Journal of the Optical Society of Korea
Vol. 19, No. 6, December 2015, pp. 592-603

ISSN: 1226-4776(Print) / ISSN: 2093-6885(Online)
DOI: http://dx.doi.org/10.3807/JOSK.2015.19.6.592

Optical Implementation of Asymmetric Cryptosystem Combined with D-H Secret Key Sharing and Triple DES

Seok Hee Jeon[1] and Sang Keun Gil[2]*

[1]Department of Electronic Engineering, Incheon National University, Incheon 406-772, Korea
[2]Department of Electronic Engineering, The University of Suwon, Whasung 440-600, Korea

(Received November 2, 2015 : accepted December 1, 2015)

In this paper, an optical implementation of a novel asymmetrical cryptosystem combined with D-H secret key sharing and triple DES is proposed. The proposed optical cryptosystem is realized by performing free-space interconnected optical logic operations such as AND, OR and XOR which are implemented in Mach-Zehnder type interferometer architecture. The advantage of the proposed optical architecture provides dual outputs simultaneously, and the encryption optical setup can be used as decryption optical setup only by changing the inputs of SLMs. The proposed cryptosystem can provide higher security strength than the conventional electronic algorithm, because the proposed method uses 2-D array data, which can increase the key length surprisingly and uses 3DES algorithm, which protects against “meet in the middle” attacks. Another advantage of the proposed asymmetrical cryptosystem is that it is free to change the user’s two private random numbers in generating the public keys at any time. Numerical simulation and performance analysis verify that the proposed asymmetric cryptosystem is effective and robust against attacks for the asymmetrical cipher system.

Keywords : Optical encryption, Optical logic, Diffie-Hellman secret key, Asymmetrical public key, Triple DES

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

With the rapid development of communication networks, there have been strong demands for information security, thus this trend brings a continuing search for more secure encryption algorithms. But, digital information of the public network tends to be not secure against unauthorized attack because of the fast development of computers. For the purpose of protecting information against hacking, various cryptographic algorithms have been introduced. A simple method to enhance the security strength is to increase the key length. Another method is to use an algorithm having multiple security keys, for example double keys or triple keys, in the cryptosystem. In order to meet these conditions, thus advanced algorithms such as D-H (Diffie-Hellman) secret key sharing [1], 3DES (triple Data Encryption Standard) [2] and asymmetric RSA public key cryptography [3] were introduced to enhance security strength. However, the electronic cryptosystem is slow and requires much time to compute the encryption procedure for the long key length and huge amount of data. On the contrary the optical cryptosystem has advantages of fast signal processing and vast data handling due to the inherent 2-D signal processing capability of optics and thus the parallelism achievable with optical signal processing. Another advantage of an optical cryptosystem is the potential for a large key length, rendering brute force attacks almost impossible. For these reasons, there has been a growing interest in optical cryptographic systems and several optical encryption techniques have been proposed in recent years [4-13]. Also, an optical XOR logic-based encryption has been introduced as one of these effective encryption algorithms [14-16].

In order to establish a secure cryptosystem, the most important thing is that the encryption key must not be

*Corresponding author: skgil@suwon.ac.kr

Color versions of one or more of the figures in this paper are available online.

known to unauthorized persons and the key must be hard to break by attacks. The symmetric private key algorithm such as DES has a risk that attackers may cryptanalyze the symmetric key because this type of cryptosystem has only one key. To solve this problem, asymmetric cryptography such as the D-H algorithm was introduced. In this algorithm, two users unknown to each other can set up a public key and share a secret key by their public key exchange cryptography. However, this shared secret key can be disclosed by "meet in the middle" attack because this shared secret key is used to encrypt messages by applying symmetric cryptography. So as to realize higher level of security, an advanced algorithm such as 3DES or asymmetric RSA public key cryptography was introduced as a means of solving this problem, which uses double key encryption technique. In our previous studies on the optical cryptosystem, a triple DES algorithm was proposed in an optical way based on dual XOR logic operation [17] and an optically modified D-H key exchange protocol was reported recently [18].

In this paper, an asymmetrical cryptosystem combined with D-H secret key sharing and triple DES and its optical implementation are proposed. Also, numerical simulation and performance analysis are discussed. The objective of this paper is to analyze how secure the proposed cryptosystem is and how efficient the proposed optical implementation is. Section II is organized as three parts. The first and second parts overview the D-H secret key sharing algorithm and the triple DES algorithm. In the third part, the proposed asymmetric cryptosystem combined with D-H secret key sharing and 3DES is explained. Section III describes the optical implementation of the proposed asymmetric cryptosystem. In Section IV, numerical simulation proves the feasibility of the optical system and performance analysis is described by showing results of the decryption error rate according to possible attacks inferred by the open public keys. Finally, the conclusions are briefly summarized in Section V.

II. THEORY

2.1. Diffie-Hellman Secret Key Sharing Algorithm

In 1976, Diffie and Hellman introduced a secret key sharing algorithm, which is focused on exchanging cryptographic secret keys. The D-H secret key sharing algorithm is a method for two users to exchange a shared secret key over a public network without any prior secrets between them. They can encrypt private messages into cipher messages by using this symmetric shared key. The D-H secret key sharing algorithm is as follows.

Let the users be named Alice and Bob. First, they agree on two prime numbers $\boldsymbol{g}$ and $\boldsymbol{p}$, where $\boldsymbol{g}$ is called a generator and is a primitive root modulo $\boldsymbol{p}$. The numbers $\boldsymbol{g}$ and $\boldsymbol{p}$ need not be kept secret from other users. At first, Alice chooses a random number $\boldsymbol{a}$ as her private key and computes $\boldsymbol{u}$ as Eq. (1), and Bob similarly chooses a random number $\boldsymbol{b}$ as his private key and computes $\boldsymbol{v}$ as Eq. (2). Then, Alice and Bob send these computed numbers to each other.

$$u = g^{a} \bmod p \tag{1}$$

$$v = g^{b} \bmod p \tag{2}$$

Now, both Alice and Bob compute their shared secret keys $\boldsymbol{s_a}$ and $\boldsymbol{s_b}$ by the same modulo $\boldsymbol{p}$ as

$$s_a = v^{a} \bmod p = (g^{b})^{a} \bmod p = g^{ab} \bmod p \tag{3}$$

$$s_b = u^{b} \bmod p = (g^{a})^{b} \bmod p = g^{ab} \bmod p \tag{4}$$

Alice and Bob can now use their shared secret key $\boldsymbol{s} = \boldsymbol{s_a} = \boldsymbol{s_b}$ to exchange messages without worrying about other users obtaining these messages. In order for a potential eavesdropper (Eve) to intrude messages, she would first need either a random number $\boldsymbol{a}$ or a random number $\boldsymbol{b}$ knowing only $\boldsymbol{g}$, $\boldsymbol{p}$, $\boldsymbol{u}$ and $\boldsymbol{v}$. This can be done by computing $\boldsymbol{a}$ from $\boldsymbol{u} = \boldsymbol{g^a}$ **(mod** $\boldsymbol{p}$**)** and $\boldsymbol{b}$ from $\boldsymbol{v} = \boldsymbol{g^b}$ **(mod** $\boldsymbol{p}$**)**. This is called the discrete logarithm problem, which is computationally infeasible for large $\boldsymbol{p}$. Computing the discrete logarithm of a number modulo $\boldsymbol{p}$ takes roughly the same amount of time as factoring the product of two primes the same size as $\boldsymbol{p}$, and it is inefficient and impractical to calculate the solution by using brute force attack. The main drawback of the D-H secret key sharing algorithm is that it suffers from the "meet in the middle" attack problem. This implies the fact that the authenticity of public keys is essential, and it is particularly obvious when new public keys are changed for each communication session.

In the case of optics, it is very difficult for the D-H key method 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 on an optical device properly. In spite of these difficulties, we proposed an optical D-H secret key sharing method by modifying the conventional D-H key secret key sharing protocol [18]. In the proposed method, modulo arithmetic was mathematically replaced by an XOR logic operation. Therefore, the XOR logic-based encryption operation which is regarded as a kind of modulo two addition could be implemented simply by an optically realizable system. Specifically, the XOR-only encryption scheme is perfectly secure if and only if the key data is perfectly random and never reused.

2.2. Triple DES Algorithm

The DES was the first symmetric block cipher protocol which was first issued as a standard in 1977 by the American National Standard Institute (ANSI). It encrypts plain text data in 64-bit blocks by using a 56-bit secret key. DES has been one of the most successful and widely used secret key cryptographic systems. However, ever since DES was released for public cryptosystems, some cryptographers have argued that the security strength of DES would not be sufficient in present days due to its short key length. In order to overcome this problem, many efforts were made to enhance DES. Recently, Triple DES (3DES) has been adopted as a temporary standard and is incorporated in several international standards. 3DES is the name now most often given one popular form of multiple DES applications and is known as Encrypt-Decrypt-Encrypt (EDE) and TDEA (Triple Data Encryption Algorithm). In general usage, 3DES algorithms use three independent security keys. This means that cryptanalysis requires triple computational efforts compared to DES. However, most 3DES algorithms use two independent security keys by using the third encryption key the same as the first encryption key. This option provides also more security than simply DES encrypting twice, because it protects against "meet in the middle" attacks. To acquire the maximum security in the 3DES algorithm, each key is assigned to a different authority so that the decryption cannot be performed. The resultant 3DES cipher text is much harder to break. The 3DES algorithm is as follows.

Assume that 3DES uses three independent keys as K_1, K_2, and K_3. The encryption process is given by

$$c_t = E_{K_3}(D_{K_2}(E_{K_1}(p_t))) \tag{5}$$

Eq. (5) represents DES encryption of plain text (p_t) with key K_1, DES decryption with key K_2, then DES encryption with key K_3 resulting cipher text (c_t). Decryption is the reverse.

$$p_t = D_{K_1}(E_{K_2}(D_{K_3}(c_t))) \tag{6}$$

About optical implementation of 3DES, we suggested a modified 3DES algorithm based on XOR logic operations [17]. In the proposed method, a triple encryption using double keys was used in a special way so as to avoid the key sharing of the double encryption with two keys.

2.3. Proposed Asymmetric Cryptosystem Combined with D-H Secret Key Sharing and 3DES

In the D-H secret sharing cryptosystem, there is a possibility that the shared secret key may be disclosed by "meet in the middle" attacks. But, the 3DES algorithm is very robust against these "meet in the middle" attacks. If we hide the shared secret key information by encrypting that key and make double encryption of the shared secret key, then more enhanced security strength will be acquired although attackers know the open public keys. With this idea, we propose an asymmetric cryptosystem combined with D-H secret key sharing and 3DES, and we also suggest an optical implementation of the proposed method by applying the logic-based optical processing such as AND, OR and XOR operations. The asymmetric cryptographic algorithm proposed in this paper can be described as follows.

1. Alice and Bob agree on and make two public numbers ***G*** and ***H***, where ***G*** and ***H*** are generated randomly instead of prime numbers. Note that these numbers are open to public and anyone can access to them.

2. Alice chooses two distinct random numbers ***A*** and ***X*** as her private keys, where these numbers are kept secret in public. Alice computes ***G* • *A*** and ***H* • *A*** by Boolean AND logic operation. Next, Alice computes her first public key $\boldsymbol{K_A}$ by OR logic operation of these two values and sends it to Bob.

$$K_A = G \cdot A + H \cdot A = (G + H) \cdot A \tag{7}$$

3. Similarly, Bob chooses two distinct random numbers ***B*** and ***Y*** as his private keys, where these numbers are kept secret in public. Bob computes ***G* • *B*** and ***H* • *B*** by Boolean AND logic operation. Next, Bob computes his first public key $\boldsymbol{K_B}$ by OR logic operation of these two values and sends it to Alice.

$$K_B = G \cdot B + H \cdot B = (G + H) \cdot B \tag{8}$$

4. Alice computes a shared secret key by some logic operations of Bob's first open public key $\boldsymbol{K_B}$ with Alice's private key ***A*** and open random numbers ***H*** and ***G***, where $\overline{H}$ and $\overline{G}$ mean the complement of ***H*** and ***G***, respectively.

$$\begin{aligned} S_A &= K_B \cdot A \cdot \overline{H} + \overline{G} \cdot H = \{(G+H) \cdot B\} \cdot A \cdot \overline{H} \\ &\quad + \overline{G} \cdot H = G \cdot B \cdot A \cdot \overline{H} + \overline{G} \cdot H \end{aligned} \tag{9}$$

5. Similarly, Bob computes a shared secret key by some logic operations of Alice's first open public key $\boldsymbol{K_A}$ with Bob's private key ***B*** and open random numbers ***H*** and ***G***.

$$\begin{aligned} S_B &= K_A \cdot B \cdot \overline{H} + \overline{G} \cdot H = \{(G+H) \cdot A\} \cdot B \cdot \overline{H} \\ &\quad + \overline{G} \cdot H = G \cdot A \cdot B \cdot \overline{H} + \overline{G} \cdot H \end{aligned} \tag{10}$$

6. Now both Alice and Bob have the same shared secret key, namely ***S***.

$$S = S_A = S_B = G \cdot A \cdot B \cdot \overline{H} + \overline{G} \cdot H \tag{11}$$

7. Alice computes her second public key $\boldsymbol{N_A}$ by XOR logic operation of the shared secret key $\boldsymbol{S_A}$ with her private

key ***X*** and sends it to Bob.

$$N_A = S_A \oplus X = S \oplus X \tag{12}$$

8. Similarly, Bob computes his second public key N_B by XOR logic operation of the shared secret key S_B with his private key ***Y*** and sends it to Alice.

$$N_B = S_B \oplus Y = S \oplus Y \tag{13}$$

9. Alice encrypts a plain text ***P*** by XOR logic operation of Bob's second open public key N_B with Alice's private key ***X*** and sends it to Bob.

$$C = P \oplus N_B \oplus X = P \oplus (S \oplus Y) \oplus X \tag{14}$$

10. Bob decrypts a cipher text ***C*** into the plain text ***P*** by XOR logic operation of Alice's second open public key N_A with Bob's private key ***Y***.

$$D = C \oplus N_A \oplus Y = C \oplus (S \oplus X) \oplus Y = P \tag{15}$$

As shown in Eq. (11), the shared secret key is composed of multiple logical encryptions by two public random numbers ***G*** and ***H***, Alice's private key ***A*** and Bob's private key ***B***. Thus, the total correct encryption key is expressed as

$$E_A = (A \cdot B \cdot G \cdot \overline{H} + \overline{G} \cdot H + G \cdot H) \oplus Y \oplus X \tag{16}$$

From Eq. (16), it is very important to understand the level of security in the proposed cryptosystem. The encryption key consists of six different random numbers, where these random numbers make a combination result by AND, OR and XOR logic operations. Even if we know the public keys ***G*** and ***H***, we cannot notice Alice's and Bob's private keys ***A***, ***X***, ***B*** and ***Y*** which are not open to the public. So as to find the perfect encryption key as Eq. (16) by brute force attack, we must find the logical combination of these random numbers. In the point of cryptanalysis, multiple-encryption of six independent random numbers gives very much security strength and is almost impossible to know the key by brute force attack.

Figure 1 shows the procedure of the proposed asymmetric cryptosystem combined with D-H secret key sharing

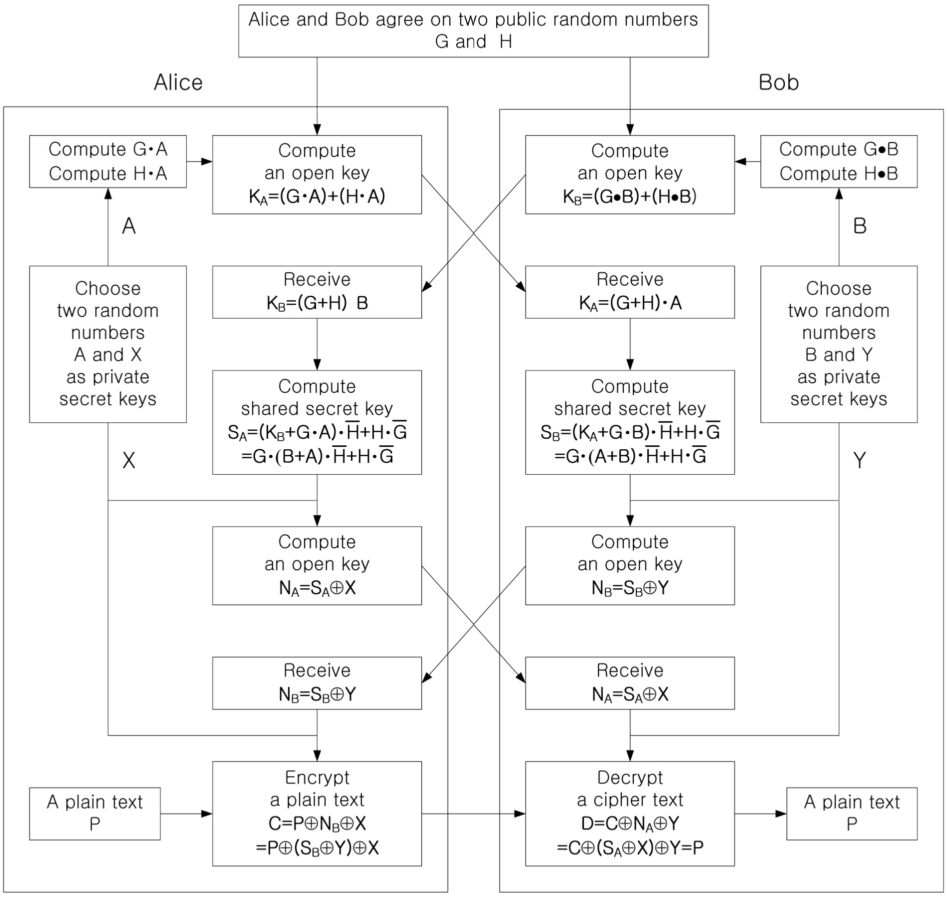

Alice and Bob agree on two public random numbers G and H
Alice
Bob
Compute G•A Compute H•A
Compute an open key K_A=(G•A)+(H•A)
Compute an open key K_B=(G•B)+(H•B)
Compute G•B Compute H•B
A
B
Choose two random numbers A and X as private secret keys
Receive K_B=(G+H) B
Receive K_A=(G+H)•A
Choose two random numbers B and Y as private secret keys
Compute shared secret key S_A=(K_B+G•A)•H̄+H•Ḡ =G•(B+A)•H̄+H•Ḡ
Compute shared secret key S_B=(K_A+G•B)•H̄+H•Ḡ =G•(A+B)•H̄+H•Ḡ
X
Y
Compute an open key N_A=S_A⊕X
Compute an open key N_B=S_B⊕Y
Receive N_B=S_B⊕Y
Receive N_A=S_A⊕X
A plain text P
Encrypt a plain text C=P⊕N_B⊕X =P⊕(S_B⊕Y)⊕X
Decrypt a cipher text D=C⊕N_A⊕Y =C⊕(S_A⊕X)⊕Y=P
A plain text P

FIG. 1. Procedure of the proposed asymmetric cryptosystem combined with Diffie-Hellman secret key sharing protocol and triple DES.

protocol and 3DES by using logic-based processing, and Fig. 2 shows the flow charts for the proposed cryptography method. As shown in Fig. 1 and Fig. 2, assume that Alice and Bob agree on two random numbers ***G*** and ***H*****,** which are open to the public. The first step is two public keys' generation. As for Alice's action shown as Fig. 2(a), Alice chooses two distinct random numbers ***A*** and ***X*** as her private keys and computes her first public key $\boldsymbol{K_A}$ and sends it to Bob. Similarly, Bob computes his first public key $\boldsymbol{K_B}$ and sends it to Alice, as shown Fig. 2(b). As obviously seen from Eqs. (7) and (8), these public keys are encrypted by their private keys ***A*** and ***B***, respectively. The second step is about the process for sharing a common secret key ***S*** by D-H key exchange algorithm. From the received Alice's and Bob's first public keys $\boldsymbol{K_A}$ and $\boldsymbol{K_B}$, they compute a shared secret key $\boldsymbol{S_A} = \boldsymbol{S_B} = \boldsymbol{S}$ by some logic operations like Eqs. (9) and (10). Eqs. (9) and (10) imply that attackers cannot infer these secret keys even if they know the public

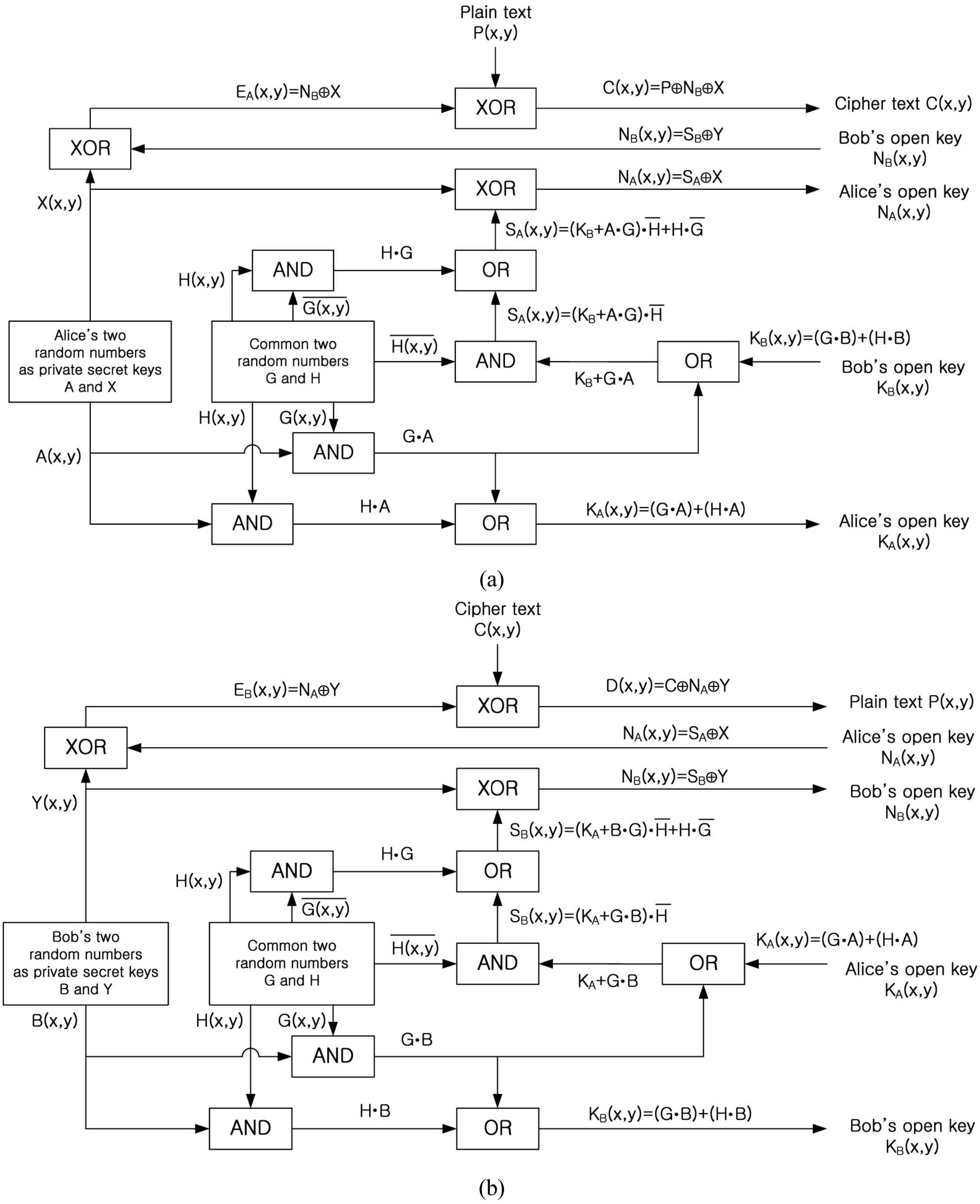


FIG. 2. Flow charts for the proposed cryptography method: (a) Alice's two public keys generation and plain text encryption, (b) Bob's two public keys generation and cipher text decryption.

keys which are open to the public. The third step is Alice's encryption of plain text which is shown as Fig. 2(a). With Bob's second public key N_B, Alice computes her encryption key $\boldsymbol{E_A} = \boldsymbol{N_B} \oplus \boldsymbol{X}$ and encrypts a plain text $\boldsymbol{P}$ into a cipher text $\boldsymbol{C}$ by this encryption key in compliance with Eq. (14). Also, this encryption key cannot be inferred although eavesdroppers notice the public keys because of encrypting Bob's second public key $\boldsymbol{N_B}$ with Alice's private key $\boldsymbol{X}$. The last and fourth step is Bob's decryption of cipher text which is shown as Fig. 2(b). Similarly, Bob computes his decryption key $\boldsymbol{E_B} = \boldsymbol{N_A} \oplus \boldsymbol{Y}$ with Alice's second public key $\boldsymbol{N_A}$ and decrypts a cipher text $\boldsymbol{C}$ into the plain text $\boldsymbol{P}$ by this decryption key in compliance with Eq. (15).

In this paper, the proposed asymmetrical cryptosystem uses the concept of 3DES algorithm. According to Eqs. (5) and (14) in the proposed method, a cipher text is given by

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P))) = P \oplus (S \oplus Y) \oplus X \tag{17}$$

From Eq. (17), encryption and decryption processes of 3DES can be explained as

$$E_{K_1}(P) = P \oplus S \tag{18}$$

$$D_{K_2}(E_{K_1}(P)) = (P \oplus S) \oplus Y \tag{19}$$

$$E_{K_3}(D_{K_2}(E_{K_1}(P))) = \{(P \oplus S) \oplus Y\} \oplus X \tag{20}$$

Here, encryption and decryption functions are substituted by XOR logic function and three independent keys are as K_1 = $\boldsymbol{S}$, K_2 = $\boldsymbol{Y}$, and K_3 = $\boldsymbol{X}$.

III. OPTICAL IMPLEMENTATION

The main idea of the proposed cryptosystem is to perform a more secure asymmetrical cryptographic system which transmits the encrypted public keys and the cipher text. This cryptographic algorithm is accomplished by combination of D-H secret key sharing and 3DES with triple keys. Referring to the block diagram shown in Fig. 1, the optical asymmetric cryptosystem is proposed with optical components such as mirror (M), beam splitter (BS), lenses, spatial light modulator (SLM) and charge coupled device (CCD). Figure 3 shows the optical schematic for implementing the proposed asymmetric cryptosystem, which is based on the dual free-space interconnected AND, OR and XOR logic operations for binary data. In this configuration, the optical setup contains four Mach-Zehnder type interferometers in order to generate the first public key and a shared secret key simultaneously, and this optical schematic can be used to generate the second public key and the cipher text simultaneously too. Also, this setup can be used for the decryption process. A collimated light is divided into two light paths and we combine these divided lights into one light path by four beam splitters BS1, BS2, BS3 and BS4. As for displaying data inputs, this architecture is composed of three SLMs. 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 the optical OR logic operation by adding two lights in parallel. As a result, the integration of these processes is equivalent to the optical XOR logic operation obtained by the combination of two logic ANDs and one logic OR. Finally, two CCDs are used for recording the resultant lights.

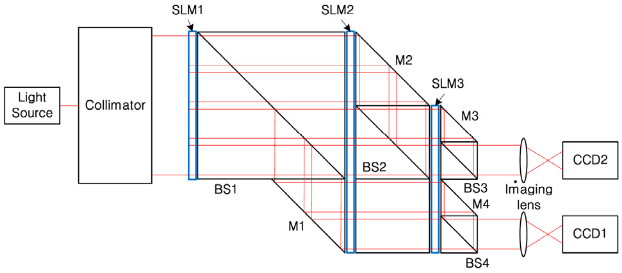


FIG. 3. Optical schematic for implementing the proposed asymmetric cryptosystem.

In order to explain operating principles of the optical configuration, the flow charts shown in Fig. 2 are considered. First, let us consider Alice's first public key and shared secret key generations shown in Fig. 2(a). In Fig. 3, SLMs display two public random numbers $\boldsymbol{G}$ and $\boldsymbol{H}$, Alice's private key $\boldsymbol{A}$, and Bob's first public key $\boldsymbol{K_B}$, where the complements of two public random numbers $\boldsymbol{G}$ and $\boldsymbol{H}$, i.e. $\overline{H}$ and $\overline{G}$, are displayed on SLMs for performing the required logic operations. The imaging lenses in front of CCDs play a role of pixel matching between light image and CCD pixel array. Figure 4(a) shows representations of input SLMs' data and output CCDs' data for generating Alice's first public key and the shared secret key, where logic '0' means blocking of the light while logic '1' means passing of the light through the SLM. Second, Alice's second public key generation and plain text encryption shown in Fig. 2(a) are carried out as follows. Alice's private key $\boldsymbol{X}$ and its complement $\overline{X}$ are displayed on SLM1. Bob's second public key N_B and Alice's shared secret key $\boldsymbol{S_A}$ are displayed on SLM2 with its complements. SLM3 display a plain text $\boldsymbol{P}$ and its complement. Dual free-space interconnected AND, OR and XOR logic operations by beam splitters and mirrors generate resultant Alice's second public key N_A on CCD1 and a cipher text $\boldsymbol{C}$ on CCD2. Fig. 4(b) shows representations of input SLMs' data and output CCDs' data for Alice's second public key and plain text encryption. Third, Bob's second public key generation and cipher text decryption shown in Fig. 2(b) are accomplished by using the same optical architecture as shown in the Fig. 3. Bob's private key $\boldsymbol{Y}$ and its complement $\overline{Y}$ are displayed on SLM1. Bob's second

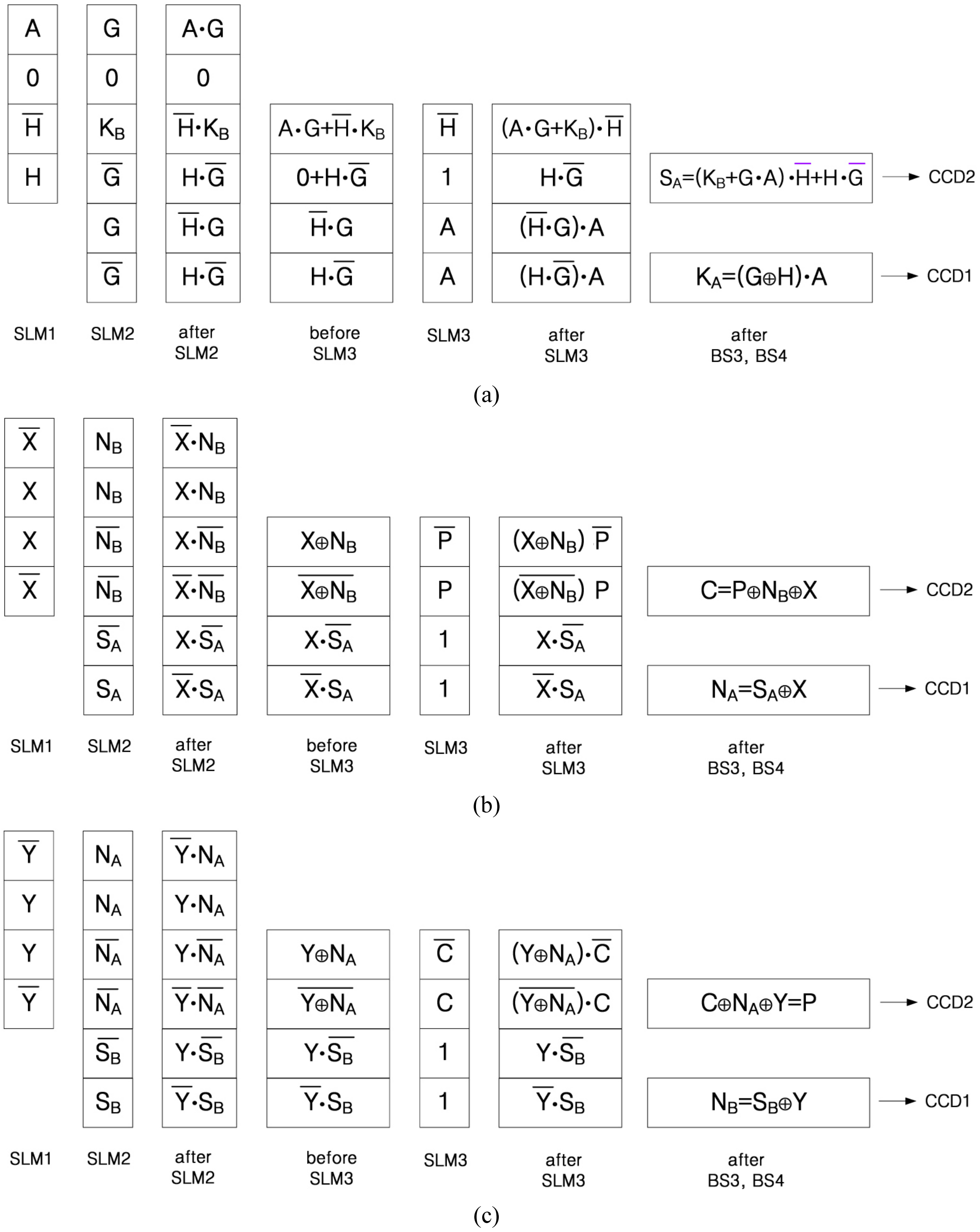


FIG. 4. Representations of input SLMs' data and output CCDs' data on the optical schematic of the proposed asymmetric cryptosystem: (a) Alice's first public key and a shared secret key generations, (b) Alice's second public key generation and plain text encryption, (c) Bob's second public key generation and cipher text decryption.

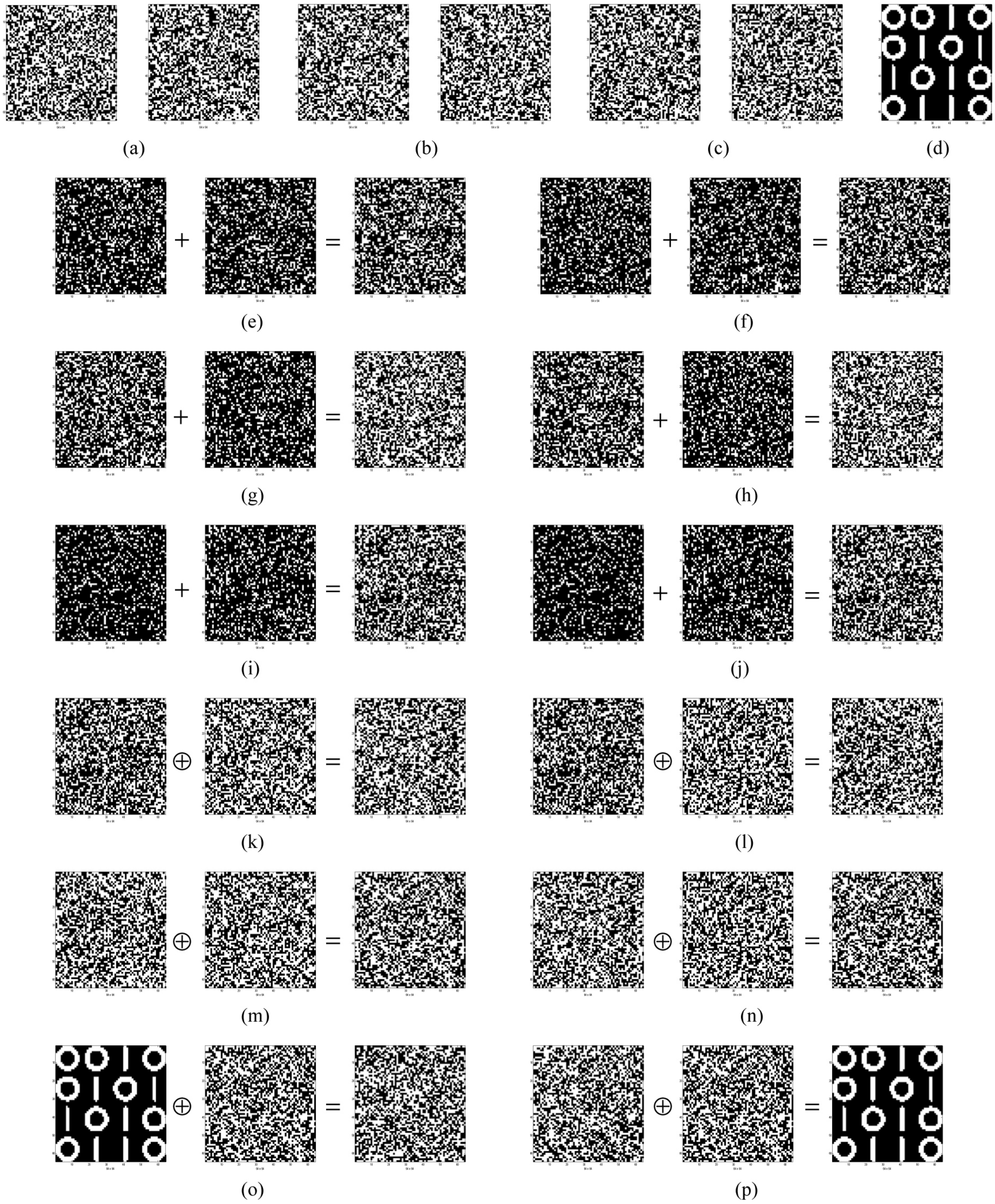
public key N_A and Bob's shared secret key S_B are displayed on SLM2 with its complements. SLM3 display the cipher text C and its complement. By the same logic operations as encryption, Bob's second public key N_B is acquired on CCD1 and the plain text P is decrypted on CCD2. Fig. 4(c) shows representations of input SLMs' data and output CCDs' data about the processes.

One of the advantages of the proposed optical cryptosystem is that it has dual outputs simultaneously. One is to generate the first public key and the shared secret key, the other is to generate the second public key and the encrypted cipher text. Also, the encryption optical setup can be used as decryption optical setup only by changing the inputs of SLMs. Another advantage of this optical setup is that it is convenient to alter the private keys at their own discretion. Changing of those private keys does not affect encryption and decryption of a plain text, because the encryption and decryption keys are changed according to the other user's private key change directly.

IV. NUMERICAL SIMULATION AND PERFORMANCE ANALYSIS

4.1. Numerical Simulation of the Proposed Optical Asymmetric Cryptosystem

Generally, an optical information processing system has an inherent merit of 2-D data processing in parallel and fast processing time. This means that the optical cryptosystem with 2-D arrayed data can perform huge data processing, and the optical cryptosystem with 2-D arrayed key can have very long key length. In this paper, we perform the simulation with 2-D arrayed data format which consists of binary 64 × 64 bits for convenience, where white areas have value of '1' and black areas have value of '0' numerically. Also, this



(a) (b) (c) (d)

(e) (f)

(g) (h)

(i) (j)

(k) (l)

(m) (n)

(o) (p)

FIG. 5. Numerical simulation for performing the feasibility of the proposed cryptosystem: (a) two randomly generated numbers $\boldsymbol{G}$ and $\boldsymbol{H}$ between Alice and Bob, (b) two randomly generated number $\boldsymbol{A}$ and $\boldsymbol{X}$ as Alice's private keys, (c) two randomly generated number $\boldsymbol{B}$ and $\boldsymbol{Y}$ as Bob's private keys, (d) a plain text $\boldsymbol{P}$ to be encrypted, (e) $(\boldsymbol{G} \cdot \boldsymbol{A})+(\boldsymbol{H} \cdot \boldsymbol{A})=\boldsymbol{K_A}$, (f) $(\boldsymbol{G} \cdot \boldsymbol{B})+(\boldsymbol{H} \cdot \boldsymbol{B})=\boldsymbol{K_B}$, (g) $\boldsymbol{K_B}+(\boldsymbol{G} \cdot \boldsymbol{A})$, (h) $\boldsymbol{K_A}+(\boldsymbol{G} \cdot \boldsymbol{B})$, (i) $\{\boldsymbol{K_B}+(\boldsymbol{G} \cdot \boldsymbol{A})\} \cdot \overline{H}+H \cdot \overline{G}=\boldsymbol{S_A}$, (j) $\{\boldsymbol{K_A}+(\boldsymbol{G} \cdot \boldsymbol{B})\} \cdot \overline{H}+H \cdot \overline{G}=\boldsymbol{S_B}$, (k) $\boldsymbol{S_A} \oplus \boldsymbol{X}=\boldsymbol{N_A}$, (l) $\boldsymbol{S_B} \oplus \boldsymbol{Y}=\boldsymbol{N_B}$, (m) $\boldsymbol{N_B} \oplus \boldsymbol{X}=\boldsymbol{E_A}$, (n) $\boldsymbol{N_A} \oplus \boldsymbol{Y}=\boldsymbol{E_B}$, (o) $\boldsymbol{P} \oplus \boldsymbol{E_A}=\boldsymbol{C}$, (p) $\boldsymbol{C} \oplus \boldsymbol{E_B}=\boldsymbol{P}$.

implies that the security key length of the cryptosystem has 64×64=4,096 bits which is very much longer key length compared to the conventional 1-D key length of electronic cryptography. Figure 5 shows numerical simulations for performing the feasibility of the proposed asymmetrical cryptosystem. Fig. 5(a) shows two randomly generated numbers $\boldsymbol{G}$ and $\boldsymbol{H}$ in prerequisite between Alice and Bob, which are open to public and anyone can access to it. Figs. 5(b) and (c) show two randomly generated numbers $\boldsymbol{A}$ and $\boldsymbol{X}$ as Alice's private keys and two randomly generated numbers $\boldsymbol{B}$ and $\boldsymbol{Y}$ as Bob's private keys, respectively. These private keys are used for generating the public keys, the shared secret key and encryption/decryption key. Fig. 5(d) represents a plain text $\boldsymbol{P}$ to be encrypted, which is chosen as a binary image intentionally in order to show the processing data patterns visually. Figs. 5(e) and (f) show Alice's first public key $\boldsymbol{K_A}$ and Bob's first public key $\boldsymbol{K_B}$ by AND and OR logic operations, respectively. Figs. 5(g) and (h) express the results obtained from pre-calculation before generating the shared secret keys, respectively. Figs. 5(i) and (j) show Alice's shared secret key $\boldsymbol{S_A}$ and Bob's shared secret key $\boldsymbol{S_B}$ by AND and OR logic operations with random numbers $\boldsymbol{G}$ and $\boldsymbol{H}$, respectively. From these figures, we know these two data patterns are exactly the same and therefore these keys will be used as a shared secret key between Alice and Bob. Figs. 5(k) and (l) show Alice's second public key $\boldsymbol{N_A}$ and Bob's second public key $\boldsymbol{N_B}$ by XOR logic operation, respectively. Fig. 5(m) shows Alice's encryption key $\boldsymbol{E_A}$ obtained by XOR logic operation of Bob's second public key $\boldsymbol{N_B}$ and Alice's private key $\boldsymbol{X}$, and Fig. 5(n) shows Bob's decryption key $\boldsymbol{E_B}$ obtained by XOR logic operation of Alice's second public key $\boldsymbol{N_A}$ and Bob's private key $\boldsymbol{Y}$. As shown in Figs. 5(m) and (n), the resultant output keys have exactly the same pattern. Fig. 5(o) represents a cipher text $\boldsymbol{C}$ by Alice's encryption key $\boldsymbol{E_A}$, and Fig. 5(p) represents a decrypted text $\boldsymbol{D}$ by Bob's decryption key $\boldsymbol{E_B}$. As expected, the decrypted data pattern is exactly the same as the original plain text $\boldsymbol{P}$. From the figures shown as (e), (f), (i), (j), (k) and (l), the patterns of the public keys and the shared keys look like a kind of random pattern because of the randomness in the private key and the common public numbers. Therefore, the pattern of the cipher text $\boldsymbol{C}$ also looks like a random pattern due to the random-like encryption key.

4.2. Performance Analysis

For the purpose of verifying the proposed asymmetric cryptosystem algorithm and of showing the effectiveness in the proposed optical cryptosystem, the security performance of the proposed system is analyzed. The first consideration for analyzing cryptographic algorithms is security strength of the cryptosystem, which depends on 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, a long encryption key takes more time than a short key to find the correct key. Generally, if a key has N-bits key length, 2^N attempts are required for a successful brute force attack. Moreover, because the optical cryptosystem has inherently a key length of N×M bits with 2-D array, $2^{N\times M}$ brute force attacks are required. In this paper, the key length of the cryptosystem is set to be 64×64=4,096 bits so that $2^{64\times 64} = 2^{4,096}$ brute force attacks are required, which needs very huge attack time to find the correct key.

In addition to the 2-D arrayed longer key length, the proposed asymmetrical cryptosystem uses the 3DES algorithm. The D-H secret key sharing algorithm has the disadvantage of suffering from the "meet in the middle" attack problem. But, the 3DES algorithm using even double keys also provides more security than simply DES encrypting twice, because it protects against "meet in the middle" attacks. From Eq. (17), the cipher text $\boldsymbol{C}$ contains three independent security keys. The first is the shared secret key of $\boldsymbol{S}$, the second is Bob's private key $\boldsymbol{Y}$, the third is Alice's private key $\boldsymbol{X}$. According to cryptanalysis, triple encryption by three independent keys gives us much security strength and is much harder to know the key. If attackers want to know the total encryption key $\boldsymbol{E_A} = \boldsymbol{S}\oplus\boldsymbol{Y}\oplus\boldsymbol{X}$, they must know both the random number $\boldsymbol{X}$ and the random number $\boldsymbol{Y}$. But, these random numbers are Alice's and Bob's private keys which are not open to public. In this paper, because two private random numbers $\boldsymbol{X}$ and $\boldsymbol{Y}$ have 64 × 64 bits of 2-D array, the combination between random numbers $\boldsymbol{X}$ and $\boldsymbol{Y}$ of $(2^{64\times64})\times(2^{64\times64})= 2^{4,096\times4,096}$ attempts are required in order to find $\boldsymbol{Y}\oplus\boldsymbol{X}$. Also, attackers must know the shared secret key $\boldsymbol{S}$ which is not open to public, too. This shared secret key is also very hard to know. Then, the combination of three keys $\boldsymbol{S}$, $\boldsymbol{X}$ and $\boldsymbol{Y}$ takes $(2^{64\times64}) \times (2^{64\times64}) \times (2^{64\times64})= 2^{4,096\times4,096\times4,096}$ brute force attacks to find the total encryption key $\boldsymbol{E_A} = \boldsymbol{S}\oplus\boldsymbol{Y}\oplus\boldsymbol{X}$.

In order to examine "meet in the middle" attack with a cipher text, we analyze decryption error rate according to possible attacks inferred by the open public keys $\boldsymbol{K_A}$, $\boldsymbol{K_B}$, $\boldsymbol{N_A}$ and $\boldsymbol{N_B}$, which are given by Eqs. (7), (8), (12) and (13). Because the XOR combination of $\boldsymbol{X}\oplus\boldsymbol{Y}$ can be easily achieved by XOR operation with $\boldsymbol{N_A}$ and $\boldsymbol{N_B}$, that is $\boldsymbol{N_A}\oplus \boldsymbol{N_B} = \boldsymbol{X}\oplus\boldsymbol{Y}$, we vary the first public keys $\boldsymbol{K_A}$, $\boldsymbol{K_B}$ and the shared secret key $\boldsymbol{S}$ specifically in the total encryption key $\boldsymbol{E_A}$. We restrict possible attacks into 6 cases in this paper. Nevertheless, the shared secret key $\boldsymbol{S}$ has logical combination of four random numbers $\boldsymbol{G}$, $\boldsymbol{H}$, $\boldsymbol{A}$ and $\boldsymbol{B}$ as shown in Eq. (11). Figure 6 shows the decryption error rate according to possible attacks inferred by the open public keys. The attack key ($\boldsymbol{A_k}$) is assumed to be inferred as

(case 1) $\boldsymbol{K_A}=(\boldsymbol{G}\cdot \boldsymbol{A})\oplus(\boldsymbol{H}\cdot \boldsymbol{A}), \boldsymbol{K_B}=(\boldsymbol{G}\cdot \boldsymbol{B})\oplus(\boldsymbol{H}\cdot \boldsymbol{B}),$
$\boldsymbol{S}=(\boldsymbol{K_B}+\boldsymbol{G}\cdot \boldsymbol{A}) \cdot \overline{H}$

(case 2) $\boldsymbol{K_A}=(\boldsymbol{G}\cdot \boldsymbol{A})+(\boldsymbol{H}\cdot \boldsymbol{A}), \boldsymbol{K_B}=(\boldsymbol{G}\cdot \boldsymbol{B})+(\boldsymbol{H}\cdot \boldsymbol{B}),$
$\boldsymbol{S}=(\boldsymbol{K_B}+\boldsymbol{G}\cdot \boldsymbol{A}) \cdot \overline{H}$

(case 3) $\boldsymbol{K_A}=(\boldsymbol{G}\cdot \boldsymbol{A}) \oplus(\boldsymbol{H}\cdot \boldsymbol{A}), \boldsymbol{K_B}=(\boldsymbol{G}\cdot \boldsymbol{B})\oplus(\boldsymbol{H}\cdot \boldsymbol{B}),$
$\boldsymbol{S}=(\boldsymbol{K_B}+\boldsymbol{G}\cdot \boldsymbol{A}) \cdot \overline{H}+H$

(case 4) $\boldsymbol{K_A}=(\boldsymbol{G}\cdot\boldsymbol{A})+(\boldsymbol{H}\cdot\boldsymbol{A})$, $\boldsymbol{K_B}=(\boldsymbol{G}\cdot\boldsymbol{B})+(\boldsymbol{H}\cdot\boldsymbol{B})$,

$\boldsymbol{S}=(\boldsymbol{K_B}+\boldsymbol{G}\cdot\boldsymbol{A})\cdot\overline{H}+H$

(case 5) $\boldsymbol{K_A}=(\boldsymbol{G}\cdot\boldsymbol{A})\oplus(\boldsymbol{H}\cdot\boldsymbol{A})$, $\boldsymbol{K_B}=(\boldsymbol{G}\cdot\boldsymbol{B})\oplus(\boldsymbol{H}\cdot\boldsymbol{B})$,

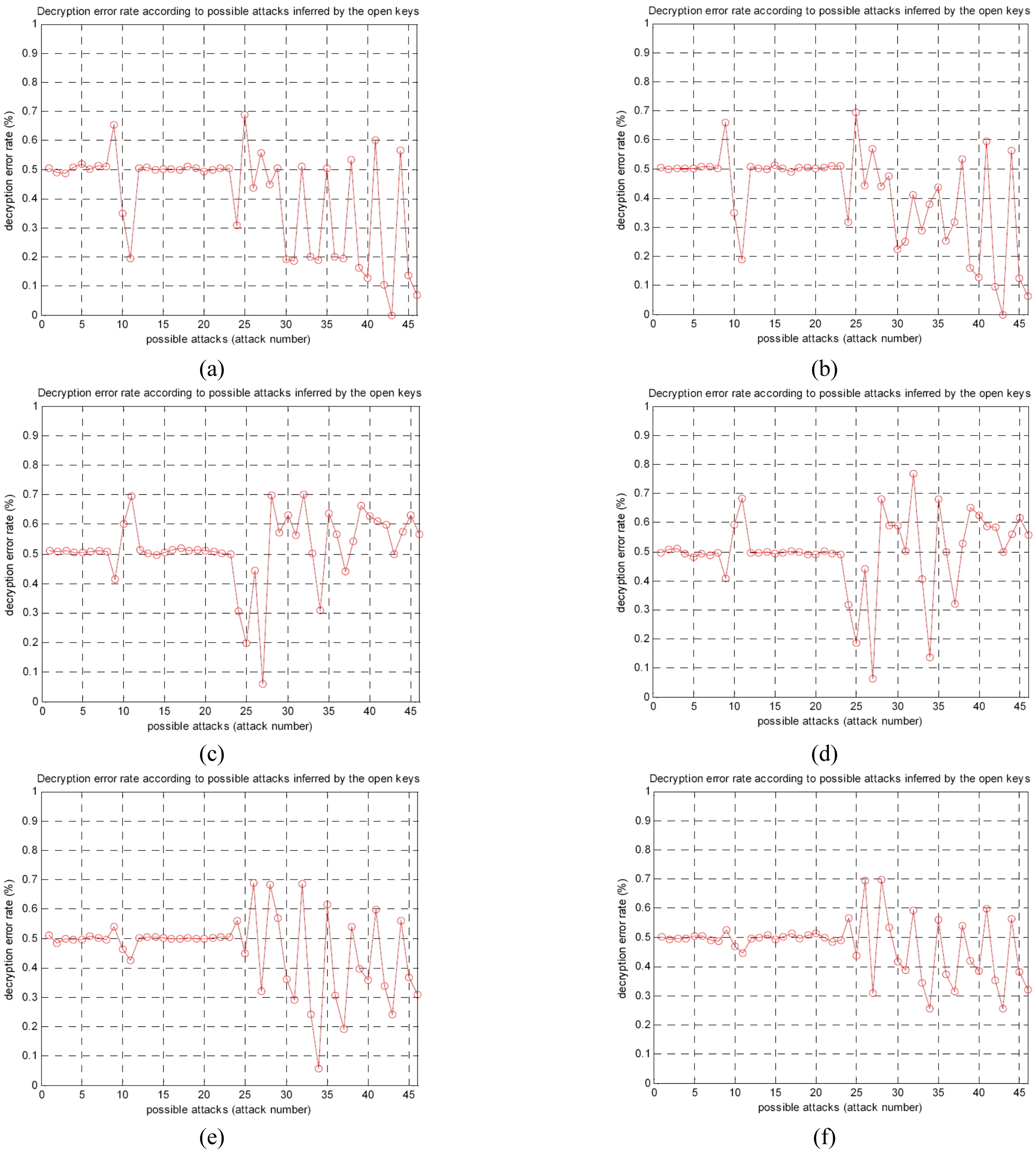
$\boldsymbol{S}=(\boldsymbol{K_B}+\boldsymbol{G}\cdot\boldsymbol{A})\cdot\overline{H}+H\cdot\overline{G}$

(case 6) $\boldsymbol{K_A}=(\boldsymbol{G}\cdot\boldsymbol{A})+(\boldsymbol{H}\cdot\boldsymbol{A})$, $\boldsymbol{K_B}=(\boldsymbol{G}\cdot\boldsymbol{B})+(\boldsymbol{H}\cdot\boldsymbol{B})$,

$\boldsymbol{S}=(\boldsymbol{K_B}+\boldsymbol{G}\cdot\boldsymbol{A})\cdot\overline{H}+H\cdot\overline{G}$

For each case, Table 1 shows the average value of decryption error rate according to possible attacks from attack key 1 to attack key 46, where the average is calculated by 10 times trials to the corresponding attack case.

From Figs. 6(a) and (b), the original plain text ***P*** is perfectly decrypted by attack key 43 in case 1 and case 2 because decryption error rate is evaluated as 0%. In the figures, decryption error rate of 50% means that the decrypted text is the same as a half of the plain text and decryption error rate of 100% means that the decrypted text is the exactly same as the reverse of the plain text. From Figs. 6(c) and (d), attack key 27 in case 3 and case 4 can reconstruct the plain text about 44% and 43.7% because decryption error rate is evaluated about 6% and 6.3%, respectively. Fig. 6(e) shows that attack key 34 in case 5 can reconstruct the plain text about 44.2% because decryption error rate is evaluated about 5.8%, and Fig. 6(f)



(a)

(b)

(c)

(d)

(e)

(f)

FIG. 6. Decryption error rate according to possible attacks inferred by the open public keys from Alice and Bob: the attack key($\boldsymbol{A_k}$) is inferred as (a) case 1, (b) case 2, (c) case 3, (d) case 4, (e) case 5, (f) case 6.

TABLE 1. Decryption error rate according to possible attacks inferred by the open public keys

Possible attacks		error rate (%)					
No	attack key (A_K)	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
1	G	50.5	50.5	50.9	49.7	51.0	50.0
2	H	49.3	49.2	50.6	50.8	48.5	49.3
3	$G \cdot H$	49.5	50.4	51.0	51.1	50.0	49.7
4	$G+H$	50.2	49.3	50.5	49.3	49.4	49.7
5	$G \oplus H$	50.5	49.0	50.3	48.2	49.5	50.3
6	$K_A \cdot K_B$	49.3	49.7	50.9	49.3	50.6	50.4
7	K_A+K_B	50.1	50.1	50.9	48.8	50.1	48.9
8	$K_A \oplus K_B$	50.6	50.5	50.8	49.6	49.6	48.8
9	$N_A \cdot N_B$	66.9	66.5	41.5	40.9	53.8	52.6
10	N_A+N_B	35.4	34.0	60.1	59.3	46.6	47.0
11	$N_A \oplus N_B$	18.3	17.7	69.4	68.4	42.5	44.7
12	$K_A \cdot N_A$	49.8	51.2	51.3	49.7	50.2	49.5
13	K_A+N_A	49.6	49.7	50.2	49.7	50.5	50.0
14	$K_A \oplus N_A$	49.4	48.6	49.6	50.0	50.3	50.7
15	$K_B \cdot N_B$	51.0	49.6	50.3	49.3	50.2	49.2
16	K_B+N_B	51.4	49.7	51.4	49.5	49.9	50.2
17	$K_B \oplus N_B$	50.2	50.2	51.8	50.2	49.8	51.3
18	$K_A \cdot N_B$	50.1	49.4	51.1	50.0	50.1	49.7
19	K_A+N_B	51.5	50.0	51.3	48.9	49.9	50.7
20	$K_A \oplus N_B$	51.1	50.8	50.9	48.9	49.9	51.3
21	$K_B \cdot N_A$	50.7	50.5	50.8	50.2	50.2	50.0
22	K_B+N_A	49.4	50.4	50.0	49.2	50.5	48.5
23	$K_B \oplus N_A$	48.5	50.1	50.0	49.1	50.3	48.8
24	$G \cdot (N_A \oplus N_B)$	31.4	32.2	30.7	31.8	56.0	56.5
25	$H \cdot (N_A \oplus N_B)$	68.7	68.2	19.6	18.5	44.9	43.7
26	$(G \cdot H) \cdot (N_A \oplus N_B)$	43.3	43.1	44.3	44.0	68.9	69.4
27	$(G+H) \cdot (N_A \oplus N_B)$	56.8	57.3	6.0	6.3	31.9	30.8
28	$(G \oplus H) \cdot (N_A \oplus N_B)$	43.4	42.5	69.7	68.0	68.3	69.6
29	$(K_A \cdot K_B) \cdot (N_A \oplus N_B)$	49.6	46.6	57.3	58.8	57.0	53.3
30	$(K_A \cdot K_B)+(N_A \oplus N_B)$	18.0	20.8	62.9	58.8	36.1	41.7
31	$(K_A \cdot K_B) \oplus (N_A \oplus N_B)$	18.2	24.4	56.4	50.1	29.2	38.7
32	$(K_A+K_B) \cdot (N_A \oplus N_B)$	49.5	40.3	70.0	76.8	68.5	59.2
33	$(K_A+K_B)+(N_A \oplus N_B)$	19.0	27.5	50.3	40.4	24.2	34.4
34	$(K_A+K_B) \oplus (N_A \oplus N_B)$	19.3	37.3	31.0	13.6	5.8	25.5
35	$(K_A \oplus K_B) \cdot (N_A \oplus N_B)$	49.7	43.8	63.4	68.0	61.5	56.3
36	$(K_A \oplus K_B)+(N_A \oplus N_B)$	19.3	24.3	56.7	49.9	30.6	37.4
37	$(K_A \oplus K_B) \oplus (N_A \oplus N_B)$	19.4	30.6	43.9	31.9	19.1	31.5
38	$\{(K_A \cdot K_B) \cdot (\sim H)\} \cdot (N_A \oplus N_B)$	53.1	52.9	54.2	52.7	53.9	53.8
39	$\{(K_A \cdot K_B) \cdot (\sim H)\}+(N_A \oplus N_B)$	15.0	14.5	66.1	65.2	39.5	41.9
40	$\{(K_A \cdot K_B) \cdot (\sim H)\} \oplus (N_A \oplus N_B)$	11.7	11.7	62.7	62.5	35.7	38.4
41	$\{(K_A+K_B) \cdot (\sim H)\} \cdot (N_A \oplus N_B)$	59.3	59.1	60.8	58.5	59.8	59.8
42	$\{(K_A+K_B) \cdot (\sim H)\}+(N_A \oplus N_B)$	9.5	9.0	59.9	58.4	33.8	35.2
43	$\{(K_A+K_B) \cdot (\sim H)\} \oplus (N_A \oplus N_B)$	0	0	49.8	49.9	24.0	25.7
44	$\{(K_A \oplus K_B) \cdot (\sim H)\} \cdot (N_A \oplus N_B)$	56.3	56.3	57.4	55.9	56.0	56.3
45	$\{(K_A \oplus K_B) \cdot (\sim H)\}+(N_A \oplus N_B)$	12.9	12.2	63.1	61.6	36.8	38.0
46	$\{(K_A \oplus K_B) \cdot (\sim H)\} \oplus (N_A \oplus N_B)$	6.6	6.0	56.4	55.7	30.9	32.0

shows that attack key 34 in case 6 can reconstruct the plain text about 24.5% because decryption error rate is evaluated about 25.5%. Figure 7 shows some decrypted text examples by the above mentioned attack keys. From the results of performance analysis, we select our asymmetric cryptosystem as case 6, which shows less decryption error rate than other cases. The maximum decryption error rate is evaluated as about 25.5%.

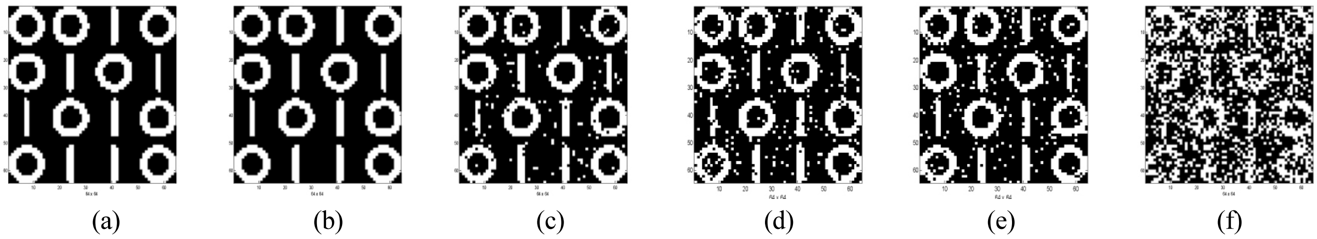


FIG.7. Some decrypted text examples by attack key: (a) when A_K is No.43 of case 1, (b) when A_K is No.43 of case 2, (c) when A_K is No.27 of case 3, (d) when A_K is No.27 of case 4, (e) when A_K is No.34 of case 5, (e) when A_K is No.34 of case 6.

V. CONCLUSION

In this paper, a novel asymmetrical cryptosystem combined with D-H secret key sharing and triple DES and its optical implementation are proposed. The proposed optical cryptosystem is realized by performing free-space interconnected optical logic operations such as AND, OR and XOR which are implemented in Mach-Zehnder type interferometer architecture. The advantage of the proposed optical architecture provides dual outputs simultaneously by generating the first public key and the shared secret key or by generating the second public key and the encrypted cipher text. Also, the encryption optical setup can be used as a decryption optical setup by changing only the displaying inputs of SLMs. The proposed cryptosystem can provide higher security strength than the conventional electronic algorithm, because the proposed method uses 2-D array data which can increase the key length surprisingly and uses 3DES algorithm which protects against “meet in the middle” attacks. Also, by using 3DES with independent three keys, XOR logic-based triple key encryption technique is implemented for enhancing security strength. Another advantage of the proposed asymmetrical cryptosystem is that it is free to change the user’s two private random numbers in generating the public keys at any time. Numerical simulation and performance analysis verify that the proposed asymmetric cryptosystem is effective and robust against attacks for the asymmetrical cipher system.

ACKNOWLEDGMENT

This work was supported by the Incheon National University (International Cooperative) Research Grant in 2013.

REFERENCES

1. W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. on Info. 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. P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, 767-769 (1995).
6. D. Weber and J. Trolinger, “Novel implementation of nonlinear joint transform correlators in optical security and validation,” Opt. Eng. **38**, 62-68 (1999).
7. E. Cuche, F. Bevilacqua, and C. Depeursinge, “Digital holography for quantitative phase-contrast imaging,” Opt. Lett. **24**, 291-293 (1999).
8. G. Unnikrishnan and K. Singh, “Double random fractional Fourier domain encoding for optical security,” Opt. Eng. **39**, 2853-2859 (2000).
9. 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).
10. B. M. Hennelly and J. T. Sheridan, “Random phase and jigsaw encryption in the Fresnel domain,” Opt. Eng. **43**, 2239-2249 (2004).
11. G. Situ and J. Zhang, “A lensless optical security system based on computer-generated phase only masks,” Opt. Commun. **232**, 115-122 (2004).
12. S. H. Jeon, Y. G. Hwang, and S. K. Gil, “Optical encryption of gray-level image using on-axis and 2-f digital holography with two-step phase-shifting method,” Opt. Rev. **15**, 181-186 (2008).
13. 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).
14. J.-W. Han, C.-S. Park, D.-H. Ryu, and E.-S. Kim, “Optical image encryption based on XOR operations,” Opt. Eng. **38**, 47-54 (1999).
15. C.-M. Shim and S.-J. Kim, “Image encryption using modified exclusive-OR rules and phase-wrapping technique,” Opt. Commun. **254**, 67-75 (2005).
16. S. K. Gil, “Optical CBC block encryption method using free space parallel processing of XOR operations,” Korean J. Opt. Photon. (Hankook Kwanghak Hoeji) **24**, 262-270 (2013).
17. S. H. Jeon and S. K. Gil, “Optical implementation of triple DES algorithm based on dual XOR logic operations,” J. Opt. Soc. Korea **17**, 362-370 (2013).
18. S. H. Jeon and S. K. Gil, “Optical secret key sharing method based on Diffie-Hellman key exchange algorithm,” J. Opt. Soc. Korea **18**, 477-484 (2014).