I. J. Computer Network and Information Security, 2015, 7, 1-9
Published Online June 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.07.01

An Ultra-secure Router-to-router Spontaneous Key Exchange System

Pramode K. Verma[1], Mayssaa El Rifai[2]
Telecommunications Engineering Program, School of Electrical and Computer Engineering,
University of Oklahoma-Tulsa, OK 74135, USA
Email: pverma[1], mayssaa[2]@ou.edu

Abstract—This paper presents an ultra-secure router-to-router key exchange system. The key exchange process can be initiated by either router at will and can be carried out as often as required. We compare the efficacy of the proposed approach with contemporary quantum key distribution (QKD) systems and show that quantum-level security is attainable without resorting to single photon generators and other attendant instrumentation associated with QKD. Furthermore, the proposed system addresses the extremely limited geographical reach of commercially available QKD systems and other environmental restrictions they must operate in. The proposed system carries out all processing in electronics and is not vulnerable to the man in the middle attack. The medium of transfer can, of course, be optical fibers as is common in telecommunication.

Index Terms—Key exchange, Discrete logarithm, Multi-stage protocol, Initialization vector, The braiding concept, Quantum Key Distribution

I. Introduction

Securing information is an increasingly important need of the modern society. As computing power increases, the ability to launch successful cryptanalytic attacks correspondingly increases. This has led to using longer and longer keys in either symmetric (e.g., AES-based) or asymmetric (e.g., RSA-based) cryptography systems, or more frequent key exchanges, or both. Neither of these or for that matter any contemporary cryptographic technique used on a commercial basis offers unconditional security. Furthermore, distribution and management of keys continues to remain an important part of the security process constituting a significant portion of the overall cost of security.

Classically, the one-time pad proposed by an Army Signal Corp officer, Joseph Mauborgne [1,2] is the only encryption scheme that offers perfect security. The one-time pad is a symmetric encryption scheme where a random key of length equal to the transmitted message is used for both encryption and decryption. Since each new message requires the use of a new random key, the one-time pad is known to be unbreakable. However, distributing keys securely between the two communicating endpoints with a length equal to the message is a requirement that cannot be practically met.

This paper proposes a novel means of distributing secure keys on a point-to-point basis between two routers that does not require any human or machine intervention. The communicating routers can exchange keys at random intervals or on a message or a session basis; indeed, based on any scheme that the customer wishes to have. The proposed scheme is independent of the medium of transmission between the two routers and does not necessitate the absence of intermediate repeaters between the routers. Intermediate repeaters are unacceptable in a contemporary quantum key distribution system. The cryptography system proposed in this paper is based on a multi-stage protocol requiring an exchange of keys between the two communicating parties in one or more steps.

A mechanical representation of the proposed system is as follows: Alice uses a lockbox with two latches, each of which can be independently locked and opened by the respective key holder. Alice puts her message in the box and a lock of her own on one of the two latches on the box. Bob receives the box and puts his own lock on the other latch, without trying to open the box. He then sends the box back to Alice. Upon receiving the box, Alice unlocks her lock and returns the box to Bob. She cannot, of course, open the box because Bob's lock is still there on the box. On the second trip of the box from Alice to Bob, the box has only Bob's lock which he can then unlock upon receiving it and retrieve the message inside the box.

The difference between the above example and the proposed scheme is that unlike the mechanical representation where we have assumed that the lock is secure, electronic bits (or their photonic representation) can be easily copied by an intruder. This has two implications. First, the message to be transmitted cannot be in the open. Second, even if this message were to be altered by some form of encryption, since the intruder can have access to each of the three legs of transmission; the encryption mechanism needs to be sufficiently robust in order to thwart an attempt to recover the message during transition. This paper presents a system based on discrete logarithms for securing the messages in transition. The proposed system is best suited for exchanging keys between two routers and can be done as frequently as necessary and can be initiated by either of the two communicating entities.

This paper is organized as follows: Section II captures the mathematical foundations of the proposed scheme based on the use of discrete logarithms as well as key distribution protocols previously used. Section III discusses the proposed technique and its cryptographic strength. Section IV introduces another contrivances that can further enhance the cryptographic strength of the proposed protocol. Section V effects a comparison with the currently available QKD systems and Section VI captures our conclusions.

II. Related Work

A. Discrete Logarithms

Discrete logarithms constitute a well-known technique in number theory [3,4]. Discrete logarithms in Z_p are related to the primitive roots of the prime number p. All prime numbers have primitive roots. One characteristic of a primitive root α of a prime number p is that successive powers of α from 1 to $p-1\, mod(p)$ generate the numbers from 1 to $p-1$, all of which are distinct, but in some unpredictable order. In other words, for any integer b and a primitive root α of a prime number p, there is a unique exponent i such that,

$$b = \alpha^i mod(p) \qquad 0 \le i \le p-1 \tag{1}$$

The exponent i is referred to as the discrete logarithm of the number b for the base $\alpha\ mod\ p$.

One of the properties of discrete logarithms is that, given α, i, and p, the computation of b is easy. However, given b and α, computation of i is difficult. This difficulty is of the same order of magnitude as factoring primes required for RSA [5]. We note that unlike the Diffie-Hellman technique (discussed in the next subsection), these parameters are not global. They are known only to the concerned router pairs.

We derive our clue from the fact that if the information to be transmitted (in other words, the key) gets embedded in the exponent i (or the discrete logarithm) and is transmitted as the number b, deriving the key will be as hard as any contemporary encryption scheme. This combined with the fact that the key exchange can take place as frequently as desired with minimal overhead in communication, we posit that the proposed scheme has the potential of approaching the level of security of contemporary quantum key distribution (QKD) systems. The following section discusses one of the contemporary key management/distribution protocols.

B. Contemporary Key Distribution Protocols

In this section, the Diffie-Hellman key distribution [6,7] technique is discussed. The Diffie-Hellman key distribution algorithm is based on using prime numbers as well as primitive roots in a similar context as in the proposed multi-stage protocol.

Fig. 1 summarizes the Diffie-Hellman key exchange algorithm. In this scheme, there are two publicly known numbers (global elements); q is a prime number with its primitive root α. X_A and X_B are two random variables chosen by Alice and Bob, respectively. Using the key exchange system presented in Fig. 1, Alice and Bob will share a key $K = (Y_B)^{X_A} mod(q) = (Y_A)^{X_B} mod(q)$.

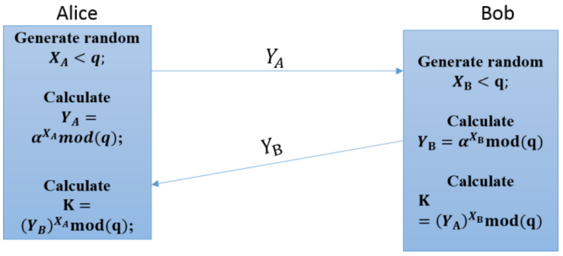


Fig. 1. Diffie-Hellman key exchange

The Diffie-Hellman key exchange algorithm depicted in Fig. 1 is, however, vulnerable to the man in the middle attack. An attacker, Eve, will proceed as shown in Fig. 2 to share a key K_1 with Alice and another key K_2 with Bob. Thus, all future communication between Alice and Bob is compromised.

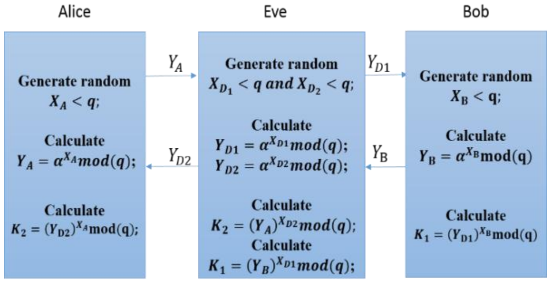

Alice
Eve
Bob
Generate random
$X_A < q;$
Calculate
$Y_A = \alpha^{X_A} mod(q);$
Calculate
$K_2 = (Y_{D2})^{X_A} mod(q);$
Y_A
Y_{D2}
Generate random
$X_{D_1} < q\ and\ X_{D_2} < q;$
Calculate
$Y_{D1} = \alpha^{X_{D1}} mod(q);$
$Y_{D2} = \alpha^{X_{D2}} mod(q);$
Calculate
$K_2 = (Y_A)^{X_{D2}} mod(q);$
Calculate
$K_1 = (Y_B)^{X_{D1}} mod(q);$
Y_{D1}
Y_B
Generate random
$X_B < q;$
Calculate
$Y_B = \alpha^{X_B} mod(q)$
Calculate
$K_1 = (Y_{D1})^{X_B} mod(q)$

Fig. 2. Man in the middle attack in case of a Diffie-Hellman key exchange system

Shared keys between different parties in a network can also be established with the help of a trusted third party. This third party is called the key distribution center [8]. Furthermore, symmetric key distribution using asymmetric encryption can be used as a key distribution scheme as proposed in [9] and [10]. It is worth noting that the scheme proposed in [9] is vulnerable to the man in the middle attack, whereas the scheme proposed in [10] assumes that Alice and Bob already exchanged a public key using a public key distribution technique. Several public key distribution techniques can be used, e.g., public announcement, publicly available directory, public-key authority, and public certificate.

The protocol proposed in this paper overcomes the overhead of maintaining an updated list of the public keys of each node in the network as well as sharing them globally by the means mentioned earlier. We do note that the proposed system, however, is deployed for encrypting messages on a link which connects two routers. It does not offer an end-to-end application level encryption scheme.

III. The Proposed Protocol

In this section, the proposed protocol which is a multi-stage router to router key distribution protocol is presented. The proposed protocol is a decentralized approach to key distribution. Sharing of public keys or symmetric keys throughout the network is not needed. Any two routers having a primitive root α and a prime number p in common can initiate the key exchange. A simulation of the proposed approach is presented in Table 1. The basis of the proposed key exchange is discussed next.

A. Multi-stage Protocol

The proposed protocol is illustrated in Fig. 3. The security of the multi-stage protocol is based on the fact that a sender Alice and a receiver Bob each have their secret transformations (keys) that are only known to them, individually [11,12,13]. Routers 1(Alice) and 2 (Bob) initially share a large prime number p and its primitive root α. Knowledge of p and α by a cryptanalyst will not result in invalidating the proposed scheme. In any event, the parameters α and p are not global parameters shared among a large number of entities. They have only local significance. A few such combinations (of α and p) can be permanently embedded within router pairs. This will help them identify each other initially and thus prevent a possible man-in-the-middle attack. Once so identified, the two communicating entities can change the values of α and p at will or, if at all necessary, for example, after a major attack and/or system outage. The proposed scheme of key exchange now follows.

The key exchange initiating party, say Alice, chooses a random positive number x, where x is less than p. Alice then generates $\alpha^{x} mod\ p$ as the key to be shared. In other words, the key K can be represented as,

$$K = \alpha^{x} mod\ p \tag{2}$$

Simultaneously, Alice chooses another random number $i_1 < p$ and generates an intermediate number N as,

$$N = \alpha^{i_1} mod\ p \tag{3}$$

Alice also computes and stores N^{-1}, or the inverse of $N\ mod\ p$. While computation of the inverse of $N\ mod\ p$ might appear to be a formidable task, in practice, it isn't due to the following relationships.

$$N^{-1} = \alpha^{-i_1} = \alpha^{p-1-i_1} mod\ p \tag{4}$$

The latter relationship follows because for any prime number p and its primitive root alpha, we have,

$$\alpha^{p-1} = 1\ mod\ p \tag{5}$$

Equation (3) converts the inversion process to a simple exponentiation process.

Alice preserves the key K and the intermediate numbers $N = \alpha^{i_1} mod\ p$ and $N^{-1}\ mod\ p$ in a table.

On the first leg of transmission, Alice generates and transmits $L_1 = \alpha^{x+i_1}\ mod\ p$. This and the subsequent transmissions are shown in Fig. 3.

Bob has similarly chosen a random number $i_2 < p$ and generated the corresponding numbers $\alpha^{i_2} mod\ p$ and generated its inverse $\alpha^{-i_2} mod\ p$ following the procedure outlined for Alice. On the second leg from Bob to Alice, Bob generates and transmits, $L_2 = \alpha^{x+i_1+i_2}\ mod\ p$ as shown in Fig. 3.

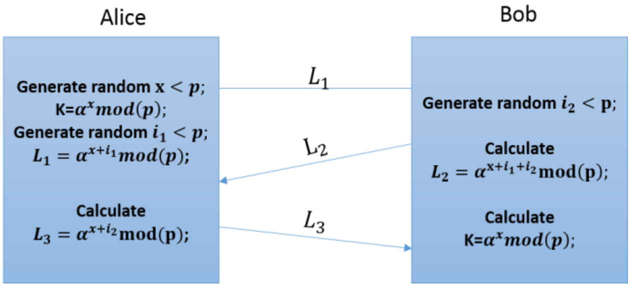

Alice
Bob
Generate random x < p;
K=$\alpha^x mod(p)$;
Generate random $i_1 < p$;
$L_1 = \alpha^{x+i_1} mod(p)$;
Calculate
$L_3 = \alpha^{x+i_2}$mod(p);
L_1
L_2
L_3
Generate random $i_2 <$ p;
Calculate
$L_2 = \alpha^{x+i_1+i_2}$mod(p);
Calculate
K=$\alpha^x mod(p)$;

Fig. 3. Key exchange scheme using discrete logarithms

Upon receiving L_2, Alice multiplies it by N^{-1} and getting $\alpha^{-i_1} mod\ p$, thus creating,

$$L_3 = \alpha^{x+i_1+i_2}\alpha^{-i_1}\ mod\ p = \alpha^{x+i_2}\ mod\ p \tag{6}$$

which she then transmits to Bob on the third leg.

Upon receiving L_3, Bob can easily evaluate the key K as, $K = L_3\alpha^{-i_2} = \alpha^{x} mod(p)$, which is the key Alice intended to share with Bob. Bob can similarly transmit a key to Alice.

A simulation of the values of L_1, L_2, and L_3 using Matlab has been done. The results for random values of i_1 and i_2 , $\alpha = 5, x = 15$, and $p = 97$ are shown in Table 1.

Table 1. Simulation of the key at Alice and Bob along with the value of each leg of the protocol

Cycle	Key At Alice's	i_1	i_2	L_1	L_2	L_3	Key at Bob's
1	46	0.958478	4.238835	89.08386	52.85938	46.83984	46
2	46	4.048701	7.071245	59.04688	58	57	46
3	46	1.851114	9.189888	75.58826	6	73	46
4	46	1.737055	7.436969	31.79602	32	53	46
5	46	2.544817	9.741039	27.98389	65	89	46
6	46	2.730982	10.93591	73.00684	66	91	46
7	46	0.983038	7.114608	37.65381	31	32	46
8	46	2.436789	5.763868	52.89453	65	71.375	46
9	46	3.325503	10.80495	92.74902	45	9	46
10	46	2.784334	5.076208	61.81592	81	27.75	46

B. Man in the middle attack on Multi-stage Protocols

In this section, the cryptographic strength of the proposed protocol is discussed by considering its vulnerability to the man in the middle attack. It can be noted from the previous section, that the key to be transmitted is based on a random number x. This random number is never transmitted into the open nor is the actual key, which is $\alpha^x mod\, p$. The transmission on the first leg L_1 is $\alpha^{x+i_1}\, mod\, p$, which is a logarithmic function of the key. An intruder having access to L_1 (see Fig. 3) is handicapped because $i_1$is an unknown quantity and even if the intruder had access to i_1, the intruder will still have to compute the discrete logarithm. The same level of difficulty is associated with the intruder's access to any of the three legs of transmission in isolation.

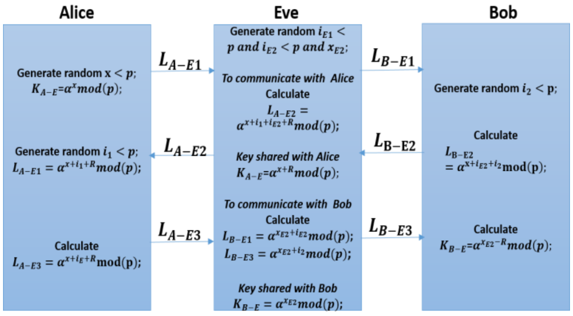

Alice
Eve
Bob
Generate random x < p;
K_{A-E}=$\alpha^x mod(p)$;
Generate random $i_1 < p$;
$L_{A-E1} = \alpha^{x+i_1+R} mod(p)$;
Calculate
$L_{A-E3} = \alpha^{x+i_E+R}$mod(p);
L_{A-E1}
L_{A-E2}
L_{A-E3}
Generate random $i_{E1} <$ p and $i_{E2} < p$ and x_{E2};
To communicate with Alice
Calculate
$L_{A-E2} =$ $\alpha^{x+i_1+i_{E2}+R} mod(p)$;
Key shared with Alice
K_{A-E}=$\alpha^{x+R} mod(p)$;
To communicate with Bob
Calculate
$L_{B-E1} = \alpha^{x_{E2}+i_{E2}} mod(p)$;
$L_{B-E3} = \alpha^{x_{E2}+i_2} mod(p)$;
Key shared with Bob
$K_{B-E} = \alpha^{x_{E2}} mod(p)$;
L_{B-E1}
L_{B-E2}
L_{B-E3}
Generate random i_2 < p;
Calculate
L_{B-E2} = $\alpha^{x+i_{E2}+i_2}$mod(p);
Calculate
K_{B-E}=$\alpha^{x_{E2}-R} mod(p)$;

Fig. 4. Man in the middle attack on the proposed system

The case of the intruder having access to each of the three legs of transmission at the same time is considered; in other words, the intruder can access *the* L_1, L_2 and L_3 messages that belong to the same information transmission (Fig.4). It is apparent from the three equations that, after some algebraic manipulation, capture of each of these three streams will result in the intruder Eve capturing $\alpha^x mod\, p$ which is the intended key. An intruder can make use of this access by either sharing the key $\alpha^x mod\, p$ with Alice, then sharing it with Bob. Or, the intruder can effect a man in the middle attack where he/she shares a key with Alice (K_{A_E}) and another key with Bob (K_{B_E}). This case is shown in Fig.4, and a simulation of the results L_{A_E1}, L_{A_E2}, and L_{A_E3} (transmissions between Alice and Eve), L_{B_E1}, L_{B_E2}, and L_{B_E3} (transmissions between Bob and Eve), using Matlab has been done. The results for random values of i_1, i_2, i_{E1}, and i_{E2} with $\alpha = 5, x = 15$, $x_{E2} = 20$, and $p = 97$ have been presented. As seen from Table 2, a secret key will be shared between Alice and Eve and a different secret key will be shared between Eve and Bob. During the communication Alice and Bob will not be able to detect the presence of Eve in the middle.

Table 2. Simulation of a successful man in the middle attack in case of a multi-stage protocol without an initialization vector

Cycle	Key shared between Alice and Eve	L_{A1}	L_{A2}	L_{A3}	L_{B1}	L_{B2}	L_{B3}	Key shared between Eve and Bob
1	46	40.56	44.5	79.70	18	69	50	93
2	46	8.32	39	30	60	34	72	93
3	46	68.18	65	56	29	38	42	93
4	46	40.31	37	33.62	87	96	44	93
5	46	23.75	87.12	10.65	5	88	40	93

These vulnerabilities are effectively addressed in the proposed protocol in the next section.

IV. Proposed Protocol Using An Initialization Vector And Its Cryptographic Strength

One can think of numerous ways to deny Eve from simultaneously accessing all of the three legs of the transmission. An obvious way is to send the information on each of the three legs on separate fibers or separate DWDM channels of one fiber. Furthermore, such assignments can be randomized.

Another way to frustrate Eve from accessing the key even after a successful capture of the three messages is to retain a subset of the last interchange of the key between Alice and Bob, and couple it with the new key $\alpha^x mod\, p$ to be transmitted with the following transformation, $\alpha^x\alpha^R mod\, p$, where α^R represents a remnant of the key successfully transferred during the last interchange. Since only Bob has access to R, he can easily derive the key $\alpha^x mod(p)$. In addition to providing security, use of the remnant R will also obviate any man-in-the-middle attack. It should be noted that since R is changing periodically, it is substantively different from the Initialization Vector used in conventional cryptography where it is fixed and therefore subject to a range of cryptanalytic attacks. The proposed approach is discussed in detail in the following section.

A. Description

As indicated in Section IV, the problem with the multi-stage algorithm is that if an intruder is present on all the stages of the communication at a given time, he/she will be able to get the ciphertext at each stage of the protocol [14]. Knowing the cipher text at each stage of the protocol, the intruder will be able to solve the following system of simultaneous equations:

$$L_1 = \alpha^{x+i_1}\, mod\, p = \mathrm{m} \qquad (7)$$

$$L_2 = \alpha^{x+i_1+i_2}\, mod\, p = \mathrm{m}' \qquad (8)$$

$$L_3 = \alpha^{x+i_2}\, mod\, p = \mathrm{m}'' \qquad (9)$$

where m, m$'$, and m$''$ are the values measured at L_1, L_2, and L_3 respectively. An underlying assumption, of course, is that α and p are known.

Since these are not global parameters, in the absence of inside information, Eve will be locked out from getting the key. In the following we address the situation when these parameters are available to the intruder and show how the use of the initialization vector will still prevent Eve from accessing the key.

In the previous section, we proposed a way to prevent such type of attacks by using a remnant from a previously used key α^R. Thus the number of stages of the protocol are only three, while the number of random variables used to protect the message are four. On the first leg of transmission, Alice generates and transmits $L_1 =$

$\alpha^{Ri_1} \, mod \, p$. On the second leg from Bob to Alice, Bob generates and transmits, $L_2 = \alpha^{R(i_1+i_2)} \, mod \, p$. Upon receiving L_2, Alice creates $L_3 = \alpha^{R(x+i_2)} \, mod \, p$ which she then transmits to Bob on the third leg. Bob has a prior knowledge of both R and i_2 thus he can recover the key sent over the channel.

Thus the set of equations that should be solved by an intruder tapping the channel can be presented as follows:

$$L_1 = \alpha^{Ri_1} \ mod \, p = \mathrm{m} \tag{10}$$

$$L_2 = \alpha^{R(i_1+i_2)} \, mod \, p = \mathrm{m}' \tag{11}$$

$$L_3 = \alpha^{R(i_2+x)} \, mod \, p = \mathrm{m}'' \tag{12}$$

Since it's impossible to solve for four unknown variables with only three equations, the key exchange is secure.

B. Mode Of Operation

We call $R_0[n]$ the initialization vector at iteration 0, cycle number n, $x_0[n]$ the bit value of the message being transferred, and $i_1^0[n]$ and $i_2^0[n]$ the values of the transformations (keys) at iteration 0, cycle number n, associated with the sender (Alice, 1) and receiver (Bob, 2), respectively. The initial length of R_0 is denoted by z, thus after z cycles R_0 will be updated to a new string of values R_1 of the same length as R_0 .

At iteration 0, cycle number n, the messages transmitted at $L_{1,0}$, $L_{2,0}$, and $L_{3,0}$ respectively are:

$$L_{1,0} = \alpha^{R_0[n] \, i_1^0[n]} \, mod \, p \tag{13}$$

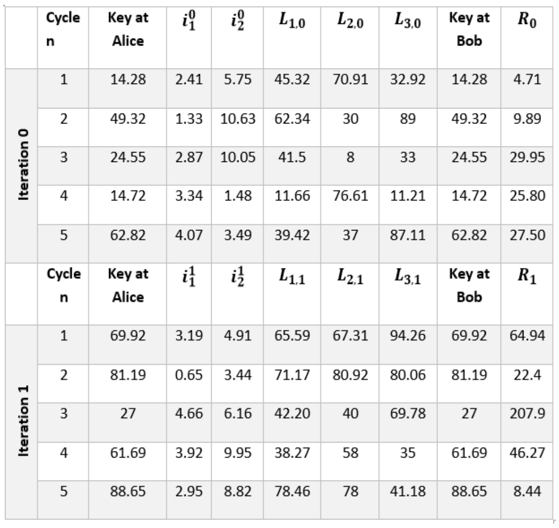
$$L_{2,0} = \alpha^{R_0[n](i_1^0[n]+i_2^0[n])} \, mod \, p \tag{14}$$

$$L_{3,0} = \alpha^{R_0[n](X_0[n]+i_2^0[n])} \, mod \, p \tag{15}$$

It should be noted that the key to be transmitted $K_0[n] = \alpha^{X_0[n]} \, mod \, p$ has been used only in the last leg. This approach can also be used in the set of equations where the initialization vector R_0 was not used. Potentially, this is an additional deterrent to a cryptanalyst.

At the next cycle, Alice will use a new transformation set $i_1^0[n+1]$ and Bob should use $i_2^0[n+1]$ and a next value in the string of the initialization vector $R_0[n+1]$ will be used. It is worth noting that Alice and Bob do not have any restrictions on the transformations associated with R, and it does not need to commute with $i_1^0[n+1]$ and $i_2^0[n+1]$. Furthermore, it is worth noting that Alice and Bob can use the bits of R in any desired order as long as there has been a previous agreement on the way of using them. The operation of the proposed approach is depicted in Fig. 5. A simulation of the proposed approach is presented in Table 3 for random i_1, i_2 , and x, with $\alpha = 5$, $x_{E2} = 20$, and $p = 97$.

Table 3. Simulation of the operation of the multi-stage protocol using an initialization vector R



	Cycle n	Key at Alice	i_1^0	i_2^0	$L_{1,0}$	$L_{2,0}$	$L_{3,0}$	Key at Bob	R_0
Iteration 0	1	14.28	2.41	5.75	45.32	70.91	32.92	14.28	4.71
	2	49.32	1.33	10.63	62.34	30	89	49.32	9.89
	3	24.55	2.87	10.05	41.5	8	33	24.55	29.95
	4	14.72	3.34	1.48	11.66	76.61	11.21	14.72	25.80
	5	62.82	4.07	3.49	39.42	37	87.11	62.82	27.50
	Cycle n	Key at Alice	i_1^1	i_2^1	$L_{1,1}$	$L_{2,1}$	$L_{3,1}$	Key at Bob	R_1
Iteration 1	1	69.92	3.19	4.91	65.59	67.31	94.26	69.92	64.94
	2	81.19	0.65	3.44	71.17	80.92	80.06	81.19	22.4
	3	27	4.66	6.16	42.20	40	69.78	27	207.9
	4	61.69	3.92	9.95	38.27	58	35	61.69	46.27
	5	88.65	2.95	8.82	78.46	78	41.18	88.65	8.44

After the addition of an extra dimension to the multi-stage protocol proposed in the previous section it is possible to consider it as a continuously refreshing key since, at each stage of the protocol, a new secret variable is added in order to secure the outcome of the previous stage. An eavesdropper having simultaneous access to the three stages of the protocol will not be able to compute the value of the sent bit, since he/she will be faced with the problem of solving a system of three equations with four variables. In addition, such an approach makes it impossible to launch a man in the middle attack.

The addition of an initialization vector to the three-stage protocol can be regarded as a door function to protect the message sent over the channel. Any illegitimate user is denied the ability of retrieving the value of the bit sent over the channel as long as he/she does not possess the value of the door function.

C. A Two-Stage Protocol

The protocol proposed in Section IV.B can be further reduced into a two-stage protocol if one allows the communication to start at Bob's side and end at Bob's side as well (shown in Fig. 6). The protocol proceeds as follows: Alice and Bob initially share a large prime number p and its primitive root α and an initialization vector R of length z to proceed with the first iteration of the protocol. Knowledge of p and α by a cryptanalyst will not result in invalidating the proposed scheme, while R is only known to Alice and Bob as a remnant from a previous exchange. In any event, the parameters α , p , and R are not global parameters shared among a large number of entities. They have only local significance. As before, a few such combinations (of α and p) can be permanently embedded within router pairs. The key exchanging party, say Alice, chooses a random positive number x, where x is less than p. Alice then generates $\alpha^x mod \, p$ as the key to be shared. In other words, as stated earlier, the key K

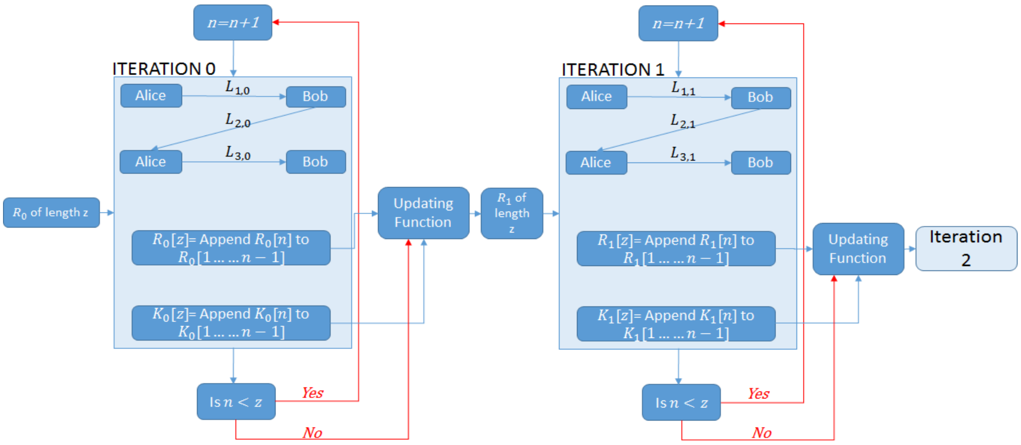


Fig. 5. The operation of the multi-stage protocol using four variables

can be represented as,

$$K = \alpha^{x} mod\ p \qquad (16)$$

As discussed before, the key at the first iteration is denoted by $K[n]_0 = \alpha^{X_0[n]}\ mod\ p$. Bob starts the communication by sending $L_1 = \alpha^{Ri_2}\ mod\ p$, where i_2 a random integer and is known only to Bob. Upon receiving the message, Alice encodes $\alpha^{x} mod\ p$, which is the key to be transmitted, and protects the message using the initialization vector R , and sends $L_2 = \alpha^{R(x+i_2)}\ mod\ p$ to Bob. Bob receives the message his prior knowledge of R and i_2 gives him the ability to decode the message sent from Alice.

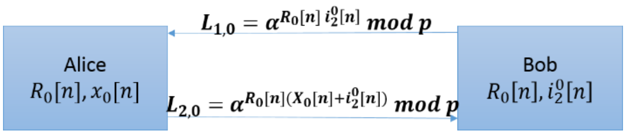

$L_{1,0} = \alpha^{R_0[n]\, i_2^0[n]}\ mod\ p$
Alice
$R_0[n], x_0[n]$
$L_{2,0} = \alpha^{R_0[n](X_0[n]+i_2^0[n])}\ mod\ p$
Bob
$R_0[n], i_2^0[n]$

Fig. 6. Key exchange scheme using the two-stage protocol (iteration zero cycle n)

The initialization vector R is updated periodically to insure a fully secure information transfer between Alice and Bob.

$R_0[n]$ is the initialization vector at iteration 0 cycle number n , $x_0[n]$ the bit value of the message being transferred, $i_2^0[n]$ the values of the transformations (keys) at iteration 0 cycle number n of the receiver (Bob). The initial length of R_0 is denoted by z, thus after z cycles R_0 will be updated to a new string of values R_1 , of the same length.

At iteration 0 cycle number n the messages transmitted at $L_{1,0}$, and $L_{2,0}$ are:

$$L_{1,0} = \alpha^{R_0[n]\, i_2^0[n]}\ mod\ p \qquad (17)$$

$$L_{2,0} = \alpha^{R_0[n](X_0[n]+i_2^0[n])}\ mod\ p \qquad (18)$$

At the next cycle Bob will use $i_2^0[n+1]$ and the next value in the string of the initialization vector $R_0[n+1]$ will be used. It is worth noting that Alice and Bob do not have any restrictions on the transformations associated with R , it can be an addition to the exponent, a multiplication or any other mathematical transformation.

At the end of each iteration an updating function having its inputs as the randomly generated key K and the initialization vector R is used to generate a new initialization vector to be used in the next iteration. As shown in Fig.7, R_0 is used to generate the key at iteration 0. Then, using $R_0$and K_0 the updating function generates a new initialization vector R_1 of length z to be used for iteration 1.

D. Braiding Concept

The concept of using different versions of the multi-stage protocol in the same communication called the braiding function was introduced in [15], and is shown in Fig. 8. Braiding is the concept of sharing keys between two parties using different number of stages, m. Alice and Bob can agree on how many stages to use at the onset of the key distribution process. The variability associated with m (which can be changed at will by the communicating parties) will be an additional means of frustrating the eavesdropper Eve.

In Fig. 8, the braiding concept of multi-stage protocols is shown. Given an initialization vector R_0 of length z Alice and Bob execute a multi-stage protocol with m=3 for z cycles. Then after sharing a key K_0 of length z, the initialization vector R_0 is updated into R_1 using an updating function. The new initialization vector R_1 is based on both K_0 and R_0. R_1 is now used to do the next iteration of the key distribution process. At this iteration Alice and Bob use $m = 2$ to share K_1.

E. Man In The Middle Attack On A Multi-Stage Protocol Using An Initialization Vector

In this section, we show that a multi-stage protocol

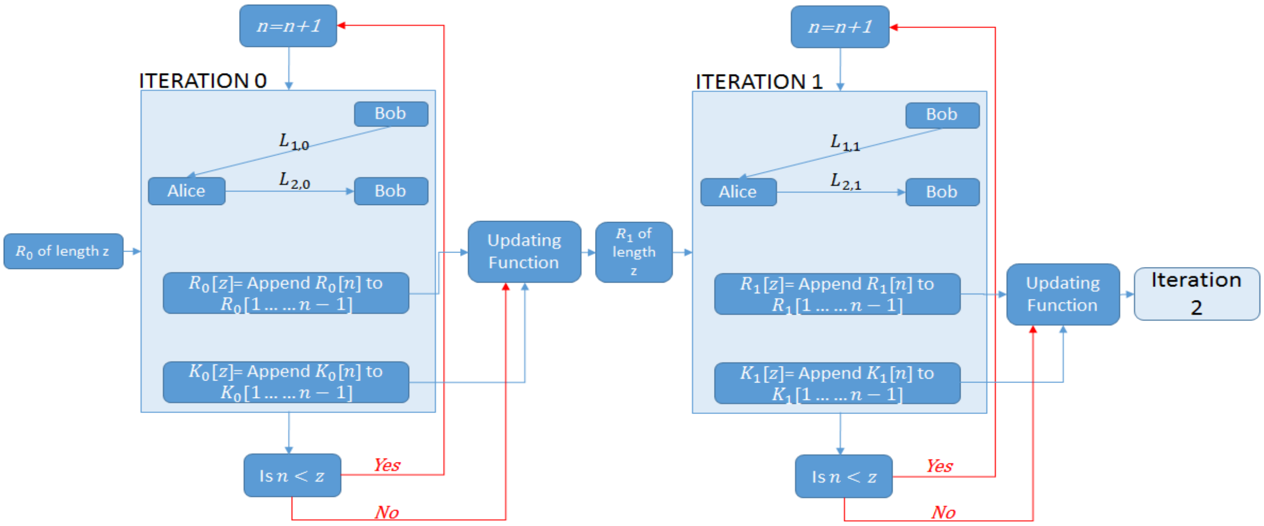


Fig. 7. The operation of the multi-stage protocol using three variables

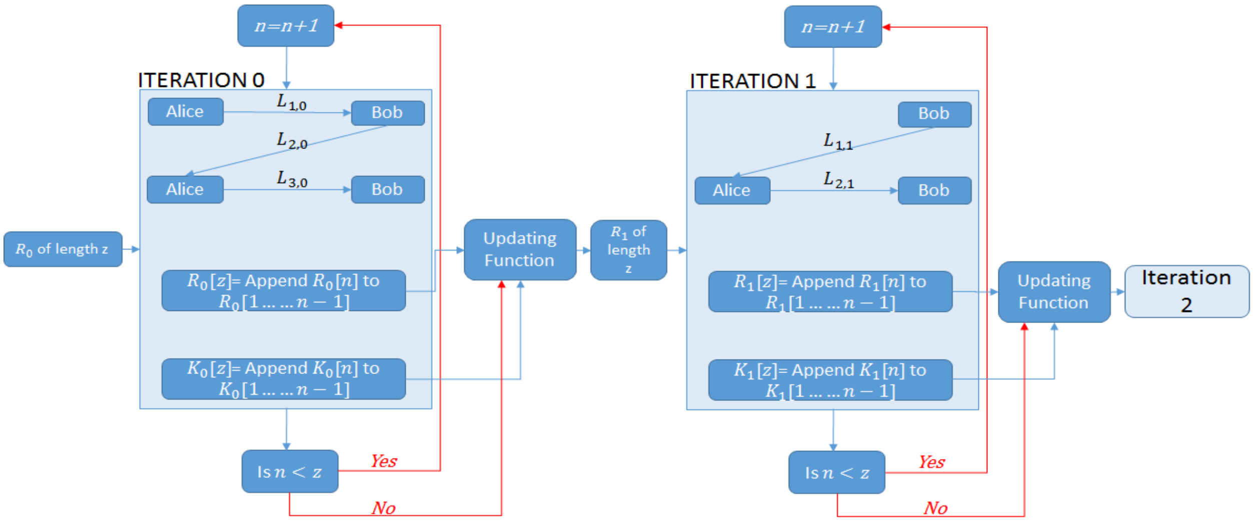


Fig. 8. The operation of the braided multi-stage protocol

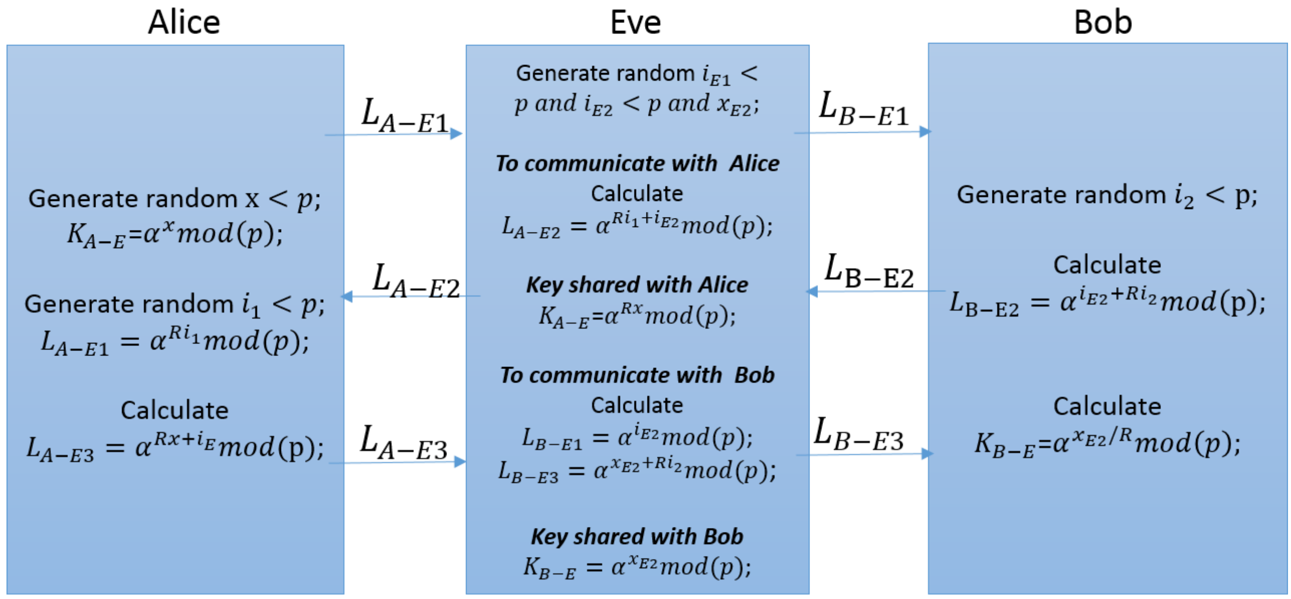

Alice
Eve
Bob
Generate random x < p;
$K_{A-E}=\alpha^{x} mod(p)$;
Generate random $i_1 < p$;
$L_{A-E1} = \alpha^{Ri_1} mod(p)$;
Calculate
$L_{A-E3} = \alpha^{Rx+i_E} mod(p)$;
L_{A-E1}
L_{A-E2}
L_{A-E3}
Generate random $i_{E1} < p$ and $i_{E2} < p$ and x_{E2};
To communicate with Alice
Calculate
$L_{A-E2} = \alpha^{Ri_1+i_{E2}} mod(p)$;
Key shared with Alice
$K_{A-E}=\alpha^{Rx} mod(p)$;
To communicate with Bob
Calculate
$L_{B-E1} = \alpha^{i_{E2}} mod(p)$;
$L_{B-E3} = \alpha^{x_{E2}+Ri_2} mod(p)$;
Key shared with Bob
$K_{B-E} = \alpha^{x_{E2}} mod(p)$;
L_{B-E1}
L_{B-E2}
L_{B-E3}
Generate random $i_2 <$ p;
Calculate
$L_{B-E2} = \alpha^{i_{E2}+Ri_2} mod(p)$;
Calculate
$K_{B-E}=\alpha^{x_{E2}/R} mod(p)$;

Fig. 9. Man in the middle attack on the Multi-stage using an Initialization Vector

using an initialization vector is not vulnerable to the man in the man in the middle attack. The man in the middle attack stage protocol is shown in Fig. 9. Table 4 shows the keys at Alice, Bob and Eve for i_1, i_2 , i_{E1}, and i_{E2} with $\alpha = 5, x = 15$, $x_{E2} = 20$, and $p = 97$, the simulation presented in this table. As shown from the table the key at Alice is different than the key that Eve will attempt to use while communicating with Alice (shown in blue). The same case applies to Eve and Bob as well (shown in red). This is due to the initialization R_0 vector used by Alice and Bob.

Table 4. Man in the middle attack to a multi-stage protocol using an initialization vector

Cycle	Key at Alice	L_{A-E1}	L_{A-E2}	L_{A-E3}	Key Alice-Eve	Key Eve-Bob	L_{B-E1}	L_{B-E2}	L_{B-E3}	Key at Bob
1	46	44.42	93	61	63.12	61	42	93	86.87	93
2	46	36.50	5	37	75.29	80.62	33	68	70	93
3	46	15.78	33	61	50.01	45.75	46	34	91	93
4	46	81.95	16	52.24	33.19	60.34	36	46	46	93
5	46	69.21	26	54	4.04	33.81	35	8	22	93

F. *Characteristics of the Proposed Protocol*

The protocol proposed in this paper is a multi-stage ultra-secure router-to-router spontaneous key exchange system. This protocol represents a decentralized approach to conventional key distribution schemes and is meant for use on a link-by-link basis between two communicating parties. In other words, the overhead of sharing public keys throughout the network is obviated as well as the need of a third party to distribute secret keys between the nodes of the network.

The proposed protocol is based on the usage of random number generators. Two random number generators at both Alice's and Bob's side are needed to generate i_1 and i_2, respectively. Furthermore, the security of the proposed approach against a man in the middle attach is guaranteed as long as an initialization vector is already in the possession of the communicating parties at the time communication first starts. This initialization vector can be embedded in each of the two communicating router pairs by the manufacturer, and then updated as often as chosen by the communicating routers.

Finally, the multi-stage protocol requires several transmissions on the channel depending on the number of stages m agreed on between Alice and Bob. Such requirement can be considered as an additional strength associated with the protocol, since, in a braided scheme, it can frustrate an eavesdropper who is unaware of the value of m.

V. Comparison with QKD Systems

Quantum key distribution systems are commercially available from at least two suppliers: MagiQ Systems [16] and IdQuantique [17], based in Boston, MA in the US, and in Geneva, Switzerland, respectively. Both these manufacturers use the BB'84 protocol [18], first discovered in 1984, and first manufactured for commercial applications in 2005. Currently available QKD equipment are based on single photons each carrying one bit of information. Since it's impossible to generate single photons with defined periodicity [19], a practical way to closely approach it is by way of reducing the beam strength to such a low value that photons are generated very sparsely and the corresponding probability of having two or more photons in a single time slot is arbitrarily small. This, of course, creates two problems. The rate at which information can be transmitted is relatively modest to the tune of a few kilobits per second. Furthermore, since the carrier is a single photon, the distance over which it can be detected with integrity is limited to about 100 km in an optical fiber. Additionally, other environmental restrictions also limit its use to all but a few commercial applications. It's unlikely that the currently available QKD techniques will notice an observable spike in their applicability space.

In comparison, the proposed system is based on a classical method of encryption and does not require a quantum channel. The key distribution can take place over the same medium that carries the payload and the speed of transmission is the same as that of the payload. There are no restrictions on the intervening medium of any kind. Even if the two routers were not directly connected or even with the intervening medium consisting of different technologies in tandem, e.g., EPON, DWDM, Wireless, etc., the process described does not change. Very importantly, the key exchange can take place as often as desired making the proposed system offer security comparable to quantum key distribution techniques.

VI. Conclusions and Future Work

This paper has presented an ultra-secure router-to-router key exchange system using multi-stage protocols. The key exchange process can be initiated by either party at will and can be carried out as often as necessary. The proposed system is based on the use of discrete logarithms. The main cryptographic strength of the proposed protocols lies in the use of multi-stage transmission where the number of variables exceeds the number of stages by one, ensuring that the number of possible measurements is one less that the number of variables. This makes the key transfer secure. Furthermore, since the keys can be exchanged as often as necessary at the payload speed, one can stipulate that the security of the proposed system approaches that of contemporary QKD systems. In other words, the level of security attainable by the proposed system is comparable to QKD systems but without the baggage of limited distance and low speed associated with the latter. Recent literature in quantum-secure communication in a multi photon environment [12-15] has suggested that the multi-photon approach can offer quantum level security obviating the need for single photon generators and thus removing the speed and distance barrier caused by single photons. This paper has shown that a cryptographic strength similar to the multi-photon approach is attainable in electronics as well.

The proposed technique has used discrete algorithms as the base for secure communication. Another possible technique can be based on the use of elliptic curve cryptography [18] while augmenting it with the use of a similar multi-stage protocol. The latter technique will offer a comparable cryptographic strength.

ACKNOWLEDGMENT

This research was supported in part by the National Science Foundation (NSF) under Grant 1117179.

REFERENCES

[1] Kaicheng Lu, Computer cryptography "Computer network data privacy and security." Tsinghua University Press, 2003.

[2] Stallings, W., "Cryptography and Network Security: Principles and Practice." Prentice Hall, 5th edition copyright 2011,2006,2003 pp. 52,53.

[3] Ore, O. "Invitation to Number theory." Washington, DC: The mathematical Association of America, 1967.

[4] Rosen, K. "Elementary Number theory and its Applications." Reading, MA: Addision-Wesley, 2010.

[5] Beth,T.;Frisch,M.;and Simmons,G.; "eds.Public-key Cryptography:state of the Art and Future Directions". New York: Springer-Verlag, 1991 .

[6] Diffie W., and Hellman M., "New directions in Cryptographiy." IEEE trans. in Information Theory, 22(1976), 644-654.

[7] Diffie W. and Hellman M., "Exhaustive cryptanalysis of the NBS data encryption strandard." Computer 10(6) (June 1977), 74-84.

[8] Popek, G., and Kline,C. " Encryption and secure compute Netwrorks." ACM computering surveys, December 1979.

[9] Merkle, R. "Secrecy,Authentication, and public key sharing." PhD. Thesis , Stanford University , June 1979.

[10] Needham, R., and Schroeder, M. "Using Encryption for Authentication in Large Networks of Computers." Communications of the ACM, December 1978.

[11] Kak, S.: A "Three-stage Quantum Cryptography Protocol". Foundations of Physics Letters 19, 293, 2006.

[12] Mandal, Sayonnha, et al. "Implementation of Secure Quantum Protocol using Multiple Photons for Communication." arXiv preprint arXiv:1208.6198 (2012).

[13] Yuhua Chen; Kak, S.; Verma, P.K.; Macdonald, G.; El Rifai, M.; Punekar, N., "Multi-photon tolerant secure quantum communication — From theory to practice." Communications (ICC), 2013 IEEE International Conference on, vol., no., pp.2111,2116, 9-13 June 2013.

[14] El Rifai, M.; Verma, P.K., "An Algorithmic Approach to Securing the Three-Stage Quantum Cryptography Protocol." Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, vol., no., pp.1803,1807, 16-18 July 2013.

[15] Bhagyashri Darunkar ; Pramode Verma; "The braided single-stage protocol for quantum secure communication" Proc. SPIE 9123, Quantum Information and Computation XII, 912308 (May 22, 2014); doi:10.1117/12.205016 .

[16] http://www.magiqtech.com/Products_files/8505_Data_Sheet.pdf.

[17] http://www.idquantique.com/scientific-instrumentation/ cla vis 2 -qkd-platform.html.

[18] Bennett, Ch. H., Brassard, G. "Quantum Cryptography: Public Key Distribution and Coin Tossing." IEEE Conference on Computer, Systems, and Signal Processing, 1984, pp. 175-90.

[19] Kollmitzer, C., Pivk, M. (Eds) "Applied Quantum Cryptography" Lect. Notes Phys. 797 Berlin Heidelberg; New York: Sprigner, c2010 pp 101-102.

[20] L. Washington, "Elliptic Curves: Number Theory and Cryptography" Chapman & Hall/ CRC Press, 2003.

Authors' Profiles

Pramode Verma (StM'67–M'70–SM'74) is Professor and Director of the Telecommunications Engineering Program in the School of Electrical and Computer Engineering of the University of Oklahoma-Tulsa. He also holds the Williams Chair in Telecommunications Networking. Prior to joining the University of Oklahoma in 1999 as the founder-director of a graduate program in Telecommunications Engineering, Dr. Verma held a variety of professional, managerial and leadership positions in the telecommunications industry at AT&T Bell Laboratories and Lucent Technologies. He is the author/co-author of over 150 journal articles and conference papers, and several books in telecommunications engineering. He is also the co-inventor of eight patents with several patents pending. He regularly serves on NSF panels and has been an External Examiner for Ph.D. theses at the University of Cape Town, South Africa, University of Ottawa, and Carleton University, Ottawa. He has been a keynote speaker at several international conferences and has lectured in several countries. He received the University of Oklahoma-Tulsa President's Leadership Award for Excellence in Research and Development in 2009. He is a Senior Member of the IEEE and a Senior Fellow of The Information and Telecommunication Education and Research Association. He obtained his Ph.D. in 1970 from the Concordia University in Montreal, Canada, and an MBA from the Wharton School, University of Pennsylvania in 1984.

Mayssaa El Rifai is a Ph.D. Candidate in the School of Electrical and Computer Engineering of the University of Oklahoma-Tulsa. She received her B.Sc. degree in Computer and Communication Engineering from the Hariri Canadian University- Lebanon in 2010. She received her M.Sc. from in Telecommunication from The University of Oklahoma-Tulsa. El Rifai has been a graduate research assistant at The University of Oklahoma since 2011. Her research is focused in Quantum communication using multi-photon, and Quantum key distribution protocols.

Manuscript received March 4, 2015; revised April 13, 2015; accepted July 21, 2009.