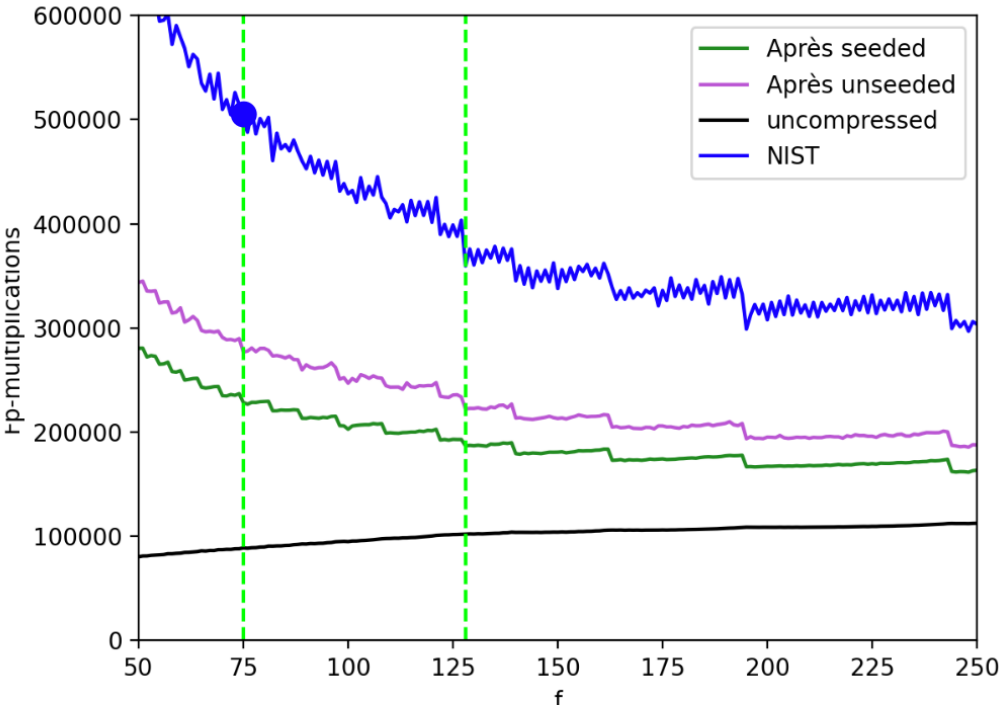
6G-RIC
Research and
Innovation Cluster

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Optimizations of Isogeny-Based Post-Quantum Signatures

MICHAEL MEYER

Can we make the performance of the SQIsign signature scheme practical enough for practical applications such as 6G use cases?



Performance of the verification process of SQIsign for the NIST submission (blue) and different optimized variants, including an uncompressed variant. The x-axis refers to the parameter f used in SQIsign, while the y-axis shows the verification performance. The blue dot at f=75 shows the current performance of the NIST variant. Our work allows to (i) increase the size of f and (ii) move to the improved variants shown in purple, green, and black.

KEY FINDINGS

Quantum-resistant cryptography is a key ingredient for all future network protocols to guarantee security even when large-scale quantum computers exist. Especially the signature schemes submitted to the recent NIST standardization process are a research focus in this area. Due to the small signature and key sizes and relatively fast verification process, the isogeny-based scheme SQIsign is a very interesting candidate for situations where signatures are verified on embedded devices, which includes 6G-specific use cases. To enhance its advantages, we optimized the performance of the verification process through several high- and low-level techniques, such as better parameters or improved algorithms. We reach speed-up factors up to 4.4, and conclude that SQIsign can be seen as a viable option for suitable use cases featuring signature verification on IoT devices.

M. Corte-Real Santos, J. K. Eriksen, M. Meyer, K. Reijnders. "AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing". EUROCRYPT 2024.

M. Corte-Real Santos, J. K. Eriksen, M. Meyer, F. Rodríguez-Henríquez. "Finding Practical Parameters for Isogeny-based Cryptography". IACR Communications in Cryptology, 1(3), 2024.