scientific reports

Check for updates

OPEN

# Quantum asymmetric key crypto scheme using Grover iteration

Chun Seok Yoon[1,2], Chang Ho Hong[3], Min Sung Kang[4], Ji-Woong Choi[5] & Hyung Jin Yang[1]✉

**Here, we propose a quantum asymmetric key cryptography scheme using Grover's quantum search algorithm. In the proposed scheme, Alice generates a pair of public and private keys, keeps the private keys safe, and only discloses public keys to the outside. Bob uses Alice's public key to send a secret message to Alice and Alice uses her private key to decrypt the secret message. Furthermore, we discuss the safety of quantum asymmetric key encryption techniques based on quantum mechanical properties.**

One of the most important advancements in modern cryptographic systems is the development of asymmetric-key cryptography algorithms. These systems allow us to solve the problems of existing symmetric key cryptography algorithms, such as sharing of secure keys between users, management of keys that increase significantly with the number of participants, and problem of not being able to perform authentication. Asymmetric key cryptography systems have become extremely useful for implementing various cryptographic services such as authentication and signatures[1–3].

In the field of quantum cryptography, which has recently been studied worldwide, various protocols such as quantum direct communication and quantum authentication/signature as well as quantum key distribution, which has entered the commercialization stage through a pilot network, are being developed[4–13]. However, most quantum authentication/signature protocols are being developed based on symmetric key encryption techniques owing to the absence of an efficient quantum asymmetric key crypto scheme. Hence, various tools were utilized to overcome the limitations of symmetry key techniques, which resulted in exposing the disadvantages of protocols being assisted by classical elements or via complex implementation[14–21].

Furthermore, quantum asymmetric key crypto schemes are studied on a smaller scale when compared to other protocols; however, they have a number of similar shortcomings, such as being aided by classical elements, application of symmetric key techniques, or having a structure that makes it difficult to apply the actual public key concept using a quantum entanglement state[22–36].

In this paper, an efficient quantum asymmetric key cryptography scheme based on Grover's algorithm has been proposed[37,38]. The asymmetric key cryptography systems used in modern cryptographic systems are analyzed, and the basic structure of Grover's algorithm is discussed in Section "Asymmetric cipher and Grover algorithm". Subsequently, a quantum asymmetric key cryptography system using Grover's algorithm is proposed in section "Quantum asymmetric key cipher scheme using Grover algorithm". Finally, the security of the system is analyzed in Section "Security analysis".

## Asymmetric cipher and grover algorithm

**Asymmetric cipher.** The specific method of the asymmetric key cryptography system was first introduced in the study, "New directions in cryptography" by Whitfield Diffie and Martin Hellman at Stanford University in 1976. Subsequently, in 1978, Ronald L. Rivest, Adi Shamir, and Leonard Adleman (RSA) at MIT implemented a public key cryptographic system, which is known as the RSA public key cryptography algorithm that is used extensively at present[39,40].

An asymmetric key cryptographic system is based on a trapdoor one-way function. Here, a one-way function refers to a problem in which the calculation in one direction is simple, whereas the calculation of an inverse function (e.g., a hash function) is impossible. A function with a trapdoor, which facilitates the calculation of an inverse function based on certain hints, is known as a trapdoor one-way function. A cryptographic system

[1]Department of Physics, Korea University, Sejong 30019, South Korea. [2]Institute of Convergence Technology KT R&D Center, 151 Taebong-Ro, Seoul 06763, Republic of Korea. [3]The Affiliated Institute of Electronics and Telecommunications Research Institute, P.O. Box 1, Yuseong, Daejeon 34188, Republic of Korea. [4]Korean Intellectual Property Office (KIPO), Government Complex Daejeon Building 4, 189, Cheongsa-Ro, Seogu, Daejeon 35208, Republic of Korea. [5]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea. ✉email: yangh@korea.ac.kr

that allows only people who possess specific information to perform decryption easily based on this function is known as an asymmetric key cryptography system[1–3].

As depicted in Fig. 1, Alice generates a public key P(A) and private key S(A) for herself. The public key is disclosed so that anyone can use it. Bob uses Alice's public key to encrypt a message to be sent to Alice. The encrypted message can be decrypted using the private key that Alice possesses. Bob can securely send a message that can be viewed only by Alice, but he is not required to have a common key with Alice in advance. This is known as asymmetric key cryptographic system.

**Grover iteration.** Grover's algorithm, also known as the quantum search algorithm, determines whether the information to be obtained exists in a database. In previous algorithms pertaining to information search schemes, the time complexity for obtaining the desired data in a database composed of N unsorted data is $O(N)$. However, the quantum search algorithm proposed by Grover in 1997 uses the quantum entanglement phenomenon to obtain the desired data faster when compared to previous methods, and the time complexity is expressed as $O\left(\sqrt{N}\right)$[7,37,38].

The operating principle of Grover's algorithm is as follows:

A database consisting of unsorted data, which contain the desired data is expressed as follows:

$$|M\rangle = \left(\frac{1}{N}\right)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}|i,\ j\rangle \tag{1}$$

The data that you want to find in a database composed of unsorted data is as follows:

$$|K\rangle = |i_0,\ j_0\rangle \tag{2}$$

The operators required to find the desired data in the database are as follows:

$$U_S = I - N|K\rangle\langle K|,\ U_V = C|M\rangle\langle M| - I \tag{3}$$

Extraction of the desired data from Eq. (2) by applying Eq. (3) into the database expressed in Eq. (1) is as follows:

$$\begin{aligned} U_V U_S|M\rangle =& (C|M\rangle\langle M| - I)(I - N|K\rangle\langle K|)|M\rangle \\ =& (C|M\rangle\langle M| - I)(|M\rangle - |K\rangle) \\ =& C|M\rangle - |M\rangle - \left(\frac{1}{(N-1)}\right)|M\rangle + |K\rangle = |K\rangle \end{aligned} \tag{4}$$

$$\because \langle K|M\rangle = \frac{1}{N},\ C = \frac{N}{(N-1)}$$

Equation (4) shows that the desired data $|K\rangle$ can be obtained using Eqs. (1, 2, 3) in the database set $|M\rangle$. Here, database $|M\rangle$ exists in an entangled state. The attacker will be unaware of the exact state of the quantum bit in entangled state because of the singularity of measurement and collapse of quantum state.

In this study, we used the properties of quantum mechanics and the abovementioned advantage to propose a quantum asymmetric cryptography system using the major operation associated with Eq. (4), which is used in Grover's algorithm.

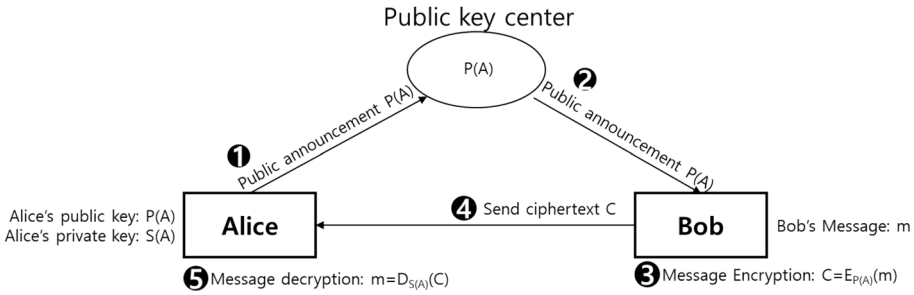


**Figure 1.** Asymmetric cryptography system uses an encryption key that consists of a public key and private key pair. Security in asymmetric key encryption systems relies on managing private keys without exposing them to the outside world. In contrast, public keys can be released to others. Anyone with a public key can create and send a secret message at any time, whereas someone with a private key can open the secret message at any time. In this figure, Bob, who shares Alice's public key P(A), encrypts the message m he wants to send to Alice, and Alice decrypts the message using her private key S(A).

## Quantum asymmetric key cipher scheme using Grover algorithm

As depicted in Fig. 2, quantum asymmetric key cryptography scheme proposed herein consists of the following phases: a phase in which Alice creates a public key and private key, similar to the modern cryptographic system; a phase where Bob uses Alice's public key to send a ciphertext; a phase in which the ciphertext is decrypted.

### Preparation phase.

**P1. Alice creates a state $|M\rangle$ that is only known to her.**

$$|M\rangle = |a\rangle \otimes |b\rangle \tag{5}$$

(Here, $|a\rangle$ and $|b\rangle$ are selected arbitrarily from $|+\rangle$ and $|-\rangle$, respectively.)

**P2.** Alice determines an arbitrary two-bit key $K_{AP}$, that is used as the material of the public key. Subsequently, the following operator is created:

$$U_P = I - 2|K_{AP}\rangle\langle K_{AP}| \tag{6}$$

**P3.** Alice uses $|M\rangle$ and $U_P$ to create a public key $U_{P(A)}$ state and sends it to the public key management center. Here, information exposure can be prevented by randomly selecting whether the operator $U_P$ is applied.

$$\begin{aligned} &U_{P(A)} = U_P|M\rangle = (I - 2|K_{AP}\rangle\langle K_{AP}|)(|a\rangle \otimes |b\rangle) \\ &or \\ &U_{P(A)} = |M\rangle = (|a\rangle \otimes |b\rangle) \end{aligned} \tag{7}$$

### Encryption phase.

**E1. Bob creates the following operator using message $|m\rangle$ to be sent to Alice.**

$$U_m = I - 2|m\rangle\langle m| \tag{8}$$

**E2.** Bob creates the following quantum state using the operator of the message that he wishes to send using Alice's public key, $U_{P(A)}$.

$$\begin{aligned} &U_m U_{P(A)} = U_m U_P|M\rangle = (I - 2|m\rangle\langle m|)(I - 2|K_{AP}\rangle\langle K_{AP}|)(|a\rangle \otimes |b\rangle) \\ &or \\ &U_m U_{P(A)} = U_m|M\rangle = (I - 2|m\rangle\langle m|)(|a\rangle \otimes |b\rangle) \end{aligned} \tag{9}$$

Equation (9) shows the encrypted state of message $|m\rangle$ that Bob wishes to send by using Alice's public key. Bob sends an encrypted message qubit to Alice.

### Decryption phase.

**D1. In the message that Alice receives from Bob, if $|U_P\rangle$ exists in the public key that Alice created, then operator $|U_P\rangle$ is re-applied.**

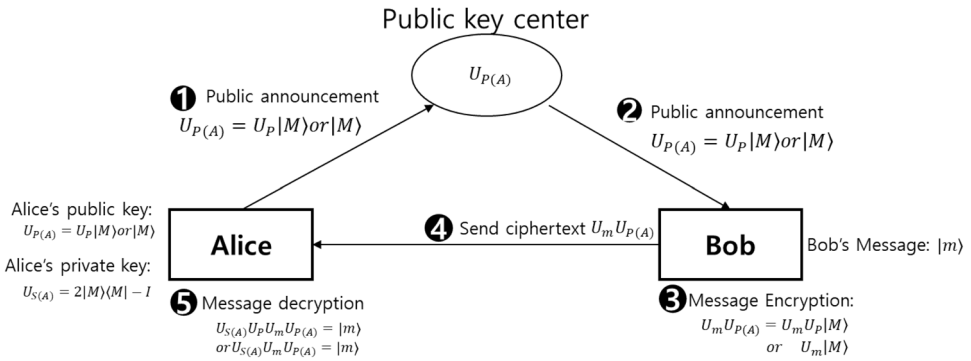


**Figure 2.** Quantum asymmetric key cipher scheme: This figure is a quantum version of the classical asymmetric key cipher scheme depicted in Fig. 1.

$$\begin{aligned} U_P U_m U_{P(A)} =& U_P U_m U_P |M\rangle \\ =& (\mathrm{I} - 2|\mathrm{K_{AP}}\rangle\langle \mathrm{K_{AP}}|)(\mathrm{I} - 2|m\rangle\langle m|)(\mathrm{I} - 2|\mathrm{K_{AP}}\rangle\langle \mathrm{K_{AP}}|)(|a\rangle \otimes |b\rangle) \\ =& (\mathrm{I} - 2|\mathrm{K_{AP}}\rangle\langle \mathrm{K_{AP}}|)\left(|M\rangle - |\mathrm{K_{AP}}\rangle + \left(2\delta_{m,\, K_{AP}} - 1\right)|m\rangle\right) \\ =& (|M\rangle - |\mathrm{K_{AP}}\rangle) - (|\mathrm{K_{AP}}\rangle - 2|\mathrm{K_{AP}}\rangle) + \left(2\delta_{m,\, K_{AP}} - 1\right)\left(|m\rangle - \left(2\delta_{m,\, K_{AP}}\right)|m\rangle\right) \\ =& (|M\rangle - |\mathrm{K_{AP}}\rangle) - (|\mathrm{K_{AP}}\rangle - 2|\mathrm{K_{AP}}\rangle) + \left(1 - 2\delta_{m,\, K_{AP}}\right)\left(2\delta_{m,\, K_{AP}} - 1\right)|m\rangle \\ =& |M\rangle - \left(2\delta_{m,\, K_{AP}} - 1\right)^2 |m\rangle = |M\rangle - |m\rangle \end{aligned} \tag{10}$$

**D2.** Alice uses $|M\rangle$ to create her own private key $U_{S(A)}$.

$$U_{S(A)} = 2|M\rangle\langle M| - I \tag{11}$$

**D3.** Alice applies her private key operator $U_{S(A)}$ to the quantum state created using Eq. (10) and obtains the message $|m\rangle$ that Bob wishes to send to her.

$$\begin{aligned} U_{S(A)} U_P U_m U_{P(A)} =& U_{S(A)} U_P U_m U_P |M\rangle \\ =& (2|M\rangle\langle M| - I)(I - 2|K_{AP}\rangle\langle K_{AP}|)(I - 2|m\rangle\langle m|) \\ & (I - 2|K_{AP}\rangle\langle K_{AP}|)(|a\rangle \otimes |b\rangle) \\ =& |m\rangle \\ & \\ & or \\ U_{S(A)} U_m U_{P(A)} =& U_{S(A)} U_m |M\rangle \\ =& (2|M\rangle\langle M| - I)(I - 2|m\rangle\langle m|)(|a\rangle \otimes |b\rangle) \\ =& |m\rangle \end{aligned} \tag{12}$$

## Security analysis

**Confidentiality.** The component that requires confidentiality in the proposed scheme is the message $|m\rangle$ that Bob wishes to send to Alice. This message must not be revealed to anyone except Bob, who sends the message, and Alice, who receives it. There is a possibility for Eve to attack once, while message $|m\rangle$ is sent from Bob to Alice.

First, the qubit that Eve uses is in an entangled quantum state based on Eq. (9). If Eve measures the qubit, the quantum state collapses and the state prior to the collapse is not known. Furthermore, it cannot be measured accurately without knowing $|U_P\rangle$ and $|U_{S(A)}\rangle$, that is, information required for decryption. In other words, Eve's measurements cannot accurately determine the entangled quantum state.

Second, methods for attacking quantum cryptography include stealing information by creating an entangled state using a CNOT operator. However, in the entangled quantum state, as expressed by Eq. (9), the information that can be obtained based on the attack method using the CNOT operator is the quantum state, which is a component of the public key expressed in Eq. (7). If this is explained on the basis of the two-bit quantum state expressed in Eq. (5), only the state of $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ will be known, and the preceding phases will not be known. However, only when the phases are known, can Eve decipher message $|m\rangle$. In other words, if Eve steals the quantum state of the encrypted message being sent, then message $|m\rangle$ will not be known.

**Kerchhoffs' principle.** A cryptographic algorithm must provide security even if all components excluding the keys used in the algorithm are disclosed.

Based on Kerchhoffs' principle, the cryptographic algorithm should provide security even if all components excluding the private key used are exposed to the attacker. In the proposed algorithm, security is ensured, unless Alice's key material $|M\rangle$ is exposed. Even if Eve steals Alice's public keys $U_P|M\rangle$ and $U_m U_P|M\rangle$ which Bob sends to Alice, an accurate measurement cannot be performed. Therefore, Eve does not know the important key material $|M\rangle$ and message $|m\rangle$ that Bob wishes to send. In other words, even if Eve knows all the stages of the algorithm, it is impossible to obtain relevant information.

**Shor's algorithm.** It has been reported that Shor's algorithm[41,42], which is a typical quantum algorithm, can effectively unravel modern public-key cryptographic algorithms. By effectively factoring integers, the possibility of performing critical attacks on modern cryptographic systems via quantum computers has been demonstrated. However, attacks by Shor's algorithm are threats to modern cryptographic systems that rely on computational complexity; however, they do not pose a specific threat to quantum cryptographic systems that are based on the characteristics of quantum mechanics.

Because the proposed quantum public-key cryptographic scheme guarantees security based on the characteristics of quantum mechanics, it is no relevant to attacks by Shor's algorithm. In other words, the proposed scheme is safe from attacks using Shor's algorithm.

**Comparison of protocol efficiencies.** We can compare the efficiency of our scheme with that of existing schemes in terms of the required quantum sources and qubit efficiency.

The qubit efficiency can be defined as follows:

| | [28] | [34] | [36] | **Proposed scheme** |
|---|---|---|---|---|
| Quantum source | Single qubit | Mixed state | Bell state | 2N single qubits |
| Key spaces | Big | Big | Small | Small |
| Security of private key | One way security | One way security | One way security | One way security |
| Qubit efficiency | 1 | < 50% | 50% | 1 |
| Decryption error | No | Yes | No | No |

**Table 1.** Comparison of the efficiency of our protocol with that of other quantum asymmetric key crypto schemes[28,34,36].

$$Qubit\ efficiency = \frac{c}{q}$$

In this definition, c denotes the total number of classical message bits and q denotes the total number of qubits.

As listed in Table 1, our quantum asymmetric key cryptography scheme is more efficient when compared to other schemes.

## Conclusion

Here, we proposed a quantum asymmetric key cryptographic scheme using Grover's algorithm. In the proposed scheme, Alice uses the public and private keys that she created, and only the public key is disclosed to the outside. Furthermore, Bob can send private messages that are only viewable by Alice without sharing any key with Alice. Even if Eve knows everything about the algorithm and steals the qubit being transmitted, she will not know the content of the private message or Alice's private key. Our proposed quantum asymmetric key cryptography scheme is safe from attacks because its security is based on entanglement, measurement, and collapse, which are the characteristics of quantum mechanics.

**Future work:** Contrary to what we have proposed in this paper, if the message is encrypted with the private key and the encrypted message is decrypted with the public key, it is expected to be used as a quantum authentication/signature protocol with integrity and non-repudiation. Discussions on this topic are considered for future works.

## Data availability

All data generated or analyzed during this study are included in this published article.

Received: 18 September 2022; Accepted: 2 March 2023
Published online: 07 March 2023

## References

1. Menezes, A. J., Paul, C., Van, O., & Scott A. Vanstone. *Handbook of Applied Cryptography*. (CRC press, Boca Raton, 1996)
2. Forouzan, B. A., & Mukhopadhyay, D. *Cryptography And Network Security (Sie)*. (McGraw-Hill Education, Noida, 2011).
3. Stallings, W. & Tahiliani, M. P. (2014). *Cryptography and network security: principles and practice*, vol 6. Editor: Pearson London.
4. Nielsen, M. A., & Chuang, I. *Quantum Computation and Quantum Information*. (American Association of Physics Teachers, College Park, 2002), pp. 558–559.
5. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE International Conf. on Computers, Systems and Signal Processing*, vol 175. p. 8. (NY, 1984).
6. Hong, C. H., Lim, J. I., Kim, J. I. & Yang, H. J. Two-way quantum direct communication protocol using entanglement swapping. *J. Korean Phys. Soc.* **56**(6), 1733–1737 (2010).
7. Yoon, C. S., Kang, M. S., Lim, J. I. & Yang, H. J. Quantum signature scheme based on a quantum search algorithm. *Phys. Scr.* **90**(1), 015103 (2014).
8. Kang, M. S., Hong, C. H., Heo, J., Lim, J. I. & Yang, H. J. Quantum signature scheme using a single qubit rotation operator. *Int. J. Theor. Phys.* **54**(2), 614–629 (2015).
9. Heo, J., Hong, C. H., Lim, J. I. & Yang, H. J. A quantum communication protocol transferring unknown photons using path-polarization hybrid entanglement. *Chin. Phys. Letters* **30**(4), 040301 (2013).
10. Zeng, G. & Keitel, C. H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **65**(4), 042312 (2002).
11. Zeng, G. Reply to comment on 'arbitrated quantum-signature scheme'. *Phys. Rev A* **78**(1), 16301 (2008).
12. Lee, H., Hong, C., Kim, H., Lim, J. & Yang, H. J. Arbitrated quantum signature scheme with message recovery. *Phys. Letters A* **321**(5), 295–300 (2004).
13. Amiri, R., Wallden, P., Kent, A. & Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **93**(3), 032325 (2016).
14. Yin, H. L. *et al.* Experimental quantum digital signature over 102 km. *Phys. Rev. A* **95**(3), 032334 (2017).
15. Yin, H. L. *et al.* Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Phys. Rev. A* **95**(4), 042338 (2017).
16. Lu, Y. S. *et al.* Efficient quantum digital signatures without symmetrization step. *Opt. Express* **29**(7), 10162–10171 (2021).
17. Weng, C. X. *et al.* Secure and practical multiparty quantum digital signatures. *Opt. Express* **29**(17), 27661–27673 (2021).
18. Yin, H. L. *et al.* Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2022**, nwac228 (2022).
19. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**(7705), 400–403 (2018).
20. Xie, Y. M. *et al.* Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **3**(2), 020315 (2022).

21. Gu, J. *et al.* Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **67**(21), 2167–2175 (2022).
22. Kawachi, A., & Portmann, C. (2007). Quantum asymmetric-key cryptosystems secure against computationally unbounded adversaries (theory of computer science and its applications). 数理解析研究所講究録. **1554**, 117–124.
23. Okamoto, T., Keisuke T., & Shigenori U. Quantum public-key cryptosystems. *Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conf. Santa Barbara*, California, 2000 Proc. (Springer, Berlin, 2000).
24. Gottesman, D., & Isaac, C. Quantum digital signatures. *arXiv preprint quant-ph/0105032* (2001).
25. Zeng, G., Saavedra, C., & Keitel, C. H. Asymmetrical quantum cryptographic algorithm. *arXiv preprint quant-ph/0202021* (2002).
26. Kawachi, A., Koshiba, T., Nishimura, H. & Yamakami, T. Computational indistinguishability between quantum states and its cryptographic application. *Eurocryption* **3494**, 2005 (2005).
27. Koshiba, T. Security notions for quantum public-key cryptography. *arXiv preprint quant-ph/0702183* (2007).
28. Nikolopoulos, G. M. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A* **77**(3), 032348 (2008).
29. Gao, F., Wen, Q., Qin, S. & Zhu, F. Quantum asymmetric cryptography with symmetric keys. *Sci. China. Ser. G Phys Mech. Astron.* **52**(12), 1925–1931 (2009).
30. Liang, M. & Yang, L. Public-key encryption and authentication of quantum information. *Sci. China Phys. Mech. Astron.* **55**, 1618–1629 (2012).
31. Luo, M. X., Chen, X. B., Yun, D. & Yang, Y. X. Quantum public-key cryptosystem. *Int. J. Theor. Phys.* **51**(3), 912–924 (2012).
32. Yang, L., Yang, B., & Pan, J. *Quantum public-key encryption protocols with information-theoretic security. Quantum Optics II*, Vol 8440. (SPIE, Bellingham, 2012).
33. Li, X. & Zhang, D. Quantum public-key cryptosystem based on super dense coding technology. *J. Comput.* **8**(12), 3168–3175 (2013).
34. Zheng, S., Gu, L. & Xiao, D. Bit-oriented quantum public key probabilistic encryption schemes. *Int. J. Theor. Phys.* **53**, 116–124 (2014).
35. Wu, C., & Yang, L. A complete classification of quantum public-key encryption protocols. *Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, Vol. 9648. (SPIE, Bellingham, 2015).
36. Wu, W., Cai, Q., Zhang, H. & Liang, X. Quantum public key cryptosystem based on bell states. *Int. J. Theor. Phys* **56**, 3431–3440 (2017).
37. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Letters* **79**(2), 325 (1997).
38. Grover, L. K. Quantum computers can search arbitrarily large databases by a single query. *Phys. Rev. Letters* **79**(23), 4709 (1997).
39. Diffie, W. & Hellman, M. E. New directions in cryptography. *IEEE Trans. Inform. Theory* **22**(6), 644–654 (2022).
40. Rivest, R. L., Adi, S. & Leonard, A. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978).
41. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. *Foundations of Computer Science, 1994 Proc., 35th Annual Symposium on*. (IEEE, NY, 1994).
42. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**(2), 303–332 (1999).


## Author contributions

C.S.Y. conceived and designed the analysis the main idea. C.S.Y., J.W.C. and H.J.Y. wrote the manuscript. C.S.Y., C.H.H and M.S.K. calculated the main calculation. All authors analyzed the results and reviewed the manuscript.

## Competing interests

The authors declare no competing interests.

## Additional information

**Correspondence** and requests for materials should be addressed to H.J.Y.

**Reprints and permissions information** is available at www.nature.com/reprints.

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.