Scientific Research Publishing

Journal of Quantum Information Science, 2022, 12, 53-63
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

A Quantum Mechanical Proof of Insecurity of the Theoretical QKD Protocols

Jianzhong Zhao

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

How to cite this paper: 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

Received: June 30, 2022
Accepted: August 27, 2022
Published: August 30, 2022

Abstract

Cryptography is crucial to communication security. In 1984, a well-known QKD (quantum key distribution) protocol, BB84, was published by Bennett and Brassard. The BB84 Protocol was followed by the QKD protocols published by Ekert (1991) (E91) and Bennett (1992) (B92). Some authors proved security of the theoretical QKD protocols in different theoretical frameworks by defining security of QKD protocols differently. My argument is that the previous proofs of security are neither unique nor exhaustive for each theoretical QKD protocol, which means that proof of security of the theoretical QKD protocols has not been completed or achieved. The non-uniqueness and the non-exhaustiveness of the proofs will lead to more proofs. However, a coming "proof" of security of the theoretical QKD protocols is possible to be a disproof. The research by quantum mechanics in this paper disproves security of the theoretical QKD protocols, by establishing the theoretical framework of quantum mechanical proof, defining security of QKD protocols, establishing the quantum state of the final key of the theoretical protocols from their information leakages, and applying Grover's fast quantum mechanical algorithm for database search to the quantum state of the final key to result in the Insecurity Theorem. This result is opposite to those of the previous proofs where the theoretical QKD protocols were secure. It is impossible for Alice and Bob to protect their communications from information leakage by stopping or canceling the protocols. The theoretical QKD keys are conventional and basically insecure. Disproof of security of the theoretical QKD protocols is logical.

Keywords

Quantum Mechanics, Quantum Cryptography, Quantum Computation, Security, Proof

1. Introduction

Cryptography is crucial to communication security. In 1984, a well-known QKD

(quantum key distribution) protocol, BB84, was published by Bennett and Brassard [1]. The BB84 Protocol was followed by the QKD protocols published by Ekert in 1991 (E91) and Bennett in 1992 (B92) [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 different theoretical frameworks by defining security of QKD protocols differently.

My argument is that the authors understand security of QKD with different perspectives, and the previous proofs of security are neither unique nor exhaustive for each theoretical QKD protocol, which means that proof of security of the theoretical QKD protocols has not been completed or achieved. On the other hand, it is possible, from the non-uniqueness and non-exhaustiveness of proofs of security of QKD, that the theoretical QKD protocols will be proved insecure in an updated theoretical framework with an updated definition of security. For insecurity, one proof is enough.

Quantum mechanics is applied to variant research fields. For example, Stanisław Olszewski examines the time intervals characteristic for the quantum emission process, partly on the basis of the Ehrenfest treatment of the adiabatic invariants and partly with the aid of a study of the mechanical properties of electrons entering the simple quantum systems [20]. Shiro Ishikawa proposes the understanding of Wittgenstein's picture theory in the framework of quantum language (or, "measurement theory", "the linguistic Copenhagen interpretation of quantum mechanics", "the quantum mechanical worldview") [21].

Quantum computation holds much promise to break cryptosystems. In 1994, Shor published an algorithm for quantum computation of factoring [22], which can be used for breaking keys of conventional RSA public-key cryptosystems efficiently [22] [23] [24] [25]. In 1996, Grover published a fast quantum mechanical algorithm for database search [26], which can be used for efficient breaking of keys of conventional encryption systems such as Data Encryption Standard (DES) cipher [24]-[30]. The success of quantum computation forces us to ask: Are quantum key distribution protocols secure, encountering powerful quantum computation?

In this research Grover's fast quantum mechanical algorithm for database search is applied to disprove security of the theoretical quantum key distribution protocols [26] [27]. The security of QKD protocols is defined in the theoretical framework of quantum mechanical proof established in this paper. The quantum state of the final key of the theoretical QKD protocols, which is based on the information leakages to Eve, the adversary, is established. Grover's fast quantum mechanical algorithm for database search is applied to the quantum state of the final key to result in the Insecurity Theorem [26] [27].

From the previous proofs the theoretical QKD protocols, free of quantum computation attack, are secure, while my research concludes, from quantum mechanics, that the theoretical QKD protocols are insecure.

BB84, E91 and B92 are the theoretical and fundamental QKD protocols. Their insecurity implies that all QKD protocols developed following their model are insecure, and the strategy or direction of the quantum cryptography based on QKD should be adjusted.

Discussions are given.

2. The Theoretical Framework of Quantum Mechanical Proof

The theoretical framework of quantum mechanical proof in this paper consists of the theoretical QKD protocols, Grover's fast quantum mechanical algorithm for database search and the rules of mathematical inference in quantum mechanics.

The variables in the framework are listed as:

k_i: the bit string of the *i-th* component of the quantum state of the final 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.

3. The Definition of Security of QKD Protocols

A QKD (quantum key distribution) protocol is secure if and only if its final key cannot be deduced from the information leakage of the protocol.

4. Insecurity Theorem of the Theoretical QKD Protocols

The theoretical QKD protocols, BB84, E91 and B92, are insecure in the theoretical framework of quantum mechanical proof in this paper.

5. Proof of Insecurity Theorem of the Theoretical QKD Protocols

5.1. Leakage of the Key-Length of BB84

After the "public discussion" of BB84 Protocol, the "remaining shared secret bits", announced or leaked over the public channel, are used as the final key [1]. Thus, Eve, the adversary, overhears the "public exchange of messages" between Alice and Bob, and counts the "remaining shared secret bits" for n, the number of the bits of the final key.

5.2. Leakage of the Key-Length of E91

Eve, the adversary, overhears the legitimate users' public announcements, neither disturbing the quantum channel nor violating the requirement of quantum mechanics, to know n, the number of the bits of the final key, by counting the

measurements or the orientations of the analyzers within the second group, which Alice and Bob used the same orientation of their analyzers for and publicly announced or leaked [2].

5.3. Leakage of the Key-Length of B92

1) Detecting the key-length of EPR and non-EPR key distribution system by Eve:

For "EPR and non-EPR key distribution" system [3], Eve repeats for k times to eavesdrop on Alice and Bob's public test in Step 9 and Step 10 of the system [3], and detects the key-length by counting the bits of the final secret key after the k repeated tests, without disturbing the quantum channel.

2) A scheme of "interferometric quantum key distribution using two non-orthogonal low-intensity coherent states" is proposed [3]. According to the scheme, "Alice would randomly send red and green flashes of < 1 photon intensity, and Bob would publicly report which flashes he saw, but not their colors, which would constitute the secret key." [3]

My argument is that it is unnecessary for Eve to "see" the same subset of flashes. She can seize the knowledge of the key-length by eavesdropping on Bob's public report and counting the subset flashes seen by Bob.

5.4. Quantum State of the Final Key

The leakage of the lengths of the final keys of BB84, E91 and B92 discussed in Sections 5.1 - 5.3 results in the establishment, in terms of quantum mechanics, of $|K\rangle$, superposition of $N(N=2^n)$ states of $|k_i\rangle$ (of n bits), as the quantum state of the final key.

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

where n is the number of the bits of the final key of any one of BB84, E91 and B92. Equation (1) and the analysis below in Section 5 are valid for any one of BB84, E91 and B92 protocols.

5.5. OTP Encryption Algorithm

Bennett and Brassard declare that "If the transmission has not been disturbed, they agree to use these shared secret bits in the well-known way as a one-time pad to conceal the meaning of subsequent meaningful communications, or for other cryptographic applications (e.g. authentication tags) requiring shared secret random information." [1]. This declaration defines and publishes the encryption algorithm of QKD protocols: one-time pad encryption algorithm (OTP) [31].

5.6. Quantum State of the Plain-Text

The length (the number of the bits) of the plain-text is n, equal to the length of the key, because the encryption algorithm of QKD is OTP encryption algorithm [31]. Therefore, the quantum state of the plain-text is

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

5.7. Encryption

After the protocol is implemented, Alice encrypts her plain-text by the operation

$$\mathrm{E}\left(k_s, p_t\right) = C \quad \left(0 \le s \le N-1, 0 \le t \le N-1\right) \tag{3}$$

where E is the OTP (one-time pad) encryption algorithm, k_s is the bit string of $|k_s\rangle$, the key, p_t is the bit string of $|p_t\rangle$, the plain-text, C is the cipher-text. Then she sends the cipher-text and the encryption algorithm (for Bob's decryption) to Bob during the communication between them.

5.8. Decryption

Bob receives the cypher-text and the encryption algorithm sent by Alice to him, and establishes his decryption equation

$$\mathrm{E}\left(k_s, p_j\right) = C \quad \left(0 \le s \le N-1, 0 \le j \le N-1\right), \tag{4}$$

where E is the OTP (one-time pad) encryption algorithm, k_s is the bit string of $|k_s\rangle$, 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 (4), to find the plain-text $|p_t\rangle$.

It is obvious that there exists at least one solution of Equation (4) because of Alice's encrypting (Equation (3)). It is obvious that solution of Equation (4) is required to be unique for successful communication between Alice and Bob.

Solving Equation (4) is to search $|P\rangle$ (expressed by Equation (2)) for the $|p_j\rangle$ whose bit string, p_j, satisfies Equation (4). Bob prefers using Grover's fast quantum mechanical algorithm for database search because Grover's quantum searching algorithm is optimal [32]. Bob's decryption, which needs $O\left(\sqrt{N}\right)$ Grover's iterations, is presented in **Appendix 1** of this paper.

5.9. Key-Equation

Eve intercepts the cipher-text and the encryption algorithm sent by Alice to Bob.

For Eve, if $|k_i\rangle$ is the key and $|p_j\rangle$ is the plain-text, they satisfy

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

where E is the OTP encryption algorithm, 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. Equation (5) is the key-equation.

5.10. Uniqueness of Solution

It is obvious that there exists at least one couple of k_i and p_j that satisfies Equation (5) because of Alice's encrypting (Equation (3)). Furthermore, multiplicity of solution of Equation (5), if any, can result in multiplicity of solution of Equation (4) because of $|k_s\rangle \in \{|k_i\rangle | (0 \le i \le N-1)\}$. Then logically, uniqueness of solution of Equation (4) can result in uniqueness of solution of Equation (5). And so, if communication between Alice and Bob is successful, solution of the key-equation Equation (5) can be unique.

5.11. Searching by Grover's Fast Quantum Mechanical Algorithm

Eve searches the quantum state of the secrete key (Equation (1)) for the key by Grover's fast quantum mechanical algorithm for database search. She succeeds as the communication between Alice and Bob is successful and solution of the key-equation is unique:

1) Defining a function $f(k_i, p_j)$ (using the key-equation Equation (5)):

$$f(k_i, p_j) = \begin{cases} 1, & \mathrm{E}(k_i, p_j) = C \\ 0, & \mathrm{E}(k_i, p_j) \neq C \end{cases} \tag{6}$$

2) Repeating the following operations (a) and (b) for $O(\sqrt{N})$ times (Grover Iteration) [26] [27]:

a) Applying the oracle operation [26] [27]:

$$|k_i\rangle \xrightarrow{O} (-1)^{f(k_i, p_j)} |k_i\rangle, \tag{7}$$

where $f(k_i, p_j)$ is the function defined by Equation (6).

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

$$D|K\rangle, \tag{8}$$

where the diffusion transform D can be implemented as

$$D = WRW, \tag{9}$$

where W is the Walsh-Hadamard Transform Matrix and R is the phase rotation matrix [26] [27].

3) Measuring the resulting state of $|K\rangle$ results in $|k_s\rangle$, the secrete key, with a probability of $O(1)$ [26] [27].

5.12. Proved Insecurity Theorem of the Theoretical QKD Protocols

From the inference of Section 5, the result of Section 5.11 and the definition of security of QKD protocols suggested in Section 3, the Insecurity Theorem of the theoretical QKD protocols suggested in Section 4 is proved.

6. Discussions

1) An alternative approach to establishing of the quantum state of the final key, Equation (1), and the quantum state of the plain-text, Equation (2), is open to Eve. Eve intercepts the cypher-text sent by Alice to Bob and counts its bits for n, then establishes Equation (1), where n is the key-length, and Equation (2), where n is the number of the bits of the plain-text, because the encryption algorithm of QKD is one-time pad (OTP) encryption algorithm [1] [31] and the three bit numbers (of the key, the plain-text and the cypher-text) are identical (n). This is a shortcut approach.

2) Bob's $O\left(\sqrt{N}\right)$ Grover's iterations are completed within a period of time decided by him, no matter how big $N\left(N<\infty\right)$ is, if and only if computing speed of quantum computation is unlimited.

Eve's $O\left(\sqrt{N}\right)$ Grover's iterations (of Equation (7) and Equation (8)) are completed within a period of time decided by her, no matter how big $N\left(N<\infty\right)$ is, if and only if computing speed of quantum computation is unlimited.

Quantum computers perform any operations allowed by quantum mechanics. Quantum computation is, in principle, of unlimited computational power (unlimited computing speed), because no limit of computing speed is possible to be defined or proved by the fundamental principles of quantum mechanics (superposition, uncertainty and entanglement) that quantum computation is based on.

Thus, the unlimited computing speed of quantum computation guarantees that both the communication between Alice and Bob and Eve's searching for the key are successful.

3) It is obvious that it is impossible for Alice and Bob to detect Eve's activities because the quantum transmission between them is not disturbed by Eve's operations of eavesdropping and quantum computation. Thus, it is impossible for Alice and Bob to protect their communications from information leakage by stopping or canceling the protocols.

4) The theoretical QKD keys are conventional ones because they are constructed by conventional bits. Therefore, the essential difficulty of the theoretical QKD protocols is that the theoretical QKD keys are basically insecure. Disproof of security of the theoretical QKD protocols is logical.

7. Conclusion

This research, based on quantum mechanics and quantum computation, proves that the theoretical QKD protocols, BB84, E91 and B92, are insecure in the theoretical framework of quantum mechanical proof in this paper. This result is opposite to those of the previous proofs where BB84 and B92 QKD protocols were secure. The information leakage of the theoretical QKD protocols is unavoidable because the quantum transmission of the protocols is not disturbed by Eve's operations. The keys of the theoretical QKD protocols are conventional ones of conventional bits and basically insecure. The Insecurity Theorem of the theoretical QKD protocols proved in this paper is a logical result. The insecurity

of the theoretical and fundamental QKD protocols implies that all QKD protocols developed following their model (featured by a quantum channel, a conventional channel, a conventional key and OTP encryption) are insecure, and the strategy or direction of the quantum cryptography based on QKD should be adjusted, that will stimulate more topics to be studied in the quantum information field.

Acknowledgements

I thank Jin Zhao for her suggestions for this manuscript.

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, 10-12 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. *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, Portland, 21-23 May 2000, 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: 12332. 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**, 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 Nonorthogonal 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 A*, **80**, Article ID: 032302. 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 Nonorthogonal 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] Olszewski, S. (2020) Ehrenfest Approach to the Adiabatic Invariants and Calculation of the Intervals of Time Entering the Energy Emission Process in Simple Quantum Systems. *Journal of Quantum Information Science*, **10**, 1-9. https://doi.org/10.4236/jqis.2020.101001

[21] Ishikawa, S. (2020) Wittgenstein's Picture Theory in the Quantum Mechanical Worldview. *Journal of Quantum Information Science*, **10**, 104-125. https://doi.org/10.4236/jqis.2020.104007

[22] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: *Proc. 35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, 124-134. https://doi.org/10.1109/SFCS.1994.365700

[23] Rivest, R.L., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Sig Natures and Public-Key Cryptosystems. *Communications of the ACM*, **21**, 120-126. https://doi.org/10.1145/359340.359342

[24] Nielsen, M.A. and Chuang, I.L. (2000) Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 11, 38-39, 232-233, 248-276.

[25] Mavroeidis, V., Vishi, K., Zych, M. and Jøsang, A. (2018) The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, **9**, 405-414. https://doi.org/10.14569/IJACSA.2018.090354

[26] 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

[27] 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

[28] Akihiro, Y. and Hirokazu, I. (2000) Quantum Cryptanalysis of Block Ciphers. Algebraic Systems, Formal Languages and Computations. *RIMS Kokyuroku*, **1166**, 235-243.

[29] Almazrooie, M., Samsudin, A., Abdullah, R. and Mutter, K.N. (2016) Quantum Exhaustive Key Search with Simplified-DES as a Case Study. *SpringerPlus*, **5**, Article No. 1494. https://doi.org/10.1186/s40064-016-3159-4

[30] Coppersmith, D., Holloway, C., Matyas, S.M. and Zunic, N. (1997) The Data Encryption Standard. Information Security Tech. Rep. No. 2, 22-24. https://doi.org/10.1016/S1363-4127(97)81325-8

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

[32] Zalka, C. (1999) Grover's Quantum Searching Algorithm Is Optimal. *Physical Review A*: *Atomic*, *Molecular and Optical Physics*, **60**, 2746-2751. https://doi.org/10.1103/PhysRevA.60.2746

[33] Patil, S. and Kumar, A. (2010) Implemented Encryption Scheme (One Time Pad) Using 9's Complement. *International Journal of Advanced Research in Computer Science*, **1**, 49-51.

Appendix 1

Bob searches the quantum state of the plain-text (Equation (2)) for the plain-text by Grover's fast quantum mechanical algorithm for database search. He succeeds as solution of the decryption equation is unique for successful communication between Alice and him:

A) Defining a function $g\left(k_s, p_j\right)$ (using the decryption equation, Equation (4)):

$$g\left(k_s, p_j\right)=\begin{cases}1, & \mathrm{E}\left(k_s, p_j\right)=C \\ 0, & \mathrm{E}\left(k_s, p_j\right)\neq C\end{cases} \tag{10}$$

B) Repeating the following operations (a) and (b) for $O\left(\sqrt{N}\right)$ times (Grover Iteration) [26] [27]:

a) Applying the oracle operation [26] [27]:

$$\left|p_j\right\rangle \xrightarrow{O}(-1)^{g\left(k_s, p_j\right)}\left|p_j\right\rangle, \tag{11}$$

where $g\left(k_s, p_j\right)$ is the function defined by Equation (10).

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

$$D\left|P\right\rangle, \tag{12}$$

where the diffusion transform D can be implemented as

$$D=WRW, \tag{13}$$

where W is the Walsh-Hadamard Transform Matrix and R is the phase rotation matrix [26] [27].

C) Measuring the resulting state of $\left|P\right\rangle$ results in $\left|p_t\right\rangle$, the plain-text, with a probability of $O(1)$ [26] [27].

Appendix 2: Example

Suppose the OTP encryption algorithm used by Alice is XOR [33], then we have the information flow in **Figure A1**.

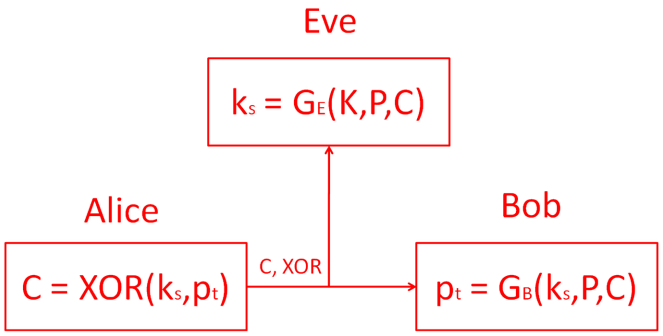

Figure A1. Information flow. G_B: Bob's Grover searching algorithm following **Appendix 1**, substituting XOR [33] for the encryption algorithm E in Equation (10). G_E: Eve's Grover searching algorithm following Section 5.11, substituting XOR [33] for the encryption algorithm E in Equation (6).