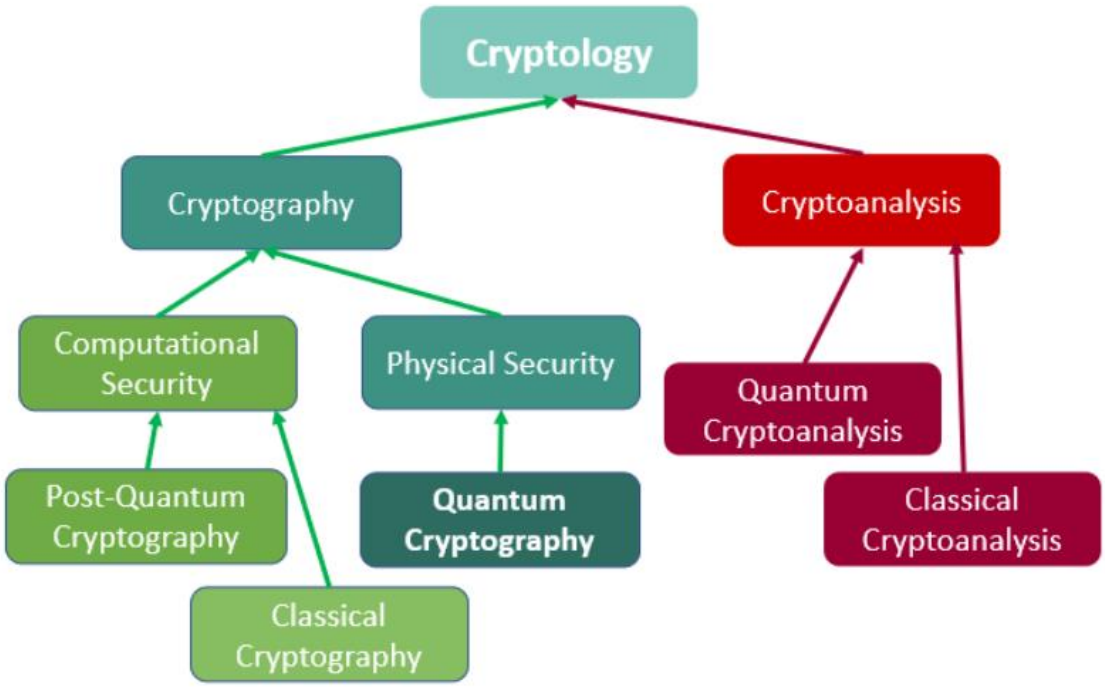
Building Quantum Cryptography Knowledge Graph and Ontology



GHZ state

Marta Misiaszek-Schreyner

Definition

Greenberger–Horne–Zeilinger state (GHZ state) is a specific type of multipartite entanglement that involves N qubits (at least three). It was first studied in 1989 by Daniel Greenberger, Michael Horne and Anton Zeilinger [1].

Description

Mathematically, N-qubit GHZ state can be written as

$$|\psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}\left(|\underbrace{00\ldots0}_{N}\rangle + |\underbrace{11\ldots1}_{N}\rangle\right). \tag{1}$$

As it can be seen it is a quantum superposition of N subsystems being in state 0 with all of them being in state 1, thus the GHZ state is a maximally entangled quantum state.

GHZ state is used in many quantum protocols and algorithms [2], among which one of most important is CKA.

References

[1] D.M. Greenberger, M.A. Horne, A. Zeilinger, *Going beyond Bell's Theorem*, arXiv:0712.0921, DOI: https://doi.org/10.48550/arXiv.0712.0921 (2007).

[2] D. Cruz et al., *Efficient Quantum Algorithms for GHZ and W States, and Implementation on the IBM Quantum Computer*, Adv. Quantum Technol. **2**, 1900015, DOI: https://doi.org/10.1002/qute.201900015 (2019).

QKD

Mirek Sopek

March 15, 2022

Definition

Quantum Key Distribution (QKD) is a provably secure communication method which implements a cryptographic protocol based on quantum mechanical properties. QKD is the most important methods of quantum cryptography. It guarantees two parties exclusive sharing of a random secret key that can be used for encryption and decryption of messages with the use of algorithms like One-Time Pad (OTP) which represent highest possible security of information exchange.

Description

The purpose of QKD is to guarantee that between the two parties, it is possible to agree on a certain random key useful for the cryptographic algorithms even in a situations where the presence of a information theft is possible.

Unlike classical key distribution systems, QKD allows for secure sharing of the key, even if the theft has access to unlimited computational resources. Its security is proven in terms of the basic laws of quantum physics, instead of the difficulty of some mathematical problem which is the base of the security of both classical and post-quantum cryptography branches.

QKD was developed in 1984 by Bennett and Brassard [1]. Their original and ingenious method (nicknamed BB84) was inspired by the work on conjugate coding of Stephen Wiesner [2]. In general, Bennett's and Brassard approach exploits uncertainty principle of quantum mechanics. In 1991, Artur Ekert has proposed an independent approach which is based on quantum entanglement [3]. Ekert's method (nicknamed E91) was inspired by the work of Einstein, Podolsky and Rosen (known as EPR paradox).

To achieve the secure key distribution, QKD uses both quantum communication channel and various classical protocols. Thus, the QKD method represent a blend of the quantum communication methods and the trusted classical cryptographical approach. The key exchange is usually split into the Quantum Communication Stage (QCS) and a classical post-processing stage. In other words, QKD protocol assumes the use of quantum channel and an authenticated classical channel.

The security of QKD is based on the impossibility to gain information about the data transmitted via quantum channel during the Quantum Communication Stage. Any attempt to do so by an adversary causes an irrecoverable disruption in the transmission that can be detected by communicating agents (honest parties). This is caused by the fundamental feature of quantum objects: any measurement causes unavoidable change of the object state. Also, any possible eavesdropping must always be active because the "no-cloning theorem" of quantum mechanics [4] prohibits copying of quantum bits.

References