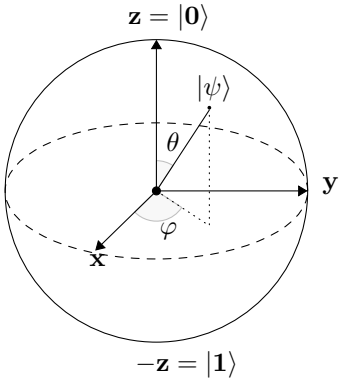
Device Independence in Quantum Cryptography



Problem description

Quantum cryptography exploits the fundamental laws of physics, in particular quantum mechanics, to perform cryptographic tasks such as encryption or key exchange. The most famous example thereof is the quantum key distribution, allowing two parties, Alice and Bob, to exchange a shared secret even in the presence of an unlimited adversary. Indeed the security is not based on *human made* cryptographic assumptions but on our current understanding of the universe.

However, quantum cryptography has some common weaknesses with classical cryptography: The implementations are not perfect. That means, that the underlying physical devices, in example the photon sources, do not provide perfect streams of single photons but instead may output a bunch of photons at once. Therefore, we consider the concept of *device-independence* in quantum cryptography, i.e. if the security of the quantum cryptographic protocol holds independently of the underlying physical device.

The aim of this thesis is to study known quantum protocols and their constructions to achieve device independence. On the other side, one might analyze the protocols to identify flaws resulting from imperfect implementations.

Keywords

quantum, cryptanalysis, unconditional security

Remarks

Prior knowledge of quantum computing or a background in physics is strongly recommended.

Point of contact

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

References

[1] Stefano Pironio et al. "Device-independent quantum key distribution secure against collective attacks." In: *New Journal of Physics* 11.4 (Apr. 2009), p. 045021. DOI: 10.1088/1367-2630/11/4/045021. URL: https://doi.org/10.1088%2F1367-2630%2F11%2F4%2F045021.