Practical Fault Injection Attacks on Constant Time CSIDH and Mitigation Techniques

Jason LeGrow

Virginia Tech, USA

Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) is an isogeny-based key exchange protocol which is believed to be secure even when parties use long-lived secret keys. To secure CSIDH against side-channel attacks, constant-time implementations with additional dummy isogeny computations are employed. In this study, we demonstrate a fault injection attack on the constant-time real-then-dummy CSIDH to recover the full static secret key. We prototype the attack using voltage glitches on the victim STM32 microcontroller. The attack scheme, which is based on existing research which has yet to be practically implemented, involves getting the faulty output by injecting the fault in a binary search fashion. Our attack reveals many practical factors that were not considered in the previous theoretical fault injection attack analysis, e.g., the probability of a failed fault injection. We bring the practice to theory and developed new complexity analysis of the attack. Further, to mitigate the possible binary search attack on real-then-dummy CSIDH, dynamic random CSIDH was proposed previously to randomize the order of real and dummy isogeny operations. We explore fault injection attacks on dynamic random CSIDH and evaluate the security level of the mitigation. Our analysis and experimental results demonstrate that it is infeasible to attack dynamic random CSIDH in a reasonable amount of time when the success rate of fault injection is not consistent over time.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T10