An efficient key recovery attack on SIDH

Leuven Isogeny Days 3, September 21

Wouter Castryck & Thomas Decru

KU LEUVEN

Outline

- SIDH recap
- Isogenies in dimension two
- The glue-and-split attack

SIDH recap

Supersingular Isogeny Diffie-Hellman

ALICE

BOB

Finite field $\mathbb{F}_{p^2}$, supersingular elliptic curve E,

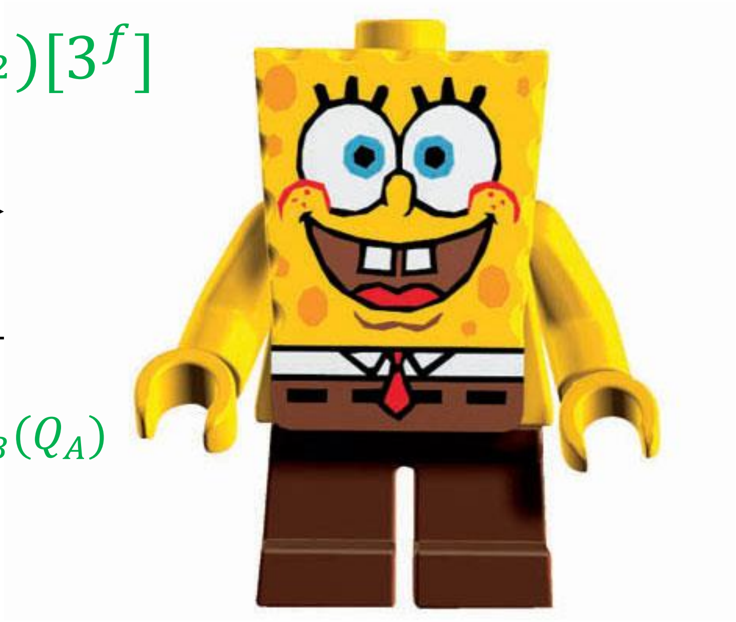
basis P_A, Q_A of $E(\mathbb{F}_{p^2})[2^e]$, basis P_B, Q_B of $E(\mathbb{F}_{p^2})[3^f]$

$\varphi_A: E \to E_A, \varphi_A(P_B), \varphi_A(Q_B)$

$\longrightarrow$

$\longleftarrow$

$\varphi_B: E \to E_B, \varphi_B(P_A), \varphi_B(Q_A)$



Shared secret: $j(E_{AB})$ obtained from

$$\varphi'_A: E_B \to E_{BA} \cong E_{AB} \leftarrow E_A: \varphi'_B$$

with $\ker(\varphi'_A) = \langle r_A \varphi_B(P_A) + s_A \varphi_B(Q_A) \rangle$,

$\ker(\varphi'_B) = \langle r_B \varphi_A(P_B) + s_B \varphi_A(Q_B) \rangle$

Secret kernel

$G_A = \langle r_A P_A + s_A Q_A \rangle$

Secret kernel

$G_B = \langle r_B P_B + s_B Q_B \rangle$

Security of SIDH/SIKE

- Quantum security is complicated in part because NIST's post-quantum security levels are vague; QRAM costs? Circuit depth? Latency? Etc.

- Best generic attack is a claw-finding attack: $O\left(p^{\frac{1}{4}}\right)$ classical and $O\left(p^{\frac{1}{6}}\right)$ quantum
- de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange, *Improved torsion-point attacks on SIDH variants* (CRYPTO 2021)
- Our work: heuristic polynomial time with precomputable integer factorization

- Galbraith, Petit, Shani, Ti, *On the security of supersingular isogeny cryptosystems* (ASIACRYPT 2016); chosen ciphertext attack against static key SIDH
- SIKE: Supersingular Isogeny Key Encapsulation ('key exchange with long term public key')

Computational versus decisional isogeny problem

Given E and E', find an isogeny of degree ℓ^k between them.

$\sim$

Given E and E', does there exist an isogeny of degree ℓ^i between them for $0 < i < k$?

$$E = E_0 \to E_1 \to E_2 \to E_3 \to \cdots \to E_{k-1} \to E_k = E'$$

$\ell + 1$ options $\quad$ ℓ options

Galbraith, Vercauteren, *Computational problems in supersingular elliptic curve isogenies* (Quantum Information Processing 2018)

Isogenies in dimension two

supersingular elliptic curves $\longrightarrow$ superspecial principally polarized abelian surfaces

A

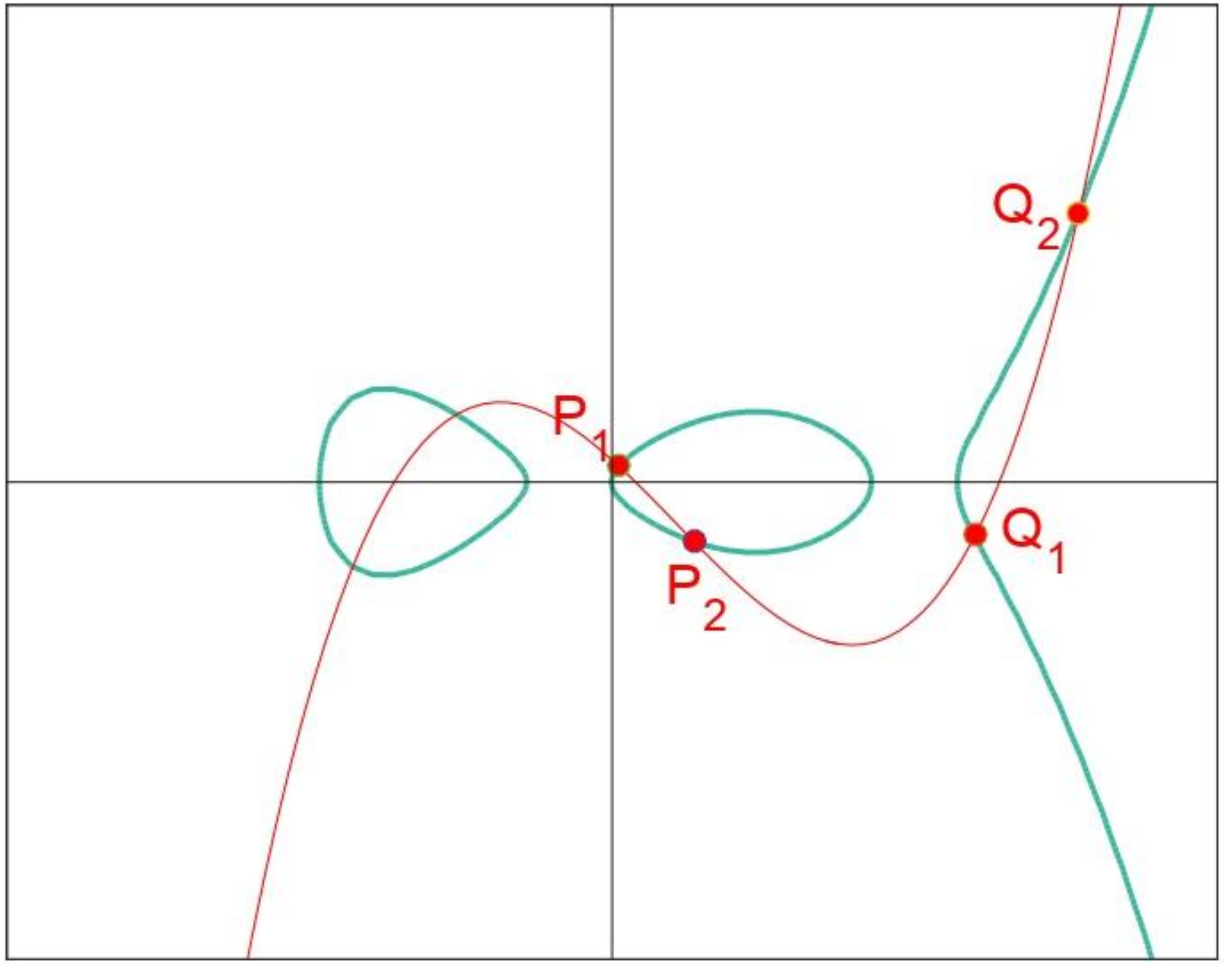
products of elliptic curves $E \times E'$

Jacobians of genus-2 curves

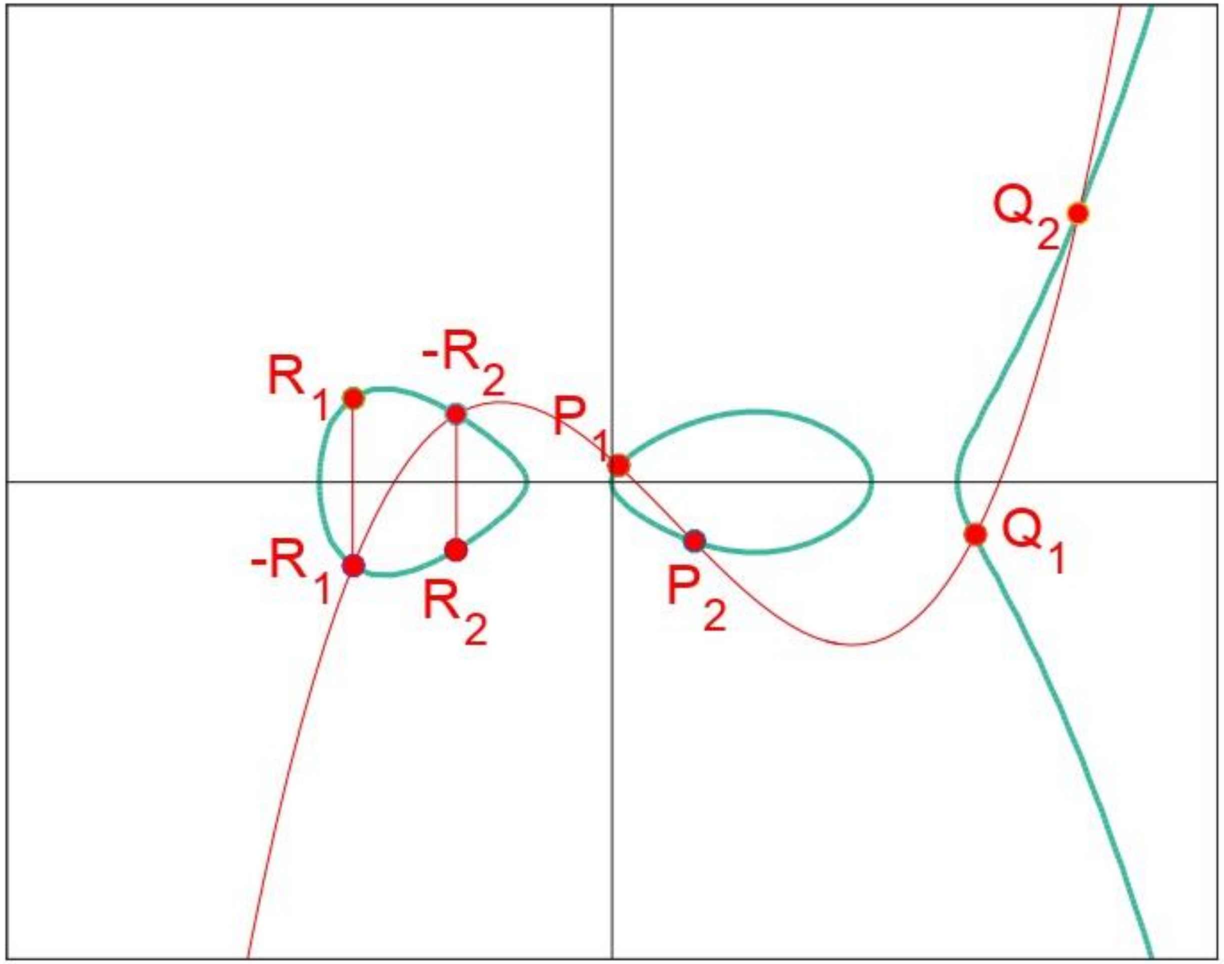
$C: y^2 = x^5 + Ax^3 + Bx^2 + Cx + D$

Smith, *Explicit Endomorphisms and Correspondences* (PhD thesis)

Castryck, Decru, Smith, *Hash functions from superspecial genus-2 curves* (Journal of Mathematical Cryptology 2020)



Q_2
P_1
Q_1
P_2



Q_2
R_1
$-R_2$
P_1
$-R_1$
R_2
P_2
Q_1

Invariants in two dimensions

A genus-2 curve is defined by a triplet of (absolute) Igusa invariants (i_1, i_2, i_3)

$\approx p^3/2880$ superspecial Jacobians of genus-2 curves

Brock, *Superspecial curves of genera two and three* (PhD thesis)

A product of elliptic curves is defined by a set of j-invariants $\{j_1, j_2\}$

$\approx p/12$ supersingular elliptic curves results in $\approx p^2/288$ superspecial products

Isogenies in dimension two

An (N, N)-isogeny $\Phi: A \to A'$ is an isogeny such that

- $\ker(\Phi) \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}$
- $\ker(\Phi)$ is maximal isotropic with regards to the N-Weil pairing, i.e.
$$\forall P, Q \in \ker(\Phi) : e_N(P, Q) = 1$$

Remark: the second condition ensures that A' comes equipped with a principal polarization!

Four types of isogenies!

$$1.\ Jac(C) \to Jac(C')$$

-> generic (N, N)-isogeny

$N = 2$, see Smith, *Explicit Endomorphisms and Correspondences* (PhD thesis)

$N = 3$, see Bruin, Flynn, Testa, *Descent via (3,3)-isogeny on Jacobians of genus 2 curves* (Acta Arithmetica 2014)

$N = \ell$, see Cosset, Robert, *Computing* (ℓ, ℓ)*-isogenies in polynomial time on Jacobians of genus 2 curves* (Mathematics of Computation 2015)

$$2.\ Jac(C) \to E_1' \times E_2'$$

-> split (N, N)-Jacobian

$N = 2$, see Smith, *Explicit Endomorphisms and Correspondences* (PhD thesis)

$N = 3$, see Bröker, Howe, Lauter, Stevenhagen, *Genus-2 curves and Jacobians with a given number of points* (LMS Journal of Computation and Mathematics 2015)

$N = \ell$, see Kuhn, *Curves of genus 2 with split Jacobian* (Transactions of the American Mathematical Society 1988)

Four types of isogenies!

3. $E_1 \times E_2 \to Jac(C')$ -> gluing elliptic curves along their (N, N)-torsion

4. $E_1 \times E_2 \to E_1' \times E_2'$ -> (N, N)-isogeny between products of elliptic curves

(N, N)-isogenies between products of elliptic curves

Let $\varphi_1\colon E_1 \to E_1'$ and $\varphi_2\colon E_2 \to E_2'$ be cyclic N-isogenies, then

$$\Phi = \varphi_1 \times \varphi_2$$

is an (N, N)-isogeny from $E_1 \times E_2$ to $E_1' \times E_2'$.

$\ker(\Phi)$ is maximal isotropic with regards to the N-Weil pairing.

It can be written as $\underbrace{\langle (P, \infty_{E_2}), (\infty_{E_1}, Q) \rangle}_{\text{this is a diagonal kernel}}$.

(N, N)-isogenies from products of elliptic curves

Let

$$\Phi: E_1 \times E_2 \to A'$$

be an (N, N)-isogeny with nondiagonal kernel

$$\ker(\Phi) = \langle (P_1, P_2), (Q_1, Q_2) \rangle.$$

When is this *not* an (N, N)-gluing; i.e. when is $A' \cong E_1' \times E_2'$?

Expected for superspecial abelian surfaces with probability $\approx \frac{10}{p}$.

The glue-and-split attack

Examples for failed gluings; i.e. $A' \cong E_1' \times E_2'$

- A $(2,2)$-isogeny $\Phi: E_1 \times E_2 \to A'$ with nondiagonal kernel *can* only have $A' \cong E_1' \times E_2'$ if $E_1 \cong E_2$.
- A $(3,3)$-isogeny $\Phi: E_1 \times E_2 \to A'$ with nondiagonal kernel *can* only have $A' \cong E_1' \times E_2'$ if there exists a 2-isogeny $\psi: E_1 \to E_2$.
- A $(5,5)$-isogeny $\Phi: E_1 \times E_2 \to A'$ with nondiagonal kernel *can* only have $A' \cong E_1' \times E_2'$ if there exists a 4- or 6-isogeny $\psi: E_1 \to E_2$.
- A $(7,7)$-isogeny $\Phi: E_1 \times E_2 \to A'$ with nondiagonal kernel *can* only have $A' \cong E_1' \times E_2'$ if there exists a 6- or 10- or 12-isogeny $\psi: E_1 \to E_2$.
- …

Kani's theorem (informal)

- **Theorem:** an (N, N)–isogeny $\Phi: E \times E' \to A'$ has A' a product of elliptic curves iff 'it comes' from an isogeny diamond configuration.

  i.e. the kernel is of the form $\langle (P, x\psi(P)), (Q, x\psi(Q)) \rangle$ for some $x \in \mathbb{Z}$

- **Definition:** an isogeny diamond configuration of order N is a tuple (ψ, G_1, G_2) with
  1. $\psi: E \to E'$ an isogeny;
  2. $G_1, G_2 \subset ker(\psi)$;
  3. $G_1 \cap G_2 = \{\infty_E\}$;
  4. $deg(\psi) = \#G_1 \cdot \#G_2$;
  5. $N = \#G_1 + \#G_2$.

Kani, *The number of curves of genus two with elliptic differentials* (Journal für die reine und angewandte Mathematik 1997)

Attacking Bob's secret key

Given

$$\underbrace{(E, P_A, Q_A)}_{\text{Alice's } 2^e\text{-torsion basis}}, (E_B, \varphi_B(P_A), \varphi_B(Q_A))$$

we want to find

$\varphi_B.$ → isogeny of degree 3^f

Idea: consider

$$E = E_0 \to E_1 \to E_2 \to \cdots \to E_{f-1} \to E_f = E_B$$

Which of the 4 options is correct? (remark that we can push P_A, Q_A through easily)

Forcing an isogeny diamond configuration

Can we force E_1, E_B into Kani's theorem?

Definition: an isogeny diamond configuration of order 2^e is a tuple (ψ, G_1, G_2) with

1. $\psi: E \to E'$ an isogeny; → $\psi = \varphi_1: E_1 \to E_B$ perhaps?
2. $G_1, G_2 \subset ker(\psi)$; → $\#G_i = 3^k$ for some k
3. $G_1 \cap G_2 = \{\infty_E\}$;
4. $deg(\psi) = \#G_1 \cdot \#G_2$; → $\deg(\psi) = 3^{f-1}$ if we have correct E_1
5. $2^e = \#G_1 + \#G_2$. → $\#G_1 = 3^{f-1}$ and $\#G_2 = 1$

Forcing an isogeny diamond configuration

Construct an isogeny $\gamma: E_1 \to C$ of degree $c = 2^e - 3^{f-1}$

$c > 0?$

How? Later!

Definition: an isogeny diamond configuration of order 2^e is a tuple (ψ, G_1, G_2) with

1. $\psi = \varphi_1 \circ \hat{\gamma}: C \to E_1 \to E_B$;
2. $G_1 = \ker(\hat{\gamma}), G_2 = \gamma(B)$ with B Bob's secret kernel;
3. $G_1 \cap G_2 = \{\infty_E\}$;
4. $deg(\psi) = \#G_1 \cdot \#G_2 = \left(2^e - 3^{f-1}\right) \cdot 3^{f-1}$;
5. $2^e = \#G_1 + \#G_2 = \left(2^e - 3^{f-1}\right) + 3^{f-1}$.

Finishing the attack

Consider $\Phi: C \times E_B \to A'$ with kernel

$$\left\langle \left(\gamma(P_{A,1}), \varphi_B(P_{A,1})\right), \left(\gamma(Q_{A,1}), \varphi_B(Q_{A,1})\right) \right\rangle.$$

In practice, compute

$$C \times E_B \to Jac(C_1) \to Jac(C_2) \to \cdots \to Jac(C_{e-2}) \to A'$$

(2,2)-isogenies

If A' is a product of elliptic curves, we picked the correct E_1 with overwhelming probability!

Finding a $\gamma: E_i \to C$ of degree $c = 2^e - 3^{f-i}$

- Known endomorphism ring ($C \cong E_i$):
  - $E_i: y^2 = x^3 + x$ has endomorphism $\iota: E_i \to E_i, (x, y) \mapsto (-x, iy)$
    -> if $c = u^2 + v^2 = (u + iv)(u - iv)$ for $u, v \in \mathbb{N}$ we can find γ easily
  - $E_0: y^2 = x^3 + 6x^2 + x$ has endomorphism 2ι → we can translate $\gamma_0: E_0 \to E_0$ to E_i
    -> similar easy trick; E_0 is actually used in SIKE as starting curve
  - E_i with small endomorphism ok too
  - In general, if $End(E_i)$ is known we can use KLPT algorithm

Finding a $\gamma: E_i \to C$ of degree $c = 2^e - 3^{f-i}$

- Unknown endomorphism ring:
  - Hope that c is smooth and work with arbitrary isogenies over extension fields
  - Add more leeway:

$$c = d \cdot 2^{e-j} - d' \cdot 3^{f-i}$$

we can guess the action of the d-torsion; in practice this means after the $(2^{e-j}, 2^{e-j})$-isogeny we check if *any* of the (d, d)-isogenies splits

probability that this happens by chance is only $O\left(\frac{d^3}{p}\right)$

if we know the action of φ_B on the 2^e-torsion, we also have it on the 2^{e-j}-torsion

we can extend φ_B with any isogeny of degree d'

we don't need all $0 < i < f$

Thanks!