# An Authenticated Key Distribution Scheme

Sara Abozied,Hassan M. Elkamchouchi,Yasmine Abouelseoud, Refaat El-Attar

***Abstract*— In this paper, a key distribution protocol based on the integration of both classical and quantum cryptography is developed. Quantum cryptography is used for secure optical transmission which employs quantum mechanisms to distribute session keys. Classical cryptography provides convenient techniques that enable efficient user authentication and prevent denial of previous commitments. The proposed scheme is based on the RSA-TBOS signcryption scheme to achieve the combined functionality of a digital signature and encryption in an efficient manner. The transmitter generates a random session key, and applies the signcryption module to it. It therefore offers three services: privacy, authenticity and non-repudiation. The ciphertext is converted to binary bits then to qubits using a pre-shared random number between the transmitter and receiver. The session key is used later for secure transmission of messages over a public optical channel.**

***Index Terms*—Quantum Cryptography (QC), Classical cryptography, RSA-TBOS signcryption, Session key, Digital signature**

## I. INTRODUCTION

Security has become a big concern in wired and wireless networks. The characteristics of networks pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. Cryptographic techniques are widely used for secure communications. The security of classical cryptosystems is based on algorithmic complexity; that is, it is difficult in practice to deduce the secret key from the public key within a reasonable delay. Nothing proves; however, that this security is not compromised in a near future because there is an accelerated evolution of the software and the special hardware. So, many cryptographic schemes in use today would be broken with either unanticipated advances in hardware and algorithms or the advent of quantum computers. An interesting solution to the delicate problem of distribution of keys met in cryptography is the use of the laws of quantum physics.

Manuscript received July 18, 2012; revised August 8, 2012. This work is supported by Faculty of Engineering, Alexandria University.
Sara Abozied is teaching assistant with Faculty of Engineering, Alexandria University (phone: 00201001970021, E-mail: saraabozied@gmail.com).
Hassan Mahamoud Elkamchouchi is professor with the Electrical Engineering Department, Alexandria University (phone:00201223718433, E-mail: helkamchouchi@gmail.com).
Yasmine Abouelseoud is professor with Faculty of Engineering, Alexandria University (phone: 00201003727019. E-mail: yasmine.abouelseoud@gmail.com).
Refaat El-Attar is professor with Physics and Mathematics Department, Faculty of Engineering, Alexandria University (phone:00201001005548, E-mail: rea5@hotmail.com).

Quantum Cryptography (QC) protocols are used to carry out the task of exchanging keys with great security. Quantum cryptography has been proven secure even against the most general attack allowed by the laws of physics and is a promising technology for adoption in realistic cryptographic applications [1]. The bit is the fundamental concept of classical computation and classical information. Quantum computation is built upon an analogous concept, the quantum bit, or qubit for short. Just as a classical bit has a state – either 0 or 1 –a qubit also has a state. Two possible states for a qubit are the states $|0>$ and $|1>$, which correspond to the states 0 and 1 for a classical bit. The difference between bits and qubits is that a qubit can be in a state other than $|0>$ or $|1>$. It is possible to form linear combinations of states, often called superpositions:

$$|\psi>=\alpha|0>+\beta|1>$$

The numbers α and β are complex numbers satisfying

$$|\alpha|^2+|\beta|^2=1.$$

Scientists claim that QC theoretically offers absolute security through the basic laws in quantum physics. Two reasons have been frequently stated. The first of these relies upon the 'uncertainty principle', which states that a single photon cannot be detected and its polarization (or phase state) measured simultaneously. In other words, the superposition of a pair of quantum observables cannot be measured without interfering with the measurement of the other. Moreover, under the 'no cloning' theorem it is not possible to clone a photon so that one can be measured and the other passed on to the recipient. By the use of suitable protocols, involving additional communication over a conventional public communications channel, any attempt to intercept the data may therefore be detected [2].

A more important task to be done prior to communication is the authentication that guarantees that the origin of the message is genuine because, if a malicious user masquerades as a legitimate user, the key distribution schemes and encryption schemes will be easily compromised. In situations where there is not complete trust between the sender and the receiver, something more than authentication is needed which is the digital signature. The digital signature is analogous to the handwritten signature. It must have the following properties:

- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Thus, the digital signature function includes the authentication function.

The straightforward use of public-key encryption provides confidentiality but not authentication. The source uses the public key $PU_b$ of the destination to encrypt M. Because only B has the corresponding private key$PR_b$, only B can decrypt the message. This scheme provides no authentication because any opponent could also use B's public key to encrypt a message, claiming to be A.

To provide authentication, A uses its private key to encrypt the message, and B uses A's public key to decrypt. This provides authentication using the same type of reasoning as in the symmetric encryption case: The message must have come from A because A is the only party that possesses $PR_a$ and therefore the only party with the information necessary to construct the ciphertext that can be decrypted with $PU_a$.

To provide both confidentiality and authentication, A can encrypt M first using its private key, which provides the digital signature, and then using B's public key, which provides confidentiality. The disadvantage of this approach is that the public-key algorithm, which is complex, must be exercised four times rather than two in each communication [3].

In this paper, a key distribution protocol based on transmission of qubits is proposed to achieve: privacy, authenticity and non-repudiation of communicating parties and the detection of eavesdroppers according to laws of physics. The protocol relies on the use of the signcryption cryptographic primitive to achieve the first three goals. Our primary goal is to construct a scheme such that the number of keys stored per user and the number of rounds are kept minimal. Moreover, no third party knows the shared session key in the proposed scheme.

## II. Related Work

### A. BB84 Protocol

The BB84 protocol was first introduced in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal [5]. It suffers from several problems. It is susceptible to man-in-the-middle attack, about 50% of the bandwidth is wasted, its number of rounds is high and there is no authentication. Moreover, it doesn't withstand the beam splitting attack.

In spite of this, it is still widely used and has become standard. It is based on Heisenberg's uncertainty principle. The BB84 protocol uses polarized photons. Alice sends polarized photons, referenced to one of two different orthogonal base sets (i.e., {horizontal, vertical} or {+ 45, - 45}), and Bob observes the received photon, randomly choosing one of the two bases. After a certain amount of data is transmitted, Alice and Bob determine which data bits should be discarded by exchanging information about the bases they used for polarizations and measurements using a classical channel. They keep the rest of the data bits after sifting as the key for future use. Hence, the length of the key is in the order of half the number of the bits transmitted [4].

### B. Quantum Authentication Protocol using Quantum Superpositioned States

It is a two-party authentication protocol. To hide transmitted data from unauthorized users, this protocol uses quantum superpositioned states instead of quantum entangled states. To authenticate a specific user (the most common use of authentication protocols) within a group of many using quantum entangled states is a difficult problem. This protocol works well under the assumption that both parties already share a secret key ($K_a$). Furthermore, it was shown that the superposition states can be realized using current technologies (e.g., linear polarizers and Faraday rotators). This protocol is secure against the beam splitting attack and the Intercept/resend attack. But this protocol in the multi-user setting will involve the storage of a large number of pre-shared keys per user in the network [4].

### C. Three-Party Quantum Authentication using Superposition States

The objective of this protocol is to let participants share a different session key for each new session while providing authentication, both implicitly and explicitly. To hide transmitted data from unauthorized users, this protocol uses quantum superposition states instead of entangled states as the previous protocol. This protocol consists of three phases. In the first phase, the participants are implicitly authenticated using the trusted center (TC). In the second phase, a session key is established between the two participants. Even the trusted center cannot listen to the secure communication between the participants because the session key shared between the participants is hidden from the trusted center. In the third phase, the participants of the communication are mutually authenticated to each other in an explicit way [6]. This protocol is secure against the beam splitting attack and the Intercept/resend attack. The presence of a TC resolves the problem of storing a huge number of pre-shared keys in the multi-user case in a large network. The problem of this protocol is that the number of its rounds is high.

### D. AMNI'09 Protocol

In this protocol, a session key is transmitted to the users by a trusted center, which generates the public key and the private key for each user in the registration phase. The trusted center uses the RSA asymmetric algorithm to encrypt the session key which is then converted to qubits for transmission to each user who wishes to participate in a communication session. In this protocol, security is achieved but the authentication is weak; i.e. not achieving non-repudiation [2]. In this protocol, a trusted center is used and it knows the session key so it will know the transmitted message.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

## III. SIGNCRYPTION

Signcryption is a combination of a digital signature algorithm and an encryption algorithm. We review a signcryption scheme based on the RSA trapdoor one-way function [7]. An attractive feature of this scheme is that it offers non-repudiation in a very simple manner. The size of the result of this signcryption scheme is about half the size of a signed and encrypted message using standard RSA techniques. For this reason, they gave it the name "Two Birds One Stone (TBOS)"; that is, signcryption at the cost of encryption.

### A. Key Parameters

- k: Even positive integer.
- Sender (Alice's) RSA Public and Private Key: $(N_A, e_A)$ and $(N_A, d_A)$, respectively.
- Receiver (Bob's) RSA Public and Private Key: $(N_B, e_B)$ and $(N_B, d_B)$ , respectively.

Note: We must have $|N_A| = |N_B| = k$.

- Two hash functions H and G, where

$H:\{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$ and $G:\{0,1\}^{k_1} \rightarrow \{0,1\}^{n+k_0}$ and $k = n + k_0 + k_1$, with $2^{-k_0}$ and $2^{-k_1}$ being negligible.

Note that the output size of H is greater than the input size.

### B. TBOS Signcryption Module

When Alice signcrypts a message $M \in \{0,1\}^n$ for Bob, she performs:

1. $r \leftarrow \{0,1\}^n$
2. $w \leftarrow H(M||r)$
3. $s \leftarrow G(w) \oplus H(M||r)$
4. If $s||w > N_A$ goto 1.
5. $c' \leftarrow (s||w)^{d_A} \bmod N_A$
6. If $c' > N_B, c' \leftarrow c' - 2^{k-1}$
7. $c \leftarrow c'^{e_b} \bmod N_B$
8. Send $c$ to Bob

### C. TBOS Unsigncryption Module

When Bob unsigncrypts a cryptogram received from Alice, he performs:

1. $c' \leftarrow c^{e_b} \bmod N_B$
2. If $c' > N_A$, reject.
3. $\mu \leftarrow c'^{e_A} \bmod N_A$
4. Parse $\mu$ as $(s||w)$
5. $M||r \leftarrow G(w) \oplus s$
6. If $H(M||r) = w$ return M.
7. $c' \leftarrow c' + 2^{k-1}$
8. If $c' > N_A$, reject.
9. $\mu \leftarrow c'^{e_A} \bmod N_A$
10. Parse $\mu$ as $(s||w)$
11. $M||r \leftarrow G(w) \oplus s$
12. If $H(M||r) \neq w$ return M .reject.
13. Return M.

It can be shown that given a valid signcrypted text, the unsigncryption algorithm returns the original plaintext.

## IV. THE PROPOSED SCHEME

In our protocol, integration of quantum cryptography for secure optical transmission and classical cryptography for identity authentication is considered. In many of the existing quantum key distribution schemes, the number of communication rounds is large and the identity of the user is not verified. The proposed protocol is an extension of the work in [2].

The ultimate goal of this protocol is that transmitter and the receiver share an authenticated session key 'SK', which is an n-bit random number.

In what follows, the steps of the proposed protocol are provided. We assume that every participant shares a secret key with the trusted center in advance. Let $K_{A,T}$ be the key shared between Alice and TC, and $K_{B,T}$ be the key shared between Bob and TC. Those keys serve for the mutual authentication between the trusted center and each of the communicating parties.

Let $h(K, M)$ be a hash value of a message M with key k, generated using a cryptographic hash function (e.g., SHA-1 or MD5).

***Step 1: Sharing a random number for bases synchronization***

(i) The TC generates a random number r. The transmitter and the receiver synchronize their quantum polarization bases in step 5 according to this pre-shared random number. Then the TC computes:

$$X = h(K_{A,T}, r) \oplus (U_A||U_B)$$
$$Y = h(K_{B,T}, r) \oplus (U_B||U_A)$$

where || indicates the concatenation of the bit strings and $U_X$ indicates the identifier of the participant X including a public key and its associated certificate.

Now, $r||X$ is encrypted with the pre-shared key $K_{A,T}$ using the scheme in [8] and the result is transmitted to the transmitter over a quantum channel. Similarly, $r||Y$ is encrypted with the pre- shared key $K_{B,T}$ using the scheme in [8] and the result is transmitted to the receiver over another quantum channel.

(ii) The transmitter decrypts and measures the received qubits. She computes a hash value using $K_{A,T}$ and r, and obtains the values of $U_A||U_B$. Then, she verifies the values of $U_A$ and $U_B$.

(iii) The receiver decrypts and measures the received qubits. She computes a hash value using $K_{B,T}$ and r and obtains the values of $U_B||U_A$. Then, she verifies the values of $U_A$ and $U_B$.

Thus, after the successful completion of the session, both the transmitter and the receiver have the random number which will be used in step 5 to generate the qubits.

***Step 2: Registration phase***

The private key and the public key are generated using RSA algorithm for each user.

1. Choose two large prime numbers P and Q.
2. Compute N = P*Q.
3. Choose e (less than N) such that e and A = (P–1)(Q–1) are relatively prime (having no common factor other than 1), the public key is (N, e).
4. Choose d such that (e*d) mod [(P–1)(Q–1)] is equal to

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

1, the private key is (A, d)

The public key of each user can be openly exchanged and the user's private key is kept secret. Each user obtains a certificate from the TC (*cert*) for its public key providing the link between the user's identity and its key.

***Step 3: Creation of a session key***

The transmitting user creates a session key (*SK*). This session key is unique for each communication between users. The first user carries out the following two steps:

- A random number is generated by using a suitable Random (.) function.
- The transmitter signcrypts the session key based on its private key and the public key of the receiver using the RSA-TBOS signcryption scheme and obtains the signcrypted text ($c_{SK}$). The aim of this step is to provide a digital signature as well as encryption of the session key for its origin to be validated by the communicating users. Moreover, the digital signature guarantees non-repudiation.

***Step 4: Conversion to Binary***

This encrypted session key ($c_{SK}$) should be converted into binary and then to qubits and finally sent to the corresponding user.

***Step5: Generation of Qubit***

Four types of polarizing filters are used in the generation phase of the quantum bits depending on the pre-shared random number (r) according to Table I.

1. Vertical represents 0.
2. Horizontal represents 1.
3. Down left to upper right '/' represents 1.
4. Down right to upper left '\' represents 0.

The polarization of a photon can be prepared in any of these states that were mentioned above. Filters exist to distinguish horizontal states from vertical ones. When passing through such a filter, the path of a vertically polarized photon is deflected to the right, while that of a horizontally polarized photon is deflected to the left. In order to distinguish between diagonally polarized photons, one must rotate the filter by 45°. If a photon is passed through a filter with the incorrect orientation – diagonally polarized photon through the non-rotated filter for example – it will be randomly deflected in one of the two directions. In this process, the photon also undergoes a transformation of its polarization state, so that it is impossible to know its orientation before the filter.

The number of bits in the signcrypted session key ($c_{SK}$) must equal the number of photons. The polarizing filter to be used for the polarization of a photon is selected based on the ith bit of the pre-shared random number (r) and the ith bit of the signcrypted session key. If the number of bits in the pre-shared random number is m and the number of bits in the signcrypted session key is n, where m < n, the random number bits are reused; i.e. till the mth bit, the corresponding values will be taken from the random number and for the (m + 1)th bit in the signcrypted session key, the first bit of the random number will be considered and so on

TABLE I
SELECTION OF QUBIT BASIS

| Bit value of ($c_{SK}$) | Bit value of the pre-shared random number | Qubit basis | Qubit value |
|---|---|---|---|
| 0 | 1 | D(diagonal) | \ |
| 1 | 1 | D(diagonal) | / |
| 0 | 0 | R(rectilinear) | \| |
| 1 | 0 | R(rectilinear) | - |

***Step 6: Unsigncryption process***

Unsigncryption is done on the receiver side based on its private key and the transmitter's public key. The received qubits are measured using the appropriate filters based on the pre-shared random number. After obtaining the binary values, the user converts the resulting binary representation of the signcrypted session to the equivalent decimal representation. The receiver unsigncrypts the decimal value. This involves verification of the key origin and the decryption of the session key.

After all previous steps, both users have shared a common session key. This session key is to be used to encrypt the messages to be communicated between those users in future.

***Step 7: Exchanging encrypted messages***

In this step, a quantum encryption algorithm is used to assure the confidentiality of the exchanged messages. The established session key in the previous steps is used here. A scheme such as that proposed in [8] can be employed.

## V. SECURITY ANALYSIS OF THE PROPOSED SCHEME

a) Intercept/resend attack

Let us assume that an eavesdropper (Eve) intercepts the transmitted photons from the transmitter. After a measurement of the photon, Eve resends it to the receiver. This attack cannot break our scheme because when Eve measures the quantum states, she will measure it in wrong bases with probability 0.5. So, the receiver will know that the message doesn't come from the original transmitter because the signature part won't be correctly verified most probably. The probability of detecting an eavesdropper in this attack is $(1 - 0.75^n)$, where *n* is the number of bits in the signcrypted session key.

b) Beam- splitting attack

It is not easy to build a single photon source with current technologies. As a matter of fact, in general, the light pulse called as a single photon in the laboratory is not a pure single photon state (i.e., zero, one or multiple photons in the same state). Therefore, the following attack is possible against BB84. First, Eve collects a fraction of the multiple photons by putting a beam-splitter in the path between the transmitter and the receiver. Eve stores the extra photons in a quantum memory until Bob detects the remaining single photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

However, this attack is not possible against the proposed protocol. Although, Eve can store the collected photon, Eve will not know the quantum state which is being transmitted because Eve doesn't know the random number required for bases synchronization which will never be disclosed in public.

## VI. DISCUSSION

In this section, a comparative study will be provided pointing out the advantages of the proposed scheme over other schemes in literature. The comparison will be held among the following schemes:

1. Quantum authentication protocol using quantum superpositioned states (Scheme 1).
2. Three party quantum authenticated key distribution protocol using superposition states (Scheme 2).
3. AMNI'09 protocol (Scheme 3).
4. The proposed scheme (Scheme 4).

All these schemes provide:

1- Security (or confidentiality)
2- Authentication
3- Sharing a session key between users

Assume a network of *n* users that need to communicate with each others.

TABLE II
Comparison between the schemes

| Schemes | Presence of TC | Information available to TC |
|---|---|---|
| 1 | No TC | No TC |
| 2 | TC | TC doesn't know session key |
| 3 | TC | TC knows the session key |
| 4 | TC | TC doesn't know session key |

| Schemes | No. of rounds in case of two users | No. of long-term keys stored per user |
|---|---|---|
| 1 | 3 rounds | (*n*-1) keys |
| 2 | 3 rounds per bit and other 4 rounds | 1 key |
| 3 | 2 rounds | 1 key |
| 4 | 3 rounds | 2 keys |

It is clear from the above table that no third party knows the session key in our protocol as in the first two schemes. However, the proposed protocol is advantageous over the first protocol with regard to the number of long-term keys stored per user and it is advantageous over the second scheme from the viewpoint of the number of rounds required to establish the session key. Finally, the proposed protocol is superior to the third scheme since the session key is only known to the communicating parties with a comparable performance in the number of rounds and storage requirements.

## VII. CONCLUSION

In this paper, an integrated security system has been developed. Initially, an authenticated key agreement protocol is used to establish a shared session key between two entities or more. A signcryption scheme is used to achieve privacy, authenticity and non-repudiation and quantum bits are transmitted over the channel to achieve detection of eavesdropping based on the uncertainty principle. The advantages of the use of the signcryption protocol rather than a sign-then-encrypt protocol are that it is computationally more efficient, and saves bandwidth. The next step in the protocol is the exchange of messages confidentially among the users sharing the session key. An advanced quantum encryption, such as the scheme in [8], is used to achieve the secrecy of messages being transmitted. The session key is known only to the transmitter and the receiver. The trusted center doesn't know the session key. It is clear that the proposed protocol is resistant to various attacks such as the intercept-resend attack [9] and the beam-splitting attack [10]. The use of a public key infrastructure enables reducing the number of keys stored per user which is an important feature in multi-user setting.

## REFERENCES

[1] M. Elboukhari, M. Azizi, and A. Azizi, "Quantum Key Distribution Protocols," Int. J. Universal Computer Sciences, vol. I 201, pp. 59–67, March 2010.
[2] B. Amutha and V.Nivedha "AMNI'09 Protocols" Int. J. Universal Computer Sciences, vol. 2, pp. 297–303, December 2009.
[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 4th ed. New York, Prentice Hall, 2005.
[4] Y. Kanamori, S.Moo Yoo, D. Gregory and T. Sheldon, "On Quantum Authentication Protocols", Proceedings of the IEEE Global Tele-communications Conference, GLOBECOM'05 vol. 3, 2005.
[5] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of the International Conference on Computers, Systems and Signal Processing", Bangalore, India, 1984.
[6] K. S. Reddy and R. K. Medapati, "Three party Quantum Authenticated Key Distribution Protocol Using Superposition States," Int. J. Comp. Appl., vol. 2, G. T. Rado and H. Suhl, Eds. New York, Academic Press, 1963, pp. 1589– 1594.
[7] Malone-Lee and W. Mao, Two Birds One Stone: Signcryption Using RSA, In Topics in Cryptology -CT-RSA 2003, volume 2612 of Lecture Notes inComputer Science, pages 211-225, 2003.
[8] Z. Cao and L. Liu, "Improvement of one Quantum Encryption Scheme", IEEE International Conference on Intelligent and Computing Systems (ICIS), vol. 1, pp. 335-339, 2010.
[9] D. Bouwmeester, A. Ekert, and A. Zeilinger, The physics ofquantum information, Springer, New York, 2000.
[10] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Amolin, "Experimental Quantum Cryptography", J. of Cryptology, vol. 5, pp, 3-28, 1992.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)