Optical Asymmetric Cryptography Modifying the RSA Public-key Protocol

Seok Hee Jeon¹ and Sang Keun Gil²*

¹Department of Electronic Engineering, Incheon National University, Incheon 22012, Korea
²Department of Electronic Engineering, The University of Suwon, Hwaseong 18323, Korea

(Received November 29, 2019 : revised January 10, 2020 : accepted January 28, 2020)

A new optical asymmetric cryptosystem is proposed by modifying the asymmetric RSA public-key protocol required in a cryptosystem. The proposed asymmetric public-key algorithm can be optically implemented by combining a two-step quadrature phase-shifting digital holographic encryption method with the modified RSA public-key algorithm; then two pairs of public-private keys are used to encrypt and decrypt the plaintext. Public keys and ciphertexts are digital holograms that are Fourier-transform holograms, and are recorded on CCDs with 256-gray-level quantized intensities in the optical architecture. The plaintext can only be decrypted by the private keys, which are acquired by the corresponding asymmetric public-key-generation algorithm. Schematically, the proposed optical architecture has the advantage of producing a complicated, asymmetric public-key cryptosystem that can enhance security strength compared to the conventional electronic RSA public-key cryptosystem. Numerical simulations are carried out to demonstrate the validity and effectiveness of the proposed method, by evaluating decryption performance and analysis. The proposed method shows feasibility for application to an asymmetric public-key cryptosystem.

Keywords: Optical encryption, Phase-shifting digital holography, Asymmetric cryptography, RSA, Public key

OCIS codes: (060.4785) Optical security and encryption; (090.1995) Digital holography; (090.2880) Holographic interferometry; (070.1170) Analog optical signal processing; (070.4560) Data processing by optical means

I. INTRODUCTION

With the rapid development of computer techniques, information security has garnered a great deal of interest recently. Basically, conventional electronic encryption methods are used widely in communication networks, but they have many weaknesses in the aspects of encryption-security strength, information-processing capacity, and processing time. In the past two decades various optical encryption techniques adopting optical information processing have been investigated for cryptography and security systems. Refregier and Javidi introduced an optical encryption method named double random-phase encoding (DRPE) [1]. Subsequently, Matoba and Javidi expanded the DRPE method to an encrypted optical memory system using three-dimensional keys in the Fresnel domain [2]. Double random-fractional-Fourier-transform-domain encoding for optical security was studied by Unnikrishnan and Singh [3]. Liu et al. proposed an image-encryption method in gyrator transform domains [4]. Moreover, Chen et al. proposed optical image encryption based on diffractive imaging [5], and Meng et al. reported hierarchical image encryption based on a cascaded iterative phase-retrieval algorithm in the Fresnel domain [6]. An asymmetric cryptosystem based on phase-truncated Fourier transformation was presented by Qin and Peng [7]. Some researchers have proposed optical encryption systems using a polarization-encoding technique [8, 9]. Multiple-image encryption by wavelength multiplexing was also developed by Situ and Zhang [10]. Hybrid optical and digital encryption methods using joint transform correlators (JTC) [11, 12] or optical XOR logic operations [13, 14] were another processing option for cryptosystems. To implement the phase component, which is the most widely used information for real-time digital
information processing, holographic recording may be required. Some methods to deal with the phase information in a cryptosystem have been studied in recent decades, such as digital holography [15, 16] and phase-shifting interferometry [17, 18]. Especially the two-step phase-shifting digital holographic technique [19-22] is more efficient than a multistep technique in a cryptosystem, due to less data handling.

Basically, encryption algorithms are categorized as symmetric or asymmetric cryptosystems. Symmetric cryptosystems have the problem of key delivery and management: A secret key must be transmitted to the receiver before the message can be transmitted. However, electronic communication is insecure unless communication channels are guaranteed with security and authentication. In contrast to symmetric encryption, asymmetric cryptosystems do not need to exchange keys, thus eliminating the key-distribution problem. Recently, some research about optical asymmetric cryptography have been reported [23-28]. Peng et al. proposed asymmetric cryptography based on wave front sensing [23], and Qin and Peng proposed an asymmetric cryptosystem based on phase-truncated Fourier transformation [7]. Since then, various optical asymmetric cryptosystems have been proposed using random binary phase modulation [24], phase truncation and phase retrieval [25], a joint-transform correlator [26], and equal-modulus decomposition in the Fresnel-transform domain [27]. The other type of asymmetric optical cryptography combines an optical encryption technique with a non-optical public-key algorithm [28-31].

In this paper, we propose optical asymmetric cryptography that combines two-step quadrature phase-shifting digital holography with a modified RSA public-key algorithm. After the sender performs two-step phase-shifting digital holography encryption with two random numbers, two public keys of digital holograms are generated by the modified RSA algorithm, and two private keys are kept in secret simultaneously. With these released public keys, the receiver encrypts a plaintext into three ciphertexts by applying the same two-step phase-shifting digital holography encryption and transmits them to the sender, in which the three ciphertexts are also generated as digital holograms. Then the transmitted ciphertexts are decrypted by the sender with the help of the private keys. The proposed asymmetric cryptosystem not only overcomes the disadvantages of symmetric-key cryptography such as key exchange, but also increases the level of security and convenience of key management. In Section II, the conventional RSA public-key protocol is briefly reviewed. Also, the proposed optical asymmetric cryptography (combining two-step phase-shifting digital holography with the modified RSA public-key algorithm) and the cryptographic process are described in detail. In Section III, the results of numerical simulations verify the feasibility and effectiveness of the proposed method. In Section IV, a security analysis is discussed. Finally, the conclusions are summarized in Section V.

II. THEORY

2.1. RSA Public-Key Protocol

In 1976, Diffie and Hellman introduced the concept of an asymmetric public-private key cryptosystem [32]. However, they had a problem in realizing a one-way function, due to the difficulty of factoring. This one-way function was realized by R. Rivest, A. Shamir, and L. Adleman, and asymmetric public-key cryptography was reported in their paper in 1978 [33], which was the first public-key cryptography, known as the RSA protocol, and is now widely used for security system. In the RSA protocol, the asymmetry is based on the fact that it is easy to multiply two large prime numbers together, but mathematically hard and time-consuming to find those prime factors from the result. A public key is created by using two large prime numbers, and then is released to the public. The prime numbers must be kept secret at this time. A message to be encrypted can be ciphered by anyone with this released public key, and the ciphered message can be decrypted only with the private decryption key. The RSA algorithm is briefly summarized as follows:

1. User A selects two prime numbers $p$ and $q$ randomly.
2. User A calculates $n = pq$ and $f = (p-1)(q-1)$.
3. User A selects an integer $e$ and determines an integer $d$ such that $ed = 1 \mod f$, where ‘mod’ denotes the modulo operation.
4. User A releases $\{e, n\}$ as public keys and $\{d, f\}$ are kept secret as private keys.
5. User B encrypts a plain text $P$ with public keys $\{e, n\}$:
   \[ C = P^e \mod n. \]  
   (1)
6. User A decrypts a cipher text $C$ with private keys $\{d, n\}$:
   \[ P = C^d \mod n. \]  
   (2)

2.2. Proposed Optical Asymmetric Cryptography

To implement the RSA public-key protocol optically, we need an optical means to realize a prime number and modulo operation. In this paper, we propose that a prime number is replaced by a randomly generated number, and modulo operation is substituted by phase-shifting digital holography. Therefore, the conventional RSA public-key protocol can be modified to an optically realizable asymmetric cryptography algorithm. Figure 1 shows the optical schematic for the proposed asymmetric cryptography, using two-step quadrature phase-shifting digital holography based on orthogonal polarization. The proposed asymmetric public-key cryptosystem is described as follows.

The optical schematic consists of a Mach-Zehnder-type interferometer. The polarization direction of $P_1$ is $45^\circ$ with respect to the horizontal axis. The collimated light is divided into two linear polarized plane waves by a beam splitter (BS1). The downward light passing through a
shutter (S1) is used as the object beam and performs XOR logic operation, while the forward light passing through another shutter (S2) is used as the reference beam and performs the two-step phase-shifting digital holography. The cryptographic principle of two-step phase-shifting digital holography using orthogonal polarization was described in the paper [21].

In the first step of generating public keys, user A selects two randomly generated numbers \( p(x, y) \) and \( q(x, y) \) (instead of prime numbers), which are not open to the public. Four spatial light modulators (SLM1, SLM2, SLM3, and SLM4) are placed in the object beam path and perform the optical XOR logic operation by the inner product, pixel by pixel. In this configuration, binary data \( p \) are displayed on SLM1, while its complement \( \overline{p} \) is displayed on SLM3. Also, other binary data \( q \) are displayed on SLM4, while its complement \( \overline{q} \) is displayed on SLM2. Combining the light results in the optical XOR logic operation. With these random numbers, user A calculates a function \( a(x, y) \) as

\[
a(x, y) = p(x, y) \oplus q(x, y),
\]

where \( x \) and \( y \) are coordinates in the spatial domain. Suppose that \( M_{\theta}(x, y) = \exp\{j\theta(x, y)\} \) is a random-phase-mask function, where \( \theta(x, y) \) is randomly distributed uniformly on the interval \([0, 2\pi]\). An object beam function from multiplication of these two functions is expressed as

\[
\tilde{a}(x, y) = a(x, y)M_{\theta}(x, y) = a(x, y)e^{j\theta(x, y)}.
\]

In the proposed digital holographic encryption system, the function \( a(x, y) \) is also used as a holographic-encryption-key function. This key is multiplied by \( \pi \) (radians) to represent a binary phase \( \theta(x, y) = \pi a(x, y) \). Then a holographic-encryption-key function \( g(x, y) \) of unit amplitude is expressed as a random phase pattern, which is represented on a phase-type SLM5 as a reference beam.

\[
g(x, y) = e^{j\pi a(x, y)} = e^{j\pi[p(x, y)\oplus q(x, y)]}.
\]

In Fig. 1, two lenses (L1, L2) make the object and reference beams respectively perform Fourier transforms onto the CCDs. The Fourier-transformed functions of Eqs. (4) and (5) are supposed to be \( A(\alpha, \beta) \) and \( G(\alpha, \beta) \) respectively, where \( \alpha \) and \( \beta \) are coordinates in the spatial frequency domain.

\[
A(\alpha, \beta) = F\{\tilde{a}(x, y)\} = |A(\alpha, \beta)|e^{j\Delta \phi A},
\]

\[
G(\alpha, \beta) = F\{g(x, y)\} = |G(\alpha, \beta)|e^{j\Delta \phi G},
\]

where \( F\{\cdot\} \) denotes Fourier transformation. A \( \lambda/4 \)-plate, which sets the fast axis along the vertical axis, carries out quadrature phase-shifting interferometry. After the 45° linearly polarized light passes through the \( \lambda/4 \)-plate, a \( \pi/2 \) phase shift of \( s \)-polarized light is obtained only on the horizontal axis, while no phase shift of \( p \)-polarized light occurs on the vertical axis. Then two interferograms with a phase shift of \( \pi/2 \) are recorded on the CCDs.

\[
I_A(\alpha, \beta) = |A(\alpha, \beta)|^2 + |G(\alpha, \beta)|^2 + 2|A(\alpha, \beta)||G(\alpha, \beta)|\cos \Delta \phi A,
\]

\[
I_G(\alpha, \beta) = |A(\alpha, \beta)|^2 + |G(\alpha, \beta)|^2 + 2|A(\alpha, \beta)||G(\alpha, \beta)|\cos \Delta \phi G - \frac{\pi}{2},
\]

where \( \Delta \phi G = \phi_A(\alpha, \beta) - \phi_A(\alpha, \beta) \) is the phase difference between the object and reference beams.

Each hologram recorded on CCD1 and CCD2, \( X_1 = I_A(\alpha, \beta) \) and \( X_2 = I_G(\alpha, \beta) \), is assumed to be quantized with 256 gray levels, which are treated as random, noise like ciphered data. Meanwhile, only the object beam’s intensity distribution \( X_1 = |A(\alpha, \beta)|^2 \) is obtained on CCD1.
by blocking the reference beam. Similarly, only the reference beam’s intensity $X_i = |G(\alpha, \beta)|^2$ is obtained on CCD1 by blocking the object beam. After calculating the dc term as $DC_1 = X_3 + X_4$ and the ac term as $A_1 = X_1 - DC_1, A_2 = X_2 - DC_1$, three cipher intensities $A_1, A_2, A_3$ are acquired.

$$A_1 = 2|A(\alpha, \beta)| |G(\alpha, \beta)| \cos \Delta \varphi_{AG},$$  \hspace{1cm} (10)

$$A_2 = 2|A(\alpha, \beta)| |G(\alpha, \beta)| \sin \Delta \varphi_{AG},$$  \hspace{1cm} (11)

$$A_3 = DC_1 = |A(\alpha, \beta)|^2 + |G(\alpha, \beta)|^2.$$  \hspace{1cm} (12)

These three intensities $\{A_1, A_2, A_3\}$ are stored in a computer, and two intensities $\{A_1, A_2\}$ among them are released as a public-key group for plaintext encryption. Next, user A computes binary numbers $e(x, y), n(x, y),$ and $f(x, y)$ by a proper thresholding calculation:

$$e(x, y) = TH[A_1(x, y)],$$  \hspace{1cm} (13)

$$n(x, y) = TH[A_2(x, y)],$$  \hspace{1cm} (14)

$$f(x, y) = TH[A_3(x, y)],$$  \hspace{1cm} (15)

where $TH\{\cdot\}$ is a threshold function to produce binary data, 0 or 1, by a proper threshold value. In this paper, each threshold value is taken as the mean of the intensities $A_1, A_2,$ and $A_3$, respectively. User A determines a decryption key $\{d, f\}$ by XOR logic operation with these three acquired numbers; it is kept secret in the private-key group $\{d, f\}$, while $\{A_1, A_2\}$ are released as public keys:

$$d(x, y) = n(x, y) \oplus f(x, y) \oplus e(x, y).$$  \hspace{1cm} (16)

In the second step of generating a ciphertext, user B computes the same binary number $e(x, y), n(x, y)$ from the released public keys $\{A_1, A_2\}$ by the same thresholding calculation as user A. In the same optical schematic as user A’s setup, a plaintext P is displayed on SLM1 while its compliment $\overline{P}$ is displayed on SLM3. Also, a function $e_b(x, y) = e(x, y) \oplus n(x, y)$ is displayed on SLM4, while its compliment $\overline{e_b}$ is displayed on the SLM2. The combined light results in a function $b(x, y)$ by optical XOR logic operation:

$$b(x, y) = P(x, y) \oplus e(x, y) \oplus n(x, y).$$  \hspace{1cm} (17)

Suppose that $M_b(x, y) = \exp[\mathrm{i} \theta_b(x, y)]$ is a random-phase-mask function in user B’s digital holographic cryptosystem, where $\theta_b(x, y)$ is randomly distributed uniformly on the interval [0, 2\pi]. The multiplication of the function $b(x, y)$ and the random phase mask $M_b(x, y)$ gives an object wave signal as

$$\tilde{b}(x, y) = b(x, y)M_b(x, y) = b(x, y)e^{\mathrm{i} \theta_b(x, y)}.$$  \hspace{1cm} (18)

In user B’s digital holographic encryption system, the function $e_b(x, y) = e(x, y) \oplus n(x, y)$ is also used as a holographic-encryption-key function. Then a randomly distributed phase pattern of the holographic-encryption-key function $k(x, y)$ of unit amplitude is expressed as a reference wave signal:

$$k(x, y) = e^{\pm e_b(x, y)} = e^{\pm e(x, y) \oplus n(x, y)}.$$  \hspace{1cm} (19)

Then two interferograms with a phase shift of $\pi/2$ are recorded on the CCDs are

$$I_B^1(\alpha, \beta) = |B(\alpha, \beta)|^2 + |K(\alpha, \beta)|^2$$

$$+ 2|B(\alpha, \beta)| |K(\alpha, \beta)| \cos \Delta \varphi_{BK},$$  \hspace{1cm} (20)

$$I_B^2(\alpha, \beta) = |B(\alpha, \beta)|^2 + |K(\alpha, \beta)|^2$$

$$+ 2|B(\alpha, \beta)| |K(\alpha, \beta)| \cos \left(\Delta \varphi_{BK} - \frac{\pi}{2}\right),$$  \hspace{1cm} (21)

where $B(\alpha, \beta)$ and $K(\alpha, \beta)$ are Fourier-transforms functions of Eqs. (18) and (19) respectively, and $\Delta \varphi_{BK} = \phi(\alpha, \beta) - \phi$ is the phase difference between object and reference beams.

Similarly, assuming $Y_1 = I_B^1(\alpha, \beta), \ Y_2 = I_B^2(\alpha, \beta), \ Y_3 = |B(\alpha, \beta)|^2, \ \text{and} \ Y_4 = |K(\alpha, \beta)|^2$, three cipher intensities $B_1, B_2,$ and $B_3$ are acquired after dc term removal, calculating

$$B_1 = 2|B(\alpha, \beta)| |K(\alpha, \beta)| \cos \Delta \varphi_{BK},$$  \hspace{1cm} (22)

$$B_2 = 2|B(\alpha, \beta)| |K(\alpha, \beta)| \sin \Delta \varphi_{BK},$$  \hspace{1cm} (23)

$$B_3 = DC_2 = |B(\alpha, \beta)|^2 + |K(\alpha, \beta)|^2.$$  \hspace{1cm} (24)

In the third step of retrieving the plaintext, user A computes a complex hologram expressed as

$$H_B(\alpha, \beta) = A_B e^{\Delta \varphi_{BK}}$$

$$= |B(\alpha, \beta)| |K(\alpha, \beta)| e^{\mathrm{i}(\varphi(\alpha) - \varphi(B))},$$  \hspace{1cm} (25)

where the amplitude component $A_B$ and the phase difference $\Delta \varphi_{BK}$ are calculated from the received ciphertexts $\{B_1, B_2, B_3\}$ as

$$A_B = |B(\alpha, \beta)| |K(\alpha, \beta)| = \frac{1}{2} \sqrt{(B_1)^2 + (B_2)^2},$$  \hspace{1cm} (26)

$$\Delta \varphi_{BK} = \varphi(B) - \varphi_K = \tan^{-1}\left(\frac{B_2}{B_1}\right).$$  \hspace{1cm} (27)
The Fourier transform of the holographic-decryption-key function can be acquired by user A’s private keys \( \{d, f\} \) such that \( e_h = e \oplus n = d \oplus f = d_h \) according to Eq. (16):

\[
K(\alpha, \beta) = F^{-1}\{e^{i\phi_{A}(x,y)}\} = F\{e^{i\phi_{D}(x,y)}\} = \{d \oplus f\}(\alpha, \beta),
\]

(28)

The complex distribution of the object wave expressed as Eq. (18) is reconstructed by using the complex hologram \( H_B(\alpha, \beta) \) and the holographic-decryption-key function \( K(\alpha, \beta) \), and the object-wave-signal function \( b(x, y) \) is restored by inverse Fourier transformation:

\[
R(\alpha, \beta) = \frac{H_B(\alpha, \beta) K(\alpha, \beta)}{K(\alpha, \beta)} = B(\alpha, \beta),
\]

(29)

\[
r(x, y) = |F^{-1}\{R(\alpha, \beta)\}| = |b(x, y)|
\]

(30)

where \( F^{-1}\{\cdot\} \) denotes inverse Fourier transformation. In the last process, user A decrypts the plain-text \( P \) with private keys \( \{d, f\} \) by XOR logic operation, as the public-key function \( e_h = e \oplus n \) is related to the private-key function \( d_h = d \oplus f \) such that \( e \oplus n = d \oplus f \) from Eq. (16):

\[
u(x, y) = r(x, y) \oplus d_h(x, y)
\]

\[
= P(x, y) \oplus \{e(x, y) \oplus n(x, y)\} \oplus \{d(x, y) \oplus f(x, y)\}
\]

(31)

In the proposed asymmetric public-key algorithm, a two-key encryption technique is used. The first key is the generated public key \( \{e, n\} \) and private key \( \{d, f\} \), the second key consists of the holographic encryption and decryption keys \( \{e_h, d_h\} \) that are made from \( \{e, n\} \) and \( \{d, f\} \) respectively. This two-key method provides stronger security than a one-key encryption method. Conventional ciphertexts expressing digital data may have a weakness to

FIG. 2. Block diagrams for the proposed optical asymmetric cryptography using digital holography: (a) generation of public keys and decryption key, (b) encryption of a plaintext, (c) decryption of ciphertext.
crytanalysis by existing attacks, such as known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. However, if the ciphertexts have an analog format, as in the proposed method, the cryptosystem is very robust against the attacks. Moreover, if we hide the public-key information by encrypting that key using digital holography, then enhanced security strength will be achieved between the sender and the receiver, although attackers know the released public keys. The main point of the conventional RSA protocol is to draw two distinct prime numbers from the entire space of prime numbers. However, it is much easier and less time consuming to generate a random number than to obtain a large prime number. Also, if the key is truly random and kept completely secret, then it will be impossible to decrypt or break the resulting cipher. Figure 2 shows block diagrams of the encryption and decryption processes for the proposed optical asymmetric cryptography using digital holography. Figures 2(a)–2(c) show the processes for generating public keys and the decryption key, encryption of a plaintext, and decryption of ciphertext, respectively. To realize the proposed method of Fig. 2 practically, the number of SLMs needs to be efficient in the optical setup, to avoid a bulky system. In the proposed optical schematic shown in Fig. 2, four SLMs (SLM1, SLM2, SLM3, and SLM4) in the object beam path can be reduced to one SLM, if the resultant data of XOR logic operation are precalculated in the processor. The proposed method of Fig. 2 practically, the number of SLMs needs to be efficient in the optical setup, to avoid a bulky system. In the proposed optical schematic shown in Fig. 2, four SLMs (SLM1, SLM2, SLM3, and SLM4) in the object beam path can be reduced to one SLM, if the resultant data of XOR logic operation are precalculated in the processor before being represented on the SLM. This reduction of SLMs can make the proposed optical system compact.

III. NUMERICAL SIMULATIONS

To experiment with the proposed algorithm of the optical schematic shown in Fig. 1, the optical setup consists of SLMs, which are the most important devices to represent input data. Unfortunately the optical experiment could not be performed, because SLMs are very expensive, and we did not have enough. Instead, numerical simulations were carried out to verify the feasibility of the proposed optical asymmetric cryptography, using MATLAB (R2018a). In this paper, binary data or images of size 256 × 256 pixels are used for simulation. The size of the data is dependent on the display capability of the SLM.

In the first step of generating public keys, Figs. 3(a) and 3(b) show randomly generated binary patterns as random numbers $p$ and $q$. Figure 3(c) shows a binary pattern $a = p \oplus q$ by XOR logic operation between $p$ and $q$. In user A’s digital holographic encryption system, the two-step phase-shifting digital holographic encryption system gives two intensity patterns, which are recorded on the CCDs with 256 quantized gray levels, in the form of a digital hologram. The first interferogram $X_1$ is recorded on CCD1 as Eq. (8) in the case where the phase shift is 0, while the second interferogram $X_2$ is recorded on the CCD2 as Eq. (9) in the case where the phase shift is $\pi/2$. In addition, the third intensity pattern $X_3$ is recorded on CD1 when only the object wave is considered, and the fourth intensity pattern $X_4$ is recorded on CD1 when only the reference wave is considered. Applying the dc-term-removal technique to Eqs. (8) and (9) gives two intensity patterns of Eqs. (10) and (11) as public keys $\{A_1, A_2\}$. Figures 4(a) and 4(b) show the ac terms of the intensity patterns $A_1$ and $A_2$, respectively. Furthermore, Fig. 4(c) shows the dc term intensity of $A_2$. After proper thresholding for these intensities is performed, randomly distributed binary numbers $e$, $n$, and $f$ are acquired, which are shown in Figs. 4(d)-4(f). With these generated binary numbers $e$, $n$, and $f$, a decryption key is determined by XOR logic operation as $d = n \oplus f \oplus e$. Figure 4(f) shows this decryption key as a private key.

In the second step of generating ciphertexts, the same binary numbers $e$ and $n$ are computed by the same thresholding for the released public keys $\{A_1, A_2\}$. A plaintext P is encrypted with these numbers $e$ and $n$. Figure 5(a) shows a plaintext P of the Lena image to be encrypted, Figs. 5(b) and 5(c) show the computed numbers $e$ and $n$, and Fig. 5(d) presents a resultant binary pattern $b$ from XOR logic operation as $b = P \oplus (e \oplus n)$. In user B’s digital holographic encryption system, user B generates a holographic-encryption-key function $e_b = e \oplus n$ that is used as a reference wave signal. Similarly, the two-step phase-shifting digital holographic encryption system gives four intensity patterns: the first interferogram $Y_1$ of Eq. (20), the second interferogram $Y_2$ of Eq. (21), the third intensity pattern $Y_3$ with only the

![Image](https://example.com/image.png)

**FIG. 3.** Binary random-number data: (a) a randomly generated number $p$, (b) a randomly generated number $q$, (c) bit pattern of $a = p \oplus q$ by XOR logic operation.
object wave, and the fourth intensity pattern $Y_4$ with only the reference wave. Applying the dc-term-removal technique to Eqs. (20) and (21) gives three intensity patterns of Eqs. (22)-(24) as cipher texts $\{B_1, B_2, B_3\}$. Figures 6(a) and 6(b) show the ac terms of the intensity patterns $B_1$ and $B_2$ respectively. Figure 6(c) shows the dc-term intensity of $B_3$.

In the third step of retrieving the plaintext, the decryption is performed by numerical calculation instead of optical decryption. The amplitude component $A_{BK}$ and phase difference $\Delta \phi_{BK}$ are calculated from the transmitted ciphertexts $\{B_1, B_2, B_3\}$, which makes a complex hologram $H_B$. Figures 7(a) and 7(b) show the amplitude map of $A_{BK}$ and phase map of $\Delta \phi_{BK}$. By using the complex hologram $H_B$ and the holographic-decryption-key function $K$ computed from the private keys $\{d, f\}$, the complex distribution $R$ of Eq. (29) is reconstructed. Inverse Fourier transformation of this complex distribution $R$ gives the restored function $r$, which is the same as the original function $b$ of Eq. (18).

Finally, the plaintext $P$ is decrypted with private keys $\{d, f\}$ by XOR logic operation as $r \oplus (d \oplus f)$. Figure 8 shows the results of reconstruction and decryption when the correct holographic decryption keys are used. Figure 8(a) shows the reconstructed image pattern obtained from complex hologram $H_B$ and the holographic-decryption-key function.
Figure 8(b) shows the correctly reconstructed binary data \( r = P \oplus (e \oplus n) = b \) from a proper threshold value for the reconstructed image pattern. Figure 8(c) shows the private keys \( d_h = d \oplus f \) for decryption. Figure 8(d) shows the correctly decrypted plaintext of the Lena image by XOR logic operation between the correctly reconstructed binary data \( r \) and the private key \( d_h \). As for a chosen-ciphertext attack, the cipher texts \( \{B_1, B_2, B_3\} \), acquired when the plaintext of the Lena image was encrypted in the former encryption stage, is assumed to be known by an eavesdropper. Figure 9 shows the results of a chosen-ciphertext attack on the proposed cryptosystem. Figure 9(a) shows a new plaintext \( P \) of a woman’s image to be encrypted. Figure 9(b) is the incorrectly reconstructed binary data \( r_i \) by the holographic encryption keys \( \{e, n\} \) used for decryption of the Lena image (instead of using correct \( e_i \oplus n_i \) for the woman-image decryption), and Fig. 9(c) is the private keys \( d_h = d \oplus f \) for Lena-image decryption as well. Figure 9(d) shows the incorrectly decrypted plaintext of the woman’s image by XOR operation between the incorrectly reconstructed binary data \( r_i \) and the private keys \( d_h \).

\[
K. \text{ Figure 8(b) shows the correctly reconstructed binary data } r = P \oplus (e \oplus n) = b \text{ from a proper threshold value for the reconstructed image pattern. Figure 8(c) shows the private keys } d_h = d \oplus f \text{ for decryption. Figure 8(d) shows the correctly decrypted plaintext of the Lena image by XOR logic operation between the correctly reconstructed binary data } r \text{ and the private key } d_h. \text{ As for a chosen-ciphertext attack, the cipher texts } \{B_1, B_2, B_3\}, \text{ acquired when the plaintext of the Lena image was encrypted in the former encryption stage, is assumed to be known by an eavesdropper. Figure 9 shows the results of a chosen-ciphertext attack on the proposed cryptosystem. Figure 9(a) shows a new plaintext } P \text{ of a woman’s image to be encrypted. Figure 9(b) is the incorrectly reconstructed binary data } r_i \text{ by the holographic encryption keys } \{e, n\} \text{ used for decryption of the Lena image (instead of using correct } e_i \oplus n_i \text{ for the woman-image decryption), and Fig. 9(c) is the private keys } d_h = d \oplus f \text{ for Lena-image decryption as well. Figure 9(d) shows the incorrectly decrypted plaintext of the woman’s image by XOR operation between the incorrectly reconstructed binary data } r_i \text{ and the private keys } d_h.\]
the key length of the proposed cryptosystem is set to be 256 bits in length, there are \(2^{256}\) possible keys for binary-key cryptography. As of 2002, an asymmetric-key length of 1,024 bits was generally considered by cryptology experts to be the minimum necessary for the RSA algorithm. Nevertheless, the National Institute of Standards and Technology (NIST) recommends 2,048-bit keys for the RSA cryptosystem until 2030. If the conventional one-dimensional key length for the RSA public-key cryptosystem has 1,024 bits, \(2^{1024}\) attempts are required for a successful brute-force attack. On the other hand, the optical cryptosystem has inherently a key length of \(M \times N\) bits with a two-dimensional array, so \(2^{M \times N}\) brute-force attacks are required. In this paper, the key length of the proposed cryptosystem is set to be 256 \(\times 256 = 65,536\) bits, so that \(2^{256} \times 256 = 265,536\) brute-force attacks are required. This means that the proposed RSA system has 32 times more security-key length than the one-dimensional key length of 1,024 bits for the conventional RSA public-key cryptosystem, and requires a huge amount of brute-force attack to find the correct key. Moreover, if the cipher has \(m\) levels in its data format, a tremendous number of brute-force attacks \(m^{M \times N}\) are required in cryptanalysis. In this paper, the public keys and ciphertext are acquired with 256 gray levels, so that \(256^{256} \times 256\) brute-force attacks are required to find the correct key theoretically.

The sensitivity of the proposed optical asymmetric cryptosystem to the plaintext decryption was tested. By altering the public key from the correct public key, some deviation could give a decryption with some error. The deviation is assumed to be missing bits randomly in the correct public key, which is performed by setting the values of the missing bits to zero. The normalized mean-square error (NMSE) between the original plaintext \(P(x, y)\) and the decrypted text \(\tilde{P}(x, y)\) is calculated as

\[
NMSE = \frac{\sum_{x,y} |P(x,y) - \tilde{P}(x,y)|^2}{\sum_{x,y} |P(x,y)|^2} \times 100%.
\]  

(32)

Similarly, the deviation from the correct ciphertexts is considered to give NMSE using Eq. (32). Figure 10 shows numerical results for NMSE with respect to the deviation from the correct public keys and the ciphertexts, when error is from 1 bit to 65,536 (256 \(\times 256\)) bits, where the binary Lena image is used as the plaintext for visual convenience. The NMSE evaluation is performed for each public key and ciphertext with 100 iterations. Figure 10(a) shows NMSE for the public keys \(A_1\) and \(A_2\), where the NMSE for the public key \(A_1\) and the public key \(A_2\) have similar values for error rate in the public key data, and \(A_1 + A_2\) means that the deviation occurs simultaneously in the public keys \(A_1\) and \(A_2\). As expected, the case of \(A_1 + A_2\) has larger NMSE than that of \(A_1\) and \(A_2\) alone. Figures 10(b) and 10(c) show the decrypted image with NMSE = 1.36% for 1% deviation error of the correct public key, and the decrypted image with NMSE = 53.87% for 10% deviation error, respectively. Figure 10(d) shows NMSE for the ciphertexts \(B_1\), \(B_2\) and \(B_3\), where \(B_1 + B_2\) means that the deviation occurs simultaneously in the ciphertexts \(B_1\) and \(B_2\). Similarly, the case of \(B_1 + B_2\) has larger NMSE than that of \(B_1\) and \(B_2\) alone. The NMSE for the ciphertext \(B_1\) and the ciphertext \(B_2\) have similar values for error rate in the cipher text data, while the NMSE for ciphertext \(B_3\) is 0%. This reflects the fact that the deviation from the ciphertext \(B_3\) does not affect the decrypted image at all. Figures 10(e) and 10(f) show the decrypted image with NMSE = 0.38% for 10% deviation error of \(B_1\) or \(B_2\) and the decrypted image with NMSE = 58.81% for 100% deviation error of \(B_1\) or \(B_2\) respectively. It is noted that Fig. 10(f) shows that 41% of the plaintext can be decrypted if only one ciphertext is correct, even though the other ciphertext is perfectly incorrect. From Fig. 10, the deviation from public keys affects the decrypted text more than the deviation from ciphertexts. The numerical results for NMSE are summarized in Table 1.
Next, system robustness against additive transmission noise is considered, to evaluate decryption error in the public keys and ciphertexts. Random noise is assumed to be introduced into the public keys and the ciphertexts. The transmitted public keys and ciphertexts with noise are expressed as $A_t = A + \text{Noise}$ and $B_t = B + \text{Noise}$ respectively. The additive random noise is assumed to be expressed by

$$\text{Noise} = \text{rand}(256) \times V_p \times P_L,$$

where $\text{rand}(256)$ denotes a $256 \times 256$ random variable distributed on the range $[0, 1]$, $V_p$ denotes a maximum peak-to-peak variation of the public keys $\{A_1, A_2\}$ or the ciphertexts $\{B_1, B_2\}$, and $P_L$ denotes a percentage of noise level. For example, if the percentage $P_L$ is $1\%$, then maximum peak-to-peak variation of noise level is $1\%$ of the maximum peak-to-peak variation of $V_p$. Figure 11 shows the numerical results for NMSE of the decrypted text with respect to the additive random noise in the public keys and ciphertexts, where the NMSE evaluation is performed for each public key and ciphertext with 1,000 iterations. Figure 11(a) shows the NMSE when the additive random noise level is from $0\%$ to $5\%$ for public keys and ciphertexts, and Figures 11(b) and 11(c) show the decrypted image with NMSE $= 48.12\%$ when the additive random noise level is $1\%$ for public keys and ciphertexts. Figure 11(d) shows the numerical results for NMSE with respect to the deviation from the correct public keys and ciphertexts, when deviation is from $1\%$ to $65,536$ ($256 \times 256$) bits (100 iterations): (a) NMSE for public keys $A_1$, $A_2$ and $A_1 + A_2$, (b) the decrypted image with NMSE $= 1.36\%$ for $1\%$ deviation error of $A_1$ or $A_2$, (c) the decrypted image with NMSE $= 53.87\%$ for $10\%$ deviation error of $A_1$ or $A_2$. (d) NMSE for ciphertexts $B_1$, $B_2$, $B_1 + B_2$, (e) the decrypted image with NMSE $= 0.38\%$ for $10\%$ deviation error of $B_1$ or $B_2$, (f) the decrypted image with NMSE $= 58.81\%$ for $100\%$ deviation error of $B_1$ or $B_2$.

<table>
<thead>
<tr>
<th>Tested data</th>
<th>Deviation (percentage of bits in error)</th>
<th>NMSE (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public key $(A_1, A_2)$</td>
<td>655 bits (1%)</td>
<td>1.36</td>
</tr>
<tr>
<td></td>
<td>3,275 bits (5%)</td>
<td>25.09</td>
</tr>
<tr>
<td></td>
<td>6,544 bits (10%)</td>
<td>53.87</td>
</tr>
<tr>
<td></td>
<td>13,107 bits (20%)</td>
<td>82.21</td>
</tr>
<tr>
<td>Public keys $(A_1 + A_2)$</td>
<td>655 bits (1%)</td>
<td>2.61</td>
</tr>
<tr>
<td></td>
<td>3,275 bits (5%)</td>
<td>44.69</td>
</tr>
<tr>
<td></td>
<td>6,544 bits (10%)</td>
<td>84.52</td>
</tr>
<tr>
<td></td>
<td>13,107 bits (20%)</td>
<td>100</td>
</tr>
<tr>
<td>Cipher text $(B_1, B_2)$</td>
<td>655 bits (1%)</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>3,275 bits (5%)</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>6,544 bits (10%)</td>
<td>0.38</td>
</tr>
<tr>
<td></td>
<td>13,107 bits (20%)</td>
<td>2.15</td>
</tr>
<tr>
<td>Cipher texts $(B_1 + B_2)$</td>
<td>655 bits (1%)</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>3,275 bits (5%)</td>
<td>0.28</td>
</tr>
<tr>
<td></td>
<td>6,544 bits (10%)</td>
<td>2.21</td>
</tr>
<tr>
<td></td>
<td>13,107 bits (20%)</td>
<td>13.69</td>
</tr>
</tbody>
</table>
Optical Asymmetric Cryptography Modifying the RSA … - Seok Hee Jeon and Sang Keun Gil

level is 1% for public keys, and the decrypted image with NMSE = 100% when the additive random noise level is 5%, respectively. Similarly, Fig. 11(d) shows the NMSE when the additive random noise level is from 0% to 5% for ciphertexts. Figures 11(e) and 11(f) show the decrypted image with NMSE = 1.61% when the additive random noise level is 2% for ciphertexts, and the decrypted image with NMSE = 41.05% when the additive random noise level is 5%, respectively. It is seen in Figs. 11(a) and 11(d) that the decrypted image can be correctly reconstructed when the additive random noise is below 0.5% for public keys and 1.5% for cipher texts, respectively. This means the proposed optical asymmetric cryptosystem has high robustness against the additive noise.

V. CONCLUSIONS

A new optical asymmetric public-key cryptosystem is proposed by modifying the conventional RSA public-key protocol, which is optically implemented by combining a two-step quadrature phase-shifting digital holographic encryption method with the modified RSA public-key algorithm. In the modified RSA public-key algorithm, two-key encryption technique is used. The first key is the generated public key of \( \{ e, n \} \) and private key of \( \{ d, f \} \), the second key is the holographic encryption and decryption keys that are also made from \( \{ e, n \} \) and \( \{ d, f \} \) respectively. The holographic encryption key is represented as the reference wave in Mach-Zehnder-type interferometry. This two-key method provides stronger security than a one-key encryption method. Public keys and ciphertexts are acquired as digital holograms, which are Fourier-transform holograms, and are recorded on CCDs with 256-gray-level quantized intensities in the digital holographic encryption architecture. This implies that the proposed digital holographic method provides an analog type of random pattern distribution in the ciphers. The use of a random pattern protects against a man-in-the-middle attack and the possibility of a replay attack, and thus enables the cryptosystem to have higher security strength. Moreover, if we hide the public-key information by encrypting that key using digital holography, then enhanced security strength will be acquired between the sender and the receiver, although attackers may know the released public keys. The plaintext can only be decrypted by the private keys, which are acquired by the asymmetric public-key-generation algorithm. Schematically, the proposed optical architecture

FIG. 11. Numerical results for NMSE with respect to the additive random noise (1,000 iterations): (a) NMSE when the additive random noise is from 0% to 5% for public keys, (b) the decrypted image with NMSE = 48.12% when the additive random noise is 1% for public keys, (c) the decrypted image with NMSE = 100% when the additive random noise is 5% for public keys, (d) NMSE when the additive random noise is from 0% to 5% for ciphertexts, (e) the decrypted image with NMSE = 1.61% when the additive random noise is 2% for ciphertexts, (f) the decrypted image with NMSE = 41.05% when the additive random noise is 5% for ciphertexts.

Optical Asymmetric Cryptography Modifying the RSA … - Seok Hee Jeon and Sang Keun Gil
has the advantage of producing a complicated asymmetric public-key cryptosystem, compared to the electronic RSA public-key cryptosystem. The results of numerical simulations, including decryption-error analysis, verify that the proposed asymmetric optical public-key encryption method shows the feasibility and effectiveness of a highly secure asymmetric public-key cryptosystem.

ACKNOWLEDGMENT

This work was supported by the Incheon National University (International Cooperative) Research Grant in 2017.

REFERENCES