Post-quantum security of cryptographic transformations in the random oracle model

Huang, Y.

Post-Quantum Security of Cryptographic Transformations in the Random Oracle Model

Yu-Hsuan Huang (黃右萱)

Post-Quantum Security of Cryptographic Transformations in the Random Oracle Model

In cryptography, generic transformations are often used to strengthen simpler but weaker schemes, into more sophisticated and stronger ones.

This thesis aims to establish rigorous, provable notions of security for various such transformations that are relevant in the scope of post-quantum cryptography.

We achieve this via formal mathematical proofs, and in some cases, via proposing new security definitions, when existing ones are inadequate. Most analyses are treated in an idealized setting known as the random oracle model.