Cryptographic Hardware and Embedded Systems

SIKE Channels
Zero-Value Side-Channel Attacks on SIKE

Élise Tasso (CEA), `elise.tasso2@cea.fr`
joint work with Luca De Feo (IBM Research), Nadia El Mrabet (EMSE), Aymeric Genêt (EPFL/Nagra), Novak Kaluđerović (EPFL), Natacha Linard de Guertechin (CYSEC SA), and Simon Pontié (CEA)

September 21st, 2022

LSCO, SAS joint research team at the Centre of Microelectronics in Provence, Gardanne, France

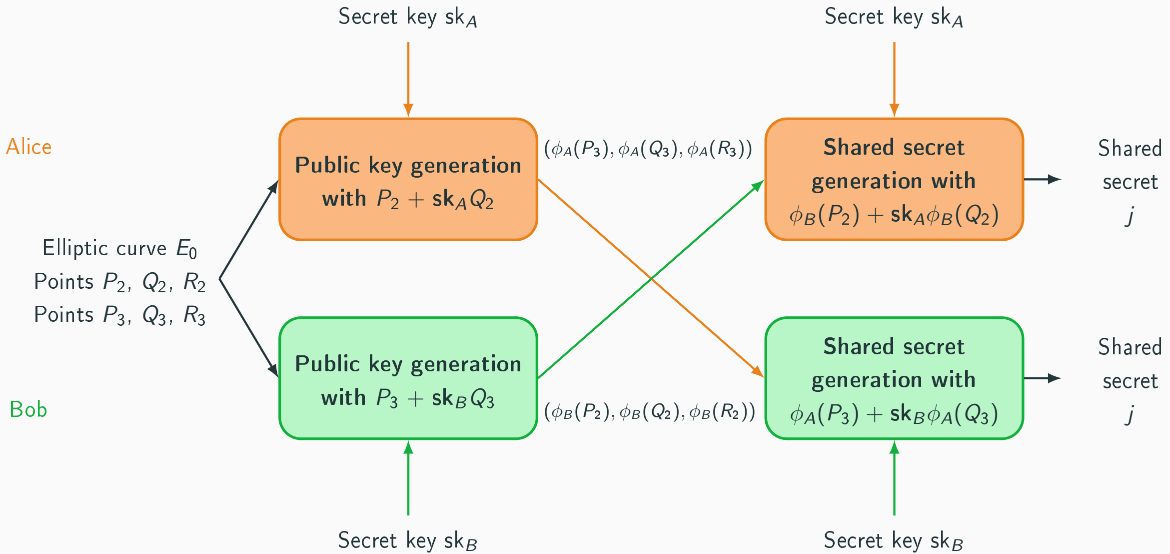
Context: SIKE and hardware attacks

SIKE in the NIST PQC Standardization Contest

SIKE was one of the NIST round 4 alternate candidates for encryption and key encapsulation.

- The only one based on isogenies between elliptic curves
- Relatively slow
- Smallest public key size
- Efficient cryptanalysis in polynomial time
- Our work is useful to study the hardware security of CSIDH: *Patient Zero and Patient Six*, Campos et al., 2022
- Portability of our attacks on variants of SIDH with masked degree (Morita) or masked torsion point images (Fouotsa) ?

SIKE: SIDH and Fujisaki-Okamoto transform



Hardware attacks on SIKE : state of the art

- Regularity of SIKE
- Attacks taking advantage of ECC or of the isogeny computation

	Fault injection	**Side-channel analysis**
Theoretical	Yan Bo Ti, 2017	Koziel et al., 2017
Simulated	Gélin et al., 2017 Adj et al., 2022	Campos et al., 2022
Experimentally verified	Tasso et al., 2021 Campos et al., 2021	Koppermann et al., 2018 Zhang et al., 2020 Genêt et al., 2021 **De Feo et al., 2022** Genêt et al., 2022 **Wang et al., 2022**

Focus on side-channel analysis

- Koppermann et al., Zhang et al. and Genêt et al. perform DPAs/CPAs on ECC.
- Masking countermeasure: projective coordinate randomization

$$(X : Z) = (\lambda X : \lambda Z) \text{ for } \lambda \neq 0, \qquad \frac{X}{Z} = \frac{\lambda X}{\lambda Z}$$

$$(3 : 1) = (-39 : -13) \quad \lambda = -13, \qquad \frac{3}{1} = \frac{-39}{-13}$$

There are $p^2 - 1$ possible values for λ, p being a "big" prime.

- **Before:** $P = (x_P : 1)$, $X_P = x_P, Z_P = 1$
- **After:** λ_P random, $P = (\lambda_P X_P : \lambda_P)$

Bypassing the coordinate randomization countermeasure

- No influence of the randomization on zero:

$$(X : Z) \xrightarrow{\lambda} (\lambda X : \lambda Z)$$

$$(X : 0) \xrightarrow{\lambda} (\lambda X : 0)$$

- **Idea:** Force computation of zero-value points (Goubin).
  - $\mathcal{O} = (1 : 0)$
  - $T = (0 : 1)$
- Koziel et al.: their ZPAs on SIDH cannot be applied to SIKE.

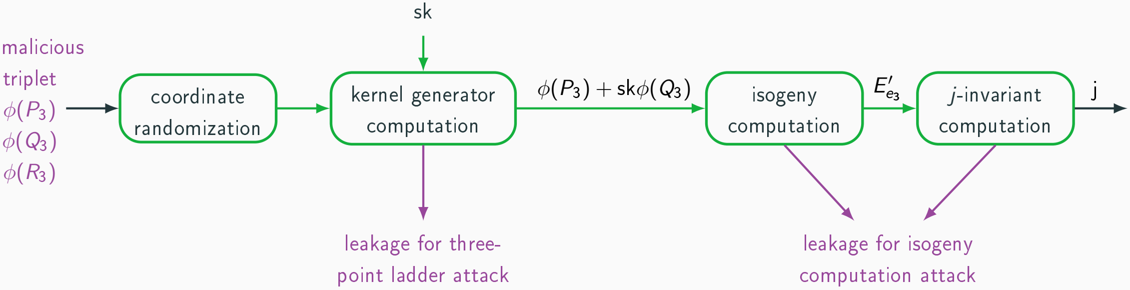
Our work

- Is there a theoretical side-channel attack on SIKE that bypasses coordinate randomization?
- Is this attack exploitable in practice?
  - Yes, with electromagnetic emissions/power consumption (our work).
  - Yes, as a remote timing attack (Hertzbleed, Wang et al., 2022).
- What are fitting countermeasures ?

Theoretical three-point ladder attack

Where and how do we attack?

Goal 1: recover the secret key bit by bit.



Assume that secret bits $sk_0, ..., sk_{k-1}$ are known. We choose a point triplet such that

- zero values appear in the computations if $sk_k = 0$ and
- arbitrary values appear if $sk_k = 1$.

Our two attacks

	Our 3-point ladder attack	Our isogeny attack	Hertzbleed
Reason for appearance of first zero-point	incomplete addition formula	isogeny evaluated on its kernel	incomplete addition formula
Observation	computation of $(0:0)$ and avalanche effect		
Side-channel	electromagnetic emissions	power consumption	timing
Countermeasure	scalar randomisation	?	scalar randomisation

Goal 2: design an efficient countermeasure for both attacks.

Attack method: find a bit $sk_k = 0$

The three-point ladder is a method to compute $P + skQ$, where P, Q are elliptic curve points and sk is a scalar. Below is a toy ladder to compute P + 50Q.

		bit 0	bit 1	bit 2	bit 3	bit 4	bit 5
bit		0	1	0	0	1	1
R0	Q	2Q	4Q	8Q	16Q	32Q	64Q
R2	Q-P	2Q-P	2Q-P	6Q-P	14Q-P	14Q-P	14Q-P
R	P	P	2Q+P	2Q+P	2Q+P	18Q+P	**50Q+P**

Let us assume we want to find bit 3, i.e. make a zero-value point T with $x_T = 0$ appear when $sk_k = 0$. We want then an input P such that $14Q - P = T$.

Attack method: find a bit $sk_k = 0$

Let us plug in P such that $14Q - P = T$.

		bit 0	bit 1	bit 2	bit 3	bit 4	bit 5
bit		0	1	0	0	1	1
R0	Q	2Q	4Q	8Q	16Q	32Q	64Q
R2	-13Q-T	-12Q-T	-12Q-T	-8Q-T	**T**	T	T
R	14Q+T	14Q+T	16Q+T	16Q+T	16Q+T	(0:0)	(0:0)

We made the correct hypothesis, T appears when bit 3 is processed.

Attack method: find a bit $sk_k = 0$

Let us plug in P such that $14Q - P = T$ when bit 3 is not 0.

		bit 0	bit 1	bit 2	bit 3	bit 4	bit 5
bit		0	1	0	1	1	1
R0	Q	2Q	4Q	8Q	16Q	32Q	64Q
R2	-13Q-T	-12Q-T	-12Q-T	-8Q-T	**-8Q-T**	-8Q-T	-8Q-T
R	14Q+T	14Q+T	16Q+T	16Q+T	24Q+T	40Q+T	72Q+T

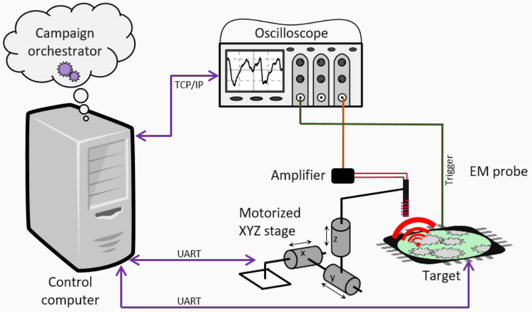
We made the wrong hypothesis, T does not appear.

Side-channel attack in a laboratory on a three-point ladder implementation

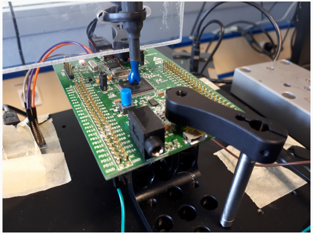
Attacked SIKE implementation

- Software implementation of the "three-point ladder" part of SIKE of the NIST PQC Standardization Process round 3 submission with added projective coordinate randomization.
- Target choice: attack in a laboratory of a STM32F407VGT6 microcontroller featuring an ARM Cortex-M4 (recommended by the NIST) at 168MHz.

Set up of an attack campaign



Set up for the realization of a side-channel attack campaign

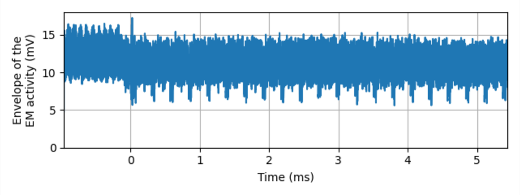


- Fixed probe.
- Goal: recover a bit sk_k of the secret knowing the previous bits $sk_0, \ldots, sk_{k-1}$.

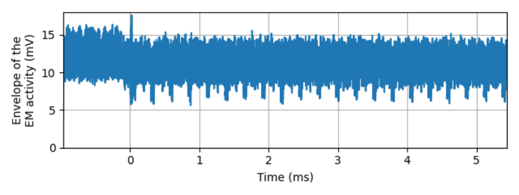
Experimental procedure

We record multiple traces of the electromagnetic emissions of the board performing the ladder computations with three types of input:

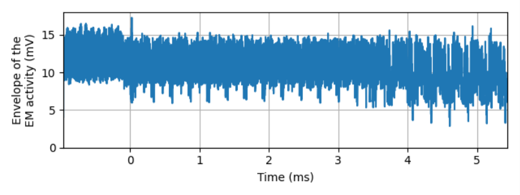
- A random, correct triplet of points,
- A malicious triplet $c_{k,0}^{T}$ (T appears when $\mathrm{sk}_k = 0$) and
- A malicious triplet $c_{k,1}^{T}$ (T appears when $\mathrm{sk}_k = 1$).



(a) Trace for random inputs.



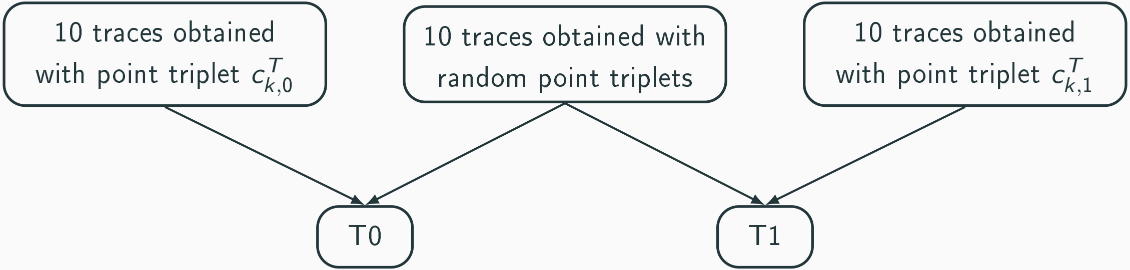
(b) Trace for the wrong hypothesis.



(c) Trace for the correct hypothesis.

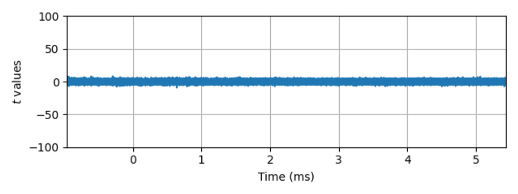
Experimental results: t-test

We compare two t-tests T0 and T1.

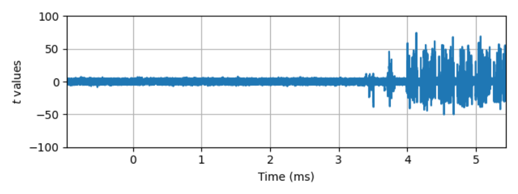


No need for a threshold.

Experimental results: t-test



(a) t-test for the wrong hypothesis.



(b) t-test for the correct hypothesis.

We found the value of sk_k.

Knowing the bits sk_0 to sk_k, we can find sk_{k+1}, and so on...

Countermeasure

Countermeasure

Both attacks use malformed input points of order

- $2 \cdot 3^n$ for the three-point ladder attack and
- 2^n for the isogeny computation attack,

instead of 3^{e_3} for legitimate inputs.

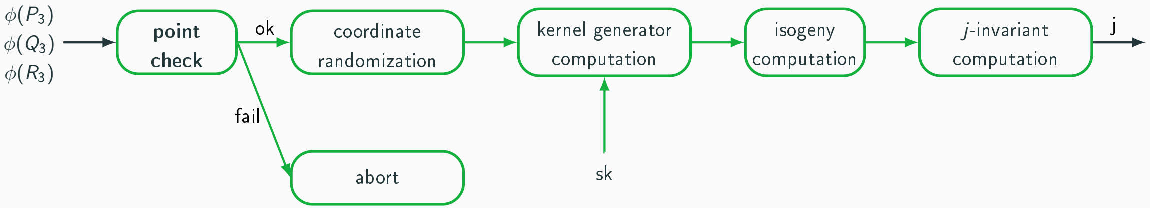
We check that

- P and Q are both of order 3^{e_3} and
- they generate the 3^{e_3}-torsion.

This is done by verifying that $3^{e_3-1}P \neq \pm 3^{e_3-1}Q \neq \mathcal{O}$ and that $3^{e_3}P = 3^{e_3}Q = \mathcal{O}$.

It protects SIKE against **both** our attacks.

Countermeasure



- This countermeasure has a 12.9% overhead (measured on a Cortex-M4).
- It has been integrated in two implementations of SIKE, PQCrypto-SIDH (submission, Microsoft) and CIRCL (Cloudflare).

Conclusion

- Both zero-point attacks,
  - the three-point ladder attack and
  - the isogeny computation attack,

  enable a bit-by-bit recovery of the secret key.
- We verified them both experimentally using respectively the electromagnetic emissions and the power consumption of a Cortex-M4 core.
- The point check is sufficient to stop both attacks.

Related work

Wang, Yingchen, Paccagnella, Riccardo, He, Elizabeth Tang, Shacham, Hovav, Fletcher, Christopher W and Kohlbrenner, David. *Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86*. In : Proceedings of the USENIX Security Symposium, 2022.

- Same three-point ladder attack (but no isogeny computation attack)
- Remote timing attack
- x86 with Turbo-boost and DVFS (Dynamic Voltage and Frequency Scaling)
- Relationship between power consumption and frequency
- Relationship between power consumption and Hamming weight/distance

$$\nearrow \text{Hamming weight} \implies \nearrow \text{power} \implies \nearrow \text{temperature} \xrightarrow{\text{DVFS}} \searrow \text{frequency} \implies \nearrow \text{runtime}$$

The same countermeasure can be used.