Commitment schemes from isogeny assumptions

by Bruno Sterner

presented by

Eduarda Assunção, Valerio Ardizio, Parsa Tasbihgou

École Polytechnique Fédérale de Lausanne, Switzerland

May 5th 2024

EPFL

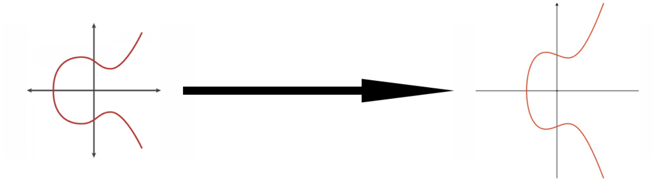
Outline

Introduction

- Post-quantum protocols are still being designed and refined.
- Isogeny-based cryptography has been promising, but still does not have every cryptographic primitive designed.
- Bruno Sterner's paper proposes the first *provably secure* isogeny-based **commitment schemes**.

Supersingular Elliptic Curve Isogenies

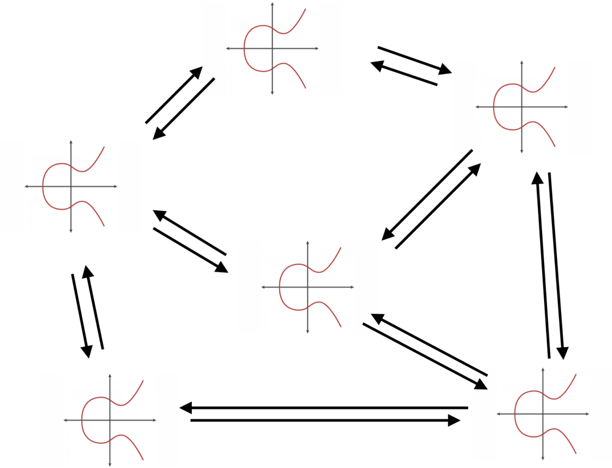
- So what is an isogeny? A function $\phi : E_{start} \longrightarrow E_{end}$



A bit more than that, an isogeny is a **homomorphism**.

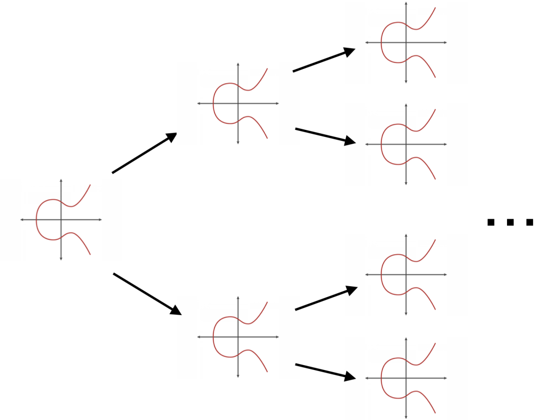
- An ℓ-isogeny is an isogeny where each point has ℓ pre-images

Let's make a graph out of this



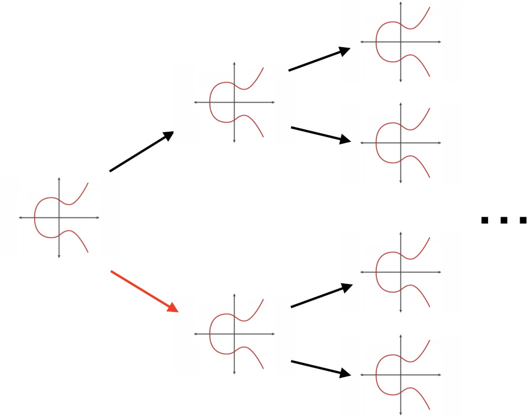
Walking the Isogeny Graph

We can walk the graph. How? Follow the message piece by piece.
Let $m = 01\ldots$



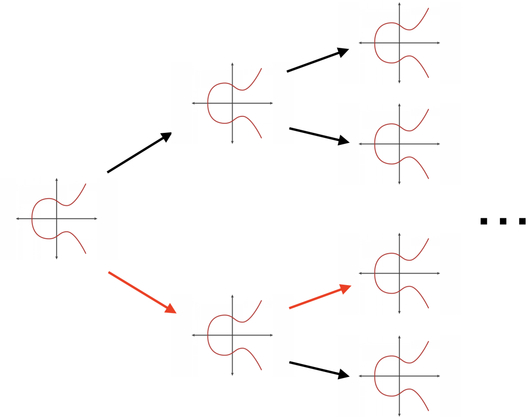
Walking the Isogeny Graph

We can walk the graph. How? Follow the message piece by piece.
Let $m = 01\ldots$
Consider $m_0 = 0$

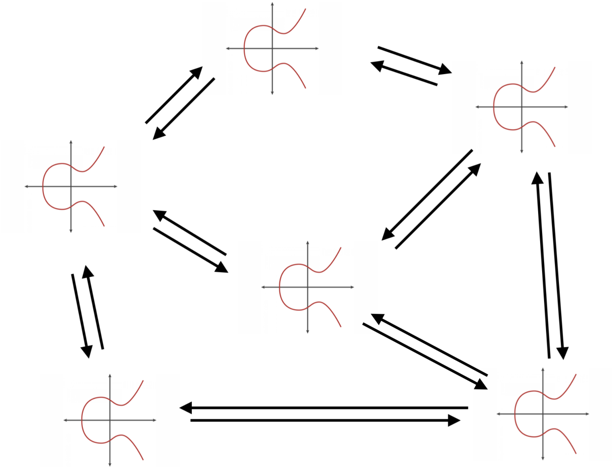


Walking the Isogeny Graph

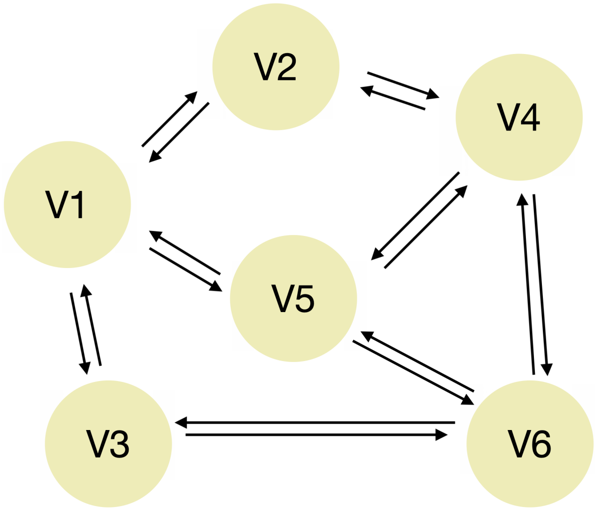
We can walk the graph. How? Follow the message piece by piece.
Let $m = 01\ldots$
Then consider $m_1 = 1$



Mixing Constant

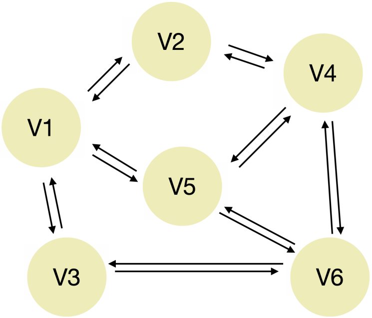


Mixing Constant



Mixing Constant

If we finished in V6, where did we come from?



Assume we finished in V6, **and we only walked one step**.
Where did we come from?

Mixing Constant

We define the mixing constant k_G to be the **minimum** amount of steps so that every two vertices are connected.

We can no longer exclude possibilities if we walk k_G steps.

More than that! It is known that isogeny graphs, which are Ramanujan graphs, have **good mixing properties**.

A random walk with k_G steps gives us a distribution of end-points very close to **uniform**.

Information-theoretically hiding!

Commitment Schemes

A commitment scheme consists of three algorithms:

- **KeyGen** $\longrightarrow$ public parameters
- **Commit**$(m, pp) \longrightarrow c, r$
- **Open**$(m, r, c, pp) \longrightarrow 0/1$

And two security notions that have to be met

- **Hiding**: c does not reveal 'anything' about m
  reveals at most a negligible amount of information
- **Binding**: hard to create $c(m_1, r_1) = c(m_2, r_2)$ where $m_1 \neq m_2$

Commitment Schemes

A commitment scheme consists of three algorithms:

- **KeyGen** $\longrightarrow$ public parameters
- **Commit**$(m, pp) \longrightarrow c, r$
- **Open**$(m, r, c, pp) \longrightarrow 0/1$

And two security notions that have to be met

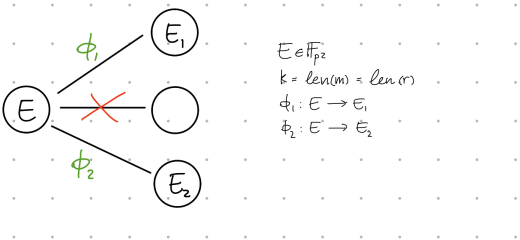
- **Information-Theoretic Hiding**: c reveals 'nothing' about m to an adversary with unbounded computational power
- **Computational Binding**: hard to create $c(m_1, r_1) = c(m_2, r_2)$ where $m_1 \neq m_2$ to an adversary with a probabilistic polynomial-time algorithm

A commitment scheme from isogeny assumptions

- Goals:
  1. Achieve *information-theoretic hiding*.
  2. Achieve *computational binding*.
- The scheme is built on a supersingular 2-isogeny graph.
- Hiding property of the scheme:
  1. *Supersingular elliptic curve isogeny graphs* are instances of Ramanujan graphs which means they mix well.
  2. Only *non-backtracking* random walks.
  3. Low mixing constant $\implies$ better scheme's performance
- Binding property of the scheme:
  - Finding an endomorphism is hard for a *supersingular elliptic curve*.

The scheme – **KeyGen**

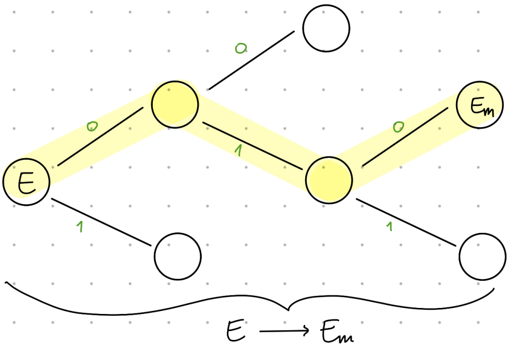
- Overview of the scheme – 3 algorithms:
  1. $(p, E, k, \phi_1, \phi_2) \leftarrow$ **KeyGen**(λ)
  2. $(c, r) \leftarrow$ **Commit**$(m, p, E, \phi_1, \phi_2)$
  3. `bool` $\leftarrow$ **Open**$(m, c, r, E, \phi_1, \phi_2)$



The scheme – **Commit**

- Overview of the scheme – 3 algorithms:
  1. $(p, E, k, \phi_1, \phi_2) \leftarrow$ **KeyGen**(λ)
  2. $(c, r) \leftarrow$ **Commit**$(m, p, E, \phi_1, \phi_2)$
  3. $\texttt{bool} \leftarrow$ **Open**$(m, c, r, E, \phi_1, \phi_2)$

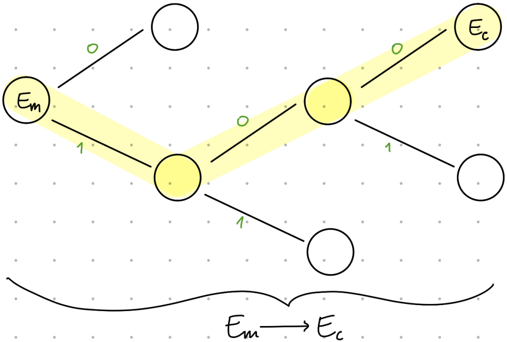
$m \in \{0,1\}^k$, $m = 010$



The scheme – **Commit**

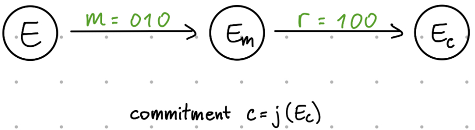
- Overview of the scheme – 3 algorithms:
  1. $(p, E, k, \phi_1, \phi_2) \leftarrow$ **KeyGen**(λ)
  2. $(c, r) \leftarrow$ **Commit**$(m, p, E, \phi_1, \phi_2)$
  3. `bool` $\leftarrow$ **Open**$(m, c, r, E, \phi_1, \phi_2)$

$r \in \{0,1\}^k, \quad r = 100$



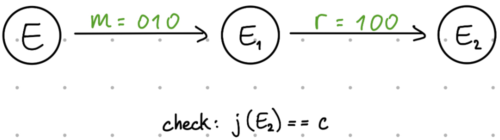
The scheme – **Commit**

- Overview of the scheme – 3 algorithms:
  1. $(p, E, k, \phi_1, \phi_2) \leftarrow$ **KeyGen**(λ)
  2. $(c, r) \leftarrow$ **Commit**$(m, p, E, \phi_1, \phi_2)$
  3. `bool` $\leftarrow$ **Open**$(m, c, r, E, \phi_1, \phi_2)$



The scheme – **Open**

- Overview of the scheme – 3 algorithms:
  1. $(p, E, k, \phi_1, \phi_2) \leftarrow \textbf{KeyGen}(\lambda)$
  2. $(c, r) \leftarrow \textbf{Commit}(m, p, E, \phi_1, \phi_2)$
  3. $\texttt{bool} \leftarrow \textbf{Open}(m, c, r, E, \phi_1, \phi_2)$



Hiding property

Prove that the commitment scheme is *information-theoretically hiding*:

Theorem (Random walks)

Given a prime number p, let j_0 be a supersingular j-invariant in characteristic p, N_p be the number of supersingular j-invariants in characterstic p and $n = \prod_i \ell_i^{e_i}$ be an integer where ℓ_i are small primes. Let $\hat{j}$ be the j-invariant reached by a random walk of degree n starting at j_0. Then for every j-invariant $\tilde{j}$ we have

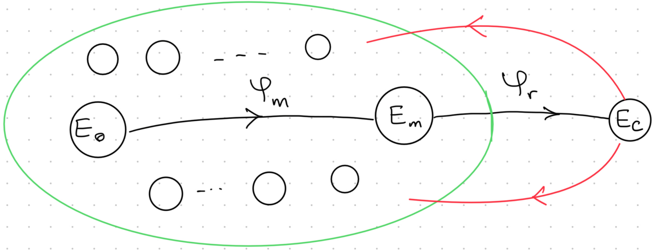
$$\left| \mathbb{P}\left[\hat{j} = \tilde{j}\right] - \frac{1}{N_p} \right| \leq \prod_i \left(\frac{2\sqrt{\ell_i}}{\ell_i + 1} \right)^{e_i}$$

Hiding property

Prove that the commitment scheme is *information-theoretically hiding*:

Theorem (Random walks)

For any random walk of degree n, the probability of ending on any node of the supersingular isogeny graph is close to uniform for a sufficiently long walk.



Hiding property – Conjectured number of steps

We have to walk at least a minimum number of steps to have proper mixing (hiding property).

What is this minimum?

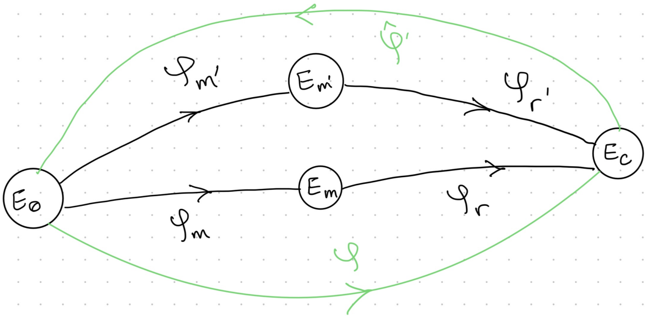
The author conjectures that it is $4\log(p)$.

Binding property

Problem (Supersingular Endomorphism Problem)

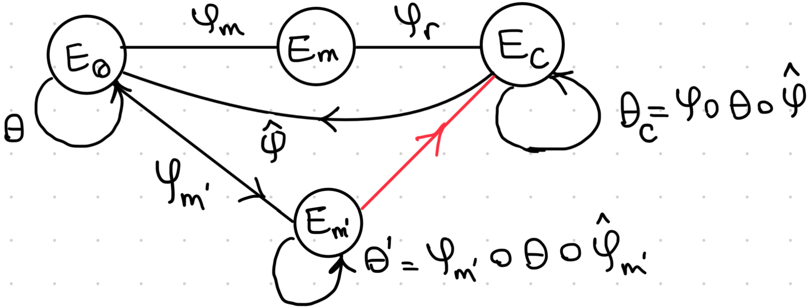
Given a prime p, a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ and a small prime ℓ, it is hard to compute a non-trivial cyclic endomorphism[a] of E whose degree is a prime power ℓ^e.

[a] An endomorphism is *non-trivial* if it is **not** a multiplication-by-m map, i.e. $[m]$, and *cyclic* if the endomorphism has a cyclic kernel.



Binding property – Trusted Third Party

- We want the endomorphism ring of E_0 to remain **unknown**
- If endomorphism ring of E_0 is known $\implies$ Break binding property!



Commitment using the SIDH approach

- We want to get the isogeny ϕ_t
- We can speedup the E_t computation using the SIDH framework
- We know we can define an isogeny by its kernel
- We want the kernel of ϕ_t
- How do we get the kernel?
- Let $p = 2^n f - 1$ be the characteristic of the field.
- There is a subgroup $E[2^n] \simeq (\mathbb{Z}_{2^n})^2$
- Let $\{P, Q\}$ be a basis for $E[2^n]$ and $t \in \mathbb{Z}_{2^n}$, then $\langle P + tQ \rangle$ is a cyclic subgroup and is the kernel of ϕ_t.

$$\begin{tikzcd} E_0 \arrow[r, bend right] & E_t \end{tikzcd}$$

$$deg\phi_t = 2^n$$

4 steps

- The longest isogeny walk that can be specified by its kernel has length n (degree 2^n) and $n \simeq \log(p)$ but as we saw we need a walk of length $k \simeq 4\log(p)$.
- Solution: repeat the isogeny walk 4 times. $\phi_t(Q)$ has order 2^n but we need another full order point to have a basis and we need to generate this point deterministically so the commitment can be opened.
- Use "Elligator 2" to compute deterministic point $R \in E(\mathbb{F}_{p^2})$ then check R is not divisible by 2. fR is a full order point and $\{\phi_t(Q), fR\}$ is a basis for $E_t(\mathbb{F}_{p^2})$.

$$\begin{tikzcd} E_0 \arrow[r, "\phi_{m_0}"] \arrow[rrrr, bend left, "\phi_m"] & E_{m_0} \arrow[r, "\phi_{m_1}"] & E_{m_1} \arrow[r, "\phi_{m_2}"] & E_{m_2} \arrow[r, "\phi_{m_3}"] & E_{m_3} \end{tikzcd}$$

SIDH vs. CGL

The SIDH variant is exponentially faster than CGL.

- Evaluation of the CGL hash function takes $kn(5.7n + 110)$ multiplications in $\mathbb{F}_{p^2}$.
- Evaluation of the SIDH variant takes $kn(13.5\log(n) + 42.4)$ multiplications in $\mathbb{F}_{p^2}$.
- The SIDH variant has to compute a new basis 3 times which takes $O(n)$ multiplications so it is not a dominant computation.
- The ratio of computation time of CGL to SIDH is $\frac{5.7n+110}{13.5\log(n)+42.4} \simeq O(\frac{n}{\log(n)})$

Commitment size

Very small commitment size compared to other post-quantum candidates

- Output is a single element in $\mathbb{F}_{p^2}$. When $\mathbb{F}_{p^2}$ is seen as a 2-dimensional extension of $\mathbb{F}_p$, output is two elements in $\mathbb{F}_p$.
- If λ is the security parameter, a prime of size 2λ should be used. The commitment size is 4λ.
- For 128-bit security the commitment size will be
  1. 64B in SIDH/CGL
  2. 9kB in known lattice-based schemes

Thank you for your attention.

Questions?