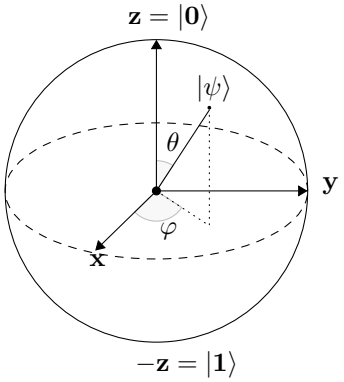
Superposition Attacks on Cryptographic Primitives



Problem description

The security of (post-quantum) schemes and protocols is usually assessed with regards to security properties, e.g. security against chosen ciphertext adversaries. The introduction of quantum technology has lead researchers to introduce new classes of attacks, e.g. quantum chosen ciphertext attacks, where an adversary is given access to superposition queries. Indeed many (symmetric) cryptographic primitives, such as multiple variants of MACs of block cipher modes of operations have been shown to be broken in this new model.

This work focuses on analyzing superposition attacks on (symmetric) cryptographic primitives, thus extending the existing results. In particular, one may consider new constructions used in lightweight or embedded cryptography. Vice versa one may study the flaws leading to the insecurity against quantum chosen ciphertext attacks and design new primitives that overcome these insecurities.

Keywords

superposition attacks, cryptographic primitive, cryptanalysis

Remarks

Prior knowledge of quantum computing and symmetric cryptography is recommended.

Point of contact

Level:	Master	
Supervisor:	Prof. Dr. Jörn Müller-Quade	
Daily supervisor:	Marcel Tiepelt	marcel.tiepelt@kit.edu