Journée thématique sur les attaques par injection de faute

Resistance of Isogeny-Based Cryptographic Implementations to a Fault Attack

Élise Tasso (CEA), elise.tasso2@cea.fr
joint work with Luca De Feo (IBM Research), Nadia El Mrabet (EMSE) and Simon Pontié (CEA)

to appear in the COSADE'21 proceedings, https://eprint.iacr.org/2021/850

September 23rd, 2021

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

1. Context: SIKE and physical attacks

2. Ti's theoretical fault attack on isogeny-based cryptography

3. Fault injection in a laboratory on a SIKE Keygen implementation

4. Countermeasure

Context: SIKE and physical attacks

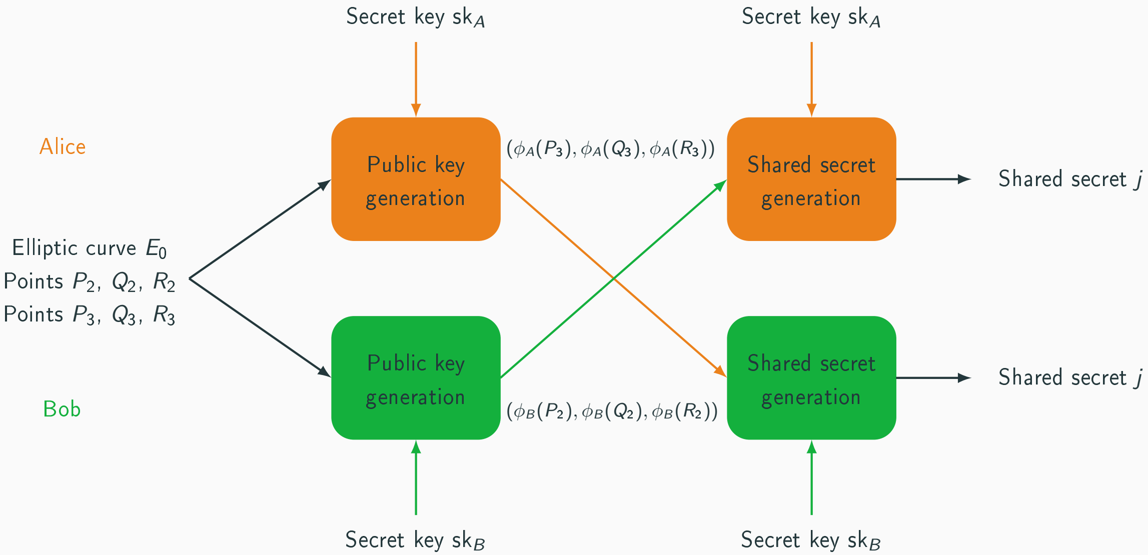
SIKE in the NIST PQC Standardization Contest

- Quantum computer threat.
- NIST Post Quantum Cryptography Standardization Contest for asymmetric cryptography algorithms (since 2016).

SIKE is one of the NIST alternate candidates for encryption and key encapsulation.

- The only one based on isogenies between elliptic curves.
- Relatively slow: on an Intel CPU, $(9681 + 10343) \cdot 10^3$ cycles for encapsulation + decapsulation **vs** $(1862 + 1747) \cdot 10^3$ cycles for the slowest among the other candidates at the lowest security level.
- Smallest public key size : 330 bytes (p434, uncompressed) **vs** 672 bytes for the smallest key among the other candidates at the lowest security level.

The SIDH key exchange



Why not use SIDH directly ?

- SIDH is mathematically insecure if one of the secret keys is static (Galbraith et al., 2016).
- SIKE is mathematically secure in "semi-static mode".

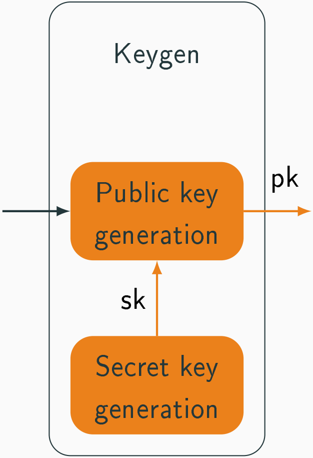
The SIKE mechanism

Public parameters

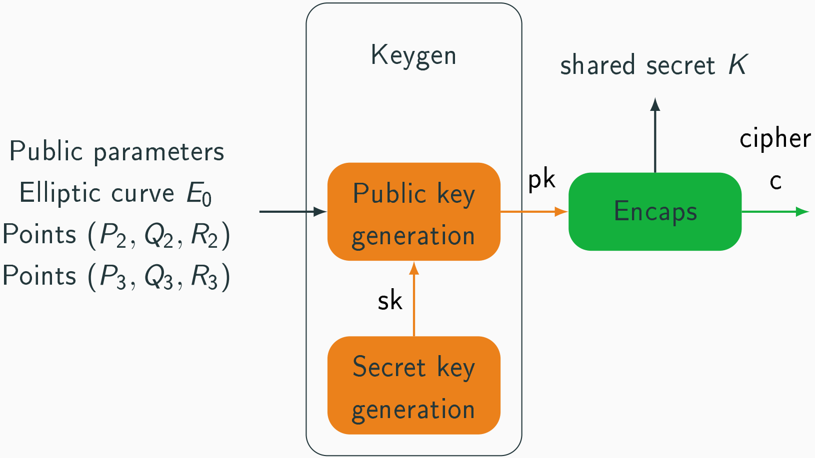
Elliptic curve E_0

Points (P_2, Q_2, R_2)

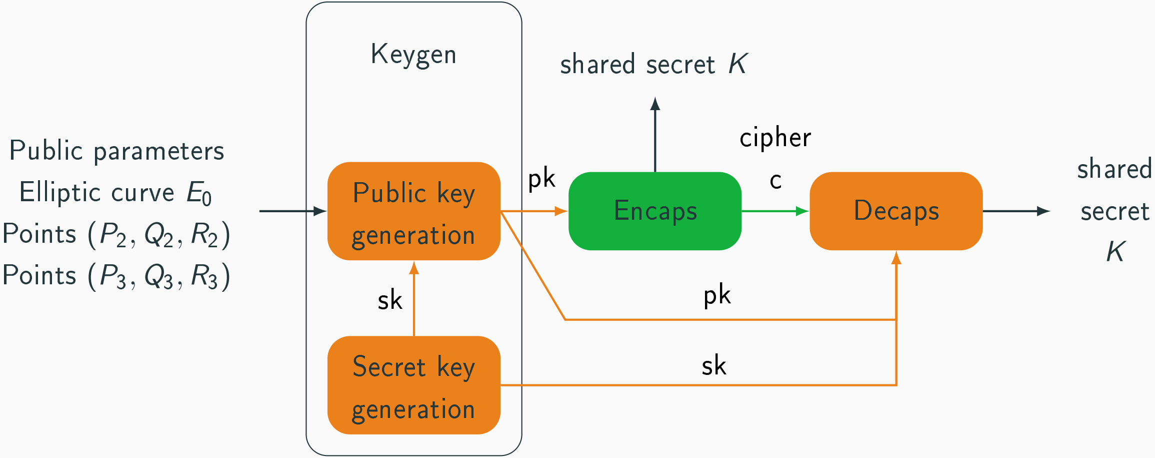
Points (P_3, Q_3, R_3)



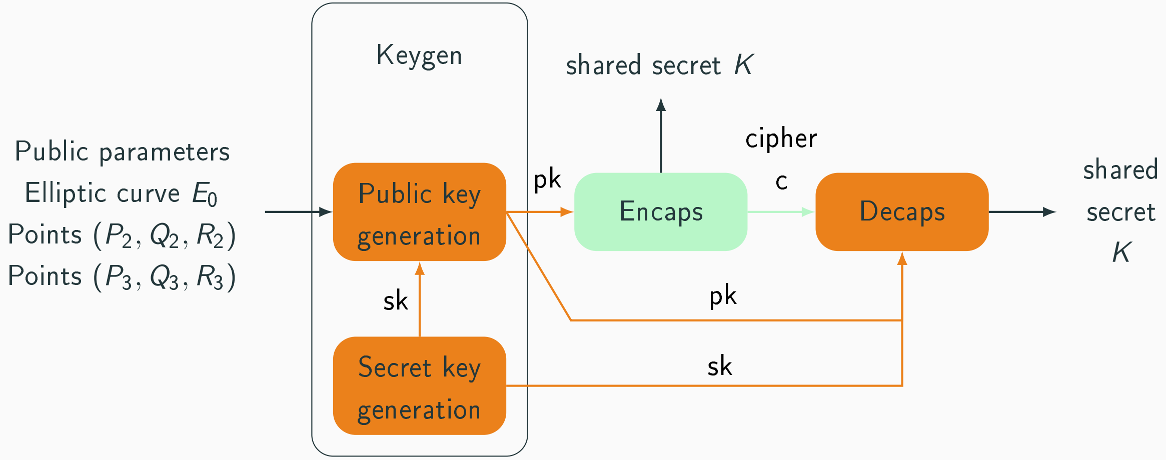
The SIKE mechanism



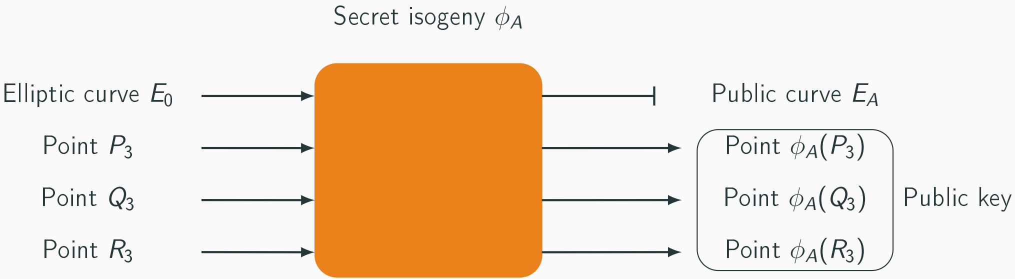
The SIKE mechanism



The SIKE mechanism



Public key computation in SIKE



Physical attacks on SIKE : state of the art

SIKE is believed to be mathematically secure, but physical attacks may exist depending on the implementation...

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

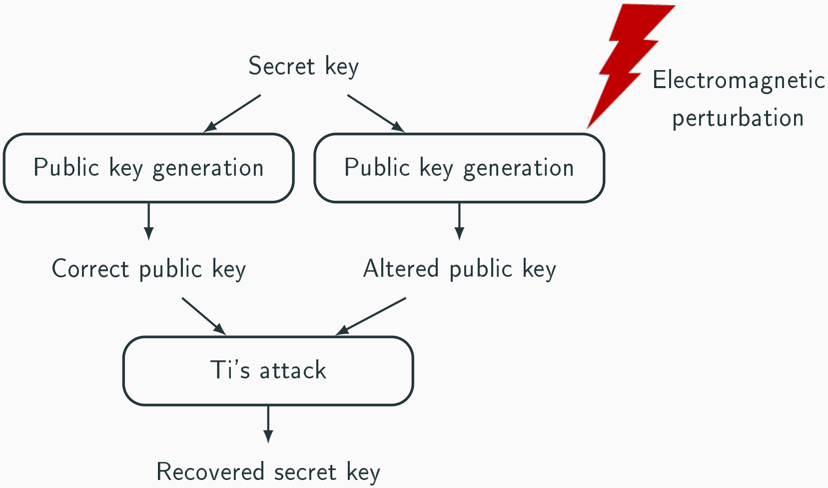
	Fault injection	**Side-channel attacks**
Theoretical	Yan Bo Ti, 2017	Koziel et al., 2017
Simulated	Gélin et al., 2017	none
Experimentally verified	**none**	Koppermann et al., 2018 Zhang et al., 2020

Our work

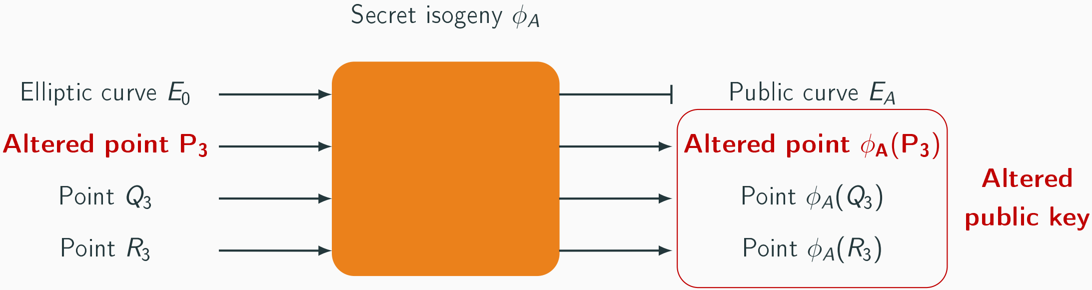
- Is Ti's 2017 fault attack on isogeny-based cryptosystems exploitable in practice ?
- What are fitting countermeasures ?

Ti's theoretical fault attack on isogeny-based cryptography

Threat model



Ti's theoretical attack

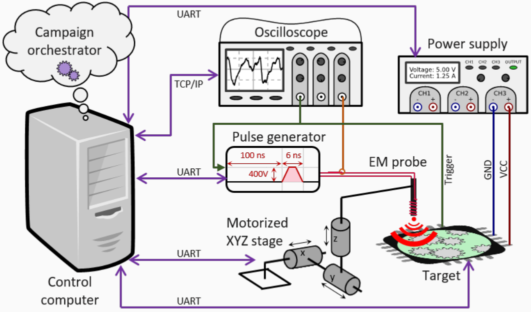


Fault injection in a laboratory on a SIKE Keygen implementation

Attacked SIKE implementation

- ARM v8 software implementation of the "key exchange" part of SIKE of the NIST PQC Standardization Process round 3 submission.
- Target choice: attack in a laboratory of a system on chip (SoC) with four cortex A53 cores at a 1.2 GHz frequency.
- Targeting an instruction we want to skip is arduous because of SoC latency (Gaine et al., WIFS 2020), but a great precision is not necessary to perform Ti's attack.

Set up of an attack campaign



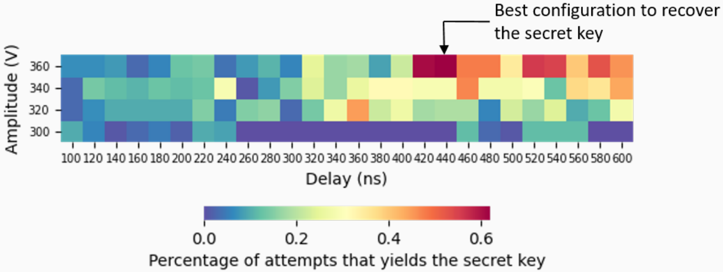
Set up for the realization of EM injection attack campaign

- Fixed probe.
- Fixed pulse width.
- Find the best (amplitude,delay) configuration to recover the secret.

1 040 000 attempts in 4.5 days.

Experimental results

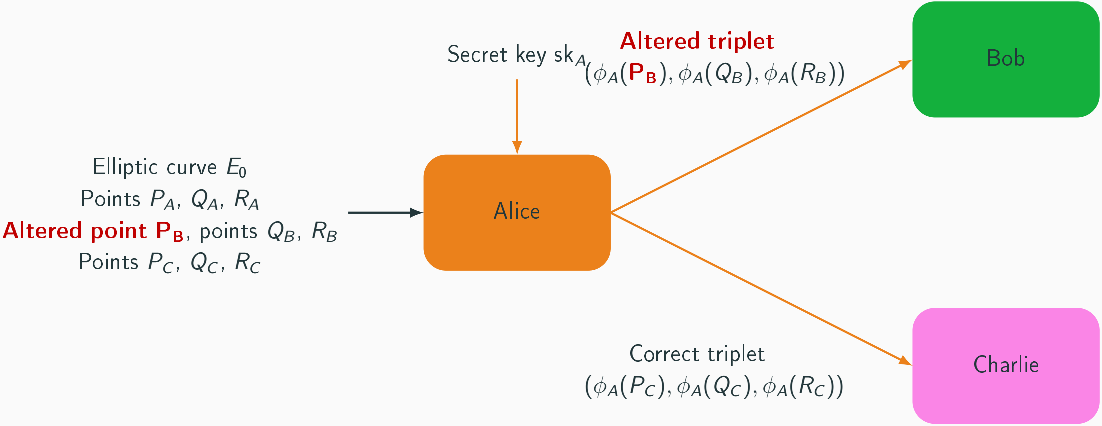
- Highest success rate for an amplitude of 360 V and a delay of 440 ns : 0.62%.
- In this case, one secret is found every 3 minutes and 10 seconds.



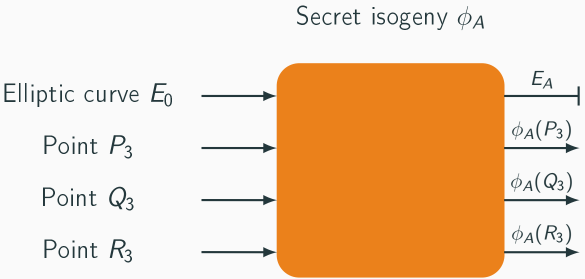
Countermeasure

Impact on SIKE

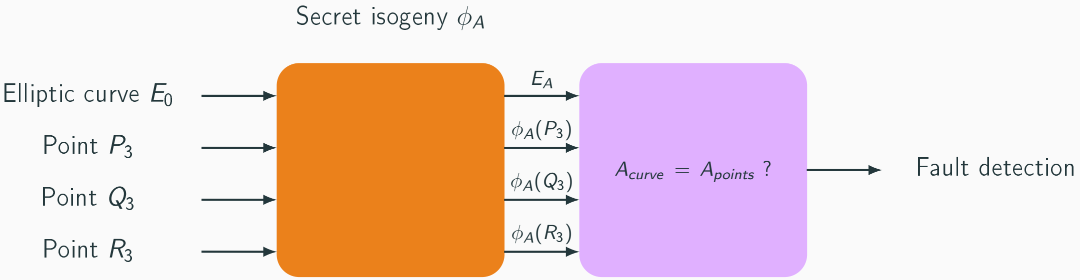
- SIKE is not broken, unless it is incorrectly implemented.
- However, in a multipartite key exchange the secret is used multiple times...



Countermeasure



Countermeasure



Conclusion

- Ti's attack is exploitable in practice if a secret is used more than once to generate a public key.
- Our countermeasure takes advantage of redundancy in SIKE's code and is cheap: there is a 1.5% overhead.
- The probability to detect a fault is high: $1 - \frac{1}{p^2}$ with $\frac{1}{p^2} \approx 1.67 \cdot 10^{-261}$ for SIKEp434.

More details...

The SIDH key exchange

SIDH : Supersingular isogeny Diffie-Hellman

Alice and Bob want to share a secret.
Public data:

- an elliptic curve E_0 defined on $\mathbb{F}_{p^2}$ with $p = 2^{e_2}3^{e_3} - 1$.
- points P_2, Q_2 of order 2^{e_2} and R_2 such that $R_2 = P_2 - Q_2$,
- points P_3, Q_3 of order 3^{e_3} and R_3 such that $R_3 = P_3 - Q_3$.

Secret keys:

- $\mathrm{sk}_2 \in [0, 2^{e_2 \log_2(2)} - 1]$ and
- $\mathrm{sk}_3 \in [0, 2^{e_3 \log_2(3)} - 1]$.

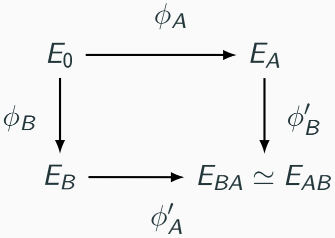
The SIDH key exchange

The associated secret isogenies are ϕ_A and ϕ_B such that

$$\mathrm{Ker}(\phi_A) = \langle P_2 + \mathrm{sk}_2 Q_2 \rangle \text{ and } \mathrm{Ker}(\phi_B) = \langle P_3 + \mathrm{sk}_3 Q_3 \rangle,$$

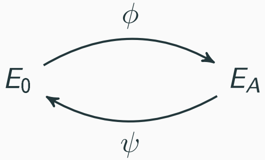
and ϕ'_A and ϕ'_B such that

$$\mathrm{Ker}(\phi'_A) = \langle \phi_B(P_2) + \mathrm{sk}_2 \phi_B(Q_2) \rangle \text{ and } \mathrm{Ker}(\phi_B) = \langle \phi_A(P_3) + \mathrm{sk}_3 \phi_A(Q_3) \rangle.$$



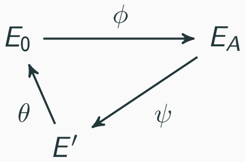
Ti's theoretical attack

- **Input:** $\phi(P_3)$, $\phi(Q_3)$, $\phi(R_3)$ and an altered point $\phi(\widetilde{P_3})$.
- **Method:** to determine ϕ of degree 2^{216}, we determine its dual τ. We have $\deg(\tau) = \deg(\phi)$.
- Computation of $T = 3^{137}\phi(\widetilde{P_3})$.
- Computation of isogeny ψ of kernel $\ker(\psi) = \langle T \rangle$.
- If $\deg(\psi) = \deg(\phi)$, then ψ is the dual of ϕ. We deduce ϕ.



Ti's theoretical attack

- If $\deg(\psi) < \deg(\phi)$, we use a brute force attack to recover θ such that $\theta \circ \psi$ i.e. the dual of ϕ.
- We deduce ϕ.



Note : If P_3 is not altered, $E' = E_A$ and computing θ is as difficult as finding Alice's secret isogeny.