On the Feasibility of Side-Channel Attacks on Lattice-based KEMs using Gaussian Sampling

Soundes Marzougui[1], Ievgen Kabin[2], Thomas Aulbach[3], Juliane Krämer[3], and Jean-Pierre Seifert[1,4]

[1] Technische Universität Berlin, Germany
soundes.marzougui@tu-berlin.de
Jean-Pierre.Seifert@external.telekom.de
[2] Innovations for High Performance Microelectronics Institute
kabin@ihp-microelectronics.com
[3] Universität Regensburg, Regensburg, Germany
{thomas.aulbach, juliane.kraemer}@ur.de
[4] Fraunhofer Institute for Secure Information Technology, Germany

Abstract. We present a single-trace attack against lattice-based KEMs that use Gaussian sampling and execute it in a real-world environment. Our analysis takes a single power trace of the decapsulation algorithm as input and exploits leakage of the Cumulative Distribution Table (CDT) sampling subroutine to reveal the session key. We investigate the feasibility of the attack and proved that the power consumption traces become less informative with higher clock frequencies. Therefore, we introduce a machine-learning noise technique, which enhances the accuracy of our attack and leverages its success rate to 100%. We underscore the necessity to mitigate this kind of attack and introduce a base sampler that samples from a much smaller standard deviation. We provide a proof-of-concept implementation of our attack and optimized implementation of our countermeasure.
We accomplish the attack exemplarily on FrodoKEM, a lattice-based KEM, and third-round NIST alternate candidate. We execute it on an STM32F4 victim board clocked at different frequencies 7, 30, and 100 MHz. Furthermore, we show that our implementation improves not only the physical security of FrodoKEM against single trace attacks but also its efficiency as compared to the reference implementation.

Keywords: FrodoKEM, Gaussian sampler, Machine-Learning, Post-quantum cryptography, Power analysis, Side-channel analysis