World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:1, No:2, 2007

Unconditionally Secure Quantum Payment System

Essam Al-Daoud

***Abstract*—**A potentially serious problem with current payment systems is that their underlying hard problems from number theory may be solved by either a quantum computer or unanticipated future advances in algorithms and hardware. A new quantum payment system is proposed in this paper. The suggested system makes use of fundamental principles of quantum mechanics to ensure the unconditional security without prior arrangements between customers and vendors. More specifically, the new system uses Greenberger-Home-Zeilinger (GHZ) states and Quantum Key Distribution to authenticate the vendors and guarantee the transaction integrity.

***Keywords*—**Bell state, GHZ state, Quantum key distribution, Quantum payment system.

I. Introduction

QUANTUM cryptography is based on laws of quantum physics and has been proposed as a solution to the classical cryptography problems. More precisely, it is based on the fact that an eavesdropper, trying to intercept the quantum communication, will inevitably leave traces which can thus be detected. Many advances have been made in quantum cryptography in recent years, including quantum key distribution QKD[1] quantum teleportation[2], quantum authentication[3] and quantum digital signature[4]. Moreover, several groups have shown that quantum cryptography is possible, even outside the laboratory. For example a team from BBN Technologies, Boston University, and Harvard University has recently built and begun to operate the quantum key distribution network under DARPA sponsorship. The DARPA quantum network is the world's first quantum cryptography network, and perhaps also the first QKD systems providing continuous operation across a metropolitan area. Many quantum key distribution products are already commercially available such as ID Quantique and MagiQ[5], [6], [7].

In this paper, a novel quantum payment system is proposed, which is based on the correlation of the GHZ triplet states and utilization of quantum one time pad and quantum key distribution. The new system offers unconditional security without prior arrangements between customers and vendors, guarantees the transaction integrity, authenticates the customers, and authenticates the vendors. The paper is arranged as below.

E. Al-Daoud is with Faculty of Science and Information Technology, Computer Science Department, Zarka Private University, Jordan (e-mail:essamdz@zpu.edu.jo).

Section 2 introduces the most robust quantum key distribution version namely SARG04. Section 3 discusses error correction and privacy amplification. Section 4 describes the new quantum payment system and its security.

II. SARG04 Protocol

The most well-known quantum key distribution protocols are Bennett-Brassard-84 (BB84), Bennett-92 (B92) protocols and (SARG04) protocol. SARG04 is a modification of the BB84 protocol that makes quantum key distribution robust against photon-number-splitting attacks [8], [9]. SARG04 protocol uses exactly the same four states as the one in BB84, These quantum qubits are equally likely to be in one of four possible states:

$$|\psi_1\rangle = |0\rangle$$
$$|\psi_2\rangle = |1\rangle$$
$$|\psi_3\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|\psi_4\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

The difference with BB84 appears in the encoding and decoding of classical information. In this protocol Alice announces publicly one of the four sets of states $\{|\psi_1\rangle, |\psi_3\rangle\}$, $\{|\psi_2\rangle, |\psi_3\rangle\}$, $\{|\psi_1\rangle, |\psi_4\rangle\}$ *or* $\{|\psi_2\rangle, |\psi_4\rangle\}$. The SARG04 protocol goes as follows:

1- Alice randomly prepares m qubits, each in one of the four states $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ or $|\psi_4\rangle$ and sends them to Bob over a quantum channel.
2- For each qubit that Bob receives, he chooses at random one of the two bases: $\{+, \times\}$.
3- For each qubit sent, Alice announces publicly one of the four sets $\{|\psi_1\rangle, |\psi_3\rangle\}$, $\{|\psi_2\rangle, |\psi_3\rangle\}$, $\{|\psi_1\rangle, |\psi_4\rangle\}$ or $\{|\psi_2\rangle, |\psi_4\rangle\}$, that contains the state of the photon sent out by her.
4- Bob tells Alice to discard the times when the output of the measurement is confusing (see the example below).
5- Alice and Bob then test the security of their key by using a randomly chosen subset of their key. Results of their subset are compared and if errors are detected, the transmission is insecure and they abort and start again.
6- Classical error correction and privacy amplification techniques are used to generate a secure key.
7- The one time pad is used to encrypt a message.

TABLE I
AN EXAMPLE OF SARG04 PROTOCOL FROM ALICE TO BOB

The Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice's Random Bits	0	0	0	1	0	1	1	1	0	1	0	1	1	0	1
Alice's States	ψ_1	ψ_1	ψ_1	ψ_4	ψ_3	ψ_4	ψ_2	ψ_2	ψ_3	ψ_4	ψ_1	ψ_2	ψ_4	ψ_3	ψ_2
Bob's Random Basis	×	×	+	×	×	+	+	×	×	×	+	×	+	+	+
Bob's Result	0	1	0	1	0	1	1	1	0	1	0	1	1	1	1
Announcement	ψ_1	ψ_1	ψ_1	ψ_1	ψ_2	ψ_2	ψ_2	ψ_2	ψ_1	ψ_1	ψ_1	ψ_2	ψ_2	ψ_2	ψ_2
States	ψ_4	ψ_4	ψ_3	ψ_4	ψ_3	ψ_4	ψ_3	ψ_4	ψ_3	ψ_4	ψ_3	ψ_3	ψ_4	ψ_3	ψ_3
Discovered States		ψ_1				ψ_4						ψ_2	ψ_4	ψ_3	
The sifted Key		0				1						1	1	0	

In the first column of Table I, Bob cannot determine the sent state because the state ψ_4 measured in the basis × must be 0 and the state ψ_1 measured in the basis × could be 0, thus Bob cannot determine the sent state whether ψ_1 or ψ_4. However, in the second column of Table II, Bob knows for sure that the sent state cannot be ψ_4, which always gives a measurement 0 if measured in the basis ×.

III. ERROR CORRECTION AND PRIVACY AMPLIFICATION

In perfect conditions Alice and Bob generate and share identical random keys, but because errors and background noise can not be avoided, Alice and Bob can never guarantee that eavesdropper (Eve) has no information at all about their keys, for example, if Eve applies Intercept-resend attack on all the qubits, she gets 50% information, while Alice and Bob have about 25% of error in their sifted key. They can easily detect the presence of Eve. If, however, Eve applies this strategy to only a fraction of the communication, 20% let's say, then the error rate will be only 5% and Eve information would be about 10%. This error rate and the communication noise cannot be distinguished (experimental studies indicate that the error rate generated by the noise and the devices imperfection is less than 10% see[10], [11]) , and so to be on the safe side Alice and Bob have to assume that all errors are due to Eve. If the error rate is more than an agreed threshold, 10% let's say, then they must regenerate the key, but if the error rate is less than an greed threshold, They can perform error correction to remove the disagreement in their keys and privacy amplification to decrease the amount of information held by Eve.

Brassard and Salvail have suggested an efficient error correction method, which is close to the optimum [12]. This method is called CASCADE. Although CASCADE requires a lot of interaction thus slowing down the rate at which secret key generation can be achieved, it allows to save more bits of key after privacy amplification. On the other hand, if for some settings the rate at which the secret key is generated is the main concern, using a less interactive version of CASCADE might be preferable. The fully interactive version of CASCADE can be briefly summarized as follows: Alice and Bob must reveal as little information as possible while still ensuring that they end up with identical keys. They can do this by agreeing upon a random permutation of the bits in their strings, and then splitting the resulting string into blocks of size b. The constant b is chosen so that each block is unlikely to contain more than one error, b was chosen by experiment rather than theory. Alice and Bob then compare the parity of each block (The parity is defined as the sum of all bits in that block modulo 2). If they find a pair of blocks with mismatched parities, they continually bisect the block into smaller and smaller blocks, comparing parities each time, until the error is found. To ensure that Eve learns nothing from this process, Alice and Bob discard the last bit of each block whose parity they disclose.

At this point, Alice and Bob share an identical key, but this key is not completely private. Eve may have gained some information about the key either by beam splitting or through intercept resend attack. Therefore Alice and Bob must eliminate Eve's knowledge. They can do so by implementing the privacy amplification procedure. A simple privacy amplification version can be summarised as follows: Alice chooses a hash function $h:\{0,1\}^c \rightarrow \{0,1\}^f$, where $c = |K_{corrected}|$ and $f = |K_{final}|$. She broadcasts this hash function to Bob, both of them apply the hash function to their corrected key and end up with a private key which they can use to encrypt data and send it over the public channel[13].

IV. BELL AND GHZ STATES

Bell's theorem states that certain statistical correlations predicted by quantum physics for measurements on two-particle systems cannot be understood within a realistic picture based on local properties of each individual particle even if the two particles are separated by large distances. A Bell state is defined as a maximally entangled quantum state of two qubits. Bell states exhibit perfect correlations which cannot be explained without quantum mechanics. There are four maximally entangled two qubit states or Bell states[14], [15]:

$$|\Phi^+> = \frac{1}{\sqrt{2}}(|00> + |11>)$$

$$|\Phi^-> = \frac{1}{\sqrt{2}}(|00> - |11>)$$

$$|\Psi^+> = \frac{1}{\sqrt{2}}(|01> + |10>)$$

$$|\Psi^-> = \frac{1}{\sqrt{2}}(|01> - |10>)$$

Entanglement in three qubits is more complicated than that in two qubits. Recently, the entanglement of three qubits was classified into separable, biseparable, *W*, and Greenberger-Horne-Zeilinger (GHZ) states. The GHZ state is an entangled quantum state in an M dimensions:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes M} + |1\rangle^{\otimes M})$$

Most notably the 3-qubit GHZ state is:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

In this paper we will use two interesting properties can be applied on the 3-qubit GHZ state, the first: if we perform a CNot operation on the first two qubits, the state of the tripartite system becomes[16]:

$$\text{CNot}(|GHZ\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= |0\rangle \otimes |\Phi^{+}\rangle$$

The second property: if we perform a unitary operation

$$\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On the third qubit of the GHZ state and then, performing a CNot operation, the GHZ state becomes:

$$|\psi\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = = |0\rangle \otimes |\psi^{+}\rangle$$

V. Quantum Payment System

Electronic transaction needs the Quantum cryptography for many purposes such as protect the transactions against attack on the network, ensure the unconditional security without prior arrangements between customers and vendors, guarantee the transaction integrity, authenticate the customers, and authenticate the vendors. In this paper we assume that the customers, the vendors and the banks have quantum channels to provide general banking services, opening account, issuing checks, insurance etc.

The proposed quantum payment system relies on quantum cheque, the format of the proposed quantum cheque consists from two parts, the first part must be filled by the vendor and send to the customer with guarantee that this information is correct, the format of the vendor part is (v_1, v_2, v_3, v_4) where v_1 is the name of the payee, v_2 is the account number, v_3 is the amount of the money and v_4 is the date and time. For simplicity we will assume that the length of v_1, v_2, v_3 and v_4 are same, and the total length is n. While the second part must be filled and signed by the customer, the format of the customer part is (c_1, c_2, c_3, c_4) where c_1, c_2 and c_3 are identical to v_1, v_2 and v_3 respectively, but c_4 is the payer name. Quantum payment system goes as follows:

1- The customer and the bank share a secret key (k) by using quantum key distribution protocol such as SAGE04. The length of k is n.
2- The vendor and the bank share a secret key (t) by using quantum key distribution protocol such as SAGE04. The length of t is n.
3- The bank generates n GHZ states and sends the third qubit of each state to the vendor, we denote these qubits as π.
4- The vendor encrypts his part (n bits) as follows: $\beta=E_t(\alpha)$ where α is the vendor information, t is the vendor secret key and E is an unconditional secure encryption method such as one time pad (this method is secure if it is used one time).
5- The vendor encodes β (the result in step 4) as follows: if the bit is "1", then perform the quantum operation σ on the corresponding qubit that sent by the bank, if the bit is "0", do nothing on the corresponding qubit.
6- The vendor sends the encoded n qubits to the customer, we denote the encoding process as $f(\pi, \beta)= \lambda_1$, where β *is* the encrypted information and λ_1 is the encoded qubits.
7- The customer signs the cheque: First the customer encrypts his part by using one time pad and the secret key k, second the customer performs a hash function $h:\{0,1\}^n \rightarrow \{0,1\}^t$ on the encrypted cheque, where $t<n$. we denote the cheque without the signature as λ2, and the signature as λ3.
8- The customer sends λ_1, λ_2 and λ_3 to the bank.
9- The bank verify the customer's signature by using the shared secret key k and the hash function $h(x)$, the signature is correct if $h(E_k(\lambda_2))= \lambda_3$.
10- The bank decodes the vendor part as follows: the bank performs CNot operation on the first two qubits of each GHZ state has generated in step 2, and then it performs Bell measurement on the last two qubits of each state, if the measurement outcome is $|\Phi^{+}\rangle$ the bank writes down "0", and when it is $|\psi^{+}\rangle$, the bank writes down "1" (note that the third qubit of each state can be extract from λ_1).
11- The bank decrypt the result in step 10 by using the shared secret key t and one time pad, the result is the original vendor information α.
12- The bank accepts the transaction if $v_1=c_1$, $v_2=c_2$ and $v_3=c_3$. Else the bank rejects the transaction and sends notifications.

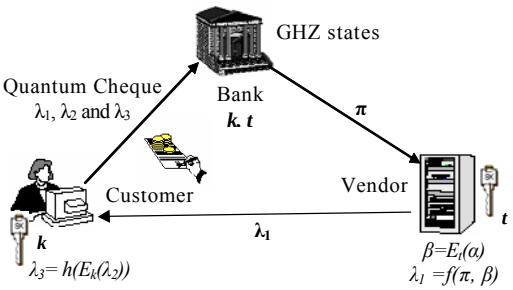

Fig. 1 The proposed quantum payment system

In the previous quantum payment system, a hacker cannot pretend as vendor, because the vendor has a unique secret key *t*, moreover, due to the sensitive natural of the quantum information, the hacker cannot measure or modify the set of qubits in $\pi \ or \ \lambda_1$ without detection. If a hacker try to modify the customer information λ_2 the transaction will be rejected because $h(E_k(\lambda_2)) \neq \lambda_3$. Another important character of the proposed system is that: an eavesdropper cannot gain information about the secret keys even if it used more than one time, because the vendor secret key *t* is encoded and the customer secret key *k* is hashed.

VI. Conclusion

The Quantum cryptography has many potential applications. It combines unconditional security with the flexibility of a public key system. In this paper, a new quantum payment system is proposed, which is based on the correlation of the GHZ triplet states, utilization of quantum one time pad and quantum key distribution. The new system offers unconditional security without prior arrangements between customers and vendors, guarantees the transaction integrity, authenticates the customers, and authenticates the vendors.

References

[1] P. Panthong, and et al, "Experimental Free Space Quantum Key Distribution" *The 4th International Conference on Optical Communication and Networks, Thailand*, 2005, pp.14-16.
[2] H. Feng, and et al, "Experimental Teleportation of a Quantum Controlled-NOT Gate," *arXiv:quant-ph/04080007 v1 2* Aug 2004.
[3] M. Curty, D. J. Santos, "Qubit authentication," *Physical Review A, 66, 022301*. 2002.
[4] L. H. Hong, and et al., "Arbitrated quantum signature scheme with message recovery*", Physics Letters A. 321*, 2004, pp.295-300.
[5] www.bbn.com/Solutions_and_Technologies/Information_Security/Quantum_Cryptography.html. last access on January 2007.
[6] www.idquantique.com. last access on January 2007.
[7] www.magiqtech.com. last access on January 2007.
[8] G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information*. World Scientific vol. I. Singapore, 2004.
[9] C. Branciard and el at, "Security of two quantum cryptography protocols using the same four qubit states," *arXiv:Quant-ph/0505035*, 2005.
[10] P. Panthong, and et al, "Experimental Free Space Quantum Key Distribution," *The 4th International Conference on Optical Communication and Networks, Thailand,* 2005, pp.14-16.
[11] C. Gobby, and et al. "Quantum key distribution over 122 km standard telecom fiber," *Appl. Phys. Lett., 84,* 2004, pp. 3762-3764.
[12] W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press. 2003.
[13] D. Deutsch, A. Ekert and R. Jozsa, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," *Phys. Rev.Lett., 77, 2818*. 1998.
[14] H. Weinfurter, "The power of entanglement," *Physics World 18*, 2005, pp. 47-51.
[15] W. Y. Chung, G. L. Khym, C. H. Hong and H. J. Yang, "Quantum Key Distribution Using GHZ States," *Journal of Institute of Science and Technology Korea University*, Vol. 11, 2003.
[16] X. J. Wen and Y. Liu, "Quantum Signature Protocol without the Trusted Third Party," *arXiv:Quant-ph/0509129*, 2006.