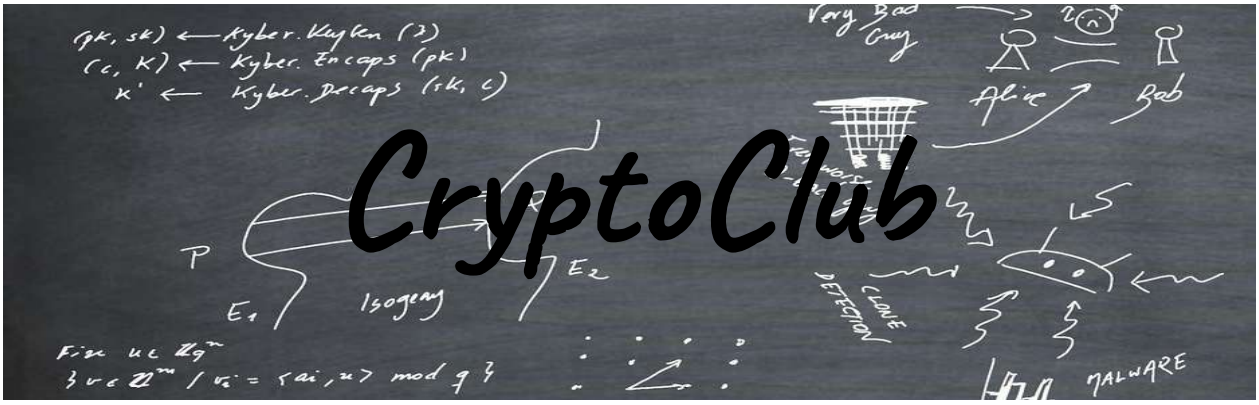

TJERAND SILDE

NTNU Norway.

JUEVES 29 DE MARZO, 13:00 to 14:15 hrs (*snacks and refreshments afterwards!)*

Aula Adoración de Miguel (1.2.C16, edificio Betancourt)

Olingo: Efficient, Distributed, Non-Interactive, and Identifiable Threshold Lattice Signatures

Abstract

We propose a new and efficient threshold lattice signature framework called Olingo. Our framework is compatible with the most efficient rejection-free lattice signature scheme Raccoon (Crypto 2024) and offers all the desired properties required for implementing threshold signatures from standard quantum safe assumptions in real-world systems: small keys and signatures, few rounds and reasonable communication, non-interactive signing, distributed key generation, and identifiable aborts. Olingo is the only scheme satisfying all of these requirements.

Identifiable aborts are particularly important; otherwise, a malicious party could misbehave in the signature computation so that the final signature does not verify and there is no mechanism to identify the malicious party and remove it from the protocol. This can lead to a denial-of-service attack and prevent honest users from ever producing a signature. Our starting point is the framework by Gur, Katz, and Silde (PQCrypto 2024). We change the underlying signature scheme, go from two to three rounds of communication, and then apply numerous improvements and optimizations for our state-of-the-art instantiation with all the above properties. We provide a detailed proof of security for the new framework and its properties, and present concrete parameters and benchmarks.

For 128 bits of security, up to 1024 users, and 2^{60} signatures, we provide verification keys of 3.8 KB, signatures of 12.9 KB, and communication of 432 KB total per party. An optimistic non-interactive version of our scheme requires only 82 KB in online communication per party when the message to be signed is known.

This is joint work with Kamil Doruk Gur (UMD), Patrick Hough (Oxford), Jonathan Katz (Google / UMD), and Caroline Sandsbråten (NTNU).