ANTRAG: Annular NTRU Trapdoor Generation

Making MITAKA As Secure As FALCON

Thi Thu Quyen NGUYEN
(3^{rd} year PhD student in University of Caen, Normandie, France)
with Thomas Espitau, Chao Sun, Mehdi Tibouchi, Alexandre Wallet.

Abstract. In 2022, NIST decided to adopt the lattice-based signature FALCON [FHK+19] for post-quantum standardization due to its advantages in speed and compactness. FALCON's signatures are generated as Gaussian vectors from trapdoor sampling. However, the sampler's complex design poses challenges in implementation, parallelization, protection against side-channels. FALCON is also strict on parameter selections, in particular, it is not suited for instantiation over non-power-of-two-dimensional rings to achieve intermediate security levels.

At Eurocrypt 2022, MITAKA [EFG+21] was introduced as a variant of FALCON. It utilizes Prest's hybrid sampler, a much simpler Gaussian sampler, which allows for parallelization, and is compatible with non-power-of-two-dimensional settings. However, when naively feeding trapdoors generated from the same approach as FALCON to Prest's sampler, the resulting signatures have far lower security in equal dimension. In MITAKA paper, certain randomness-recycling techniques were additionally employed to partially compensate this security loss. In the end, MITAKA has slower key generation and is still substantially less secure than FALCON (by around 20 to 50 bits of CoreSVP security depending on the parameters).

In this work, we reassess MITAKA's key generation algorithms. I will present Antrag, a novel technique for generating trapdoors that better complements Prest's hybrid sampler. Antrag offers simple keygen algorithms which return trapdoors that confidently reach the same NIST security levels as FALCON. Additionally, it is faster than the original MITAKA and even achieves similar speed to FALCON. Antrag is also adaptable to accommodate rings of intermediate dimensions, providing the same flexibility in ring selection as MITAKA. Furthermore, our thorough control over Antrag's behavior allows us to safely explore alternative parameter selections.

References

EFG+21. Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. Mitaka: a simpler, parallelizable, maskable variant of falcon. Cryptology ePrint Archive, Paper 2021/1486, 2021. https://eprint.iacr.org/2021/1486.

FHK+19. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. 2019.