Quantum key distribution (QKD) is one of the best-known examples of an application of quantum mechanics to cryptography. This article serves as a resource letter, a brief description to the introduction of QKD is provided before surveying the most prominent QKD protocols present in the literature from theoretical initialization by Wiesner to the attempts at practical implementations. We have also given an overview of the different security proofs proposed, for the variations in protocols and highlighted their significance.

References

- S.J. Wiesner; “Conjugate Coding”; SIGACT News 15:1; 1983. pp. 78-88
- Michael O. Rabin; “How To Exchange Secrets with Oblivious Transfer”; Harvard University Technical Report 81
- Bennett C.H.; “Quantum cryptography using any two nonorthogonal states”; Physical
Quantum Key Distribution: A Resource Letter

- Norbert Ltkenhau “Security against individual attacks for realistic quantum key distribution”; Physical Review A, Vol. 61, 052304(2000);
- Mayers, D.; “Self-Checking Quantum Apparatus and Violation of Classical Locality”; Manuscript
- Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Du, Norbert
- Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, Li Qian; “Experimental Quantum Key Distribution with Decoy States”; Physical Review Letters 96, 070502 (2006).
- Martin Hendrych; Experimental Quantum Cryptography; PhD. Thesis 2002
- Hiroki Takesue, Sae Woo Nam, Qiang Zhang, Robert H. Hadfield, Toshimori Honjo, Kiyoshi Tamaki, Yoshihisa Yamamoto; “Quantum key distribution over 40 dB channel loss using superconducting single photon detectors”; Nature Photonics 1, 343 (2007) (revised version)
- W.-Y. Hwang; “Quantum Key Distribution with High Loss: Toward Global Secure Communication”; Physical Review Letters 91, 057901 (2003);
- Zhen-Sheng Yuan, Yu-Ao Chen, Bo Zhao, Shuai Chen, Joerg Schmiedmayer, Jian-Wei
- Joern Mueller-Quade, Renato Renner; “Composability in quantum cryptography”; New Journal of Physics, 11, 085006, 2009 (Focus on Quantum Cryptography: Theory and Practice)
- Gilles Brassard, Norbert Ltkenhaus, Tal Mor, and Barry C. Sanders; “Limitations on Practical Quantum Cryptography”; Physical Review Letters, Volume 85, No. 6
- Llus Masanes, Stefano Pironio, Antonio Acn; “Secure device-independent quantum key distribution with causally independent measurement devices”; Nature Communications 2, Article number:238, 2011
- G Brassard; “Bibliography of Quantum Cryptography”;
- Douglas Stebila, Michele Mosca and Norbert Ltkenhaus; “The Case for Quantum Key Distribution”; arXiv:0902.2839v2

Index Terms

Computer Science  Security

Keywords

Quantum Key Distribution  BB84  Quantum Cryptography  Security  Implementation