Improved Digital Signatures Based on Elliptic Curve Endomorphism Rings

Xiu Xu [3,4,5] **Christopher Leonardi** [1] Anzo Teh[1] David Jao [1,2]
Kunpeng Wang [3,4,5] Wei Yu [3,4,5] Reza Azarderakhsh [6]

[1] Department of Combinatorics and Optimization, University of Waterloo

[2] evolutionQ, Inc., Waterloo, Ontario, Canada

[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

[4] Data Assurance and Communications Security Research Center, Beijing, China

[5] School of Cyber Security, University of Chinese Academy of Sciences

[6] Department of Computer and Electrical Engineering and Computer Science, Florida Atlantic University

1. Introduction

2. Digital Signature Scheme
   - Elliptic Curve Background
   - GPS Signatures

3. Our Improvements
   - #1: Isogeny-to-Ideal
   - #2: Ideal-to-Isogeny
   - #3: Parallel Instances
   - Performance

4. Conclusion

- Topic of discussion: Galbraith-Petit-Silva digital signature scheme (AsiaCrypt 2017).

- Topic of discussion: Galbraith-Petit-Silva digital signature scheme (AsiaCrypt 2017).

- Implementations are not widely available because:
  – one subroutine is mathematically complicated, and
  – signing would be too inefficient to be practical.

- Topic of discussion: Galbraith-Petit-Silva digital signature scheme (AsiaCrypt 2017).
- Implementations are not widely available because:
  – one subroutine is mathematically complicated, and
  – signing would be too inefficient to be practical.
- Our work presents three major ways to improve efficiency, and implements the scheme in SAGE.

- **Elliptic curve** $E : y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_{p^n}$ is a finite Abelian group (operation is "+", identity is ∞).

- **Elliptic curve** $E : y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_{p^n}$ is a finite Abelian group (operation is "+", identity is ∞).

- The m-**torsion** subgroup $E[m] = \{P \in E(\overline{\mathbb{F}}_p) : [m]P = \infty\}$.

- **Elliptic curve** $E : y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_{p^n}$ is a finite Abelian group (operation is "+", identity is ∞).
- The m-**torsion** subgroup $E[m] = \{P \in E(\overline{\mathbb{F}}_p) : [m]P = \infty\}$.
- If $\forall r \in \mathbb{N}, E[p^r] = \{\infty\}$, then E is called **supersingular**. Otherwise $\forall r \in \mathbb{N}, E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ and is called **ordinary**.

- **Elliptic curve** $E : y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_{p^n}$ is a finite Abelian group (operation is "+", identity is ∞).
- The m-**torsion** subgroup $E[m] = \{P \in E(\overline{\mathbb{F}}_p) : [m]P = \infty\}$.
- If $\forall r \in \mathbb{N}, E[p^r] = \{\infty\}$, then E is called **supersingular**. Otherwise $\forall r \in \mathbb{N}, E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ and is called **ordinary**.
- The j-**invariant** is a unique element of $\mathbb{F}_{p^n}$ associated to each $\overline{\mathbb{F}}_{p^n}$-isomorphism family of elliptic curves.

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

- **Elliptic curve** $E : y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_{p^n}$ is a finite Abelian group (operation is "+", identity is ∞).
- The m-**torsion** subgroup $E[m] = \{P \in E(\overline{\mathbb{F}}_p) : [m]P = \infty\}$.
- If $\forall r \in \mathbb{N}, E[p^r] = \{\infty\}$, then E is called **supersingular**. Otherwise $\forall r \in \mathbb{N}, E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ and is called **ordinary**.
- The j-**invariant** is a unique element of $\mathbb{F}_{p^n}$ associated to each $\overline{\mathbb{F}}_{p^n}$-isomorphism family of elliptic curves.

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

- Supersingular elliptic curves are always defined over $\mathbb{F}_{p^2}$.

- **Isogenies** are rational morphisms between elliptic curves, and have associated degrees.

- **Isogenies** are rational morphisms between elliptic curves, and have associated degrees.

$$\text{e.g. } E(\mathbb{F}_{23}) : y^2 = x^3 + x,\ E'(\mathbb{F}_{23}) : y^2 = x^3 + 13$$

$$\phi : E(\mathbb{F}_{23}) \to E'(\mathbb{F}_{23}),\ \deg(\phi) = 3$$

$$\phi(x, y) = \left(\frac{x^3 + 10x^2 + 16x + 10}{x^2 + 10x + 2}, \frac{(x^3 + 15x^2 + 15x + 14)y}{x^3 + 15x^2 + 6x + 10} \right)$$

- **Isogenies** are rational morphisms between elliptic curves, and have associated degrees.

$$\text{e.g. } E(\mathbb{F}_{23}) : y^2 = x^3 + x,\ E'(\mathbb{F}_{23}) : y^2 = x^3 + 13$$

$$\phi : E(\mathbb{F}_{23}) \to E'(\mathbb{F}_{23}),\ \deg(\phi) = 3$$

$$\phi(x, y) = \left(\frac{x^3 + 10x^2 + 16x + 10}{x^2 + 10x + 2}, \frac{(x^3 + 15x^2 + 15x + 14)y}{x^3 + 15x^2 + 6x + 10} \right)$$

- Isogenies can be composed: if $\phi : E_1 \to E_2$ has degree d_1, and $\psi : E_2 \to E_3$ has degree d_2, then $\psi \circ \phi : E_1 \to E_3$ has degree $d_1 d_2$.

- **Isogenies** are rational morphisms between elliptic curves, and have associated degrees.

$$\text{e.g. } E(\mathbb{F}_{23}) : y^2 = x^3 + x,\ E'(\mathbb{F}_{23}) : y^2 = x^3 + 13$$

$$\phi : E(\mathbb{F}_{23}) \to E'(\mathbb{F}_{23}),\ \deg(\phi) = 3$$

$$\phi(x, y) = \left(\frac{x^3 + 10x^2 + 16x + 10}{x^2 + 10x + 2}, \frac{(x^3 + 15x^2 + 15x + 14)y}{x^3 + 15x^2 + 6x + 10} \right)$$

- Isogenies can be composed: if $\phi : E_1 \to E_2$ has degree d_1, and $\psi : E_2 \to E_3$ has degree d_2, then $\psi \circ \phi : E_1 \to E_3$ has degree $d_1 d_2$.
- The **endomorphism ring** of an elliptic curve, $\mathrm{End}(E)$, is the (non-commutative) ring of all isogenies from E to itself.

- **Isogenies** are rational morphisms between elliptic curves, and have associated degrees.

$$\text{e.g. } E(\mathbb{F}_{23}) : y^2 = x^3 + x,\ E'(\mathbb{F}_{23}) : y^2 = x^3 + 13$$

$$\phi : E(\mathbb{F}_{23}) \to E'(\mathbb{F}_{23}),\ \deg(\phi) = 3$$

$$\phi(x, y) = \left(\frac{x^3 + 10x^2 + 16x + 10}{x^2 + 10x + 2}, \frac{(x^3 + 15x^2 + 15x + 14)y}{x^3 + 15x^2 + 6x + 10} \right)$$

- Isogenies can be composed: if $\phi : E_1 \to E_2$ has degree d_1, and $\psi : E_2 \to E_3$ has degree d_2, then $\psi \circ \phi : E_1 \to E_3$ has degree $d_1 d_2$.
- The **endomorphism ring** of an elliptic curve, $\mathrm{End}(E)$, is the (non-commutative) ring of all isogenies from E to itself.
- Right ideals of $\mathrm{End}(E)$ are associated to isogenies with domain E.

- **Isogenies** are rational morphisms between elliptic curves, and have associated degrees.

$$\text{e.g. } E(\mathbb{F}_{23}) : y^2 = x^3 + x,\ E'(\mathbb{F}_{23}) : y^2 = x^3 + 13$$

$$\phi : E(\mathbb{F}_{23}) \to E'(\mathbb{F}_{23}),\ \deg(\phi) = 3$$

$$\phi(x, y) = \left(\frac{x^3 + 10x^2 + 16x + 10}{x^2 + 10x + 2}, \frac{(x^3 + 15x^2 + 15x + 14)y}{x^3 + 15x^2 + 6x + 10} \right)$$

- Isogenies can be composed: if $\phi : E_1 \to E_2$ has degree d_1, and $\psi : E_2 \to E_3$ has degree d_2, then $\psi \circ \phi : E_1 \to E_3$ has degree $d_1 d_2$.
- The **endomorphism ring** of an elliptic curve, $\mathrm{End}(E)$, is the (non-commutative) ring of all isogenies from E to itself.
- Right ideals of $\mathrm{End}(E)$ are associated to isogenies with domain E.
- Knowledge of an elliptic curve's endomorphism ring can be used as Trapdoor Information.

Hard and Easy Problems with Isogenies

Consider a supersingular $E(\mathbb{F}_{p^2})$, and a hash function H which outputs isogenies with domain E.

	End(E) known	End(E) unknown
Preimage resistant	✓	✓
2^{nd} Preimage resistant	X	✓
Collision resistant	X	✓

Easy Problems Hard Problems Let $E(\mathbb{F}_{p^2})$ be a supersingular elliptic curve.

- Given E, compute an arbitrary isogeny with domain E and smooth degree (e.g. 2^m).

[1] Kohel, Lauter, Petit, Tignol "On the quaternion ℓ-isogeny path problem", 2014.

Easy Problems Hard Problems Let $E(\mathbb{F}_{p^2})$ be a supersingular elliptic curve.

- Given E, compute an arbitrary isogeny with domain E and smooth degree (e.g. 2^m).
- Given E and $E'(\mathbb{F}_{p^2})$, find an isogeny from E to E'.

[1] Kohel, Lauter, Petit, Tignol "On the quaternion ℓ-isogeny path problem", 2014.

Easy Problems Hard Problems Let $E(\mathbb{F}_{p^2})$ be a supersingular elliptic curve.

- Given E, compute an arbitrary isogeny with domain E and smooth degree (e.g. 2^m).
- Given E and $E'(\mathbb{F}_{p^2})$, find an isogeny from E to E'.
- Given E, $E'(\mathbb{F}_{p^2})$, $\mathrm{End}(E)$, and $\mathrm{End}(E')$, and $d \in \mathbb{N}$, find an isogeny from E to E' of degree d. [1]

[1] Kohel, Lauter, Petit, Tignol "On the quaternion ℓ-isogeny path problem", 2014.

Easy Problems Hard Problems Let $E(\mathbb{F}_{p^2})$ be a supersingular elliptic curve.

- Given E, compute an arbitrary isogeny with domain E and smooth degree (e.g. 2^m).
- Given E and $E'(\mathbb{F}_{p^2})$, find an isogeny from E to E'.
- Given E, $E'(\mathbb{F}_{p^2})$, $\mathrm{End}(E)$, and $\mathrm{End}(E')$, and $d \in \mathbb{N}$, find an isogeny from E to E' of degree d. [1]
- Given E, $E'(\mathbb{F}_{p^2})$, and $\mathrm{End}(E)$, find an isogeny from E to E'.

[1] Kohel, Lauter, Petit, Tignol "On the quaternion ℓ-isogeny path problem", 2014.

Easy Problems Hard Problems Let $E(\mathbb{F}_{p^2})$ be a supersingular elliptic curve.

- Given E, compute an arbitrary isogeny with domain E and smooth degree (e.g. 2^m).
- Given E and $E'(\mathbb{F}_{p^2})$, find an isogeny from E to E'.
- Given E, $E'(\mathbb{F}_{p^2})$, $\mathrm{End}(E)$, and $\mathrm{End}(E')$, and $d \in \mathbb{N}$, find an isogeny from E to E' of degree d. [1]
- Given E, $E'(\mathbb{F}_{p^2})$, and $\mathrm{End}(E)$, find an isogeny from E to E'.
- Given E, $\mathrm{End}(E)$, and $\phi : E \to E'$, find $\mathrm{End}(E')$.

[1] Kohel, Lauter, Petit, Tignol "On the quaternion ℓ-isogeny path problem", 2014.

Easy Problems Hard Problems Let $E(\mathbb{F}_{p^2})$ be a supersingular elliptic curve.

- Given E, compute an arbitrary isogeny with domain E and smooth degree (e.g. 2^m).
- Given E and $E'(\mathbb{F}_{p^2})$, find an isogeny from E to E'.
- Given E, $E'(\mathbb{F}_{p^2})$, $\mathrm{End}(E)$, and $\mathrm{End}(E')$, and $d \in \mathbb{N}$, find an isogeny from E to E' of degree d. [1]
- Given E, $E'(\mathbb{F}_{p^2})$, and $\mathrm{End}(E)$, find an isogeny from E to E'.
- Given E, $\mathrm{End}(E)$, and $\phi : E \to E'$, find $\mathrm{End}(E')$.
- The GPS signature scheme uses these discrepancies to make an Identification Protocol.

[1] Kohel, Lauter, Petit, Tignol "On the quaternion ℓ-isogeny path problem", 2014.

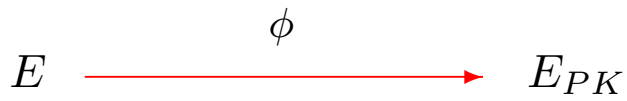
- Setup: Elliptic curve $E(\mathbb{F}_p^2)$, $\mathrm{End}(E)$, and $L \in \mathbb{N}$.

- Setup: Elliptic curve $E(\mathbb{F}_p^2)$, $\mathrm{End}(E)$, and $L \in \mathbb{N}$.

- Private key: Isogeny $\phi : E \to E_{PK}$ with L-smooth degree (all prime powers dividing $\deg \phi$ are less than L).
  Public Key: E_{PK}.

- Setup: Elliptic curve $E(\mathbb{F}_p^2)$, $\mathrm{End}(E)$, and $L \in \mathbb{N}$.

- Private key: Isogeny $\phi : E \to E_{PK}$ with L-smooth degree (all prime powers dividing $\deg \phi$ are less than L).
  Public Key: E_{PK}.

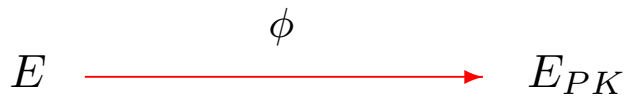


- Setup: Elliptic curve $E(\mathbb{F}_p^2)$, $\mathrm{End}(E)$, and $L \in \mathbb{N}$.
- Private key: Isogeny $\phi : E \to E_{PK}$ with L-smooth degree (all prime powers dividing $\deg \phi$ are less than L).
  Public Key: E_{PK}.

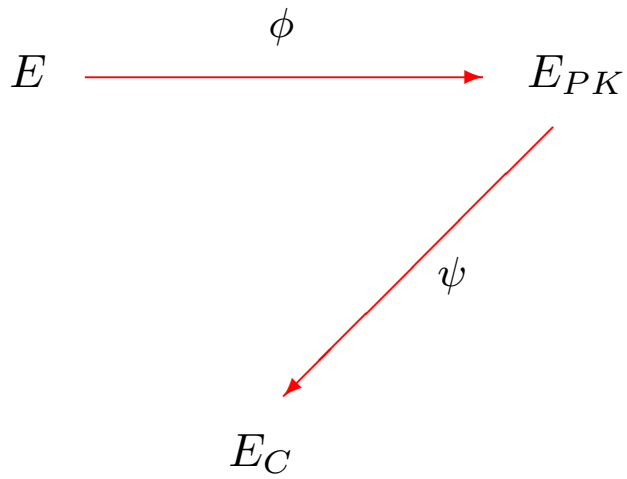
$$E \xrightarrow{\phi} E_{PK}$$

- Prover computes an isogeny $\psi : E_{PK} \to E_C$ with L-smooth degree.
  Commitment: E_C.

- Setup: Elliptic curve $E(\mathbb{F}_p^2)$, $\mathrm{End}(E)$, and $L \in \mathbb{N}$.
- Private key: Isogeny $\phi : E \to E_{PK}$ with L-smooth degree (all prime powers dividing $\deg \phi$ are less than L).
  Public Key: E_{PK}.

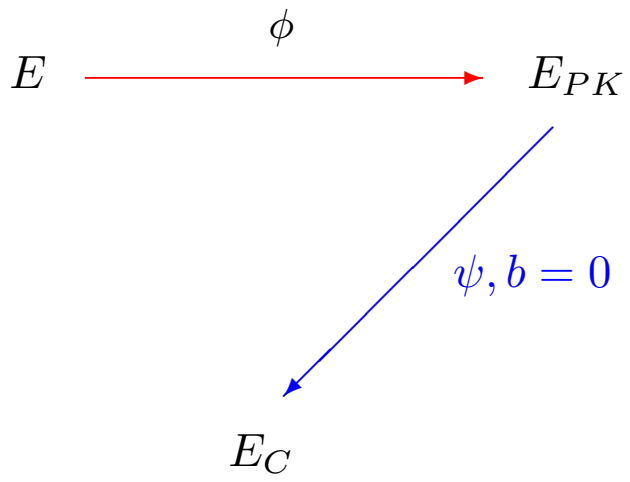


- Prover computes an isogeny $\psi : E_{PK} \to E_C$ with L-smooth degree.
  Commitment: E_C.

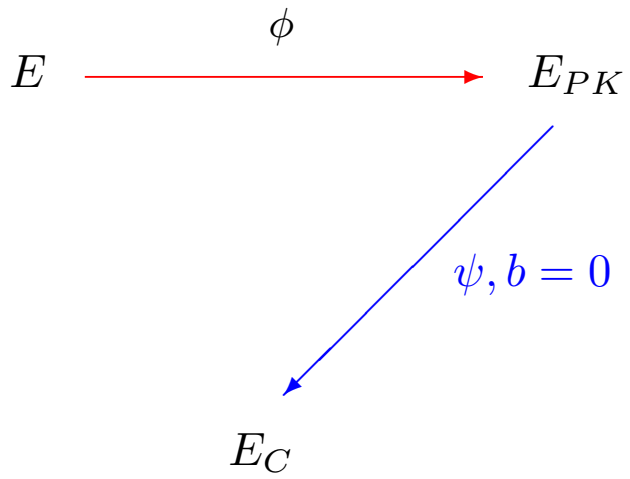


- Challenge is $b = 0$ or $b = 1$. When $b = 0$, the Prover reveals ϕ.

- Challenge is $b = 0$ or $b = 1$. When $b = 0$, the Prover reveals ϕ.

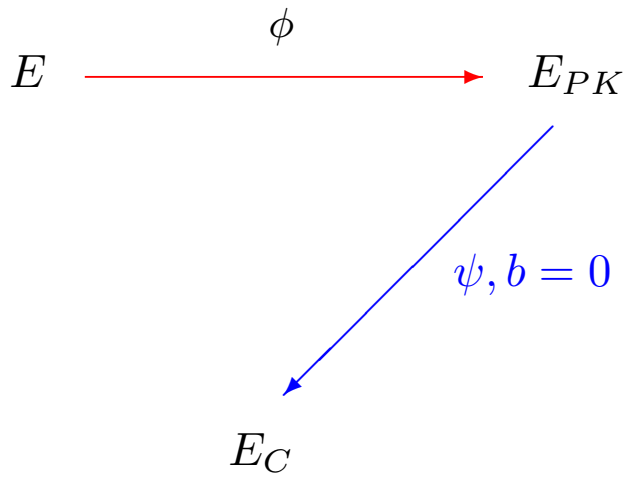


- Challenge is $b = 0$ or $b = 1$. When $b = 0$, the Prover reveals ϕ.

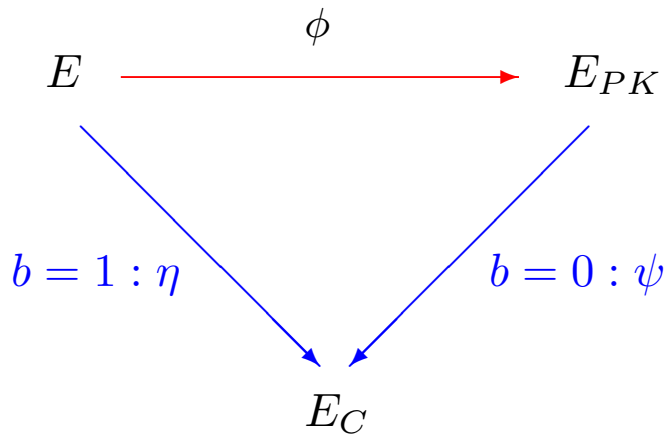


- When $b = 1$, the Prover reveals some isogeny η from E to E_C with L-smooth degree.

- Challenge is $b = 0$ or $b = 1$. When $b = 0$, the Prover reveals ϕ.



- When $b = 1$, the Prover reveals some isogeny η from E to E_C with L-smooth degree.



Warning: $\eta \neq \psi \circ \phi$

- When $b = 1$, η is computed as follows:

  (i) Compute $\mathrm{End}(E_C)$ by pushing $\mathrm{End}(E)$ through $\psi \circ \phi$.

- When $b = 1$, η is computed as follows:

  (i) Compute $\mathrm{End}(E_C)$ by pushing $\mathrm{End}(E)$ through $\psi \circ \phi$.

  (ii) (Isogeny-to-ideal) Use $\psi \circ \phi$ to compute a right ideal I of $\mathrm{End}(E)$ which is a left ideal of $\mathrm{End}(E_C)$.

- When $b = 1$, η is computed as follows:

  (i) Compute $\mathrm{End}(E_C)$ by pushing $\mathrm{End}(E)$ through $\psi \circ \phi$.

  (ii) (Isogeny-to-ideal) Use $\psi \circ \phi$ to compute a right ideal I of $\mathrm{End}(E)$ which is a left ideal of $\mathrm{End}(E_C)$.

  (iii) Renormalize I to another ideal J so that it corresponds to an isogeny with L-smooth degree.

- When $b = 1$, η is computed as follows:

  (i) Compute End(E_C) by pushing End(E) through $\psi \circ \phi$.

  (ii) (Isogeny-to-ideal) Use $\psi \circ \phi$ to compute a right ideal I of End(E) which is a left ideal of End(E_C).

  (iii) Renormalize I to another ideal J so that it corresponds to an isogeny with L-smooth degree.

  (iv) (Ideal-to-isogeny) Translate J to an isogeny η.

- When $b = 1$, η is computed as follows:

  (i) Compute $\mathrm{End}(E_C)$ by pushing $\mathrm{End}(E)$ through $\psi \circ \phi$.

  (ii) (Isogeny-to-ideal) Use $\psi \circ \phi$ to compute a right ideal I of $\mathrm{End}(E)$ which is a left ideal of $\mathrm{End}(E_C)$.

  (iii) Renormalize I to another ideal J so that it corresponds to an isogeny with L-smooth degree.

  (iv) (Ideal-to-isogeny) Translate J to an isogeny η.

- The output isogeny η will have domain E, codomain E_C, and L-smooth degree.

- The goal: given $\psi \circ \phi$, improve the computation of the ideal I

- The goal: given $\psi \circ \phi$, improve the computation of the ideal I
- This step includes a "half point" computation, which is: given $P \in E(\mathbb{F}_{p^n})$, find some P' such that $[2]P' = P$.

- The goal: given $\psi \circ \phi$, improve the computation of the ideal I
- This step includes a "half point" computation, which is: given $P \in E(\mathbb{F}_{p^n})$, find some P' such that $[2]P' = P$.
- The original method involved solving a large degree polynomial.

- The goal: given $\psi \circ \phi$, improve the computation of the ideal I
- This step includes a "half point" computation, which is: given $P \in E(\mathbb{F}_{p^n})$, find some P' such that $[2]P' = P$.
- The original method involved solving a large degree polynomial.
- We observe that since the order of P is known at this step, some odd $N \in \mathbb{Z}$, we can compute P' as $\left[\frac{N+1}{2}\right] P$.

- The goal: given $\psi \circ \phi$, improve the computation of the ideal I
- This step includes a "half point" computation, which is: given $P \in E(\mathbb{F}_{p^n})$, find some P' such that $[2]P' = P$.
- The original method involved solving a large degree polynomial.
- We observe that since the order of P is known at this step, some odd $N \in \mathbb{Z}$, we can compute P' as $\left[\frac{N+1}{2}\right] P$.
- This decrease in cost from this modification is only marginal, but this computation is used widely throughout the signing algorithm.

- When $b = 1$, the output isogeny η will be a composition of isogenies, each with prime power degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

$$\eta_i : E_{i-1} \to E_i, \text{ where } E_0 = E \text{ and } E_k = E_C.$$

- When $b = 1$, the output isogeny η will be a composition of isogenies, each with prime power degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

$$\eta_i : E_{i-1} \to E_i, \text{ where } E_0 = E \text{ and } E_k = E_C.$$

- Suppose the degree of η_i is the prime power ℓ^e.

- When $b = 1$, the output isogeny η will be a composition of isogenies, each with prime power degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

$$\eta_i : E_{i-1} \to E_i, \text{ where } E_0 = E \text{ and } E_k = E_C.$$

- Suppose the degree of η_i is the prime power ℓ^e.

- When constructing the ideal I, it can be done for each ℓ^e individually and then combined.

- When $b = 1$, the output isogeny η will be a composition of isogenies, each with prime power degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

$$\eta_i : E_{i-1} \to E_i, \text{ where } E_0 = E \text{ and } E_k = E_C.$$

- Suppose the degree of η_i is the prime power ℓ^e.
- When constructing the ideal I, it can be done for each ℓ^e individually and then combined.
- We improve the runtime of step (ii) (isogeny-to-ideal) from $poly(\ell^e)$ to $poly(\ell, e)$.

- Let $\langle Q \rangle = \ker \eta_i \subset E(\mathbb{F}_{p^n})$. To find the ideal I, we need a solution $\alpha \in \mathrm{End}(E)$ to

$$\alpha(Q) = 0, \text{ and } \deg \alpha \equiv 0 \mod \ell^e.$$

- Let $\langle Q \rangle = \ker \eta_i \subset E(\mathbb{F}_{p^n})$. To find the ideal I, we need a solution $\alpha \in \mathrm{End}(E)$ to

$$\alpha(Q) = 0, \text{ and } \deg \alpha \equiv 0 \mod \ell^e.$$

- Once α is found, the ideal I can be updated to $I\ell^e + \mathrm{End}(E)\alpha$.

- Let $\langle Q \rangle = \ker \eta_i \subset E(\mathbb{F}_{p^n})$. To find the ideal I, we need a solution $\alpha \in \mathrm{End}(E)$ to

$$\alpha(Q) = 0, \text{ and } \deg \alpha \equiv 0 \mod \ell^e.$$

- Once α is found, the ideal I can be updated to $I\ell^e + \mathrm{End}(E)\alpha$.

- The original GPS work determines α by searching randomly.

- Let $\langle Q \rangle = \ker \eta_i \subset E(\mathbb{F}_{p^n})$. To find the ideal I, we need a solution $\alpha \in \mathrm{End}(E)$ to

$$\alpha(Q) = 0, \text{ and } \deg \alpha \equiv 0 \mod \ell^e.$$

- Once α is found, the ideal I can be updated to $I\ell^e + \mathrm{End}(E)\alpha$.
- The original GPS work determines α by searching randomly.
- We instead propose finding random solutions to $\alpha_j(Q) = 0$ and $\deg \alpha_j \equiv 0 \mod \ell^j$ iteratively for $j = 1, \ldots, e$.

- Reminder: When $b = 1$, the output isogeny η will be a composition of isogenies, each with degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

- Reminder: When $b = 1$, the output isogeny η will be a composition of isogenies, each with degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

- Our main improvement is for constructing/evaluating the isogenies η_i efficiently.

- Reminder: When $b = 1$, the output isogeny η will be a composition of isogenies, each with degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

- Our main improvement is for constructing/evaluating the isogenies η_i efficiently.

- For each η_i, we must construct an extension field $\mathbb{F}_{p^n}$ such that $E_{i-1}[\deg \eta_i] \subset E_{i-1}(\mathbb{F}_{p^n})$.

- Reminder: When $b = 1$, the output isogeny η will be a composition of isogenies, each with degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

- Our main improvement is for constructing/evaluating the isogenies η_i efficiently.

- For each η_i, we must construct an extension field $\mathbb{F}_{p^n}$ such that $E_{i-1}[\deg \eta_i] \subset E_{i-1}(\mathbb{F}_{p^n})$.

- The original work explains how to construct each extension efficiently, but not how to maneuver between the extensions as i varies.

- Reminder: When $b = 1$, the output isogeny η will be a composition of isogenies, each with degrees less than L.

$$\eta = \eta_k \circ \cdots \circ \eta_1.$$

- Our main improvement is for constructing/evaluating the isogenies η_i efficiently.

- For each η_i, we must construct an extension field $\mathbb{F}_{p^n}$ such that $E_{i-1}[\deg \eta_i] \subset E_{i-1}(\mathbb{F}_{p^n})$.

- The original work explains how to construct each extension efficiently, but not how to maneuver between the extensions as i varies.

- In the worst case, this would result in an extension of degree $\mathrm{LCM}\{\deg \eta_i\}_{i=1}^{k} \leq L^k$.

- Recall that supersingular elliptic curves are always defined over $\mathbb{F}_{p^2}$.

- Recall that supersingular elliptic curves are always defined over $\mathbb{F}_{p^2}$.
- Our proposal: after each $\eta_i : E_{i-1}(\mathbb{F}_{p^n}) \to E_i(\mathbb{F}_{p^n})$ is computed, take an isomorphism to reduce the extension field:

$$\Phi_i : E_i(\mathbb{F}_{p^n}) \to E_i(\mathbb{F}_{p^2}).$$

- Recall that supersingular elliptic curves are always defined over $\mathbb{F}_{p^2}$.
- Our proposal: after each $\eta_i : E_{i-1}(\mathbb{F}_{p^n}) \to E_i(\mathbb{F}_{p^n})$ is computed, take an isomorphism to reduce the extension field:

$$\Phi_i : E_i(\mathbb{F}_{p^n}) \to E_i(\mathbb{F}_{p^2}).$$

- We provide formulas for the isomorphisms in terms of the j-invariant of E_i.

- Recall that supersingular elliptic curves are always defined over $\mathbb{F}_{p^2}$.
- Our proposal: after each $\eta_i : E_{i-1}(\mathbb{F}_{p^n}) \to E_i(\mathbb{F}_{p^n})$ is computed, take an isomorphism to reduce the extension field:

$$\Phi_i : E_i(\mathbb{F}_{p^n}) \to E_i(\mathbb{F}_{p^2}).$$

- We provide formulas for the isomorphisms in terms of the j-invariant of E_i.
- This process bounds the necessary extension degree by $\max\{\deg \eta_i\}_{i=1}^{k} \leq L$.

- Our third major contribution is a proof of security for multiple parallel instances of the GSP signature scheme.

[2] Stachowiak "Proofs of Knowledge with Several Challenge Values", 2008.

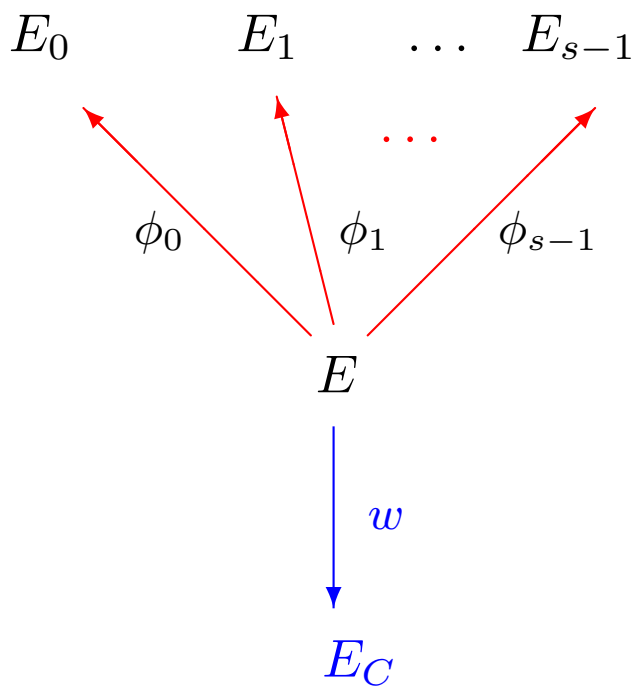
- Our third major contribution is a proof of security for multiple parallel instances of the GSP signature scheme.

- The idea of using multiple challenge bits is not novel[2], but the application is.

[2] Stachowiak "Proofs of Knowledge with Several Challenge Values", 2008.

- Our third major contribution is a proof of security for multiple parallel instances of the GSP signature scheme.

- The idea of using multiple challenge bits is not novel[2], but the application is.



[2] Stachowiak "Proofs of Knowledge with Several Challenge Values", 2008.

- Given a challenge bit $i \in \{0, 1, \ldots, s-1\}$ the signer constructs an isogeny from E_i to E_C.

- Given a challenge bit $i \in \{0, 1, \ldots, s-1\}$ the signer constructs an isogeny from E_i to E_C.
- Allowing for a greater number of challenge bits decreases the number of rounds by a logarithmic factor.

- Given a challenge bit $i \in \{0, 1, \ldots, s-1\}$ the signer constructs an isogeny from E_i to E_C.
- Allowing for a greater number of challenge bits decreases the number of rounds by a logarithmic factor.
- We provide a proof of Completeness, Soundness, and Zero-Knowledge.

- Given a challenge bit $i \in \{0, 1, \ldots, s-1\}$ the signer constructs an isogeny from E_i to E_C.
- Allowing for a greater number of challenge bits decreases the number of rounds by a logarithmic factor.
- We provide a proof of Completeness, Soundness, and Zero-Knowledge.
- Output of the algorithm for step (iii) (ideal renormalization) in the original work has a particular form. This makes our ZK proof highly non-trivial, which is why this modification has not achieved before.

n	$\log_2 p$	Isogenies	(ii)	(iii)	(iv)
[3,10]	8.7	0.100	0.073	0.064	0.109
[3,20]	24.2	0.217	0.215	0.366	0.190
[3,43], [97]	61.1	1.000	1.356	0.883	0.492
[3,113]	155.4	6.356	9.442	6.989	2.297
[3,373], [587]	510.7	174.917	126.520	173.020	45.270

Table: Time (sec) per step

- Major improvements to all three steps of the GPS signature scheme.

- Major improvements to all three steps of the GPS signature scheme.
- This scheme may be feasible in the future.

- Major improvements to all three steps of the GPS signature scheme.
- This scheme may be feasible in the future.
- The runtime is still too inefficient, the bottleneck is computing the extension fields.

- Major improvements to all three steps of the GPS signature scheme.
- This scheme may be feasible in the future.
- The runtime is still too inefficient, the bottleneck is computing the extension fields.
- Our code for the KLPT subroutine is fast.

Bibliography:

[1] D. Kohel, K. Lauter, C. Petit, J.-P. Tignol. "On the quaternion ℓ-isogeny path problem." *LMS Journal of Computation and Mathematics*, 17.A (2014): 418-432

[2] G. Stachowiak. "Proofs of Knowledge with Several Challenge Values." IACR Cryptology ePrint Archive (2008): 181.

[3] S. Galbraith, C. Petit, J. Silva. "Identification protocols and signature schemes based on supersingular isogeny problems." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Cham, 2017.