Optics and Lasers in Engineering 86 (2016) 303–308

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

# Generation of plaintext-independent private key based on conditional decomposition strategy

Chao Lin [a,*], Xueju Shen [a], Ming Lei [b]

[a] Department of Opto-electronic Engineering, Shijiazhuang Mechanical Engineering College, Shijiazhuang 050003, PR China
[b] China Defense Science & Technology Information Center, Peking 100138, PR China

ARTICLE INFO

*Article history:*
Received 14 January 2016
Received in revised form
26 June 2016
Accepted 27 June 2016
Available online 9 July 2016

*Keywords:*
Optical asymmetric cryptography
Private key
Conditional decomposition
Spiral phase key

ABSTRACT

We propose to generate the plaintext-independent private keys in optical asymmetric cryptosystem (OACS) based on the strategy of conditional decomposition (CD). Following this strategy, an OACS is designed with the principle of superposition of two vectorial beams. The proposed cryptosystem can remove the silhouette which is discovered in the two beams interference-based cryptosystem. To relieve the difficulty of key distribution, a structured spiral phase key (SSPK) is utilized instead of the random phase key (RPK). And a comparison on the performance of two kinds of keys in both the encryption and decryption process is made to show the advantage of SSPK over RPK.



## 1. Introduction

As a promising alternative or complement to digital signal processing methods, optical information processing has shown great superiority in pattern recognition, image processing and security applications [1–3]. Thanks to the high speed parallel processing capability and multiple degree of freedom in encoding, optical security technique has attracted increasingly interests [4,5]. Basically, optical cryptosystem based on Fourier optics is linear and symmetric such as the double random phase encoding (DRPE) technique [6]. However, the linear cryptosystem is not only vulnerable to attacks but also difficult in the implementation of key distribution which is one of the main concerns in cryptography. Under this circumstance, nonlinear optical cryptosystem and asymmetric optical cryptography, which are dedicated to reinforce the security and relieve the key distribution difficulty is suggested [7,8].

Originated from the most relevant optical asymmetric cryptosystem (OACS), i.e., the phase-truncated Fourier transform (PT-FT) based OACS [9], many derivative OACS have been proposed. The main challenge is to find out effective trapdoor one-way function to meet the design rule of asymmetric cryptography. A lot of optical trapdoor one-way functions have been proposed based on such as, wavefront sensing [10], phase-truncated Fourier transform [11], phase retrieval algorithm [12,13], truncation on elliptical polarized light [14] and coherent superposition [15]. And these methods have enriched the methodology of OACS. From a wider perspective, OACS has been extended from the Fourier transform domain to the fractional Fourier transform domain to achieve multiple-image encryption [16], further more, it is extended to gyrator wavelet transform domain to perform double image encryption [17], and single-channel color image encryption [18]. What's addition, the Rivest–Shamir–Adelman (RSA) public-key algorithm and elliptic curve (EC) algorithm have also been introduced into OACS [19,20]. However, both the RSA and EC algorithms which are directly borrowed from traditional cryptography will downgrade the global speed of cryptosystem. And, the PT-FT based OACS has been proved to be vulnerable to know public key attack [21] and known plaintext attack in different transform domains [22]. Since the attack-free OACS has been suggested [23], the security level of PT-FT based OACS has been significantly enhanced. More importantly, the private key generated in the encryption process of current OACS is related to the plaintext [24]. Typically, this one-time-pad cryptography has higher robustness against attacks [25], however, it will violate the exact design rule of ACS. Even though that the OACS is not obligated to follow the exact terminology and algorithm of ACS [26], optical trapdoor one-way functions should be further investigated and optimized to enhance the security and practicability of OACS.

In fact, it is difficult to optically implement the trapdoor one-way function, because this function is always related to a mathematical puzzled problem. However, in the framework of OACS, we still expect that the private key generated in OACS is independent

* Corresponding author.
*E-mail address:* vestigelinchao@163.com (C. Lin).

http://dx.doi.org/10.1016/j.optlaseng.2016.06.023
0143-8166/

of the plaintext in order to lower the risk of interception of keys in the secure transmission of key. Hence, the current OACS can be classified into more the category of nonlinear optical cryptosystem than that of the ACS in a strict sense. Typically, previous OACS generates the private keys by separating the optical field distribution on a certain diffractive plane in a certain step of the encryption procedure into two parts. For example, the generation of private keys in PT-FT based OACS is realized with the multiplicative decomposition of phasor into amplitude part and phase part. However, if we look depth into these OACS, it is not difficult to notice that these decomposition algorithms are deterministic, that is, the private key is directly calculated and related to the undecomposed optical field distribution. In this case, private key is related to the plaintext because the undecomposed optical field is always the function of the plaintext and keys.

In the practical delivery of keys, two vital factors will affect the risk of interception. One is the size of key and the other is the times of key distribution. The larger the above two factors' quantity, the more danger of keys being hacked. Because the key is commonly a random phase mask and its data size is large, in order to cover up the presence of key during transmission, optical asymmetric watermarking technique using modified wavelet fusion and diffractive imaging is proposed [27]. Except for the watermarking method, the risk of interception of keys can also be reduced by compressing the data size of key utilizing, for example, the structured phase mask. In our work, to secure the key distribution process, a combination of improvement is used. First, we propose to replace the RPK with a novel SSPK to minimize the key size. Second, we propose to generate the private keys using the conditional decomposition (CD) strategy. In this strategy, a predefined and fixed private key is generated in advance, then, the other private keys are calculated with specific decomposition algorithm using the pre-defined private key. As a result, other than the deterministic decomposition (DD), at least one plaintext-independent private key can be obtained. Finally, the risk of interception of keys is thereby reduced. Following both the CD and DD strategy, an OACS based on both a two-step decomposition algorithm and the superposition of two vectorial beams is designed.

## 2. Principle

### 2.1. Principle of the conditional decomposition strategy

We first present a general description on the CD and DD strategy. Let $f$ and $k_{pub}$ denote the plaintext and public key, respectively. The encryption process of OACS can be separated into two steps. The first step involves the generation of an intermediate variable denoted as $e_{in}$. We can formulate the first step with Eq. (1),

$$e_{in} = E_1(f, k_{pub}). \tag{1}$$

In which $E_1$ is the encoding algorithm in the first step. Then, the second step includes the generation of both cyphertext and private keys applying Eq. (2) and Eq. (3), respectively

$$c = E_2(e_{in}), \tag{2}$$

$$k_{pri} = E_3(e_{in}). \tag{3}$$

In which $E_2$ and $E_3$ denote the decomposition algorithms for the calculation of cyphertext and private keys. The form of decomposition algorithms can be diverse. However, it is obvious in Eq. (3) that the algorithm is deterministic. Therefore, private key is directly related to plaintext and public key. The above mentioned algorithm is the commonly used DD strategy. In the CD strategy,

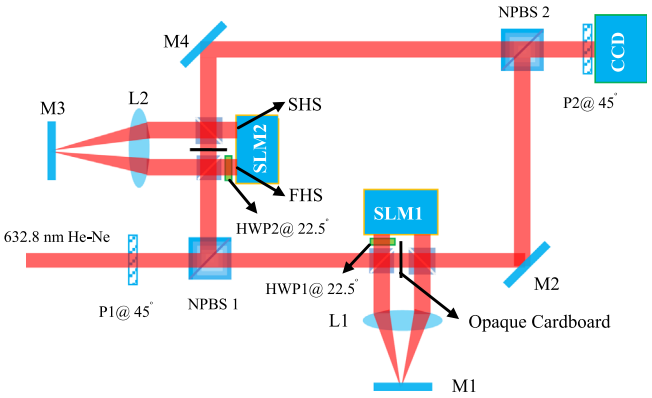


**Fig. 1.** Optical decryption setup. P stands for polarizer, NPBS stands for non-polarizing beam splitter, HWP stands for half-wave plate, FHS and SHS stands for the first or second half screen of the SLM, M stands for mirror, and L stands for lens.

the generation of private keys is controlled by an additional predefined parameter $k$, as denoted with Eq. (4),

$$K_{pri} = E_3(e_{in}, k). \tag{4}$$

This pre-defined parameter $k$ is shared by the sender and receiver in advance, and it is independent of the plaintext. So, this decomposition algorithm is deterministic only when $k$ is given. That is to say, this algorithm is "conditional". Based on the CD strategy, mathematically, a novel OACS can be designed. However, it is not so easy to optically implement the CD. In this paper, we design an OACS based on the principle of superposition of two vectorial beams to implement the CD strategy.

### 2.2. Generation of the structured spiral phase key

Before elaborating the OACS, we introduce the SSPK to replace the RPK. The proposed SSPK can be obtained by assembling several distorted and twisted spiral phase plate (SPP) as basic cells. A cell of the SSPK is constructed by imposing structured phase offsets with phase distribution $\phi(r, \theta) = p \times \theta + \phi_0$ on the SPP. In this phase offset, $r$ and $\theta$ are the radial and azimuthal coordinates, $p$ is the vortex topological charge with an integer or fractional value. And $\phi_0$ is a constant and space-invariant phase term. However, in our case, this phase term $\phi_0$ are set to be spatially variant by superimposing linear, quadric even higher order phase distribution on it. First, a linear phase shift $\phi_0 = m \times r\cos(\theta) + n \times r\sin(\theta)$ is imposed, in which $m$ and $n$ denote the slopes of linear phases in horizontal and vertical directions. Second, a quadratic phase shift is further added, that is, $\phi_0 = q \times r^2$, in which $q$ denotes the strength of quadratic phase. The value for $m$, $n$ and $q$ can be an arbitrary constant integer or fraction. When both the two terms are applied on the SPP, the resultant phase distribution shows a distorted and twisted pattern of spiral phase. We can conclude the phase distribution of the designed cell in SSPK as [28],

$$\phi_i(r, \theta) = p_i \times \theta + m_i \times r\cos(\theta) + n_i \times r\sin(\theta) + q_i r^2 + c_i. \tag{5}$$

In Eq. (5), $c_i$ is a constant value selected from $[0, 2\pi]$ which sets an initial constant phase, the subscript $i$ denotes the $i$th cell within SSPK. It is also worth noting that the range of $\phi_i$ should be within $(0 \sim 2\pi)$ by taking the modulus after the division of $\phi_i$ by $2\pi$. The resultant SSPK is extracted by splicing a quantity of basic cells with different structure parameters into a whole key mask without mutual overlap.

### 2.3. Principle of the proposed optical asymmetric cryptosystem

We then design an OACS following the CD strategy. As indicated by Eq. (1)–(4), DD and CD algorithms for the generation of