070 20$

$p = 123750488001680300225547143744210956825371951665359953718445722524055721280173789901068 38\backslash$
$46900137044533158636865121780449150388200579571278651418385190719188432037638936246733 81$

$r = 96334084882307579170484479523446531977849376800299152827628262599 \approx 2^{216}$ $j(\mathcal{E}) = p - 3375$

$j(E) = 23807584437682490848874255592611071730909184125151969774494440150001785649531223581229311\backslash$
$28399361874602073784104081098289325239146423438033575529643001178371305054930690866 2$

$j(\hat{\mathcal{E}}) = 11490741826213250474278490699650806704827331632754835779261059387196229669285244539270404\backslash$
$96893999029775989534773737821678166900136576248820202472962086637780450974103110303419 85$

$E[r]$ offers 107-bit ECDLP security.

$\mathbb{F}_{p^4}^{\times}$ offers 109-bit DLP security.

Outline

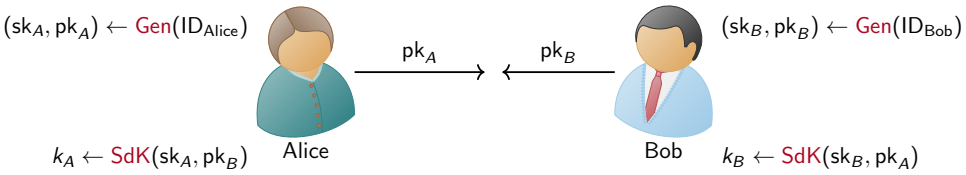
1 SNARK
¬(unkind criticism)
Coda/Mina
superMNT cycle

2 NIKE
¬(Greek goddess)
['siːsaɪd]
Gross lattice

3 Sigma
¬(Internet slang)
SQIsign
Degree map

Non-Interactive Key Exchange

A triple of probabilistic polynomial-time algorithms $(\mathsf{S}, \mathsf{Gen}, \mathsf{SdK})$ such that



here $k_A = k_B$ under the system parameters $\mathsf{S}(\lambda)$ for the security parameter λ.

Montgomery curve: Curve25519

1. Setup: $p = 2^{255} - 19$, $E_{486662} : y^2 = x^3 + 486662x^2 + x$, $G = (9, 43\ldots48)$, $\mathbb{G} = \langle G \rangle$ is a subgroup of co-factor 8.
2. Key-pair generation: $(\mathsf{sk}_A, \mathsf{pk}_A) = (a, [a]G)$ and $(\mathsf{sk}_B, \mathsf{pk}_B) = (b, [b]G)$
3. Shared key establishment: $k_A = [a]([b]G)$ and $k_B = [b]([a]G)$.

3-party NIKE

1. Setup: $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.
2. Key-pair generation: $(\mathsf{sk}_A, \mathsf{pk}_A) = (a, ([a]G_1, [a]G_2))$, $(\mathsf{sk}_B, \mathsf{pk}_B) = (b, ([b]G_1, [b]G_2))$, and $(\mathsf{sk}_C, \mathsf{pk}_C) = (c, ([c]G_1, [c]G_2))$
3. Shared key establishment: $k_A = e([b]G_1, [c]G_2)^a$, $k_B = e([a]G_1, [c]G_2)^b$, and $k_C = e([b]G_1, [a]G_2)^c$.

Outline

1 SNARK
¬(unkind criticism)
Coda/Mina
superMNT cycle

2 NIKE
¬(Greek goddess)
['siːsaɪd]
Gross lattice

3 Sigma
¬(Internet slang)
SQIsign
Degree map

Quantum-resistant key exchange

1. (EC)DLP can be solved in polynomial time on a quantum computer.
2. Post-quantum key encapsulation mechanisms (KEM)
   - Lattices: CRYSTALS-Kyber (ML-KEM), FrodoKEM
   - Error-correcting codes: HQC, BIKE, Classic McEliece
3. No NIKE standardized yet.
4. Need diversity.

Endomorphism ring

1. A non-constant rational map $\varphi : E \to E'$ between elliptic curves defined over $\mathbb{F}_{p^n}$ is called $\mathbb{F}_{p^n}$-isogeny; $\varphi(0_E) = 0_{E'}$ and $\varphi(E) = E'$.
2. $\mathrm{End}_{\mathbb{F}_{p^n}}(E)$ is the set of all $\mathbb{F}_{p^n}$-isogenies from E to itself and the zero map.
3. $\mathrm{End}_{\bar{\mathbb{F}}_p}(E)$ is isomorphic to either
   - an imaginary quadratic order $O := \mathbb{Z} + \mathbb{Z}\alpha$ with $\alpha \in \mathbb{Q}(\sqrt{-D}) = O \otimes_{\mathbb{Z}} \mathbb{Q}$ where D is a squarefree positive integer; or
   - a maximal quaternion order $\mathcal{O} := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$ with $\alpha_i \in \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ where $\mathbf{j}^2 = -p$ and $\mathbf{i}^2 = -q$ with $\left(\frac{p}{q}\right) = -1$ if $p \equiv 1 \pmod 4$ or $\mathbf{i}^2 = -1$ otherwise.
4. E is called supersingular if $\mathrm{End}_{\bar{\mathbb{F}}_p}(E) \cong \mathcal{O}$. Then $j(E) \in \mathbb{F}_{p^2}$.
   - $j(E) \in \mathbb{F}_p$ iff $\mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}$
   - If $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \hookrightarrow \mathcal{O}$ then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\frac{1+\mathbf{j}}{2} + \mathbb{Z}\frac{\mathbf{i}(r+\mathbf{j})}{2q}$ with $r^2 + p \equiv 0 \pmod{4q}$.
   - otherwise, $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$ and $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{1+\mathbf{i}}{2} + \mathbb{Z}\frac{(1+\mathbf{i})\mathbf{j}}{2} + \mathbb{Z}\frac{\mathbf{i}(s+\mathbf{j})}{q}$ with $s^2 + p \equiv 0 \pmod{q}$.

Commutative Supersingular Isogeny Diffie-Hellman

- $\mathrm{Ell}_p(O)$ be the set of supersingular curves with $\mathbb{Z}[\sqrt{-p}] \subseteq O \cong \mathrm{End}_{\mathbb{F}_p}(E)$.
- The ideal class group $\mathrm{cl}(O)$ acts freely and transitively on $\mathrm{Ell}_p(O)$ via the map

$$\mathrm{cl}(O) \times \mathrm{Ell}_p(O) \to \mathrm{Ell}_p(O)$$
$$([\mathfrak{a}], E) \mapsto [\mathfrak{a}]E$$

  where $[\mathfrak{a}]E$ is the co-domain of $\mathbb{F}_p$-isogeny $\varphi_{\mathfrak{a}} : E \to E/\mathfrak{a}$.
- Vectorization problem: There is subexponential quantum algorithm to find $\mathfrak{a}$ given E and $E' = [\mathfrak{a}]E$.

Let $O = \mathbb{Z}[\sqrt{-p}]$, $p \equiv 3 \pmod 8$ of the form $4 \cdot \ell_1 \cdots \ell_m - 1$.

1. $\mathrm{End}_{\mathbb{F}_p}(E) \cong O$ iff there exists a unique $A \in \mathbb{F}_p \setminus \{\pm 2\}$ so that E is $\mathbb{F}_p$-isomorphic to the curve $E_A : y^2 = x^3 + Ax^2 + x$.
2. For $j = 1728$, $E_0 : y^2 = x^3 + x$. For $A \neq 0$, if $E_A \in \mathrm{Ell}_p(O)$ then its quadratic twist is $E_{-A} \in \mathrm{Ell}_p(O)$
3. $[\mathfrak{a}] = [\mathfrak{l}_1^{a_1} \cdots \mathfrak{l}_m^{a_m}]$ where $\mathfrak{l}_i = \langle \ell_i, \sqrt{-p} - 1 \rangle$ allows efficient computation of group action as $\#E(\mathbb{F}_p) = p + 1$, where $[\mathfrak{a}]^{-1}E$ is the quadratic twist of $[\mathfrak{a}]E^t$.
4. $\#\mathrm{Ell}_p(O) = \#\mathrm{cl}(O) = h(-4p)$.

CSIDH-512 (128-bit security)

1. Setup: $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$ with

$$p = 4 \cdot (3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127 \cdot 131 \cdot 137 \cdot 139 \cdot 149 \cdot 151 \cdot 157 \cdot 163 \cdot 167 \cdot 173 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 197 \cdot 199 \cdot 211 \cdot 223 \cdot 227 \cdot 229 \cdot 233 \cdot 239 \cdot 241 \cdot 251 \cdot 257 \cdot 263 \cdot 269 \cdot 271 \cdot 277 \cdot 281 \cdot 283 \cdot 293 \cdot 307 \cdot 311 \cdot 313 \cdot 317 \cdot 331 \cdot 337 \cdot 347 \cdot 349 \cdot 353 \cdot 359 \cdot 367 \cdot 373 \cdot 587) - 1 \approx 2^{511}$$

$$\#\mathrm{cl}(\mathcal{O}) = 3 \cdot 37 \cdot 1407181 \cdot 51593604295295867744293584889 \cdot 31599414504681995853008278745587832204909 \approx 2^{257}$$

2. Key-pair generation: Sample 74-tuple from $\{-5, \ldots, 5\}$ because $10^{74} \approx \sqrt{p}$.
   - $(\mathsf{sk}_A, \mathsf{pk}_A) = ((a_1, \ldots, a_{74}), [\mathfrak{l}_1^{a_1} \cdots \mathfrak{l}_{74}^{a_{74}}]E_0)$ and $(\mathsf{sk}_B, \mathsf{pk}_B) = ((b_1, \ldots, b_{74}), [\mathfrak{l}_1^{b_1} \cdots \mathfrak{l}_{74}^{b_{74}}]E_0)$.
   - Publish the Montgomery coefficient.
3. Shared key establishment: $k_A = [\mathfrak{a}]([\mathfrak{b}]E_0)$ and $k_B = [\mathfrak{b}]([\mathfrak{a}]E_0)$, where $[\mathfrak{a}] = [\mathfrak{l}_1^{a_1} \cdots \mathfrak{l}_{74}^{a_{74}}]$ and $[\mathfrak{b}] = [\mathfrak{l}_1^{b_1} \cdots \mathfrak{l}_{74}^{b_{74}}]$.

128-bit security against the meet-in-the middle key search attack.

Outline

1 SNARK
¬(unkind criticism)
Coda/Mina
superMNT cycle

2 NIKE
¬(Greek goddess)
['siːsaɪd]
Gross lattice

3 Sigma
¬(Internet slang)
SQIsign
Degree map

CSIDH security reduction (2019)

- Public: E_0, E supersingular curves over $\mathbb{F}_p$ with $\mathrm{End}_{\mathbb{F}_p}(E_0) \cong \mathrm{End}_{\mathbb{F}_p}(E) \cong O$.
- Private: An invertible ideal $\mathfrak{a} \subseteq O$ such that $E = [\mathfrak{a}]E_0$.
- Attack: Recover $\mathfrak{a}$ in polynomial time if $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ are known.

Castryck, Panny and Vercauteren

1. Use the embedding $O \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$ (resp. $O \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$) to find invertible ideal $\mathfrak{b} \subseteq O$ such that $[\mathfrak{b}]E_0 = E_0^t$ (resp. $\mathfrak{c} \subseteq O$ such that $[\mathfrak{c}]E = E^t$).
2. Since $[\mathfrak{a}]E_0 = E \Longleftrightarrow [\mathfrak{a}]^{-1}E_0^t = E^t$, we have

$$[\mathfrak{a}]^{-1}E_0^t = [\mathfrak{a}]^{-1}[\mathfrak{b}]E_0$$
$$E^t = [\mathfrak{c}]E = [\mathfrak{c}][\mathfrak{a}]E_0$$

Therefore, $[\mathfrak{a}]$ is the square root of $[\mathfrak{b}][\mathfrak{c}]^{-1}$ in $\mathrm{cl}(O)$.

Quaternion algebra

1. Every isomorphism class of maximal order $\mathcal{O} \subset B_p$ corresponds to either one $j(E) \in \mathbb{F}_p$ or two $j(E), \overline{j(E)} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.
2. B_p is equipped with a standard involution $x \mapsto \overline{x}$ which we call conjugation of $x \in B_p$; we denote the reduced trace by $\mathrm{trd}(x) = x + \overline{x} \in \mathbb{Q}$ and the reduced norm by $\mathrm{nrd}(x) = x\overline{x} \in \mathbb{Q}$. If $\alpha \in \mathcal{O}$ then $\mathrm{trd}(\alpha) \in \mathbb{Z}$ and $\mathrm{nrd}(\alpha) \in \mathbb{Z}$.
3. The quaternion algebra B_p is equipped with an inner product $(x, y) = \frac{1}{2}\mathrm{trd}(x\overline{y})$. The norm associated to this inner product is the square root of the usual reduced norm because $\|x\|^2 = (x, x) = \frac{1}{2}\mathrm{trd}(x\overline{x}) = \mathrm{nrd}(x)$.
4. If $\mathcal{O} := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$ then $\mathcal{O}^T := \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \mathbb{Z}\beta_3$ where $\beta_i = 2\alpha_i - \mathrm{trd}(\alpha_i)$ is called Gross lattice of $\mathcal{O}$; $\det(\mathcal{O}^T) = 4p^2$.
5. Chevyrev and Galbraith (2013); Goren and Love (2023): The values of the successive minima δ_1, δ_2 and δ_3 of $\mathcal{O}^T$ determine the isomorphism class of a maximal order $\mathcal{O}$ in B_p.

Geometry of Gross lattice

Rank three lattice

Let $\beta_1, \beta_2, \beta_3$ be a successive minimal bases of a Gross lattice $\mathcal{O}^T$. Then the Gram matrix can be written in the form

$$G_{\mathcal{O}^T} = \begin{pmatrix} \delta_1 & \omega_{12} & \omega_{13} \\ \omega_{12} & \delta_2 & \omega_{23} \\ \omega_{13} & \omega_{23} & \delta_3 \end{pmatrix}$$

where $\omega_{ij} = \frac{1}{2}\mathrm{trd}(\beta_i\bar{\beta}_j)$, $\delta_i = \omega_{ii} = \mathrm{nrd}(\beta_i)$, $\delta_1 \leq 2p^{2/3}$, $0 \leq \omega_{12}, \omega_{13} \leq \frac{\delta_1}{2}$ and $|\omega_{23}| \leq \frac{\delta_2}{2}$.

Rank two lattice

1. Kaneko, 1989: Every rank-2 sublattice of $\mathcal{O}^T$ has determinant $4np$ for some positive integer n.
2. $j(E) \in \mathbb{F}_p$ iff its Gross lattice $\mathcal{O}^T$ has a rank-2 sublattice of determinant $4p$.
3. $j(E) \in \mathbb{F}_p$ iff the rank-2 sublattice $\Lambda_{12} = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2$ of $\mathcal{O}^T$ has determinant $4p$.

The third successive minimum - I

He, Korpal, Tran, and Vincent

E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$. $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ iff $\delta_3 \leq \frac{3}{5}p + 5$.

$\max_{x \in [\sqrt{a}, b]} \left\{ x + \frac{a}{x} \right\} = b + \frac{a}{b}$ for different cases like $a = 8p, b = \frac{2}{5}p$ for $p \geq 51$.

$p \equiv 13 \pmod{20}$

There exists a supersingular elliptic curve E with $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, such that

$$G_{\mathcal{O}^T} = \begin{pmatrix} 20 & 6 & 2 \\ 6 & \frac{2p+9}{5} & -\left(\frac{p-3}{5}\right) \\ 2 & -\left(\frac{p-3}{5}\right) & \frac{3p+1}{5} \end{pmatrix}$$

$p \equiv 17 \pmod{20}$

There exists a supersingular elliptic curve E with $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, such that

$$G_{\mathcal{O}^T} = \begin{pmatrix} 20 & 2 & 4 \\ 2 & \frac{2p+1}{5} & -\left(\frac{p-2}{5}\right) \\ 4 & -\left(\frac{p-2}{5}\right) & \frac{3p+4}{5} \end{pmatrix}$$

The third successive minimum - II

He, Korpal, Tran, and Vincent

E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$.

1. If $j(E) \in \mathbb{F}_p$ then $G_{\mathcal{O}^T}$ is independent of successive minimal bases; and $\delta_1 \neq \delta_2$.
2. $j(E) = 0 \Longleftrightarrow \delta_2 = \delta_3 = \frac{4p+1}{3}$. Otherwise, $\delta_2 \neq \delta_3$.
3. $j(E) = 1728 \Longleftrightarrow \delta_2 = p \Longleftrightarrow \delta_3 = p+1$.
4. $j(E) \in \mathbb{F}_p \setminus \{0\}$ iff $p \leq \delta_3 \leq \frac{8}{7}p + \frac{7}{4}$.

$p \equiv 3 \mod 7, j = -15^3$

$$G_{\mathcal{O}^T} = \begin{pmatrix} 7 & 3 & 2 \\ 3 & \frac{4p+9}{7} & -\left(\frac{2p-6}{7}\right) \\ 2 & -\left(\frac{2p-6}{7}\right) & \frac{8p+4}{7} \end{pmatrix}$$

$p \equiv 5 \mod 7, j = -15^3$

$$G_{\mathcal{O}^T} = \begin{pmatrix} 7 & 1 & 3 \\ 1 & \frac{4p+1}{7} & -\left(\frac{2p-3}{7}\right) \\ 3 & -\left(\frac{2p-3}{7}\right) & \frac{8p+9}{7} \end{pmatrix}$$

$p \equiv 6 \mod 7, j = -15^3$

$$G_{\mathcal{O}^T} = \begin{pmatrix} 7 & 2 & 1 \\ 2 & \frac{4(p+1)}{7} & \frac{2(p+1)}{7} \\ 1 & \frac{2(p+1)}{7} & \frac{8p+1}{7} \end{pmatrix}$$

Gram matrix types conjecture

E be a supersingular elliptic curve with $j(E) \in \mathbb{F}_p$ then $\delta_1 \leq \frac{4}{\sqrt{3}}\sqrt{p}$. $\mathrm{End}_{\mathbb{F}_p}(E) \cong O$.

$\delta_1 \equiv 0 \pmod 4$

1. $O = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $j(E) \neq 1728$

   then $G_{\mathcal{O}^T} = \begin{pmatrix} \delta_1 & \omega_{12} & 0 \\ \omega_{12} & \frac{4p+\omega_{12}^2}{\delta_1} & 0 \\ 0 & 0 & p \end{pmatrix}$, ω_{12} even.

2. $O = \mathbb{Z}[\sqrt{-p}]$ then

   $G_{\mathcal{O}^T} = \begin{pmatrix} \delta_1 & \omega_{12} & \frac{\delta_1}{2} \\ \omega_{12} & \frac{4p+\omega_{12}^2}{\delta_1} & \frac{\omega_{12}}{2} \\ \frac{\delta_1}{2} & \frac{\omega_{12}}{2} & p+\frac{\delta_1}{4} \end{pmatrix}$, ω_{12} even.

   If $j(E) = 1728$ then $\delta_1 = 4, \omega_{12} = 0$.

$\det(\Lambda_{13}) = \left\lceil \frac{\delta_1}{4} \right\rceil 4p$ and $\det(\Lambda_{23}) = \left\lceil \frac{\delta_2}{4} \right\rceil 4p$.

$\delta_1 \equiv 3 \pmod 4$

3. $O = \mathbb{Z}[\sqrt{-p}]$ and ω_{12} even, then

   $G_{\mathcal{O}^T} = \begin{pmatrix} \delta_1 & \omega_{12} & \frac{\omega_{12}}{2} \\ \omega_{12} & \frac{4p+\omega_{12}^2}{\delta_1} & \frac{4p+\omega_{12}^2}{2\delta_1} \\ \frac{\omega_{12}}{2} & \frac{4p+\omega_{12}^2}{2\delta_1} & \frac{4p(\delta_1+1)+\omega_{12}^2}{4\delta_1} \end{pmatrix}$

4. $O = \mathbb{Z}[\sqrt{-p}]$ and ω_{12} odd, $G_{\mathcal{O}^T} =$

$$\begin{pmatrix} \delta_1 & \omega_{12} & \frac{\delta_1-\omega_{12}}{2} \\ \omega_{12} & \frac{4p+\omega_{12}^2}{\delta_1} & -\left(\frac{4p-(\delta_1-\omega_{12})\omega_{12}}{2\delta_1}\right) \\ \frac{\delta_1-\omega_{12}}{2} & -\left(\frac{4p-(\delta_1-\omega_{12})\omega_{12}}{2\delta_1}\right) & \frac{4p(\delta_1+1)+(\delta_1-\omega_{12})^2}{4\delta_1} \end{pmatrix}$$

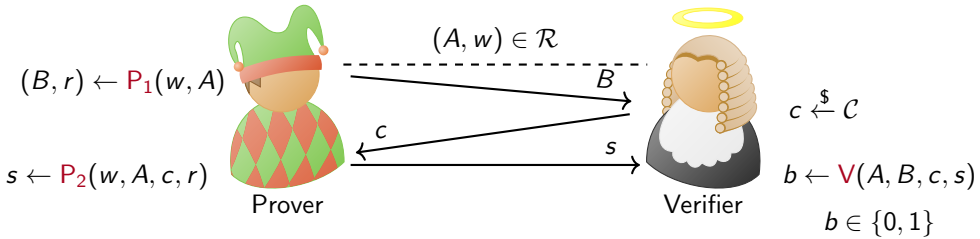
If $j(E) = 0$ then $\delta_1 = 3, \omega_{12} = 1$.

Outline

1. SNARK
   - ¬(unkind criticism)
   - Coda/Mina
   - superMNT cycle
2. NIKE
   - ¬(Greek goddess)
   - ['siːsaɪd]
   - Gross lattice
3. Sigma
   - ¬(Internet slang)
   - SQIsign
   - Degree map

Zigzag Marlin-Arthur

A triple of probabilistic polynomial time algorithms $(\mathsf{P}_1, \mathsf{P}_2, \mathsf{V})$ such that



EdDSA (128-bit security)

$E : -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$ over $\mathbb{F}_p$ with $p = 2^{255} - 19$ and $\#\mathbb{G} = q = \#E(\mathbb{F}_p)/2^3$.
We prove knowledge of w such that $A = [w]G$.

1. Commitment: Choose a random $r \in \mathbb{Z}/q\mathbb{Z}$, and send $B = [r]G$.
2. Challenge: The verifier replies with $c \in \mathbb{Z}/q\mathbb{Z}$.
3. Response: We respond with $s = r + cw \pmod{q}$.

Our knowledge of w can be verified by checking that $[s]G = B + [c]A$.

Fiat-Shamir transformation

1. Choose a random oracle cryptographic hash function H with appropriate domain and co-domain.
2. Make Σ-protocol non-interactive by replacing the verifier with the hash function.
3. A popular approach for constructing signature schemes from identification protocols.
4. We can attach signature s to a message m by using $c = \mathrm{H}(m||B)$.

Outline

1 SNARK
¬(unkind criticism)
Coda/Mina
superMNT cycle

2 NIKE
¬(Greek goddess)
['siːsaɪd]
Gross lattice

3 Sigma
¬(Internet slang)
SQIsign
Degree map

Quantum-resistant digital signature

1. (EC)DLP can be solved in polynomial time on a quantum computer.
2. Post-quantum signature schemes
   - Lattices: CRYSTALS-Dilithium (ML-DSA), Falcon (FN-DSA)
   - Cryptographic hash functions: SPHINCS+ (SLH-DSA), LMS, XMSS
3. Ongoing NIST selection round for additional digital signature schemes.
4. Need diversity.

Supersingular isogeny

1. $\mathrm{Hom}_{\mathbb{F}_{p^n}}(E, E')$ is the set of all $\mathbb{F}_{p^n}$-isogenies and zero-map from E to E'.
2. If $\#E(\mathbb{F}_{p^n}) = \#E'(\mathbb{F}_{p^n})$ then there exists an $\mathbb{F}_{p^n}$-isogeny $\varphi : E \to E'$.
3. Let E, E' be supersingular elliptic curves over $\overline{\mathbb{F}}_p$.
   - There exists an isogeny $\varphi : E \to E'$.
   - φ corresponds to $I_\varphi = \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E', E) \circ \varphi \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$, that is a left ideal in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$, and a right ideal in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E')$.
   - Left ideal $I \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ with norm coprime to p, corresponds to the (separable) supersingular isogeny $\varphi_I : E \to E/E[I]$ where $E[I] = \cap_{\alpha \in I} \ker \alpha$.
   - Given $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$, can efficiently translate between isogenies and ideals.
   - Given $\mathcal{O}, \mathcal{O}' \subseteq B_p$, we can efficiently find a connecting ideal I.
4. φ is said to be a cyclic isogeny if $\ker(\varphi)$ is a cyclic group. If supersingular curves, then I_φ is said to be primitive because $I_\varphi \not\subset q \cdot \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ for any prime q.

Computations

Consider supersingular curves over $\mathbb{F}_{p^2}$.

Very hard

1. Given E and E', construct an isogeny $\varphi : E \to E'$.
2. Given E, E', and d, find a degree d isogeny $\varphi : E \to E'$ if it exists.
3. Given E compute $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$.
4. Given E, find one non-scalar endomorphism.

Not so hard

1. Given E and $\mathbb{G} \subseteq E(\mathbb{F}_{p^2})$ with $\#\mathbb{G}$ smooth, compute $\varphi : E \to E/\mathbb{G}$.
2. Given $\varphi : E \to E'$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$, compute $\mathrm{End}_{\overline{\mathbb{F}}_p}(E')$.
3. Given $E, E', \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E')$, find an isogeny $\varphi : E \to E'$.
4. Given $\mathcal{O} \subseteq B_p$, find E so $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \cong \mathcal{O}$.

Short Quaternion and Isogeny Signature (2020)

We prove knowledge of d_{sk}-isogeny $\varphi_{\mathsf{sk}} : E_0 \to E_{\mathsf{pk}}$, where $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$.

1. Commitment: A d_{com}-isogeny φ_{com} from E_0, and send $E_{\mathsf{com}} = \varphi_{\mathsf{com}}(E_0)$.
2. Challenge: A cyclic d_{chl}-isogeny $\varphi_{\mathsf{chl}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$.
3. Response: A d_{rsp}-isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{pk}} \to E_{\mathsf{chl}}$ such that $\hat{\varphi}_{\mathsf{chl}} \circ \varphi_{\mathsf{rsp}}$ is cyclic.

SQIsign-256 (128-bit security)

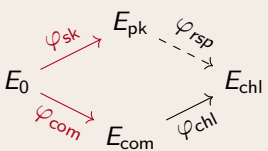
$$p = 23920667128620486487914848107166358953830561597426178123910317653495243603967 \approx 2^{254}$$

$$d_{\mathsf{sk}} = 43240197307742040547 \equiv 3 \mod 4 \approx p^{1/4}$$

$$d_{\mathsf{com}} = 7^4 \cdot 11 \cdot 13 \cdot 23^2 \cdot 37 \cdot 59^2 \cdot 89 \cdot 97 \cdot 101^2 \cdot 107 \cdot 109^2 \cdot 131 \cdot 137 \cdot 197^2 \cdot 223 \cdot 239 \cdot 383 \cdot 389 \cdot 491^2 \cdot 499 \cdot 607 \cdot 743^2 \cdot 1033 \cdot 1049 \cdot 1193 \cdot 1913^2 \cdot 1973 \approx 2^{272} \approx p; \quad 3^{36} \cdot d_{\mathsf{com}} \mid (p^2 - 1)$$

$$d_{\mathsf{chl}} = 2^{75}3^{36} \approx 2^{132} \approx p^{1/2}; \quad 2^{75} \mid (p+1)$$

$$d_{\mathsf{rsp}} = 2^{952} \approx p^{3.75}; \quad \gcd(d_{\mathsf{com}}, d_{\mathsf{chl}}) = 1$$



Hard: Given E, find a non-trivial cyclic endomorphism of smooth degree.

Outline

1 SNARK
¬(unkind criticism)
Coda/Mina
superMNT cycle

2 NIKE
¬(Greek goddess)
['siːsaɪd]
Gross lattice

3 Sigma
¬(Internet slang)
SQIsign
Degree map

Isogeny degree

Degree map

A positive definite quadratic form $\deg : \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E, E') \to \mathbb{Z}$ where $\varphi = \varphi_{\mathsf{sep}} \circ \pi_p^n$ and $\deg(\varphi) = \deg_s(\varphi_{\mathsf{sep}})p^n$ with $\deg_s(\varphi_{\mathsf{sep}}) = \#\ker(\varphi_{\mathsf{sep}})$.

Norm form for supersingular curves

$\varphi : E \to E'$ with $\deg(\varphi) = M$ corresponds to $\alpha \in I$ with $O_{\mathsf{L}}(I) = \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ and $O_{\mathsf{R}}(I) = \mathrm{End}_{\overline{\mathbb{F}}_p}(E')$, such that $\mathrm{nrd}(\alpha) = \mathrm{nrd}(I)M$.
A positive definite quadratic form $N_I : I \to \mathbb{Z}$ such that $N_I(\alpha) = \frac{\mathrm{nrd}(\alpha)}{\mathrm{nrd}(I)}$. Note that $\mathrm{nrd}(I) = \deg(\varphi_I)$.

1. Since the diameter of the supersingular ℓ-isogeny graph is $O(\log p)$, we know that there exist isogenies of degree $\ell^e \approx p$ between any two supersingular curves.
2. Random pairs of supersingular elliptic curves over $\mathbb{F}_{p^2}$ are unlikely to be connected by isogenies of degrees significantly smaller than $\sqrt{p}$.
3. New incarnations of SQIsign use higher-dimensional isogenies to achieve $d_{\mathsf{rsp}} \approx \sqrt{p}$, which speeds up the protocol significantly.

Refined Humbert invariant

Principally polarized abelian surface (A, θ) is either Jacobian of genus 2 hyperelliptic curve $(J(C), \theta_C)$ or product of two elliptic curves $(E_1 \times E_2, \theta_{E_1} \otimes \theta_{E_2})$.
Néron-Severi group of A is $\mathrm{NS}(A) := \mathrm{Div}(A)/\equiv$ where $D_1 \equiv D_2$ if intersection number $(D_1 \cdot D) = (D_2 \cdot D)$ for all $D \in \mathrm{Div}(A)$.

Kani [several works since 1994]

1. $\widetilde{\mathrm{RHI}}_{(A,\theta)} : \mathrm{NS}(A) \to \mathbb{Z}$ such that $\widetilde{\mathrm{RHI}}_{(A,\theta)}([D]) = (D \cdot \theta)^2 - 2(D \cdot D)$
2. $\mathrm{RHI}_{(A,\theta)} : \mathrm{NS}(A)/\mathbb{Z}\theta \to \mathbb{Z}$ such that $\mathrm{RHI}_{(A,\theta)}([D]) = (D \cdot \theta)^2 - 2(D \cdot D)$
3. θ is reducible if and only if $\mathrm{RHI}_{(A,\theta)}$ represents 1.
4. $\mathcal{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(E_1 \times E_2)$.
5. Let $(A, \theta) = (E_1 \times E_2, \theta_{E_1} \otimes \theta_{E_2})$. For $a, b \in \mathbb{Z}$ and $\varphi \in \mathrm{Hom}(E_1, E_2)$, $\mathrm{RHI}_{(A,\theta)}(\mathcal{D}(a, b, \varphi)) = (a - b)^2 + 4 \deg_{E_1,E_2}(\varphi)$

Principally polarized superspecial abelian surfaces

$B_p = (-q, -p|\mathbb{Q})$ where q is the smallest possible such integer. That is, $B_p = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{ij}$ with $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$, and $\mathbf{ij} = -\mathbf{ji}$.

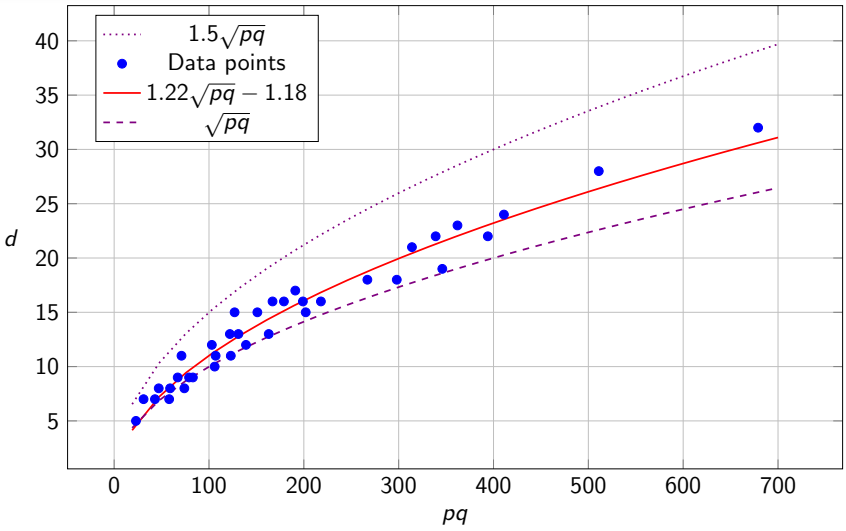
Kırımlı and Korpal

1. $D = \begin{pmatrix} u & w + x\mathbf{i} + y\mathbf{j} + z\mathbf{ij} \\ w - x\mathbf{i} - y\mathbf{j} - z\mathbf{ij} & v \end{pmatrix}$ with $u, v, w, x, y, z \in \mathbb{Z}$; positive definite quaternion hermitian matrix.
2. $\theta = \begin{pmatrix} m & \alpha_0 \\ \overline{\alpha}_0 & m \end{pmatrix}$, $m^2 - \mathrm{nrd}(\alpha_0) = 1$, $p \nmid \mathrm{nrd}(\alpha_0)$, $\alpha_0 \in \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij}$
3. $\widetilde{\mathrm{RHI}}_{(E_1 \times E_2, \theta)}(u, v, w, x, y, z) = (D \cdot \theta)^2 - 2(D \cdot D)$; $\det(\widetilde{\mathrm{RHI}}) = 0$.
4. $\mathrm{RHI}_{(E_1 \times E_2, \theta)}(t_0, t_1, t_2, t_3, t_4) = t_0^2 + 4\deg_{E_1, E_2}(t_1, t_2, t_3, t_4)$; $\det(RHI) = 2^{13}p^2q^2$.

Compute $d := \max_{\deg_{E_1,E_2}} \{\min\{M : \deg_{E_1,E_2}(t_1, t_2, t_3, t_4) = M\}\}$.

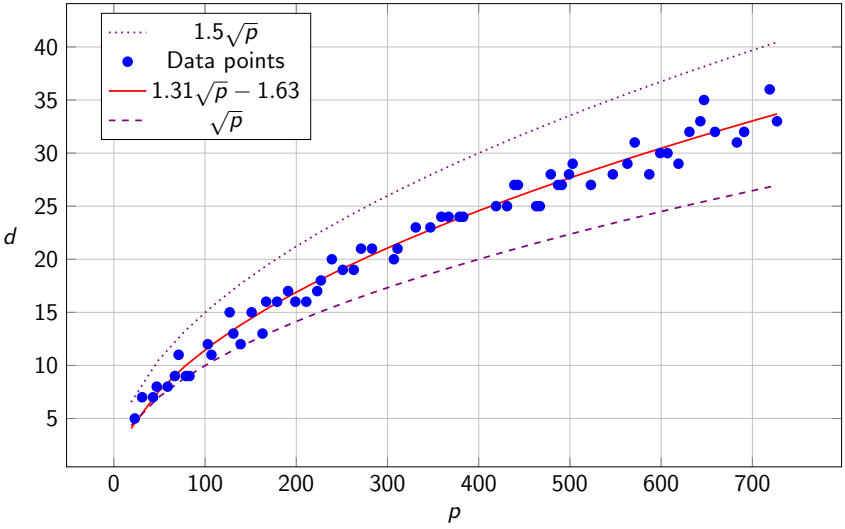
The trend of d values for 38 primes $20 < p < 200$ (not shown: $p = 193$, $q = 11$, and $d = 55$)

- $2pq \leq m \leq 2pq + p$
- $\#\Theta \gg \mathbf{H} = O(p^3)$
- $\#\underset{\text{red}}{\text{RHI}} \approx 0.1 \cdot \#\Theta$
- $\#\underset{\text{iso}}{\text{RHI}} \gg \dfrac{\mathbf{h}(\mathbf{h}+1)}{2}$
- $\#\underset{\text{iso}}{\text{RHI}} \stackrel{?}{=} \#\text{Gen}_4(2^4 p^2 q^2)$



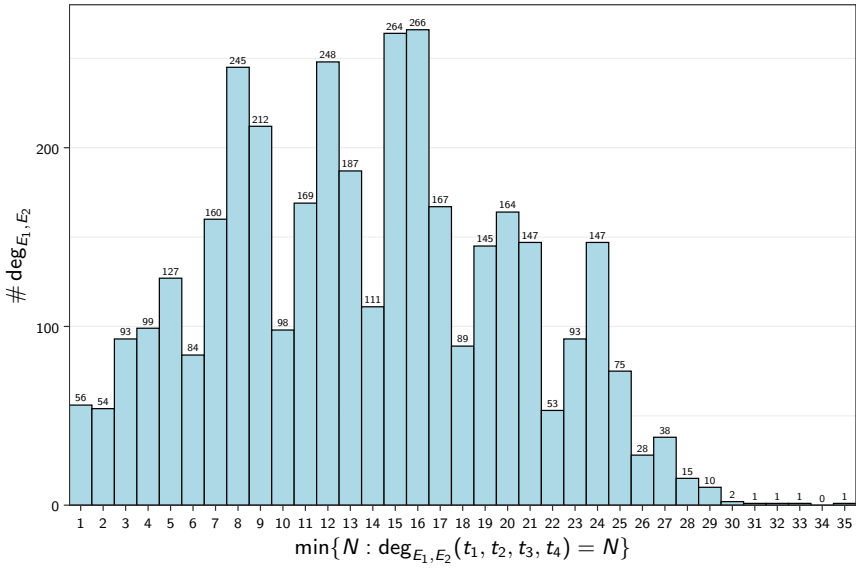
The trend of d values for 63 primes $p > 20$ such that $p \equiv 3 \pmod 4$.

- $2p \leq m \leq 3p$
- $\#\Theta \gg \mathbf{H} = O(p^3)$
- $\#\underset{\text{red}}{\text{RHI}} \approx 0.1 \cdot \#\Theta$
- $\#\underset{\text{iso}}{\text{RHI}} \gg \dfrac{\mathbf{h}(\mathbf{h}+1)}{2}$
- $\#\underset{\text{iso}}{\text{RHI}} \stackrel{?}{=} \#\text{Gen}_4(2^4 p^2)$



The frequency distribution of minimum values of all the degree maps for $p = 647$, $q = 1$; $25 < \sqrt{p} < 26$.

- $\mathbf{H} = 99,102$
- $\dfrac{\mathbf{h}(\mathbf{h}+1)}{2} = 1,540$
- $1294 \leq m \leq 1941$
- $\#\Theta = 699,249$
- $\#\underset{\text{red}}{\text{RHI}} = 65,693$
- $\#\underset{\text{iso}}{\text{RHI}} = 3,650$



Thank you!