Journal of Computing and Security

July 2014, Volume 1, Number 3 (pp. 179–186)

http://www.jcomsec.org

A Weak Blind Signature Based on Quantum Key Distribution

Siavash Khodambashi [a,*]
Ali Zakerolhosseini [a]

[a] *Electrical and Computer Engineering Department, Shahid Beheshti University; G.C., Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 3 July 2014
Revised: 1 December 2014
Accepted: 17 February 2015
Published Online: 28 February 2015

Keywords:
Quantum Weak Blind Signature, Quantum Key Distribution, Quantum Cryptography, Quantum Payment

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 weak 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 weak blind signature achieves a good position 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.

1 Introduction

A considerable issue in cryptography is to authenticate a message the same way as a handwritten signature on a paper document would certify the originality of the document. 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.

A fundamentally new kind of signature was introduced by Chaum in 1983 which provided an automated payment system with some properties that were not existed with the previous digital signatures including the inability of third parties to determine payee, the ability of individuals to provide the proof of payment and the ability to stop use of the stolen payments [1]. Blind signature is a form of digital signature in which the content of a message is disguised prior to getting 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 the originality of the message the same way as a regular digital signature. Blind signatures are typically employed in protocols where the signer and the message author are different parties and the anonymity of the message owner is important, such as 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, whose content is not seen by Bob.

Originally, the blind signature concept was proposed by Chaum based on the complexity of factoring

* Corresponding author.

Email addresses: siavashyp@yahoo.com (S. Khodambashi), a-zaker@sbu.ac.ir (A. Zakerolhosseini)

ISSN: 2322-4460 © 2014 JComSec. All rights reserved.

large integers. Recently, some other blind signatures based on elliptic curves have also been proposed in [2] and [3]. In fact, all of the classical blind signatures are based on the computational complexities and their security is guaranteed mathematically and by considering the limited computational power of classical computers. Hence, they are safe with the classical processors. But 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 in 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 achieve 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 weak blind signature and so the verifier would not be able to authenticate the message half of the times as criticized by Naseri [10] and Su et. al. [11]. Hence, Wen's scheme does not adequately complete the task of blind signature. Subsequently, Su proposed a quantum blind signature based on the two-state vector formalism to overcome the deficiency of Wen's signature. Their protocol seemed practical because the signatory and the message owner have to perform only measurement operations to complete the signature's process [11]. Nevertheless, Yang et. al. pointed out that a dishonest signatory in Su's scheme can reveal both the message owner's secret key and the message without being detected using Trojan horse attack or the fake photon attack [12]. A modified scheme was then proposed by Yang et. al. to avoid these kinds of attacks [12]. But Yang's protocol also had a loophole that Alice could utilize an entanglement swapping attack to obtain Bob's secret key and forge Bob's valid signature at will [13]. Later, a sessional blind signature based on quantum entangled states was proposed by Khodambashi and Zakerolhosseini in 2014 [14]. Their proposed scheme is reliable and secure against quantum attacks including Trojan horse attacks and so on. It also fulfills the ideal blind signature requirements, e.g., blindness, non-disavowal and no-counterfeiting. All mentioned schemes employ 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 [15], therefore our proposed scheme is unconditionally secure and efficient. Furthermore, QKD has been commercialized in recent years by several corporations around the world [16, 17]. Hence, it is possible to easily realize our proposed quantum weak blind signature.

The rest of the paper is organized as follows: in Section 2, blind signature types and their properties are addressed. Section 3 reviews QKD protocol in brief. The proposed quantum blind signature scheme is presented in Section 4. In Section 5, the security of the proposed quantum blind signature is analyzed. At last, Section 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 Figure 1. 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.

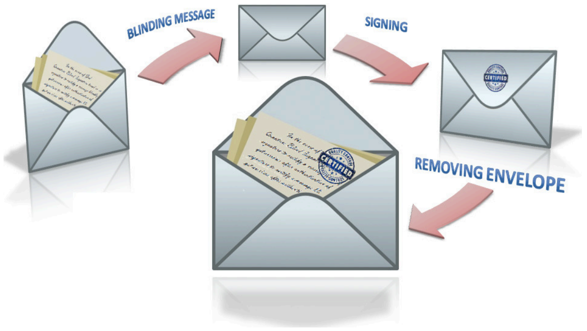

Figure 1. Classic blind signature process

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. So it does not matter whether a blind signature remains anonymous later, when it is presented to the signatory since he 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:

(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 should not be 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 [18, 19] 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 [20, 21].

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 to 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 are only connected by a classical authentic communication channel [22, 23]. The story changes dramatically with the help of quantum mechanics.

Bennett and Brassard[24, 25] 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 that 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 about the generated key is negligible[15].

Before we go to explain QKD protocol, it is better to give some introductory information about quantum mathematics. The basic unit of information in quantum physics is called qubit. Like a bit, a qubit can also be in one of two states, we call $|0\rangle$ and $|1\rangle$. In quantum theory an object enclosed by the notation $|\ \rangle$ can be called a *state*, *vector* or a *ket*. In contrast to a bit, a qubit can also exist in a superposition state *i.e.* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Here, α and β are complex numbers. While a qubit can exist in a superposition, whenever we make a measurement on a qubit, it is only going to be found in the state $|0\rangle$ or the state $|1\rangle$.

Consider a quantum system with quantum states lying in a two dimensional Hilbert space H. For this space, there are many orthonormal bases. We only use two for our proposed qucheck protocol, the rectilinear basis $\{|0\rangle, |1\rangle\}$ and the diagonal basis $|\pm\rangle$. Hence, there are four quantum states with these two bases $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. The bases are maximally conjugate in the sense that any pair of vectors, one from each basis, has the same overlap, e.g. $\|\langle 0|-\rangle\|^2 = \frac{1}{2}$. Conventionally, one attributes the binary value '0' to states $|0\rangle$ and $|+\rangle$ and the value '1' to the other two states, *i.e.*, $|1\rangle$ and $|-\rangle$, and calls the states qubits.

Assume that the system is in the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. We make a measurement in the rectilinear basis $\{|0\rangle, |1\rangle\}$, and the original state of the system is lost. Suppose we obtain measurement result $|0\rangle$. Then in the $|\pm\rangle$ basis, the state is now different than it was originally since $|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt{2}}$ and there is only a 50% chance of finding $|+\rangle$ if we measure in the $|\pm\rangle$ basis. Hence, the state has been irreversibly altered. This example illustrates a fact in quantum physics that taking a measurement with incompatible basis would unavoidably perturb the system and yield incomplete information about the state of the system before the measurement.

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. This property of quantum mechanics makes quantum cryptography advantageous over classical cryptography which gets help 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 a 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 any bit 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 string. 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 [26, 27]. Others are designed to cope with high channel noise or noise in the detector, which lends themselves to practical implementations [28]. The structure of these protocols is mostly very similar to the BB84 protocol e.g. [26, 27, 29].

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 the form of an n-bit binary message M. Due to the privacy reasons, she does not like her message content to 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 the blind message $M^{'}$ into the 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 is illustrated in Figure 2. The main goal of our proposed protocol is similar to the ones in [9, 11, 12, 14], *i.e.* presenting a quantum weak blind signature. Nevertheless, the weak blind signature proposed here only takes advantage of QKD which makes it easier for implementation. We suggest the use of modified QKD protocol in [15].

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 [30], 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 [15]. From this statement, it can be inferred that Eve is not capable of gaining proper information of the transferred qubits, so she can neither 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 [31].

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

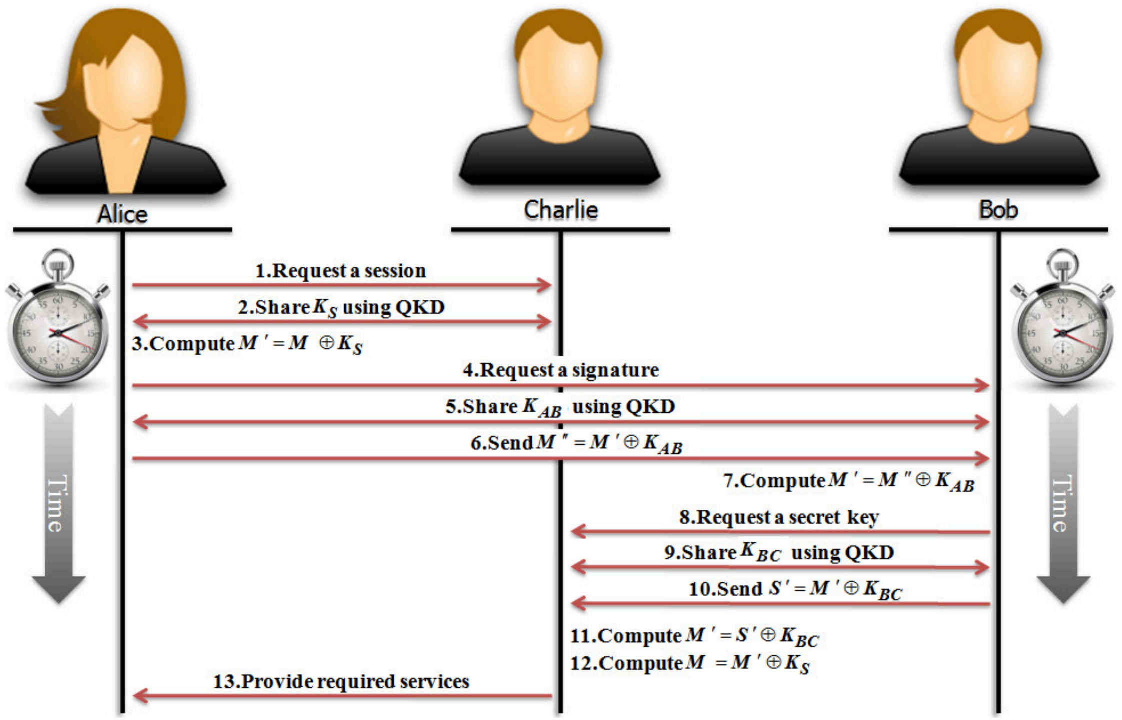
Alice
Charlie
Bob
1.Request a session
2.Share K_S using QKD
3.Compute $M' = M \oplus K_S$
4.Request a signature
5.Share K_{AB} using QKD
6.Send $M'' = M' \oplus K_{AB}$
7.Compute $M' = M'' \oplus K_{AB}$
8.Request a secret key
9.Share K_{BC} using QKD
10.Send $S' = M' \oplus K_{BC}$
11.Compute $M' = S' \oplus K_{BC}$
12.Compute $M = M' \oplus K_S$
13.Provide required services
Time
Time

Figure 2. The proposed quantum blind signature protocol

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

QKD protocol and XOR binary operator are only used throughout our proposed quantum weak blind signature. Hence, There is a bit-to-bit correspondence between the blind message and the blind signature in the scheme which can be verified precisely meaning that the verifier Charlie can testify the signature bit by bit in order to confirm the integrity of both message and the blind signature. Hence it is useful for electronic payment or access control systems. In other words, our proposed quantum blind signature is reliable.

5.6 Comparison

In Wen's quantum weak blind signature [9], Charlie can decisively confirm 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 in which high reliability is required. This criticism has also been applied by Naseri in [10].

Su's quantum weak blind signature also has some failures which have been reported in [12]. A dishonest signer in Su's scheme can use Trojan horse or the fake photon attacks to reveal the blind signature requester's secret key and message without being detected. Yang tried to modify Su's quantum blind signature to avoid these kind of attacks [12]. Although the modified scheme can prevent the signatory from deriving Alice's message, however Alice can utilize an entanglement swapping attack to obtain the Bob's secret key and forge Bob's valid signature [13].

Despite the schemes in [9, 11, 12, 14] which use EPR entangled pairs, our proposed approach uses only QKD and one-time pad protocols together to provide an unconditional secure quantum weak blind signature which is simpler to be implemented. Different types of QKD protocols, as the quantum part of our proposed scheme for generation of fully random shared keys, have been suggested and the security of some of them have been verified in [15]. Hence, our proposed quantum weak blind signature is secure against quantum attacks. Moreover, there is a bit-to-bit correspondence between the blind message and the blind signature in the scheme due to one-time pad protocol. Hence, it can be derived that the proposed protocol is highly reliable and lends itself to many sensitive applications.

6 Conclusion

In this paper, we introduced a novel weak 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 [16, 17, 32, 33]. 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 the owner of the message when a disagreement happens. This is useful in some applications including e-payment to prevent yeggmen and launderers.

References

[1] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[2] Morteza Nikooghadam and Ali Zakerolhosseini. An efficient blind signature scheme based on the elliptic curve discrete logarithm problem. *ISeCure*, 1(2), 2009.

[3] Morteza Nikooghadam, Ali Zakerolhosseini, and Mohsen Ebrahimi Moghaddam. Efficient utilization of elliptic curve cryptosystem for hierarchical access control. *Journal of Systems and Software*, 83(10):1917–1929, 2010.

[4] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[5] Charles H Bennett and David P DiVincenzo. Quantum information and computation. *Nature*, 404(6775):247–255, 2000.

[6] A Galindo and Miguel Angelo Martin-Delgado. Information and computation: Classical and quantum aspects. *Reviews of Modern Physics*, 74 (2):347, 2002.

[7] Guihua Zeng, Wenping Ma, Xinmei Wang, and Hong-wen Zhu. Signature scheme based on quantum cryptography. *Acta Electronica Sinica*, 29 (8):1098–1100, 2001.

[8] Daniel Gottesman and Isaac Chuang. Quantum digital signatures. *arXiv preprint quant-ph/0105032*, 2001.

[9] Xiaojun Wen, Xiamu Niu, Liping Ji, and Yuan Tian. A weak blind signature scheme based on quantum cryptography. *Optics Communications*, 282(4):666–669, 2009.

[10] Mosayeb Naseri. A weak blind signature based on quantum cryptography. *International Journal of Physical Sciences*, 6(21):5051–5053, 2011.

[11] Su Qi, Huang Zheng, Wen Qiaoyan, and Li Wenmin. Quantum blind signature based on two-state vector formalism. *Optics Communications*, 283 (21):4408–4410, 2010.

[12] Chun-Wei Yang, Tzonelih Hwang, and Yi-Ping Luo. Enhancement on "quantum blind signature based on two-state vector formalism". *Quantum Information Processing*, 12(1):109–117, 2013. ISSN 1570-0755. doi: 10.1007/s11128-012-0362-2. URL http://dx.doi.org/10.1007/s11128-012-0362-2.

[13] Qi Su and Wen-Min Li. Cryptanalysis of enhancement on "quantum blind signature based on two-state vector formalism". *Quantum Information Processing*, 13(5):1245–1254, 2014. ISSN 1570-0755. doi: 10.1007/s11128-013-0722-6. URL http://dx.doi.org/10.1007/s11128-013-0722-6.

[14] Siavash Khodambashi and Ali Zakerolhosseini. A sessional blind signature based on quantum cryptography. *Quantum information processing*, 13(1):121–130, 2014.

[15] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, PhD Thesis, 2005, 2005.

[16] *www.idquantique.com*, Sep. 2014. URL www.idquantique.com.

[17] *www.magiqtech.com*, Sep. 2014. URL www.magiqtech.com.

[18] Douglas R. Stinson. Universal hashing and authentication codes. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 74–85. Springer, 1991. doi: 10.1007/3-540-46766-1_5. URL http://dx.doi.org/10.1007/3-540-46766-1_5.

[19] Peter Gemmell and Moni Naor. Codes for interactive authentication. In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO '93,*

13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings, volume 773 of *Lecture Notes in Computer Science*, pages 355–367. Springer, 1993. doi: 10.1007/3-540-48329-2_30. URL http://dx.doi.org/10.1007/3-540-48329-2_30.

[20] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In *Advances in Cryptology-CRYPTO 2003*, pages 78–95. Springer, 2003.

[21] Renato Renner and Stefan Wolf. The exact price for unconditionally secure asymmetric cryptography. In *Advances in Cryptology-EUROCRYPT 2004*, pages 109–125. Springer, 2004.

[22] Claude E Shannon. Communication theory of secrecy systems*. *Bell system technical journal*, 28(4):656–715, 1949.

[23] Ueli M Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[24] C.H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Computers, Systems and Signal Processing, 1984. IEEE Conference on*, page 8. IEEE, 1984.

[25] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[26] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.

[27] Helle Bechmann-Pasquinucci and Nicolas Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238, 1999.

[28] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

[29] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[30] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 1982.

[31] Vishnu Teja, Payel Banerjee, NN Sharma, and RK Mittal. Quantum cryptography: state-of-art, challenges and future perspectives. In *Nanotechnology, 2007. IEEE-NANO 2007. 7th IEEE Conference on*, pages 1296–1301. IEEE, 2007.

[32] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[33] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S Gray, CR Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003, 2009.

Siavash Khodambashi received the BSc degree from university of Isfahan, Iran, in 2008, MSc from the Shahid Beheshti University, Iran, in 2010, and currently he is a PhD student in computer architecture in the department of Electrical and Computer Engineering at Shahid Beheshti University, Iran. His research focuses on quantum cryptography under Supervisory of Dr. Ali Zakerolhosseini. His current research interests are quantum computing, Cryptography and Network Security.

Ali Zakerolhosseini received the BSc degree from university of Coventry, UK, in 1985, MSc from the Bradford University, UK, in 1987, and PhD degree in Fast transforms from the University of Kent, UK, in 1998. He is currently been an assistant professor in the department of Electrical and Computer Engineering at Shahid Beheshti University, Iran. His research focuses on Reconfigurable device and multi classifiers. His current research interests are Data Security, Cryptography and Reconfigurable computing.