Fault Attacks Friendliness of Post-quantum Cryptosystems

Alessandro Barenghi, Gerardo Pelosi
Department of Electronics, Information and Bioengineering - DEIB
Politecnico di Milano
Milan, Italy
Email: *name.surname*@polimi.it

2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC) | 979-8-3503-4252-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/FDTC60478.2023.00006

***Abstract*—Post-quantum cryptosystems are often designed starting from a public key encryption algorithm and augmented with widely recognized cryptographic constructions, which in turn are shared among the majority of proposals and create common targets for fault attacks, but also opportunities for overarching countermeasures. In this talk, we survey the fault resilience of these recurring structures in both Key Encapsulation Methods (KEMs) and signature schemes, taking as case studies both the current KEMs selected for the fourth round in the US NIST standardization process, and its on-ramp for post-quantum signatures.**

***Index Terms*—Post-quantum cryptosystems, Cryptographic protocols, Fault attacks**

I. Summary

The significant societal push for the construction of large scale quantum computers [1], due to their capability of substantially reducing the solution time for computationally hard problems, also pushes for the design and prompt adoption of cryptographic primitives built on problems that are computationally hard also for a quantum computer. This in turn has spurred national standardization entities, such as the US NIST to issue a call for proposals for both asymmetric encryption schemes and digital signatures [2], managed as an international competition started in 2017. The competition is now in its fourth round, having selected one candidate for standardization in both the asymmetric encryption primitives and two digital signatures (Kyber, Dilithium and Falcon, respectively), and going forward with the intent of enlarging the portfolio of ciphers with primitives based on different computationally hard problem. In particular, three key encapsulation methods are still under evaluation (BIKE, HQC, and Classic McEliece), and a separate additional call for digital signature systems was issued in September 2022 [3].

From an engineering standpoint, the large majority of KEMs involved in this standardization effort share a common structure, due to the adoption of widely recognized cryptographic constructions [4] to turn weakly secure (i.e., OW-CPA or IND-CPA) public key encryption (PKE) algorithms into strongly secure (i.e., IND-CCA2) ones. Furthermore, a well known and common construction to build digital signature systems, starting from interactive identification schemes, is the one originally proposed by Fiat and Shamir in [5]. The widespread use of such constructions has the potential of making both attacks and countermeasures somehow portable across different cryptosystems. A further engineering challenge is posed by some of the PKE algorithms that do not enjoy perfect correctness, that is, it is possible for them not to correctly decrypt a valid ciphertext [6]. Often, such decryptions reveal information on the value of the private key, turning an apparent reliability-only issue into a security one. While the designers of such ciphers tackled this problem through the adoption of appropriate constructions, bringing fault attacks into the picture allows to overcome the provided mathematical and algorithmic guarantees.

This talk will survey and systematize the current state of fault attacks and countermeasures against post-quantum cryptosystems, highlighting research directions for designers and implementors.

References

[1] M. Biondi and A. Heid, "Quantum computing use cases are getting real – what you need to know," McKinsey's Report, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know, Dec 2021.

[2] US National Institute of Standards and Technology, "Post-Quantum Cryptography - Call for Proposals," https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals, 2017.

[3] ——, "Post-Quantum Cryptography: Digital Signature Schemes - Additional call for proposals," https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals, 2023.

[4] D. Hofheinz, K. Hövelmanns, and E. Kiltz, "A Modular Analysis of the Fujisaki-Okamoto Transformation," in *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, ser. Lecture Notes in Computer Science, Y. Kalai and L. Reyzin, Eds., vol. 10677. Springer, 2017, pp. 341–371. [Online]. Available: https://doi.org/10.1007/978-3-319-70500-2_12

[5] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," in *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, ser. Lecture Notes in Computer Science, A. M. Odlyzko, Ed., vol. 263. Springer, 1986, pp. 186–194. [Online]. Available: https://doi.org/10.1007/3-540-47721-7_12

[6] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "Analysis of In-Place Randomized Bit-Flipping Decoders for the Design of LDPC and MDPC Code-Based Cryptosystems," in *E-Business and Telecommunications - 17th International Conference on E-Business and Telecommunications, ICETE 2020, Online Event, July 8-10, 2020, Revised Selected Papers*, ser. Communications in Computer and Information Science, M. S. Obaidat and J. Ben-Othman, Eds., vol. 1484. Springer, 2020, pp. 151–174. [Online]. Available: https://doi.org/10.1007/978-3-030-90428-9_7