Information Leakage and Code-Based Cryptography

Giovanni Tognolini (Università di Trento)

Abstract: The talk aims to highlight some critical aspects in the development of code-based digital signature schemes following the hash&sign framework, taking as an example a signature scheme presented at ICISC 2023. To achieve this goal, we will first outline the historical context regarding code-based cryptography and how the cryptographic community has approached the challenge of designing code-based signature schemes. Having outlined this, we analyze HWQCS, a scheme that uses quasi-cyclic low density parity check codes (QC-LDPC). The scheme introduces high Hamming weight errors and signs each message using a fresh ephemeral secret key rather than using only one secret key, so to avoid known attacks on QC-LDPC signature schemes. In this talk, we show that the signatures of HWQCS leak substantial information concerning the ephemeral keys and formally describe this behavior. It turns out that for some signatures the leakage is large enough to allow us to completely reconstruct the ephemeral values. With this knowledge we will be able to mount a universal forgery attack.