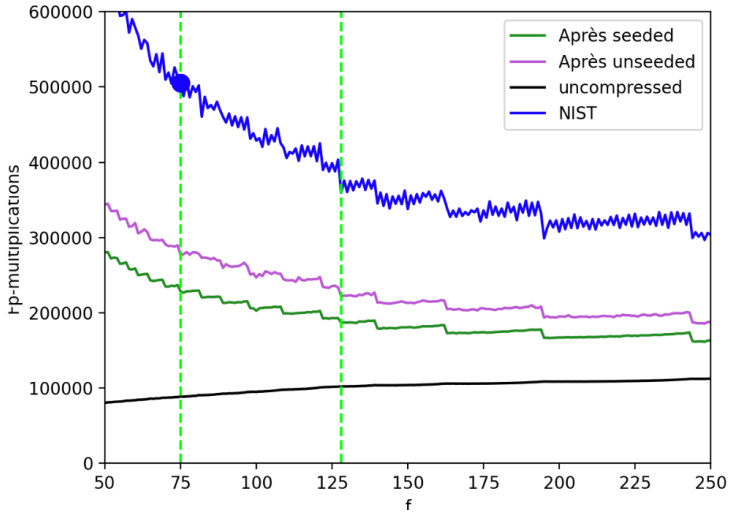
GEFÖRDERT VOM
Bundesministeriu
für Bildung
und Forschung

# Performance and BUFF-Security Analysis of Post-Quantum Signatures

THOMAS AULBACH, MARIA CORTE-REAL SANTOS, SAMED DÜZLÜ, JONATHAN KOMADA ERIKSEN, MICHAEL MEYER, KRIJN REIJNDERS, PATRICK STRUCK, MAXIMILIANE WEISHÄUPL

## Can we make the performance of the SQIsign signature scheme more practical? Do post-quantum signatures in the NIST standardization satisfy the advanced BUFF security notions?




| Scheme | S-CEO | S-DEO | MBS | NR | Type |
|---|---|---|---|---|---|
| Cross [3] | ✓ | ✓ | ✓ | ✓ | Code (Sect. 3) |
| Less [2] | ✓ | ✓ | ✓ | ✗ | |
| Meds [12] | ✓ | ✓ | ✓ | ✗ | |
| Wave [4] | ✗ | ✗ | ✗ | ✗ | |
| SQISign [10] | ✦ | ✓ | ✓ | ✗ | Isogeny (Sect. 4) |
| Haetae [11] | ✓ | ✓ | ✓ | ✓ | Lattice (Sect. 5) |
| Hawk [9] | ✓ | ✓ | ✓ | ✓ | |
| HuFu [36] | ✗ | ✗ | ✓ | ✗ | |
| Raccoon [16] | ✓ | ✓ | ✓ | ✓ | |
| Squirrels [20] | ✗ | ✗ | ✗† | ✗ | |
| Mayo [6] | ✗ | ✗ | ✓ | ✗ | Multivariate (Sect. 6) |
| Prov [23] | ✓ | ✓ | ✓ | ✓ | |
| QR-UOV [21] | ✗ | ✗ | ✓ | ✗ | |
| Snova [35] | ✗ | ✗ | ✓ | ✗ | |
| Tuov [17] | ✗ | ✗ | ✓ | ✗ | |
| Uov [7] | ✗ | ✗ | ✓ | ✗ | |
| Vox [32] | ✗† | ✗† | ✓ | ✗† | |

*(left) 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 performance. The blue dot at f=75 shows the current performance of the NIST variant. (right) Digital signature schemes submitted to the NIST standardization and their security with respect to the advanced BUFF security notions. Ticks and crosses show that schemes satisfy resp. do not satisfy the notions S-CEO, S-DEO, MBS, and NR.*

### KEY FINDINGS

Quantum-resistant cryptography is a key ingredient for all future network protocols. Especially the signature schemes submitted to the recent NIST standardization effort are a research focus in this area. SQIsign is a very interesting candidate for situations where each signature is verified often, but its verification may not be fast enough in some cases. To enhance its advantages, we optimized the performance of the verification process through several high- and low-level techniques, such as better parameters. 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 signatures that are verified often. Furthermore, in a separate work, we analyzed the advanced BUFF security notions for many candidate signature schemes, labeled as "desirable feature" by NIST. However, only few submissions consider BUFF security. We found that most schemes do not satisfy all notions, while the number of satisfied notions varies between schemes. We further show that simple changes are enough to reach all BUFF notions for most of the submitted schemes.

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

*T. Aulbach, S. Düzlü, M. Meyer, P. Struck, M. Weishäupl. "Hash your Keys before Signing: BUFF Security of the Additional NIST PQC Signatures".*