

Beullens, Ward; Dobson, Samuel; Katsumata, Shuichi; Lai, Yi-Fu; Pintore, Federico. Group signatures and more from isogenies and lattices: generic, simple, and efficient : [review]

Henno, Jaak Zentralblatt MATH 2024 / 1 p. <https://zbmath.org/1530.94050>

An experimental study of building blocks of lattice-based NIST post-quantum cryptographic algorithms

Imran, Malik; Abideen, Zain Ul; Pagliarini, Samuel Nascimento Electronics 2020 / art. 1953, 26 p. : ill

<https://doi.org/10.3390/electronics9111953> Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Identifying obstacles of PQC migration in e-Estonia

Vakarjuk, Jelizaveta; Snetkov, Nikita; Laud, Peeter 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon) 2024 / p. 63-81 <https://doi.org/10.23919/CyCon62501.2024.10685570> Conference proceedings at Scopus Article at ScopusScopus Article at WOS

Post-quantum trails: an educational board game about post-quantum cryptography

Vakarjuk, Jelizaveta; Snetkov, Nikita Proceedings of the 7th International Conference on Historical Cryptology (HistoCrypt 2024) 2024 / p. 244-248 : ill <https://dspace.ut.ee/items/1e6331fb-6e1c-4374-a2c1-2ef2eab3190a> <https://doi.org/10.58009/aere-perennius0115>

A systematic study of lattice-based NIST PQC algorithms : from reference implementations to hardware accelerators

Imran, Malik; Abideen, Zain Ul; Pagliarini, Samuel Nascimento arXiv.org 2020 / 36 p. : ill

Zheng, Zhiyong; Tian, Kun; Liu, Fengxia. Modern cryptography. Volume 2. A classical introduction to informational and mathematical principle : [review]

Henno, Jaak Zentralblatt MATH 2023 / 1 p. <https://zbmath.org/1520.94001>