Volume : 2 | Issue : 6 | June 2013 • ISSN No 2277 - 8160

Research Paper | Engineering

A New Approach for Blind Signature Using Quantum Cryptography: Blind Arbitrated Quantum Signature

Ashutosh Kaushik IIIT Bhubaneswar, Gothapatana , Malipadam Bhubaneswar

Ajit Kumar Das IIIT Bhubaneswar, Gothapatana , Malipadam Bhubaneswar

Debasish Jena IIIT Bhubaneswar, Gothapatana , Malipadam Bhubaneswar

ABSTRACT

In the recent years signing messages using quantum cryptography has received a lot of attention. Here we describe blinding mechanism in signing message for blind signature using quantum cryptography. In particular, we study the cryptanalysis of Arbitrated Quantum Signature (AQS). Based on our study, we discuss about the possible attacks on it. After discussion about the attacks, we propose a blind signature algorithm for signing messages based on improvements in AQS. Finally we present some interesting topics in future on study of blind signature using AQS.

KEYWORDS: quantum cryptography, blind signatures, AQS, security analysis.

1. Introduction

Cryptography is the approach to protect data secrecy in public environment [3]. Conventional cryptosystem such as ENIGMA, DES or even RSA, are based on the guess-work and mathematics [2]. In classical cryptography, there is either a need of sharing of secret key (symmetric cryptography) or need of mathematical complex problem to solve (asymmetric cryptography). The security of these approaches depends on unproven mathematical assumptions. Apart from the data privacy, for authentication and non-repudiation one more cryptographic primitive is used namely Digital Signature. Digital Signature is mainly used for the authenticity of the message. A valid signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message As we know their security might be susceptible to the strong ability of the quantum computation [1]. Fortunately, this shortcoming is overcome by Quantum cryptography.

For the classical schemes, it has been shown by Shor's algorithm [1] that if in coming future the quantum computers would be developed then it can solve integer factorization problem in polynomial time i.e. RSA problem would be solvable and no more security is possible with that algorithm. Here we discuss about a new kind of cryptography that is based on the principles of physics instead on unproven assumption of mathematics, Quantum cryptography.

Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model. Quantum Cryptography ([2]–[4]) is an emerging technology that could, in a few years, provide a totally secure Internet architecture. The most interesting point is that QC uses single photons instead of electrical or optical signals to obtain secured communications [6].

The BB84 consists of four stages [7] for secret sharing of key. These four stages are transmission of encoded photons, sifting key, reconciliation stage for error detection and corrections and privacy amplification. The benefits of QKD are that it can generate and distribute provably secure keys over unsecured channels and that potential eavesdropping can be detected. QKD is not subject to threats from quantum computers [8].

Apart from the key distribution services, later researchers proved and proposed that quantum cryptography can be used as for authentication and non-repudiation by Quantum Digital Signature. Daniel Gottesman has initially proposed digital signature that uses quantum principles of physics in [9]. In [9] , for signing purpose to generate public-private keys using quantum principles Quantum One-Way Functions are used. A function is said to be one-way if it is easy to compute output from the given input but it is impossible to determine input for a given output.

The rest of this paper is organized as follows. In Sec. II and Sec. III we respectively describe the motivation and applications of QC protocols and in subsequent sections we discuss in detail about the existing AQS scheme and its analysis and our proposed work and attack strategies are demonstrated. And Sec. V is our conclusion.

2. Motivation

The reasons for migrating from classical cryptography to quantum cryptography are the loopholes present in classical scheme. In [10], motivation behind this cryptography is the weakness of classical schemes, which can be classified as "public-key systems", "private key systems", "one-time pad systems". In classical cryptography communicating parties need to share a secret, the key that is exchanged and thus open to security loopholes [11-13]. The current encryption protocols based on mathematical algorithms introduce security holes related to the key refresh and key expansion ratio [10].

The classical cryptography, such as RSA, Diffie-Hellman, and AES, does not detect eavesdropping, but protects data instead based on the computational difficulty of solving an underlying problem [14,15].

However, classical schemes for key distribution rely on the unproven computational assumptions, and if someone discovers a fast technique for factoring large integers, the RSA cryptosystem will not survive anymore [13,16]. Also the higher amount of computation in the process of encryption and decryption significantly reduces the channel capacity bits per second of message information [10]. As computing power increases, and new classical computational techniques are developed, time elapsed in a message can be considered secure will decrease, and numerical keys will no longer be able to provide acceptable levels of secure communications.

3. Applications

Quantum Cryptography can be applicable any where, where we requires the unconditionally secure transmission of information. It requires LOS transmission over open atmosphere; Dedicated, switchless high quality fiber optic connection and in free space channels such as:

- Aircraft-LEO satellite Link
- Earth(MSL)-LEO satellite Link
- Earth-GEO satellite Link

4. Existing Scheme

a. QOTP

As the analog of classical one-time pad, quantum one- time pad (QOTP), also called quantum Vernam cipher [17], uses classical key bits to encrypt quantum states. This cipher plays an important role in AQS protocols and it is meaningful for us to make it clear. Suppose $|P\rangle = \otimes^{k}_{i=1} |p_i\rangle$ is a quantum message composed of n qubits $|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, and the key is K ε {0, 1}2n. The QOTP encryption E_K on the quantum message can be described by

$|C\rangle = E_K |P\rangle = \otimes^k_{i=1} \sigma_x^{k2i} \sigma_z^{k2i-1} |p_i\rangle$,

Decryption is given by

$|P\rangle = E_K |C\rangle = \otimes^k_{i=1} \sigma_z^{k2i-1} \sigma_x^{k2i} |c_i\rangle$,

b. Algorithm

Now we will briefly describe AQS signature scheme without using bell pairs according to [18]. The AQS protocol without using bell states is as follows:-

Initializing Phase:-

Three keys K_{AB}, K_{AT}, K_{BT} are shared between parties Alice and Bob, Alice and Trent, Bob and Trent respectively.

Signing Phase:-

1. Alice obtains three copies of quantum message $|P\rangle = \otimes^n_{i=1} |p_i\rangle$ and encrypts each of them into $|P'\rangle$ using a random number r as the key.

2. Alice performs the following encryptions $|R_{AB}\rangle = E_{KAB} |P'\rangle$, $|S_A\rangle = E_{KAT}|P'\rangle$ and $|S\rangle = E_{KAB}(|P'\rangle, |R_{AB}\rangle, |S_A\rangle)$, and sends $|S\rangle$ to Bob.

Verification Phase:-

1. Bob decrypts $|S\rangle$ and sends $|Y_B\rangle = E_{KBT} (|P'\rangle, |S_A\rangle)$ to Trent.
2. Trent decrypts $|Y_B\rangle$ and verifies whether $|S_A\rangle = E_{KAT} |P'\rangle$. He publishes $V_T = 1$ and sends $|Y_B\rangle$ back to Bob if the equation holds, otherwise $V_T = 0$.
3. Bob decrypts $|Y_B\rangle$ and verifies whether $|R_{AB}\rangle = E_{KAB}|P'\rangle$. If it is, he publishes $V_B = 1$, otherwise $V_B = 0$.
4. When $V_T = V_B = 1$, Bob accepts Alice's signature. In this condition Alice publishes r and Bob recovers $|P\rangle$ from $|P'\rangle$. Finally Bob stores ($|P\rangle$, $|S_A\rangle$, r) as the signed message.

4. Analysis of AQS

Now we will discuss the security of AQS signature without bell pairs. Its analysis is similar to the security discussion of AQS signature with bell pairs in [5]. There are two ways to analyze security of signatures: 1) Bob's Forgery 2) Alice disavowal. We will describe each one by one. Afterwards we discuss one more characteristic.

Bob's Forgery

From Bob's point of view, he can forge signature by one method if he knows the shared signing key. Since key is shared using QKD which has been proven unconditionally secure. Hence for him, forging of signature is not possible in this way. Now we look at a different approach to determine how secure it is against bob's forgery.

Bob can forge signature in some other way like, the value of r is published once then he can proceed in the following manner:

$|P\rangle = D_r |P'\rangle$

Now let he chooses one Pauli operator U_i to apply on $|P\rangle$ to get $|P\rangle$ i.e.

$|P\rangle = U_i |P\rangle$

$|P\rangle = \otimes^k_{i=1} U_i |p_i\rangle$

To forge signature, he needs to modify $|S_A\rangle$ so that it always pass test at Trent. Now we'll see whether it is possible to get $|S_A\rangle$ corresponding to $|P\rangle$ from $|S_A\rangle$ i.e.

$|S_A\rangle = E_{Kat} E'_{Kat} E_r |P\rangle$

$|S_A\rangle = \otimes^k_{i=1} E_{Kat} E'_{Kat} E_r |p_i\rangle$

Now apply same Pauli operator on $|S_A\rangle$ then

$= U_i |S_A\rangle$

$= U_i (E_{Kat} E'_{Kat} E_r |P\rangle)$

$= \otimes^k_{i=1} U_i (E_{Kat} E'_{Kat} E_r |p_i\rangle)$

Since E_{Kat} and E_r are QOTP which are also using Pauli operators. Hence according to the commutation of Pauli operators

$U_i E_{Kat} E'_{Kat} E_r = \pm E_{Kat} E'_{Kat} E_r U_i$

Then

$U_i E_{Kat} E'_{Kat} E_r |P\rangle = \pm E_{Kat} E'_{Kat} E_r U_i |P\rangle$

And now

$U_i |S_A\rangle = \otimes^k_{i=1} U_i E_{Kat} E'_{Kat} E_r |p_i\rangle$

$U_i |S_A\rangle = \pm \otimes^k_{i=1} E_{Kat} E'_{Kat} E_r U_i |p_i\rangle$ (10)

Note that every $|pi\rangle$ is a pure state of a single particle, which is limited by the probabilistic comparison of two unknown quantum states [18]. In this condition, all the

Minus signs in above Eq. are global phases and can be omitted. Therefore, we have

$U_i |S_A\rangle = \otimes^k_{i=1} E_{Kat} E'_{Kat} E_r U_i |p_i\rangle$

$U_i |S_A\rangle = \pm \otimes^k_{i=1} E_{Kat} E'_{Kat} E_r U_i |p_i\rangle$

$U_i |S_A\rangle = \otimes^k_{i=1} E_{Kat} E'_{Kat} E_r |p_i\rangle$

$U_i |S_A\rangle = E_{Kat} E'_{Kat} E_r |P\rangle$

$U_i |S_A\rangle = |S_A\rangle$

Accordingly in the same way he can change $|R_{AB}\rangle$ and when provide the new signature to Trent for the new message, then it will always pass verification test at Trent. In this way Bob can achieve forgery in Alice's signature.

Alice's Disavowal

After discussion about Bob's forgery, now we will analyze another security metric of the scheme viz is Sender's disavowal or Alice's Disavowal. This is main security concern with the signature algorithms i.e. signer cannot deny from his signature once he has signed.

Alice can disavow from his signature. Since in 3rd step of verification, Trent sends $|S_A\rangle$ in the Y_B which is cipher text for Bob due to not knowing key K_{AT}. Trent sends $|Y_B\rangle = (|P'\rangle \otimes |S_A\rangle \otimes |V_T\rangle)$. Now, Alice can modify few last n qubits of the $|S_A\rangle$ so that it is not a valid signature for message and she can identify this qubits in $|Y_B\rangle$ very easily since $|P'\rangle$, $|S_A\rangle$ and $|V_T\rangle$ are determinate. After identifying these qubits in $|Y_B\rangle$ she can change them accordingly so that it will not be a valid message-signature pair any more.

Since Bob does not now key K_{AT} hence he can not determine modifications in $|S_A\rangle$. After verification, when he will say Alice to fulfill her contract at later time, then Alice can deny from the contract by declaring that this contract doesn't have her sign and when Bob will send this modified signature to Trent for verification, then it will fail the test and Trent will stand on Alice's side by announcing that Bob forged signature.

Blindness

In AQS[18] signature scheme author's name did not discuss any blinding factor to generate blind signature using quantum mechanics principles which can be further used in applications like digital Cash.

5. Proposed Algorithm

Before discussing about our proposed work, we will introduce few operations which we will use in our scheme.

Apart from QOTP we will use one more encryption operation which is given as Encryption operation En

$|Cn\rangle = En_K |P\rangle$

Where $En = \sigma_x$ if $K_i = 0$ and $En = \sigma_z$ if $K_i = 1$

$|P\rangle = Dn_K (|Cn\rangle)$

Where $Dn = \sigma_x$ if $K_i = 0$ and $Dn = \sigma_z$ if $K_i = 1$

Another operation, that we will use, is CONV. This is very simple operation that we consider for our simplicity to convert bits to quantum states and quantum states bits. i.e.

$|R> = CONV(R)$

If R = 0 then CONV(R) = |0> and R = 1 then CONV(R) = |1> and vice-versa.

Algorithm

Now we will propose an algorithm for blind arbitrated quantum signature. Algorithm is as:

Initial Phase:-

Requestor Alice, Signer Bob and verifier Charlie establish keys between them by unconditionally secure method QKD. i.e.

- Alice and Bob K_{ab}
- Alice and Charlie K_{ac}
- Bob and Charlie K_{bc}

Blind Phase:-

- Requestor Alice calculates fingerprint of message M as $R = H(M)$
- Use CONV operation to convert R into quantum string |R>.
- Use K_{ac} to encode |R> with encryption operation En. i.e. $|R'> = En_{Kac}(|R>)$
- Requestor sends |R'> to signer by creating string $E_{KAB}(|R>')$.

Signature Phase:-

- Signer gets string |R'> and creates its one copy and encodes one copy using K_{bc} with encryption operation En. $|S'> = En_{Kbc}(|R'>)$
- Now signer selects a random string of 0 & 1 of length 2n and encrypts |S'> using QOTP and r as a key i.e. $|S>=E_r(|S'>)$
- Signer converts r to |r> and encodes it using QOTP and K_{bc} i.e. $|r> = CONV(r)$, $|r_c> = E_{Kbc}(|r>)$
- Now signer sends (|S> , $|r_c>$) to requestor as a blind signature.

Verification Phase:-

- After signature generation, signature is sent to Trent for verification.
- Trent decodes $|r_c>$ and gets r'. $|r'> = D_{Kbc}(|r_c'>)$, $r' = CONV(|r'>)$
- Now verifier checks for the following condition

$CONV(Dn_{Kac}(Dn_{Kbc}(D_{r'}(|S>)))) = H(M)$

- If above condition satisfies then signature is accepted as valid signature and verifier stores value of r' and |S> for future reference.

7. Security Analysis

Now we will discuss security measures of our proposed work in sequence.

- **Proof Of correctness**

If all entities perform each step correctly then the given condition in verification phase must be satisfied.

$CONV(Dn_{Kac}(Dn_{Kbc}(D_{r'}(|S>)))) = H(M)$

Consider LHS:

$CONV(Dn_{Kac}(Dn_{Kbc}(D_{r'}(|S>))))$

$= CONV(Dn_{Kac}(\underline{Dn_{Kbc}(|S'>)}))$

$= CONV(\underline{Dn_{Kac}(|R'>)})$

$\underline{= CONV(|R'>)}$

$= R$

$= H(M)$

$= RHS$

- **Blindness**

It can be seen from the blinding step where requestor calculates finger-print of message and encrypt it with verifier's key which is unknown to signer due to unconditional security of key. Hence content is cipher text for signer and remains hidden from him.

- **Receiver's Forgery**

We will prove that receiver is unable to forge the signature. We will prove it by contradiction. Suppose that receiver tries the attack on signature forgery in the same way as we discussed earlier, then he has to apply Pauli operator on the |R> to generate |*R*> and same operator has to be applied on |S'> to get corresponding |*S'*> as,

$|R> = U_i|R>$ and

$|S'> = U_i|S'>$

But for *R* he has to determine the corresponding message M that will always pass verification test at verifier. But this is impossible to determine a message from the given hash code due to the one-way property of hash functions. Hence he will not be able to generate a valid message-signature pair.

- **Sender's Disavowal**

It can be seen from the fact that after verification, verifier keeps copy of signature |S'> and r with himself. In future if any dispute occurs then receiver will be asked to present message M and Trent will check for the condition in verification phase. If ti satisfies then he announces that signer is disavowing form his sign.

7. Conclusion

We discuss the security of AQS protocol without using bell pairs. In discussion describe the attacking strategies on scheme from sender's as well as receiver's perspective. We also discuss about the blindness of the signature scheme. After that discussion we proposed an algorithm that resolves loopholes of the AQS without using bell pairs.

As we presented in previous sections AQS is a simple model. To our knowledge, this is the only model which can overcome Barnum et al's limit [19] now, and is feasible in theory. But AQS protocol is still valuable and a topic of interest for further study in future. In our opinion some other topics for study in field of quantum cryptography are study of public key Quantum cryptosystem which can provide more security and less computation.

REFERENCES

[1] P. W. Shor, 1994, "Algorithms for quantum computation: Discrete logarithms and factoring", in Proc. 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico, p.124. | [2] C. H. Bennett and G. Brassard, 1984, "Quantum cryptography: Public key distribution and coin tossing or BB84", in Proc. IEEE International Conference on Computers, Systems and Signal, Bangalore, India, , p.175. | [3] C. Bennett, F. Bessettee, G. Brassard, L. Salvail, and J. Smolin, September 1991, "Experimental quantum cryptography,". | [4] N. Gisin and al, January 2002, "Quantum cryptography", Reviews Modern Physics, vol. 74, pp. 145–195. | [5] Fei Gao et al, 22 jun 2011, "Cryptanalysis of the arbitrated quantum signature protocols ", Technical report available at http://arxiv.org/abs/1106.4398 ,. | [6] Quoc-Cuong Le, Patrick Bellot, 2006, "Enhancement of AGT Telecommunication Security using Quantum Cryptography ", Research, Innovation and Vision for the Future, 2006 International Conference on , vol., no., pp.7,16, Feb. 12-16. | [7] R. Lalu Naik et al, December 2011, "Quantum Cryptography with Key Distribution in Wireless Networks on Privacy Amplification", International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1. | [8] Alan Mink et al, July 2009, "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, pp. 101-112 | [9] D. Gottesman, I. Chuang, 2001, "Quantum digital signatures", Technical report, available at http://arxiv.org/abs/quant-ph/0105032. | [10] Mehrdad S. Sharbaf, 2009, "Quantum Cryptography: A New Generation of Information Technology Sec urity System", 2009 Sixth International Conference on Information Technology: New Generations p.1644-1648 | [11] Bruss, D., Erdelyi, G., Meyer, T., Riege, T., & Rothe, J., 2007, " Quantum cryptography: A survey". ACM Computing Surveys, 39(2), p. 1-27. | [12] Buchmann, J., May, A., & Vollmer U., 2006, " Perspective for cryptographic long-term security" Communications of ACM Vol.49, No. 9, pp. 50-56. | [13] Coron, J. S., 2006, " What is cryptography?", IEEE Security & Privacy Journal, 12(8), p. 70-73. | [14] Simmon, G. J., 1979 ,"Symmetric and asymmetric encryption", ACM Computing Surveys, 11(4), p. 305-330. | [15] Bruss, D., Erdelyi, G., Meyer, T., Riege, T., & Rothe, J., 2007, " Quantum cryptography: A survey". ACM Computing Surveys, 39(2), p. 1-27. | [16] Papanikolaou, N., "An introduction to quantum cryptography", ACM Crossroads Magazine, Vol.11 No.3, 2005, pp. 1-16. | [17] D. W. Leung, (2002), Quantum Inf. Comput. 2, 14. | [18] X. Zou and D. Qiu, (2010) Phys. Rev. A 82, 042325. | [19] H. Barnum, C. Cr´epeau, D. Gottesman, A. Smith, and Alain Tapp, e-print quant-ph/0205128.