

SIDH and its Applications

Simon-Philipp Merz

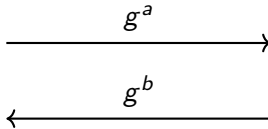


March 2022

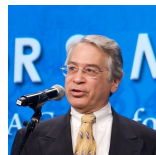
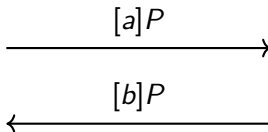
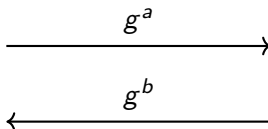
Isogeny-based Cryptography Workshop, Birmingham

- Isogenies and isogeny graphs
- SIDH
- B-SIDH
- Séta
- Applications
 - SIKE
 - Static-static key exchange
 - SI-X3DH
 - Proof of isogeny knowledge
 - Oblivious pseudorandom functions
 - Updateable public key encryption
- Conclusion

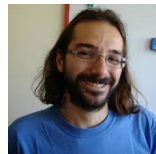
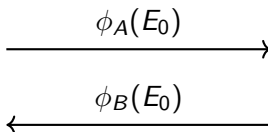
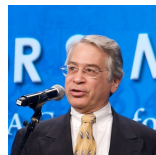
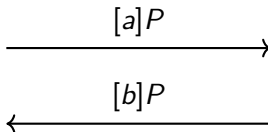
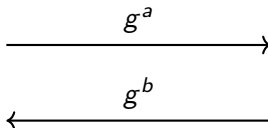
Evolution of Diffie-Hellman



Evolution of Diffie-Hellman



Evolution of Diffie-Hellman



credits: Craig Costello's ECC2017 talk

Definition

Let E, E' be two elliptic curves, and let $\varphi : E \rightarrow E'$ be a map between them. φ is called an *isogeny*, if

- φ is a surjective group homomorphism
- φ is a group homomorphism with finite kernel
- φ is a non-constant rational map with $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$

Definition

Let E, E' be two elliptic curves, and let $\varphi : E \rightarrow E'$ be a map between them. φ is called an *isogeny*, if

- φ is a surjective group homomorphism
 - φ is a group homomorphism with finite kernel
 - φ is a non-constant rational map with $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$
-
- For any finite subgroup $H \subset E$, there exists an isogeny $\varphi : E \rightarrow E' := E/H$ with kernel H
 - For (separable) isogenies, $\# \ker(\varphi)$ is the degree of φ

Factoring isogenies

Definition (Universal property)

Let $\varphi : E \rightarrow E'$ be an isogeny. If $P \in \ker(\varphi)$, then there exist isogenies ψ, ϕ such that $\ker(\psi) = \langle P \rangle$ and

$$\varphi = \phi \circ \psi$$

$$\text{with } \deg(\varphi) = \deg(\phi) \cdot \deg(\psi)$$

Factoring isogenies

Definition (Universal property)

Let $\varphi : E \rightarrow E'$ be an isogeny. If $P \in \ker(\varphi)$, then there exist isogenies ψ, ϕ such that $\ker(\psi) = \langle P \rangle$ and

$$\varphi = \phi \circ \psi$$

$$\text{with } \deg(\varphi) = \deg(\phi) \cdot \deg(\psi)$$

- Factorisation is unique up to composition with isomorphisms

Factoring isogenies

Definition (Universal property)

Let $\varphi : E \rightarrow E'$ be an isogeny. If $P \in \ker(\varphi)$, then there exist isogenies ψ, ϕ such that $\ker(\psi) = \langle P \rangle$ and

$$\varphi = \phi \circ \psi$$

with $\deg(\varphi) = \deg(\phi) \cdot \deg(\psi)$

- Factorisation is unique up to composition with isomorphisms

Definition (j -invariant)

Let $E : y^2 = x^3 + ax + b$. Then, the j -invariant of E is

$$j(E) := 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_{p^2}.$$

Supersingular isogeny graphs

Definition (ℓ -isogeny graph)

The supersingular ℓ -isogeny graph over \mathbb{F}_{p^2} consists of

- vertices are j -invariants of supersingular elliptic curves defined over \mathbb{F}_{p^2}
- edges between j and j' correspond to an ℓ -isogeny between two elliptic curves with j -invariants j and j' .

Supersingular isogeny graphs

Definition (ℓ -isogeny graph)

The supersingular ℓ -isogeny graph over \mathbb{F}_{p^2} consists of

- vertices are j -invariants of supersingular elliptic curves defined over \mathbb{F}_{p^2}
 - edges between j and j' correspond to an ℓ -isogeny between two elliptic curves with j -invariants j and j' .
- connected, $\ell + 1$ -regular graph

Supersingular isogeny graphs

Definition (ℓ -isogeny graph)

The supersingular ℓ -isogeny graph over \mathbb{F}_{p^2} consists of

- vertices are j -invariants of supersingular elliptic curves defined over \mathbb{F}_{p^2}
 - edges between j and j' correspond to an ℓ -isogeny between two elliptic curves with j -invariants j and j' .
-
- connected, $\ell + 1$ -regular graph
 - graph has $\approx p/12$ vertices

Supersingular isogeny graphs

Definition (ℓ -isogeny graph)

The supersingular ℓ -isogeny graph over \mathbb{F}_{p^2} consists of

- vertices are j -invariants of supersingular elliptic curves defined over \mathbb{F}_{p^2}
 - edges between j and j' correspond to an ℓ -isogeny between two elliptic curves with j -invariants j and j' .
-
- connected, $\ell + 1$ -regular graph
 - graph has $\approx p/12$ vertices
 - expander property: random walk of $\log(p)$ steps is almost as good as uniformly sampling the vertices

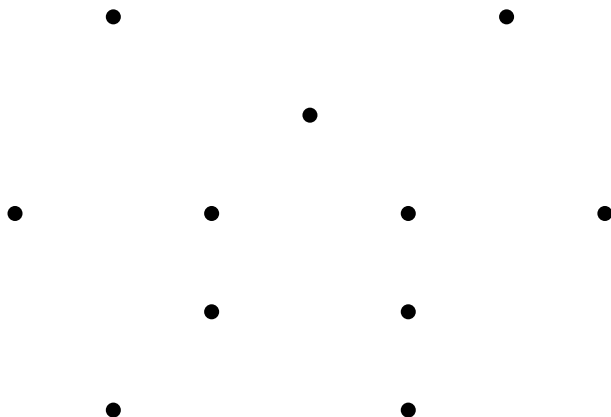
Supersingular isogeny graphs

Definition (ℓ -isogeny graph)

The supersingular ℓ -isogeny graph over \mathbb{F}_{p^2} consists of

- vertices are j -invariants of supersingular elliptic curves defined over \mathbb{F}_{p^2}
 - edges between j and j' correspond to an ℓ -isogeny between two elliptic curves with j -invariants j and j' .
-
- connected, $\ell + 1$ -regular graph
 - graph has $\approx p/12$ vertices
 - expander property: random walk of $\log(p)$ steps is almost as good as uniformly sampling the vertices
 - path finding is postulated to be exponentially hard both classically and quantumly

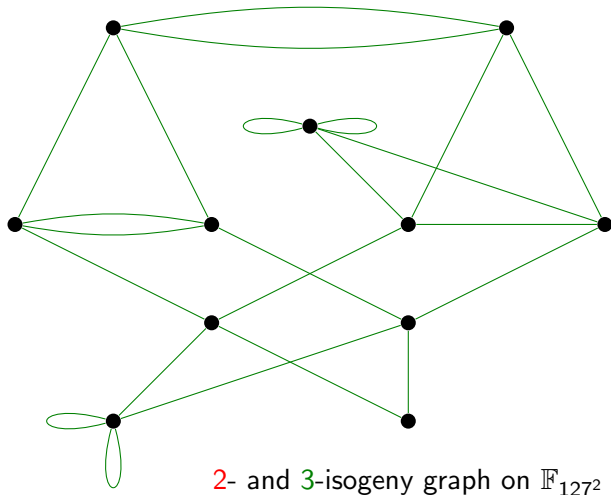
Idea: **Alice** and **Bob** walk in two *different* isogeny graphs on the *same* vertex set.



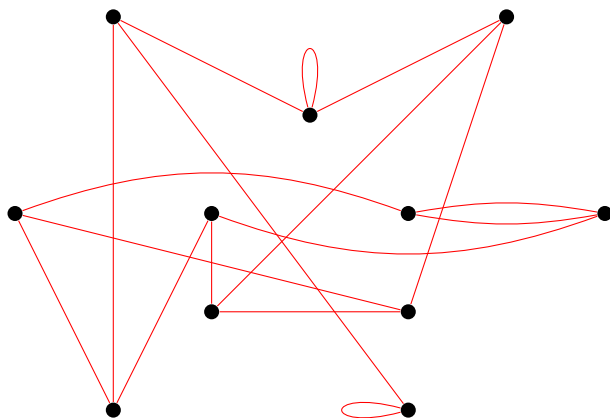
2- and **3**-isogeny graph on \mathbb{F}_{127^2}

SIDH [JD11]

Idea: **Alice** and **Bob** walk in two *different* isogeny graphs on the *same* vertex set.

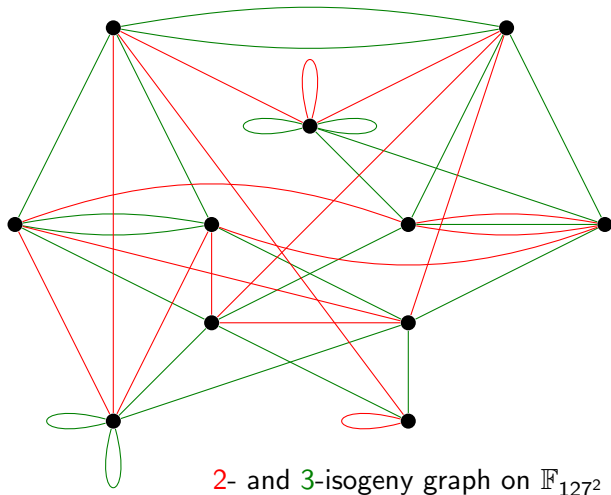


Idea: **Alice** and **Bob** walk in two *different* isogeny graphs on the *same* vertex set.



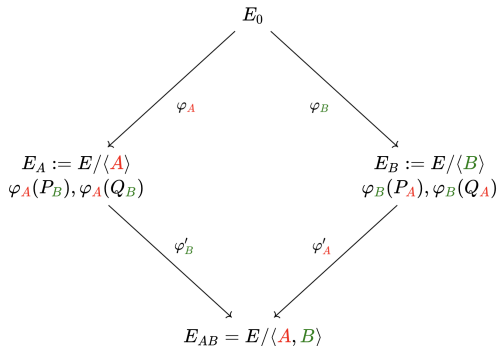
2- and 3-isogeny graph on \mathbb{F}_{127^2}

Idea: **Alice** and **Bob** walk in two *different* isogeny graphs on the *same* vertex set.



SIDH (cont.)

- Fix a prime p such that $p = N_1 N_2 - 1$, E_0/\mathbb{F}_p^2 and bases $\langle P_A, Q_A \rangle = E_0[N_1]$, $\langle P_B, Q_B \rangle = E_0[N_2]$



SIDH (cont.)

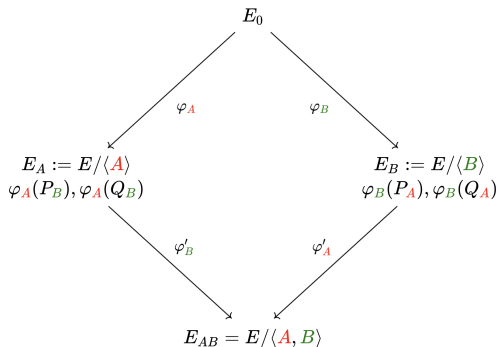
- Fix a prime p such that $p = N_1 N_2 - 1$, E_0/\mathbb{F}_p^2 and bases $\langle P_A, Q_A \rangle = E_0[N_1]$, $\langle P_B, Q_B \rangle = E_0[N_2]$

- Alice's secret is

$$A := P_A + [\text{sk}_A]Q_A$$

- Bob's secret is

$$B := P_B + [\text{sk}_B]Q_B$$



SIDH (cont.)

- Fix a prime p such that $p = N_1 N_2 - 1$, E_0/\mathbb{F}_p^2 and bases $\langle P_A, Q_A \rangle = E_0[N_1]$, $\langle P_B, Q_B \rangle = E_0[N_2]$

- Alice's secret is

$$A := P_A + [\text{sk}_A]Q_A$$

- Bob's secret is

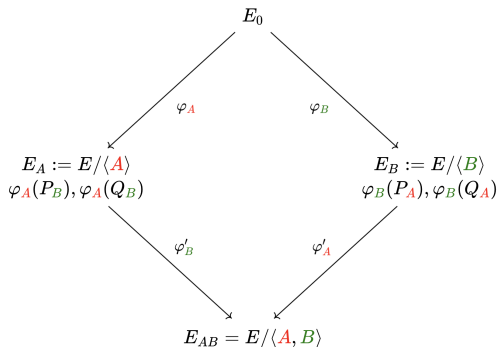
$$B := P_B + [\text{sk}_B]Q_B$$

- Alice sends

$$E_A, \varphi_A(P_B), \varphi_A(Q_B)$$

- Bob sends

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



SIDH (cont.)

- Fix a prime p such that $p = N_1 N_2 - 1$, E_0/\mathbb{F}_p^2 and bases $\langle P_A, Q_A \rangle = E_0[N_1]$, $\langle P_B, Q_B \rangle = E_0[N_2]$

- Alice's secret is

$$A := P_A + [\text{sk}_A]Q_A$$

- Bob's secret is

$$B := P_B + [\text{sk}_B]Q_B$$

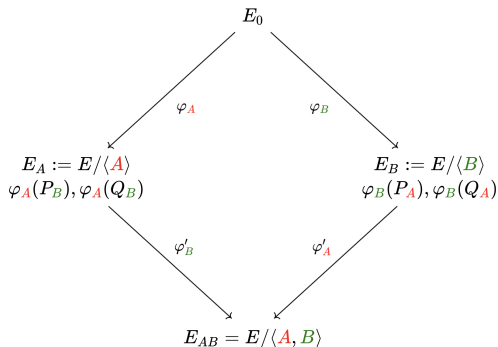
- Alice sends

$$E_A, \varphi_A(P_B), \varphi_A(Q_B)$$

- Bob sends

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

- The shared secret is the j -invariant of E_{AB}



- In SIDH the secret isogenies are relatively short
($N_1 \approx N_2 \approx \sqrt{p}$)
- Between two randomly chosen supersingular elliptic curves an isogeny of this degree does not exist in general

- In SIDH the secret isogenies are relatively short ($N_1 \approx N_2 \approx \sqrt{p}$)
- Between two randomly chosen supersingular elliptic curves an isogeny of this degree does not exist in general
- Main idea of B-SIDH: Use isogenies such that $N_1 \approx N_2 \approx p$ and $p^2 - 1 = N_1 N_2 f$
- To make this efficient, one works with curves and their twists simultaneously (torsion-points are defined over \mathbb{F}_{p^4} but all computations can be done over \mathbb{F}_{p^2})

- In SIDH the secret isogenies are relatively short ($N_1 \approx N_2 \approx \sqrt{p}$)
- Between two randomly chosen supersingular elliptic curves an isogeny of this degree does not exist in general
- Main idea of B-SIDH: Use isogenies such that $N_1 \approx N_2 \approx p$ and $p^2 - 1 = N_1 N_2 f$
- To make this efficient, one works with curves and their twists simultaneously (torsion-points are defined over \mathbb{F}_{p^4} but all computations can be done over \mathbb{F}_{p^2})
- Keys are even smaller than in SIDH but it is also slower as N_1, N_2 are less smooth

Hard problems

Definition (Pure isogeny problem)

Given two isogenous supersingular elliptic curves E_1 and E_2 , compute an isogeny $\phi : E_1 \rightarrow E_2$.

Definition (SSI-T Problem)

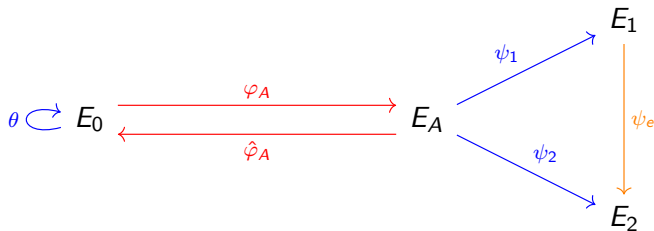
Let $\phi : E_1 \rightarrow E_2$ of degree N_1 and let $E_1[N_2] =: \langle P, Q \rangle$.
Given $E_1, E_2, \phi(P), \phi(Q)$, compute ϕ .

Torsion point attacks [Pet17, QKL⁺21]

Target: **SSI-T**, when $\text{End}(E_0)$ is known.

$\varphi_A : E_0 \rightarrow E_A$ implies

$$\mathbb{Z} + \varphi_A \circ \theta \circ \hat{\varphi}_A \hookrightarrow \text{End}(E_A)$$

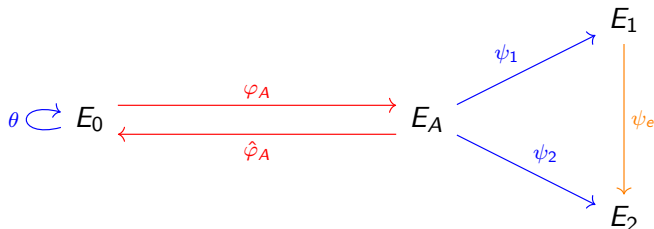


Torsion point attacks [Pet17, QKL⁺21]

Target: **SSI-T**, when $\text{End}(E_0)$ is known.

$\varphi_A : E_0 \rightarrow E_A$ implies

$$\mathbb{Z} + \varphi_A \circ \theta \circ \hat{\varphi}_A \hookrightarrow \text{End}(E_A)$$



- Consider $\tau = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ and assume $\deg(\tau) = N_2^2 e$
- Compute $\tau = \hat{\psi}_2 \circ \psi_e \circ \psi_1$ using torsion point information and small meet-in-the-middle search

Torsion point attacks (cont.)

Once $\tau = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A = \ker(\tau - [d]) \cap E_A[N_A]$$

Torsion point attacks (cont.)

Once $\tau = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A = \ker(\tau - [d]) \cap E_A[N_A]$$

To break SSI-T problem, sufficient to find d and θ such that

$$\deg([d] + \varphi_A \circ \theta \circ \hat{\varphi}_A) = N_2^2 e$$

Torsion point attacks (cont.)

Once $\tau = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A = \ker(\tau - [d]) \cap E_A[N_A]$$

To break SSI-T problem, sufficient to find d and θ such that

$$\deg([d] + \varphi_A \circ \theta \circ \hat{\varphi}_A) = N_2^2 e$$

- For $j(E_0) = 1728$, this yields norm equation

$$d^2 + N_1^2 (c^2 + p(b^2 + a^2)) = N_2^2 e$$

- Know how to find solutions when $N_2 > pN_1$.

Previous work [Pet17, QKL⁺21, KMPW21]:

- $E_0 : y^2 = x^3 + x$ or E_0 can be chosen by the adversary
- depending on E_0 unbalanced parameters (i.e. $N_2 \gg N_1$) give rise to key recovery attacks

Previous work [Pet17, QKL⁺21, KMPW21]:

- $E_0 : y^2 = x^3 + x$ or E_0 can be chosen by the adversary
- depending on E_0 unbalanced parameters (i.e. $N_2 \gg N_1$) give rise to key recovery attacks

Séta public key encryption:

- *backdoor curve* used as public parameter
- message corresponds to an isogeny from this starting curve
- ciphertext contains codomain of isogeny and torsion point images
- decryption performed using torsion point attacks

SIKE: Supersingular Isogeny Key Encapsulation

- Submission to NIST's PQ standardisation process:
 - SIKE.PKE: El Gamal-type system with IND-CPA security proof
 - SIKE.KEM: generically transformed system with IND-CCA security
- *Smallest* communication complexity for each of the security levels (1,3,5)
- *Slowest* among all proposals for each of the security levels
- <https://sike.org/>

Static-static key exchange

Can we use SIDH as a drop-in replacement for Diffie-Hellman?

- Adaptive attacks [GPST16] and [FP22]

Static-static key exchange

Can we use SIDH as a drop-in replacement for Diffie-Hellman?

- Adaptive attacks [GPST16] and [FP22]

Static-static key exchange:

- FO-transform? **X** (one party has to use ephemeral keys)

Static-static key exchange

Can we use SIDH as a drop-in replacement for Diffie-Hellman?

- Adaptive attacks [GPST16] and [FP22]

Static-static key exchange:

- FO-transform? ✗ (one party has to use ephemeral keys)
- k-SIDH [AJL17]? ✓ (very inefficient)

Static-static key exchange

Can we use SIDH as a drop-in replacement for Diffie-Hellman?

- Adaptive attacks [GPST16] and [FP22]

Static-static key exchange:

- FO-transform? ✗ (one party has to use ephemeral keys)
- k-SIDH [AJL17]? ✓ (very inefficient)
- HealSIDH [FP21]? ✓ (interactive)

Static-static key exchange

Can we use SIDH as a drop-in replacement for Diffie-Hellman?

- Adaptive attacks [GPST16] and [FP22]

Static-static key exchange:

- FO-transform? ✗ (one party has to use ephemeral keys)
- k-SIDH [AJL17]? ✓ (very inefficient)
- HealSIDH [FP21]? ✓ (interactive)
- New proofs of knowledge for SIDH keys [DDGZ21] ✓

Static-static key exchange

Can we use SIDH as a drop-in replacement for Diffie-Hellman?

- Adaptive attacks [GPST16] and [FP22]

Static-static key exchange:

- FO-transform? ✗ (one party has to use ephemeral keys)
- k-SIDH [AJL17]? ✓ (very inefficient)
- HealSIDH [FP21]? ✓ (interactive)
- New proofs of knowledge for SIDH keys [DDGZ21] ✓

Post-quantum version of Signal's initial X3DH key exchange:

- SI-X3DH [DG21] ✓

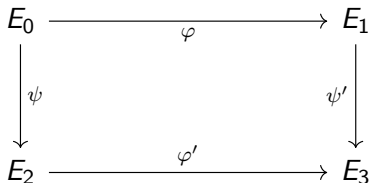
Proof of Isogeny Knowledge

Goal: Prove knowledge of secret isogeny φ of degree $\ell_1^{e_1}$.

De Feo-Jao-Plût scheme: Let $E_0[\ell_2^{e_2}] = \langle P_0, Q_0 \rangle$. (E_0, P_0, Q_0) are public parameters and $(E_1, \varphi(P_0), \varphi(Q_0))$ are the public key.

1 Prover generates randomly $\ell_2^{e_2}$ -torsion point

$K_\psi := [a]P_0 + [b]Q_0$ corresponding to $\psi : E_0 \rightarrow E_2$



and commits to E_2 and E_3 .

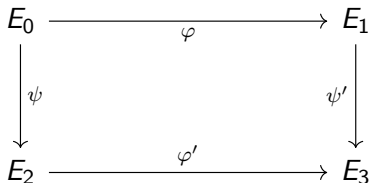
Proof of Isogeny Knowledge

Goal: Prove knowledge of secret isogeny φ of degree $\ell_1^{e_1}$.

De Feo-Jao-Plût scheme: Let $E_0[\ell_2^{e_2}] = \langle P_0, Q_0 \rangle$. (E_0, P_0, Q_0) are public parameters and $(E_1, \varphi(P_0), \varphi(Q_0))$ are the public key.

- 1 Prover generates randomly $\ell_2^{e_2}$ -torsion point

$K_\psi := [a]P_0 + [b]Q_0$ corresponding to $\psi : E_0 \rightarrow E_2$



and commits to E_2 and E_3 .

- 2 Verifier challenges the prover with a random bit $c \leftarrow \{0, 1\}$
- 3 Prover reveals (a, b) , if $c = 0$, and $\psi(\ker(\varphi))$, if $c = 1$.

Proof of Isogeny Knowledge (cont.)

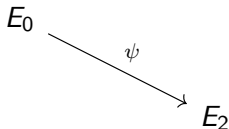
Soundness issue of De Feo-Jao-Plût scheme [DDGZ21]:

$$E_0$$

Proof of Isogeny Knowledge (cont.)

Soundness issue of De Feo-Jao-Plût scheme [DDGZ21]:

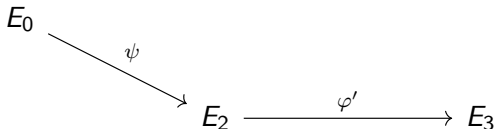
- Prover generates randomly $\ell_2^{e_2}$ -torsion point
 $K_\psi := [a]P_0 + [b]Q_0$ corresponding to $\psi : E_0 \rightarrow E_2$



Proof of Isogeny Knowledge (cont.)

Soundness issue of De Feo-Jao-Plût scheme [DDGZ21]:

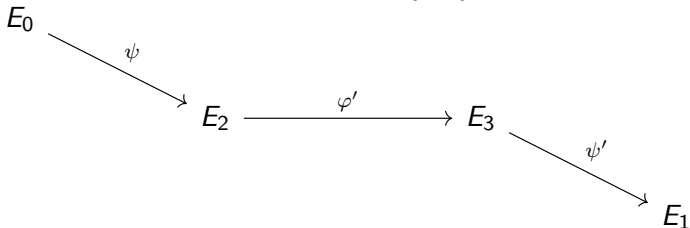
- Prover generates randomly $\ell_2^{e_2}$ -torsion point $K_\psi := [a]P_0 + [b]Q_0$ corresponding to $\psi : E_0 \rightarrow E_2$
- Prover generates randomly $\varphi' : E_2 \rightarrow E_3$ of degree $\ell_1^{e_1}$



Proof of Isogeny Knowledge (cont.)

Soundness issue of De Feo-Jao-Plût scheme [DDGZ21]:

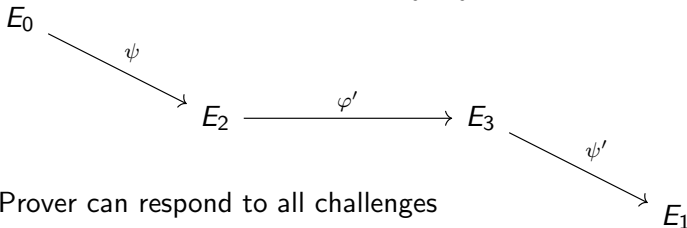
- Prover generates randomly $\ell_2^{e_2}$ -torsion point $K_\psi := [a]P_0 + [b]Q_0$ corresponding to $\psi : E_0 \rightarrow E_2$
- Prover generates randomly $\varphi' : E_2 \rightarrow E_3$ of degree $\ell_1^{e_1}$
- Prover generates random isogeny $\psi' : E_3 \rightarrow E_1$ of degree $\ell_2^{e_2}$ and picks P'_0, Q'_0 such that $\ker(\hat{\psi}') = [a]P'_0 + [b]Q'_0$
- Prover publishes public key (E_1, P'_0, Q'_0)



Proof of Isogeny Knowledge (cont.)

Soundness issue of De Feo-Jao-Plût scheme [DDGZ21]:

- Prover generates randomly $\ell_2^{e_2}$ -torsion point $K_\psi := [a]P_0 + [b]Q_0$ corresponding to $\psi : E_0 \rightarrow E_2$
- Prover generates randomly $\varphi' : E_2 \rightarrow E_3$ of degree $\ell_1^{e_1}$
- Prover generates random isogeny $\psi' : E_3 \rightarrow E_1$ of degree $\ell_2^{e_2}$ and picks P'_0, Q'_0 such that $\ker(\hat{\psi}') = [a]P'_0 + [b]Q'_0$
- Prover publishes public key (E_1, P'_0, Q'_0)

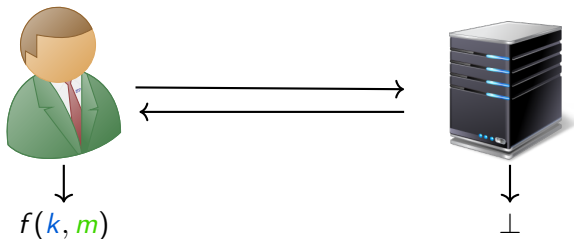


- Prover can respond to all challenges
- Isogeny $E_0 \rightarrow E_1$ of degree $\ell_1^{e_1}$ will not exist in general

Oblivious Pseudorandom Function (OPRF)

An OPRF is a two-party protocol to evaluate a PRF $f(k, m)$ where:

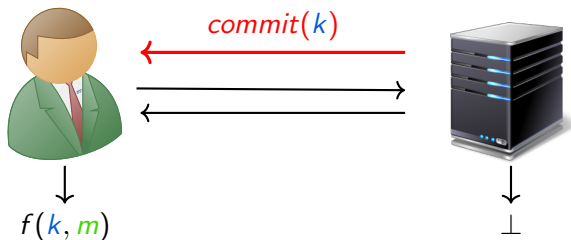
- The **client** learns $f(k, m)$, one evaluation of a PRF on a chosen input
- The **server** learns nothing about m



Oblivious Pseudorandom Function (OPRF)

An OPRF is a two-party protocol to evaluate a PRF $f(k, m)$ where:

- The **client** learns $f(k, m)$, one evaluation of a PRF on a chosen input
- The **server** learns nothing about m



- An OPRF is called *verifiable*, if the **server** proves to the **client** that output was computed using the key k

Existing Constructions

Parameters: group \mathbb{G} of order q , hash functions H_1, H_2 onto \mathbb{G} and $\{0, 1\}^\ell$ resp.

Client $C(m)$

Server $S(k)$

Pick $r \leftarrow_R \mathbb{Z}_q$
Set $a \leftarrow (H_1(m))^r$

\xrightarrow{a}

If $a \in \mathbb{G}$, set $b \leftarrow a^k$

\xleftarrow{b}

If $b \in \mathbb{G}$, set $v \leftarrow b^{1/r}$
Output $H_2(m, v)$

Existing Constructions

Parameters: group \mathbb{G} of order q , hash functions H_1, H_2 onto \mathbb{G} and $\{0, 1\}^\ell$ resp.

Client $C(m)$

Server $S(k)$

Pick $r \leftarrow_R \mathbb{Z}_q$
Set $a \leftarrow (H_1(m))^r$

\xrightarrow{a}

If $a \in \mathbb{G}$, set $b \leftarrow a^k$

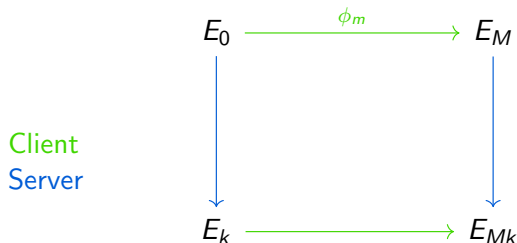
\xleftarrow{b}

If $b \in \mathbb{G}$, set $v \leftarrow b^{1/r}$
Output $H_2(m, v)$

Post-quantum OPRF:

- Construction from lattices [ADDs19]
- Construction from isogenies [BKW20]

Oblivious Pseudorandom Functions from Isogenies [BKW20]



Oblivious Pseudorandom Functions from Isogenies [BKW20]

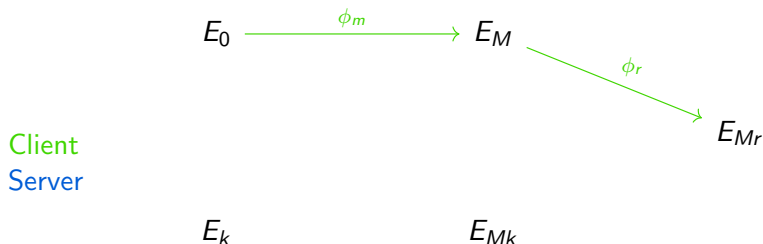
$$E_0 \xrightarrow{\phi_m} E_M$$

Client
Server

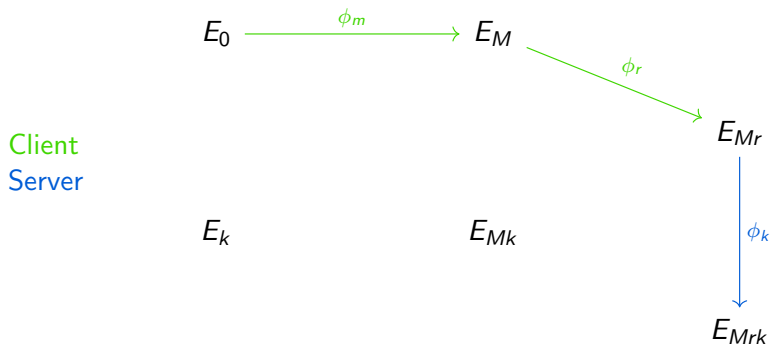
E_k

E_{Mk}

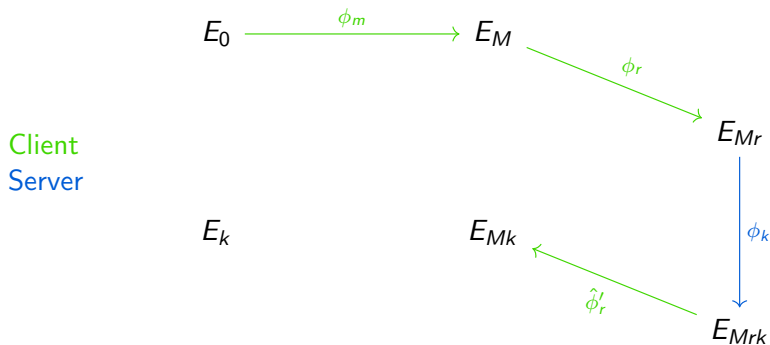
Oblivious Pseudorandom Functions from Isogenies [BKW20]



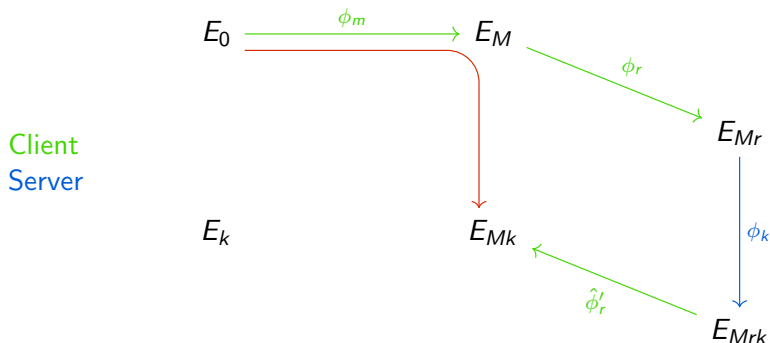
Oblivious Pseudorandom Functions from Isogenies [BKW20]



Oblivious Pseudorandom Functions from Isogenies [BKW20]

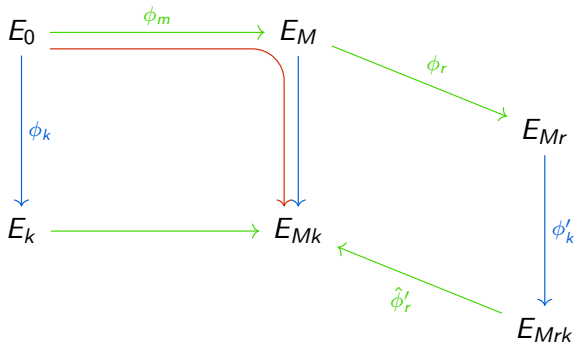


Oblivious Pseudorandom Functions from Isogenies [BKW20]



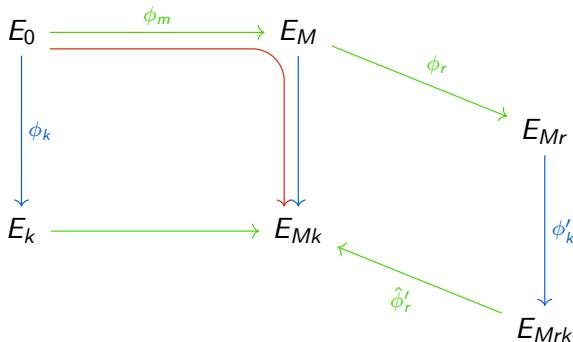
$$f(k, m) = H(m, j(E_{Mk}), \text{pk})$$

Attacking the Pseudorandomness [BKM⁺21]



- Use queries to the OPRF to obtain E_k and $\phi_k(E_0[2^n])$ up to scalar multiplication

Attacking the Pseudorandomness [BKM⁺21]



- Use queries to the OPRF to obtain E_k and $\phi_k(E_0[2^n])$ up to scalar multiplication
- Given $P \in E_0[2^n]$, compute $\langle \phi_k(P) \rangle$ and $E_k / \langle \phi_k(P) \rangle = E_{Pk}$

Updateable Public-Key Encryption

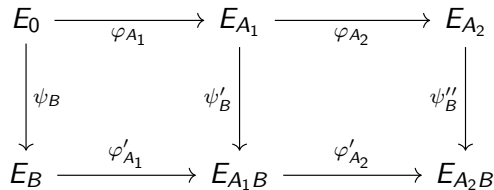
Desired properties:

- Correctness
- Forward secrecy
- Post-compromise security
- Asynchronicity
- Key indistinguishability

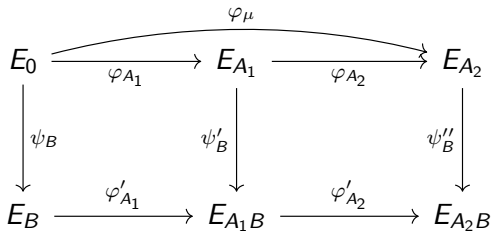
Updateable Public-Key Encryption from SIDH [EJKM20]

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_{A_1}} & E_{A_1} \\ \downarrow \psi_B & & \downarrow \psi'_B \\ E_B & \xrightarrow{\varphi'_{A_1}} & E_{A_1 B} \end{array}$$

Updateable Public-Key Encryption from SIDH [EJKM20]

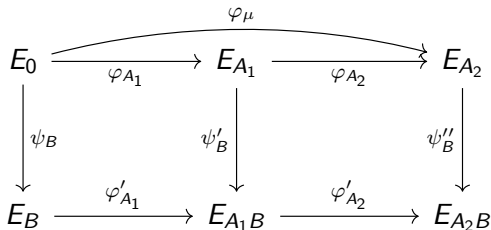


Updateable Public-Key Encryption from SIDH [EJKM20]



Idea: Use [KLPT14] to compute φ_μ from $\varphi_{A_2} \circ \varphi_{A_1}$ to achieve post-compromise security and forward secrecy

Updateable Public-Key Encryption from SIDH [EJKM20]



Idea: Use [KLPT14] to compute φ_μ from $\varphi_{A_2} \circ \varphi_{A_1}$ to achieve post-compromise security and forward secrecy

Caveats:

- Very unbalanced parameters
- No asynchronicity
- No key indistinguishability

Conclusion

- SIDH has small keys and is reasonably fast
- Some advanced cryptographic protocols from SIDH exist
- Many subtle issues when building schemes from SIDH
- Further work is required:
 - Find new isogeny-based protocols
 - Remove limitations of existing constructions
(e.g. sample supersingular elliptic curves without revealing their endomorphism ring)
 - Cryptanalyse existing constructions

References

- [AJL17] Reza Azarderakhsh, David Jao, and Christopher Leonardi. Post-quantum static-static key agreement using multiple protocol instances. In *International Conference on Selected Areas in Cryptography*, pages 45–63. Springer, 2017.
- [BKM⁺21] Andrea Basso, Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Antonio Sanso. Cryptanalysis of an oblivious prf from supersingular isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 160–184. Springer, 2021.
- [BKW20] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, pages 520–550, 2020.
- [Cos19] Craig Costello. B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion. Technical report, Cryptology ePrint Archive, Report 2019/1145, 2019. <https://eprint.iacr.org/2019/1145>, 2019.
- [DDF⁺21] Luca De Feo, Cyprien Delpech de Saint Guilhem, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Christophe Petit, Javier Silva, and Benjamin Wesolowski. Séta: Supersingular encryption from torsion attacks. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 249–278. Springer, 2021.

References (cont.)

- [DDGZ21] Luca De Feo, Samuel Dobson, Steven D Galbraith, and Lukas Zobernig. Sidh proof of knowledge. *Cryptology ePrint Archive*, 2021.
- [DG21] Samuel Dobson and Steven D Galbraith. Post-quantum signal key agreement with sidh. *Cryptology ePrint Archive*, 2021.
- [EJKM20] Edward Eaton, David Jao, Chelsea Komlo, and Youcef Mokrani. Towards post-quantum updatable public-key encryption via supersingular isogenies. *Cryptology ePrint Archive*, 2020.
- [FP21] Tako Boris Fouotsa and Christophe Petit. Sheals and heals: isogeny-based pkes from a key validation method for sidh. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 279–307. Springer, 2021.
- [FP22] Tako Boris Fouotsa and Christophe Petit. A new adaptive attack on sidh. In *Cryptographers' Track at the RSA Conference*, pages 322–344. Springer, 2022.
- [GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in Cryptology - ASIACRYPT 2016*, pages 63–91, 2016.
- [JD11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

References (cont.)

- [KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ -isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.
- [KMPW21] Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Charlotte Weitkämper. One-way functions and malleability oracles: Hidden shift attacks on isogeny-based protocols. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 242–271. Springer, 2021.
- [Pet17] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In *Advances in Cryptology - ASIACRYPT 2017*, pages 330–353, 2017.
- [QKL⁺21] Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E Stange. Improved torsion-point attacks on sidh variants. In *Annual International Cryptology Conference*, pages 432–470. Springer, 2021.