Scientific Research Publishing

Journal of Quantum Information Science, 2022, 12, 91-98
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

On Security of Quantum Cryptography by Probabilistic Analysis

Jianzhong Zhao

Geophysics Department, Yunnan University, Kunming, China
Email: jzhzhao@ynu.edu.cn

How to cite this paper: Zhao, J.Z. (2022) On Security of Quantum Cryptography by Probabilistic Analysis. *Journal of Quantum Information Science*, **12**, 91-98.
https://doi.org/10.4236/jqis.2022.124008

Received: November 3, 2022
Accepted: November 28, 2022
Published: December 1, 2022

Abstract

The existing quantum cryptography is a classical cryptography in nature and basically insecure because of its classical (conventional) bits, classical encryption algorithm and classical (public) channel. A novel topic about successful communication between the legitimate users, Alice and Bob, is discussed with probability of solution uniqueness of Bob's decryption equation. We find, by probabilistic analysis, that success of communication between Alice and Bob is probabilistic with a probability bigger than 1/2. It is also novel to define insecurity of the quantum cryptography by probability of solution uniqueness of the search equation of Eve, the eavesdropper. The probability of Eve's success to find the plain-text of Alice (and Bob) is greater than 1/2, and so the quantum cryptography is seriously insecure.

Keywords

Quantum Cryptography, Classical Cryptography, Fundamental Equations, Unique Solution, Probability, Insecure

1. Introduction

Bennett and Brassard, Ekert and Bennett established the quantum cryptography by publishing the theoretical quantum key distribution (QKD) protocols, BB84, E91 and B92 [1] [2] [3].

Some authors (E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury; P. W. Shor and J. Preskill; D. Mayers; D. Gottesman and H.-K. Lo; H.-K. Lo, H. F. Chau and M. Ardehali; R. Renner, N. Gisin and B. Kraus; M. Boyer, R. Liss and T. Mor; H.-Y. Su) proved security of BB84 [4]-[13], others (Q. Zhang and C.-J. Tang; K. Tamaki, M. Koashi and N. Imoto; K. Tamaki and N. Lütkenhaus; K.Tamaki, N. Lütkenhaus, M. Koashi and J. Batuwantudawe; M. Lucamarini, G. D. Giuseppe and K. Tamaki) proved security of B92 [14]-[19], in differ-

ent theoretical frameworks by defining security of QKD protocols differently.

However, J.Z. Zhao argued that the previous proofs were neither unique nor exhaustive, which meant that proof of security of the theoretical QKD protocols was not completed or achieved [20]. The research proved, by quantum mechanics, that the theoretical QKD protocols were insecure in an updated theoretical framework with an updated definition of security of QKD protocols [20].

This research shows, by probabilistic analysis, that the existing quantum cryptography is a classical cryptography in nature. Success of communication between the legitimate users, Alice and Bob, is probabilistic. The probability of success of searching for the plain-text by the eavesdropper, Eve, is bigger than 1/2, and so the quantum cryptography is seriously insecure.

2. Quantum Cryptography Is a Classical Cryptography in Nature

Quantum cryptography based on the theoretical QKD protocols, BB84, E91 and B92, is a classical cryptography in nature because: [1] [2] [3]

1) The key, the plain-text and the cipher-text are classical ones because they are constructed by classical (conventional) bits;

2) The encryption algorithm is classical OTP (One-time Pad) encryption algorithm;

3) Alice sends the encryption algorithm and the cypher-text to Bob through the classical (public) channel.

The analysis below is valid for BB84, E91 and B92 protocols.

3. The Fundamental Equations of the Theoretical QKD Protocols

3.1. Alice's Encryption Equation

At the end of any theoretical QKD protocol, Alice encrypts her plain-text following the encryption equation

$$\mathrm{OTP}\left(k_s, p_t\right) = C \tag{1}$$

where OTP is the OTP (one-time pad) encryption algorithm [21], k_s is the key, p_t is the plain-text, C is the cipher-text. Each of the key, the plain-text and the cypher-text is of n bits long because of the OTP encryption algorithm [21]. Then she sends the cipher-text and the encryption algorithm (for Bob's decryption) to Bob during the communication between them.

3.2. Quantum State of the Plain-Text and Bob's Decryption Equation

Bob receives the cypher-text and the OTP encryption algorithm [21] sent by Alice to him. He knows that the length of the plain-text is n, equivalent to the length of the key, because of the OTP encryption algorithm [21]. Then, Bob establishes the quantum state of the plain-text, superposition of $N\,(N = 2^n)$ states of $\left|p_j\right\rangle$ (of n bits),

$$\begin{aligned}|P\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\cdots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\\ &= \frac{1}{\sqrt{2^n}}\left(|00\cdots0\rangle+|00\cdots1\rangle+\cdots+|11\cdots1\rangle\right)\\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|p_j\rangle\end{aligned} \tag{2}$$

for any theoretical QKD protocol, BB84, E91 and B92.

After that, Bob establishes his decryption equation

$$\mathrm{OTP}\left(k_s, p_j\right) = C \quad (0 \le j \le N-1), \tag{3}$$

where OTP is the OTP encryption algorithm [21], k_s is the key, p_j is the bit string of $|p_j\rangle$, C is the cipher-text.

Bob's decryption is to solve the decryption equation, Equation (3), to find the plain-text p_t.

3.3. Quantum State of the Key and Eve's Search Equation

Eve intercepts the cipher-text and the encryption algorithm sent by Alice to Bob. She obtains the knowledge of the length of the key and the length of the plain-text, n, which is equivalent to the length of the cipher-text intercepted. Then Eve establishes the quantum state of the key, $|K\rangle$, superposition of $N\,(N=2^n)$ states of $|k_i\rangle$ (of n bits):

$$\begin{aligned}|K\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\cdots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\\ &= \frac{1}{\sqrt{2^n}}\left(|00\cdots0\rangle+|00\cdots1\rangle+\cdots+|11\cdots1\rangle\right)\\ &= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|k_i\rangle\end{aligned} \tag{4}$$

where n is the number of the bits of the key of any one of BB84, E91 and B92.

Eve also establishes the quantum state of the plain-text (2).

After that, Eve establishes her search equation

$$\mathrm{OTP}\left(k_i, p_j\right) = C \quad (0 \le i \le N-1, 0 \le j \le N-1) \tag{5}$$

where OTP is the OTP encryption algorithm [21], k_i is the bit string of $|k_i\rangle$, p_j is the bit string of $|p_j\rangle$, C is the cipher-text.

Eve's searching is to solve the search equation to find the plain-text p_t.

3.4. Summary of Variables

k_i: the bit string of the i-th component of the quantum state of the key;
p_j: the bit string of the j-th component of the quantum state of the plain-text;
k_s: the bit string of the key, whose value is set by Alice;
p_t: the bit string of the plain-text, whose value is set by Alice;
C: the bit string of the cypher-text produced by Alice's encryption;
q_1: the probability of solution uniqueness of Bob's decryption equation;
q_2: the probability of solution uniqueness of Eve's search equation.

4. Probability of Successful Communication between Alice and Bob

There is no doubt that there exists at least one solution of Equation (3) because of Alice's encrypting (Equation (1)). Furthermore, Equation (3) is probable to provide a unique solution for successful communication between Alice and Bob, though the maximum of solution multiplicity of Equation (3) may reach the big number N.

Suppose that the probability of uniqueness of solution of Equation (3) is $q_1\left(q_1<1\right)$, then the probability of double solution of the equation is $q_1^2\ldots$ The total probability of all possible solutions of the equation should be 1. Then we have

$$1=q_1+q_1^2+q_1^3+\cdots+q_1^N=\frac{q_1\left(1-q_1^N\right)}{1-q_1}<\frac{q_1}{1-q_1}. \tag{6}$$

It is from Equation (6) that

$$1-q_1<q_1, \tag{7}$$

then

$$q_1>\frac{1}{2}. \tag{8}$$

From Equation (8) we know that the probability of uniqueness of solution of Equation (3) is bigger than 1/2, that is, the probability of successful communication between Alice and Bob is bigger than 1/2. Solving Equation (3) is to search $\left|P\right\rangle$ (expressed by Equation (2)) for the $\left|p_j\right\rangle$ whose bit string, p_j, satisfies Equation (3). Bob can use Grover's fast quantum mechanical algorithm for database search for his searching to find p_t [20]. Bob succeeds with the probability bigger than 1/2.

5. Probability of Successful Searching by Eve

There is no doubt that there exists at least one solution of Equation (5) because of Alice's encrypting (Equation (1)). Furthermore, Equation (5) is probable to give a unique solution for Eve's successful search, though the maximum of solution multiplicity of Equation (5) may reach a big number N^2.

Suppose that the probability of uniqueness of solution of Equation (5) is $q_2\left(q_2<1\right)$, then the probability of double solution of the equation is $q_2^2\ldots$ The total probability of all possible solutions of the equation should be 1. Then we have

$$1=q_2+q_2^2+q_2^3+\cdots+q_2^{N^2}=\frac{q_2\left(1-q_2^{N^2}\right)}{1-q_2}<\frac{q_2}{1-q_2}. \tag{9}$$

It is from Equation (9) that

$$1-q_2<q_2, \tag{10}$$

then

$$q_2 > \frac{1}{2}. \tag{11}$$

From Equation (11) we know that the probability of uniqueness of solution of Equation (5) is bigger than 1/2, that is, the probability of Eve's successful searching for the plain-text is bigger than 1/2.

6. Eve's Searching by Grover's Fast Quantum Mechanical Algorithm for Database Search

Eve searches the quantum state of the plain-text (Equation (2)) for the plain-text by Grover's fast quantum mechanical algorithm for database search. She succeeds as solution of the search equation, Equation (5), is unique:

1) Defining a function $h\left(k_i, p_j\right)$ (using the search equation, Equation (5)):

$$h\left(k_i, p_j\right) = \begin{cases} 1, & \mathrm{OTP}\left(k_i, p_j\right) = C \\ 0, & \mathrm{OTP}\left(k_i, p_j\right) \neq C \end{cases} \tag{12}$$

2) Repeating the following operations (a) and (b) for $O\left(\sqrt{N}\right)$ times (Grover Iteration) [22] [23]:

(a) Applying the oracle operation [22] [23]:

$$\left|p_j\right\rangle \xrightarrow{O} (-1)^{h\left(k_i, p_j\right)} \left|p_j\right\rangle, \tag{13}$$

where $h\left(k_i, p_j\right)$ is the function defined by Equation (12).

(b) Performing Grover operation (in terms of inversion about average operation)

$$D\left|P\right\rangle, \tag{14}$$

where the diffusion transform D can be implemented as

$$D = WRW, \tag{15}$$

where W is the Walsh-Hadamard Transform Matrix and R is the phase rotation matrix [22] [23].

3) Measuring the resulting state of $\left|P\right\rangle$ gives $\left|p_t\right\rangle$, the plan-text, with a probability of $O(1)$ [22] [23].

7. Discussions

1) Success of communication between Alice and Bob is taken for granted so far in the theory of the theoretical QKD protocols, with a default probability 1. However, the research in this paper shows that success of communication between Alice and Bob is probabilistic with a probability $q_1\left(\frac{1}{2} < q_1 < 1\right)$.

2) Eve's interception and quantum computation are free of detection of Alice and Bob because the quantum transmission between them is not disturbed. Eve's probability of successful searching for the plain-text is big ($\frac{1}{2} < q_2 < 1$), and so the existing quantum cryptography based on the theoretical QKD protocols is

seriously insecure.

3) The strategy of the existing quantum cryptography should be adjusted. P. Ndagijimana, F. Nahayo, M.K. Assogba, A.F.-X. Ametepe, and J. Shabani proposed a random number generation model using the thermal noise theory, intending to exploit the laws of quantum physics associated to basic principle of cryptology for the implementation of new cryptographic primitives, towards post-quantum cryptography [24].

8. Conclusion

The existing quantum cryptography based on the theoretical QKD protocols is a classical cryptography in nature. Successful communication between the legitimate users, Alice and Bob, is taken for granted so far in the theory of QKD, but proved probabilistic in this research. The probability of Eve's successful searching for the plain-text is big, and so the quantum cryptography based on the theoretical QKD protocols is seriously insecure. Insecurity of the quantum cryptography is a logical result. Adjustment of the strategy of the existing quantum cryptography is necessary.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 9-12 December 1984, 175-179.

[2] Ekert, A.K. (1991) Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, **67**, 661-663. https://doi.org/10.1103/PhysRevLett.67.661

[3] Bennett, C.H. (1992) Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, **68**, 3121-3124. https://doi.org/10.1103/PhysRevLett.68.3121

[4] Biham, E., Boyer, M., Boykin, P.O., Mor, T. and Roychowdhury, V. (2000) A Proof of the Security of Quantum Key Distribution. In: *Proceedings of the* 32*nd Annual ACM Symposium on Theory of Computing*, ACM Press, New York, 715-724. https://doi.org/10.1145/335305.335406

[5] Shor, P.W. and Preskill, J. (2000) Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, **85**, 441-444. https://doi.org/10.1103/PhysRevLett.85.441

[6] Mayers, D. (2001) Unconditional Security in Quantum Cryptography. *Journal of the ACM*, **48**, 351-406. https://doi.org/10.1145/382780.382781

[7] Mayers, D. (2002) Shor and Preskill's and Mayers's Security Proof for the BB84 Quantum Key Distribution Protocol. *The European Physical Journal D*, **18**, 161-170. https://doi.org/10.1140/epjd/e20020020

[8] Gottesman, D. and Lo, H.-K. (2003) Proof of Security of Quantum Key Distribution with Two-Way Classical Communications. *IEEE Transactions on Information Theory*, **49**, 457-475. https://doi.org/10.1109/TIT.2002.807289

[9] Lo, H.-K., Chau, H.F. and Ardehali, M. (2005) Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *Journal of Cryptology*, **18**, 133-165. https://doi.org/10.1007/s00145-004-0142-y

[10] Renner, R., Gisin, N. and Kraus, B. (2005) Information-Theoretic Security Proof for Quantum-Key-Distribution Protocols. *Physical Review A*, **72**, Article ID: 012332. https://doi.org/10.1103/PhysRevA.72.012332

[11] Boyer, M., Liss, R. and Mor, T. (2020) Composable Security against Collective Attacks of a Modified BB84 QKD Protocol with Information Only in One Basis. *Theoretical Computer Science*, **801**, 96-109. https://doi.org/10.1016/j.tcs.2019.08.014

[12] Su, H.-Y. (2020) Simple Analysis of Security of the BB84 Quantum Key Distribution Protocol. *Quantum Information Processing*, **19**, Article No. 169. https://doi.org/10.1007/s11128-020-02663-z

[13] Tsurumaru, T. (2020) Leftover Hashing from Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution. *IEEE Transactions on Information Theory*, **66**, 3465-3484. https://doi.org/10.1109/TIT.2020.2969656

[14] Zhang, Q. and Tang, C.-J. (2002) Simple Proof of the Unconditional Security of the Bennett 1992 Quantum Key Distribution Protocol. *Physical Review A*, **65**, Article ID: 062301. https://doi.org/10.1103/PhysRevA.65.062301

[15] Tamaki, K., Koashi, M. and Imoto, N. (2003) Unconditionally Secure Key Distribution Based on Two Non-Orthogonal States. *Physical Review Letters*, **90**, Article ID: 167904. https://doi.org/10.1103/PhysRevLett.90.167904

[16] Tamaki, K. and Lütkenhaus, N. (2004) Unconditional Security of the Bennett 1992 Quantum Key Distribution Protocol over Lossy and Noisy Channel. *Physical Review A*, **69**, Article ID: 032316. https://doi.org/10.1103/PhysRevA.69.032316

[17] Tamaki, K., Lütkenhaus, N., Koashi, M. and Batuwantudawe, J. (2009) Unconditional Security of the Bennett 1992 Quantum-Key-Distribution Scheme with a Strong Reference Pulse. *Physical Review*, **80**, 32302-32310. https://doi.org/10.1103/PhysRevA.80.032302

[18] Lucamarini, M., Giuseppe, G. and Tamaki, K. (2009) Robust Unconditionally Secure Quantum Key Distribution with Two Non-Orthogonal and Uninformative States. *Physical Review A*, **80**, Article ID: 032327. https://doi.org/10.1103/PhysRevA.80.032327

[19] Ali, N., Radzi, N.A.N., Aljunid, S.A. and Endut, R. (2020) Security of B92 Protocol with Uninformative States in Asymptotic Limit with Composable Security. *AIP Conference Proceedings*, **2203**, Article ID: 020049. https://doi.org/10.1063/1.5142141

[20] Zhao, J.Z. (2022) A Quantum Mechanical Proof of Insecurity of the Theoretical QKD Protocols. *Journal of Quantum Information Science*, **12**, 53-63. https://doi.org/10.4236/jqis.2022.123006

[21] Shannon, C.E. (1949) Communication Theory of Secrecy Systems. *Bell System Technical Journal*, **28**, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[22] Grover, L.K. (1996) A Fast Quantum Mechanical Algorithm for Database Search. In: *Proceedings 28th ACM Symposium on the Theory of Computation*, ACM Press, New York, 212-219. https://doi.org/10.1145/237814.237866

[23] Grover, L.K. (1997) Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Physical Review Letters*, **79**, 325-328.

https://doi.org/10.1103/PhysRevLett.79.325

[24] Ndagijimana, P., Nahayo, F., Assogba, M.K., Ametepe, A.F.-X. and Shabani, J. (2020) Towards Post-Quantum Cryptography Using Thermal Noise Theory and True Random Numbers Generation. *Journal of Information Security*, **11**, 149-160. https://doi.org/10.4236/jis.2020.113010