A Highly Secure Quantum Communication Scheme for Blind Signature using Qubits and Qutrits

Arafat Abu Malluh, Khaled M. Elleithy, Ramadhan J. Mstafa, Adwan Alanazi

***Abstract*—The advances in hardware speed has being rapidly increased rapidly in the recent years, which will lead to the ability to decrypt well known decryption algorithms in short time. This motivated many researchers to investigate better techniques to prevent disclosing and eavesdropping of communicated data. Quantum Cryptography is a promising solution, since it relies on the prosperities of quantum physics that ensure no change in the quantum state without the knowledge of the sender/receiver. Quantum Communication Scheme for Blind Signature with Two-Particle Entangled Quantum-Trits was proposed by Jinjing *et al.* [1] That scheme uses qutits during the communications and the process of the encryption is not clearly defined. In this paper we suggest a modification of Jinjing *et al.* protocol using qubits and qutrits during the encryption and decryption which proposed by Zhou *et al.* [2] The proposed algorithms enhances the efficiency of that scheme and creates a quantum cryptosystem environment to exchange the data in a secure way. During the communications, all the messages are encrypted using the the private key of the sender and a third party verifies the authenticity and the blindness of the signature.**

Keywords*— *Quantum communication; Blind signature; Quantum signature; Quantum cryptography

I. Introduction

The security of information, either local or being transmitted over the internet, is a main goal for individuals or organizations because it contains private or valuable data that could be used by intruders in a way that affect their life in different aspects. Cryptography is a field that is concerned on how to protect and secure the information from attackers and unauthorized users. In general, cryptography is divided into two parts; symmetric encryption and asymmetric encryption. For symmetric encryption, the same key is used for cipher and decipher by sender and receiver, which implies that this key must be kept secured. For asymmetric encryption, there are two different keys; private and public. Both techniques' strength is inversely related with the computational power. That means that encryption fails under brute force attack with sufficient powerful computers.

Quantum Cryptography was introduced in 1984 by Charles Bennett and Gilles Brassard [3]. The authors proposed a new algorithm (BB86) based on Quantum Communication Networks, where the transmission depends on photons. Quantum cryptography utilizes Heisenberg's Uncertainty principle which states that when a quantum state is measured, then it is disturbed and leads to incomplete information about the system. Eavesdropping on a quantum communication alerts legal users and this feature is the main advantage of quantum cryptography[4].

A digital signature is used to insure the authenticity and the validity of who sent the message and signed the transmitted document. It ensures that the original message has not been changed by someone who tries to break the security of the message [5].

The signature in classical cryptography has some characteristics including identifiability, undeniableness and unforgeability which provide a mechanism to decide who verifies that signature. David Chaum [6]introduced the idea of a blind signature as an electronic signature where the content of a message is blinded prior the process to sign it. Blind signature is involved in privacy-related protocols where the party that signs the message and party who writes it are different[7]. Several algorithms that use Quantum Cryptography were proposed in literature. They differ essentially in the choice of the parameters between the communicating parties such as the number of states that a quantum bit has, and the key process forming. In this paper we present an ideal environment of quantum communication scheme for blind signature with two-particle entangled quantum qubits and qutrits.

II. Related Work

Jinjing *et al.* [1] proposed a quantum communication scheme for blind signature with two-particle entangled quantum-trits (qutrit). The authors introduced a third fully trusted participant Trent (the arbitrator and proxy) which is responsible to help Alice and Bob trust each other before communication verify the legalization and authenticity of the blind signature and provide a batch of efficient proxy blind signatures to Alice. Their model utilizes public key principle with qutrit usage; transformation of a message to qutrits.

Manuscript received February 10, 2014. Manuscript revised February 27, 2014.

A. Abu Malluh is with the Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT 06604, USA (e-mail: aabumall@bridgeport.edu).

K. M. Elleithy is the Associate Dean for Graduate Studies in the School of Engineering at the University of Bridgeport. He is with the Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT 06604, USA (e-mail: elleithy @bridgeport.edu). He is IEEE senior member.

R. J. Mstafa was with the Computer Science Department, University of Zakho, Duhok, Iraq. Now he is with the Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT 06604, USA (e-mail: rmstafa@bridgeport.edu).

A. Alanazi is with the Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT 06604, USA (e-mail: aalanazi@bridgeport.edu).

In [2], the authors introduced a new algorithm to qubit with hybrid keys .The encryption and decryption operations uses a quantum key and classical key which are shared between Alice and Bob before starting the communication between the two parties. Alice and Bob are communicating through a classical channel which is also used to check the presence of Eve who is trying to attack the communication. The encryption and the decryption operations use the basic Hadamard gate and Controlled-NOT gates. To start the communication, Alice adds random bits to her message and encrypts it with quantum block encryption algorithm. Then, Bob decrypts the cipher text that was received from Alice. After that, Alice declares her check bits and their corresponding positions to Bob who is going to compare the received check bits with the bits that Alice already declared. If the bits are the same, they continue the communication. Otherwise, if the bits are different, which means someone attacked the channel, the shared keys are canceled and they must establish new keys to continue the communication in safe way.

In[8] a quantum signature in service-oriented vehicular networks was proposed. In the initial phase, the sender and the receiver share a quantum key and generate EPR pairs to construct a special correlation between each other. In the signature phase, the signatory produces the signature by using EPR pairs and sends it to Bob. In the verification phase, the receiver has the capability to identify the signature by using a quantum key and EPR pairs. Based on this relation, the receiver can reconstruct the original quantum states to verify whether the signature is derived from initial quantum entangled state or not. Also, two quantum unitary operations are used, I gate and X gate, to represent classical bits 0 and 1.

In[9], the authors proposed a quantum digital signature scheme based on quantum mechanics. The security in the protocol depends on the quantum one-way function that should be easy to compute and hard to invert. An arbitrator was introduced to authenticate and validate the signing message. Public quantum keys are used to ensure the validity of the signature and one time pad to verify the security of quantum information. There are three algorithms in a digital signature scheme, a key generation algorithm which randomly selects the private key, a signing algorithm and a verifying algorithm. The proposed scheme provides some security services such as security against repudiation since Alice cannot deny her signature because Bob will return to the arbitrator who has a copy of the signature. Also, the arbitrator tests if the signature has been forged or not by comparing that with its current information. Also, it provides Security against forgery. In this case any attempt to alter the signed quantum states or to recover Alice's private keys and generates a "legal" signature will be detected.

Wen and Liu [10], proposed a quantum message signature scheme without an arbitrator. This scheme has N-pairs M and $M^{'}$ of particles that are created by Alice to carry the quantum message. Bob creates N-pairs of particles A and B in EPR (Einstein-Podolsky-Rosen) states. Alice saves the particle M and transmits the particle $M^{'}$ to Bob. When Bob receives the particle $M^{'}$ he sends particle A to Alice and keeps particle B. Then the state with triplet particles A_i, B_i, and M_i is produced. For each triplet state, Bell-base measurement is implemented by Alice on both M_i and A_i and her result will be recorded as R_i. Each Bell state R_i represents two classical bits which Alice encrypted those states by using Vernam algorithm to make signature S. Bob decrypts the signature that was received from Alice through the classical channel. Unitary operations U_i have to be applied on Bob's particle B_i to extract the initial state M_i. Then Alice's signature S is accepted by Bob only when both B_i and $M^{'}_i$ states are equivalent. This kind of scheme has a private symmetric key for both sender and receiver without having to share it with the third party which means that the arbitrator is not needed in this system.

In [11], the authors discuss three problems of the scheme presented in [9]. First, the quantum one way function is not defined clearly. Second, the private key was not used for signing the message and third, there are some problems during the signing and the verification phases of the algorithm. While generating the key, the authors do not specify the quantum states. During the generation process, we know the signer's public key and its corresponding private key. If we combine the signing process we can see the signer Alice does not use her private key which is a significant security flaw.

III. Quantum Communication for Blind Signature

The classical blind signature algorithm contains three parties: Alice, Bob and the third Party Trend. Alice who is the sender is able to generate a signature for her message. Bob who is the receiver can identify if the signature is from Alice or not by the third party Trend whose main task is the authentication of the signed message[12]. The quantum communication scheme for blind signature is shown in Fig. 1 and works as follows:

(1) Alice sends a message that is encrypted by her private key to the receiver Bob.
(2) Bob adds his information to the received message which he encrypts by the key that is shared between him and Alice.
(3) Bob sends that message as well as his information to Alice which is considered as the blind signature.
(4) Alice receives the blind signature and decrypts it with the shared key with Bob and checks if the received message has not been changed.
(5) Now, the two parties Alice and Bob send a message to the third party Trend containing the result of the signature and Trend checks and validate the signature.
(6) If the result of the validation of the signature is positive, Alice sends a message to Trend.
(7) Trend checks those messages by applying Bob's personal information and Trend's random checking photons

A. Initialization of the Communication

We assume that the secret keys K_{ab}, K_{ac}, K_{bc} are distributed for Alice and Bob; K_{ab} is the secret key between Alice and Bob and can be used in two cases twice for Bob's encryption and Alice's decryption in the first communication. However, K_{ac} and K_{bc} are used for the communications

between Alice and the third party Trend and between Bob and Trend. Alice has her key K_a which can be used for encrypting the received message that Bob signed it before. Fig. 2 shows the relationship in the communications between Alice, Bob and Trend. Furthermore, Alice has amount of message that Bob should sign. We annotate the message as$\{M_1, M_2, \ldots, M_m\}$, where every message has n trits. $M_1 = [M_{i1}, M_{i2}, \ldots, M_{ij}, \ldots, M_{in}]$, where M_1 is selected initially as the first attempt for trying quantum blind signature.

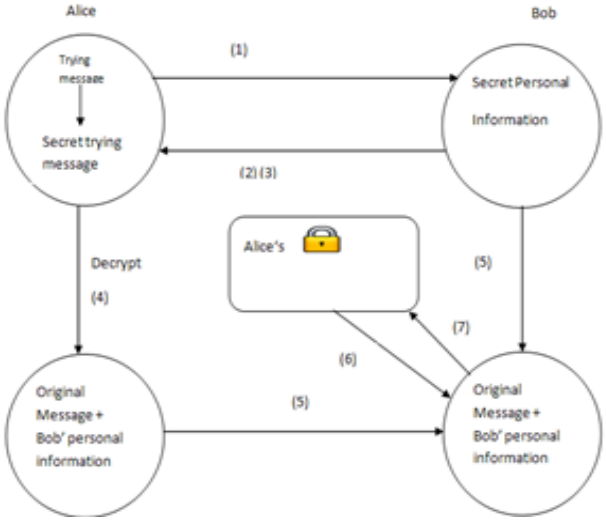

Fig. 1: Quantum communication protocol for blind signature.

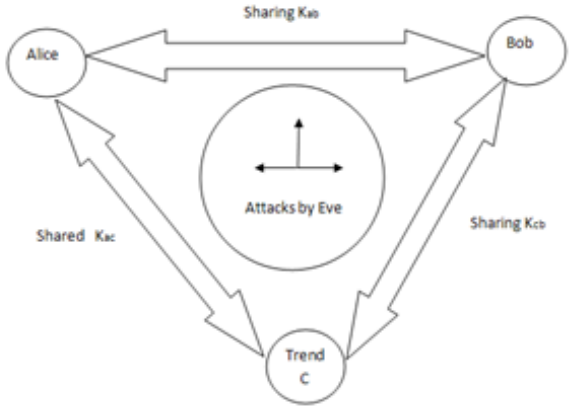

Fig. 2: Distribution of the quantum keys for blind signature.

B. Trying Blind Signature

Alice generates a qutrit string $|\psi_{M1}>$ to be used for trying message. Alice converts the trying message M_1 into a qutrit string $|\psi_{M1}>$ that we have in the following string n qutrits, where:

$$|\psi_{M1}> = \{|\psi_{11}>, |\psi_{12}>, \ldots, |\psi_{1j}>, \ldots, |\psi_{1n}>\}$$

Also, $|\psi_{M1}>$ has a single qutrit $|\psi_{1j}>$ where can be shown as:

$|\psi_{1j}> = \alpha_0|0> + \alpha_1|1> + \alpha_2|2>$, where α_0, α_1, α_2 are complex number where $\alpha_0|0 + \alpha_1|1 + \alpha_2|2 = 1$.

Then, Alice generates a secret string of qutrits |T> and the private key is related with measurement operators where:

$K_a = \{|K_{1a}>, |K_{2a}>, \ldots, |K_{ja}>, \ldots, |K_{na}>\}$ and measurement operators

$M_{ka} = \{M_{1_{K1}}, M_{2_{K2}}, \ldots, M_{j_{Kj}}, \ldots, M_{n_{Kn}}\}$.

After that, the secret string qutrits is measured with the related key measurement operators, this value will be used later to compare with the signer value to check whether it was changed during signing.

$$|T>= \{M_{ka}|\psi_{M1}>= \{|t_1>, |t_2, \ldots, |t_j>, \ldots, |t_n>\}$$

To sign the secret message, Bob inserts his private information in to it without knowing that the contents of the message. Bob generates a qutrit string of his own personal information $|\psi_p>$, where n qutrits in the string, can be shown as:

$$|\psi_p>= \{\psi_{p1}>, \psi_{p2}>, \ldots, \psi_{pj}>, \ldots, \psi_{pn}>\}$$

Also, Bob assume that Alice does not know the content of his personal information and cannot access it. $|\psi_p>$ is encrypted using K_{bc} which will be combined with a sequence of measurement operators M_{kbc}, where:

The key $K_{bc} = \{|K_{1_{bc\_}}, |K_{2_{bc\_}}, \ldots, |K_{j_{bc\_}}, \ldots., |K_{n_{bc\_}}\}$

Bob should check his qutrits $|\psi_p>$ and gets*:*

$$|P\_ = M_{kbc}\{|P_{1\_}, |P_{2\_}, \ldots, |P_{j\_}, \ldots, |P_{n\_},\}$$

In order to have a quantum blind signature for the secret trying message, Bob will use k_{ab}, to encrypt $|T>$ and $|P>$ to obtain the blind signature:

$$S_b = K_{ab}(|T>, |P>)$$

Finally, Bob sends Sb to Alice and waits for the signature Verification.

C. Verifying the signature

First, Alice got S_b as shown before and he decrypts it using k_{ab}. Alice obtains $|T'>$ and $|P'>$, then she can get $|\psi'_{M1}>$ by decrypting $|T'>$ using her private key K_a.

Second, Alice checks if the signature is blind. She verifies that by comparing $|\psi'_{M1}>$ to her $|\psi_{M1}>$ that chosen in the first trying quantum blind signature. If $|\psi'_{M1}>$ does not equal $|\psi_{M1}>$, then the message has been compromised by someone who was trying to reveal part of the content of the secret message. This will lead to dropping the message and start again. However, if they are equal, we can assume that the content of the message were not compromised and at this stage the blind signature has started. Then, |P> will be sent by Bob to Trend. It can be obtained by encrypting $|\psi_p>$ using M_{kbc}. Bob will send it to Trend through the quantum channel since no other than them can know |P>. After that, Alice sends $|P'>$ to Trent.

Finally, since Trend has |P> and $|P'>$, he will verify the authenticity of the signature. He checks if |P> = $|P'>$, and decrypts |P> and $|P'>$, using K_{bc}. Trend has already $|\psi_p>$ and $|\psi'_p>$ and he will check if |P> = $|P'>$, $|\psi_{M1}>= |\psi'_{M1}>$ and $|\psi_p>$ =

$|\psi'_p>$, which means we got successfully the trying blind signature. Since we got the trying blind signature authentic and blindness, Trend sends a message to Alice and Bob about the result and can communicate safely. However, if one of the previous conditions has not been met, the communication will be dropped.

IV. PROCESS OF ENCRYPTION AND DECRYPTING OF QUBIT

As shown in Fig. 3, we have a string of n qubit that can be expressed as:

$$|\psi >= \{|\psi_1 > \otimes\ |\psi_2 >, \dots, \otimes\ |\psi_m >, \dots, \otimes\ \psi_{1n} >\}$$

Also, the hybrid key contains two types of keys, quantum key and binary key that are involved in the process of encryption and decryption. The quantum key can be represented as follow:

$$|K_1 >= \{|K_{11} > \otimes\ |K_{12} >, \dots, \otimes\ |K_{1m} >, \dots, \otimes\ |K_{1n} >\}$$

Binary key as: $K_2=k_{21}k_{22}\dots k_{2s} \in \{0, 1\}$

We assume that the two keys are distributed in advance to Alice and Bob in a secure way and can be used for future communications if it has not been hacked. The purpose of the classical channel is to detect the presence of Eve who wants to access the information. We will apply Hadamard gate and Controlled-NOT gate in the encryption and decryption.

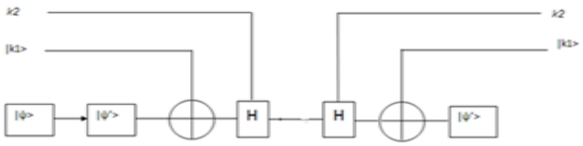

Fig. 3: Qubit of encryption and decryption

V. PROCESS OF DECRYPTION OF QUBIT WITHOUT HAVING EVE IN BETWEEN

Trend Decrypts Bob's Qubits (Original Data) using BC key (part1), after that, Trend Decrypts Bob's Qubits that was send by Alice by BC key (part2). The process is shown in Table 1.

TABLE1: DECRYPTION OF QUBITS WITHOUT EVE

Part1			Part2		
M	α 0	α 1	M	α 0	α 1
Q1	0.4	0.6	Q1	0.4	0.6
Q2	0.3	0.7	Q2	0.3	0.7
Q3	0.2	0.8	Q3	0.2	0.8
Q4	0.1	0.9	Q4	0.1	0.9
Q5	0.7	0.3	Q5	0.7	0.3
Q6	0.8	0.2	Q6	0.8	0.2
Q7	0.9	0.1	Q7	0.9	0.1
Q8	0.3	0.7	Q8	0.3	0.7
Q9	0.2	0.8	Q9	0.2	0.8
Q10	0.4	0.6	Q10	0.4	0.6
Q11	0.5	0.5	Q11	0.5	0.5
Q12	0.8	0.2	Q12	0.8	0.2

VI. THE PROCESS OF THE DECRYPTION OF QUBIT HAVING EVE IN BETWEEN

Trend Decrypted Bobs Qubits that was send by Alice by BC key as in Table 2.

TABLE2: DECRYPTION OF QUBITS WITH EVE

M	α 0	α 1
Q1	-0.2	0.0
Q2	-0.1	0.3
Q3	-1.1	-0.5
Q4	-0.4	0.4
Q5	0.3	-0.1
Q6	0.2	-0.4
Q7	0.6	-0.2
Q8	-0.1	0.3
Q9	-1.1	-0.5
Q10	-0.4	-0.2
Q11	0.0	0.0
Q12	-1.7	-2.3

VII. PROCESS OF DECRYPTION OF QUTRITS WITHOUT HAVING EVE IN BETWEEN

Trend decrypts Bob's Qutrits (original data) using BC key (Part1), after that, Trent Decrypted Bobs Qutrits that was send by Alice by BC key (part2) as shown in Table 3.

TABLE3: DECRYPTION OF QUIRITS WITHOUT EVE

Part1				Part2			
M	α 0	α 1	α 2	M	α 0	α 1	α 2
Q1	0.1	0.6	0.3	Q1	0.1	0.6	0.3
Q2	0.3	0.4	0.3	Q2	0.3	0.4	0.3
Q3	0.2	0.6	0.2	Q3	0.2	0.6	0.2
Q4	0.3	0.6	0.1	Q4	0.3	0.6	0.1
Q5	0.2	0.3	0.5	Q5	0.2	0.3	0.5
Q6	0.2	0.2	0.6	Q6	0.2	0.2	0.6
Q7	0.6	0.1	0.3	Q7	0.6	0.1	0.3
Q8	0.3	0.4	0.3	Q8	0.3	0.4	0.3
Q9	0.3	0.5	0.2	Q9	0.3	0.5	0.2
Q10	0.3	0.6	0.1	Q10	0.3	0.6	0.1
Q11	0.2	0.3	0.5	Q11	0.2	0.3	0.5
Q12	0.2	0.2	0.6	Q12	0.2	0.2	0.6

VIII. THE PROCESS OF THE DECRYPTION OF QUTRITS HAVING EVE IN BETWEEN

Trend Decrypts Bobs Qutrits that was send by Alice by BC key as shown in Table 4.

TABLE4: DECRYPTION OF QUTRITS WITH EVE

M	α 0	α 1	α 2
Q1	-1.6	-1.1	-1.4
Q2	-2.2	-2.1	-2.2
Q3	-1.5	-1.1	-1.5
Q4	-1.4	-1.1	-1.6
Q5	-3.1	-3	-2.8
Q6	-4.8	-4.8	-4.4
Q7	-9.4	-9.9	-9.7
Q8	-2.2	-2.1	-2.2
Q9	-1.7	-1.5	-1.8
Q10	-1.4	-1.1	-1.6
Q11	-3.1	-3	-2.8
Q12	-4.8	-4.8	-4.4

IX. ANALYSIS OF THE PROPOSED ALGORITHM

The scheme introduced in [1] is using qutrits during the communication and the encryption is not discussed clearly in the paper. In this paper we propose that during the communication, the qubit and qutrits should be encrypted to improve the security of the scheme. Also we have shown that the new development can make it easier to detect any attempt by any illegitimate node to change the original content at any phase with the help of Trend who is responsible for authentication and verification of the signature during the communication.

In general we can say that the current scheme is more secure and more efficient. Also, it provides many security features such Impossibility of forgery and prevention of denial by the receiver. These two features are explained in this section

A. Preventing forgery

During the communication steps that we have discussed before, there are two eigenstate for qubit bit and three eigenstate for qutrits. This is a main feature that enables us to make it impossible for Eve to attack the communication. Also, if one of the communicating parties turns to be malicious and wants to access unauthorized, it can be detected. If Alice tries to sign one of Bob's messages pretending by forging Bob's personal signature, she will be detected in the verification phase. If Trend compares $|P_s\rangle$ and $|P\rangle$, he will find out they are different which leads to abolishing the signing phase. Also, if an attacker tried to imitate Bob's signature, he will be detected in the initial phase.

B. Preventing repudiation by the receiver

Another feature that is supported by this scheme is preventing denial by the receiver. Let's assume Alice tried to deny Bob's signature. In the Verification phase, Alice obtains $|P\rangle$ and $|T\rangle$ by encrypting Sb using K_{ab}. If $|P'\rangle$ is fake information of Bob. when Trend finds $|P\rangle = |P'\rangle$ and $|\psi_p\rangle = |\psi'_p\rangle$, in this case, Trend will send the result to Alice and Bob telling them that trying blind signature is authentic but if one of the conditions is missing, the process will stop at this stage. In other words, Alice and Bob are not able to deny the signature of one of them. However, if one of them denies the signature, Trend will detect it that and they will stop the communication.

TABLE5

Hadamard and C-Not Gates Sizes (Matrices) for Qubits and Qutrits (After Tensor Product Between Encrypted Qubit and Quantum Key)

Hadamard		C-not	
Qubits	Qutrits	Qubits	Qutrits
4 X 4	16 X 16	4 X 4	16 X 16
8 X 8	64 X 64	8 X 8	64 X 64

X. CONCLUSIONS

In this paper, we have improved the communication Scheme for Blind Signature with Two-Particle Entangled Quantum-Trits. We have applied a two-particle entangled quantum-qubits and qutrits. The new implementation improves security of the scheme where it is harder for attackers to break. Furthermore, implementation of encryption t using encrypted qubits and qutrits during the communication provides higher efficiency. Finally, the scheme has several new enhanced security features such as preventing forgery within the parties and eliminating the possibility of repudiation of a signee.

REFERENCES

[1] S. Jinjing, et al., "Quantum communication scheme for blind signature with two-particle entangled quantum-trits," in Advanced Communication Technology (ICACT), 2012 14th International Conference on, 2012, pp. 558-561.

[2] N. Zhou, et al., "Novel qubit block encryption algorithm with hybrid keys," Physica A: Statistical Mechanics and its Applications, vol. 375, pp. 693-698, 2007.

[3] G. B. C.H. Bennett, "Quantum cryptography:Public key distribution and coin tossing," Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, 1984.

[4] W. Tittel, et al., "Experimental demonstration of quantum secret sharing," Physical Review A, vol. 63, p. 042301, 2001.

[5] S. William, "Cryptography and Network Security: Principles and Practice," Prentice Hall, New Jersey, p. 67, 2003.

[6] D. Chaum, "Advance in Cryptography, Proceedings of Crypto'82 Springer- Verlag, Berlin," p. 267, 1982.

[7] K. Baoyuan and H. Jinguang, "On the security of blind signature and partially blind signature," in Education Technology and Computer (ICETC), 2010 2nd International Conference on, 2010, pp. V5-206-V5-208.

[8] L. Tien-Sheng, et al., "Quantum signature scheme for vehicular networks using entangled states," in Security Technology (ICCST), 2011 IEEE International Carnahan Conference on, 2011, pp. 1-6.

[9] L. Xin and F. Dengguo, "Quantum digital signature based on quantum one-way functions," in Advanced Communication

Technology, 2005, ICACT 2005. The 7th International Conference on, 2005, pp. 514-517.
[10] W. Xiaojun and L. Yun, "Quantum Message Signature Scheme without an Arbitrator," in Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on, 2007, pp. 496-500.
[11] C. Zhengjun and O. Markowitch, "Security Analysis of One Quantum Digital Signature Scheme," in Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on, 2009, pp. 1574-1576.
[12] B. Schneier, "Applied Cryptography:Protocols, Algorithms, and Source Code in C," John Wiley and Sons, New York, 2nd ed, p. 79, 1996

Arafat Abu Mallouh

Arafat Abu Mallouh is originally from Jordan. He is pursuing his Doctorate in Computer Science and Engineering at the University of Bridgeport in Bridgeport, Connecticut, USA. He received his Bachelor's degree in Computer Science from The Hashemite University, Zarqa, Jordan. Mr. Abu Mallouh received his Master's degree in Computer Science from Amman Arab University for Graduate Studies, Amman, Jordan. His research interests include artificial intelligence, image processing, Machine Learning, and Data Mining.. Currently Mr Abu Mallouh works on new techniques for voice processing.

Khaled M. Elleithy

Dr. Elleithy is the Associate Dean for Graduate Studies in the School of Engineering at the University of Bridgeport. He has research interests are in the areas of network security, mobile communications, and formal approaches for design and verification. He has published more than two hundred and fifty research papers in international journals and conferences in his areas of expertise.

Dr. Elleithy is the co-chair of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). CISSE is the first Engineering/Computing and Systems Research E-Conference in the world to be completely conducted online in real-time via the internet and was successfully running for six years. Dr. Elleithy is the editor or co-editor of 12 books published by Springer for advances on Innovations and Advanced Techniques in Systems, Computing Sciences and Software.

Ramadhan J. Mstafa

Ramadhan Mstafa is originally from Dohuk, Kurdistan Region, Iraq. He is pursuing his Doctorate in Computer Science and Engineering at University of Bridgeport, Bridgeport, Connecticut, USA. He received his Bachelor's degree in Computer Science from University of Salahaddin, Erbil, Iraq. Mr. Mstafa received his Master's degree in Computer Science from University of Duhok, Duhok, Iraq. His research interests include image processing, mobile communication, security and steganography.

Adwan Alanazi

Adwan Alanazi is originally from Saudi Arabia He is pursuing his Doctorate in Computer Science and Engineering at the University of Bridgeport in Bridgeport, Connecticut, USA. He received his Bachelor's degree in Computer Science from University of Hail, Hail, Saudi Arabia. Mr. Alanazi received his Master's degree in Computer Science from University of Missouri Kansas City. His research interests include Wireless Sensor Networks and Network Security.