JOURNAL OF COMPUTING AND SECURITY manuscript No.
(will be inserted by the editor)

A Blind Signature Based on Quantum Key Distribution

Siavash Khodambashi* ·
Ali Zakerolhosseini

Received: date / Accepted: date

Abstract Recently, the laws of quantum physics have amazed classical cryptography and aided researchers to provide secure communications in presence of adversaries. In this paper we present a novel blind signature scheme whose security is guaranteed by fundamental principles of quantum physics. Despite previous schemes which are taking advantage of quantum entangled states, our proposed quantum blind signature relies only on Quantum Key Distribution (QKD) protocol. We show throughout this paper that our proposed quantum blind signature outperforms previous schemes in security and reliability. In addition, it is feasible for the proposed scheme to become commercialized with current technology. Hence, it can be widely used for e-payment, e-government, e-business and etc.

Keywords Quantum blind signature · Quantum key distribution · Quantum cryptography · Quantum payment

1 Introduction

A considerable issue in cryptography is how to authenticate a message as if a handwritten signature on a paper document would certify the originality of the message. Digital signatures are widely used to guarantee the authenticity, integrity and non-disavowal of transmitted messages. However, standard digital signatures may harm the owner's privacy due to the fact that they are not capable of protecting the anonymity of message owners.

Siavash Khodambashi
Electrical and Computer Engineering Department, Shahid Beheshti University; G.C., Tehran, Iran
E-mail: siavashyp@yahoo.com

Ali Zakerolhosseini
Electrical and Computer Engineering Department, Shahid Beheshti University; G.C., Tehran, Iran
E-mail: a_zaker@sbu.ac.ir

A fundamentally new kind of signature was introduced by Chaum in 1983 which allows an automated payments system with some properties that were not possible in the previous digital signatures including inability of third parties to determine payee, ability of individuals to provide proof of payment and ability to stop use of stolen payments [1]. Blind signature is a form of digital signature in which the content of a message is disguised prior to get signed. Therefore, the signatory learns nothing about the message he signs while the user can not compute any additional signature without the help of the signatory. However, the produced blind signature can be publicly verified with respect to its original message in the manner of a regular digital signature. Blind signatures are typically employed in protocols where signer and message author are different parties and anonymity of the message owner is important, e.g. cryptographic election systems and digital cash schemes.

As an analogy, consider that Alice has a letter which ought to be signed by her boss, i.e. Bob. However, due to her privacy, the content of her letter should not be revealed to Bob. So, she puts the letter in an envelope lined with carbon paper and hands it to Bob. Later, Bob will sign the outside of the carbon envelope without opening it and then return it back to Alice. Alice can then open the envelope to find her signed letter, so that Bob has not seen its content.

The blind signature proposed by Chaum was based on the complexity of factoring large integers. Some other blind signatures based on elliptic curves were also proposed in [2] and [3]. In fact, all of the classical blind signatures are based on the computational complexities and their security is guaranteed by mathematics as well as limited computational power of classical computers. Hence, they are safe in front of classical processors. Unfortunately, they are vulnerable to quantum computers. Quantum parallelism can solve some complex problems, e.g. the factoring problem and the discrete logarithm problem, much faster than the classical computers [4–6]. Hence, researchers have shown great interest on quantum methods which are secure even against quantum processors.

For the first time, a quantum signature was introduced by Zeng et al. in 2001 [7]. Zeng's quantum signature was taking advantage of the correlation of quantum entangled states. In that year, Gottesman and Chuang [8] proposed a quantum one-way function and introduced their quantum digital signature. Although the early mentioned quantum signatures fulfill unconditional security and message authenticity, they can not please message blindness.

The idea of quantum blind signature was originally proposed by Wen et al. [9] in 2009. There would not be a unique blind signature for a blind message in Wen's quantum blind signature and so the verifier is not able to authenticate the message half the times as criticized by Naseri [10] and Su [11]. Hence, Wen's scheme does not fairly complete the task of blind signature. Later, a sessional blind signature based on quantum entangled states was proposed by Khodambashi and Zakerolhosseini in 2013 [12]. Their proposed scheme is reliable and secure against quantum attacks including Trojan horse attacks and etc.. It also fulfills the ideal blind signature requirements e.g. blindness, non-

disavowal and no-counterfeiting. Their scheme employs Einstain-Podolskey-Rosen (EPR) entangled pairs in the signing process. Although it is feasible to implement entangled pairs with current technology, there exist some limitations in their usage for real applications. Hence, a quantum blind signature which does not rely on quantum entanglement is of interest.

In this paper we present a quantum blind signature based on Quantum Key Distribution (QKD) protocol. Our proposed scheme uses QKD for safe transfer of classical data and unlike classical methods it does not rely on computational complexities. Since the security of QKD has been proved in [13], therefore our proposed scheme is unconditionally secure and efficient. Furthermore, QKD has been commercialized in recent years by several corporations around the world. Hence, it is possible to simply implement our proposed quantum blind signature for everyday applications.

The rest of the paper is organized as follows: in Sect. 2, blind signature types and their properties are addressed. Sect. 3 reviews QKD protocol in brief. The proposed quantum blind signature scheme is presented in Sect. 4. In Sect. 5, the security of the proposed quantum blind signature is analyzed. At last, Sect. 6 concludes the paper.

2 Blind signature requirements

There are three parties in a blind signature protocol: the message owner Alice, who requests for an endorsement, the signatory Bob, who confirms the message by signing it and the verifier Charlie, who checks the authenticity of the message. In a classical blind signature, a message needs to pass a three-step procedure in order to be effective as illustrated in Fig. 2. At first, Alice blinds her message and gives it to Bob who is the signatory. Bob confirms Alice's message by signing it blindly. Thus, he knows nothing about the message and returns the signed message back to Alice. Subsequently, Alice removes the blinding factor from the signed message while preserving the signature. Later, she can deliver her message to the verifier Charlie who checks the validity of the signed message.

After that the concept of blind signature was initially proposed by David Chaum in 1983, there have been many efforts to construct blind signature schemes. They lend themselves to electronic commerce, electronic cash, electronic voting and anonymous access control systems. In some cases, the security of the blind signatures is considered at the moment when the signatory signs the message. It was taken for granted whether a blind signature remains anonymous when it is presented later to the signatory who can store the signature parameters of all signed messages. On the other side, it is required for some applications that the generated blind signature remains anonymous at the time of verification by the signatory. This new aspect leads to a classification of blind signatures.

It is possible to distinguish two classes of blind signatures depending on the strength of anonymity given by the signature:

Fig. 1 Classic blind signature process

(a) Weak blind signatures in which there exists a relation between the blind signature parameters and the message. Therefore, the signatory can store the signature parameters to identify the owner of the message at a later time. This fact can be beneficial in some applications e.g. e-payment and e-commerce in order to prevent yeggmen and launderers.
(b) Strong blind signatures in which the signatory will not recognize the owner of the message even if he stores the signature parameters while he signs the message, so that the signature is totally anonymous. Many applications take advantage of this ultimate anonymity e.g. electronic voting where the identity of voters has to be unknown.

Generally speaking, there are four main characteristics for blind signatures listed as follows:

(a) *Blindness*, the scheme should be blind i.e. the signatory is not able to read the message as he signs it.
(b) *Anonymity*, the owner of the message must remain anonymous in strong blind signatures, so that the signatory can not trace the message owner.
(c) *Originality*, no one can counterfeit a legitimate signature generated by a certified signatory.
(d) *Non-refusal*, the signatory can not disavow his signature.

In weak blind signatures, it is possible for a signatory to trace the owner of the message when disagreement happens. Hence, the second characteristic is only limited to strong blind signatures. Like classical cryptography, quantum blind signatures are also required to have above characteristics.

3 Quantum key distribution overview

A secret key establishment between two spatially separated parties is of immediate interest for practical cryptographic applications such as secure message transmission. We consider a setting where two distant parties, traditionally called Alice and Bob, want to establish a common secret key i.e. a string of random bits which is unknown to an adversary, Eve. We assume that Alice

and Bob already have some means to exchange classical messages authentically i.e., upon receiving a message, Bob can verify whether the message was indeed sent by Alice, and vice-versa. In fact, only relatively weak resources are needed to turn a completely insecure communication channel into an authentic channel. For instance, Alice and Bob might invoke an authentication protocol presented in [14,15] for which they need a short initial key. Practically, it is sufficient for Alice and Bob to start with only weakly correlated and partially secret information instead of a short secret key as indicated in [16,17].

The information-theoretic security which is actually the strongest reasonable notion of security, guarantees that an adversary does not get any information correlated to the key, except with negligible probability, in contrast with computational security which is time-consuming for an adversary but not impossible. It is impractical for Alice and Bob to share a secret key if they only connected by a classical authentic communication channel [18,19]. The story changes dramatically with the help of quantum mechanics.

Bennett and Brassard [20,21] proposed a quantum key distribution (QKD) for the first time. Their scheme is well-known as BB84 and uses communication over a completely insecure quantum channel in addition to the classical authentic channel. QKD is generally based on the fact that observing a quantum mechanical system would change its state. An eavesdropper trying to wiretap the quantum communication between Alice and Bob would thus inevitably leave traces which can be detected. Thus, as long as the adversary is passive, QKD generates a secret key. On the condition that the eavesdropper tampers with the quantum channel, the attack is recognized by the protocol and the computation of the secret key is aborted. Note that this situation is actually the best one can hope for. Due to insecurity of the quantum channel, an adversary might always interrupt the quantum communication between Alice and Bob, in which case it is impossible to share a secret key. For any attack on the quantum channel, the probability that QKD does not abort and the adversary gets information on the generated key is negligible [13].

QKD uses an encoding of binary bits in qubits i.e. two-level quantum systems. This encoding regards to one of two different orthogonal bases, called the rectilinear and the diagonal basis. Because these two bases are mutually unbiased, a measurement in one of the bases reveals no information on a bit encoded with other basis. Such a property of quantum mechanics makes quantum cryptography advantageous over classical cryptography which aids only from limited computational power of classical processors. QKD protocol is described as follows:

Step1- Alice generates n random qubits $x_1, \ldots, x_n$ either in the rectilinear or the diagonal basis and transmits them to Bob through quantum channel.

Step2- Bob measures each of the qubits he receives with respect to the basis chosen randomly to obtain binary values $y_1, \ldots, y_n$. The pair of binary strings $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ held by Alice and Bob are called raw key.

Step3- Alice and Bob announce their chosen bases publicly and discard all bits of their raw key for which the encoding and the measurement bases are not compatible. The remained key is called sifted key.

Step4- Alice and Bob compare some randomly chosen set of bits of the sifted key in order to estimate the error rate i.e. the fraction of positions i in which x_i and y_i disagree. If the error rate is high, Alice and Bob abort the protocol due to the possibility of an eavesdropper corrupting the transmitted qubits. At the end of this step, they discard all bits they have compared and preserve the remaining bits ($X^{'}$ and $Y^{'}$).

Step5- Alice sends certain error correcting information on $X^{'}$ to Bob. It allows Bob to guess $X^{'}$ with the aid of $Y^{'}$. Note that $X^{'}$ and $Y^{'}$ only differ in a limited number of positions.

Step6- Alice and Bob use an agreed hashing to turn the string $X^{'}$ into a shorter but secure. Hence, they have a shared secret key. This step is called privacy amplification.

The security of the BB84 protocol is based on the fact that an eavesdropper cannot gain information about the encoded bits without disturbing the qubits sent over the quantum channel. If the disturbance is too large, Alice and Bob will abort the protocol in the error estimation step. On the other hand, if the error rate is below a certain threshold, then the strings $X^{'}$ and $Y^{'}$ held by Alice and Bob are sufficiently correlated and secret in order to distill a secret key. In the course of this research, a large variety of alternative QKD protocols has been proposed. Some of them are very efficient with respect to the number of key bits generated per channel use [22,23]. Others are designed to cope with high channel noise or noise in the detector, which lends themselves to practical implementations [24]. The structure of these protocols is mostly very similar to the BB84 protocol e.g. [22,23,25].

4 The proposed quantum blind signature

We describe our quantum blind signature in details throughout this section by giving a feasible instance. Assume a situation involving three parties: the requester Alice, the manager Bob and the attendant Charlie. Alice is going to receive some services from Charlie. However, she requires Bob's authorization first. Alice writes down her request in form of an n-bit binary message M. Due to the privacy reasons, she does not like her message content be revealed. Hence, she gets her message signed blindly by Bob in order to make it certified. Finally, Charlie verifies the signature of Alice's message and provides her the services that she requested on the condition that the signature is valid.

This scenario exhibits one of the applications of our proposed quantum blind signature. Here, we describe all steps of the quantum blind signature consisting of four phases:

4.1 Requesting a session

Step1- Charlie and Alice agree on an n-bit binary secret key K_S using QKD at the moment that Alice makes a request for some services from Charlie. Note that K_S is completely a random binary string.
Step2- Alice forms her message, M which is an n-bit binary string containing her request. It is assumed that Alice can fit her request in an n-bit string.

4.2 Blinding the message

Step1- Alice uses exclusive OR to transform message M into $M^{'} = M \oplus K_S$. Due to the randomness of K_S, retrieval of M without knowing K_S is impossible.

4.3 Signing the blind message

Step1- Alice and Bob agree on an n-bit secret key K_{AB} using QKD. K_{AB} is completely random.
Step2- Alice combines her blind message $M^{'}$ with K_{AB} using XOR to form $M^{"} = M^{'} \oplus K_{AB}$ and sends it to Bob through classical channel using one-time pad protocol.
Step3- Bob receives $M^{"}$ and use XOR to restore $M^{'} = M^{"} \oplus K_{AB}$.
Step4- Bob and Charlie share an n-bit random secret key K_{BC} by applying QKD protocol.
Step5- Bob uses XOR to transform blind message $M^{'}$ into blind signature $S^{'} = M^{'} \oplus K_{BC}$ which is an n-bit string.

4.4 Verification

Step1- Charlie receives blind signature $S^{'}$ from Bob and retrieves blind message $M^{'}$ by applying XOR, so that $M^{'} = S^{'} \oplus K_{BC}$.
Step2- Charlie removes blinding factor to recover original message by using XOR as $M = M^{'} \oplus K_S$. Hence, Charlie can read Alice's message M and provide the requested services.

It is remarkable to note that Alice, Bob and Charlie, as participants in this protocol, use authentication protocols to identify themselves when performing QKD. Otherwise, any adversary can impersonate them and take advantage of his misbehavior. The procedure of our proposed scheme has been illustrated in Fig. 2.

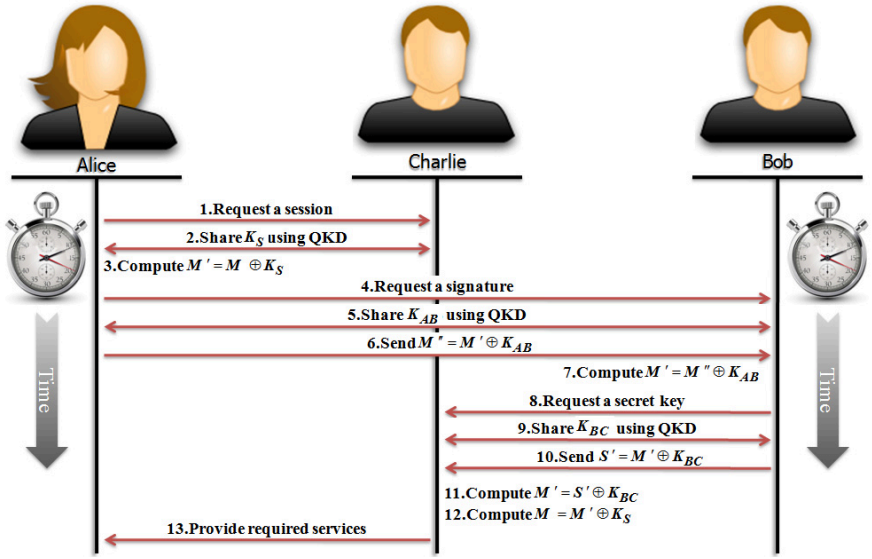

Fig. 2 The proposed quantum blind signature protocol

5 Security analysis

The security of our proposed quantum blind signature is discussed throughout this section. We show that our scheme fulfills all the requirements that an ideal blind signature needs to have including blindness, no-counterfeiting and no-disavowing. The security of the scheme is analyzed in presence of adversaries equipped with quantum technology. We also consider situations in which one or more of the parties may behave maliciously and prove that the proposed scheme is still secure.

5.1 Quantum attack failure

Assume an eavesdropper called Eve who has knowledge of our proposed quantum blind signature. Due to the no-cloning theorem [26], it is impossible for Eve to make a perfect copy of a qubit without knowing the basis in which it has initially been created. Hence, eavesdropping can not be done while two parties in the protocol are transferring qubits using QKD since it can be detected by the protocol. This fact has been proved in [13]. From the statement, it can be inferred that Eve is not capable of gaining proper information of the transferred qubits, so that she can not discover the message M nor the blind signature S'. This scheme is also secure against intercept-resend and man-in-the-middle attacks due to the unconditional security of both QKD and one-time pad protocols [27].

5.2 No-counterfeiting

Imagine that Charlie is not honest and tries to tamper the message or the blind signature by taking advantage of secret keys K_S and K_{BC} to get some benefit. On such a disagreement, Alice and Bob can publicly announce the message and the blind signature and catch Charlie red-handed. A situation can be imagined in which Alice behaves maliciously in order to modify her message after being signed blindly by Bob. This would be impossible since Bob delivers his blind signature to Charlie by QKD and one-time pad protocol which are unconditionally secure. Also Bob can not alter the message because it has been blinded by Alice. All data exchanges in the scheme are carried out through QKD and one-time pad protocols, so that no one can eavesdrop or counterfeit the data.

5.3 Blindness

When Alice requests a session from Charlie, they agree on a secret key K_S which is completely a random binary string. No one except them has knowledge of K_S. Alice makes her message illegible using XOR i.e. $M^{'} = M \oplus K_S$. Due to the randomness of K_S, it is impossible for Bob to discover the original message M without knowing K_S, still with a quantum processor. Hence, only Alice and Charlie can remove the blinding factor of the message.

5.4 Non-disavowal

The verifier, Charlie receives the blind signature $S^{'}$ from Bob, encrypted with secret key K_{BC} which is only known to them both. Hence, Bob can not deny his ownership of the blind signature. Similarly, Alice is not able to disavow her message M due to K_S.

5.5 Reliability

In Wen's quantum blind signature [9], Charlie can decisively confirms the i^{th} bit of the message when $m(i) = K_{bc}^{2i-1}$. However, he knows nothing when $m(i) \neq K_{bc}^{2i-1}$. Due to the randomness of K_{bc}, this situation happens half the times in a bit-to-bit verification process. Therefore, Wen's scheme does not lend itself to delicate applications which high reliability is required. However, there is a bit-to-bit correspondence between the blind message and the blind signature in the sessional quantum blind signature, proposed in [12], and also our proposed scheme which can be verified precisely and is useful for electronic payment or access control systems. In other words, our proposed quantum blind signature is reliable.

6 Conclusion

In this paper, we introduced a novel blind signature whose security is guaranteed by quantum physics. The scheme takes advantage of Quantum Key Distribution (QKD) in order to provide security for data exchange. To the best of our knowledge, QKD has been commercialized in recent years by several corporations [28,29]. Thus, our scheme can be truly employed in some applications e.g. electronic payment, access control systems and etc.. Although the message content is invisible to the signatory, it is correlated to the blind signature. Hence, the signatory can trace owner of the message when a disagreement happens. This is worthwhile in some applications including e-payment to prevent yeggmen and launderers.

References

1. D. Chaum. Blind signature for untraceable payments. In *Advances in cryptology, proceeding of CRYPTO'82*, pp. 199-203, Springer, 1983.
2. M. Nikooghadam and A. Zakerolhosseini. An effcient blind signature scheme based on the elliptic curve discrete logarithm problem. *The ISC Int'l Journal of Information Security*, 1(2):125-131, 2009.
3. M. Nikooghadam, A. Zakerolhosseini and M. Ebrahimi Moghaddam. Efficient utilization of elliptic curve cryptosystem for hierarchical access control. *The Journal of Systems and Software*, 83:1917-1929, 2010.
4. M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. *Cambridge University Press*, Cambridge, 2000.
5. C.H. Bennett and D.P. DiVincenzo. Quantum information and computation. *Nature 404*, pp. 247-255, 2000.
6. M.A. Galindo and M. Delgado. Information and computation: classical and quantum aspects. *Rev. Mod. Phys. 74*, pp. 347-423, 2002.
7. G. Zeng, W. Ma, X. Wang and H. Zhu, Signature scheme based on quantum cryptography. *Acta Electron. Sinica* (in Chinese), 29(8):1098-1100, 2001.
8. D. Gottesman and I.L. Chuang. Quantum digital signatures. 2001. arXiv:quant-ph/0105032v2, Available at: http://arxiv.org/abs/quant-ph/0105032v2
9. X.J. Wen, X.M. Niu, L.P. Ji and Y. Tian. A weak blind signature scheme based on quantum cryptography. *Opt. Commun.* 282:666-669, 2009.
10. M. Naseri. Comment on a weak blind signature based on quantum cryptography. *Int. J. Phys. Sci.*, 6(21):5051-5053, 2011.
11. Q. Su, Z. Huang, Q. Wen and W. Li. Quantum blind signature based on two-state vector formalism. *Opt. Commun.*, 283:4408-4410, 2010.
12. S. Khodambashi and A. Zakerolhosseini. A sessional blind signature based on quantum cryptography. *Quantum Information Processing*, 13(1):121-130, 2014.
13. R. Renner and U. Maurer. Security of Quantum Key Distribution. Dissertation submitted to *swiss federal institute of technology*, Zurich, 2005.
14. D.R. Stinson. Universal hashing and authentication codes. In *advances in Cryptology-CRYPTO'91*, LNCS, Springer, 576:74-85, 1991.
15. P. Gemmell and N. Naor. Codes for interactive authentication. In *Advances in Cryptology-CRYPTO '93*, LNCS, 773, pp. 355-367, Springer, 1993.
16. R. Renner and S. Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In *Advances in Cryptology-CRYPTO'03*, LNCS, Springer, pp. 78-95, 2003.
17. R. Renner and S. Wolf. The exact price for unconditionally secure asymmetric cryptography. In *Advances in Cryptology-EUROCRYPT'04*, LNCS, Springer, pp. 109-125, 2004.
18. C.E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656-715, 1949.

19. U.M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733-742, 1993.
20. C.H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179, 1984.
21. S. Wiesner. Conjugate coding. *Sigact News*, 15(1):78-88, 1983.
22. D. Bruss. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett. 81*, pp. 3018, 1998.
23. H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A 59*, pp.4238, 1999.
24. V. Scarani, A. Acin, G. Ribordy and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, 2004.
25. C.H. Bennett. Quantum cryptography using any two non-orthogonal states. *Phys. Rev. Lett.*, 68(21):3121-3124, 1992.
26. W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802-803, 1982.
27. V. Teja, P. Banerjee, N.N. Sharma and R.K. Mittal. Quantum cryptography: state-of-art, challenges and future perspectives. In *IEEE Int. Conf. on Nanotechnology*, pp. 1296-1301, 2007.
28. T. Schmitt-Manderbach. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504-1, 2007.
29. D. Stucki. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, pp. 075003-11, 2009.