International Journal of the Physical Sciences Vol. 6(21), pp. 5051-5053, 30 September, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.1111
ISSN 1992 - 1950 ©2011 Academic Journals

Short Communication

A weak blind signature based on quantum cryptography

Mosayeb Naseri

Islamic Azad University, Kermanshah Branch, Kermanshah, Iran. E-mail: m.naseri@iauksh.ac.ir.
PACS: 03.67.Hk, 03.65.Ud

Accepted 6 September, 2011

In general, a weak blind signature has the characteristics of no-counterfeiting, no-disavowing, blindness and traceability. In this paper, a weak blind signature scheme based on the correlation of Einstein-Padolsky-Rosen (EPR) pairs (Xiaojun et al., 2009) is revisited, and it will be shown that the scheme in its original form does not complete the task of a blind signature fairly.

Key words: Quantum cryptography, blind signature, weak blind signature.

INTRODUCTION

Cryptography digital signature, which offers authenticity, integrity of messages and forestalls disavowal of transmitted messages, plays an important role in cryptography. But in some specific applications, e.g. in e-voting and e-cash systems, the required signature scheme should protect the privacy of message owners. Such demand on digital signature gives birth to the concept of blind signature scheme. In an e-voting system, a ballot (message) needs to be signed by the manager in order to take effect, but the content of the message could never be revealed to the manager or anyone else. Blind signature schemes provide a type of solution that the manager signs the message blindly and the voter then converts it to the signature of the original message for anyone who would probably verify it. The manager signs the message in such a way that he can neither know the content of the message nor recollect the message and corresponding signature he has signed. The concept of blind signature scheme was first introduced (Chaum, 1983).

Blind signature is a special digital signature in which the message owner's anonymity could be protected to ensure privacy. In blind signature, the message owner could always get the authentic signature of his own message even though the signatory knows nothing about the content that was signed.

As such, the blind signature is essential in the applications of e-voting and digital cash. In an e-voting system, the votes need to be signed by the manager to be effective, but the content of the votes cannot be known by anyone including the manager. In an e-payment system, the bank should sign the digital cash but protect the anonymity of the digital cash holders in each transaction. The aforementioned systems both depend on the blind signature technology. Blind signature could be classified into weak blind signature and strong blind signature according to whether or not the signatory can trace the message owner. In an e-payment system, the bank could use the weak blind signature scheme to trace the illegal customers (e.g. yeggmen and launderers). On the other hand, in an e-voting system, in order to guarantee that the voters cannot be traced by the manager, the strong blind signature scheme should be used.

A weak blind signature scheme based on the correlation of Einstein-Padolsky-Rosen (EPR) pairs has been proposed by Xiaojun et al. (2009), where quantum key distribution and one-time pad were used to guarantee the unconditional security and signature anonymity. In this paper it has been shown that the original weak blind signature scheme based on the correlation of EPR does complete the task of a blind signature fairly. Let us start with the brief description of an original protocol for weak blind signature based on quantum cryptography.

EXPERIMENTAL

The original weak blind signature scheme based on quantum cryptography is separated in four phases, such as the initial phase, blind the message phase, sign the blind message phase and verification phase.

In the first phase, which is the initial phase, Alice shares secret key K_{AC} with Charlie, while Bob shares secret key K_{BC} with Charlie using quantum key distribution (QKD) protocols (Xiaojun et al., 2009; Hughes et al., 2000). Afterwards, according to Alice's n-bit

sequence $M = \{m(1), m(2),..., m(n))\}$.Bob generates n EPR pairs such that $\psi_i = \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{a_i b_i}$, where a_i, b_i denote the i-th two entangled particles and i = 1, 2,…, n. In each EPR pair, Bob sends a_i particle to Alice while leaving particle b_i with himself. In the second phase, that is, blind the message phase, according to message m(i) = 0 or m(i) = 1, Alice measures her particle sequence a_i with the base $B_Z = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $B_X = |+\rangle\langle +| + |-\rangle\langle -|$, respectively. Then Alice converts the measuring results $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ into two classical bits 00, 01, 10 and 11, respectively and records the results as $m' = \{m'(1), m'(2),..., m'(n))\}$. Thus, m' comprises 2n-bit classical information, and the message m(n-bit) has been blinded into m' (2n-bit). Then Alice encrypts m' with the key K_{AC} to get the secret message M, which is defined as $M = E_{K_{AC}}\{m'(1), m'(2),..., m'(n))\}$. Since both m' and K_{AC} are 2n-bit, the one-time pad is adopted to guarantee the unconditional security. Afterwards, Alice sends the secret message M to the verifier Charlie.

In the sign the blind message phase, Bob measures his particle sequence according to the odd bits of his key K_{BC}. If $K^{2i-1}{}_{BC} = 0$, he measures b_i with the base $B_Z = |0\rangle\langle 0| + |1\rangle\langle 1|$; If $K^{2i-1}{}_{BC} = 1$, he measures b_i with the base $B_X = |+\rangle\langle +| + |-\rangle\langle -|$. Then he converts the measuring results $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ into two classical bits 00, 01, 10 and 11, respectively and records the results as $s' = \{s'(1), s'(2),..., s'(n))\}$. Afterwards, Bob encrypts s' with the key K_{BC} to get the secret message S, which is defined as $s = E_{K_{BC}}\{s'(1), s'(2),..., s'(n))\}$, where one-time pad is used to guarantee the unconditional security. Then, Bob sends the blind signature S to the verifier Charlie.

Finally, in the last phase, the verification phase, Charlie will be able to recover the blind message m', the original message m and the secret message S by using the keys K_{AC} and K_{BC} and applying inverse operation of aforementioned rule. At last, Charlie will accept S as the valid blind signature for message m if parameters m, m', s' and K_{BC} satisfy the following conditions:

1. If $m(i) = K^{2i-1}{}_{BC}$, then $m'(i) = s'(i)$,

2. If $m(i) \neq K^{2i-1}{}_{BC}$, then $m'(i) = s'(i)$ or $m'(i) \neq s'(i)$.

Otherwise, he rejects it.

RESULTS AND DISCUSSION

The crucial issue of quantum communication protocol is its security. Here, we will show that a weak blind signature scheme based on quantum cryptography protocol in it is original form does not complete the task of a weak blind signature fairly.

By closer inspection of the aforementioned protocol, one can see that the protocol has not proposed any security checking procedure; it has only considered that the two mentioned conditions meets the security requirements. Here, it will be shown that the conditions cannot preserve the security of the scheme perfectly. Regardless of the proposed protocol, there are some logical misunderstandings in the conditions.

With a closer look at the conditions, one can easily see that the probability of both conditions $m(i) = K^{2i-1}{}_{BC}$ or $m(i) \neq K^{2i-1}{}_{BC}$ 50%, but it is clear that $m'(i)$ either equals $s'(i)$ or is not equal to $s'(i)$.

In other words, when $m(i) \neq K^{2i-1}{}_{BC}$, that is, in half of the situations (the second condition), the security of the scheme cannot be guaranteed. To put it simply, here, the protocol contains 50% insecurity.

Let's analyze the first condition now. In half of the situations when $m(i) = K^{2i-1}{}_{BC}$, without considering the scheme, the probability of $m'(i) = s'(i),$ is $\frac{1}{2}$.

To put it in another way, here, the scheme contains $\frac{1}{2}(50\%) = 25\%$ of insecurity. Since in a perfect condition only half of the bits, the bits which satisfy the condition $m(i) = K^{2i-1}{}_{BC}$ are useful for insuring the validity of the signature and Charlie know nothing if $m(i) \neq K^{2i-1}{}_{BC}$ (Rui et al., 2011), the scheme overlay contains $50\% + 25\% = 75\%$ insecurity. However, but it is proper to notice the probability of 75% that one can forge a signature only occurs in the sense of a single bit. When taking an n-bit message in application, the probability of successfully forging a signature reduces to $(75\%)^n$, this is an exponentially decreasing probability. So the scheme turns to be insecure when the message is not so long.

In general, a good quantum blind signature should satisfy three properties: no-counterfeiting, no-disavowing and blindness. Essentially, there are two possible types of attacks. Firstly, the eavesdropper (Eve) who is outside the network wants to change the content of the blind message. Secondly, an insider dishonest Bob wants to replace his bits with the blind message before the opening of the message by the Charlie. In fact, the eavesdropper can never be more powerful than an insider dishonest Bob with

access to all transmitted bits. Eavesdroppers are usually considered only in case where the participants are fully trusted, so, to insure the honesty of the insider parties is more important than to check the eavesdropping.

Conclusion

Conclusively, since the protocol does not propose any security checking procedure, Alice may be malicious in the scheme, so, according to her message, she may try to forge Bob's signature. Although, she does not know the secret key K_{BC}, she may replace Bob's bits with her faked ones while she employs her strategy to manage the fake bits to achieve her own proper benefits. Since Alice could be a possible forger, she can intercept Bob's bits, forge them and send the replaced ones as original bits. As stated, the probability of her success is 75% in each run of single bit transmitting, 50% of the probability materializes when $m(i) \neq K^{2i-1}{}_{BC}$ and 25% when $m(i) = K^{2i-1}{}_{BC}$ (when she is lucky enough to $m'(i) = s'(i)$). When taking an n-bit message in application, the probability of successfully forging a signature reduces to $(75\%)^n$, this is an exponentially decreasing probability. So the scheme turns to be insecure when the message is not so long.

ACKNOWLEDGEMENTS

The author would like to thank Alimorad Ahmadi for his helpful comments with English and also Soheila Gholipour and Yasna Naseri for their interest in this work. This work is supported by Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.

REFERENCES

Chaum D (1983). Blind signatures for untraceable payments, Proc CRYPTO82 199.

Xiaojun Wen et al Niu X, Ji L, Tian Y (2009). A weak blind signature scheme based on quantum cryptography, Opt. Commun., pp. 282-666.

Hughes R, Morgan G, Peterson C (2000), Practical quantum key distribution over a 48 km optical fiber network, J. Modern Opt., 47 (23): 533.

Rui X, Huang L, Yang W, Hi L (2011). Quantum group blind signature scheme without entanglement. Opt. Commun. pp. 284- 3654.