Optics Communications 309 (2013) 50–56

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Asymmetric cryptosystem and software design based on two-step phase-shifting interferometry and elliptic curve algorithm

Desheng Fan [a], Xiangfeng Meng [a,*], Yurong Wang [a], Xiulun Yang [a], Xiang Peng [b], Wenqi He [b], Guoyan Dong [c], Hongyi Chen [d]

[a] Department of Optics, School of Information Science and Engineering and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan 250100, China
[b] College of Optoelectronics Engineering, Shenzhen University, Shenzhen 518060, China
[c] College of Materials Science and Opto-Electronic Techology, University of Chinese Academy of Sciences, Beijing 100049, China
[d] College of Electronic Science and Technology, Shenzhen University, Shenzhen 518060, China

ARTICLE INFO

Article history:
Received 26 April 2013
Received in revised form
4 June 2013
Accepted 18 June 2013
Available online 6 July 2013

Keywords:
Image encryption
Public key
Phase-shifting interferometry

ABSTRACT

We propose an asymmetric cryptosystem based on two-step phase-shifting interferometry (PSI) and elliptic curve (EC) public-key cryptographic algorithm, in which one image is encrypted to two interferograms by double random-phase encoding (DRPE) in Fresnel domain and two-step PSI, and the session keys such as geometrical parameters and pseudo-random seeds, are asymmetrically encoded and decoded with the aid of EC algorithm. The receiver, who possesses the corresponding private key generated by EC algorithm, can successfully decipher the transmitted data using the extracted session keys. The utilization of EC asymmetric cryptosystem solves the problem of key management and dispatch, which is inevitable in the conventional optical symmetric cryptosystems. Not only computer simulation, but also software design and development are carried out to verify the feasibility of the proposed cryptosystem.

1. Introduction

Optical security technology has been extensively studied in recent years because of its nature of parallel processing and high-freedom encoding since Réfrégier and Javidi proposed the double random phase encoding (DRPE) technique [1], and it has been further extended from Fourier domain [1,2] to other domains [3–23]. However, most of the optical cryptographic algorithms or encryption techniques developed so far belong to the category of symmetric cryptosystem (or private-key cryptosystem), in which the encryption key and decryption key are generally identical or mutually conjugate. From the point of view of cryptography, a symmetric cryptosystem would suffer from security problems such as key management and dispatch under an environment of network security; therefore, to solve these problems, the asymmetric cryptosystem (or public-key cryptosystem) plays an important role in modern cryptography. Unlike a symmetric encryption algorithm, asymmetric cryptography utilizes a pair of keys: one published publicly (known as the public key) for encryption and the other (known as the private key) for decryption. Public-key schemes are typically used to transport or exchange keys for symmetric-key ciphers [24–27].

Recently, some pioneer research work has been proposed to explore asymmetric optical image cryptosystems [28–32]. Peng et al. proposed an asymmetric cryptography based on wavefront sensing [28], in which the public key was derived from optical and geometrical parameters, while the private key was obtained from a kind of regular point array [28]. Subsequently, Peng and Qin presented an alternative asymmetric cryptosystem based on phase-truncated Fourier transform and DRPE in an optical 4*f* system [29]. To expand the DRPE scheme to usage in the framework of the public-key infrastructure, Lin et al. proposed an asymmetric algorithm based on data embedding to encode and decode the session key [30]. Zhou et al. [31] and we [32] reported two kinds of asymmetric cryptosystems separately on the basis of Rivest–Shamir–Adelman (RSA) public-key cryptography, the security of which is based on the fact that the factorization of integers into their prime factors would be very difficult. However, recent cryptanalytic advances have caused increased discussion about public key sizes and the security required. Elliptic curve cryptography (ECC) introduced by Miller [33] and Koblitz [34] is gaining favor as an efficient and attractive alternative to established public-key systems such as RSA, and the main attraction of ECC over RSA is that significantly smaller parameters can be used in ECC than RSA, but with equivalent levels of security [24–27].

[*] Corresponding author. Tel.: +86 531 88362857; fax: +86 531 88364613.
E-mail address: xfmeng@sdu.edu.cn (X. Meng).

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.06.044

Therefore, to increase security and bring more convenience for key management and dispatch than RSA, in this paper, we propose an asymmetric cryptosystem based on two-step PSI and elliptic curve (EC) public-key cryptographic algorithm, in which, an image is encrypted to two interferograms, using DRPE and two-step PSI with session keys enciphered by EC algorithm. The receiver who possesses the corresponding private keys can successfully decipher the transmitted data by the extracted session keys. Furthermore, we design a kind of asymmetric cryptosystem software by mixed programming between Visual C++ and Matlab based on the Matcom software environments. In the following sections, we will first describe the basis idea of ECC and the procedure of this method, then present its simulation verification and software implementation, and finally give the conclusions.

2. Elliptic curve cryptography (ECC)

To design public-key cryptographic systems, the EC cryptosystem proposed by Koblitz [34] and Miller [33] independently is now gaining a lot attention in industry and academia as an alternative to established RSA public-key cryptosystem. The primary advantage of ECC over RSA and other competing technologies is that the fastest known algorithm (known as the Pollard rho method) for solving the underlying hard mathematical problem in ECC takes fully exponential time, in contrast to the subexponential-time algorithms known for the integer factorization problem (the underlying mathematical problem in RSA) [26]. This means that a desired security level can be attained with significantly smaller keys in ECC than is possible with RSA. It is generally accepted, given current algorithmic knowledge, that the strength of an EC system based on 160-bit keys is roughly equivalent to that of a 1024-bit RSA system [25]. The result is smaller key sizes, bandwidth savings, and faster implementations, features which are especially attractive for security applications. An overview of ECC is given below [35,36].

The equation of a non-singular EC $E_p(a, b)$ over a finite field Z_p ($p > 3$ and is a large prime number) takes the form

$$y^2 \equiv x^3 + ax + b(\text{mod} p), \tag{1}$$

where the operator 'mod' denotes the modular operation, a and b are two constant such that $4a^3+27b^2 \not\equiv 0(\text{mod}\, p)$ must be satisfied for its non-singularity. Any point $P(x_p, y_p) \in E_p(a, b)$, $x, y \in Z_p$ together with O, called 'point at infinity' forms an abelian group $E = \{(x, y) \in E_p(a, b) \cup \{O\}\}$ under the EC addition operation, where O serves as additive identity element of the group. Given Q, $P \in E$, finding k such that $Q = kP$ is referred to as the EC discrete logarithm problem (ECDLP), whose hardness is essential for the security of all EC cryptographic schemes.

The implementation of the ECC is briefly summarized as follows.

- Elliptic curve key generation:
  – select a large prime number p and the EC cryptosystem $E_p(a, b)$.
  – Select a base point G on the EC cryptosystem $E_p(a, b)$, having a prime number n as the order (the smallest positive integer n such that $nG = O$).
  – Choose a random or pseudo-random integer d from the interval $[1, n-1]$ as the private key, and the corresponding public key is $Q = dG$.
  – Publicize the system parameter ($E_p(a, b)$, G, n) and public key Q.
- Encryption: the ciphertext of an arbitrary plaintext $m = (m_1, m_2)$ takes the form $c = \{C_0, (c_1, c_2)\}$, where $C_0 = kG$, $(t_1, t_2) = kQ$ (k is a randomly selected integer from the interval $[1, n-1]$), $c_1 = t_1 m_1 \bmod p$, $c_2 = t_2 m_2 \bmod p$.
- Decryption: the recipient who possesses the corresponding private key d can decrypt the ciphertext $c = \{C_0, (c_1, c_2)\}$ by computing $m = (c_1 t_1^{-1} \bmod p,\ c_2 t_2^{-1} \bmod p)$, where $(t_1, t_2) = dC_0$, t^{-1} and t are multiplicative inverses mod p, which satisfy $t^{-1} t \equiv 1 \bmod p$.

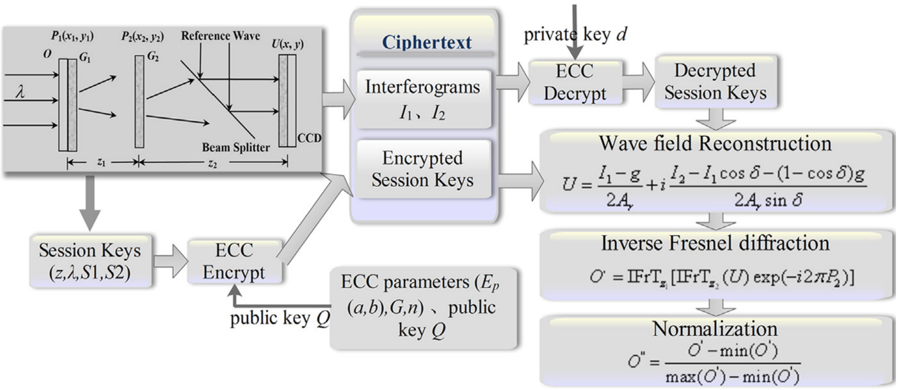
3. Procedure of the proposed asymmetric cryptosystem

Fig. 1 schematically depicts the proposed asymmetric cryptosystem, the working principle of which is described in detail in the following sub-sections.

3.1. Optical encryption based on DRPE and two-step PSI

Assume that Alice utilizes two seeds $S1$ and $S2$ to generate two RPMs G_1 and G_2 to encrypt an image in the Fresnel domain. G_1 and G_2 are placed in the object plane (x_1, y_1) and the transform plane (x_2, y_2), respectively. The complex amplitude transmittances of the two RPMs G_1 and G_2 may be denoted as $\exp[i2\pi P_1(x_1, y_1)]$ and $\exp[i2\pi P_2(x_2, y_2)]$, respectively, where P_1 and P_2 are two independent white noises uniformly distributed in the interval [0, 1]. The distance between the object and the transform plane is z_1 and that between the transform plane and the recording plane (x, y) is z_2. When an image O in the object plane is illuminated by an on-axis plane wave of wavelength λ, the complex wave in the recording plane (x, y) can be mathematically represented by [16,32]

$$U(x, y) = \text{FrT}_{z_2}\{\text{FrT}_{z_1}\{O(x_1, y_1) \exp[i2\pi P_1(x_1, y_1)]\} \exp[i2\pi P_2(x_2, y_2)]\}, \tag{2}$$



$P_1(x_1, y_1)$
$P_2(x_2, y_2)$
Reference Wave
$U(x, y)$
O
G_1
G_2
λ
CCD
Beam Splitter
z_1
z_2
Ciphertext
Interferograms I_1、I_2
Encrypted Session Keys
private key d
ECC Decrypt
Decrypted Session Keys
Wave field Reconstruction
$U = \frac{I_1 - g}{2A_r} + i\frac{I_2 - I_1\cos\delta - (1-\cos\delta)g}{2A_r \sin\delta}$
Inverse Fresnel diffraction
$O' = \text{IFrT}_{z_1}[\text{IFrT}_{z_2}(U)\exp(-i2\pi P_2)]$
Normalization
$O'' = \frac{O' - \min(O')}{\max(O') - \min(O')}$
Session Keys $(z, \lambda, S1, S2)$
ECC Encrypt
public key Q
ECC parameters ($E_p(a,b), G, n$)、public key Q

Fig. 1. Schematic diagram of the proposed asymmetric cryptosystem.