Journal of the Optical Society of Korea
Vol. 18, No. 5, October 2014, pp. 477-484

ISSN: 1226-4776(Print) / ISSN: 2093-6885(Online)
DOI: http://dx.doi.org/10.3807/JOSK.2014.18.5.477

Optical Secret Key Sharing Method Based on Diffie-Hellman Key Exchange Algorithm

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 July 14, 2014 : revised September 4, 2014 : accepted September 12, 2014)

In this paper, we propose a new optical secret key sharing method based on the Diffie-Hellman key exchange protocol required in cipher system. The proposed method is optically implemented by using a free-space interconnected optical logic gate technique in order to process XOR logic operations in parallel. Also, we present a compact type of optical module which can perform the modified Diffie-Hellman key exchange for a cryptographic system. Schematically, the proposed optical configuration has an advantage of producing an open public key and a shared secret key simultaneously. Another advantage is that our proposed key exchange system uses a similarity to double key encryption techniques to enhance security strength. This can provide a higher security cryptosystem than the conventional Diffie-Hellman key exchange protocol due to the complexity of the shared secret key. Results of numerical simulation are presented to verify the proposed method and show the effectiveness in the modified Diffie-Hellman key exchange system.

Keywords : Deffie-Hellman key exchange, Secret key sharing, Optical encryption, Cryptosystem
OCIS codes : (070.4560) Data processing by optical means; (200.3050) Information processing; (200.3760) Logic-based optical processing; (200.4660) Optical logic; (200.4960) Parallel processing

I. INTRODUCTION

Secure personal communication and information security of the public network are becoming more and more important with the progress in internet or mobile networks. According to demands for following such a trend of the times, information security technology has been developed for protecting information during data transmission in communication channels [1]. One of the cryptosystems was the private or symmetric key encryption method. In this method, two users, for example Alice and Bob, select a key in advance, which is their private key, then they use the key in a private key cryptosystem to communicate messages over the public channel. Sometimes they can change these keys periodically. However, this cryptosystem may have lost the private key when these keys are changed. To solve this problem, public key cryptography such as Diffie-Hellman key exchange protocol was introduced [2]. In this protocol, two users unknown to each other can set up a private but random key for their symmetric key cryptosystem. There is no need for Alice and Bob to meet in advance, or use some other secret means to select a key. In recent years, there has been increasing interest in the use of optical encryption methods for security systems [3-14]. In addition, we have presented several papers on the optical encryption techniques by using phase-shifting digital holography [15-19]. Optoelectronic methods using digital logic may be adequate for encryption. Some researchers reported XOR(exclusive OR)-based optical encryptions [20-22]. Recently, a technique using fractional Fourier transform based key exchange was reported [23]. However, until now there has been no other research to present an optical method of the Diffie-Hellman key exchange protocol.

In this paper, we propose a new optical secret key sharing method based on the Diffie-Hellman key exchange protocol, and show the performance of the proposed method. The secret key sharing algorithm is carried out optically by using dual free-space interconnected optical XOR logic operations. Section Ⅱ is organized as three parts. In the first part, the Diffie-Hellman key exchange algorithm is overviewed. The second part explains the proposed optical

*Corresponding author: skgil@suwon.ac.kr

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

secret key sharing method. In the third part, we propose an optical schematic and a compact optical module of the proposed system and explain the optical secret key sharing process. In Section Ⅲ, computer experiments confirm the performance by showing results of the shared secret key generation with the proposed method. Finally, conclusions are briefly summarized in Section Ⅳ.

II. THEORY

2.1. Diffie-Hellman Key Exchange Protocol

In 1976, Diffie and Hellman introduced a key exchange protocol [2]. The protocol is a specific algorithm of exchanging cryptographic keys. The Diffie-Hellman key exchange algorithm allows two users to exchange a shared secret key over an insecure communications medium without any prior secrets between each other. As to secret messages encryption, this shared key can be used to encrypt subsequent communications using a symmetric key cipher. In this protocol, two users(i.e., Alice and Bob) wish to communicate with 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 secret key for their private key system, using a public but authenticated channel. The Diffie-Hellman key exchange algorithm is as follows.

1. Alice and Bob agree upon and make public two numbers ***g*** and ***p***, where ***g*** is called a generator and ***p*** is a prime number. Note that anyone has access to these numbers in public.

2. Alice chooses a random number ***a*** and computes ***u*** by modulo ***p*** and sends it to Bob.

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

3. Bob chooses a random number ***b*** and computes ***v*** by modulo ***p*** and sends it to Alice.

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

4. Alice computes a secret key ***s****ₐ* by the same modulo ***p***.

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

5. Bob computes a secret key $\boldsymbol{s_b}$ by the same modulo ***p***.

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

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

$$s = s_a = s_b = g^{ab} \mod p \tag{5}$$

7. Both Alice and Bob store this shared secret key as a private key, and it will be used in message encryption to each other.

Figure 1 shows the Diffie-Hellman key exchange algorithm. As you see in Fig. 1, Alice generates a random number ***a*** and computes ***u*** by modulo arithmetic with a generator ***g*** and a prime number ***p***. Alice sends the computed values ***u*** to Bob as a public key. From the received Alice's public key, Bob computes a secret key $\boldsymbol{s_b}$ by the same modulo ***p*** arithmetic. Similarly, Alice computes a secret key $\boldsymbol{s_a}$ by Bob's public key and this secret key is the same as Bob's secret key to share. If an intruder Eve wants to compute the secret key ***s***, she would need either a random number ***a*** or a random number ***b***. Even though Eve notices the set {***g***, ***u***, ***v***}, which is now public information, it is not easy to get ***a*** or ***b*** from the set {***g***, ***u***, ***v***} because she needs to solve a discrete logarithm problem. There is no known algorithm to accomplish this problem in a reasonable amount of time. If the prime number ***p*** is large enough, a fair amount of time is needed to solve this discrete logarithm problem and it is not efficient and practical to calculate the solution by using brute force attack.

2.2. Proposed Optical Secret Key Sharing Method

Fundamentally, it is very difficult for the Diffie-Hellman key exchange 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 on an optical device properly. It may be possible to encode the prime number into binary digits by conversion. Despite these difficulties, we propose an optical secret key sharing method by modifying the Diffie-Hellman key exchange algorithm. In the proposed method, the conventional Diffie-Hellman key exchange algorithm can be modified to an optically realizable algorithm, where modulo arithmetic can be substituted with an XOR logic based encryption simply. Therefore, modulo arithmetic is

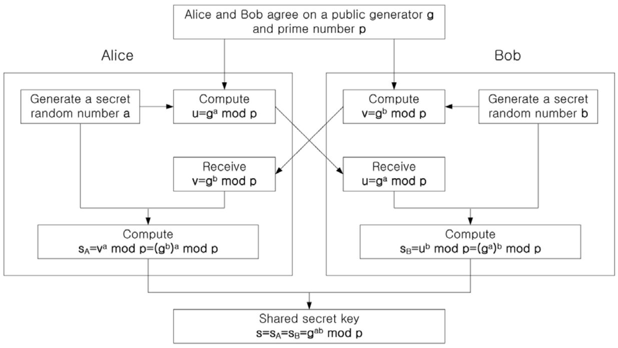

Alice and Bob agree on a public generator g and prime number p
Alice
Bob
Generate a secret random number a
Compute $u=g^{a}$ mod p
Compute $v=g^{b}$ mod p
Generate a secret random number b
Receive $v=g^{b}$ mod p
Receive $u=g^{a}$ mod p
Compute $s_A=v^{a}$ mod $p=(g^{b})^{a}$ mod p
Compute $s_B=u^{b}$ mod $p=(g^{a})^{b}$ mod p
Shared secret key $s=s_A=s_B=g^{ab}$ mod p

FIG. 1. Diffie-Hellman key exchange algorithm.

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. When we apply the XOR-based encryption method to the above Diffie-Hellman key exchange algorithm, the modified Diffie-Hellman key exchange algorithm proposed in this paper can be described as follows.

1. Alice and Bob agree upon and make public two numbers ***G*** and ***P***, where ***G*** is a generator number which is generated randomly and ***P*** is also a random number instead of a prime number. Note that anyone has access to these numbers in public.

2. Alice chooses a random number ***A*** and computes firstly ***GA*** and ***PA*** by Boolean AND logic operation. Next, Alice computes a public key ***K_A*** by XOR logic operation of these two values, and sends it to Bob.

$$K_A = GA \oplus PA = (G \oplus P)A \tag{6}$$

3. Bob chooses a random number ***B*** and computes firstly ***GB*** and ***PB*** by Boolean AND logic operation. Next, Alice computes a public key $\boldsymbol{K_B}$ by XOR logic operation of these two values, and sends it to Alice.

$$K_B = GB \oplus PB = (G \oplus P)B \tag{7}$$

4. Alice computes firstly $\boldsymbol{K_B A}$ by AND logic operation and computes a secret key $\boldsymbol{S_A}$ by XOR operation with ***P***.

$$\begin{aligned} S_A &= K_B A \oplus P = \{(GB \oplus PB)A\} \oplus P = \\ &= \{(G \oplus P)BA\} \oplus P = GBA \oplus PBA \oplus P \end{aligned} \tag{8}$$

5. Bob computes $\boldsymbol{K_A B}$ firstly by AND logic operation and computes a secret key $\boldsymbol{S_B}$ by XOR operation with ***P***.

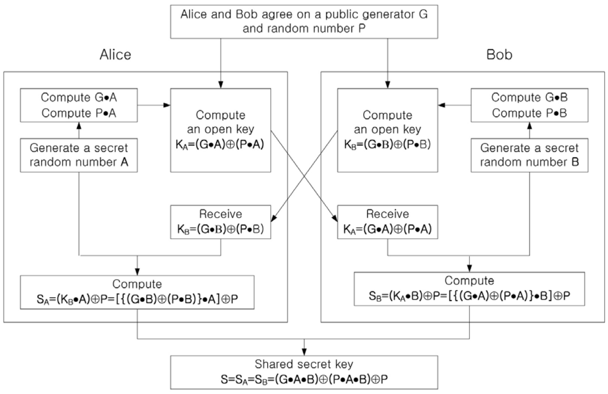
$$\begin{aligned} S_B &= K_A B \oplus P = \{(GA \oplus PA)B\} \oplus P \\ &\{(G \oplus P)AB\} \oplus P = GAB \oplus PAB \oplus P \end{aligned} \tag{9}$$

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

$$S = S_A = S_B = GAB \oplus PAB \oplus P \tag{10}$$

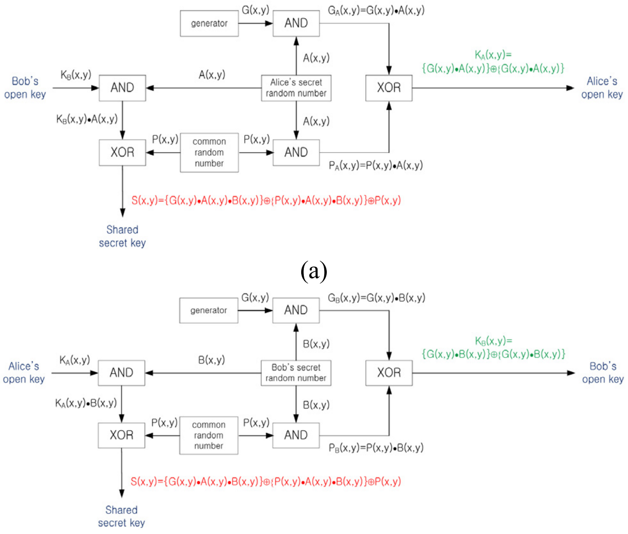
7. Both Alice and Bob store this shared secret key as a private key, and it will be used in message encryption.

Figure 2 shows the modified Diffie-Hellman key exchange algorithm, and Fig. 3 shows the flow charts for the proposed optical secret key sharing method. As shown in Fig. 2, Alice generates a secret random number **A** which is not open to public. Then, Alice pre-encrypts this random number **A** with a generator **G** and a random number **P** by AND logic operation at first. With these pre-encrypted values, **GA** and **PA**, Alice encrypts her own secret random number **A** again by XOR logic operation in order to open her public key $\mathbf{K_A}$. Alice sends this double encrypted key information $\mathbf{K_A}$ to Bob as public key. From the received Alice's public key, Bob computes a secret key $\mathbf{S_B}$ by AND operation with his secret random number **B** and its sequent XOR operation with **P**. Similarly, Alice computes a secret key $\mathbf{S_A}$ by Bob's public key, and this key is as same as Bob's secret key to share. Also, Fig. 3 shows that the proposed method has a realizable optical setup to provide the open public key and the shared secret key at the same time. In our proposed secret key sharing method,



Alice and Bob agree on a public generator G and random number P
Alice
Bob
Compute G•A Compute P•A
Generate a secret random number A
Compute an open key K_A=(G•A)⊕(P•A)
Receive K_B=(G•B)⊕(P•B)
Compute S_A=(K_B•A)⊕P=[{(G•B)⊕(P•B)}•A]⊕P
Compute an open key K_B=(G•B)⊕(P•B)
Compute G•B Compute P•B
Generate a secret random number B
Receive K_A=(G•A)⊕(P•A)
Compute S_B=(K_A•B)⊕P=[{(G•A)⊕(P•A)}•B]⊕P
Shared secret key S=S_A=S_B=(G•A•B)⊕(P•A•B)⊕P

FIG. 2. Modified Diffie-Hellman key exchange algorithm by using XOR logic operations.



(b)

FIG. 3. Flow charts for the proposed optical secret key sharing method: (a) Alice, (b) Bob.

we use an XOR-based double encryption. This technique is very similar to the triple DES (Data Encryption Standard) algorithm and was reported in the previous paper [22]. Most 3DES algorithms use two security keys. Double encryption by two security keys gives us much security strength, and it is much harder to break the key. If Eve wants to compute the secret key **S**, she must know either a random number **A** or a random number **B**. Although Eve notices the set {$\mathbf{K}_A$, $\mathbf{K}_B$}, which is now open to public, it is hard to get **A** and **B** from the set {**G**, **P**, $\mathbf{K}_A$, $\mathbf{K}_B$} because these secret numbers are double encrypted. The longer the length of these random numbers is, then Eve requires very much more time to break.

In our proposed method, one of the advantages is that it is a more advanced cryptosystem to exchange keys compared to the conventional Diffie-Hellman protocol because our method uses double encryption in making the public key and the shared secret key. Another advantage of this method is that it is convenient to change Alice's and Bob's secret random numbers in producing the public key and to exchange the public key without knowing the other user's private key directly. This means this method has a property that users can change the secret random numbers at their own discretion. The last merit is that the proposed optical method has an expansibility of key length in 2-dimensions, which strengthens the security of the cipher system.

2.3. Optical Implementation of the Proposed Method

Generally, an optical information processing system has an inherent advantage of 2-dimensional (2-D) data processing and fast parallel information processing time. This implies that the optical encryption system can have huge key length and vast data processing in the cryptosystem. For this reason, the public key and the shared secret key lengths can increasingly be chosen by expanding these keys to 2-D array, but this 2-D expansion does not increase processing speed. With these properties, we propose an optical implementation of the modified secret key sharing method which has 2-D page-typed input format, resulting in the same 2-D arrayed public key and the shared secret key output formats.

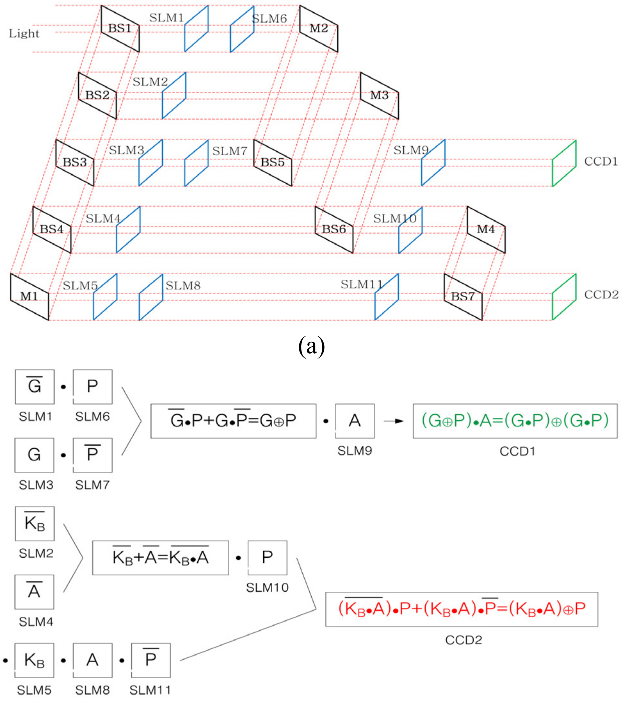
In this paper, the main idea of the proposed method is that the modified Diffie-Hellman key exchange algorithm is implemented in an optical way by using the bitwise XOR-based encryption technique with a free-space interconnected optical logic gate method. The advantage of the free-space interconnected optical logic gate method is that no cell encoding-decoding process is required and the output has the same format as the input. In the optical configuration of a logic gate, binary input variables are spatially dual encoded by using two's complement [22]. The architecture of XOR logic operation can be made by combining the logic AND scheme with the logic OR scheme. The 2-dimensional XOR logic operation is expressed as follows simply.

$$X(x,y) \oplus Y(x,y) = X(x,y) \bullet \overline{Y}(x,y) + \overline{X}(x,y) \bullet Y(x,y), \tag{11}$$

where symbols •, +, and ⊕ represent AND, OR and XOR logic operations, and $\overline{X}$ means the complement of X.

Referring to the modified Diffie-Hellman key exchange algorithm by using XOR logic operations shown in Fig. 2, we design the proposed optical Diffie-Hellman key exchange configuration with optical components such as mirrors, beam splitters(BSs), and spatial light modulators(SLMs). In this configuration, all the SLMs are used as free-space interconnected optical logic gates. Figure 4(a) shows the optical schematic for the proposed optical Diffie-Hellman key exchange method so as to generate an open public key and a shared secret key simultaneously, which is based on the dual free-space interconnected AND, OR and XOR logic operations for binary data. Schematically, the optical setup contains three Mach-Zehnder type interferometers. Four beam splitters BS1, BS2, BS3 and BS4 divide a collimated light into two lights and three beam splitters BS5, BS6 and BS7 combine these divided lights into one light, resulting in records on two CCDs. Also, this architecture is composed of eleven SLMs which are used for displaying data inputs.

In order to investigate operating principles of the optical



(a)

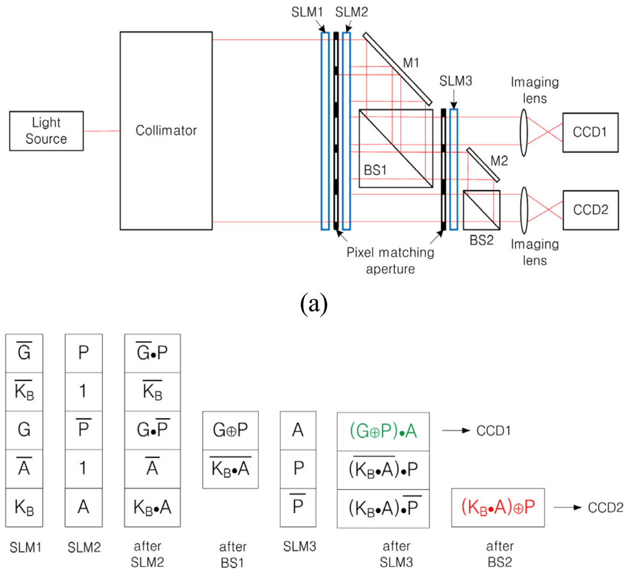
$\overline{G}$ • P
SLM1 SLM6
G • $\overline{P}$
SLM3 SLM7
$\overline{G}$•P+G•$\overline{P}$=G⊕P • A
SLM9
(G⊕P)•A=(G•P)⊕(G•P)
CCD1
$\overline{K_B}$
SLM2
$\overline{A}$
SLM4
$\overline{K_B}$+$\overline{A}$=$\overline{K_B•A}$ • P
SLM10
($\overline{K_B•A}$)•P+(K_B•A)•$\overline{P}$=(K_B•A)⊕P
CCD2
• K_B • A • $\overline{P}$
SLM5 SLM8 SLM11

(b)

FIG. 4. Proposed optical Diffie-Hellman key exchange method to generate a shared secret key: (a) optical schematic using dual free-space interconnected XOR logic operations, (b) representations of input SLMs' data and output CCDs' data.

schematic, the flow charts for the proposed optical secret key sharing method shown in Fig. 3 are considered. For convenience, let us consider Alice's open public key and shared secret key generation procedure shown in Fig. 3(a). 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 are arranged with a purpose of operating optical AND, OR and XOR logics 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 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. First, Alice pre-encrypts her secret random number(A) with a common generator(G) and a random number(P). To do this pre-encryption, G and P are displayed on SLM3 and SLM6, while the complements of these numbers, $\overline{G}$ and $\overline{P}$, are displayed on SLM1 and SLM7, respectively. Therefore, $G\oplus P$ is propagated after BS5 and goes to SLM9 which displays Alice's random number(A). After passing through SLM9, the resultant light represents Alice's open public key $G\oplus P \cdot A$ which is recorded on CCD1 and is sent to Bob. Second, Bob's received open public key(K_B) and Alice's random number(A) are displayed on SLM5 and SLM8, while the complements of these, $\overline{K_B}$ and $\overline{A}$, are displayed on SLM2 and SLM4 respectively. When the light continuously passes SLM5 and SLM8 in series, this operation gives optical AND logic of K_B and A, that is $K_B \cdot A$. On the other hand, the combined light after passing through BS6 represents optical NAND logic between $\overline{K_B}$ and $\overline{A}$, that is $\overline{K_B}+\overline{A}=\overline{K_B \cdot A}$. At this time, when a common random number(P) and its complement($\overline{P}$) are displayed on SLM10 and SLM11, two optical AND operations occurs. The one is $(\overline{K_B \cdot A}) \cdot P$, the other is $(K_B \cdot A) \cdot \overline{P}$. Finally, the resultant combined light by these two lights, which is recorded on CCD2 in the form of $(K_B \cdot A) \oplus P$, represents the shared secret key of Alice. This secret key is used to encrypt Alice's message transmitted to Bob. Fig. 4(b) shows representations of input SLMs' data and output CCDs' data about the processes.

The proposed optical schematic for the secret key sharing method shown in Fig. 4(a) can also be fabricated in the form of an optical module. This module is implemented by rearranging the optical elements geometrically and by reducing the number of SLMs and mirrors. Figure 5(a) shows the simplified optical module for the proposed Diffie-Hellman key exchange architecture. In this module, pixel matching apertures are placed in front of SLMs for the purpose of blocking the unwanted diffraction wave propagation and of pixel matching between SLMs, and the imaging lens plays a role of another pixel matching between output image pattern and CCD pixel array. The advantage of this module is that it can be manufactured compactly and can be used for realistic applications. Figure 5(b) shows representations of input SLMs' data and output CCDs' data in the process of light propagation, and also it shows light distribution after passing through SLM2, BS1, SLM3 and BS2.



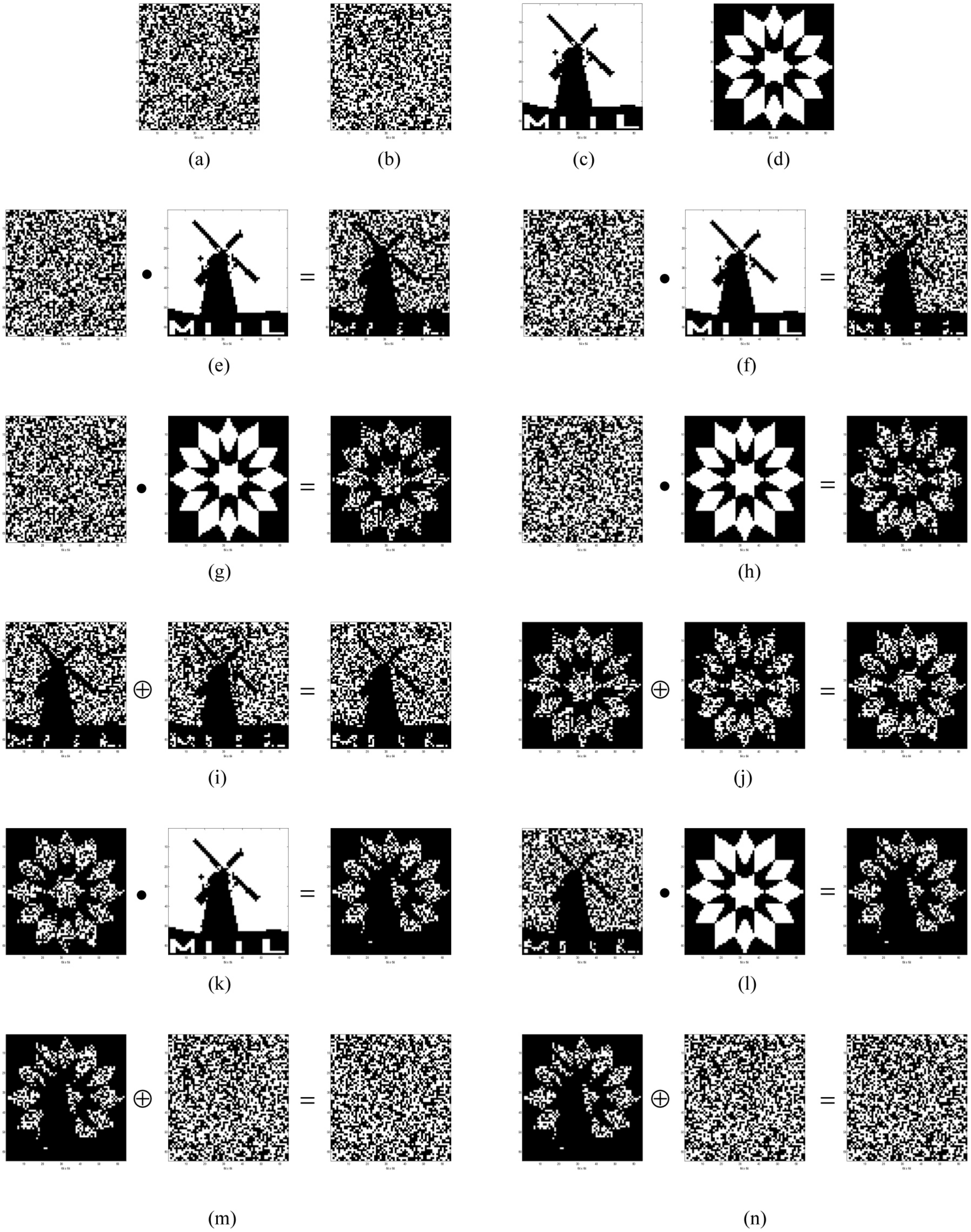
(a)

(b)

FIG. 5. Optical implementation for the proposed secret key sharing based on Diffie-Hellman key exchange architecture: (a) the proposed optical module, (b) representations of input SLMs' data and output CCDs' data.

III. COMPUTER EXPERIMENTS

In order to verify the proposed method and show the effectiveness in the modified Diffie-Hellman key exchange system, we carry out numerical simulations. In our method, input data to be processed is binary bit data or a binary image. In computer simulations, all input data have the form of page-typed 2-D arrays which consists of 64×64 binary pixels for convenience. This data size provides the total heights of SLM1 and SLM2 shown in Fig. 5(a) with 64×5=320 pixels, which is easily obtained by the practical SLM. Also, this means 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. If we expand the data size to 128×128 pixels array, then the height of SLM increases twice to 128×5=640 pixels which is also allowable in the practical SLM, and the key length increases to 16,384 bits surprisingly.



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

(e) (f)

(g) (h)

(i) (j)

(k) (l)

(m) (n)

FIG. 6. Numerical simulations: (a) a generator G in public, (b) a random number P in public, (c) a binary mill image A as Alice's secret number, (d) a binary flower image B as Bob's secret number, (e) G AND A, (f) P AND A, (g) G AND B, (h) P AND B, (i) K_A=(G AND A) XOR (P AND A), (j) K_B=(G AND B) XOR (P AND B), (k) K_B AND A, (l) K_A AND B, (m) (K_B AND A) XOR P, (n) (K_A AND B) XOR P.

A generator G shown in Fig. 6(a) is a random generated binary code and is used like a common key for pre-encrypting Alice's secret random number, where white areas have value of 1 and black areas are 0 numerically. Figure 6(b) shows another random generated binary code which is also used in Alice's secret random number pre-encryption. Figure 6(c) and (d) show Alice's and Bob's secret images respectively, where we use binary images instead of random number in order to show the processing data patterns visually. Figure 6(e) and (f) express AND-based Alice's secret image pre-encryption results with a generator G and P, $G \cdot A$ and $P \cdot A$, respectively. The similar pre-encryptions about Bob's secret image, $G \cdot B$ and $P \cdot B$, are shown in Fig. 6(g) and (h). Figure 6(i) represents continuously XOR-based encryption result $(G \oplus P) \cdot A$ between the pre-encrypted $G \cdot A$ and $P \cdot A$ of Alice's secret image according to Eq. (6), and Fig. 6(j) represents continuously $(G \oplus P) \cdot B$ between the pre-encrypted $G \cdot B$ and $P \cdot B$ of Bob's secret image according to Eq. (7). These two encrypted keys are exchanged with each other as public keys and are used to generate the shared secret keys to the opposite user. Figure 6(k) and (l) show the computed result of $K_B \cdot A$ and $K_A \cdot B$, respectively. From these figures, we know these two data patterns are exactly same because of $K_B \cdot A = (G \oplus P) \cdot B \cdot A = (G \oplus P) \cdot A \cdot B = K_A \cdot B$. The final shared secret keys are computed by $(K_B \cdot A) \oplus P$ and $(K_A \cdot B) \oplus P$ according to Eqs. (8) and (9). The generation processes of the shared secret key are shown in Fig. 6(m) and (n). As shown in Fig. 6(m) and (n), the resultant output keys have exactly the same pattern and therefore they will be used as a shared secret key between them.

IV. CONCLUSION

In this paper, we propose a new optical secret key sharing method based on the Diffie-Hellman key exchange protocol required in encryption systems. The proposed optical secret key sharing method is realized by using optical XOR logic operations to modify the Diffie-Hellman key exchange algorithm, where XOR logic operation is implemented by using a free-space interconnected optical logic gate method. The optical schematic of the proposed method consists of three Mach-Zehnder type interferometers to perform dual XOR logic operations. Also, we present a compact type of optical module. Schematically, the proposed optical module has a merit of being able to produce the open public key and the shared secret key simultaneously with a compact form. Our proposed key exchange system uses a kind of double key encryption technique which consequently enhances security strength. This can provide a higher security cryptosystem than the conventional Diffie-Hellman key exchange protocol due to the double encrypted complexity of a shared secret key. 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 parallel processing property despite increase in 2-D data. Another advantage of this method is that it is convenient to change the user's secret random number in generating the open public key and to exchange the public key without knowing the other user's private key directly. This means our method has a property that users can change secret random numbers at their own discretion. Computer experiments verify that the proposed method is effective and suitable for the Diffie-Hellman key exchange system and secure communication system. To the best of our knowledge, this proposed optical schematic may be the first report on the Diffie-Hellman key exchange protocol by optical means.

ACKNOWLEDGMENT

This work was supported by the Incheon National University (International Cooperative) Research Grant in 2012.

REFERENCES

1. B. Schneier, *Applied Cryptography*, 2nd ed. (John Wiley, New York, USA, 1994).
2. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. on Info. Theory **22**, 644-654 (1976).
3. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752-1756 (1994).
4. 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).
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. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng. **37**, 565-569 (1998).
7. D. Weber and J. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," Opt. Eng. **38**, 62-68 (1999).
8. E. Cuche, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging," Opt. Lett. **24**, 291-293 (1999).
9. B. Javidi and T. Nomura, "Securing information by means of digital holography," Opt. Lett. **25**, 28-30 (2000).
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 Fraesnel domain," Opt. Eng. **43**, 2239-2249 (2004).
13. G. Situ and J. Zhang, "A lensless optical secyrity system based on computer-generated phase only masks," Opt. Commun. **232**, 115-122 (2004).
14. T. Nomura, A. Okazaki, M. Kameda, and Y. Morimoto, "Image reconstruction from compressed encrypted digital hologram," Opt. Eng. **44**, 2313-2320 (2005).
15. S. K. Gil, S. H. Jeon, N. Kim, and J. R. Jeong, "Successive encryption and transmission with phase-shifting digital holography," Proc. SPIE **6136**, 339-346 (2006).
16. 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).
17. S. H. Jeon and S. K. Gil, "QPSK modulation based optical image cryptosystem using phase-shifting digital holography," J. Opt. Soc. Korea **14**, 97-103 (2010).
18. S. H. Jeon and S. K. Gil, "2-step phase-shifting digital holographic optical encryption and error analysis," J. Opt. Soc. Korea **15**, 244-251 (2011).
19. S. H. Jeon and S. K. Gil, "Dual optical encryption for binary data and secret key using phase-shifting digital holography," J. Opt. Soc. Korea **16**, 263-269 (2012).
20. 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).
21. C.-M. Shin and S.-J. Kim, "Image encryption using modified exclusive-OR rules and phase-wrapping technique," Opt. Commun. **254**, 67-75 (2005).
22. 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).
23. A. Sinha, "Fractional Fourier transform based key exchange for asymmetric key cryptography," in *Proc. the 6th WSEAS Int. Conf. on Electronics, Hardware and Optical Communications* (Corfu Island, Greece, Feb. 2007), pp. 51-54.