Journal of the Optical Society of Korea
Vol. 20, No. 1, February 2016, pp. 55-63

ISSN: 1226-4776(Print) / ISSN: 2093-6885(Online)
DOI: http://dx.doi.org/10.3807/JOSK.2016.20.1.055

Asymmetric Public Key Cryptography by Using Logic-based Optical Processing

Sang Keun Gil*

Department of Electronic Engineering, The University of Suwon, Whasung 440-600, Korea

(Received September 8, 2015 : revised November 20, 2015 : accepted December 10, 2015)

In this paper, a new asymmetric public key cryptography based on the modified RSA algorithm is proposed by using logic-based optical processing. The proposed asymmetric public key algorithm is realized into an optical schematic, where AND, OR and XOR logic operations are implemented by using free space digital optics architecture. Schematically, the proposed optical configuration has an advantage of generating the public keys simultaneously. Another advantage is that the suggested optical setup can also be used for message encryption and decryption by simply replacing data inputs of SLMs in the optical configuration. The last merit is that the optical configuration has a 2-D array data format which can increase the key length easily. This can provide longer 2-D key length resulting in a higher security cryptosystem than the conventional 1-D key length cryptosystem. Results of numerical simulation and differential cryptanalysis are presented to verify that the proposed method shows the effectiveness in the optical asymmetric cryptographic system.

Keywords : Optical encryption, Optical logic, RSA cryptosystem, Asymmetrical public key, Cryptography
OCIS codes : (070.4560) Data processing by optical means; (100.3010) Image reconstruction techniques; (200.2610) Free-space digital optics; (200.3760) Logic-based optical processing; (200.4660) Optical logic

I. INTRODUCTION

Nowadays as public communication networks such as the internet and mobile networks develop, there has been a strong need for information security. However, because the public network is not secure from information cracking, important personal information such as IDs and passwords are hacked. For this reason, information security of the public network has become a great issue. In order to solve this security problem, various kinds of cryptography algorithms have been proposed for cipher systems. One of the cryptography protocols was a symmetric key encryption method. In this method, two users share a secret private key in advance, and then they transmit cipher messages over the public network by using this private key in plain message encryption. However, the symmetric private key may be intercepted by an unauthorized user because this type of cryptosystem has only one-key. To solve this problem, public key cryptography such as Diffie-Hellman key exchange protocol was introduced [1]. In this protocol, two users unknown to each other can set up a public key for their asymmetric key(two-key) exchange cryptosystem and share a secret key. However, this private key can be attacked because this shared secret key is used to encrypt messages by applying the symmetric cryptography. Therefore, an advanced algorithm such as 3DES(triple Data Encryption Standard) [2] or asymmetric RSA public key cryptography [3] was introduced to enhance security strength, using two-key encryption.

In general, the electronic cryptosystem is slow and requires much time to compute the encryption procedure if the key length is very long and two-key encryption is adopted. In contrast the optical cryptosystem has advantages of fast processing and vast data encryption. In recent years, there have been a number of optical encryption methods for cryptographic systems [4-16] and several optical asymmetric key cryptosystems have been presented [17-21]. Also, we have presented several papers on the optical encryption technique by using Boolean logic-based operations [22-23], and we have recently reported on the optical modified Diffie-Hellman key exchange protocol [24]. These asymmetric cryptographic methods enhance the security greatly against

*Corresponding author: skgil@suwon.ac.kr
Color versions of one or more of the figures in this paper are available online.

attacks. Therefore, there is still interest in research to present an optical method of asymmetric public key cryptography.

In this paper, a modified asymmetric RSA public key cryptography by using logic-based optical processing is proposed and the performance of the proposed method is shown. The proposed algorithm is implemented into an optical schematic by using dual free-space interconnected optical logic operations. Section II is organized as three parts. In the first part, the RSA public key cryptography algorithm is overviewed. The second part explains the proposed asymmetric cryptography. In the third part, the optical schematic of the proposed asymmetric cryptosystem is proposed and the optical cryptographic process is explained. In Section III, numerical simulations and differential cryptanalysis prove the performance by showing results of the proposed optical asymmetric cryptosystem with the modified algorithm. Finally, conclusions are briefly summarized in Section IV.

II. THEORY

2.1. RSA Public Key Cryptography

The idea of an asymmetric public-private key cryptosystem is attributed to Diffie and Hellman, who published the concept in 1976 [1]. However, they left open the problem of realizing a one-way function, possibly because the difficulty of factoring was not well studied at the time. R. Rivest, A. Shamir, and L. Adleman made several attempts to create a one-way function that is hard to invert. This asymmetrical public key cryptography is now known as the RSA algorithm. RSA is made of the initial letters of the surnames in the same order as on their paper where they first publicly described the algorithm in 1978 [3]. RSA is one of the first practical public key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key, which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. A user of the RSA cryptosystem creates and then releases a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but the encrypted cipher message cannot be decrypted without knowing the private decryption key.

The RSA public key algorithm allows two users to transmit a cipher text over an insecure communications medium. For example, two users (i.e., Alice and Bob) wish to exchange messages each other but do not want an eavesdropper (i.e., Eve) to know their message. To do this, they will agree upon and set up a random public-private key for their cryptosystem. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted by using the corresponding private key. The RSA algorithm involves three steps as follows: key generation, encryption and decryption.

1. Bob chooses two distinct prime numbers p and q. Note that not anyone can access these numbers in public. For security purposes, the integers p and q should be chosen at random.
2. Bob computes $n = pq$, where n is used as the modulus for both the public and private keys. Its length, usually expressed in one-dimensional (1-D) bits, is the key length.
3. Bob computes $\mathbf{f}(n) = (p - 1)(q - 1)$, where $\mathbf{f}(\bullet)$ is Euler's totient function. This value is kept secret.
4. Bob chooses an integer e and determines an integer d such that $ed = 1 \bmod \mathbf{f}(n)$; i.e., e and $\mathbf{f}(n)$ are coprime and d is the modular multiplicative inverse of e (modulo $\mathbf{f}(n)$). Bob releases $\{e\}$ as a public key exponent, and $\{d\}$ is kept secret as a private key exponent.
5. Alice encrypts a plain text **P** with public key $\{n, e\}$ by modulo n and sends it to Bob.

$$C = P^e \bmod n \tag{1}$$

6. Bob decrypts a cipher text **C** with private key $\{n, d\}$ by modulo n.

$$P = C^d \bmod n \tag{2}$$

Figure 1 shows the asymmetric RSA public key cryptography algorithm. As you see in Fig. 1, Bob chooses two distinct prime numbers p, q and sends the computed values $\{n, e\}$ to Alice as public key while he keeps $\{\mathbf{f}(n), d\}$ secret as private key. With these public keys, Alice encrypts a plain text **P** and sends it to Bob. After receiving Alice's cipher text, Bob decrypts a cipher text **C** with the private key $\{d\}$ by modulo n. If Eve wants to decrypt the cipher text **C**, she would need both the random number p and the random number q. Even though Eve notices the public key set $\{n, e\}$, it is not easy to get Alice's plain text **P** from the set $\{n, e\}$ because she doesn't know the private key $\{d\}$. Besides, there is no known algorithm to

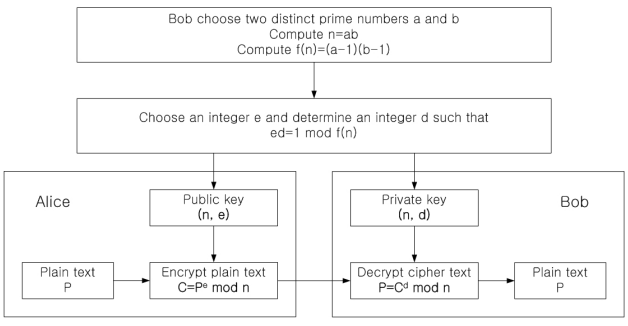

FIG. 1. Asymmetric RSA public key cryptography algorithm.

accomplish this problem in a reasonable amount of time. If the prime numbers p and q are large enough, a fair amount of time is needed to solve this RSA problem and it is not efficient and practical to calculate solution by using brute force attack.

2.2. Proposed Asymmetric Cryptography

Basically, it is very difficult for the RSA algorithm to be implemented by optical means due to two main reasons. The first one is that there is no proper method to perform modulo arithmetic by optical techniques. The second is that it is hard to represent a prime number onto an optical device properly. It may be possible to encode the prime number into binary digits by conversion. Despite these difficulties, an optical asymmetric public key cryptographic method is proposed in this paper by modifying the conventional RSA algorithm. In the proposed method, the conventional RSA algorithm can be modified to an optically realizable algorithm, where modulo arithmetic can be simply substituted with a logic-based optical processing. Therefore, modulo arithmetic is mathematically replaced by the XOR logic operation, that is, modulo two addition. Specifically, XOR-only encryption schemes will be perfectly secure if and only if the key data is perfectly random and never reused [23]. When the logic-based optical processing such as AND, OR and XOR operations is applied to the above RSA algorithm, the modified asymmetric algorithm can be described as follows.

1. Alice and Bob agree upon and share a common key number S secretly.
2. Bob chooses two distinct random numbers A and B, where A and B are generated randomly instead of as prime numbers. Note that anyone cannot access these numbers in public. For security purposes, the integers A and B should be chosen at random.
3. Bob computes $N = A \cdot B$ by Boolean AND logic operation. N is used as modulo of the XOR logic-based operation for both the public and private keys. Its length, usually expressed in two-dimensional (2-D) bits, is the key length.
4. Bob computes $F = A + B$ by Boolean OR logic operation. This value is kept secret.
5. Bob computes $K = N \oplus F \oplus S$ by Boolean XOR logic operation.
6. Bob chooses a random number D as a decryption key and determine a random number E such that $E \oplus D = K$, i.e., $E = K \oplus D$ and $D = K \oplus E$. Bob releases $\{N, E\}$ as public keys, and $\{F, D\}$ are kept secret as private keys.
7. Alice encrypts a plain text **P** with the public keys $\{N, E\}$ and shared key $\{S\}$ by the XOR logic-based operation and sends it to Bob.

$$C = P \oplus N \oplus E \oplus S \tag{3}$$

8. Bob decrypts a cipher text **C** with private keys $\{F, D\}$ by the XOR logic-based operation.

$$P = C \oplus F \oplus D \tag{4}$$

Figure 2 shows the modified asymmetric public key cryptography algorithm by using logic-based processing, and Fig. 3 shows the flow charts for the proposed asymmetric cryptographic method. As shown in Fig. 2 and Fig. 3, suppose that Alice and Bob agree upon and share a common key number S. First step is public key generation which is shown as Fig. 3(a). Firstly, Bob generates two distinct random numbers A and B which are not open to the public. Secondly, with these numbers, Bob computes $N = A \cdot B$ and $F = A + B$ by logic operations. Thirdly, Bob computes K by XOR logic operation as follows.

$$K = N \oplus F \oplus S = (A \cdot B) \oplus (A + B) \oplus S = A \oplus B \oplus S \tag{5}$$

In order to get public-private key pairs, Bob chooses a random number D as a decryption key and determines a random number E such that

$$E \oplus D = K \tag{6}$$

$$E = K \oplus D = N \oplus F \oplus S \oplus D = A \oplus B \oplus S \oplus D \tag{7}$$

$$D = K \oplus E = N \oplus F \oplus S \oplus E = A \oplus B \oplus S \oplus E \tag{8}$$

Now, Bob releases $\{N, E\}$ as public keys and keeps $\{F, D\}$ secret as private keys.

The second step is Alice's encryption of plain text which is shown as Fig. 3(b). With Bob's public keys $\{N, E\}$, Alice computes an encryption key A_k and encrypts a plain text **P** into a cipher text **C** by XOR logic operation as follows.

$$\begin{aligned} A_k &= N \oplus E \oplus S = AB \oplus (A \oplus B \oplus S \oplus D) \oplus S \\ &= (A + B) \oplus D \end{aligned} \tag{9}$$

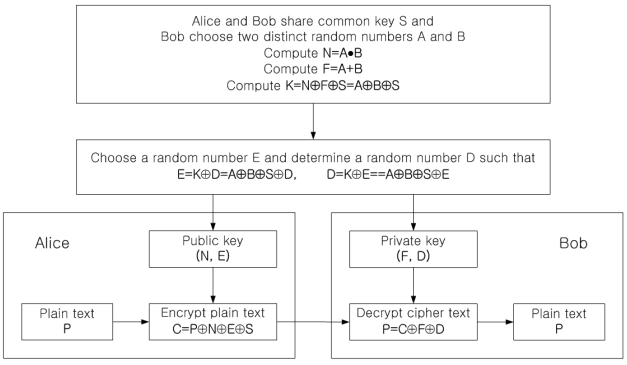

FIG. 2. Modified asymmetric public key cryptography algorithm by using logic-based processing.

$$C = P \oplus A_k = P \oplus (N \oplus E \oplus S) \\ = P \oplus (A + B) \oplus D = P \oplus F \oplus D \quad (10)$$

Equation (10) means that the plain text cannot be decrypted if we do not know the private keys ***F*** and ***D***, which are not open to the public as Bob's private keys.

The third step is Bob's decryption of the cipher text which is shown as Fig. 3(c). In the proposed asymmetric cryptography algorithm, the decryption can be easily accomplished by using the similar procedure as key generation which is shown as Fig. 3(a). Bob uses still two distinct random numbers ***A*** and ***B*** which are already set in the key generation step, and computes ***F*** = ***A*** + ***B***. Next, by replacing the common key ***S*** with the cipher text **C**, Bob computes a decryption key $\boldsymbol{B_k}$ and decrypts the cipher text **C** into the plain text **P** by XOR logic operation as follows.

$$B_k = (A + B) \oplus D = F \oplus D \quad (11)$$

$$R = C \oplus B_k = (P \oplus F \oplus D) \oplus (F \oplus D) = P \quad (12)$$

Also, Fig. 3 shows that the proposed asymmetric cryptography has a realizable optical schematic by using logic-based optical processing. In the proposed method, an XOR-based double encryption technique is used. This technique is very similar to the 3DES algorithm and was reported in the previous paper [22]. From Eq. (10), the cipher text **C** contains two security keys. One is the decryption key ***D***, the other is the private key ***F*** = ***A*** + ***B***. Double encryption by two security keys gives us much security strength and is much harder to break the key. If an eavesdropper wants to compute the private key ***F***, he/she must know both the random number ***A*** and the random number ***B***. Although eavesdropper notices the public key set {***N***, ***E***}, which is now open to public, it is hard to get ***A*** and ***B*** from the set {***N***, ***E***} because these secret random numbers are pre-encrypted by AND logic-based operation and XOR logic-based operation, respectively. Another important view on the security strength concerns the key length. The security of a cryptosystem is a function of the length of the key. Assuming there is no better way to break the cryptosystem, other than to try every possible key with a brute force attack, the longer the key is, the longer it will take to make the number of attacks necessary to find the correct key. In fact, every extra key bit generally doubles the number of possible keys and therefore increases the effort required for a successful brute force attack against most key algorithms. Generally, a key length of N bits means that 2^N attempts are required. About the proposed asymmetric algorithm in this paper, the longer the length of these random numbers (A and B) are, then the more time the eavesdropper requires to break. Thus increase of key length improves the security and results in the robustness against the cipher-text-only attack.

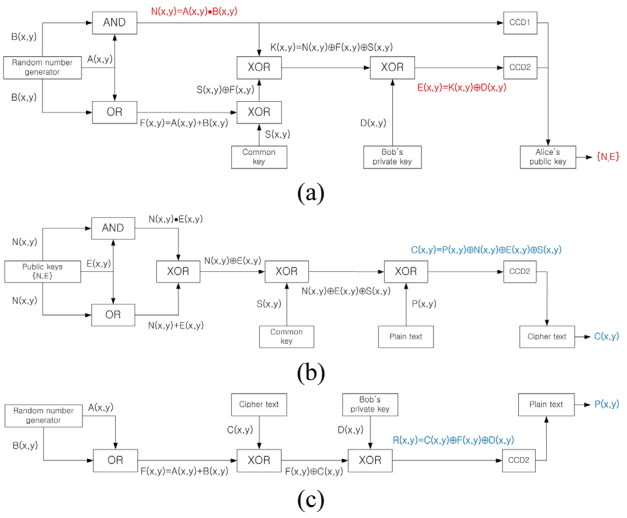

FIG. 3. Flow charts for the proposed asymmetric cryptography method: (a) public keys generation, (b) Alice's encryption, (c) Bob's decryption.

2.3. Optical Implementation of the Proposed Cryptosystem

Inherently, an optical information processing system has an advantage of 2-D data processing and fast parallel information processing time. This implies that the optical cryptosystem can have very long key length and massive data processing by expanding the key to 2-D array, but this 2-D key expansion does not increase processing time due to parallel processing of all bits in the array. Moreover, a cryptosystem has a key length of M×N bits with 2-D arrayed format, it means that $2^{M\times N}$ brute force attacks are required. With these properties, an asymmetrical public key cryptosystem by using logic-based optical processing is proposed, which uses 2-D page-typed input format in the public-private key pair and then results in the same 2-D arrayed output format in the cipher text. In this paper, the main idea of the proposed asymmetric method is that the modified RSA algorithm is implemented in an optical way by using the bitwise logic-based and free-space inter-connected optical processing technique.

The advantage of the bitwise 2-D arrayed optical logic processing technique is that no pixel encoding-decoding process is required because the output has the same format as the input. In order to implement optically the logic-based operations, 2-D binary input variables are spatially dual encoded by using two's complement [22-24]. Referring to the modified RSA algorithm by using logic-based optical processing as shown in Fig. 2 and Fig. 3, an optical configuration of the proposed asymmetric cryptography is designed with optical components such as mirrors (M), beam splitters (BS), and spatial light modulators (SLM). In this configuration, all the SLMs are used as free-space interconnected optical logic gates. Figure 4 shows the optical schematic of the proposed asymmetric public key cryptography using dual free-space interconnected logic operations.

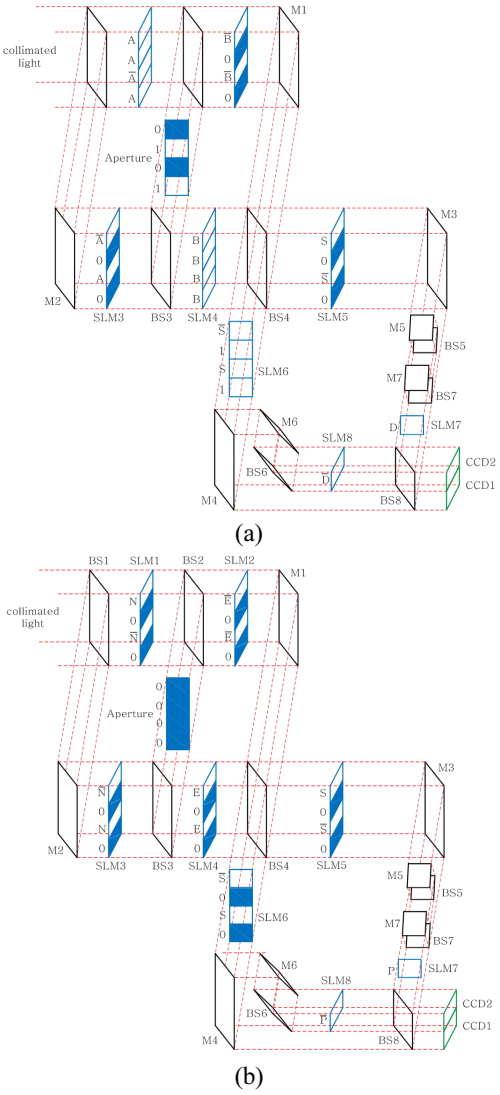

FIG. 4. Optical schematic of the proposed asymmetric public key cryptography using dual free-space interconnected logic operations: (a) public keys generation, (b) Alice's encryption.

Schematically, the optical setup contains Mach-Zehnder type interferometer architecture. Four beam splitters BS1, BS2, BS3 and BS4 divide a collimated light into two lights, and two beam splitters BS4 and BS8 combine these divided lights into one light. Two beam splitters BS2 and BS3 perform optical AND, OR and XOR logic operations, while two beam splitters BS4 and BS8 perform optical OR logic operations and the resultant combined lights from BS8 are recorded on two CCDs. In addition, three beam splitters BS5, BS6 and BS7 are used for performing XOR logic operations. Also, this architecture is composed of eight SLMs which are used for displaying data inputs and one aperture which is used for logic control.

In order to investigate the operating principles of the optical schematic of the modified RSA algorithm, the flow charts for the proposed asymmetric cryptography method shown in Fig. 3 are considered. As to public key generation, let us consider the public keys generation procedure shown in Fig. 3(a). Figure 4(a) shows the optical configuration for the proposed asymmetric cryptosystem so as to generate the public keys {***N***, ***E***} simultaneously, which is based on dual free-space interconnected AND, OR and XOR logic operations for 2-D binary data. In Fig. 4(a), the collimating light after being reflected by the beam splitters and the mirrors illuminates and passes through the SLMs, where all the SLMs and one aperture are arranged with a purpose of operating optical AND, OR and XOR logic operations as free-space interconnected optical logic gates. When the light continuously passes two SLMs in series, optical AND logic operation is obtained by inner production pixel by pixel. On the other hand, the combining beam splitter performs optical OR logic operation by adding two lights in parallel. In this public keys generation step, two random numbers ***A*** and ***B***, the common key ***S***, and Bob's private key ***D*** are displayed on the appropriate SLMs. For the purpose of operating XOR logic, dual free-space interconnected logic operation is done by using the complements of these values. The logically processed and combined light of the first row and the third row of SLMs is recorded on CCD2 as the public key {***E***}, and the logically processed and combined light of the second row and the fourth row of SLMs is recorded on CCD1 as the public key {***N***}. The detailed representations of input SLMs' data and output CCDs' data are shown in Fig. 5(a).

With these public keys {***N***, ***E***}, Alice performs the encryption procedure shown in Fig. 3(b). Figure 4(b) shows the optical configuration for the proposed asymmetric cryptosystem so as to encrypt a plain text **P** into a cipher text **C** by the public keys {***N***, ***E***}. In Alice's encryption step shown in Fig. 4(b), the public keys {***N***, ***E***}, the common key ***S***, and a plain text **P** are displayed on the appropriate SLMs. The logically processed and combined light of the first row and the third row of SLMs is recorded on CCD2 as a cipher text **C**, while the processing of the second row and the fourth row of SLMs is not carried out. The detailed representations of input SLMs' data and output CCDs' data are shown in Fig. 5(b).

As to Bob's decryption step, the same optical configuration shown in Fig. 4(a) is used for decrypting the cipher text **C** into the plain text **P**. In this paper, the optical schematic for Bob's decryption is omitted because of duplication. According to the flow chart shown in Fig. 3(a), Bob's decryption can be done simply by replacing the common key ***S*** with the private key ***D***. The detailed representations of input SLMs' data and output CCDs' data are shown in Fig. 5(c).

III. NUMERICAL SIMULATIONS AND ANALYSIS

3.1. Security Strength

For the purpose of verifying the modified RSA algorithm

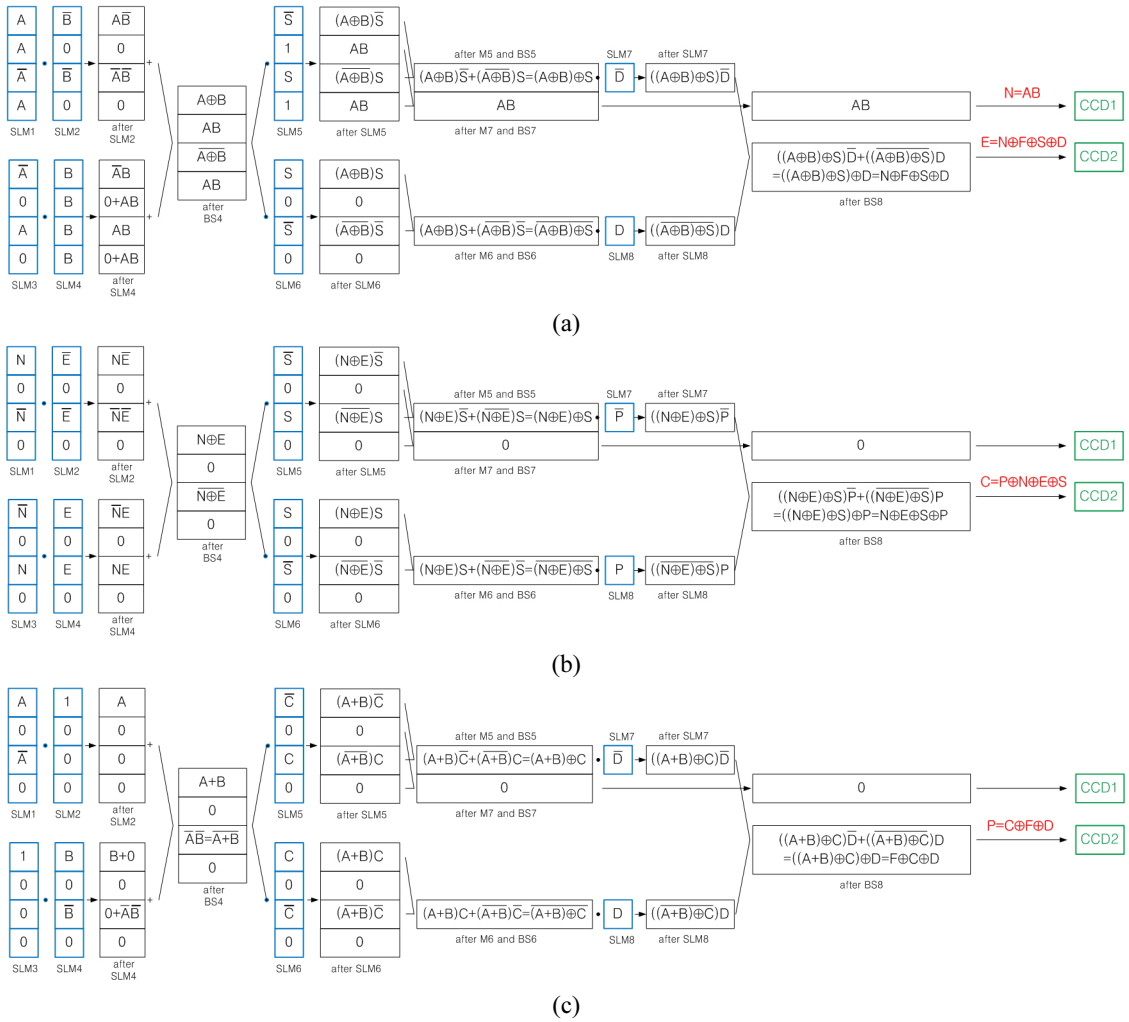

FIG. 5. Representations of input SLMs' data and output CCDs' data on the optical schematic of the proposed asymmetric public key cryptography: (a) public keys generation, (b) Alice's encryption, (c) Bob's decryption.

and of showing the effectiveness in the proposed optical asymmetric cryptosystem, the proposed cryptosystem is analyzed and computer numerical simulations are carried out. In the proposed method, input data to be processed is binary bit data or a binary image. In numerical simulation, all input data have the form of page-typed 2-D array which consists of 64 × 64 binary pixels for convenience. Also, this means that the security key length has 64 × 64 = 4,096 bits which is very much longer key length compared to the conventional electronic cryptography. For example, the conventional 1-D key length for the RSA public key cryptosystem has 512 bits, 768 bits or 1,024 bits. According to the pilot examples of metrics for cryptographic algorithms of the reference [25], if the key length is 1,024 bits in the conventional RSA cryptography, then 2.4×10^{17} years of attack time is needed. In this paper, the key length is assumed to be 64 × 64 = 4,096 bits so that $2^{64\times64} = 2^{4,096}$ brute force attacks are required to find the correct key, which implies very huge attack time. Moreover, if we expand the data size to 128×128 pixels array, then the key length increases to 16,384 surprisingly. This means that $2^{128\times128} = 2^{16,384}$ brute force attacks are required to find the correct key. In addition to the 2-D arrayed longer key length, the proposed asymmetric cryptosystem has a difficulty in finding the decryption private key $\boldsymbol{D}$ and $\boldsymbol{F} = \boldsymbol{A} + \boldsymbol{B}$ even if the public keys $\{\boldsymbol{N}, \boldsymbol{E}\}$ are known. Furthermore, the exactly correct decryption key is also encrypted as Eq. (11). Therefore, if two secret random numbers $\boldsymbol{A}$ and $\boldsymbol{B}$ have 64×64 bits of 2-D arrayed format, the combination between random numbers A and B $(2^{64\times64})\times(2^{64\times64}) = 2^{4,096\times4,096}$ attempts are required in order to find $\boldsymbol{F} = \boldsymbol{A} + \boldsymbol{B}$. Also, even if the attacker might know $\boldsymbol{F} = \boldsymbol{A} + \boldsymbol{B}$, the attacker should need to know the decryption key $\boldsymbol{D}$ for perfect decryption as Eq. (11). If three random numbers $\boldsymbol{A}$, $\boldsymbol{B}$ and $\boldsymbol{D}$ are used only once in the encryption session and never used in the next encryption session, then it is hard to deduce the encryption key from the whole data by known-plain text and chosen-plain text attack.

A shared common key $\boldsymbol{S}$ between Alice and Bob is shown in Fig. 6(a). For convenience, a randomly generated

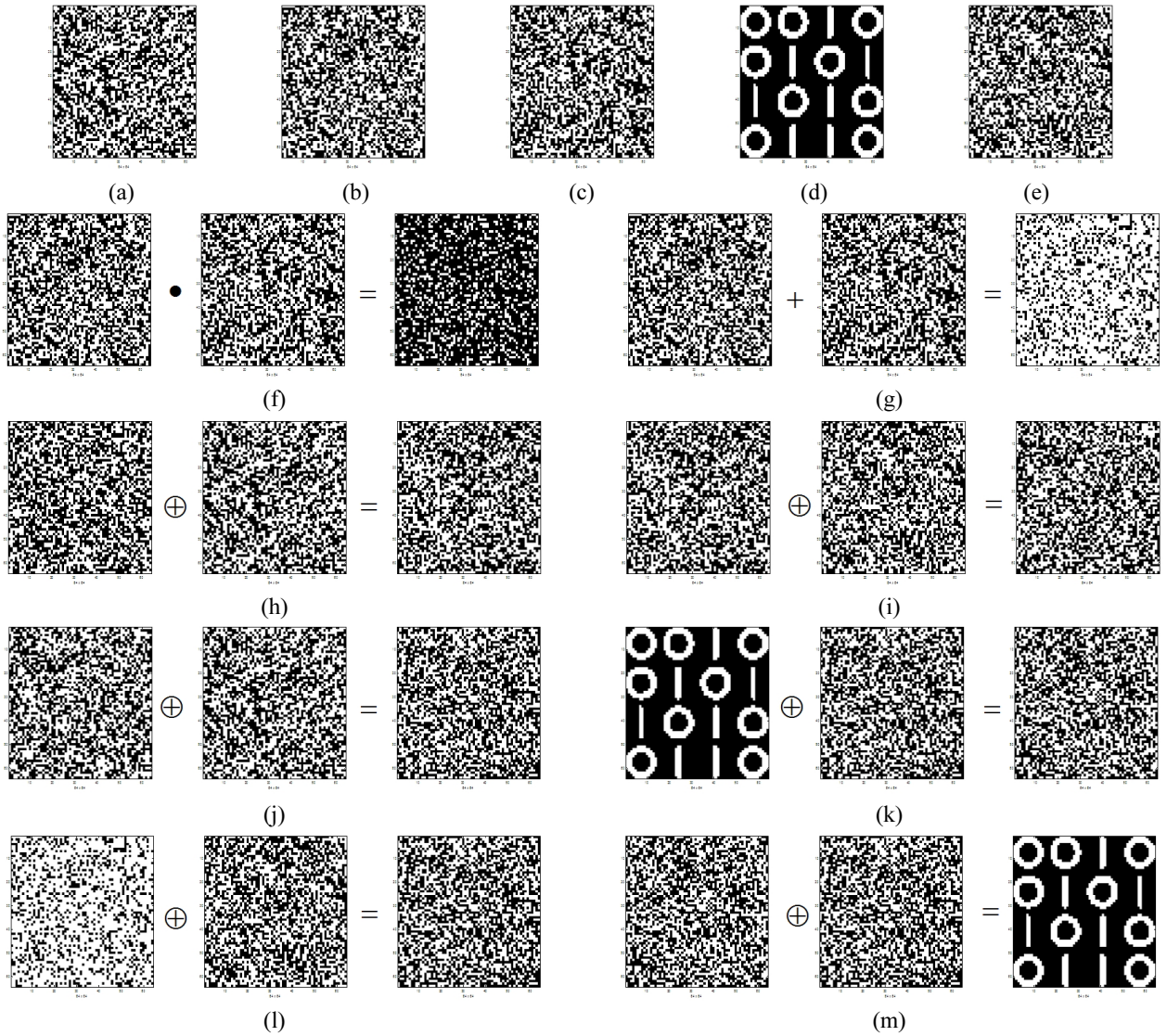

FIG. 6. Numerical simulation for the proposed method: (a) a shared common key S between Alice and Bob, (b) a randomly generated number A, (c) a randomly generated number B, (d) Alice's binary image P to be encrypted as a plain text, (e) a randomly generated number D as Bob's decryption key, (f) A · B=N, (g) A + B = F, (h) (N ⊕ F) ⊕ S=K, (i) K ⊕ D = E, (j) (N ⊕ E) ⊕ S = A_k, (k) P ⊕ A_k = C, (l) F ⊕ D = B_k, (m) R = C ⊕ B_k = P.

number $\boldsymbol{S}$ is suggested in this paper, where white areas have value of 1 and black areas are 0 numerically. This key is initially stored in both users' memory like a Diffie-Hellman shared secret key. Figures 6(b) and (c) show two randomly generated numbers $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, which is used for producing the resultant public and private keys. Figure 6(d) is a plain text **P** to be encrypted, which is chosen as a binary image intentionally in order to show the processing data patterns visually. Figure 6(e) shows another randomly generated binary number $\boldsymbol{D}$ which is also used in encryption and decryption. Figure 6(f) expresses AND logic-based operation result $\boldsymbol{N} = \boldsymbol{A} \cdot \boldsymbol{B}$ and Fig. 6(g) expresses OR logic-based operation result $\boldsymbol{F} = \boldsymbol{A} + \boldsymbol{B}$. Figures 6(h) and (i) represent continuously XOR logic-based operation results $\boldsymbol{K} = (\boldsymbol{N} \oplus \boldsymbol{F}) \oplus \boldsymbol{S}$ and $\boldsymbol{E} = \boldsymbol{K} \oplus \boldsymbol{D}$ according to Eqs. (6) and (7), respectively. Through the optical key generation step, the resultant public keys $\{\boldsymbol{N}, \boldsymbol{E}\}$ are open to the public. Figures 6(j) and (k) represent continuously XOR logic-based operation results $\boldsymbol{A_k} = (\boldsymbol{N} \oplus \boldsymbol{E}) \oplus \boldsymbol{S}$ and $\boldsymbol{C} = \boldsymbol{P} \oplus \boldsymbol{A_k}$ according to Eqs. (9) and (10), respectively. The pattern of the cipher text **C** looks like a random pattern due to the random-like encryption key $\boldsymbol{A_k}$. Figure 6(l) represents XOR logic-based operation result $\boldsymbol{B_k} = \boldsymbol{F} \oplus \boldsymbol{D}$ according to Eq. (11), which shows the combination of two private keys $\{\boldsymbol{F}, \boldsymbol{D}\}$. Figure 6(m) represents XOR logic-based operation result $\boldsymbol{R} = \boldsymbol{C} \oplus \boldsymbol{B_k} = \boldsymbol{P}$ according to Eq. (12). From the figure shown as Fig. 6(m), the reconstructed data $\boldsymbol{R}$ is exactly the same as the original plain text $\boldsymbol{P}$, which is correctly decrypted by the private decryption keys $\{\boldsymbol{F}, \boldsymbol{D}\}$.

(a) (b) (c) (d) (e) (f)

FIG. 7. Numerical simulation for the cipher-text-only attack: Reconstructed data are shown when (a) R = C ⊕ X, (b) R = C ⊕ N, (c) R = C ⊕ E, (d) R = C ⊕ (N · E), (e) R = C ⊕ (N + E), (f) R = C ⊕ (N ⊕ E).

TABLE 1. Numerical results for AMSE for cipher-text-only key attacks

Case	AMSE(%)
R = C ⊕ X	49.9844
R = C ⊕ N	49.9827
R = C ⊕ E	50.1130
R = C ⊕ (N · E)	49.9133
R = C ⊕ (N + E)	50.2686
R = C ⊕ (N ⊕ E)	50.1813

On the other hand, in order to analyze cipher-text-only key attack, some possible key attacks which should be made from the open public keys {***N***, ***E***} are assumed as follows: (1) when $\boldsymbol{B_k} = \boldsymbol{X}$(a randomly generated number), $\boldsymbol{R} = \boldsymbol{C} \oplus \boldsymbol{X}$, (2) when $\boldsymbol{B_k} = \boldsymbol{N}$, $\boldsymbol{R} = \boldsymbol{C} \oplus \boldsymbol{N}$, (3) when $\boldsymbol{B_k} = \boldsymbol{E}$, $\boldsymbol{R} = \boldsymbol{C} \oplus \boldsymbol{E}$, (4) when $\boldsymbol{B_k} = \boldsymbol{N} \cdot \boldsymbol{E}$, $\boldsymbol{R} = \boldsymbol{C} \oplus (\boldsymbol{N} \cdot \boldsymbol{E})$, (5) when $\boldsymbol{B_k} = \boldsymbol{N} + \boldsymbol{E}$, $\boldsymbol{R} = \boldsymbol{C} \oplus (\boldsymbol{N} + \boldsymbol{E})$, (6) when $\boldsymbol{B_k} = \boldsymbol{N} \oplus \boldsymbol{E}$, $\boldsymbol{R} = \boldsymbol{C} \oplus (\boldsymbol{N} \oplus \boldsymbol{E})$. Figures 7(a)~(f) show the reconstructed data image ***R*** which are not the same as the original plain text ***P*** when attacking decryption keys are as the above cases, respectively. To analyze the differences between the plain text shown in Fig. 6(d) and the decrypted text image with cipher-text-only key attack shown in Figs. 7(a)~(f), the average mean square error (AMSE) is calculated as follows.

$$AMSE = \frac{1}{I}\sum_{i=1}^{I}\frac{1}{64\times 64}\sum_{x,y}\{P(x,y) - R_i(x,y)\}^2 \tag{13}$$

Table 1 shows numerical results for AMSE for some cipher-text-only key attacks. These AMSE are average values calculated from 1,000 evaluations for each case. For the binary text cryptographic system, MSE value of 0% means that the decrypted text is exactly the same as the original plain text and MSE value of 100% means that the decrypted text represents the reversed data of the original plain text. From the table, MSE is close to 50% for each attack, which means that the decryption is almost incorrect because MSE of 50% means that the decrypted text is the same as a half of the plain text.

3.2. Differential Cryptanalysis

In image encryption, the cipher resistance to differential attacks is commonly analyzed via the NPCR (number of pixel changing rate) test [26]. The NPCR $N(C_1,C_2)$ can be mathematically defined by Eqs. (14) and (15).

$$d(x,y) = \begin{cases} 0, & if\ C_1(x,y) = C_2(x,y) \\ 1, & if\ C_1(x,y) \neq C_2(x,y) \end{cases} \tag{14}$$

$$N(C_1,C_2) = \sum_{x,y}\frac{d(x,y)}{T}\times 100\% \tag{15}$$

Here, C_1 and C_2 are cipher text image before and after one pixel change in a plain text image, respectively, and T is total pixels in the cipher text. If two test cipher text images of size M×N are ideally encrypted, then the theoretical expectation and the variance of a random variable are

$$\mu_N = F/(F+1) \tag{16}$$

$$\sigma_N = F/MN(F+1)^2 \tag{17}$$

F denotes the largest pixel value compatible with the cipher text format. For the binary image case, F=1. In this paper, C_1 and C_2 are cipher texts of size M × N encrypted by Boolean logic combination of random numbers ***A***, ***B*** and ***D***. In this paper, these random numbers are generated by a pseudo-random number generator which is a built-in function in MATLAB. To show the simulated expectation and the variance of cipher texts C_1 and C_2, C_1 and C_2 are obtained from Eq. (10) by choosing different ***D*** for each plain text P_1 and P_2, where P_1 and P_2 have the difference of one pixel change. The simulated expectation and the variance are calculated from 10,000 pairs of C_1 and C_2. More specifically, the estimated statistics are obtained by

$$\mu_S = \frac{1}{I}\sum_{i=1}^{I}N(C_1,C_2) = \frac{1}{I}\sum_{x,y}\frac{D(x,y)}{MN}\times 100\% \tag{18}$$

$$\sigma_S = \frac{1}{(I-1)}\sum_{i=1}^{I}\{N(C_1,C_2) - \mu_S\}^2 \times 100\% \tag{19}$$

TABLE 2. Numerical results for NPCR randomness test for the proposed cryptosystem

Tested data size (M×N)	Theoretical values(%)		Simulated values(%) for the proposed method	
	μ_N	σ_N	μ_S	σ_S
64×64	50.0000	0.7813	50.0033	0.6231
128×128	50.0000	0.3906	49.9967	0.3124
256×256	50.0000	0.1953	49.9996	0.1544
512×512	50.0000	0.0977	50.0005	0.0774
1024×1024	50.0000	0.0488	50.0005	0.0389

Here, I denotes the number of iterations and $M \times N$ is total pixels in the cipher text. Table 2 shows numerical results for NPCR randomness test for the proposed asymmetric cryptosystem. From the table, the simulated expectation and the variance of cipher texts C_1 and C_2 are very close to the theoretical values.

IV. CONCLUSION

In this paper, a novel asymmetric public key cryptography based on the modified RSA algorithm is proposed by using logic-based optical processing. The proposed asymmetric algorithm is realized by optical logic-based operations to modify the conventional RSA algorithm, where AND, OR and XOR logic operations are implemented by using free space digital optics architecture. The optical schematic of the proposed method consists of dual free-space interconnected logic operation to perform Boolean logic operations. Schematically, the proposed optical configuration has an advantage of generating the public keys simultaneously. The proposed asymmetric cryptosystem can provide higher secure cryptosystem than the conventional RSA algorithm because the proposed algorithm uses a kind of XOR logic-based double key encryption technique which consequently enhances security strength. Also, the proposed optical configuration has 2-D array data format which can increase the key length easily to strengthen the security system. In addition, 2-D expansion of data size does not increase information processing time owing to the parallel processing property despite increase in 2-D data. Another advantage of the proposed method is that it is convenient to alter the user's two secret random numbers and the decryption key in generating the public keys, which means the proposed method has a property that users can change three random numbers at their own discretion. Computer numerical simulations and differential cryptanalysis verifies that the proposed cryptographic method is effective and suitable for the asymmetric data encryption system.

ACKNOWLEDGMENT

This work was supported by the University of Suwon in 2013.

REFERENCES

1. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. on Inf. Theory **22**, 644-654 (1976).
2. W. C. Barker and E. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher," NIST Special Publication 800-67, Revision 1 (2012).
3. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," ACM **21**, 120-126 (1978).
4. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752-1756 (1994).
5. J. F. Heanue, M. C. Bashaw, and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt. **34**, 6012-6015 (1995).
6. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
7. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng. **37**, 565-569 (1998).
8. D. Weber and J. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," Opt. Eng. **38**, 62-68 (1999).
9. E. Cuche, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging," Opt. Lett. **24**, 291-293 (1999).
10. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," Opt. Eng. **39**, 2853-2859 (2000).
11. G.-S. Lin, H. T. Chang, W.-N. Lie, and C.-H. Chuang, "Public-key-based optical image cryptosystem based on data embedding techniques," Opt. Eng. **42**, 2331-2339 (2003).
12. B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," Opt. Eng. **43**, 2239-2249 (2004).
13. G. Situ and J. Zhang, "A lensless optical security system based on computer-generated phase only masks," Opt. Commun. **232**, 115-122 (2004).
14. S. H. Jeon and S. K. Gil, "2-step quadrature phase-shifting digital holographic optical encryption using orthogonal polarization and error analysis," J. Opt. Soc. Korea **16**, 354-364 (2012).
15. I.-H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," J. Opt. Soc. Korea **18**, 201-206 (2014).
16. I.-H. Lee, "Accumulation encoding technique based on double random phase encryption for transmission of multiple images," J. Opt. Soc. Korea **18**, 401-405 (2014).