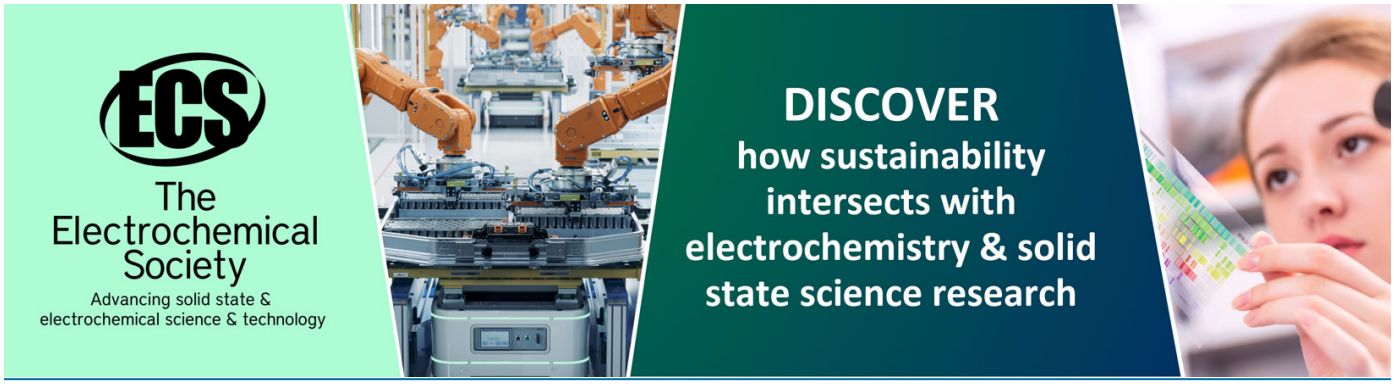
Arbitrated Quantum Signature Protocol with Asymmetric Key Based on Qubit Block Encryption



IOP Conf. Series: Journal of Physics: Conf. Series **1176** (2019) 062056 doi:10.1088/1742-6596/1176/6/062056

Arbitrated Quantum Signature Protocol with Asymmetric Key Based on Qubit Block Encryption

Wenjing Li[1], Qinghai Ou[1], Hongfa Li[2], Qing Wu[1], Changgui Huang[3], Linmu Xieshi[3], Jingran Li[4,*]

[1]State Grid Information and Communication Industry Group Co., Ltd., Beijing, China
[2]State Grid Fujian Power Co., Ltd., FuZhou, China
[3]State Grid Xintong Yili Technology Co., Ltd.,FuZhou, China
[4]School of Beijing University of Posts and Telecommunications, Beijing, China

*Corresponding author e-mail: 15733205015@163.com

Abstract. Here, The new arbitrated quantum signature (AQS) protocol assisted by asymmetric key based on qubit block encryption algorithm is given. Interestingly, our protocol with the asymmetric key can be easily extended to multi-party verification. Unlike all previous quantum works on arbitrated quantum signature, the encryption algorithm of the pre- sented protocol is qubit block encryption. Since, the proposed protocol has a better performance in resisting existential forgery attack. In addi- tion, with the help of the arbitrator, it can be proved that our protocol is secure.

1. Introduction

To the best of our knowledge classical cryptography is not safe in a quantum envi- ronment. This general setting broadly defines the field of quantum cryptography [1]. Quantum signature [2–4] plays an important role in quantum cryptography. AQS is central in quantum signature. Historically, it was an important milestone in the discovery by Zeng and Keitel of his celebrated AQS protocol to solve the identification of the original information [5]. Since then, some meaningful re- sults have been presented. For instance, Bell-states-based AQS protocol [6] and single-states-based AQS protocol [7].

In the work, a new AQS assisted by the asymmetric key based on qubit block encryption algorithm. Interestingly, our protocol with the asymmetric key can be easily extended to multi-party verification. Unlike all previous quantum works on arbitrated quantum signature, our protocol is based on quantum block encryption algorithm. Since, the existential forgery attack cannot work well in this proposed protocol. In addition, with the help of the arbitrator, Bob can verify the validity of a signature. Finally, a detailed analysis and discussion are depicted.

The specific work is as follows. In Section 2, we describe qubit block encryp- tion algorithm. Section 3, with the qubit block encryption, a novel arbitrated quantum protocol with the asymmetric key is proposed. In Section 4, we provide a detailed analysis and discussion. Conclusion is depicted in the last section.

2. The Qubit Block Encryption Algorithm with Hybrid Keys

The proposed algorithm based on the hybrid keys [8] is depicted as follows: For an n-qubit plaintext |P⟩, where

$$\left|P_i^{\backslash}\right\rangle = \alpha_i\left|0^{\backslash}\right\rangle + \beta_i\left|1^{\backslash}\right\rangle, \left|\alpha_i\right|^2 + \left|\beta_i\right|^2 = 1$$

/ / / (1)

The proposed algorithm includes two kinds of keys. The quantum key K1:

$$|K_1\rangle = |K_{11}\rangle \otimes |K_{12}\rangle \otimes \cdots \otimes |K_{1n}\rangle, |K_{1i}\rangle = \alpha_i|0\rangle + \beta_i|1\rangle, \tag{2}$$

where $|\alpha i|2 + |\beta i|2 = 1$. The other is the classical binary key K2,

$$K2 = K21K22\cdots K2n, K2i \in \{0,1\}. \tag{3}$$

In the proposed algorithm, two basic operations are required, including Hadamard gate and Controlled-NOT gate. The Hadamard gate can be depicted as:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(X + Z), \tag{4}$$

with

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{5}$$

And CNOT gate can be depicted as $C|A\rangle|B\rangle \rightarrow |A\rangle|A \oplus B\rangle$, where $A, B \in \{0, 1\}$.

Here, quantum encryption EK can be depicted as (See Fig. 1):

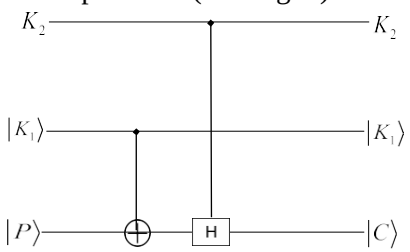


Figure 1. Circuit representation of qubit block encryption.

For one qubit message $|P_i\rangle$, suppose the corresponding quantum key is $|K_{1i}\rangle$, and apply Controlled-Not gate to $|K_{1i}\rangle$ and $|P_i\rangle$, the result turns out to be:

$$\begin{aligned} |P_i'\rangle &= C_{K_{1i}}, P_i|K_{1i}\rangle|p_i\rangle \\ &= C_{K_{1i}}, P_i[(a_i|0\rangle + b_i|1\rangle) \otimes (\alpha_i|0\rangle + \beta_i|1\rangle)] \\ &= C_{K_{1i}}, P_i(a_i\alpha_i|00\rangle + b_i\alpha_i|10\rangle + \alpha_i\beta_i|01\rangle + b_i\beta_i|11\rangle) \\ &= a_i\alpha_i|00\rangle + b_i\alpha_i|11\rangle + \alpha_i\beta_i|01\rangle + b_i\beta_i|10\rangle \end{aligned}$$

Furthermore, Alice encrypts the quantum message $|p_i'\rangle$ with H gate,

$$\begin{aligned} |C_i\rangle &= H^{K_{2i}}|P_i'\rangle \\ &= \delta_{K_{2i,0}}|P_i'\rangle + \delta_{K_{2i,1}}|P_i'\rangle \\ &= \delta_{K_{2i,0}}(a_i\alpha_i|00\rangle + a_i\beta_i|01\rangle + b_i\alpha_i|11\rangle + b_i\beta_i|10\rangle) \\ &+ \delta_{K_{2i,1}}(a_i\alpha_i|0+\rangle + a_i\beta_i|0-\rangle + b_i\alpha_i|1-\rangle + b_i\beta_i|1+\rangle) \end{aligned}$$

3. The Proposed Protocol

The novel AQS protocol is inspired by the ideas from quantum private queries(QPQ) [10].

3.1. Initializing Phase

(I1) Quantum key distribution.

By calling Gao et al.'s protocol [10], Alice and Bob share the asymmetric key Kr1. That is to say, Alice knows the whole key Kr1, and Bob knows q bits of Kr1, where q is a security parameter. Moreover, Trent shares the whole key Kr1 and with Alice and Bob, respectively.

(I2) Shared the classical key.

Similarly, all participants share the classical key for each other, which is respectively denoted by Kr2, K2BT.

3.2. Signing Phase

Alice generates quantum signature RA by encrypting plaintext P in this phase. This presented quantum encryption have two kinds of keys. For simplicity, hybrid keys are respectively denoted by KAB, KAT , KBT .

(S1) Moreover, Alice encrypts |P⟩ with a random number r, where |Pi⟩ =αi|0⟩ + βi|1⟩ . In this protocol, we need two plaintexts.

(S2) With qubit block encryption algorithm, Alice generates |RA⟩ as:

$$\left|R_A\right\rangle = E_{K_{AB}}\left|P^{'}\right\rangle \tag{6}$$

(S3) Alice sends $\left|S\right\rangle = E_{K_{AT}}\left(\left|R_A\right\rangle\right)$ to Trent, and sends $E_{K_{AB}}\left(\left|p^{'}\right\rangle\right)$ to Bob.

3.3. Verifying Phase

With the help of arbitrator, Bob verifies the validity of the signature.

(V1) After receiving $E_{K_{AB}}\left(\left|P^{'}\right\rangle\right)$, Bob obtains |P ′⟩, and he computes

$$\left|R_B^{\mathrm{i}}\right\rangle = E_{K_{AB}}\left|P_i^{'}\right\rangle \tag{7}$$

where i is the ith qubit of the whole key KAB. Then, Bob sends $\left|Y_B\right\rangle = E_{K_{BT}}\left(R_B^{\mathrm{i}}\right)$ to Trent.

(V2) Trent decrypts $|Y_B\rangle$ with K_{BT} and obtains R^i_B, then If $|R^i{}_b\rangle = |R^i{}_A\rangle$,he announces $V_T = 1$; otherwise, he announces $V_T = 0$.

(V3) If $V_T = 1$, Trent upsets the order of |P ′⟩ and $|R_A\rangle$with a permutation function S:

$$\left|P_T\right\rangle = S\left|P^{'}\right\rangle, \left|S_A\right\rangle = S\left|R_A\right\rangle \tag{8}$$

(V4) Trent generates $|Y_T\rangle = E_{KBT}(|P_T\rangle, |S_A\rangle)$ and sends it back to Bob.

(V5) If Trent announces VT = 1, Bob considers signature is valid, and then Alice publishes r; otherwise, Bob considers signature is invalid. If the signature is valid, Bob can obtain $\left|p_T\right\rangle, \left|S_A\right\rangle$. Subsequently, Bob decrypts |PA⟩ with $r\left(s.t.\left|p_A\right\rangle = S\left|p\right\rangle\right)$. Finally, Bob stores $\left(\left|p_A\right\rangle, \left|S_A\right\rangle, r\right)$ as valid signature.

For simplicity, Bob only knows one qubit key, and Alice knows all the keys in proposed protocol. We can make the protocol more secure by letting Bob know more qubits of the final key. Interestingly, our protocol with the asymmetric key can be easily extended to multi-party verification.

4. Security Analysis and Further Discussion

So far, we have designed a new AQS protocol with the asymmetric key based on qubit block encryption algorithm. The security analysis be depicted in the following sections.

4.1. Outside Attack

In this case, the attacker Eve is assumed as an outside eavesdropper. In the proposed protocol, there is a chance for Eve to extract useful information in the stage of sharing keys. However, the security of sharing keys is determined by the unconditional security of QKD protocol. Hence, any secrets cannot be revealed to outside attacker.

Interestingly, Eve can intercept the quantum message. In order to resist this attack, the eavesdropper-checking phase in Ref. [9] should be involved. That is to say, sender choose a lot of

decoy states, i.e. he randomly chooses four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, and randomly inserts them into ciphertext.

Suppose Eve intercepts quantum message and prepares the quantum sequence $|0\rangle^{\otimes n}$. He can obtain four results,

$$C|0\rangle|0\rangle = |0\rangle|0\rangle$$
$$C|1\rangle|0\rangle = |1\rangle|1\rangle$$
$$C|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$
$$= \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$$
$$C|-\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$
$$= \frac{1}{\sqrt{2}}(|+\rangle|-\rangle + |-\rangle|+\rangle)$$

In other words, this presented attack cannot work well in this protocol, and we have

$$P(\text{average}) = (\frac{1}{2})^m \tag{9}$$

4.2 Participant Attack

Unforgeability. If Bob wants to forge a valid signature, then he need to know key K_{AB} to generate $E_{K_{AB}}(|P'\rangle)$. Obviously, this is impossible, because the key is assigned by QKD.

Theorem 1. The Pauli operation σ_X and σ_H cannot be exchanged.

Proof. For Pauli operation σ_H, we have

$$\sigma_H\sigma_X = \frac{1}{\sqrt{2}}(\sigma_X + \sigma_Z)\sigma_X = \frac{1}{\sqrt{2}}(I + \sigma_Z\sigma_X). \tag{10}$$

and

$$\sigma_X\sigma_H = \sigma_X\frac{1}{\sqrt{2}}(\sigma_X + \sigma_Z) = \frac{1}{\sqrt{2}}(I + \sigma_X\sigma_Z) = \frac{1}{\sqrt{2}}(I - \sigma_Z\sigma_X) \tag{11}$$

due to the relation $\sigma_X\ \sigma_Z = \sigma_Z\ \sigma_X$. Obviously the conclusion is established.

More precisely, we give a simple example. Suppose n = 1, $|K_1\rangle = a|0\rangle + b|1\rangle$, $|K_2\rangle = 1$, $|P'\rangle = \alpha|0\rangle + \beta|1\rangle$. It is straightforward to check that the corresponging encryption is $|S_A\rangle = \mathrm{E}_K|P'\rangle = \alpha|-\rangle + \beta|+\rangle$. The dishonest Bob can also mount the existential forgery attacks, i.e. he generates a fake quantum signature pair $(|S_E\rangle,|P_E\rangle)$,

$$|S_E\rangle = \sigma_u|S\rangle, |P_E\rangle = \sigma_u|P\rangle \tag{12}$$

with $\sigma_u \in \{\sigma_x,\sigma_z,\sigma_y\}$. That is, Trent compares whether the quantum signature pair satisfies that $|S_E\rangle = E_K(|P_E\rangle)$. Since Theorem 1, it is sufficient to prove that $|S_E\rangle \neq E_K(|P_E\rangle)$

Suppose that dishonest Bob want to forge signature by obtaining an equivalent key, which this key and the correct key have the same encryption effect. In the qubit block encryption, based on the

different encryp results of the message $\left|P'\right\rangle$, we have $\left|M_{\mathrm{i}}\right\rangle$ kinds of key. Moreover, a kind of key have the number of xj . And, dishonest Bob obtains an equivalent key as,

$$p(k)=\sum_{j=1}^{M_i}(\frac{x_j}{2n})^2 \tag{13}$$

Then, the total probability is

$$p(average)=(\sum_{i=1}^{2^n}\sum_{j=1}^{M^{\mathrm{i}}}(\frac{x_j}{2^n})^2)/2^n \tag{14}$$

The probability can be depicted as

$$p(average)\approx 2^{-0.65n+1.10} \tag{15}$$

In eavesdropper-checking phase, the probability (see Fig.2) is

$$p\approx 2^{-0.65n+1.10}(\frac{1}{2})^m \tag{16}$$

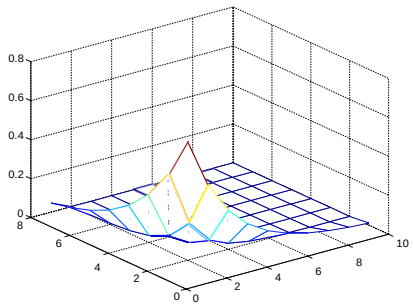


Figure 2. Bob's successful forgery.

Undeniability If the dishonest Alice wants Trent to think that this signature is invalid, i.e. $\left|R_A^i\right\rangle\neq\left|R_B^i\right\rangle$. Obviously, it is impossible. Because she cannot know the quantum key K_{BT} . Bob's denial means that he denied that h Bob's denial means that he denied that he had received

the signature. Due to the secret key is distributed by the QKD protocol, then no one knows the key K_{AB} and K_{BT}. Therefore, Bob cannot refuse to receive the signature. In other words, the arbitrator can judge the truth about Bob's lying. Therefore, Bob cannot successfully deny it.

5. Conclusion

In this paper, the presented encryption with hybrid keys, which is named qubit block encryption algorithm, can be used in our AQS protocol to make more secure. Moreover, this proposed protocol is secure. More importantly, the presented with the asymmetric key can be easily extended to multi-party verification.

References

[1] Gisin, N., Ribordy, G., Tittel, W., et al.: Quantum cryptography. Rev. Mod. Phys. 74, 145-195 (2002)
[2] Zhang L, Sun H W, Zhang K J, et al.: The Security Problems in Some Novel Arbi- trated Quantum Signature Protocols. International Journal of Theoretical Physics 1-12 (2017)
[3] Zhang L, Sun H W, Zhang K J, et al.: An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. Quantum Informa- tion Processing 16(3), 70 (2017)
[4] Sun, H. W., Zhang, L., Zuo, H. J., Zhang, K. J., Ma, C. G.: Offline arbitrated quan- tum blind dual-signature protocol with better performance in resisting existential forgery attack. International Journal of Theoretical Physics 57(9), 2695-2708 (2018)
[5] Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A 65, 042312 (2002)

[6] Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A 79, 054307 (2009)
[7] Zou, X.F., Qiu, D.W.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A 82, 042325 (2010)
[8] Zhou, Nanrun, et al.: Novel qubit block encryption algorithm with hybrid keys. Physica A: Statistical Mechanics and its Applications 375(2), 693-698 (2007)
[9] Zuo H.: Cryptanalysis of quantum blind signature scheme. International Journal of Theoretical Physics 52(1), 322-329 (2013)
[10] Gao F, Liu B, Huang W, et al.: Postprocessing of the oblivious key in quantum private query. IEEE Journal of Selected Topics in Quantum Electronics 21(3), 98- 108 (2015)