

# On the security of a class of diffusion mechanisms for image encryption

Leo Yu Zhang<sup>a,\*</sup>, Yuansheng Liu<sup>b</sup>, Kwok-Wo Wong<sup>a</sup>, Fabio Pareschi<sup>c</sup>, Yushu Zhang<sup>d</sup>, Riccardo Rovatti<sup>e</sup>, Gianluca Setti<sup>c</sup>

<sup>a</sup>Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China

<sup>b</sup>School of Software, Dalian University of Technology, Dalian, China

<sup>c</sup>Engineering Department in Ferrara, University of Ferrara, Italy

<sup>d</sup>School of Electronics and Information Engineering, Southwest University, Chongqing, China

<sup>e</sup>Department of Electrical, Electronic and Information Engineering, University of Bologna, Italy

---

## Abstract

The need for fast and strong image cryptosystems motivates researchers to develop new techniques to apply traditional cryptographic primitives in order to exploit the intrinsic features of digital images. One of the most popular and mature technique is the use of complex dynamic phenomena, including chaotic orbits and quantum walks, to generate the required key stream. In this paper, under the assumption of plaintext attacks we investigate the security of a classic diffusion mechanism (and of its variants) used as the core cryptographic primitive in some image cryptosystems based on the aforementioned complex dynamic phenomena. We have theoretically found that regardless of the key schedule process, the data complexity for recovering each element of the equivalent secret key from these diffusion mechanisms is only  $O(1)$ . The proposed analysis is validated by means of numerical examples. Some additional cryptographic applications of our work are also discussed.

**Keywords:** Image encryption, Cryptanalysis, Diffusion, Plaintext attack, Permutation

---

## 1. Introduction

The recent years increase in the popularity of the internet and multimedia communication has resulted in the fast development of information exchange and consumer electronics applications. However, it has also led to an increase in the demand of secure and real-time transmission of these data. The easiest way to cope with this is to consider the multimedia stream as a standard bit stream and apply traditional cryptographic approaches like 3DES [1] and AES [2] with proper mode of operation. Yet, the desire for cryptosystems more efficient and specifically designed for multimedia stream has drawn increasing research attention in the past decade [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. A particular field of interest in this area is the development of strong and fast image cryptosystems.

Two major approaches can be identified in the literature for the design of image encryption algorithms. The first one exploits some complex dynamic phenomena, such as chaotic behavior and quantum walks, as the image encryption algorithm core. Many schemes belonging to this approach are based on the permutation-diffusion architecture depicted in Fig. 1, which was first proposed by Fridrich in [10]. The encryption process is based on the iteration of permutation (i.e., image element transposition) and diffusion (i.e., value modification) operations. Almost all works proposing an extension of Fridrich's work can be categorized into the following two classes:

1. Developing novel permutation techniques. In Fridrich's original design, permutation is implemented by iterating a 2D discretized chaotic map like Baker or Cat map. Chen *et al.* suggested using 3D chaotic map to de-correlate the relationship among pixels in a more efficient way [11, 12]. In [19], Wong *et al.* proposed an "add-and-then-shift" strategy to include certain amount of diffusion effect into permutation, thus reducing the overall number of iteration rounds, and improving the efficiency. For the same purpose, Zhu *et al.* suggested

---

\*Corresponding author.

Email address: leocityu@gmail.com (Leo Yu Zhang)

carrying out permutation to bit-level instead of pixel-level [18, 17]. It is also worth mentioning that there are permutation techniques based on general Gray code [20, 21], which can be considered as permutation carried out at an arbitrary bit length.

2. Developing novel diffusion techniques. As illustrated by Fridrich in [10], the diffusion operation aims to spread the information of plaintext to the whole ciphertext. This process can be formulated as

$$c(l) = p(l) \dot{+} G(c(l-1), k(l)),$$

where  $\dot{+}$  denotes the modulo addition,  $p(l)$ ,  $c(l)$  and  $k(l)$  denote the  $l$ -th plaintext element, ciphertext element and element derived from the secret key, respectively. For security and efficiency considerations, the function  $G$  should be both simple and nonlinear, a typical example is a chaos-based look-up table [22]. By taking advantage of the low complexity and non-commutable properties between the bitwise exclusive or and the modulo addition operation, which are popular in traditional cryptosystems like IDEA and RC6, Chen *et al.* in [11] suggested implementing diffusion according to the following formula

$$c(l) = (p(l) \dot{+} k(l)) \oplus k(l) \oplus c(l-1),$$

where  $\oplus$  stands for bitwise exclusive or. Many other works adopt similar (or even the same) diffusion mechanisms, see [23, 24, 17, 16, 25, 14, 15, 26, 27, 28] for examples. It is not surprising that the computational efficient modulo multiplication can also be incorporated into the diffusion stage [23, 29]. Moreover, recent works suggested using real number arithmetic to enhance the security level of the diffusion stage [15, 16] at the cost of a reduced computational efficiency due to the employment of complicated arithmetic operations.

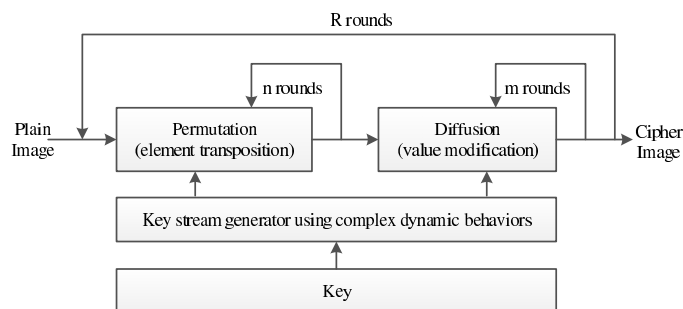


Figure 1: Schematic diagram of Fridrich's permutation-diffusion architecture.

The second major approach in the design of image cryptosystem is based on optical technology schemes, which are supposed to benefit from the intrinsic property of optic systems to process high dimensional complex data in parallel. The most classic image cryptosystem based on optical technology is the double random phase encoding (DRPE) method developed by Réfrégier and Javidi in [30]. A comprehensive review on this topic can be found in [31]. Though the DRPE technique has several advantages, like high speed, multidimensional processing and robustness, the underlying arithmetic operation, which is matrix multiplication, is linear. From the cryptanalysis point of view, linearity leads to a low security level. Thus the DRPE method is vulnerable under various kinds of attack [32, 33, 34] and the adoption of image cryptosystem based on optical technology for real application should be cautious.

In this paper we take into account the first approach only, i.e., that exploiting complex dynamic phenomena. In particular, we investigate on some security-related aspects of these systems. Note that in any image cryptosystem, security is a critical issue. In fact, due to the particular structure of digital image files (such as, for example, horizontal/vertical correlation) many statistical analysis based methods may reduce the security. Typical statistical tests include histogram analysis, correlation analysis, entropy analysis [35], sensitivity analysis [11] and randomness analysis [36].

In recent years, a lot of image ciphers employing complex dynamic phenomena and fulfilling all the aforementioned statistical tests requirements, have been proposed but afterwards found to be insecure under various attack

models [37, 38, 39, 40, 41, 29, 42]. For example, the equivalent key stream used for permutation of Fridrich’s design can be retrieved in chosen-plaintext (CP) attack scenario [42] and a chaos-based image cipher with Feistel structure is insecure with respect to differential attack when the round number is smaller than 5 [43]. Note that in the literature, the cryptanalysis of these image ciphers is usually performed case-by-case, since any cryptanalytic method is usually effective only on a particular image cipher. Conversely, despite being more useful from a theoretical point of view, only a few works provide security evaluation of some general cryptographic components. In [44], Li *et al.* presented a general quantitative study of permutation-only encryption algorithms against plaintext attacks. Their result was further improved in [45] with respect to data and computation complexity. In [46, 47, 48], Chen *et al.* studied the period distribution of the generalized discrete Cat map, which is a fundamental building block in many permutation schemes.

In this paper we want to make a step further in the evaluation of generic cryptographic components for image cryptosystem by studying the security of the differential equation of modulo addition (DEA) in the form  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$ . This analysis is not completely new. In [38], it was reported that 3 pairs of chosen queries  $(\alpha, \beta)$  are sufficient to reveal the unknown  $k$  of the formula  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$ . It is further reduced to 2 pairs of chosen  $(\alpha, \beta)$  in [39]. As far as we know, these works must be considered as independent analyses of particular image ciphers [26, 25]. In our previous work [41], it was reported that the diffusion mechanism suggested by Chen *et al.* [11] can be cast to the form  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  under CP attack and the similar method can be also used to analyze other DEA that includes modulo multiplication operation.

In more detail, we take into account the three image cryptosystems proposed in [14], in [15] and in [16] as case studies, all of them adopting Fridrich’s permutation-diffusion scheme, and we study the resistance against plaintext attack of the adopted diffusion mechanisms by exploiting security results achieved by the aforementioned DEA equation analysis. Specifically, we evaluate the data complexity (i.e., required number of pairs of  $(\alpha, \beta)$ ) for solving  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  and its extension in a known-plaintext (KP) attack scenario. The main difference between this work and previous ones is that we assume that  $\alpha$  and  $\beta$  cannot be freely chosen, as for example in [38, 39]. This allows us to apply obtained results to the security analysis of the three aforementioned cryptosystem schemes. A full analytic result is presented to derive a sufficient condition for solving the equation  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$ ; furthermore, some design weakness of its variants are pointed out. Numerical simulation results are then provided to support our analyses.

The innovative contribution of this paper is three-fold. First, we analyze the relationship between a class of popular diffusion mechanisms and the DEA  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  by studying three example image ciphers [14, 15, 16]. It is also worth mentioning that the similar DEA can be found in many other designs [23, 24, 17, 16, 25, 14, 15, 26, 27, 28] so the application of our analyses is not limited to the three case studies. Second, we analytically investigate the sufficient condition to solve  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  and we also experimentally present a simple KP attack to a variant of this DEA. The conclusion drawn from our result is that security is substantially lower than the desired one. Third, we study the three encryption schemes [14, 15, 16] which combines the investigated diffusion mechanism and secret random permutation. Their security is evaluated in detail.

The rest of this paper is organized as follows. Section 2 introduces the notations that is used in this paper and the assumptions we work on. The three image cryptosystem case studies are reviewed in Sec. 3 and the differential equations of modulo addition are derived in Sec. 4. Section 5 presents security analyses and numerical results of the equations derived above against KP attack. The applications of our results are discussed in Sec. 6 and conclusion remarks are drawn in the last section.

## 2. Notations and main assumptions

In the following, we will use the notation  $\{p(i, j)\}_{i=1, j=1}^{H, W}$  and  $\{p(k)\}_{k=1}^L$  to represent the 2D and 1D format of a plain-image of size  $L = H \times W$  (Height  $\times$  Width). The 2D and 1D representations of the cipher-image  $C$  are  $\{c(i, j)\}_{i=1, j=1}^{H, W}$  and  $\{c(k)\}_{k=1}^L$ , respectively. We use  $a_i$  to denote the  $i$ -th bit of an  $n$ -bit integer  $a$  ( $a \in \mathbb{Z}_2^n$ ) and  $(a_{n-1} \cdots a_0)_2$  to denote the binary form of  $a$ . The default value of  $n$  is 8 unless otherwise specified. The symbols ‘ $\dot{+}$ ’, ‘ $\dot{-}$ ’, ‘ $\oplus$ ’, ‘ $\wedge$ ’ and ‘ $\parallel$ ’ denote *modulo  $2^n$  addition*, *modulo  $2^n$  subtraction*, *bitwise exclusive or (XOR)*, *bitwise and* and *bitwise or*, respectively. We will use  $ab$  to represent  $a \wedge b$  and  $\lfloor x \rfloor$  ( $\lceil x \rceil$ ) to represent the largest (smallest) integer not greater (less) than the real number  $x$ . The cardinality of a set  $A$  is denoted by  $\#A$ . With the term *KS* we will refer to all the key schedule

operations of a specific algorithm, and use  $KS(Seed)$  to indicate the process generating all necessary key streams given a secret  $Seed$  by the  $KS$ .

In order to correctly evaluate the security level of a diffusion mechanism either in known- or chosen-plaintext attack scenario, we clarify here the power of the adversary. In the KP attack model, the adversary has access to some plaintexts and their corresponding ciphertexts. In the CP attack model, we assume that the adversary can obtain ciphertexts from any plaintext of his choice. In both scenarios, the goal of the attack is either to collect information on the secret key  $Seed$  or, equivalently, on the key stream(s)  $KS(Seed)$  generated from  $Seed$ . Hereinafter, we will consider only the problem of recovering  $KS(Seed)$ .

### 3. Image cryptosystems review

In this section, we briefly review the three cryptosystems for image encryption proposed in [14], in [15], and in [16]. A detailed description of the three schemes can be found in the original works<sup>1</sup>. Here, we want to highlight that, though the key schedule process of these schemes are different from the each other, all of the schemes share a very similar diffusion mechanism in the encryption process. In the next section, we will exploit this to cast the three diffusion mechanisms into the same general form and evaluate their cryptographic strength.

**A. Parvin's cryptosystem.** The key schedule operation of the cipher proposed in [14] is based on two chaotic functions and the encryption process is composed by a row/column circular permutation and a sequential pixel diffusion.

1 *Initialization:* Generate three key streams  $U = \{u(i)\}_{i=1}^H$ ,  $V = \{v(i)\}_{i=1}^W$  and  $K = \{k(i)\}_{i=0}^L$  from  $KS(Seed)$ , where  $U$ ,  $V$  and  $K$  are composed of random integers in interval  $[1, W]$ ,  $[1, H]$  and  $[0, 255]$ , respectively.

2 *Permutations:* Carry out row circular permutation to the plain-image  $P$  using

$$p'(i, (j + u(i)) \bmod W) = p(i, j), \quad (1)$$

and denote the result by  $P'$ . Then permute  $P'$  further using the circular column permutation as follows

$$s((i + v(j)) \bmod H, j) = p'(i, j). \quad (2)$$

3 *Diffusion:* Stretch  $S$  to a 1D sequence  $\{s(l)\}_{l=1}^L$  and calculate the pixel values of the cipher-image by the following diffusion equation

$$c(l) = s(l) \oplus (c(l-1) \dot{+} k(l)) \oplus k(l), \quad (3)$$

where  $l \in [1, 2, \dots, L]$  and  $c(0) = k(0)$ . Rearrange  $\{c(l)\}_{l=1}^L$  to a matrix of size  $H \times W$  to get the cipher-image  $C$ .

**B. Norouzi's cryptosystem.** The key schedule suggested in [15] is based on the hyper-chaotic system introduced in [49]. The encryption process is composed by a single diffusion process, which can be viewed as the generalized version of the previous diffusion scheme.

1 *Initialization:* Produce a key stream  $K = \{k(i)\}_{i=0}^L$  by running  $KS(Seed)$ , where  $k(i)$  is 8-bit integer in  $[0, 255]$ .

2 *Diffusion:* Calculate the pixel values of the cipher-image sequentially by the following bidirectional diffusion equation

$$c(l) = p(l) \oplus (c(l-1) \dot{+} k(l)) \oplus f(P, k(l)), \quad (4)$$

where  $l \in [1, 2, \dots, L]$ ,  $c(0) = k(0)$  and

$$f(P, k(l)) = \lfloor \left( \sum_{i=l+1}^L p(i) \right) \cdot k(l) \cdot 10^8 / 256^4 \rfloor \bmod 256. \quad (5)$$

Rearrange  $\{c(l)\}_{l=1}^L$  to a matrix of size  $H \times W$  and denote it as  $C$ .

---

<sup>1</sup>For the sake of both clarity and uniformity, some notations and/or some operations may have been changed without affecting the security level of the schemes.

C. **Yang's cryptosystem.** The key schedule of the image cryptosystem proposed in [16] is derived from the one-dimensional two-particle discrete-time quantum random walks, which is totally different from those suggested in [14, 15]. However, the encryption process, which is composed of a diffusion stage and a permutation stage, is an extension of Norouzi's work [15].

- 1 *Initialization:* Obtain the key streams  $K = \{k(i)\}_{i=0}^L$ ,  $U = \{u(i)\}_{i=1}^W$  and  $V = \{v(i)\}_{i=1}^H$  by running the key schedule  $KS(Seed)$ , where  $K$  is composed of 8-bit integers in the interval  $[0, 255]$  and  $U$  and  $V$  are permutation of the set  $\{1, 2, \dots, W\}$  and  $\{1, 2, \dots, H\}$ , respectively.
- 2 *Diffusion:* Run the bidirectional diffusion technique characterized by Eq. (4) to the plain-image pixels as follows

$$p'(l) = p(l) \oplus (p'(l-1) \dot{+} k(l)) \oplus f(P, k(l)), \quad (6)$$

where  $l \in [1, 2, \dots, L]$ ,  $p'(0) = k(0)$  and  $f(P, k(l))$  is defined by Eq. (5). Rearrange  $\{p'(l)\}_{l=1}^L$  to a matrix of size  $H \times W$  and denote it as  $P'$ .

- 3 *Permutations:* Permute the intermediate result  $P'$  using the key streams  $U$  and  $V$  and get the cipher-image  $C$ , i.e.,

$$s(i, u(j)) = p'(i, j), \quad (7)$$

$$c(v(i), j) = s(i, j), \quad (8)$$

where  $i \in [1, H]$  and  $j \in [1, W]$ .

#### 4. Problem formulation

The cryptosystems shown in the previous section are based either on a single round permutation-diffusion architecture (Parvin's and Yang's cipher) or on a bidirectional diffusion stage (Norouzi's cipher). In this paper, we focus our attention on the security of the considered diffusion schemes in a plaintext attack. To this aim, we will neglect at this moment all the effects of the permutation schemes in [14, 15, 16], that will be considered in Sec. 6 only, along with the security of the whole cryptosystems. Mathematically, we assume that all elements of the key streams  $U$  and  $V$  used for permutation in Parvin's cryptosystem are zeros, and that  $U$  and  $V$  in Yang's cryptosystem are both given by the identity permutation. Note that a similar approach, with a general quantitative plaintext attack on permutation-only ciphers can be found in [44].

In the diffusion mechanism proposed by Parvin we will show that the problem of finding the key stream  $K$  used in the diffusion scheme with a KP attack is equivalent to solve the DEA  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$ , where  $\alpha, \beta, y$  are known parameters and  $k$  is unknown. Note that the same DEA, under the assumption that  $\alpha$  and  $\beta$  can be freely chosen, have already been analyzed by other works, that are also briefly reviewed. We will also show that also the problem of retrieving the key stream for diffusion in Norouzi and Yang's design under CP attack scenario is equivalent to solve this DEA. In addition, we will also investigate the security level of the diffusion approach proposed by Norouzi and Yang with respect to a KP attack.

##### 4.1. Parvin's diffusion scheme

In Parvin's scheme, we assume that two plain-images,  $P_1$  and  $P_2$ , and their corresponding cipher-images,  $C_1$  and  $C_2$ , are available. Referring to Eq. (3), we have

$$\begin{cases} c_1(l) = p_1(l) \oplus (c_1(l-1) \dot{+} k(l)) \oplus k(l) \\ c_2(l) = p_2(l) \oplus (c_2(l-1) \dot{+} k(l)) \oplus k(l), \end{cases}$$

where  $l \in [1, L]$ . Their difference can be calculated as

$$(c_1(l-1) \dot{+} k(l)) \oplus (c_2(l-1) \dot{+} k(l)) = c_1(l) \oplus c_2(l) \oplus p_1(l) \oplus p_2(l). \quad (9)$$

More generally, we can recast this expression by observing that for any value of  $l$  we have

$$(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y. \quad (10)$$

In the present context, the problem of finding the key stream  $\{k(l)\}_{l=1}^L$  of Parvin's cryptosystem is turned into solving Eq. (10) under some pairs of known parameters  $(\alpha, \beta, y)$ . Note that  $k(0)$ , and so the full stream  $K$ , can be easily calculated according to Eq. (3) after  $\{k(l)\}_{l=1}^L$  are revealed.

It is already known that, under the assumption that  $\alpha$  and  $\beta$  can be chosen freely,  $k$  can be determined by only two groups of chosen queries by referring to the following

**Theorem 1.** [39, Proposition 3 and Corollary 3.1] Suppose  $\alpha, \beta, k, y \in \mathbb{Z}_2^n$  and  $n > 2$ , two groups of chosen queries  $(\alpha, \beta)$  and their corresponding  $y$  are sufficient to determine  $k$  of the following equation

$$(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$$

in terms of modulo  $2^{n-1}$ . Specifically the two chosen queries can be  $(\hat{\alpha}, \hat{\beta}) = (\sum_{j=0}^{\lceil n/2 \rceil - 1} (00)_2 \cdot 4^j, \sum_{j=0}^{\lceil n/2 \rceil - 1} (10)_2 \cdot 4^j)$  and  $(\bar{\alpha}, \bar{\beta}) = (\sum_{j=0}^{\lceil n/2 \rceil - 1} (10)_2 \cdot 4^j, \sum_{j=0}^{\lceil n/2 \rceil - 1} (01)_2 \cdot 4^j)$ .

The proof of Theorem 1 can be found in [38, 39], and an interpretation from the computational point of view about this theorem can be found in [41]. It is worth mentioning that the most significant bit (MSB) of  $k$ , i.e.,  $k_{n-1}$ , cannot be determined even with additional queries of  $(\alpha, \beta)$ . This is intrinsic in the fact that the carry bit generated by the highest bit plane is discarded after the modulo operation [41]. Consequently, both  $k$  and  $\hat{k} = k \oplus 2^{n-1}$  are two equivalent solutions of the considered equation. For this reason, in the following we consider only the problem of determining the  $(n-1)$  least significant bits (LSBs) of  $k$  in Eq. (10).

Note however that, by referring to Eq. (9), neither a KP nor a CP attack scenario allows us to choose the value of  $\alpha$  and  $\beta$  since they represent ciphertext elements. In order get a result similar to that of Theorem 1 that can be applied to the considered cryptosystems, we systematically analyze Eq. (10) in Sec. 5.1 under the assumption that  $\alpha$  and  $\beta$  are known to the attacker but cannot be freely chosen.

#### 4.2. Norouzi and Yang's diffusion scheme

In Norouzi's and Yang's cryptosystems, the diffusion stage is characterized by Eq. (4), where some computational-intensive operations are added to the XOR and modulo addition. Regardless of their computational efficiency, we are curious whether this new diffusion mechanism will improve the security of the resultant cryptosystem. Given a plain-image  $P_1 = \{p_1(l)\}_{l=1}^L$ , we define the real number sequence  $T_1 = \{t_1(l)\}_{l=1}^L$  as

$$t_1(l) = \sum_{i=l+1}^L p_1(i) / 256^4. \quad (11)$$

Then, the diffusion scheme characterized by Eq. (4) can be written as

$$c_1(l) = p_1(l) \oplus (c_1(l-1) \dot{+} k(l)) \oplus g(t_1(l), k(l)), \quad (12)$$

where  $g(t_1(l), k(l)) = \lfloor t_1(l) \cdot (10^8 \cdot k(l)) \rfloor \bmod 256$ . Under a CP attack scenario, an adversary can choose another plain-image  $P_2$ , which differs from  $P_1$  by a single pixel at location  $l_0$ . In this way the real number sequence  $T_2 = \{t_2(l)\}_{l=1}^L$  associated to  $P_2$  satisfies

$$t_2(l) = t_1(l) \quad \text{if } l \geq l_0.$$

Referring to Eq. (12), it is easy to observe that the difference between  $C_1$  and  $C_2$  at location  $l_0$  will satisfy

$$\begin{aligned} c_1(l_0) \oplus c_2(l_0) \oplus p_1(l_0) \oplus p_2(l_0) &= (c_1(l_0-1) \dot{+} k(l_0)) \oplus g(t_1(l_0), k(l_0)) \\ &\quad \oplus (c_2(l_0-1) \dot{+} k(l_0)) \oplus g(t_2(l_0), k(l_0)) \\ &= (c_1(l_0-1) \dot{+} k(l_0)) \oplus (c_2(l_0-1) \dot{+} k(l_0)), \end{aligned}$$

which coincides exactly with Eq. (10). In conclusion, under the CP attack scenario, the problem of finding the equivalent secret key stream for diffusion of Norouzi and Yang's designs is converted into solving Eq. (10) with some pairs of known parameters  $(\alpha, \beta, y)$ .

Conversely, under the assumption of a KP attack scenario, we can observe from Eq. (11) that the calculation of the real number sequence  $T$  is independent of the secret key (stream). Then, limiting ourselves to consider the plain image  $P_1$ , we can recast Eq. (12) as

$$(\alpha \dot{+} k) \oplus g(\beta, k) = y, \quad (13)$$

where  $g(\beta, k) = \lfloor \beta \cdot (10^8 \cdot k) \rfloor \bmod 256$  is a nonlinear function. The problem of determining  $k$  for Eq. (13) from some groups of known  $(\alpha, \beta, y)$  is considered in Sec. 5.2. Here, special attention should be paid to the fact that  $\beta$  is no longer 8-bit integer but a non-negative real number.

## 5. Main results

### 5.1. Cryptographic strength of the equation $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$

According to Sec. 4.1, both KP and CP attacks to Parvins diffusion scheme are equivalent to solve Eq. (10) under the assumption that the value of  $\alpha$ ,  $\beta$  and  $y$  are known but none of them can be chosen. In the ideal case, the data complexity for to determine  $k$  should be  $2^{2n}$  because there are  $2^{2n}$  possible combinations of  $\alpha$  and  $\beta$  in total. However, we can theoretically show (and we will confirm this with simulation results) that the actual complexity substantially deviates from the ideal one.

Let us assume that an adversary successfully collects a set of known triples  $(\alpha, \beta, y)$  and denote this set by

$$\mathbb{G} = \{(\alpha, \beta, y) \mid y = (\alpha \dot{+} k) \oplus (\beta \dot{+} k)\}$$

with  $\#\mathbb{G} = g$ . The candidate solutions of  $k$  given  $\mathbb{G}$  can be computed by means of a brute-force search according to the following algorithm whose computational complexity is  $O(2^{n-1} \cdot g)$ .

- Step (1) Let  $l = 1$  and the solution set  $\mathbb{K}_l = \emptyset$ .
- Step (2) Select the  $l$ -th element of  $\mathbb{G}$  and exhaustively test all the  $2^{n-1}$  possible values of  $k$  (the MSB of  $k$  is ignored here) to check whether it satisfies Eq. (10). Collect all the possible values of  $k$  that meet the requirement and denote them as  $\mathbb{K}_l$ .
- Step (3) Set  $l = l + 1$  if  $l < g$ . Go to Step (2) and update the solution set by  $\mathbb{K}_{l+1} = \mathbb{K}_{l+1} \cap \mathbb{K}_l$ .

This algorithm ends up with a solution set  $\mathbb{K}_g$  which contains all the possible values of  $k$  that are consistent with the known parameter set  $\mathbb{G}$ . Nevertheless, it is concluded that the computational complexity is  $O(2^{n-1} \cdot g)$  steps. Nevertheless, this algorithm has two shortcomings: 1) there is no hint on how to choose the correct  $k$  from  $\mathbb{K}_g$  if  $\#\mathbb{K}_g \geq 2$ ; 2) the efficiency is not satisfactory when  $n$  is large. In the case of Parvin's cryptosystem,  $n$  is fixed to 8, and this makes this algorithm working pretty well. However, in the scheme proposed in [26, 25], where  $n = 32$ , this algorithm becomes inefficient. These two questions are solved on the basis of Theorem 2, where the sufficient condition to determine the bit plane of  $k$  is given.

**Theorem 2.** Suppose  $\alpha, \beta, k, y \in \mathbb{Z}_2^n$  and  $n \geq 2$ . Given  $\alpha, \beta$  and  $y$ , the  $i$  least significant bits ( $0 \leq i < n - 1$ ) of  $k$  of the following equation

$$(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$$

can be solely determined if  $y = \sum_{j=0}^{i-1} 2^j = \overbrace{(0 \dots 0 1 \dots 11)}^{MSB \leftarrow LSB}_i 2$ .

*Proof.* The proof of this theorem can be found in Appendix A. □

For a given known parameter triple  $(\alpha, \beta, y)$ , Theorem 2 states that some least significant bits of  $k$  can be confirmed when consecutive ones are observed at the LSBs of  $y$ . A more surprising inference drawn from Theorem 2 is that Eq. (10) can be solved using only a single query  $(\alpha, \beta)$  when the adversary obtains the oracle machine outputs  $(2^n - 1)$  or  $(2^{n-1} - 1)$ .

Furthermore, it is also easy to conclude that the result given by Theorem 1 is just a special case of that by Theorem 2. In detail, for the two chosen queries used in Theorem 1, we have

$$\begin{aligned} \hat{y} \parallel \bar{y} &= (\hat{\alpha} \dot{+} k) \oplus (\hat{\beta} \dot{+} k) \parallel (\bar{\alpha} \dot{+} k) \oplus (\bar{\beta} \dot{+} k) \\ &= 2^n - 1 \end{aligned}$$

and we can also indicate other two groups of queries satisfying the requirements of Theorem 1, specifically  $(\tilde{\alpha}, \tilde{\beta}) = (\sum_{j=0}^{\lceil n/2 \rceil - 1} (10)_2 \cdot 4^j, \sum_{j=0}^{\lceil n/2 \rceil - 1} (00)_2 \cdot 4^j)$  and  $(\check{\alpha}, \check{\beta}) = (\sum_{j=0}^{\lceil n/2 \rceil - 1} (00)_2 \cdot 4^j, \sum_{j=0}^{\lceil n/2 \rceil - 1} (01)_2 \cdot 4^j)$ . Based on Theorem 2, we propose the following efficient algorithm to get a candidate solution of  $k$  from the known parameters set  $\mathbb{G}$ , with  $\#\mathbb{G} = g$ .

- Step (1) Generate parameter sets  $\mathbb{G}_j \subseteq \mathbb{G}$  using the following rule

$$\mathbb{G}_j = \{(\alpha, \beta, y) \mid y = (\alpha \dot{+} k) \oplus (\beta \dot{+} k), y_j = 1\},$$

where  $j = 0 \sim n - 2$ .

- Step (2) Let  $i = 0$ ,  $c_0 = 0$  and set the default value of  $k$  to a random number in  $[0, 2^n - 1]$ .
- Step (3) Refresh the  $i$ -th bit  $k_i$  by look up Table 1 if  $\#\mathbb{G}_i \neq 0$  and then calculate  $c_{i+1}$  by Eq. (A.2).
- Step (4) If  $i < n - 2$ , increase  $i$  by 1. Go to Step (3) if  $\#\mathbb{G}_i \neq 0$ .
- Step (5) Calculate  $k$  using the equation  $k = \sum_{i=0}^{n-1} k_i \cdot 2^i$ .

Table 1: The values of  $k_i$  corresponding to the values of  $\alpha_i, \beta_i, c_i, y_i$ , and  $\tilde{y}_{i+1}$ .

$(y_i, \tilde{y}_{i+1})$	$(\alpha_i, \beta_i, c_i)$							
	(0, 0, 0)	(1, 0, 0)	(0, 1, 0)	(0, 0, 1)	(1, 1, 0)	(1, 0, 1)	(0, 1, 1)	(1, 1, 1)
(0, 0)	0, 1	0, 1	-	0, 1	0, 1	-	0, 1	0, 1
(0, 1)	-	-	0, 1	-	-	0, 1	-	-
(1, 0)	0	0	0	0	1	1	1	1
(1, 1)	1	1	1	1	0	0	0	0

The complexity of the above steps is mainly introduced by Step (1), which involves the exploration of all the first  $(n - 1)$  bit planes of  $y$  in  $\mathbb{G}$  to obtain  $\mathbb{G}_j$ . It can be inferred that the computational complexity is only  $O((n - 1) \cdot g)$ , which is much smaller than the complexity of the previous algorithm  $O(2^{n-1} \cdot g)$ . Besides, this algorithm generates only a single possible candidate  $k$ , thus avoiding the problem of selecting  $k$  from its candidate set<sup>2</sup>  $\mathbb{K}_g$ . Without loss of generality, assume that all the known parameters  $\alpha, \beta$  and  $y$  are uniformly distributed in the interval  $[0, 2^{n-1}]$ . Finally, the probability that the first  $i$  ( $0 \leq i < n - 1$ ) LSBs can be confirmed by  $\mathbb{G}$ , denoted as  $\text{Prob}(k_{0-i} \mid \mathbb{G})$ , is given as

$$\text{Prob}(k_{0-i} \mid \mathbb{G}) = \left(1 - \left(\frac{1}{2}\right)^g\right)^{i+1}.$$

Assuming  $n = 8$  as in the three image cryptosystems studied in Sec. 3, we depict in Fig. 2 this probability with respect to different values of  $g$ . As we can observe from this figure, the probability is relative high for small  $i$  when  $g$  equals 3. This result is further verified by carrying out experiments to Parvin’s cryptosystem under the assumption that the key streams  $K$  is generated using the key schedule described in [14, Sec. 2] while we artificially set  $U$  and  $V$  to zeros to fit our model proposed in Sec. 4.1. Then, we use 2 and 4 known plain-images and their corresponding cipher-images, i.e,  $g = 1$  and  $g = 3$ , to recover the key stream  $K$  using the algorithm described above. The recovered key stream is used to decrypt the cipher-image of “Baboon”, as shown in Fig. 3b), and the deciphered results are shown respectively in Fig. 3c) and Fig. 3d).

<sup>2</sup>In fact, every element in  $\mathbb{K}_g$  contains the same number of correct bits of  $k$  in average.



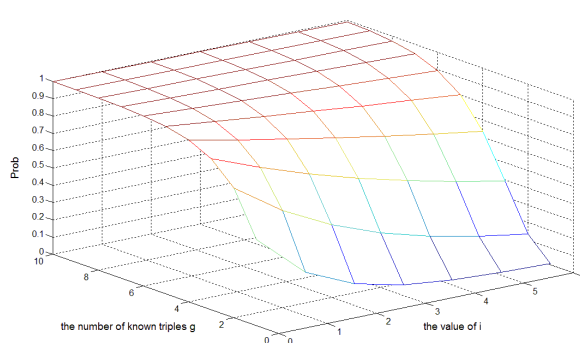


Figure 2: The probability that the first  $i$  LSBs of  $k$  can be confirmed with respect to different  $g$ .

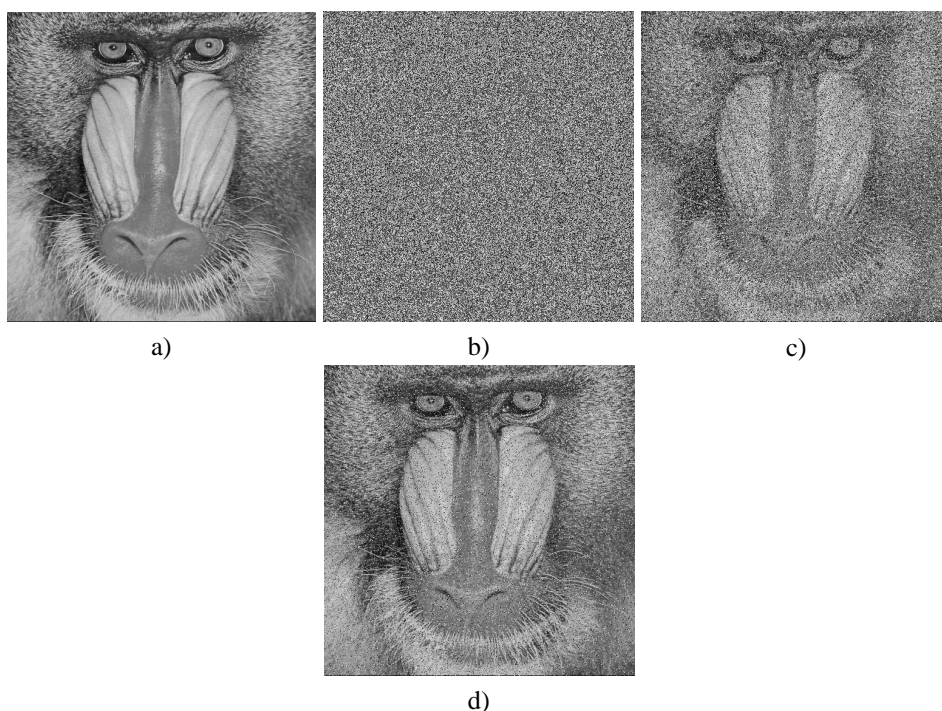


Figure 3: Numerical tests on simplified Parvin’s cryptosystem: a) Plain-image “Baboon” of size  $512 \times 512$ ; b) Encryption result of Fig 3a) using the modified Parvin’s cryptosystem; c) Recovery result using 2 pairs of known plain-images and their corresponding cipher-images; d) Recovery result using 4 pairs of known plain-images and their corresponding cipher-images.

### 5.2. Cryptographic strength of the equation $(\alpha + k) \oplus g(\beta, k) = y$

Accordingly to the results obtained in the previous section, the diffusion mechanism characterized by Eq. (10) is weak with respect to both CP and KP attacks. Specifically, two groups of chosen parameters are enough to uniquely determine  $k$ , while a few groups of known parameters are sufficient to determine  $k$  with overwhelming probability. The bidirectional diffusion scheme introduced in [15] and in [16], and defined by Eqs. (4) and (5), is suggested as a workaround. The idea of the new design is that all the pixels located after the current one are used in the diffusion process, with an avalanche effect (and so, an improvement) in the encryption of plain-images.

In the context of a CP attack scenario, thanks to the results shown in Sec. 4, the birectional diffusion scheme is immediately proven to be weak, since Eq. (4) can be converted to the form of Eq. (10). Considering that there are

$L$  pixels in an image, the data complexity (i.e., required number of plain-images and cipher-images) for breaking the cipher in [15] is only  $O(L)$ .

Furthermore, we can show that in the context of a KP attack scenario, the data complexity for breaking the cipher in [15] is the same as above. Let us consider the equation

$$(\alpha \dot{+} k) \oplus g(\beta, k) = y,$$

where  $g(\beta, k) = \lfloor \beta \cdot (10^8 \cdot k) \rfloor \bmod 256$ ,  $\alpha, y, k \in [0, 255]$  and  $\beta$  is a non-negative real number. Under the assumptions of a KP attack, i.e., that  $\alpha, \beta$  and  $y$  are known to the adversary, we can show that the data complexity for revealing  $k$  is only  $O(1)$ . In other words, the inefficient bidirectional diffusion scheme actually does not improve the security level of Eq. (10) with respect to KP attack.

We start our analysis from the trivial case  $\beta \equiv 0$ . Under this assumption, Eq. (13) is simplified to

$$y = \alpha \dot{+} k$$

since  $g(\beta, k) = \lfloor \beta \cdot (10^8 \cdot k) \rfloor \bmod 256 \equiv 0$ . Thus,  $k$  can be calculated as  $k = y \dot{-} \alpha$ . For the general case  $\beta > 0$ , it is easy to observe that the value of  $g(\beta, k)$  is sensitive to the changes of  $k$ . In other words, given  $\alpha, \beta$  and  $y$ , the result of  $(\alpha \dot{+} k) \oplus g(\beta, k)$  will be different from  $y$  with an overwhelming probability even if  $k$  slightly deviates from its true value. For convenience, let  $\mathbb{G} = \{(\alpha, \beta, y) \mid y = (\alpha \dot{+} k) \oplus g(\beta, k)\}$  and assume  $\#\mathbb{G} = g = O(1)$ . The following procedures describe a method to determine  $k$  from  $\mathbb{G}$  by using this observation.

- Step (1) Let  $l = 1$  and the solution set  $\mathbb{K}_l = \emptyset$ .
- Step (2) Select the  $l$ -th element of  $\mathbb{G}$  and exhaustively test all the  $2^8$  possible values of  $k$  to check whether it satisfies Eq. (13). Collect all the possible values of  $k$  that meet the requirement and denote them as  $\mathbb{K}_l$ .
- Step (3) Go to Step (5) if  $\#\mathbb{K}_l = 1$ .
- Step (4) Set  $l = l + 1$  if  $l < g$ . Go to Step (2) and update the solution set by  $\mathbb{K}_{l+1} = \mathbb{K}_{l+1} \cap \mathbb{K}_l$ .
- Step (5) Print the value of the single element of  $\mathbb{K}_l$  if  $\#\mathbb{K}_l = 1$ . Otherwise output  $\#\mathbb{K}_l$ .

We verify the validity of this algorithm by carrying out experiments to Norouzi's cryptosystem (that can be viewed as the simplified version of Yang's design). Three  $512 \times 512$  known plain-images with different statistical characteristics are employed as our test images (Fig. 4a-c)). These images are encrypted using Norouzi's cryptosystem under the secret key that was adopted in [15, Sec. 3]. Using the techniques illustrated in Sec. 4, we cast the relationship between the plaintext pixels and ciphertext pixels to the form of Eq. (13). Then, we respectively use 1, 2 and 3 pairs of plain-images and their corresponding cipher-images to retrieve the equivalent secret key stream  $K$  by the above algorithm. The average *recovery rates* of the proposed KP attack using different numbers of known plain-images are

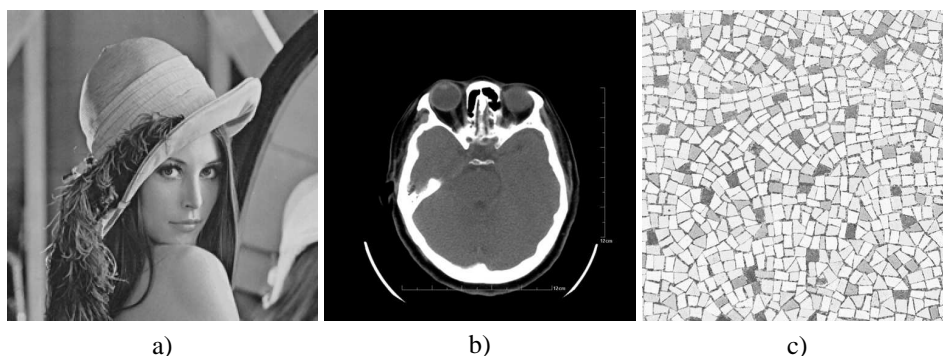


Figure 4: Three test images for recovering the equivalent key stream of Norouzi's cryptosystem: a) "Lena"; b) CT image; c) Mosaic image.

Table 2: Average recovery rate using different numbers of known plain-images.

Number of known plain-images	average <i>recovery rate</i>
1	66.6637%
2	99.8247%
3	100%

listed in Table 2. Here, the *recovery rate* is defined as

$$\text{recovery rate} = \frac{\text{number of correctly recovered elements of } K}{\text{total number of elements in } K} \times 100\%.$$

It can be observed that the average *recovery rate* raises as the number of known plain-images increase. Even the number of known plain-images is only 1, the average *recovery rate* is close to 67%. When the number of known plain-images is 3, the *recovery rate* grows to 100%. Furthermore, we utilize these recovered equivalent key streams to decrypt an intercepted cipher-image and the result is shown in Fig. 5a)-c). From Fig. 5, it is concluded that 100% *recovery rate* of the key stream guarantees perfect reconstruction of the intercepted cipher-image, while a high *recovery rate* of the key stream does not lead to good or acceptable visual quality. This phenomenon is attributable to the bidirectional diffusion property of Eq. (12), where the error of a wrongly decrypted pixel will spread to all successive decryption in a pseudo-random manner.

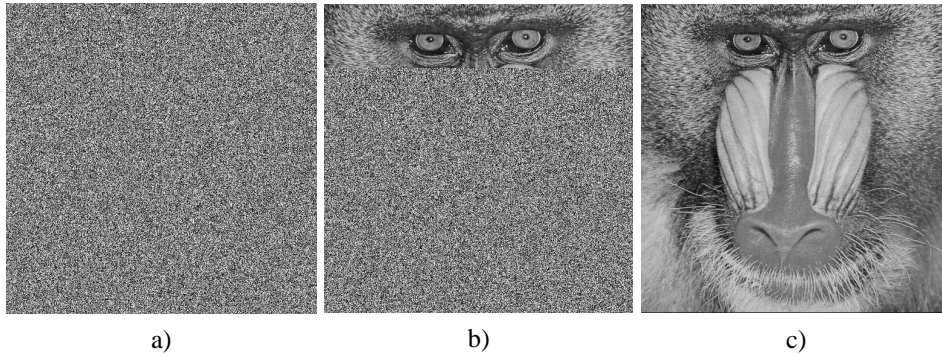


Figure 5: Recovery results: a) Deciphered result using the key stream retrieved from Fig. 4a); b) Deciphered result using the key stream retrieved from Fig. 4a) and b); c) Deciphered result using the key stream retrieved from Fig. 4a)-c).

## 6. Cryptographic applications

Exploiting the security analyses of Eq. (10) and Eq. (13) shown above, this section presents plaintext attacks to the full cryptosystems proposed in [14, 15, 16] and briefly discusses other security implications related to our analyses.

### A. Cryptanalysis of Parvin's cryptosystem

As described in Sec. 3, Parvin's cryptosystem is composed of circular permutations and a single diffusion stage. To apply our analysis result presented in Sec. 5.1, we need first to recover the equivalent key streams used for row and column circular permutation. The underlying strategy is to study the relationship between cipher-images produced by some some bottom-line chosen plain-images whose elements are invariant with respect to row and column permutations. Similar ideas are also employed to analyze other chaos-based cryptosystems [29, 37, 40]. Here, we suppose that an image having fixed gray value is available and denote it as  $P_1 = \{p_1(i, j) \equiv 0\}_{i=1, j=1}^{H, W}$ . Then, we set  $p_1(1, 1) = 128$  and keep all the other pixels unchanged and denote the modified image by  $P_2 = \{p_2(i, j)\}_{i=1, j=1}^{H, W}$ .

Figure 6a) and b) depict the cipher-images corresponding to  $P_1$  and  $P_2$ , respectively. Here,  $H = W = 512$  is chosen. The difference of the two cipher-images is shown in Fig. 6c). Find the first pixel whose value is 128 and denote its position by  $(i_1, j_1)$ . Referring to Eqs. (1), (2) and (3), it can be concluded that  $u(1) = ((j_1 - 1) \bmod H) + 1$  and  $v(1) = ((i_1 - 1) \bmod W) + 1$ . Repeat this test for all the diagonal pixels of  $P_1$ ,  $U$  and  $V$ , the key streams for row and column permutations, can be retrieved completely. Combining with the analysis presented in Sec. 5.1, the data complexity of the CP attack is  $O(1) + \max(H, W)$  with an overwhelming probability.

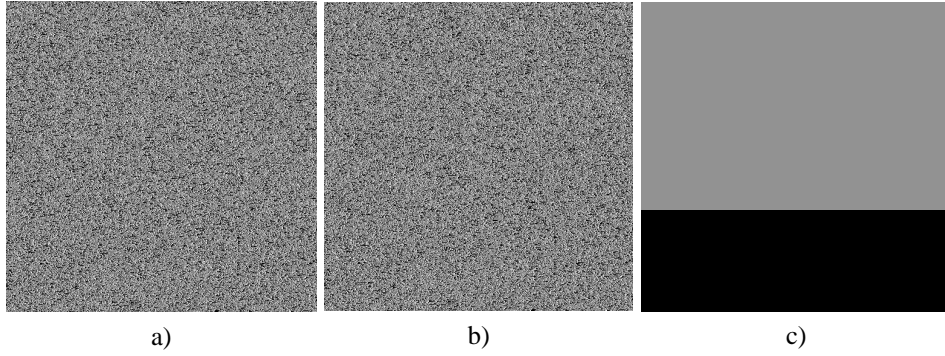


Figure 6: Example test for recovering the equivalent permutation key streams of Parvin’s cryptosystem: a) The cipher-image of  $P_1$ ; b) The cipher-image of  $P_2$ ; c) The difference between Figs. 6a) and b) using XOR operation.

## B. Cryptanalysis of Norouzi’s and Yang’s cryptosystems

Applying the analysis presented in Sec. 5.2, it is readily to conclude that Norouzi’s cryptosystem can be compromised in KP attack scenario at data complexity  $O(1)$ . For Yang’s scheme, the remaining task is to recover the remaining key streams used for permutation. By noting that Yang’s scheme is different from Parvin’s only by the order of diffusion and permutation in the present context, we use the similar strategy to reveal the equivalent permutation key streams of Yang’s cryptosystem. For example, to reveal  $v(H)$  and  $u(W - 2)$ , we employ three chosen-images  $P_1$ ,  $P_2$  and  $P_3$  with the form

$$\begin{aligned} P_1 &= [0, 0, 0, \dots, 0, 0, 0, 1], \\ P_2 &= [0, 0, 0, \dots, 0, 0, 1, 0], \\ P_3 &= [0, 0, 0, \dots, 0, 1, 0, 0]. \end{aligned}$$

According to Eqs. (6), (7) and (8), their corresponding cipher-images  $C_1$ ,  $C_2$  and  $C_3$  satisfy the following two conditions: 1) there are two distinct ciphertext elements between  $C_1$  and  $C_2$ , 2) there are three distinct ciphertext elements between  $C_3$  and  $C_1$  (or  $C_2$ ). Comparing  $C_1$ ,  $C_2$  and  $C_3$ , the location of  $c_1(H, W - 2)$  can be identified. Figure 7 sketches the rules involved in this procedure. Repeat this test to the last row and column of  $P_1$ , the equivalent permutation key streams  $U$  and  $V$  can be fully recovered at the data complexity<sup>3</sup>  $O(H + W)$  under CP attack.

## C. Other cryptographic implications

Observing that the analysis with respect to the equation  $(\alpha \dot{+} k) \oplus g(\beta, k) = y$  involves exhaustive searching the possible key space, an intuitive workaround for Norouzi’s and Yang’s cryptosystems is to group several pixels as a single element to enlarge the real key space. For example, combine 15 pixels together will make the key space grows to  $2^{120}$  and frustrate the KP attack presented in Sec. 5.2. However, Norouzi’s and Yang’s cryptosystems can be cast to the form of  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  in CP attack scenario and cryptanalysis of this equation is regardless of the bit length of the plaintext. It can be concluded that using composite pixel representation as a remedy is futile.

<sup>3</sup>The permutation for the last two pixels can be retrieved by brute force search.

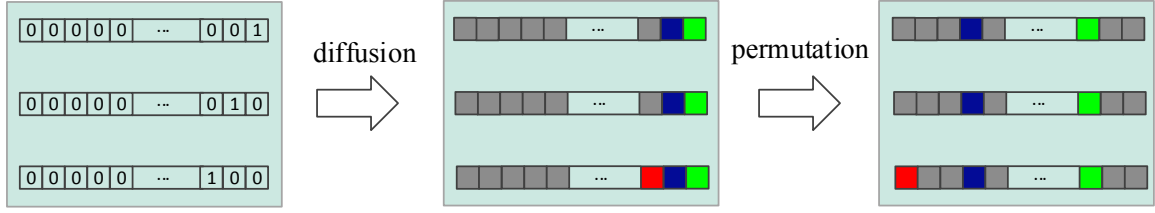


Figure 7: Illustration of the CP attack on Yang's cryptosystem to recover the equivalent secret key used for permutation.

Regarding the widely usage of the diffusion equation (3) [10, 24, 50, 51, 11, 12, 27, 28], our analysis on the equation  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  seems useful in evaluating security of other ciphers also based on this kind of diffusion mechanism. The fact that the search space of the unknown  $k$  could be reduced from  $2^{2n}$  to  $O(1)$  indicates that a loophole exists in the corresponding cryptosystems, and that it can be used to retrieve information about the key. Even worse, this loophole cannot be fixed by choosing a larger  $n$ . With this concern, we recommend using some relative strong diffusion schemes with respect to KP and CP attacks, such as  $(k_1 \dot{+} k_2) \oplus (k_1 \dot{+} (k_2 \oplus \beta)) = y$  [52].

## 7. Conclusion

Considering the three cryptosystems proposed in [14, 15, 16] as case studies, we have studied the security properties of equations (i)  $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$  and (ii)  $(\alpha \dot{+} k) \oplus g(\beta, k) = y$ . The underlying theory of the key scheduling process employed in these example cryptosystems ranging from chaotic/hyper-chaotic function to quantum computation, which are regarded as having different characteristics. However, our analyses reveal that all the three ciphers are very weak upon plaintext attacks. Specifically, the equivalent key streams used in these designs can be retrieved using a small number of plain-images. We provide a sufficient condition to determine the unknown  $k$  of equation (i) under the KP attack scenario. The relationship of our result and the existing ones under CP attack assumption [38, 39, 29] is also investigated. The algorithms provided and the extensive numerical experiments confirm that both equation (i) and (ii) can be solved using only  $O(1)$  known plaintexts. In this concern, it is readily to conclude that most image ciphers based on a single round permutation-diffusion architecture are insecure with respect to plaintext attacks. Our work can be extended to investigate diffusion equations involves more complex cryptographic primitives, such as modulo multiplication [41].

## Acknowledgements

This research was partly supported by the Research Activities Fund of City University of Hong Kong and Fundamental Research Funds for the Central Universities (XDJK2015C077).

## Appendix A. Proof of Theorem 2

Let us consider the equivalent form of Eq. (10), i.e.,

$$\tilde{y} = (\alpha \dot{+} k) \oplus (\beta \dot{+} k) \oplus \alpha \oplus \beta. \quad (\text{A.1})$$

Observe that the  $(i+1)$ -th bit of  $\tilde{y}$ , i.e.,  $\tilde{y}_{i+1}$ , can be calculated using only the previous bits  $\alpha_i, \beta_i, k_i, c_i, \tilde{c}_i$ , ( $i \in [0, n-2]$ ) by the following three equations

$$\begin{cases} \tilde{y}_{i+1} = c_{i+1} \oplus \tilde{c}_{i+1}, \\ c_{i+1} = k_i \alpha_i \oplus k_i c_i \oplus \alpha_i c_i, \\ \tilde{c}_{i+1} = k_i \beta_i \oplus k_i \tilde{c}_i \oplus \beta_i \tilde{c}_i, \end{cases} \quad (\text{A.2})$$

Table A.3: The values of  $\tilde{y}_{i+1}$  corresponding to the values of  $\alpha_i, \beta_i, \tilde{y}_i, k_i$  and  $c_i$ .

$(k_i, c_i)$	$(\alpha_i, \beta_i, \tilde{y}_i)$							
	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
(0, 0)	0	0	0	1	0	0	0	1
(0, 1)	0	0	1	0	1	1	0	1
(1, 0)	0	1	1	1	1	0	0	0
(1, 1)	0	1	0	0	0	1	0	0
	Col(1)	Col(2)	Col(3)	Col(4)	Col(5)	Col(6)	Col(7)	Col(8)

where  $c_i$  is the carry bit at the  $i$ -th bit plane of  $(\alpha \dot{+} k)$  and  $\tilde{c}_i = \tilde{y}_i \oplus c_i$ . Table A.3 lists the values of  $\tilde{y}_{i+1}$  that computed from Eq. (A.2) under all the possible values of  $\alpha_i, \beta_i, \tilde{y}_i, k_i$  and  $c_i$ .

Table A.3 indicates that  $k_i$  can be determined if  $(\alpha_i, \beta_i, \tilde{y}_i)$  falls in  $\{\text{Col}(2), \text{Col}(3), \text{Col}(5), \text{Col}(8)\}$ , i.e.,  $y_i = \tilde{y}_i \oplus \alpha_i \oplus \beta_i = 1$ , and  $c_i$  is known. Based on this observation, the theorem can be proved by mathematical induction on  $i$  ( $0 \leq i \leq n-2$ ). We first consider the case for  $i = 0$ . Since  $c_0 \equiv \tilde{c}_0 \equiv 0$ , the condition

$$\begin{aligned} y_0 &= \tilde{y}_0 \oplus \alpha_0 \oplus \beta_0 \\ &= c_0 \oplus \tilde{c}_0 \oplus \alpha_0 \oplus \beta_0 \\ &= \alpha_0 \oplus \beta_0 \\ &= 1 \end{aligned}$$

implies

$$\begin{aligned} \tilde{y}_1 &= c_1 \oplus \tilde{c}_1 \\ &= k_0 \alpha_0 \oplus k_0 \beta_0 \\ &= k_0 (\alpha_0 \oplus \beta_0) \\ &= k_0. \end{aligned}$$

Hence the theorem is proved for the case  $i = 0$ . Assume that it is valid for  $i = m$  ( $m \leq n-3$ ), i.e., all the  $m$  least significant bits of  $k$  are confirmed when  $y = \sum_{j=0}^{m-1} 2^j$  and thus all the  $c_i$  and  $\tilde{c}_i$  can be derived by Eq. (A.2) for all  $i \in [0, m+1]$ . Then, for the case  $i = m+1$ , the condition  $y_{m+1} = 1$  implies that

$$y_{m+1} = c_{m+1} \oplus \tilde{c}_{m+1} \oplus \alpha_{m+1} \oplus \beta_{m+1} = 1$$

holds when referring to Eqs. (A.1) and (A.2). When computing  $y_{m+2}$  by Eq. (A.2), we have

$$\begin{aligned} \tilde{y}_{m+2} &= c_{m+2} \oplus \tilde{c}_{m+2} \\ &= k_{m+1} \alpha_{m+1} \oplus k_{m+1} \beta_{m+1} \oplus k_{m+1} c_{m+1} \oplus k_{m+1} \tilde{c}_{m+1} \oplus \alpha_{m+1} c_{m+1} \oplus \beta_{m+1} \tilde{c}_{m+1} \\ &= k_{m+1} (\alpha_{m+1} \oplus \beta_{m+1} \oplus c_{m+1} \oplus \tilde{c}_{m+1}) \oplus \alpha_{m+1} c_{m+1} \oplus \beta_{m+1} \tilde{c}_{m+1} \\ &= k_{m+1} \oplus \alpha_{m+1} c_{m+1} \oplus \beta_{m+1} \tilde{c}_{m+1}. \end{aligned}$$

Observing that  $\alpha_{m+1}, \beta_{m+1}$  and  $\tilde{y}_{m+2}$  are known parameters in our KP attack scenario,  $c_{m+1}$  and  $\tilde{c}_{m+1}$  are the result from the previous induction step, we conclude that

$$k_{m+1} = \tilde{y}_{m+2} \oplus \alpha_{m+1} c_{m+1} \oplus \beta_{m+1} \tilde{c}_{m+1},$$

thus completing the mathematical induction and hence proving the theorem.

## References

- [1] W. C. Barker, E. B. Barker, NIST Special Publication 800-67 revision 1: Recommendation for the triple data encryption algorithm (TDEA) block cipher, National Institute of Standards & Technology.

- [2] J. Daemen, V. Rijmen, The design of Rijndael: AES-the advanced encryption standard, Springer Science & Business Media, 2002.
- [3] F. Liu, H. Koenig, A survey of video encryption algorithms, *Computers & Security* 29 (1) (2010) 3–15.
- [4] S. Lian, X. Chen, On the design of partial encryption scheme for multimedia content, *Mathematical and Computer Modelling* 57 (11) (2013) 2613–2624.
- [5] S. Lian, Z. Liu, Z. Ren, H. Wang, Commutative encryption and watermarking in video compression, *IEEE Transactions on Circuits and Systems for Video Technology* 17 (6) (2007) 774–778.
- [6] H. Cheng, X. Li, Partial encryption of compressed images and videos, *IEEE Transactions on Signal Processing* 48 (8) (2000) 2439–2451.
- [7] S. Li, G. Chen, A. Cheung, B. Bhargava, K.-T. Lo, On the design of perceptual MPEG-video encryption algorithms, *IEEE Transactions on Circuits and Systems for Video Technology* 17 (2) (2007) 214–223.
- [8] E. Magli, M. Grangetto, G. Olmo, Transparent encryption techniques for H. 264/AVC and H. 264/SVC compressed video, *Signal Processing* 91 (5) (2011) 1103–1114.
- [9] W. Zeng, S. Lei, Efficient frequency domain selective scrambling of digital video, *IEEE Transactions on Multimedia* 5 (1) (2003) 118–129.
- [10] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *International Journal of Bifurcation and Chaos* 8 (06) (1998) 1259–1284.
- [11] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos, Solitons & Fractals* 21 (3) (2004) 749–761.
- [12] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, *International Journal of Bifurcation and Chaos* 14 (10) (2004) 3613–3624.
- [13] L. Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, J. Gan, A chaotic image encryption scheme owning temp-value feedback, *Communications in Nonlinear Science and Numerical Simulation* 19 (10) (2014) 3653–3659.
- [14] Z. Parvin, H. Seyedarabi, M. Shamsi, A new secure and sensitive image encryption scheme based on new substitution with chaotic function, *Multimedia Tools and Applications* (2014) 1–18.
- [15] B. Norouzi, S. Mirzakhaki, S. M. Seyedzadeh, M. R. Mosavi, A simple, sensitive and secure image encryption algorithm based on hyperchaotic system with only one round diffusion process, *Multimedia Tools and Applications* 71 (3) (2014) 1469–1497.
- [16] Y.-G. Yang, Q.-X. Pan, S.-J. Sun, P. Xu, Novel image encryption based on quantum walks, *Scientific Reports* 5 (7784).
- [17] W. Zhang, K. W. Wong, H. Yu, Z.-L. Zhu, A symmetric color image encryption algorithm using the intrinsic features of bit distributions, *Communications in Nonlinear Science and Numerical Simulation* 18 (3) (2013) 584–600.
- [18] Z. L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, *Information Sciences* 181 (6) (2011) 1171–1186.
- [19] K.-W. Wong, B. S.-H. Kwok, W.-S. Law, A fast image encryption scheme based on chaotic standard map, *Physics Letters A* 372 (15) (2008) 2645–2652.
- [20] Y. Zhou, K. Panetta, S. Agaian, C. Chen,  $(n, k, p)$ -Gray code for image systems, *IEEE Transactions on Cybernetics* 43 (2) (2013) 515–529.
- [21] M. Zanin, A. N. Pisarchik, Gray code permutation algorithm for high-dimensional data encryption, *Information Sciences* 270 (2014) 288–297.
- [22] K.-W. Wong, A fast chaotic cryptographic scheme with dynamic look-up table, *Physics Letters A* 298 (4) (2002) 238–242.
- [23] H. Zhu, C. Zhao, X. Zhang, L. Yang, An image encryption scheme using generalized arnold map and affine cipher, *Optik-International Journal for Light and Electron Optics* 125 (22) (2014) 6672–6677.
- [24] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, *Optics Communications* 285 (1) (2012) 29–37.
- [25] K. Rao, C. Gangadhar, Modified chaotic key-based algorithm for image encryption and its VLSI realization, in: *Proceedings of the 2007 15th International Conference on Digital Signal Processing*, 2007, pp. 439–442.
- [26] C. Gangadhar, K. D. Rao, Hyperchaos based image encryption, *International Journal of Bifurcation and Chaos* 19 (11) (2010) 3833–3839.
- [27] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, *Optics Communications* 284 (16) (2011) 3895–3903.
- [28] Y. Zhou, Z. Hua, C. Pun, C. Chen, Cascade chaotic system with applications, to appear in *IEEE Transactions on Cybernetics*.
- [29] X. Wang, D. Luan, X. Bao, Cryptanalysis of an image encryption algorithm using Chebyshev generator, *Digital Signal Processing* 25 (2014) 244–247.
- [30] P. Refregier, B. Javidi, Optical image encryption based on input plane and fourier plane random encoding, *Optics Letters* 20 (7) (1995) 767–769.
- [31] W. Chen, B. Javidi, X. Chen, Advances in optical security systems, *Advances in Optics and Photonics* 6 (2) (2014) 120–155.
- [32] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, *optics letters* 31 (8) (2006) 1044–1046.
- [33] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys, *Optics letters* 30 (13) (2005) 1644–1646.
- [34] X. Peng, H. Wei, P. Zhang, Chosen-plaintext attack on lensless double-random phase encoding in the fresnel domain, *Optics letters* 31 (22) (2006) 3261–3263.
- [35] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, P. Natarajan, Local shannon entropy measure with statistical tests for image randomness, *Information Sciences* 222 (2013) 323–342.
- [36] A. Rukhin, et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22rev1a (2010).
- [37] D. Arroyo, J. Diaz, F. B. Rodriguez, Cryptanalysis of a one round chaos-based substitution permutation network, *Signal Processing* 93 (5) (2013) 1358–1364.
- [38] C. Li, M. Z. Chen, K.-T. Lo, Breaking an image encryption algorithm based on chaos, *International Journal of Bifurcation and Chaos* 21 (07) (2011) 2067–2076.
- [39] C. Li, Y. Liu, L. Y. Zhang, M. Z. Chen, Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation, *International Journal of Bifurcation and Chaos* 23 (04) (2013) 1–12.
- [40] C. Li, L. Y. Zhang, R. Ou, K.-W. Wong, S. Shu, Breaking a novel colour image encryption algorithm based on chaos, *Nonlinear dynamics*

70 (4) (2012) 2383–2388.

- [41] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, K. W. Wong, Chosen-plaintext attack of an image encryption scheme based on modified permutation-diffusion structure, arXiv:1503.06638.
- [42] E. Solak, C. Çokal, O. T. Yildiz, T. Biyikoğlu, Cryptanalysis of Fridrich's chaotic image encryption, *International Journal of Bifurcation and Chaos* 20 (05) (2010) 1405–1413.
- [43] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, G. Chen, Cryptanalyzing a chaos-based image encryption algorithm using alternate structure, *Journal of Systems and Software* 85 (9) (2012) 2077–2085.
- [44] S. Li, C. Li, G. Chen, N. G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, *Signal Processing: Image Communication* 23 (3) (2008) 212–223.
- [45] A. Jolfaei, X.-W. Wu, V. Muthukkumarasamy, On the security of permutation-only image encryption schemes, *IEEE Transactions on Information Forensics and Security*.
- [46] F. Chen, K.-W. Wong, X. Liao, T. Xiang, Period distribution of generalized discrete arnold cat map for  $n = p^e$ , *IEEE Transactions on Information Theory* 58 (1) (2012) 445–452.
- [47] F. Chen, K.-W. Wong, X. Liao, T. Xiang, Period distribution of generalized discrete arnold cat map for  $n = 2^e$ , *IEEE Transactions on Information Theory* 59 (5) (2013) 3249–3255.
- [48] F. Chen, K.-W. Wong, X. Liao, T. Xiang, Period distribution of generalized discrete arnold cat map, *Theoretical Computer Science* 552 (2014) 13–25.
- [49] Y. Niu, X. Wang, M. Wang, H. Zhang, A new hyperchaotic system and its circuit implementation, *Communications in Nonlinear Science and Numerical Simulation* 15 (11) (2010) 3518–3524.
- [50] Z. Eslami, A. Bakhshandeh, An improvement over an image encryption method based on total shuffling, *Optics Communications* 286 (2013) 51–55.
- [51] G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, *Optics Communications* 284 (12) (2011) 2775–2780.
- [52] S. Paul, B. Preneel, Solving systems of differential equations of addition, in: *Proceedings of the 10th Australasian Conference on Information Security and Privacy*, Springer, 2005, pp. 75–88.