Lattice cryptography: isomorphisms & dual attacks

Pulles, L.N.

LATTICE CRYPTOGRAPHY: ISOMORPHISMS & DUAL ATTACKS

Ludo N. Pulles

Post-Quantum Cryptography · Lattices · Cryptanalysis · Heuristics · Learning with Errors · Dual Attack · Fast Fourier Transform · Bessel Functions · Lattice Isomorphism Problem · Signatures · Concrete Design · Automorphism

L.N. Pulles

LATTICE CRYPTOGRAPHY:
ISOMORPHISMS & DUAL ATTACKS