Zero-Value and Correlation Attacks on CSIDH and SIKE†

Institute of Information Science - Academia Sinica

15 December 2022

Fabio Campos[1,2] Michael Meyer[3] Krijn Reijnders[2] Marc Stöttinger[1]

[1]RheinMain University of Applied Sciences Wiesbaden, Germany

[2]Radboud University, Nijmegen, The Netherlands

[3]University of Regensburg, Germany

Who am I?

- Fabio Campos, https://sopmac.org
- since 2018
  - external PhD student at Radboud University, NL
  - supervisor: Peter Schwabe
  - researcher at University of Wiesbaden, DE
  - implementations of isogeny-based crypto

Who am I?

- Fabio Campos, https://sopmac.org
- since 2018
  - external PhD student at Radboud University, NL
  - supervisor: Peter Schwabe
  - researcher at University of Wiesbaden, DE
  - implementations of isogeny-based crypto
- before 2018
  - collecting money@industry / lecturer@Wiesbaden
  - computer science M.Sc.

Who am I?

- Fabio Campos, https://sopmac.org
- since 2018
  - external PhD student at Radboud University, NL
  - supervisor: Peter Schwabe
  - researcher at University of Wiesbaden, DE
  - implementations of isogeny-based crypto
- before 2018
  - collecting money@industry / lecturer@Wiesbaden
  - computer science M.Sc.
- born in Rio de Janeiro, BR (no questions about football) ;-(

Wait, what?

Zero-Value and Correlation Attacks on CSIDH and SIKE

Wait, what?

Zero-Value and Correlation Attacks on CSIDH and SIKE

- side-channel attacks
- power analysis whether secret computation pass over certain values
- leaking secret information

Wait, what?

Zero-Value and Correlation Attacks on CSIDH and SIKE

- isogeny-based schemes
- CSIDH : allows for non-interactive key exchange
- SIKE : key encapsulation mechanism

Agenda

- Zero-value attacks
- Isogeny paths in CSIDH
- Vulnerable curves in CSIDH
- Attacking SQALE and CTIDH
- Simulation
- Countermeasures
- Applicability to SIKE

Zero-value attacks

Motivation: Zero-value attacks

Zero-value attacks: Identify secret-dependent occurrences of zero-values in the power trace.
$\rightsquigarrow$ information on private key.

Motivation: Zero-value attacks

Zero-value attacks: Identify secret-dependent occurrences of zero-values in the power trace.
$\rightsquigarrow$ information on private key.

- Proposed for SIDH in [Koziel–Azarderakhsh–Jao-2017].

Motivation: Zero-value attacks

Zero-value attacks: Identify secret-dependent occurrences of zero-values in the power trace.

$\rightsquigarrow$ information on private key.

- Proposed for SIDH in [Koziel–Azarderakhsh–Jao-2017].
- Demonstrated for SIKE in [De Feo–El Mrabet–Genêt–Kaluđerović–de Guertechin–Pontié–Tasso-2022].

Motivation: Zero-value attacks

Zero-value attacks: Identify secret-dependent occurrences of zero-values in the power trace.

$\rightsquigarrow$ information on private key.

- Proposed for SIDH in [Koziel–Azarderakhsh–Jao-2017].
- Demonstrated for SIKE in [De Feo–El Mrabet–Genêt–Kaluđerović–de Guertechin–Pontié–Tasso-2022].
- Does this work in CSIDH too?

Isogeny paths in CSIDH

CSIDH

- Prime of the form $p = 4 \cdot \ell_1 \cdot \dots \cdot \ell_n - 1$ with small distinct odd primes ℓ_i.

CSIDH

- Prime of the form $p = 4 \cdot \ell_1 \cdot \dots \cdot \ell_n - 1$ with small distinct odd primes ℓ_i.
- Work with supersingular elliptic curves over $\mathbb{F}_p$.
  $\rightsquigarrow$ $\#E(\mathbb{F}_p) = p + 1$ for all involved curves.

CSIDH

- Prime of the form $p = 4 \cdot \ell_1 \cdot \dots \cdot \ell_n - 1$ with small distinct odd primes ℓ_i.
- Work with supersingular elliptic curves over $\mathbb{F}_p$.
  $\rightsquigarrow$ $\#E(\mathbb{F}_p) = p + 1$ for all involved curves.
- We can efficiently compute isogenies of degrees ℓ_i.

CSIDH

- Prime of the form $p = 4 \cdot \ell_1 \cdot \cdots \cdot \ell_n - 1$ with small distinct odd primes ℓ_i.
- Work with supersingular elliptic curves over $\mathbb{F}_p$.
  $\rightsquigarrow$ $\#E(\mathbb{F}_p) = p + 1$ for all involved curves.
- We can efficiently compute isogenies of degrees ℓ_i.
- Each of the ℓ_i-isogeny graphs consists of one or more cycles with identical vertex set.

CSIDH

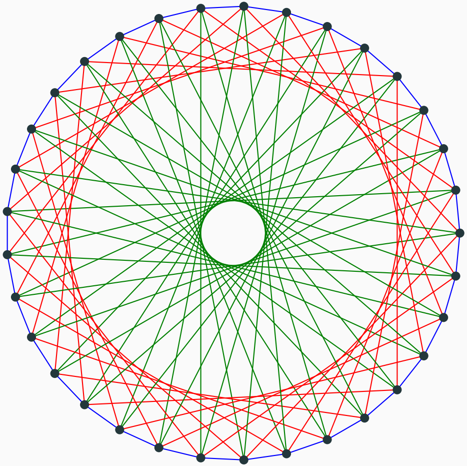
- Prime of the form $p = 4 \cdot \ell_1 \cdot \cdots \cdot \ell_n - 1$ with small distinct odd primes ℓ_i.
- Work with supersingular elliptic curves over $\mathbb{F}_p$.
  $\rightsquigarrow$ $\#E(\mathbb{F}_p) = p + 1$ for all involved curves.
- We can efficiently compute isogenies of degrees ℓ_i.
- Each of the ℓ_i-isogeny graphs consists of one or more cycles with identical vertex set.
- CSIDH isogeny graph: union of these cycles

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

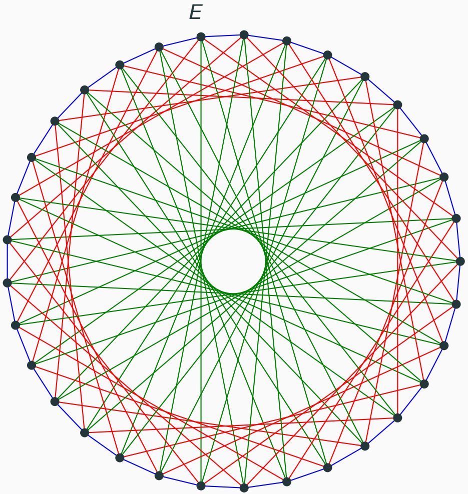
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

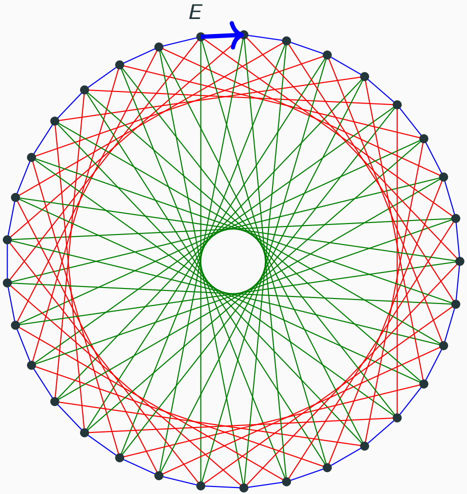
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

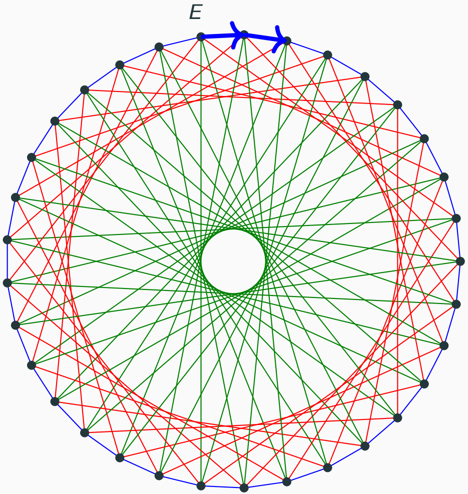
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

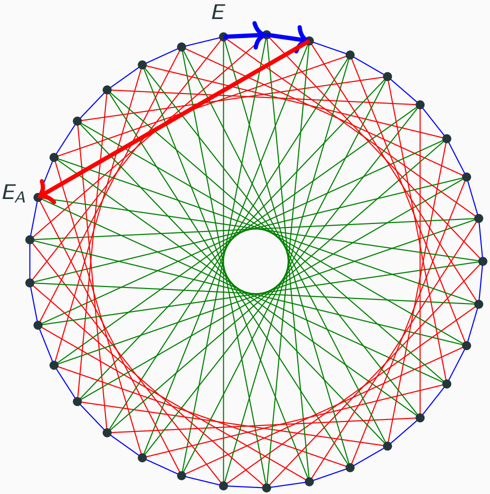
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$

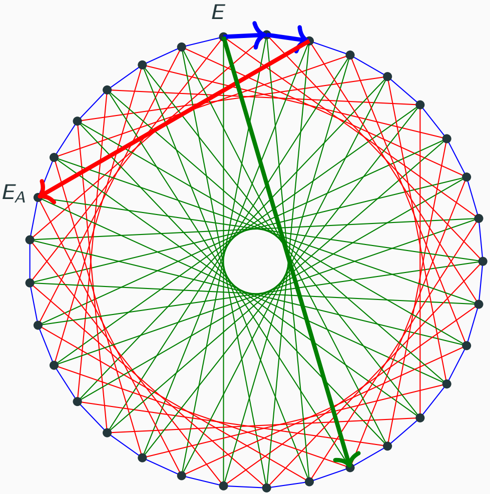


Bob

secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot \textcolor{blue}{3} \cdot \textcolor{green}{5} \cdot \textcolor{red}{11} - 1$



Alice

secret: $(+, +, -)$

Bob

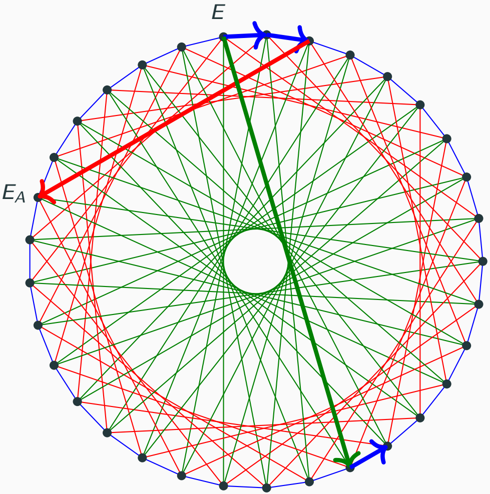
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

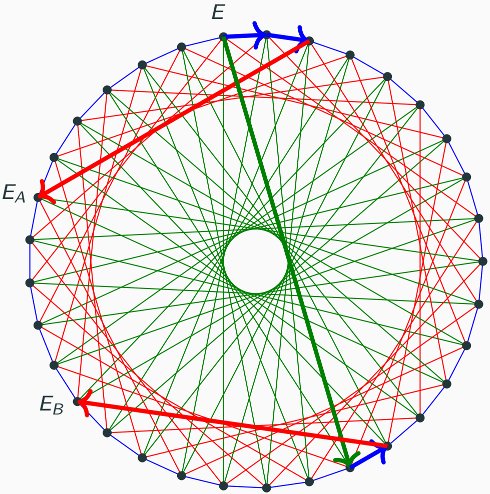
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

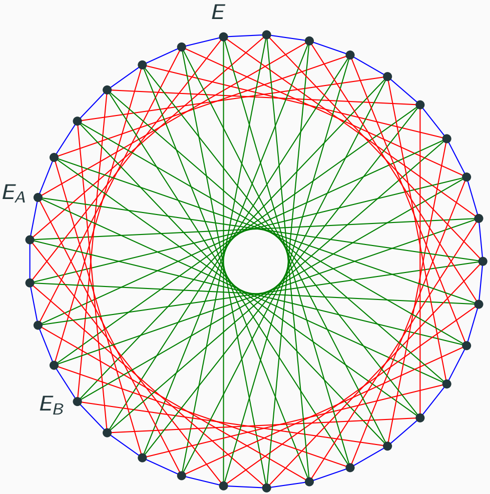
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$

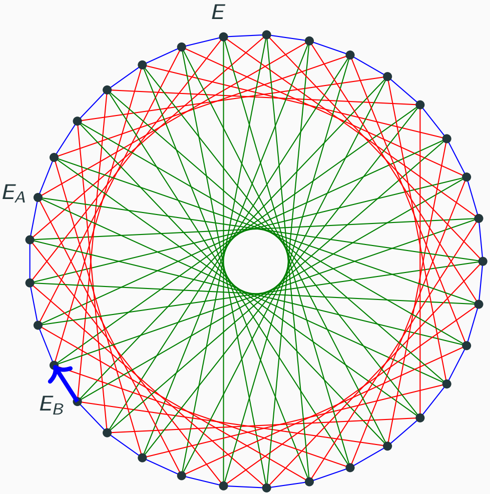


Bob

secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$



Alice

secret: $(+, +, -)$

Bob

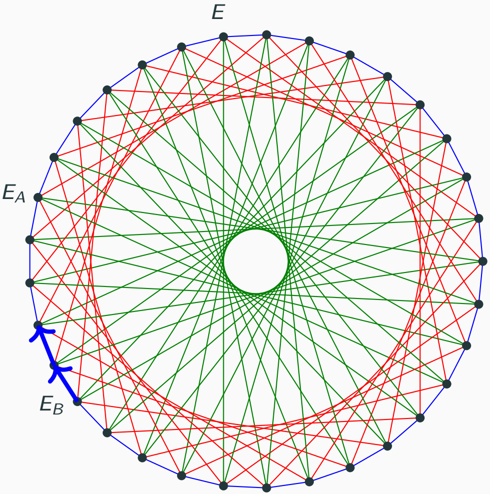
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

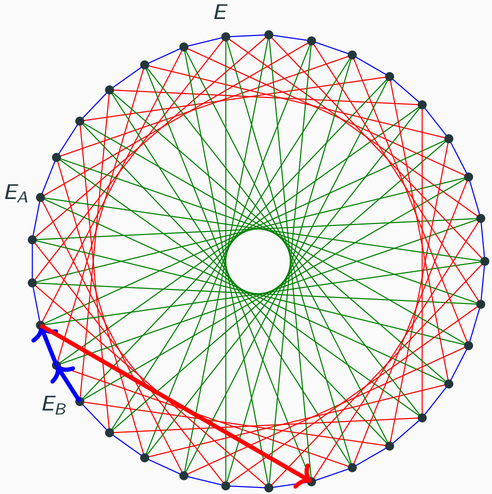
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

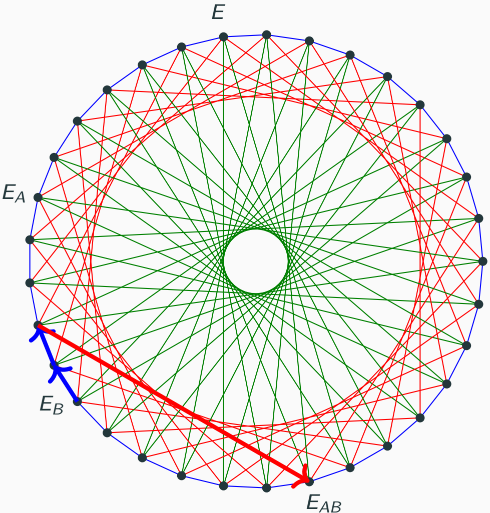
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

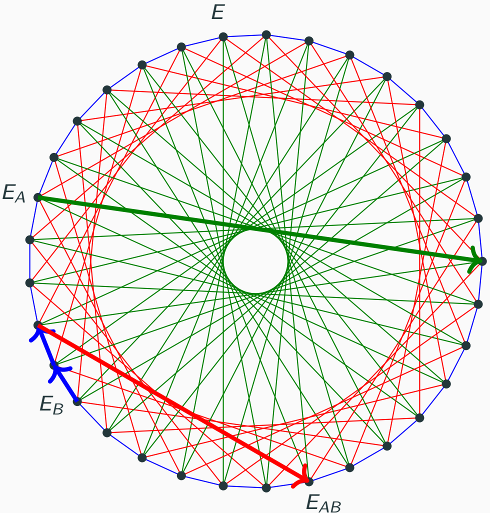
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

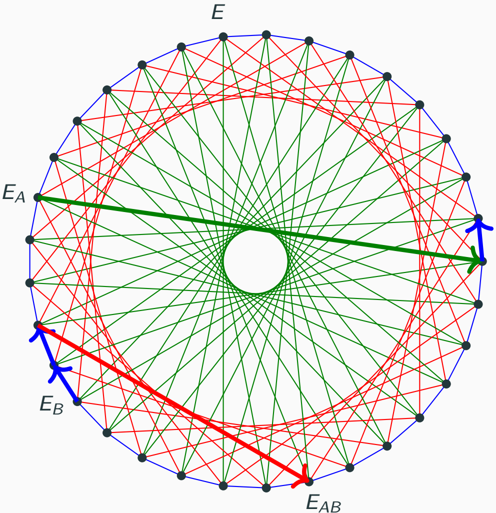
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

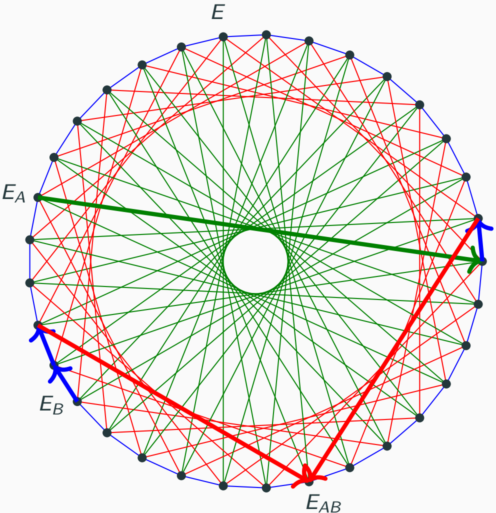
secret: $(+, -, +)$

CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$



Bob

secret: $(+, -, +)$

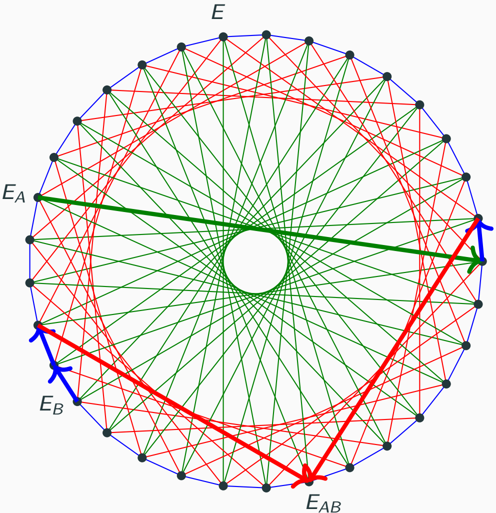
CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$

$\rightsquigarrow (2, 0, -1)$



Bob

secret: $(+, -, +)$

$\rightsquigarrow (-1, 1, 1)$

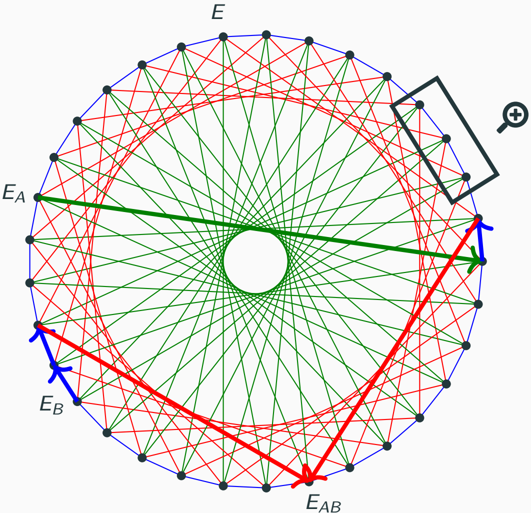
CSIDH

Toy example: $p = 659 = 4 \cdot 3 \cdot 5 \cdot 11 - 1$

Alice

secret: $(+, +, -)$

$\rightsquigarrow (2, 0, -1)$



Bob

secret: $(+, -, +)$

$\rightsquigarrow (-1, 1, 1)$

CSIDH

$$E_a : y^2 = x^3 + ax^2 + x \quad \bullet$$

CSIDH

$$E_a : y^2 = x^3 + ax^2 + x$$

$$E_{a'} : y^2 = x^3 + a'x^2 + x$$

CSIDH

$$E_a : y^2 = x^3 + ax^2 + x$$

ℓ_i-isogeny: $(+)$

$$E_{a'} : y^2 = x^3 + a'x^2 + x$$

CSIDH

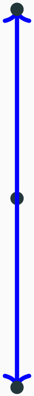
$E_{\tilde{a}} : y^2 = x^3 + \tilde{a}x^2 + x$

$E_a : y^2 = x^3 + ax^2 + x$

$E_{a'} : y^2 = x^3 + a'x^2 + x$

ℓ_i-isogeny: $(+)$

$$E_{\tilde{a}} : y^2 = x^3 + \tilde{a}x^2 + x$$



ℓ_i-isogeny: $(-)$

$$E_a : y^2 = x^3 + ax^2 + x$$

ℓ_i-isogeny: $(+)$

$$E_{a'} : y^2 = x^3 + a'x^2 + x$$

CSIDH

$$E_{\tilde{a}} : y^2 = x^3 + \tilde{a}x^2 + x$$

ℓ_i-isogeny: $(-)$

$$E_a : y^2 = x^3 + ax^2 + x$$

ℓ_i-isogeny: $(+)$

$$E_{a'} : y^2 = x^3 + a'x^2 + x$$

CSIDH 🔍🔍

Usual representations of curves E_a in projective coefficients:

- Montgomery form $(A : C)$ with $a = A/C$ and C non-zero
- alternative Montgomery form $(A + 2C : 4C)$ with $a = A/C$ and C non-zero

CSIDH 🔍🔍

Usual representations of curves E_a in projective coefficients:

- Montgomery form $(A : C)$ with $a = A/C$ and C non-zero
- alternative Montgomery form $(A + 2C : 4C)$ with $a = A/C$ and C non-zero

Our attack aims at two types of vulnerable representations:

CSIDH 🔍🔍

Usual representations of curves E_a in projective coefficients:

- Montgomery form $(A : C)$ with $a = A/C$ and C non-zero
- alternative Montgomery form $(A + 2C : 4C)$ with $a = A/C$ and C non-zero

Our attack aims at two types of vulnerable representations:

- Zero-value representation: Represents the Montgomery coefficient $a \in \mathbb{F}_p$ in projective coordinates $(\alpha : \beta)$ such that $\alpha = 0$ or $\beta = 0$.

CSIDH

Usual representations of curves E_a in projective coefficients:

- Montgomery form $(A : C)$ with $a = A/C$ and C non-zero
- alternative Montgomery form $(A + 2C : 4C)$ with $a = A/C$ and C non-zero

Our attack aims at two types of vulnerable representations:

- Zero-value representation: Represents the Montgomery coefficient $a \in \mathbb{F}_p$ in projective coordinates $(\alpha : \beta)$ such that $\alpha = 0$ or $\beta = 0$.
- Strongly-correlated representation: Represents the Montgomery coefficient $a \in \mathbb{F}_p$ in projective coordinates $(\alpha : \beta)$ such that the bit representations of α and β are bit shifts.

Vulnerable curves in CSIDH

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

- E_0 in Montgomery form: $(0 : C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

- E_0 in Montgomery form: $(0 : C)$ with $C \in \mathbb{F}_p \setminus \{0\}$

  $\rightsquigarrow$ zero-value representation

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

- E_0 in Montgomery form: $(0 : C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ zero-value representation
- E_0 in alternative Montgomery form: $(2C : 4C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

- E_0 in Montgomery form: $(0 : C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ zero-value representation
- E_0 in alternative Montgomery form: $(2C : 4C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ strongly-correlated representation if $2C < p/2$

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

- E_0 in Montgomery form: $(0 : C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ zero-value representation

- E_0 in alternative Montgomery form: $(2C : 4C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ strongly-correlated representation if $2C < p/2$

$\rightsquigarrow$ Both are detectable via side-channel analysis!

Vulnerable Curves

E_0 is a valid supersingular curve in the usual CSIDH setting.

- E_0 in Montgomery form: $(0 : C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ zero-value representation

- E_0 in alternative Montgomery form: $(2C : 4C)$ with $C \in \mathbb{F}_p \backslash \{0\}$

  $\rightsquigarrow$ strongly-correlated representation if $2C < p/2$

$\rightsquigarrow$ Both are detectable via side-channel analysis!

Also works for E_6 in alternative Montgomery form: $(8C : 4C)$ with $C \in \mathbb{F}_p$ is strongly-correlated if $4C < p/2$.

Attacking SQALE and CTIDH

Attack idea

Idea: Guess a secret key bit, and let the target's isogeny path pass over E_0 or E_6 if the guess was correct.

$\rightsquigarrow$ Correct guess can be confirmed by side-channel analysis.

Attack idea

Idea: Guess a secret key bit, and let the target's isogeny path pass over E_0 or E_6 if the guess was correct.
$\rightsquigarrow$ Correct guess can be confirmed by side-channel analysis.

- Constant-time CSIDH usually has an ordered evaluation of isogenies (modulo point rejections).

Attack idea

Idea: Guess a secret key bit, and let the target's isogeny path pass over E_0 or E_6 if the guess was correct.

$\rightsquigarrow$ Correct guess can be confirmed by side-channel analysis.

- Constant-time CSIDH usually has an ordered evaluation of isogenies (modulo point rejections).
- Task: Find out the direction of the next step (also considering dummy isogenies).

Generic attack for the k-th bit

- Assume we know the first $k-1$ isogeny steps $a_{k-1} = (-, +, -, \cdots, -)$.

Generic attack for the k-th bit

- Assume we know the first $k-1$ isogeny steps $a_{k-1} = (-, +, -, \cdots, -)$.
- Guess e ($+$ or $-$) and set $a_{k,e} = a_{k-1} \mid\mid e$.

Generic attack for the k-th bit

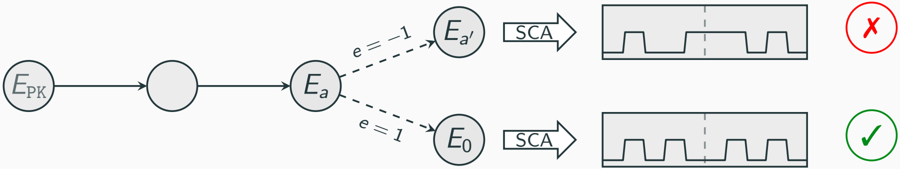
- Assume we know the first $k-1$ isogeny steps $a_{k-1} = (-, +, -, \cdots, -)$.
- Guess e ($+$ or $-$) and set $a_{k,e} = a_{k-1} \mid\mid e$.
- Pass E_{PK} calculated using $a_{k,e}^{-1}$ as public key.

Generic attack for the k-th bit

- Assume we know the first $k-1$ isogeny steps $a_{k-1} = (-, +, -, \cdots, -)$.
- Guess e $(+$ or $-)$ and set $a_{k,e} = a_{k-1} \mid\mid e$.
- Pass E_{PK} calculated using $a_{k,e}^{-1}$ as public key.
- If the k-th step passes over E_0, the guess was correct; otherwise, guess a different e and repeat.

Generic attack for the k-th bit

- Assume we know the first $k-1$ isogeny steps $a_{k-1} = (-, +, -, \cdots, -)$.
- Guess e $(+$ or $-)$ and set $a_{k,e} = a_{k-1} \mid\mid e$.
- Pass E_{PK} calculated using $a_{k,e}^{-1}$ as public key.
- If the k-th step passes over E_0, the guess was correct; otherwise, guess a different e and repeat.



SQALE [Chávez-Saab–Chi-Domínguez–Jaques–Rodríguez-Henríquez-2020]

- SQALE uses the alternative Montgomery form $(A + 2C : 4C)$.
  $\rightsquigarrow$ we can detect E_0.

SQALE [Chávez-Saab–Chi-Domínguez–Jaques–Rodríguez-Henríquez-2020]

- SQALE uses the alternative Montgomery form $(A + 2C : 4C)$.
  $\rightsquigarrow$ we can detect E_0.
- SQALE uses large parameters (2048-bit to 9216-bit primes) and secret keys from $\{-1, 1\}^n$.

SQALE [Chávez-Saab–Chi-Domínguez–Jaques–Rodríguez-Henríquez-2020]

- SQALE uses the alternative Montgomery form $(A + 2C : 4C)$.
  $\rightsquigarrow$ we can detect E_0.
- SQALE uses large parameters (2048-bit to 9216-bit primes) and secret keys from $\{-1, 1\}^n$.
- Ordered evaluation

SQALE [Chávez-Saab–Chi-Domínguez–Jaques–Rodríguez-Henríquez-2020]

- SQALE uses the alternative Montgomery form $(A + 2C : 4C)$.
  $\rightsquigarrow$ we can detect E_0.
- SQALE uses large parameters (2048-bit to 9216-bit primes) and secret keys from $\{-1, 1\}^n$.
- Ordered evaluation
- Adaptively recover key bits e_i with the generic approach.

SQALE [Chávez-Saab–Chi-Domínguez–Jaques–Rodríguez-Henríquez-2020]

- SQALE uses the alternative Montgomery form $(A + 2C : 4C)$.
  $\rightsquigarrow$ we can detect E_0.
- SQALE uses large parameters (2048-bit to 9216-bit primes) and secret keys from $\{-1, 1\}^n$.
- Ordered evaluation
- Adaptively recover key bits e_i with the generic approach.
- Each step can fail with a probability of $1/\ell_i$
  $\rightsquigarrow$ increases the number of measurements.

CTIDH [Banegas–Bernstein–Campos–Chou–Lange–Meyer–Smith–Sotáková-2021]

- CTIDH switches between Montgomery and alternative Montgomery form.
  ⇝ we can detect E_0.

Figure 1: CTIDH aka *the isogeny bus*[1]

[1]Talk by Krijn Reijnders: `https://tinyurl.com/CTIDHBeepBeep`
Original pic of bus by Teddy O on `https://unsplash.com/photos/jtpcrnqP2Mc`

CTIDH [Banegas–Bernstein–Campos–Chou–Lange–Meyer–Smith–Sotáková-2021]

- CTIDH switches between Montgomery and alternative Montgomery form.
  $\rightsquigarrow$ we can detect E_0.
- CTIDH uses a more complicated key space and hides the actual isogeny degrees in use.

Figure 1: CTIDH aka *the isogeny bus*[1]

[1]Talk by Krijn Reijnders: `https://tinyurl.com/CTIDHBeepBeep`
Original pic of bus by Teddy O on `https://unsplash.com/photos/jtpcrnqP2Mc`

CTIDH [Banegas–Bernstein–Campos–Chou–Lange–Meyer–Smith–Sotáková-2021]

- CTIDH switches between Montgomery and alternative Montgomery form.
  $\rightsquigarrow$ we can detect E_0.
- CTIDH uses a more complicated key space and hides the actual isogeny degrees in use.
- CTIDH uses an ordered evaluation, but we have to guess the direction and the degree of each isogeny.

Figure 1: CTIDH aka *the isogeny bus*[1]

---

[1] Talk by Krijn Reijnders: `https://tinyurl.com/CTIDHBeepBeep`
Original pic of bus by Teddy O on `https://unsplash.com/photos/jtpcrnqP2Mc`

CTIDH [Banegas–Bernstein–Campos–Chou–Lange–Meyer–Smith–Sotáková-2021]

- CTIDH switches between Montgomery and alternative Montgomery form.
  $\rightsquigarrow$ we can detect E_0.
- CTIDH uses a more complicated key space and hides the actual isogeny degrees in use.
- CTIDH uses an ordered evaluation, but we have to guess the direction and the degree of each isogeny.
- Each step can fail with a probability of $\approx 1/\ell_i$

Figure 1: CTIDH aka *the isogeny bus*[1]

[1] Talk by Krijn Reijnders: `https://tinyurl.com/CTIDHBeepBeep`
Original pic of bus by Teddy O on `https://unsplash.com/photos/jtpcrnqP2Mc`

CTIDH [Banegas–Bernstein–Campos–Chou–Lange–Meyer–Smith–Sotáková-2021]

- CTIDH switches between Montgomery and alternative Montgomery form.
  $\rightsquigarrow$ we can detect E_0.
- CTIDH uses a more complicated key space and hides the actual isogeny degrees in use.
- CTIDH uses an ordered evaluation, but we have to guess the direction and the degree of each isogeny.
- Each step can fail with a probability of $\approx 1/\ell_i$
- This increases the number of measurements.

Figure 1: CTIDH aka *the isogeny bus*[1]

[1]Talk by Krijn Reijnders: `https://tinyurl.com/CTIDHBeepBeep`
Original pic of bus by Teddy O on `https://unsplash.com/photos/jtpcrnqP2Mc`

Simulation

Simulation

Simulation of our attacks exploiting strong correlation:

- We require ordered evaluations
  $\rightsquigarrow$ exact positions of computations involving A and C resp. $A + 2C$ and $4C$ are known!

Simulation

Simulation of our attacks exploiting strong correlation:

- We require ordered evaluations
  $\rightsquigarrow$ exact positions of computations involving A and C resp. $A + 2C$ and $4C$ are known!
- Simulation gets Hamming weights of all limbs and adds noise.

Simulation

Simulation of our attacks exploiting strong correlation:

- We require ordered evaluations
  $\rightsquigarrow$ exact positions of computations involving A and C resp. $A + 2C$ and $4C$ are known!
- Simulation gets Hamming weights of all limbs and adds noise.
- Checks for strong correlation.

Simulation

Simulation of our attacks exploiting strong correlation:

- We require ordered evaluations
  $\rightsquigarrow$ exact positions of computations involving A and C resp. $A+2C$ and $4C$ are known!
- Simulation gets Hamming weights of all limbs and adds noise.
- Checks for strong correlation.
- average #measurements in SQALE-2048: 8,273

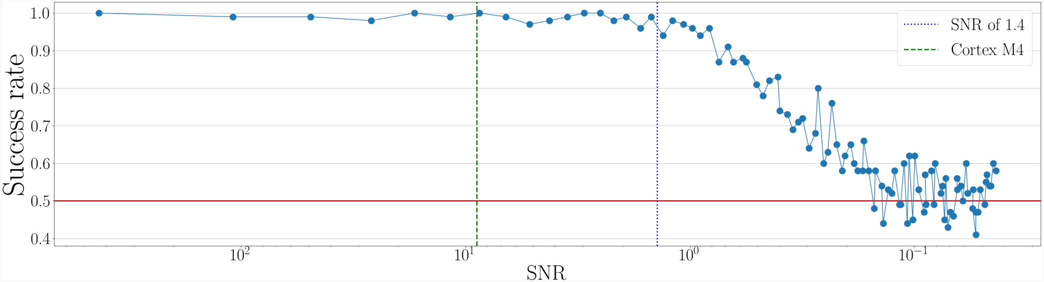
Simulation

Simulation of our attacks exploiting strong correlation:

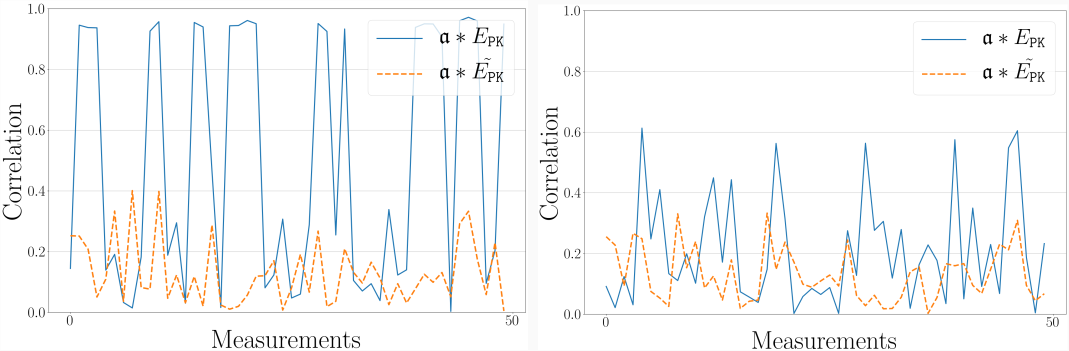
- We require ordered evaluations
  $\rightsquigarrow$ exact positions of computations involving A and C resp. $A + 2C$ and $4C$ are known!
- Simulation gets Hamming weights of all limbs and adds noise.
- Checks for strong correlation.
- average #measurements in SQALE-2048: 8,273
- average #measurements in CTIDH-511: 85,000

Simulation

Simulation for different noise levels (signal-to-noise-ratio):



Simulation



(a) Correlation results without noise. **(b)** Correlation results with SNR of 1.40.

Countermeasures

Countermeasures

- Masking isogeny: Compute $\mathfrak{a} * E$ as $\mathfrak{z}^{-1} * (\mathfrak{a} * (\mathfrak{z} * E))$ with a masking isogeny $\mathfrak{z} * E$ of key space 2^k.
  $\rightsquigarrow$ increases required #samples by factor 2^k

[1] Thanks to the reviewers for this suggestion!

Countermeasures

- Masking isogeny: Compute $\mathfrak{a} * E$ as $\mathfrak{z}^{-1} * (\mathfrak{a} * (\mathfrak{z} * E))$ with a masking isogeny $\mathfrak{z} * E$ of key space 2^k.
  $\rightsquigarrow$ increases required #samples by factor 2^k
- Move to the surface:[1] Pick $p \equiv 7 \mod 8$ and work on the surface of the isogeny graph (see [Castryck-Decru-2020]).
  $\rightsquigarrow$ We are not aware of vulnerable curves in this setting.

[1] Thanks to the reviewers for this suggestion!

Applicability to SIKE†

SIKE

- The attack applies to SIKE too: E_0 and E_6 are valid curves in SIKE

Figure 2: Who is next?[1]

[1] PQC^2 : Post-Quantum Cryptography Cemetery
Original pic of cemetery by Caleb Fisher on `https://unsplash.com/photos/pWLgynLQfgE`

SIKE

- The attack applies to SIKE too: E_0 and E_6 are valid curves in SIKE
- Attack guesses secret bits/trits and detects which leads to path over E_0 or E_6.

Figure 2: Who is next?[1]

[1] PQC^2 : Post-Quantum Cryptography Cemetery
Original pic of cemetery by Caleb Fisher on `https://unsplash.com/photos/pWLgynLQfgE`

SIKE

- The attack applies to SIKE too: E_0 and E_6 are valid curves in SIKE
- Attack guesses secret bits/trits and detects which leads to path over E_0 or E_6.
- Required number of samples:

Scheme	SIKEp434	SIKEp503	SIKEp610	SIKEp751
Samples	228	265	320	398

Figure 2: Who is next?[1]

[1] PQC^2 : Post-Quantum Cryptography Cemetery
Original pic of cemetery by Caleb Fisher on https://unsplash.com/photos/pWLgynLQfgE

Zero-Value and Correlation Attacks on CSIDH and SIKE†

Thank you!

Paper: https://eprint.iacr.org/2022/904.pdf

Simulation: https://github.com/PaZeZeVaAt/simulation