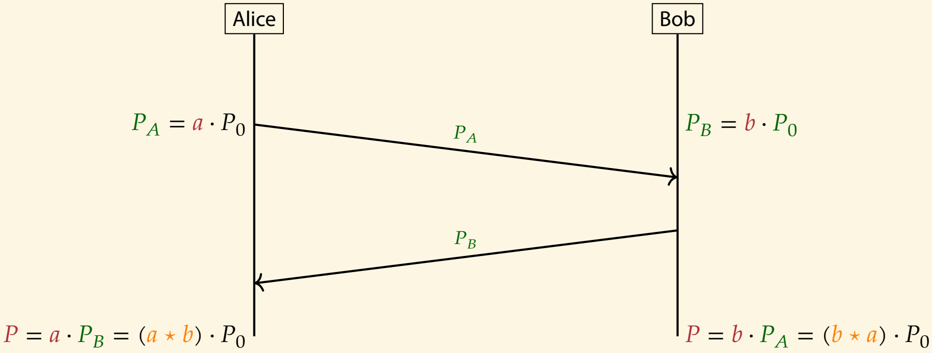
The module action for isogeny based cryptography

2025/06/13 — AGC^{2}T — Luminy

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

NIKE: Non Interactive Key Exchange



CRS Key Exchange ([Couveignes (1997)], [Rostovtsev–Stolbunov (2006)])

The ideal action on ordinary elliptic curves:

$$\begin{array}{ccc} E_0 & \longrightarrow & E_{[\mathfrak{a}]} = \mathfrak{a} \cdot E_0 \\ \downarrow & & \downarrow \\ E_{[\mathfrak{b}]} = \mathfrak{b} \cdot E_0 & \longrightarrow & E_{[\mathfrak{a}\mathfrak{b}]} \simeq \mathfrak{a}\mathfrak{b} \cdot E_0 \end{array}$$

☺ Commutative group action

- Restricted group action $\rightsquigarrow$ Unrestricted group action:
  CSI-FiSh (2019), [Pearl-]Scallop[-HD] (2023–2024), [CKQ]lapoti[s]/Pegasis (2023–2025)

- Classical security $\approx \Delta^{1/4}$

☹ Susceptible to Kuperberg's subexponential quantum algorithm
$\Rightarrow$ need to work with $\Delta \gg 512$ bits

The ordinary ideal action

- $E/\mathbb{F}_q$ ordinary elliptic curve
- $\mathfrak{a} \subset R := \mathrm{End}_{\mathbb{F}_q}(E)$ invertible ideal in a quadratic imaginary order

Definition (The ideal action)

$\mathfrak{a} \cdot E$ is the elliptic curve $E/E[\mathfrak{a}]$, where

$$E[\mathfrak{a}] := \{P \in E(\overline{\mathbb{F}}_q) \mid \alpha(P) = 0_E, \forall \alpha \in \mathfrak{a}\}$$

☹ This conflates the codomain $\mathfrak{a} \cdot E$ with the way we compute it as an isogeny $E \to E/E[\mathfrak{a}]$

- Not obvious that $\mathfrak{a} \cdot \mathfrak{b} \cdot E \simeq (\mathfrak{a}\mathfrak{b}) \cdot E$ (Can use that $\deg E[\mathfrak{a}] = N(\mathfrak{a})$)
  What happens at non invertible ideals?
- As in Deuring's correspondence, can kinda be reframed as an equivalence of category between (equivalence classes of) invertible ideals in R and (isomorphism classes of) elliptic curves "horizontally" isogeneous to E
- An isogeny $\phi : \mathfrak{a} \cdot E \to \mathfrak{b} \cdot E$ corresponds to the invertible ideal $\mathfrak{b}\mathfrak{a}^{-1}$
- Not clear distinction of objects and morphisms
- **Question 1**: intrinsic characterisation of $\mathfrak{a} \cdot E$?

SIDH/SIKE: supersingular isogeny key exchange ([De Feo, Jao (2011)],[De Feo, Jao, Plût (2014)])

- **Idea**: Switch to maximal supersingular curves over $\mathbb{F}_{p^2}$
- No commutative group action $\Rightarrow$ no Kuperberg attack

SIDH/SIKE: supersingular isogeny key exchange ([De Feo, Jao (2011)],[De Feo, Jao, Plût (2014)])

SIDH/SIKE: supersingular isogeny key exchange ([De Feo, Jao (2011)],[De Feo, Jao, Plût (2014)])

- **Observation:** The CRS diagram

$$\begin{tikzcd} E_0 \arrow[r] \arrow[d] & E_{[\mathfrak{a}]} = \mathfrak{a} \cdot E_0 \arrow[d] \\ E_{[\mathfrak{b}]} = \mathfrak{b} \cdot E_0 \arrow[r] & E_{[\mathfrak{a}\mathfrak{b}]} \simeq \mathfrak{a}\mathfrak{b} \cdot E_0 \end{tikzcd}$$

  is a pushforward if $N(\mathfrak{a})$ is coprime to $N(\mathfrak{b})$

- **SIDH**:

$$\begin{tikzcd} E_0 \arrow[r] \arrow[d] & E_A = E_0/K_A \arrow[d] \\ E_B = E_0/K_B \arrow[r] & E_{AB} \simeq E_0/(K_A + K_B) \end{tikzcd}$$

  where $K_A \subset E_0[2^a]$, $K_B \subset E_0[3^b]$ and $E_0/\mathbb{F}_{p^2}$ is a maximal supersingular curve

☹ To compute E_{AB} from E_A and K_B, Bob needs extra torsion information on E_A from Alice

☹☹☹ SIDH attacks [Castryck-Decru; Maino-Martindale-Panny-Pope-Wesolowski; R. 2023]

A commutative supersingular key exchange?

- There is also a supersingular ideal action [Deuring]
- $K_A = E_0[I_A], K_B = E_0[I_B], I_A, I_B \subset \mathfrak{O}_0 := \mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$

- **Problem**: the endomorphism ring $\mathfrak{O}_A$ of E_A is distinct from $\mathfrak{O}_0$, so I_B is not an ideal of it
- Instead, Bob needs to act by a different ideal $I'_B \subset \mathfrak{O}_A$ to get $E_{AB} = I'_B \cdot E_A$

- **Idea**: What if I_A, I_B are generated by ideals $\mathfrak{a}, \mathfrak{b} \subset R$ of a commutative quadratic order $R \subset \mathfrak{O}$?
- Then $R \subset \mathfrak{O}_A$, and I'_B is also generated by $\mathfrak{b}$ (Assume R saturated in $\mathfrak{O}$ and the ideals $\mathfrak{a}, \mathfrak{b}$ invertible in R)
- And $E_A[I'_B] = E_A[\mathfrak{b}]$ can be computed as long as Bob knows how R acts on E_A

- CSIDH [Castryck-Lange-Martindale-Panny-Renes 2018]: start with a supersingular $E_0/\mathbb{F}_p$ and $R = \mathbb{Z}[\sqrt{-p}] = \mathbb{Z}[\pi_p]$
- Oriented group actions [Colò-Kohel 2020], [Onuki 2020] on a (maximal) supersingular curve $E_0/\mathbb{F}_{p^2}$, with $R \subset \mathfrak{O}_0$ arbitrary

Frobenius orientation (CSIDH) and arbitrary orientations (SCALLOP)

$$\begin{tikzcd} E_0 \arrow[r] \arrow[d] & E_{[\mathfrak{a}]} = \mathfrak{a} \cdot E_0 \arrow[d] \\ E_{[\mathfrak{b}]} = \mathfrak{b} \cdot E_0 \arrow[r] & E_{[\mathfrak{a}\mathfrak{b}]} \simeq \mathfrak{a}\mathfrak{b} \cdot E_0 \end{tikzcd}$$

- $E_0/\mathbb{F}_{p^2}$ supersingular curve
- $R \subset \mathfrak{O}_0$ orientation by a quadratic imaginary order; $\mathfrak{a}, \mathfrak{b} \subset R$ invertible ideals

CSIDH: $E_0/\mathbb{F}_p$ + natural Frobenius orientation $\pi_p \curvearrowright E_0$ (like in CRS)

☺ Great control on torsion (e.g. if $2^e \mid p+1$, the points in $E_0[2^e]$ are rational over $\mathbb{F}_{p^2}$)

😐 $\Delta_R = -4p$

SCALLOP: arbitrary orientation $R \subset \mathfrak{O}_0$

☺ Decouple the arithmetic ($\mathbb{F}_p$) with the discriminant Δ_R (For an ordinary curve, $\Delta(\pi_p) \approx p$)

😐 Needs a way to represent the orientation

☹ Both still susceptible to Kuperberg's subexponential quantum algorithm

A commutative supersingular key exchange (round 2)?

$$\begin{array}{ccc} E_0 & \longrightarrow & E_{I_A} = I_A \cdot E_0 \\ \downarrow & & \\ E_{I_B} = I_B \cdot E_0 & & \end{array}$$

- **Goal**: complete the diagram for I_A, I_B arbitrary ideals of $\mathfrak{O}_0$
- **Idea**: if $R \subset \mathfrak{O}_0$ is an orientation by a quadratic order, I_A, I_B are rank 2 R-modules
- $I_A I_B$ is not a well defined ideal, but $I_A \otimes_R I_B$ is a well defined rank 4 R-module
- Commutativity: $I_A \otimes_R I_B \simeq I_B \otimes_R I_A$
- **Question 2**: Can we make sense of a module action?

The module action

- If $A_1, A_2/k$ are two abelian varieties oriented by R, then $\mathrm{Hom}_R(A_1, A_2)$ is a R-module

Definition (The power object)

If A is an abelian variety oriented by R and M a (finite type) R-module, $M \cdot A := \mathcal{H}om_R(M, A)$ is the (unique) R-oriented abelian variety, if it exists, such that

$$\mathrm{Hom}_{R-\mathrm{Ab}}(X, \mathcal{H}om_R(M, A)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{R-\mathrm{Ab}}(X, A)) \quad \forall X \in R - \mathrm{Ab}$$

$R - \mathrm{Ab}$: category of R-oriented abelian varieties and R-oriented morphisms

[Giraud 1968] (credits Serre+Tate), [Serre 1985]

- Functoriality: an R-linear map $\psi : M_2 \to M_1$ induces an oriented morphism

$$\phi : \mathcal{H}om_R(M_1, A) \to \mathcal{H}om_R(M_2, A)$$

- Left exactness: $M_1 \twoheadrightarrow M_2 \to 0 \quad \rightsquigarrow \quad 0 \to \mathcal{H}om_R(M_2, A) \hookrightarrow \mathcal{H}om_R(M_1, A)$
  $0 \to A_1 \hookrightarrow A_2 \quad \rightsquigarrow \quad 0 \to \mathcal{H}om_R(M, A_1) \hookrightarrow \mathcal{H}om_R(M, A_2)$
- Commutativity: if R is commutative, $M_2 \cdot M_1 \cdot A = \mathcal{H}om_R(M_2, \mathcal{H}om_R(M_1, A)) = \mathcal{H}om_R(M_1 \otimes_R M_2, A) = (M_1 \otimes_R M_2) \cdot A = M_1 \cdot M_2 \cdot A$

Construction of the module action

- Embed both categories into $\underline{R}$-modules for the (big) fppf-topos (sheafs for the fppf site of $\operatorname{Spec} k$)
- $\mathcal{H}om_R(M, A) := \mathcal{H}om_{R-fppf}(\underline{M}, A)$ is the $\underline{R}$-Hom sheaf (internal $\underline{R}$-Hom in the fppf-topos)
  $\underline{M}$ is the fppf-sheafification of the constant sheaf M

- Functor of points: If S/k is a f.t. k-algebra,

$$\mathcal{H}om_R(M, A)(S) = \operatorname{Hom}_R(M, A(S))$$

  [Waterhouse 1969, Appendix A] (cites [Serre 1965, 1967])

- This is always the (sheaf associated to) a proper commutative group scheme, of dimension

$$\dim \mathcal{H}om_R(M, A) = \operatorname{rank} M \times \dim A$$

- $\mathcal{H}om_R(M, A)$ is an abelian variety if M is projective [Serre]
- Exactness: if $0 \to M_2 \to M_1 \to M_1/M_2 \to 0$ is exact, and $\mathcal{H}om_R(M_2, A)$ is an abelian variety, then

$$0 \to \mathcal{H}om_R(M_1/M_2, A) \to \mathcal{H}om_R(M_1, A) \to \mathcal{H}om_R(M_2, A) \to 0$$

  is exact

An equivalence of category

Oriented case: E_0/k elliptic curve primitively oriented by R quadratic imaginary

Theorem (Module anti-equivalence of category)

The action $M \mapsto M \cdot E_0 = \mathcal{H}om_R(M, E_0)$ gives an antiequivalence of category between the category of R-oriented abelian varieties [a] A k-isogenous to E_0^g and R-oriented k-morphisms; and the category of f.p. torsion free R-modules M of rank g and R-module morphisms.

Inverse map: $A \mapsto \mathrm{Hom}_R(A, E_0)$: module of (oriented) morphisms from A to E_0

[a] with the technical condition $\rho_R(A) \simeq \oplus_{i=1}^{g} \rho_R(E_0)$, where $\rho_R(A)$ is the representation of R/pR on Lie A

[Kani 2011], [Jordan, Keeton, Poonen, Rains, Shepherd-Barron, Tate 2018], [Page-R. 2023]

Example

- Frobenius orientation for $E_0/\mathbb{F}_p$: all $\mathbb{F}_p$-rational isogenies at level above E_0^g
- If p is inert in R, the Frobenius isogeny $\pi_p : E_0 \to E_0^{(p)}$ cannot be represented by an R-module morphism $\Rightarrow$ Needs extra "Dieudonné" information to handle general inseparable isogenies, see [Centeleghe-Stix 2015, 2023; Bergström, Karemaker, Marseglia 2024]

- Symmetric monoidal structure: $(M_1 \cdot E_0) \otimes_{E_0} (M_2 \cdot E_0) := (M_1 \otimes_R M_2) \cdot E_0 = M_1 \cdot M_2 \cdot E_0$
This is an abelian variety if $M_1 \otimes_R M_2$ is torsion free.

Computing the module action

- Needs to work with polarised abelian varieties. For simplicity: stick to ppavs.
- Since the Rosati involution on E_0 induces the complex conjugation on R, a principal polarisation on $M \cdot E_0$ corresponds to a unimodular R-Hermitian form on M [Serre 1985, 2001], [Kirschmer, Narbonne, Ritzenthaler, R. 2021],
- If $(M_1, H_1), (M_2, H_2)$ are unimodular torsion free Hermitian R-modules of rank g then $(A_i, \lambda_i) = (M_i, H_i) \cdot (E_0, \lambda_0)$ are principally polarised abelian varieties of dimension g
- We have a M_1-module orientation on A_1: if $m_1 \in M_1$, the map $R \to M_1, r \mapsto rm_1$ induces

$$m_1 : A_1 \to E_0.$$

Proposition ([Kirschmer, Narbonne, Ritzenthaler, R. 2021])

If $\psi : (M_2, H_2) \hookrightarrow (M_1, H_1)$ is an N-similitude (i.e. $\psi^* H_1 = N H_2$), then $\phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ is an N-isogeny of ppavs, with kernel

$$\operatorname{Ker} \phi = M_1/M_2 \cdot A = A_1[M_2] = \{P \in A_1(\bar{k}) \mid m(P) = 0_{E_0} \forall m \in M_2\}$$

Corollary (Clapoti for the module action)

If we can find two N_i-similitudes $(M, H_M) \to (R^g, H_{R^g})$, with N_1 coprime to N_2, we can compute $(M, H_M) \cdot E_0$ in polynomial time.

Computing the module action

Proposition ([Kirschmer, Narbonne, Ritzenthaler, R. 2021])

If $\psi : (M_2, H_2) \hookrightarrow (M_1, H_1)$ is an N-similitude (i.e. $\psi^* H_1 = N H_2$), then $\phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ is an N-isogeny of ppavs, with kernel

$$\operatorname{Ker} \phi = M_1 / M_2 \cdot A = A_1[M_2] = \{P \in A_1(\bar{k}) \mid m(P) = 0_{E_0} \forall m \in M_2\}$$

Example (The ideal action)

If $\mathfrak{a} \subset R$, we have a canonical unimodular Hermitian form:

$$H_{\mathfrak{a}}(x, y) = \frac{x\bar{y}}{N(\mathfrak{a})}$$

The inclusion $(\mathfrak{a}, H_{\mathfrak{a}}) \subset (R, H_R)$ is a $N(\mathfrak{a})$-similitude, hence we obtain a $N(\mathfrak{a})$-isogeny

$$\phi_{\mathfrak{a}} : E = R \cdot E \to \mathfrak{a} \cdot E$$

with kernel $(R/\mathfrak{a}) \cdot E = E[\mathfrak{a}]$.

Linking the supersingular ideal action with an oriented rank 2 module action

$E_0/\mathbb{F}_p$ primitively oriented by $R = \mathbb{Z}[\pi_p]$.

Proposition (Weil restriction)

If $I \subset \mathfrak{O}_0$ and $E_I = I \cdot E_0$, then

$$(M_I, H_I) \cdot (E_0, \lambda_0) = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_I, \lambda_I)$$

where $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ is the Weil restriction, M_I is I seen as an R-module, and H_I is derived from the quaternionic Hermitian form

$$H_{\mathfrak{O}_0,I} : x, y \in I \mapsto x\overline{y}/N(I).$$

Corollary (Module inversion)

The rank 2 unimodular module supersingular action inversion problem over $\mathbb{F}_p$ is at least as hard as the supersingular isogeny path problem over $\mathbb{F}_{p^2}$.

⊗-MIKE

$$\begin{tikzcd} E'_0 \arrow[r] \arrow[d] & E_{I_1} \arrow[d, squiggly] \\ E_{I_2} \arrow[r, squiggly] & A_{12} = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_{I_1} \otimes_{E'_0} W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_{I_2} \end{tikzcd}$$

- $E'_0 : y^2 = x^3 - x/\mathbb{F}_p, \quad p = u2^e - 1.$ (Ex: $p = 5 \cdot 2^{248} - 1$.)
- Alice and Bob each compute a 2^e-isogeny from E'_0 over $\mathbb{F}_{p^2}$
- Then the common key A_{12} requires computing a 2^e-isogeny in dimension 4 over $\mathbb{F}_p$

- No need for coprime degrees!
- Conjecture: 512 bits NIKE for 128 bits of quantum security
  This conjecture holds if:
  1. the module Diffie-Helmann problem is as hard as module inversion;
  2. The difficulty of recovering the supersingular isogeny $E'_0 \to E_{I_1}$ has $e/2$ bits of quantum security.

Help needed!

Need good dimension 4 modular invariants to represent A_{12} (e.g. suitable symmetric polynomials in the theta constants?)

Perspectives

- Implement this!
- Public Key Encryption via an ElGamal approach
- Signatures?
- Other protocols? (Problem: the dimension grows exponentially with the number of actions…)

- Can handle twists by looking at Galoisian $R[G]$-modules actions to encode descent data

Example (Quadratic twists: $G = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \langle \sigma \rangle$)

- if $R' = R$ with σ acting by -1, then $R' \cdot E_0 = E_0^t$ is the quadratic twist, and
$$R' \cdot I \cdot R' \cdot E_0 \simeq \bar{I} \cdot E_0$$
- $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_0 = R[G] \cdot E_0$

- Extend the module equivalence of category to a ppav (A_0, λ_0) primitively oriented by a CM order O with maximal real multiplication.
(And such that the Rosati involution restricts to the complex conjugation on O. Maximal real multiplication ensures that O is a Bass order)

Constructing the power object

- Embed $R - \mathrm{Ab}$ into R-oriented proper commutative group schemes to get an abelian category
- Embed both categories (R-modules and R-oriented proper commutative group schemes) inside the (big) fppf-topos (sheafs for the fppf site of $\operatorname{Spec} k$)
- We obtain abelian subcategories of fppf $\underline{R}$-modules.
  More precisely we have exact fully faithful morphisms:
  - to an R-oriented proper commutative group scheme G we associate its functor of points $S \mapsto G(S)$, which is an fppf sheaf
  - to an R-module M we associate $\underline{M}$ is the fppf-sheafification of the constant (pre)sheaf M

- $\mathcal{H}om_R(M, A) := \mathcal{H}om_{R-fppf}(\underline{M}, A)$ is the $\underline{R}$-Hom sheaf (internal $\underline{R}$-Hom in the fppf-topos)

☡ This is only the power object in the larger category of $\underline{R}$-modules. Still, if this is (the sheaf associated to) an abelian variety, then it has to be the power object for (R-oriented) abelian varieties.

- If M is f.p., this is always (the sheaf associated to) a proper commutative group scheme.

Exactness properties

- Recall: if $0 \to M_2 \to M_1 \to M_1/M_2 \to 0$ is exact, and $\mathcal{H}om_R(M_2, A)$ is an abelian variety, then
$$0 \to \mathcal{H}om_R(M_1/M_2, A) \to \mathcal{H}om_R(M_1, A) \to \mathcal{H}om_R(M_2, A) \to 0$$
is exact

- In general, we have a long exact sequence
$$0 \to \mathcal{H}om_R(M_1/M_2, A) \to \mathcal{H}om_R(M_1, A) \to \mathcal{H}om_R(M_2, A) \to \\ \mathcal{E}xt^1_R(M_1/M_2, A) \to \mathcal{E}xt^1_R(M_1, A) \to \mathcal{E}xt^1_R(M_1, A) \to \dots$$

There are different variants of $\mathcal{E}xt^1_R$ we can take here:

- $\mathcal{E}xt^1_R(M, A) := \mathcal{E}xt^1_{R-fppf}(\underline{M}, A) = H^1(\mathcal{R}\mathcal{H}om_{R-fppf}(\underline{M}, A))$
- $\mathcal{E}xt^1_R(M, A) := i^*_{fppf}\mathcal{E}xt^1_{R-PSh}(M, A)$ where i^*_{fppf} is the fppf sheafification of presheaves

Since $i^*_{fppf}\mathcal{R}\mathcal{H}om_{R-PSh}(M, A) = \mathcal{R}\mathcal{H}om_{R-fppf}(\underline{M}, A)$ these are related by a spectral sequence.

Scholten's construction

- To have lots of 2^e-torsion, we work with $p \equiv 7 \pmod 8$, so we have a non trivial 2-volcano
- For technical reasons, we will start with a curve E_0' on the crater of the 2-volcano rather than on the floor
- $\mathrm{End}_{\mathbb{F}_p}(E_0')$ is the maximal order O_R of $R = \mathbb{Z}[\pi_p]$, and the conductor $\mathfrak{f} \subset \mathbb{Z}[\pi_p]$ is of index 2
- We use a slight variant of the Weil restriction: $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} = \mathfrak{f} \cdot_R W_{\mathbb{F}_{p^2}/\mathbb{F}_p}$

  (we can prove that $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ gives Scholten's construction)
- If $E_{I'} = I' \cdot E_0'$ for $I' \subset \mathfrak{O}_0'$, we still have $(M_{I'}, H_{I'}) \cdot_{O_R} (E_0', \lambda_0') = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_{I'}, \lambda_{I'})$
- In practice: take $E_0' : y^2 = x^3 - x / \mathbb{F}_p$, so that $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_0' \simeq {E_0'}^2$