MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

Safe-Error Attacks on SIKE and CSIDH

Fabio Campos[1] Juliane Krämer[2] Marcel Müller[2]

SPACE 2021 - December 11, 2021

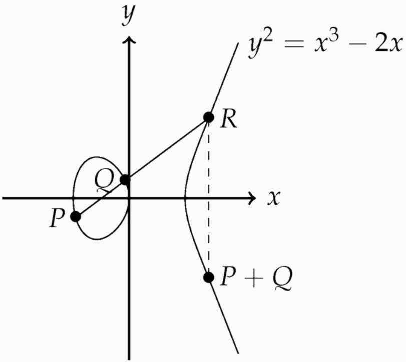
[1] Max Planck Institute for Security and Privacy, Germany
[2] Technische Universität Darmstadt, Germany

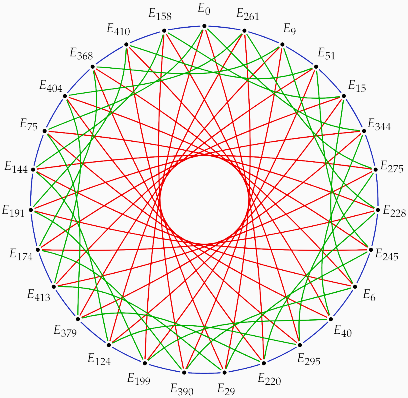
Motivation

- quantum computing $\rightarrow$ impact on cryptography
- NIST PQC standardization process
- isogeny-based youngest field of post-quantum cryptography
- only little attention with respect to fault attack resilience
- we aim to fill this gap

Preliminaries

ECC vs Isogeny





Fundamental operation: $P \mapsto [n]P$

Nodes: curves over $\mathbb{F}_{419}$

Edges: 3-, 5-, 7-isogenies

Fundamental operation: $\varphi_A : E_0 \to E_a$

Isogeny graph mostly "stolen" from Chloe Martindale

https://www.martindale.info/talks/QIT-Bristol.pdf

SIKE (Supersingular Isogeny Diffie-Hellman)

- key encapsulation
- over the quadratic extension field with $p = 2^n * 3^m \pm 1$
- alternate candidate at round 3 of NIST's (not a) competition
- four parameter sets: SIKEp434, SIKEp503, SIKEp610, SIKEp751.
- slow, but small key sizes

CSIDH (Commutative Supersingular Isogeny Diffie-Hellman)

- non-interactive key exchange protocol $\rightarrow$ potential drop-in replacement for Diffie-Hellman
- over F_p with $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small distinct odd primes
- private key $= (e_1, \ldots, e_n)$, where $|e_i| =$ number of isogenies of degree ℓ_i ($\sim$ steps in the graph)
- not submitted to NIST's process designed after deadline
- post-quantum security under discussion
- even slower, but small key sizes

Safe-Error Attacks

- adversary uses fault injections to perturb a specific location
- presence or absence of an error gives insight into the ”codepath”
- memory (M) safe-error: the attacker modifies the memory
- computational (C) safe-error: computation attacked (skipping instructions)

Practical Experiments

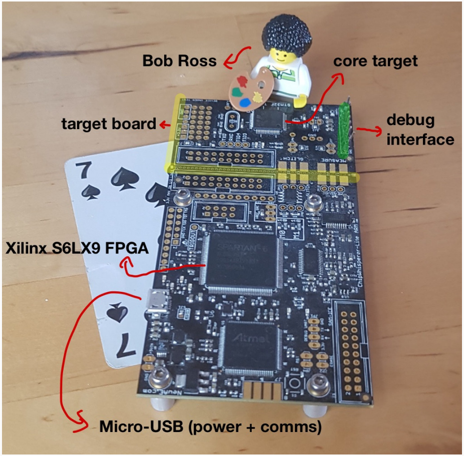
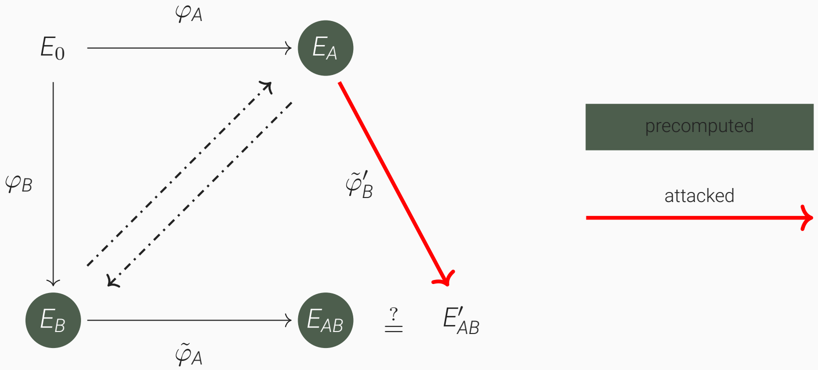


Figure 1: ChipWhisperer cw1173

- ChipWhisperer-Lite ARM
- 32-bit STM32F303
- open source toolchain
- power analysis
- voltage and clock glitching

- attacker performs single fault injection per run
- check if fault impacts shared secret
- Bob's, Alice's public key, and shared secret precomputed
- computation of shared secret attacked



Attacking SIKE

- SIKEp434 Cortex-M4 implementation available at pqm4[1]
- vulnerability remains the same across all available implementations
- 21,800 fault injections (100 injections for each bit)
- injections during computation of the three-point ladder
- number of injections for full key recovery only depends on length of private key
- critical spots empirically determined with manageable effort

[1] https://github.com/mupq/pqm4

Attacking SIKE 2/2

```
[...]
// main loop
for (i = 0; i < nbits; i++) {
    bit = (m[i >> LOG2RADIX] >> (i & (RADIX-1))) & 1;
    swap = bit ^ prevbit;
    prevbit = bit;
    mask = 0 - (digit_t)swap;

    swap_points(R, R2, mask);
    xDBLADD(R0, R2, R->X, A24);
    fp2mul_mont(R2->X, R->Z, R2->X);
}
[...]
```

Listing 1: LADDER3PT@SIKE

Attacking CSIDH

- reduced the key space in CSIDH512 from 11^{74} to 3^2
- attacker aims to distinguish a real from a dummy isogeny
- degree of attacked isogeny recovered with manageable effort
- 5,000 fault injections with high accuracy
- injections during the isogeny computation
- number of injections depends on many aspects

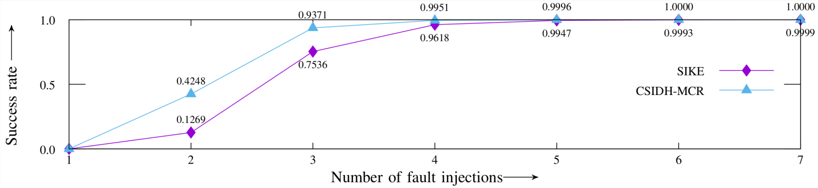
key	# of trials	faulty shared secret	accuracy
$S_1 = (-1, 1)$	2500	0.0%	100.0%
$S_2 = (0, 1)$	2500	92.4%	92.4%

Table 1: Results for CSIDH attacking the first isogeny

```
[...]
bool xISOG(proj *A, ..., int mask)
{
    proj Acopy = *A;
    [...]
    // calculate new curve A
    [...]
    // CONSTANT TIME : swap back
    fp_cswap(&A->x, &Acopy.x, mask);
    fp_cswap(&A->z, &Acopy.z, mask);
    [...]
}
[...]
```

Listing 2: xISOG@CSIDH

Results



SIKE

- 5 fault injections at each bit leads to success rate above 99%
- full key recovery requires about 4 hours

CSIDH/MCR

- 1184 injections required for full key recovery
- full key recovery requires about 98 hours

Conclusions

- no big scandal
- securing cryptosystems against safe-error attacks is non-trivial
- dummy-free implementations of CSIDH, not vulnerable to the attacks
- more effort into the cryptanalysis of post-quantum candidates
- ChipWhisperer: perfectly adequate

Thank you for your attention!

Paper: https://eprint.iacr.org/2021/1132
Code: https://github.com/Safe-Error-Attacks-on-SIKE-and-CSIDH/SEAoSaC