Quantum Cryptography

Boxiang Fu (998092) [1]

[1]Faculty of Science, University of Melbourne

Introduction

Charles Bennett & Gilles Brassard's seminal 1984 paper solved the problem of establishing a channel for communication that is provably secure against adversarial eavesdropping [2]. The physical underpinning of the protocol is based on the collapse postulate, which states that the act of measurement on a quantum system irreversibly alters the system. As such, the sender and receiver would be alerted to the presence of an adversary eavesdropping the communication. This is of practical importance in giving rise to secure protocols for key distribution in the post-quantum cryptography era.

Key Distribution Problem

A fundamental problem in cryptography is to establish a secure channel for communication. This is done through a "cryptographic key", and is used to encrypt the sender's (Alice) message and decrypt on the receiver's (Bob) side. The encryption is done so that the message during transit cannot be intercepted by an eavesdropper (Eve) and obtain information on its contents [12].

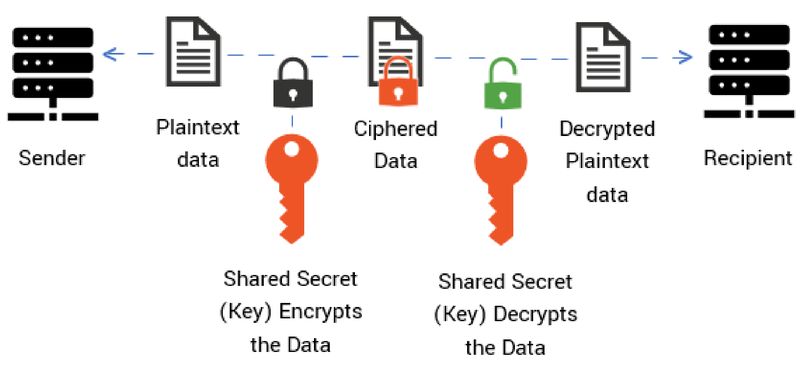

Figure 1. A symmetric private encryption scheme [1]

BB84 Quantum Key Distribution (QKD) Protocol

The first QKD protocol was developed by Charles Bennett & Gilles Brassard and published in their seminal 1984 paper (hence the name BB84) [2]. The steps of the protocol are as follows:

1. Alice chooses a random bit string and a corresponding random sequence of rectilinear (↕ and ↔) or diagonal (↗ and ↖) polarization bases
2. Alice sends Bob a sequence of photons, each representing one bit of the string and polarized in the chosen basis
3. Bob measures the received photons using either polarization basis
4. Alice and Bob announce via a public channel on their chosen basis, and discard any bits where their basis differs
5. Alice and Bob use a subset of their remaining bits to test for eavesdropping (more on this later). They they find none, discard the testing subset and use the remaining bits as their shared secret key.

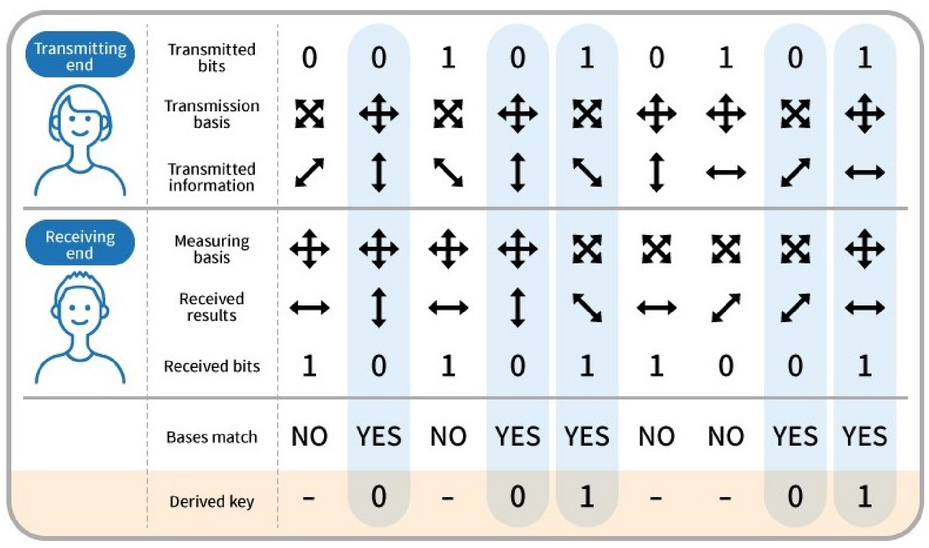

Figure 2. BB84 protocol scheme [7]

Physical Underpinning of the BB84 Protocol

The protocol is based fundamentally on the quantum nature of polarized photons. The state postulate dictates that the quantum system is represented by a ket $|\psi\rangle$ in Hilbert space. The Hilbert space is 2-dimensional, corresponding to the fact that the orientation of the polarization is on a 2-dimensional surface. Therefore, we can use $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ as an orthonormal basis of the Hilbert space. This is called its **rectilinear basis**. The choice of basis vectors is not unique. $|\nearrow\rangle$ and $|\nwarrow\rangle$ also represents an orthonormal basis of the Hilbert space. This is called its **diagonal basis**. An arbitrary ket representing a polarized photon is in general a superposition of the basis vectors. For the rectilinear basis, we have:

$$|\psi\rangle = \cos(\alpha)\,|\leftrightarrow\rangle + \sin(\alpha)\,|\updownarrow\rangle$$

where the photon is polarized at an angle α to the horizontal. This is in essence the projection of $|\psi\rangle$ onto the basis vectors $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ [3].

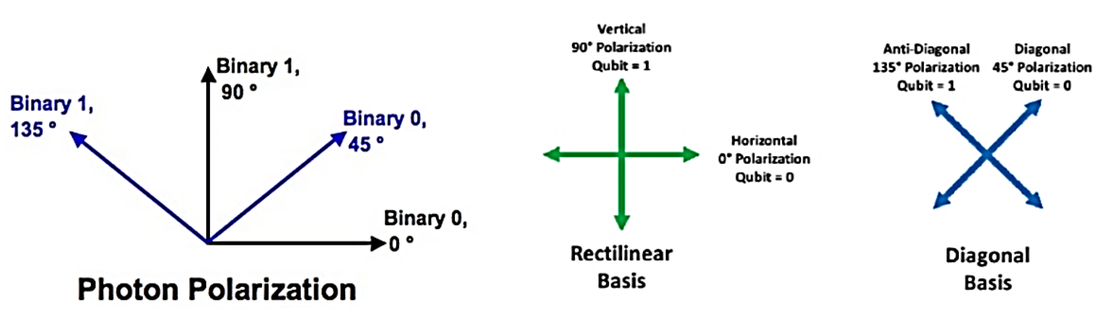

Figure 3. Rectilinear and diagonal basis of the photon polarization Hilbert space [4]

Once measurement occurs at Bob's end, the collapse postulate (in the Copenhagen interpretation) implies that the photon's polarization is measured as ↔ with probability $\cos^2\alpha$ and ↕ with probability $\sin^2\alpha$. Specifically, if $\alpha = 45°$ or $\alpha = 135°$ (i.e. the photon was prepared in the diagonal basis but measured in the rectilinear basis), then there is equal probability of measuring ↔ and ↕. The case of the photon being prepared in the rectilinear basis but measured in the diagonal basis is analogous. However, if the prepared and measurement basis are the same, Bob measures the polarization that is prepared by Alice with 100% probability (in the ideal case) [3].

If an eavesdropper (Eve) is intercepting the photon sequence, she will need to randomly choose a measurement basis to extract the polarization. She does not know what basis Alice used to encode the photon, so she guesses wrong 50% of the time. Her act of measurement collapses the wavefunction, and if Eve resends the photon consistent with her measurement, it would have randomized the polarization originally sent by Alice (this is known as the no-cloning theorem). This would mean that **1 out of 4 bits would be different** once Alice and Bob finish comparing their bases. So comparing 72 key bits would detect an eavesdropper with 99.9999999% probability [4].

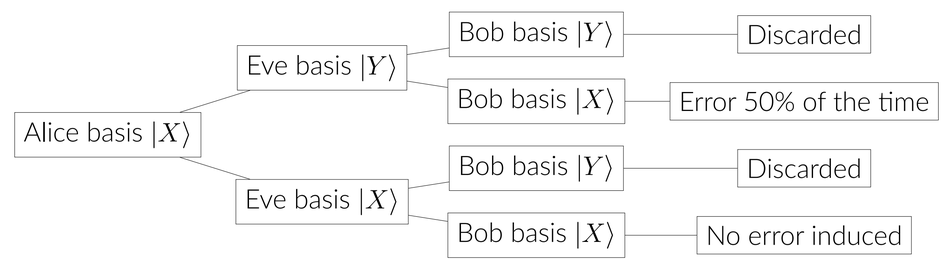

Figure 4. Error rate of BB84 protocol with eavesdropper

Significance of the Work & Future Developments

The BB84 protocol laid the seminal groundwork for quantum key distribution protocols that are provably secure barring fundamental violations of accepted physical laws [11]. This allows it to be a proof-of-concept for secure key distribution in the post-quantum cryptography era. In particular, the ubiquitous RSA public-key encryption algorithm used today is no longer post-quantum secure due to Shor's algorithm [10]. The BB84 protocol also accelerated government action taken to evaluate and standardize cryptosystems resistant to quantum attacks.

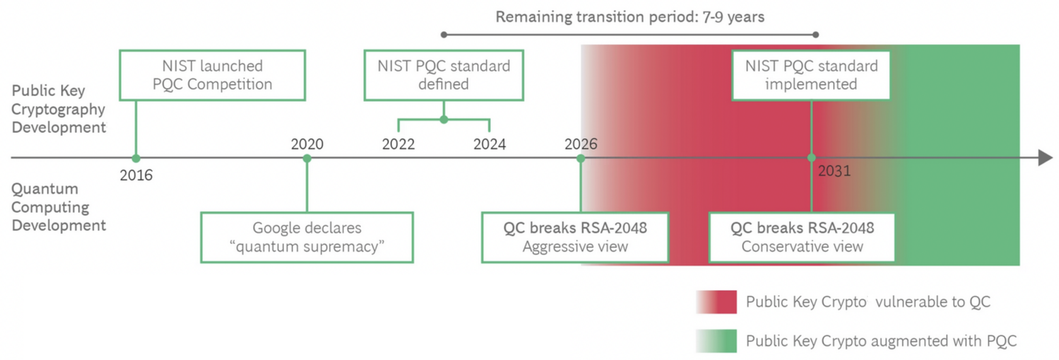

Figure 5. National Institute of Standards and Technology post-quantum cryptography adoption timeline [5]

Bennett & Brassard's 1984 paper presented the theoretical framework of the QKD protocol. To be of practical use, it evidently needs to be implemented experimentally. This was done by **Dixon, et al. in 2008 at a secure key rate of 1.02 Mbit/s over a distance of 20 km** and by **Liao, et al. in 2017 at a key rate of 1 kbit/s over a distance of 1,200 km** (from space!) [6, 9]. The advent of BB84 also spearheaded the direction of future research concerning secure quantum cryptosystems. A non-exhaustive list of more recent developments are tabulated below:

Protocol	Year	Inventors	Physical Principle
BB84	1984	Bennett & Brassard	Uncertainty principle
E91	1991	Ekert	Quantum entanglement
BBM92	1992	Bennett, Brassard & Mermin	Quantum entanglement
B92	1992	Bennett	Uncertainty principle
SSP	1999	Bechmann-Pasquinucci & Gisin	Uncertainty principle
DPS	2003	Inoue, Waks & Yamamoto	Quantum entanglement
SARG04	2004	Scarani, Acin, Ribordy & Gisin	Uncertainty principle

Table 1. Recent developments of QKD protocols [8]

References

[1] What is public key and private key cryptography, and how does it work?, 2023.
Available online: `https://cheapsslsecurity.com/p/what-is-public-key-and-private-key-cryptography-and-how-does-it-work/` (accessed on 7 May 2023).

[2] Charles H. Bennett and Gilles Brassard.
Quantum cryptography: Public key distribution and coin tossing.
Theoretical Computer Science, 560:7–11, 2014.
Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[3] Charles H. Bennett, Gilles Brassard, and Artur K. Ekert.
Quantum cryptography.
Scientific American, 267(4):50–57, 1992.

[4] Larissa V. Cherckesova, Olga A. Safaryan, Alexey N. Beskopylny, and Elena Revyakina.
Development of quantum protocol modification csloe-2022, increasing the cryptographic strength of classical quantum protocol bb84.
Electronics, 11(23), 2022.

[5] Lucian Comandar, Jean-François Bobier, Michael Coden, and Stefan Deutscher.
Ensuring online security in a quantum future.
Available online: `https://www.bcg.com/publications/2021/quantum-computing-encryption-security` (accessed on 7 May 2023).

[6] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields.
Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate.
Opt. Express, 16(23):18790–18797, Nov 2008.

[7] Shinya Murai.
Running feature: Quantum key distribution, protecting the future of digital society.
Available online: `https://www.global.toshiba/ww/company/digitalsolution/articles/tsoul/38/004.html` (accessed on 7 May 2023).

[8] Ali Ibnun Nurhadi and Nana Rachmana Syambas.
Quantum key distribution (qkd) protocols: A survey.
In *2018 4th International Conference on Wireless and Telematics (ICWT)*, pages 1–5, 2018.

[9] Liao Shengkai, Wen-Qi Cai, Weiyue Liu, Liang Zhang, Yang Li, Jianyu Wang, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xiawei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Feng-Jian Wang, Yong-Mei Huang, Qiang Wang, and Jian-Wei Pan.
Satellite-to-ground quantum key distribution.
Nature, 549, 07 2017.

[10] Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5):1484–1509, oct 1997.

[11] Peter W. Shor and John Preskill.
Simple proof of security of the bb84 quantum key distribution protocol.
Phys. Rev. Lett., 85:441–444, Jul 2000.

[12] Chia-Wei Tsai, Chun-Wei Yang, Jason Lin, Yao-Chung Chang, and Ruay-Shiung Chang.
Quantum key distribution networks: Challenges and future research issues in security.
Applied Sciences, 11(9), 2021.