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

On the Security of a Class of Diffusion Mechanisms for Image Encryption

Leo Yu Zhang, *Member, IEEE*, Yuansheng Liu, Fabio Pareschi, *Member, IEEE*, Yushu Zhang, Kwok-Wo Wong, *Senior Member, IEEE*, Riccardo Rovatti, *Fellow, IEEE*, and Gianluca Setti, *Fellow, IEEE*

***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 this paper are also discussed.**

***Index Terms*—Cryptanalysis, diffusion, image encryption, plaintext attack.**

I. 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. In this concern, some researchers suggested incorporating the traditional ciphers into the multimedia coding procedure then selectively encrypting part of the data volume [3]–[5] and the rest advocated designing specialized ciphers by taking advantage of the particular structure of multimedia data [6]. The image cryptosystems discussed below belong to the latter category.

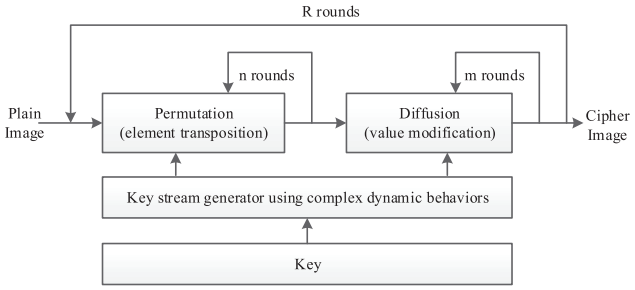


Fig. 1. Schematic of Fridrich's permutation-diffusion architecture.

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. Among all the image ciphers belonging to this class, the permutation-diffusion architecture, which is originated from the substitution-permutation network [7] and proposed by Fridrich in [8], is the most popular candidate. As depicted in Fig. 1, its 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 2-D discretized chaotic map like Baker or Cat map. Chen *et al.* [9] and Mao *et al.* [10] suggested using 3-D

Manuscript received April 8, 2016; revised November 17, 2016; accepted March 11, 2017. This work was supported in part by the Research Activities Fund of City University of Hong Kong, in part by the National Natural Science Foundation of China under Grant 61502399, and in part by the Natural Science Foundation Project of Chongqing CSTC under Grant cstc2015jcyjA40039. This paper was recommended by Associate Editor P. Chen.

L. Y. Zhang is with the Guangdong Key Laboratory of Data Security and Privacy Preserving, College of Information Science and Technology, Jinan University, Guangzhou 510632, China, and also with the Department of Electronic Engineering, City University of Hong Kong, Hong Kong (e-mail: leocityu@gmail.com).

Y. Liu is with the Advanced Analytics Institute, University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: yuansheng.liu@student.uts.edu.au).

F. Pareschi and G. Setti are with the Department of Engineering, University of Ferrara, 44122 Ferrara, Italy, and also with the Advanced Research Center on Electronic Systems, University of Bologna, 40125 Bologna, Italy (e-mail: fabio.pareschi@unife.it; gianluca.setti@unife.it).

Y. Zhang is with the School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China (e-mail: yushuboshi@163.com).

K.-W. Wong, deceased, was with the Department of Electronic Engineering, City University of Hong Kong, Hong Kong.

R. Rovatti is with the Department of Electrical, Electronic, and Information Engineering, University of Bologna, 40136 Bologna, Italy, and also with the Advanced Research Center on Electronic Systems, University of Bologna, 40125 Bologna, Italy (e-mail: riccardo.rovatti@unibo.it).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCYB.2017.2682561

chaotic map to de-correlate the relationship among pixels in a more efficient way. Wong *et al.* [11] 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.* [12] and Zhang *et al.* [13] suggested carrying out permutation to bit-level instead of pixel-level. It is also worth mentioning that there are permutation techniques based on general gray code [14], [15], which can be considered as permutation carried out at an arbitrary bit length.

2) Developing novel diffusion techniques. As illustrated by Fridrich [8], the diffusion operation aims to spread the information of plaintext to the whole ciphertext. This process can be formulated as

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

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. In line with this concern, Chen *et al.* [9] suggested mixing modulo addition and bitwise exclusive or (XOR) operations in an output feedback manner via

$$c(l) = (p(l) \dot{+} k(l)) \oplus k(l) \oplus c(l-1) \tag{2}$$

where $\oplus$ stands for XOR. Many other works adopt similar (or even the same) diffusion mechanisms, see [16]–[19] for examples. It is not surprising that the computational efficient modulo multiplication can also be incorporated into the diffusion stage [20], [21]. Moreover, recent works suggested using real number arithmetic to enhance the security level of the diffusion stage [22], [23] at the cost of a reduced computational efficiency due to the employment of complicated arithmetic operations.

The second major approach in the design of image cryptosystem is based on optical technology, 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 Refregier and Javidi [24]. Many other symmetric cryptosystems are based on this design, such as [25] and [26]. A comprehensive review on this topic can be found in [27] and [28]. 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 [29]–[31] and the adoption of image cryptosystem based on optical technology for real application should be cautious.[1]

[1]Note that there also exist optical asymmetric cryptosytems, which are deemed more secure than their symmetric counterparts (i.e., those based on DRPE) since they are nonlinear by nature [28].

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, many statistical analysis-based methods should be conducted as a preliminary security evaluation of the considered image cipher. For instances, employing the horizontal/vertical relationship enables the attacker to launch ciphertext-only attack to row/column permuted image ciphers [32], and designing images with specific patterns would bypass the effect of global entropy measure [33].

More in general, any deviation of the statistical properties of the ciphertext stream from that of a random stream may be exploited by an attacker to infer information on the plain text. For this reason, any coding should pass statistical tests for randomness developed so far in [34]. Other tests specifically developed for image cryptosystems may include histogram analysis, correlation analysis, and sensitivity analysis [10].

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 [35]–[37]. For example, the equivalent key stream used for permutation of Fridrich's design can be retrieved in chosen-ciphertext attack scenario [36] and a chaos-based image cipher with Feistel structure is insecure with respect to differential attack when the round number is smaller than 5 [37]. 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. Li *et al.* [38] presented a general quantitative study of permutation-only encryption algorithms against plaintext attacks. Their result was further improved in [39] with respect to data and computation complexity. Chen *et al.* [40]–[42] 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

$$(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y. \tag{3}$$

As of the high implementation speed and nonlinearity over GF(2), mixing modulo addition and XOR becomes very popular for designing traditional algorithms, such as stream cipher [43], block cipher [44], [45], and the MD-family of hash functions. As a result, there is also a boom in the cryptanalyses about modulo addition, XOR and different forms of their combination. The fact that the linear properties of modulo addition reduce to the linear properties of the carry function was reported in [46] and the biased probability distribution of the carry function in modulo addition was explored by [47]. The fact that approximating the combination of modulo addition and XOR pseudo-linearly in small window enables a

key recovery attack on 11 rounds of Threefish-256 [44] was reported by McKay and Vora [48]. Utilizing the linearity of the carry function, Paul *et al.* [49]–[51] reported that the number of queries (α, β) [or $(0, \beta)$ for (5)] to obtain the unknown (k_1, k_2) of the following two kinds of DEA:

$$(k_1 \dot{+} k_2) \oplus ((k_1 \oplus \alpha) \dot{+} (k_2 \oplus \beta)) = y \tag{4}$$

$$(k_1 \dot{+} k_2) \oplus (k_1 \dot{+} (k_2 \oplus \beta)) = y \tag{5}$$

are 6 and 2^{n-2}, respectively, (n is the bit-length of $k_1, k_2, \alpha, \beta, y$). This finding can be used in a chosen-plaintext (CP) attack to recover the secret key of Helix [43]. Despite being extensively studied, these two operations and their different combinations are still continuously used in many fields of information security, such as enabling signal processing techniques in the encrypted domain [52] and hiding data in multimedia signals [53].

Following the similar ideas used in [50], it was reported in [54] and [55] that two pairs of chosen queries (α, β) are sufficient to reveal the unknown k of our interested DEA (3). As far as we know, these two works must be considered as independent analyses of particular image ciphers [56], [57] and cannot be directly applied in the analyses of other similar image ciphers. Starting from the linearity of the carry function, this paper reports that (a special form of) the biased output y of (3) leaks information of the unknown parameter k, regardless of the value of the query (α, β) and the number of queries required.

In more detail, we take into account the three image cryptosystems proposed in [19], [22], and [23] 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 (α, β)] 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 paper and previous ones is that we assume that α and β cannot be freely chosen, as for example in [54] and [55]. 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 weaknesses of its variants are pointed out. Numerical simulation results are then provided to support our analyses. This paper is reproducible, and the corresponding codes are openly accessible at https://sites.google.com/site/leoyuzhang/.

The major innovative contribution of this paper is to take the three image cryptosystems proposed in [19], [22], and [23] as case studies, all of them adopting Fridrich's permutation-diffusion structure, and to study the relationship between their diffusion mechanisms and the DEA $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$ under KP attack as well as the sufficient condition to solve this DEA. Since the similar or exact DEA can be found in many other designs so the application of our analyses is not limited to the three case studies. Besides, we experimentally present a simple KP attack to a variant of this DEA. As a proof of usefulness of the analyses, we demonstrate a detailed security evaluation of the whole version of the encryption schemes in [19], [22], and [23], which combine the investigated diffusion mechanism and secret permutation.

The rest of this paper is organized as follows. Section II introduces the notations that is used in this paper and the assumptions we work on. Three case studies of image cryptosystem are reviewed in Section III and the differential equations of modulo addition are derived in Section IV. Section V presents security analyses and numerical results of the equations derived above against KP attack. The applications of our results are discussed in Section VI and conclusion remarks are drawn in the last section.

II. Notations and Main Assumptions

In the following, we will use the matrix $[p(i,j)]_{H,W}$ to represent the 2-D format of a plain-image $\boldsymbol{P}$ of size $H \times W$ (Height $\times$ Width). Scanning it in the raster order, the 1-D format of the plain-image can be denoted as the vector $[p(1), p(2), \ldots, p(L)]$ ($L = H \times W$). The 2-D and 1-D representations of the cipher-image $\boldsymbol{C}$ are $[c(i,j)]_{H,W}$ and $[c(k)]$, respectively. We use a_i to denote the ith 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 "$\|$" denote *modulo* 2^n *addition*, *modulo* 2^n *subtraction*, *bitwise exclusive or*, *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 $\mathbb{G}$ is denoted by $\#\mathbb{G}$. With the term *KSA* we will refer to the key-setup algorithm of a specific cipher, and use *KSA*(*Seed*) to indicate the process generating all necessary key streams given a secret *Seed* by the *KSA*.

In order to correctly evaluate the security level of a diffusion mechanism either in known- or CP 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 attacker requires only one encryption machine (computing oracle) and the goal of the attack is either to collect information on the secret key *Seed* or, equivalently, on the key stream(s) *KSA*(*Seed*) generated from *Seed*. Note that security evaluation of the discussed diffusion mechanisms under other cryptanalysis models, such as brute-force attack, is as important as the evaluation of them under KP attack, but they are not the focus of this paper. Also, the setting here is slightly different from literature works [49]–[51], where the computing oracle is defined as a machine that faithfully calculates the output of DEA (4) and (5) under given parameters. Hereinafter, we will consider only the problem of recovering *KSA*(*Seed*).

III. Image Cryptosystems Review

In this section, we briefly review the three cryptosystems for image encryption proposed in [19], [22], and [23]. A detailed

description of the three schemes can be found in the original works.[2] Here, we want to highlight that, though the key schedule processes 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.

1) *Parvin's Cryptosystem:* The key schedule operation of the cipher proposed in [19] is based on two chaotic functions and the encryption process is composed by a row/column circular permutation and a sequential pixel diffusion.
   a) *Initialization:* Generate three key streams $\boldsymbol{U} = [u(1), \ldots, u(H)]$, $\boldsymbol{V} = [v(1), \ldots, v(W)]$, and $\boldsymbol{K} = [k(0), k(1), \ldots, k(L)]$ from $KSA(Seed)$, where $\boldsymbol{U}$, $\boldsymbol{V}$, and $\boldsymbol{K}$ are composed of random integers in interval $[1, W]$, $[1, H]$, and $[0, 255]$, respectively.
   b) *Permutations:* Carry out row circular permutation to the plain-image $\boldsymbol{P}$ using
   $$p'(i, (j + u(i)) \bmod W) = p(i, j) \tag{6}$$
   and denote the result by $\boldsymbol{P}'$. Then permute $\boldsymbol{P}'$ further using the circular column permutation as follows:
   $$s((i + v(j)) \bmod H, j) = p'(i, j). \tag{7}$$
   c) *Diffusion:* Stretch $\boldsymbol{S}$ to a vector $[s(1), s(2), \ldots, s(L)]$ and calculate the pixel values of the cipher-image by the following diffusion equation:
   $$c(l) = s(l) \oplus (c(l-1) \dot{+} k(l)) \oplus k(l) \tag{8}$$
   where $l \in [1, 2, \ldots, L]$ and $c(0) = k(0)$. Rearrange the vector $[c(l)]$ to a matrix of size $H \times W$ to get the cipher-image $\boldsymbol{C}$.
2) *Norouzi's Cryptosystem:* The key schedule suggested in [22] is based on the hyper-chaotic system introduced in [58]. The encryption process is composed by a single diffusion process, which can be viewed as the generalized version of the previous diffusion scheme.
   a) *Initialization:* Produce a key stream $\boldsymbol{K} = [k(0), k(1), \ldots, k(L)]$ by running $KSA(Seed)$, where $k(l)$ is 8-bit integer in $[0, 255]$.
   b) *Diffusion:* Calculate the pixel values of the cipher-image sequentially by the following bidirectional diffusion equation:
   $$c(l) = p(l) \oplus (c(l-1) \dot{+} k(l)) \oplus f(\boldsymbol{P}, k(l)) \tag{9}$$
   where $l \in [1, 2, \ldots, L]$, $c(0) = k(0)$, and
   $$f(\boldsymbol{P}, k(l)) = \left\lfloor \left(\sum_{i=l+1}^{L} p(i) \right) \cdot k(l) \cdot 10^8 / 256^4 \right\rfloor \bmod 256. \tag{10}$$
   Rearrange $[c(l)]$ to a matrix of size $H \times W$ and denote it as $\boldsymbol{C}$.
3) *Yang's Cryptosystem:* The key schedule of the image cryptosystem proposed in [23] is derived from the 1-D two-particle discrete-time quantum random walks, which is totally different from those suggested in [19] and [22]. However, the encryption process, which is composed of a diffusion stage and a permutation stage, is an extension of Norouzi's work [22].
   a) *Initialization:* Obtain the key streams $\boldsymbol{K} = [k(0), k(1), \ldots, k(L)]$, $\boldsymbol{U} = [u(1), \ldots, u(W)]$, and $\boldsymbol{V} = [v(1), \ldots, v(H)]$ by running the key schedule $KSA(Seed)$, where $\boldsymbol{K}$ is composed of 8-bit integers in the interval $[0, 255]$ and $\boldsymbol{U}$ and $\boldsymbol{V}$ are permutation of the set $\{1, 2, \ldots, W\}$ and $\{1, 2, \ldots, H\}$, respectively.
   b) *Diffusion:* Run the bidirectional diffusion technique characterized by (9) to the plain-image pixels as follows:
   $$p'(l) = p(l) \oplus (p'(l-1) \dot{+} k(l)) \oplus f(P, k(l)) \tag{11}$$
   where $l \in [1, 2, \ldots, L]$, $p'(0) = k(0)$ and $f(\boldsymbol{P}, k(l))$ is defined by (10). Rearrange the obtained vector $[p'(l)]$ to a matrix of size $H \times W$ and denote it as $\boldsymbol{P}'$.
   c) *Permutations*: Permute the intermediate result $\boldsymbol{P}'$ using the key streams $\boldsymbol{U}$ and $\boldsymbol{V}$ and get the cipher-image $\boldsymbol{C}$, that is
   $$s(i, u(j)) = p'(i, j) \tag{12}$$
   $$c(v(i), j) = s(i, j) \tag{13}$$
   where $i \in [1, H]$ and $j \in [1, W]$.

IV. 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 [19], [22], and [23], which will be considered in Section VI only, along with the security of the whole cryptosystems. Mathematically, we assume that all elements of the key streams $\boldsymbol{U}$ and $\boldsymbol{V}$ used for permutation in Parvin's cryptosystem are zeros, and that $\boldsymbol{U}$ and $\boldsymbol{V}$ 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 image ciphers can be found in [38].

In the diffusion mechanism proposed by Parvin we will show that the problem of finding the key stream $\boldsymbol{K}$ used in the diffusion scheme with a KP attack is equivalent to solving the DEA $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$, where α, β, y are known parameters and k is unknown. Note that the same DEA, under the assumption that α and β can be freely chosen, has already been analyzed by other works, that are also briefly reviewed. We will also show that the problem of retrieving the key stream for

[2]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.

diffusion in Norouzi and Yang's design under CP attack scenario is equivalent to solving 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.

A. Parvin's Diffusion Scheme

In Parvin's scheme, we assume that two plain-images, $\boldsymbol{P}_1$ and $\boldsymbol{P}_2$, and their corresponding cipher-images, $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$, are available. Referring to (8), we have the relation

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

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

$$\begin{aligned} &(c_1(l-1) \dot{+} k(l)) \oplus (c_2(l-1) \dot{+} k(l)) \\ &\quad = c_1(l) \oplus c_2(l) \oplus p_1(l) \oplus p_2(l). \end{aligned} \tag{14}$$

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

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

In the present context, the problem of finding (part of) the key stream, i.e., $\{k(l)\}_{l=1}^{L}$, of Parvin's cryptosystem is turned into solving (3) under some pairs of known parameters (α, β, y). Note that $k(0)$, and so the full strem $\boldsymbol{K}$, can be easily calculated according to (8) after $\{k(l)\}_{l=1}^{L}$ are revealed.

It is already known that, under the assumption that α and β can be chosen freely, k can be determined by only two groups of chosen queries by referring to the following.

Theorem 1 [55, Proposition 3 and Corollary 3.1]: Suppose $\alpha, \beta, k, y \in \mathbb{Z}_2^n$, and $n > 2$, two groups of chosen queries (α, β) 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 [54] and [55], and an interpretation from the computational point of view about this theorem can be found in [35]. 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 (α, β). This is intrinsic in the fact that the carry bit generated by the highest bit plane is discarded after the modulo operation [35]. 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 (3).

Note however that, by referring to (14), neither a KP nor a CP attack scenario allows us to choose the value of α and β since they represent ciphertext elements. In order to get a result similar to that of Theorem 1 that can be applied to the considered cryptosystems, we systematically analyze (3) in Section V-A under the assumption that α and β are known to the attacker but cannot be freely chosen.

B. Norouzi and Yang's Diffusion Scheme

In Norouzi and Yang's cryptosystems, the diffusion stage is characterized by (9), 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 $\boldsymbol{P}_1$, whose corresponding vector format is $[p_1(l), \ldots, p_1(L)]$, we define the real number sequence $\boldsymbol{T}_1 = [t_1(l), \ldots, t_1(L)]$ as

$$t_1(l) = \sum_{i=l+1}^{L} p_1(i)/256^4. \tag{15}$$

Then, the diffusion scheme characterized by (9) can be written as

$$c_1(l) = p_1(l) \oplus (c_1(l-1) \dot{+} k(l)) \oplus g(t_1(l), k(l)) \tag{16}$$

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 $\boldsymbol{P}_2$, which differs from $\boldsymbol{P}_1$ by a single pixel at location l_0. In this way the real number sequence $\boldsymbol{T}_2 = [t_2(l), \ldots, t_2(L)]$ associated to $\boldsymbol{P}_2$ satisfies

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

Referring to (16), it is easy to observe that the difference between $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ at location l_0 will satisfy the relation

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

which coincides exactly with (3). 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 (3) with some pairs of known parameters (α, β, y).

Conversely, under the assumption of a KP attack scenario, we can observe from (15) that the calculation of the real number sequence $\boldsymbol{T}$ is independent of the secret key (stream). Then, limiting ourselves to consider the plain image $\boldsymbol{P}_1$, we can recast (16) as

$$(\alpha \dot{+} k) \oplus g(\beta, k) = y \tag{17}$$

where $g(\beta, k) = \lfloor \beta \cdot (10^8 \cdot k) \rfloor \bmod 256$ is a nonlinear function. The problem of determining k for (17) from some groups of known (α, β, y) is considered in Section V-B. Here, special attention should be paid to the fact that β is no longer 8-bit integer but a non-negative real number.

V. Main Results

A. Cryptographic Strength of the Equation $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$

According to Section IV-A, both KP and CP attacks to Parvins diffusion scheme are equivalent to solving (3) under the assumption that the values of α, β, and y are known but none of them can be chosen. In the ideal case, the data complexity to determine k should be 2^{2n} because there are 2^{2n}

possible combinations of α and β 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 (α, β, 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 lth 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 (3). 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 $\mathbb{G}$. It is concluded that its computational complexity is $O(2^{n-1} \cdot g)$ steps and two shortcomings can be identified: 1) there is no hint on how to choose the correct k from $\mathbb{K}_g$ if $\#\mathbb{K}_g \geq 2$ and 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 work pretty well. However, in the schemes proposed in [56] and [57], 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 α, β, and y, the i LSBs $(0 \leq i < n-1)$ of k of the following equation:

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

can be solely determined if $y = \sum_{j=0}^{i-1} 2^j = \overbrace{(0 \ldots 0 \underbrace{1 \cdots 11}_{i})_2}^{\text{MSB} \leftarrow \text{LSB}}$.

Proof: The proof of this theorem can be found in the Appendix. ∎

For a given known parameter triple (α, β, y), Theorem 2 states that some LSBs 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 (3) can be solved using only a single query (α, β) 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 more detail, with the two chosen queries used in Theorem 1, it can be observed that $\hat{y}_i \| \bar{y}_i = 1$ holds for all $i = 0 \sim n-1$. So, one can compute that

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

And with the similar underlying rules, we can also indicate other two groups of queries satisfying the requirements of Theorem 1, specifically, they could be $(\tilde{\alpha}, \tilde{\beta}) = (\sum_{j=0}^{\lceil n/2 \rceil - 1} (10)_2 \cdot 4^j, \sum_{j=0}^{\lceil n/2 \rceil - 1} (00)_2 \cdot 4^j)$, and $(\breve{\alpha}, \breve{\beta}) = (\sum_{j=0}^{\lceil n/2 \rceil - 1} (00)_2 \cdot 4^j, \sum_{j=0}^{\lceil n/2 \rceil - 1} (01)_2 \cdot 4^j)$.

As mentioned before, none of the value of α, β, y can be chosen under KP attack for all our interested diffusion mechanisms [see (14) for example]. So even when g groups of known triples (α, β, y) are collected by the adversary, the probability[3] that he can observe i consecutive ones in y is only $(g/2^i)$. The larger i is, the smaller the probability will be. In other words, if applying Theorem 2 directly to the set $\mathbb{G}$, the significant bits of k are undetermined with large probability. When using the estimated value of k for the attack of the whole encryption schemes (see Section VI for detail), the more significant bit planes, which carry more visual information than LSBs by the nature of digital images, of the recovered image tend to be wrong.

Conversely, the probability that there exists certain $y \in \mathbb{G}$ whose ith bit $(0 \leq i < n-1)$ is nonzero is very high. For example, the probability that there exists at least a y such that its LSB (i.e., $i = 0$) is nonzero is $(1 - (1/2)^g)$. From Theorem 2, the LSB of k can be determined with this concrete known triple (α, β, y) whose $y_0 = 1$. Once k_0 is determined, we can discard the LSB of (3) and formulate a new version of it with only $(n-1)$ bits[4] and repeat the similar process to determine k_1. And so on and so forth, the value of k can be finally recovered. Let $\tilde{y} = y \oplus \alpha \oplus \beta$ and denote c_i the carry bit at the ith bit plane of $(\alpha \dot{+} k)$, the following steps characterize the above idea and determine the bits of k sequentially from the known parameters set $\mathbb{G}$.

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

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

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 ith bit k_i by look up Table I if $\#\mathbb{G}_i \neq 0$ and then compute c_{i+1} for the parameter in $\mathbb{G}_{i+1}$ using (20).

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 $k = \sum_{i=0}^{n-1} k_i \cdot 2^i$.

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[5] $\mathbb{K}_g$. Without loss of generality, assume

[3] We implicitly assume y follows the uniform distribution.

[4] Note that carry bit of the new equation [with bit length $(n-1)$] should be updated correspondingly.

[5] In fact, every element in $\mathbb{K}_g$ contains the same number of correct bits of k in average.

TABLE I
VALUES OF k_i CORRESPONDING TO THE VALUES OF α_i, β_i, c_i, y_i, AND $\tilde{y}_{i+1}$

$(y_i, \tilde{y}_{i+1})$	(α_i, β_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

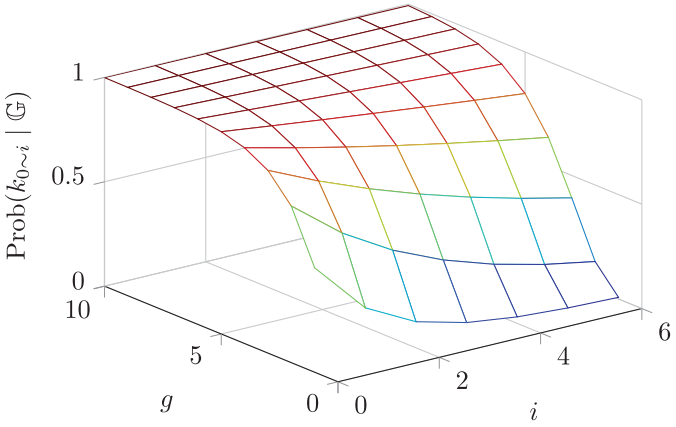


Fig. 2. Probability that the first i LSBs of k can be confirmed with respect to different g.

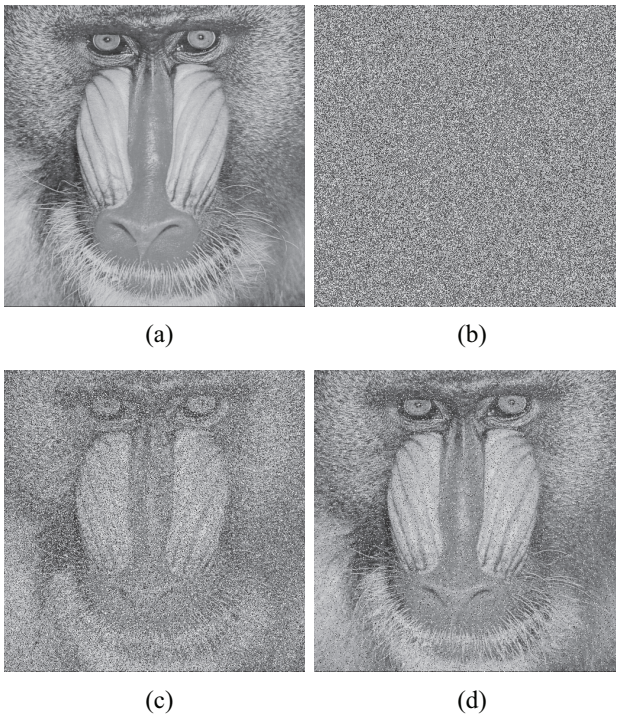


Fig. 3. Numerical tests on simplified Parvin's cryptosystem. (a) Plain-image "Baboon" of size 512×512. (b) Encryption result of (a) using the modified Parvin's cryptosystem. (c) Recovery result using two pairs of known plain-images and their corresponding cipher-images. (d) Recovery result using four pairs of known plain-images and their corresponding cipher-images.

that all the known parameters α, β, 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 $\text{Prob}(k_{0\sim i} \mid \mathbb{G})$, is given as

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

Assuming $n = 8$ as in the three image cryptosystems studied in Section III, 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 stream $\boldsymbol{K}$ is generated using the key schedule described in [19, Sec. 2] while we artificially set $\boldsymbol{U}$ and $\boldsymbol{V}$ to zeros to fit our model proposed in Section IV-A. Then, we use two and four known plain-images and their corresponding cipher-images, i.e., $g = 1$ and $g = 3$, to recover the key stream $\boldsymbol{K}$ using the algorithm described above. The recovered key stream is used to decrypt the cipher-image of "Baboon," as shown in Fig. 3(b), and the deciphered results are shown, respectively, in Fig. 3(c) and (d).

B. Cryptographic Strength of the Equation $(\alpha \dot{+} k) \oplus g(\beta, k) = y$

According to the results obtained in the previous section, the diffusion mechanism characterized by (3) 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 schemes introduced in [22] and [23], and defined by (9) and (10), are 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 Section IV, the bidirectional diffusion scheme is immediately proven to be weak, since (9) can be converted to the form of (3). 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 [22] 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 [22] is the same as above. Let us consider the equation

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

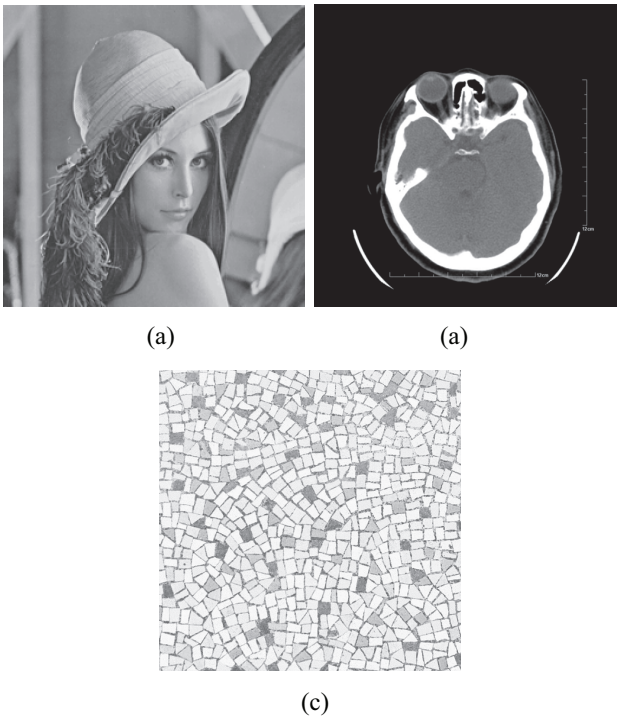


Fig. 4. Three test images for recovering the equivalent key stream of Norouzi's cryptosystem. (a) *Lena*. (b) CT image. (c) Mosaic image.

where $g(\beta, k) = \lfloor \beta \cdot (10^8 \cdot k) \rfloor \bmod 256$, $\alpha, y, k \in [0, 255]$ and β is a non-negative real number. Under the assumptions of a KP attack, i.e., that α, β, 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 (3) with respect to KP attack.

We start the analysis from the trivial case $\beta \equiv 0$. Under this assumption, (17) is simplified to

$$y = \alpha \dot{+} k \tag{18}$$

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 α, β 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 lth element of $\mathbb{G}$ and exhaustively test all the 2^8 possible values of k to check whether it satisfies (17). 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 $\mathbb{K}_{l+1} = \mathbb{K}_{l+1} \cap \mathbb{K}_l$.

TABLE II
AVERAGE RECOVERY RATE USING DIFFERENT NUMBERS OF KNOWN PLAIN-IMAGES

Number of known plain-images	average *recovery rate*
1	66.6637%
2	99.8247%
3	100%

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 512×512 known plain-images with different statistical characteristics are employed as our test images [Fig. 4(a)–(c)]. These images are encrypted using Norouzi's cryptosystem under the secret key that was adopted in [22, Sec. 3]. Using the techniques illustrated in Section IV, we cast the relationship between the plaintext pixels and ciphertext pixels to the form of (17). Then, we, respectively, use 1, 2, and 3 pairs of plain-images and their corresponding cipher-images to retrieve the equivalent secret key stream $\boldsymbol{K}$ by the above algorithm. The average *recovery rates* of the proposed KP attack using different numbers of known plain-images are listed in Table II. Here, the *recovery rate* is defined as

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

It can be observed that the average *recovery rate* raises as the number of known plain-images increases. 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. 5(a)–(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 (16), where the error of a wrongly decrypted pixel will spread to all successive decryption operations in a pseudo-random manner.

VI. CRYPTOGRAPHIC APPLICATIONS

Exploiting the security analyses of (3) and (17) shown above, this section presents chosen plaintext attacks to the full cryptosystems proposed in [19], [22], and [23] and briefly discusses other security implications related to our analyses.

A. Cryptanalysis of Parvin's Cryptosystem

As described in Section III, Parvin's cryptosystem is composed of circular permutations and a single diffusion stage. To apply our analysis result presented in Section V-A, we need first to recover the equivalent key streams used for

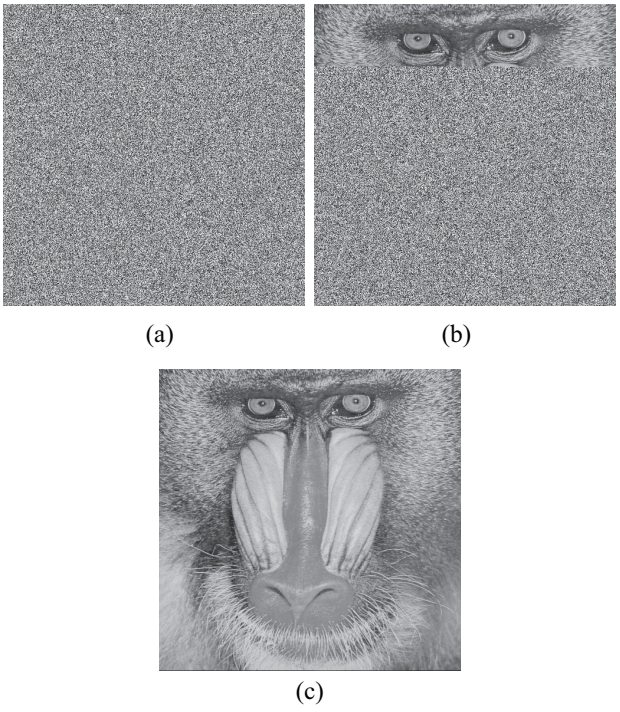


Fig. 5. Recovery results. Deciphered result using the key stream retrieved from (a) Fig. 4(a), (b) Fig. 4(a) and (b), and (c) Fig. 4(a)–(c).

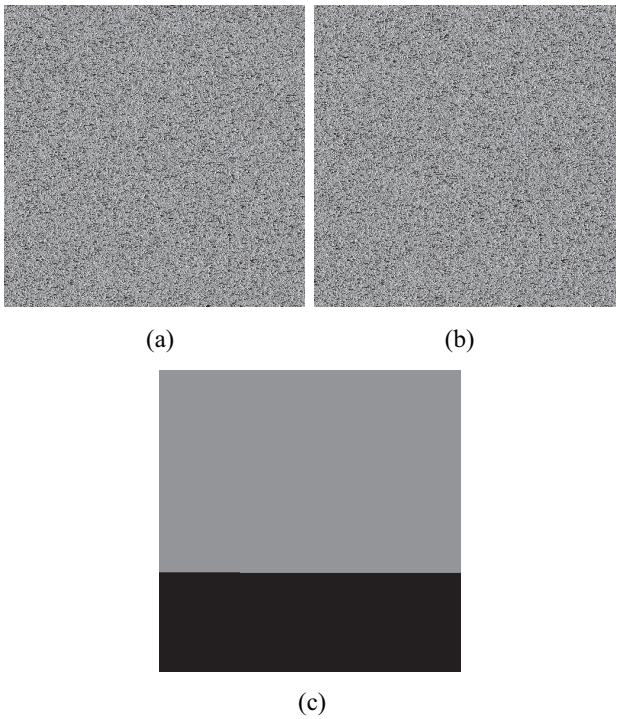


Fig. 6. Example test for recovering the equivalent permutation key streams of Parvin's cryptosystem. (a) Cipher-image of $\boldsymbol{P}_1$. (b) Cipher-image of $\boldsymbol{P}_2$. (c) Difference between (a) and (b) using XOR operation.

row and column circular permutation. The underlying strategy is to study the relationship between cipher-images produced by 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 [21], [35]. Here, we suppose that an image having fixed gray value is available and denote it as $\boldsymbol{P}_1 = \boldsymbol{0} = [p_1(i,j) \equiv 0]_{H,W}$. Then, we set $p_1(1,1) = 128$ and keep all the other pixels unchanged and denote the modified image by $\boldsymbol{P}_2 = [p_2(i,j)]_{H,W}$. Fig. 6(a) and (b) depict the cipher-images corresponding to $\boldsymbol{P}_1$ and $\boldsymbol{P}_2$, respectively. Here, $H = W = 512$ is chosen. The difference of the two cipher-images is shown in Fig. 6(c). Find the first pixel whose value is 128 and denote its position by (i_1, j_1). Referring to (6)–(8), it can be concluded that $u(1) = ((j_1 - 1) \bmod H) + 1$ and $v(1) = ((i_1 - 1) \bmod W) + 1$. Repeating this test for all the diagonal pixels of $\boldsymbol{P}_1$, $\boldsymbol{U}$, and $\boldsymbol{V}$, the key streams for row and column permutations, can be retrieved completely. Combining with the analysis presented in Section V-A, the data complexity of the CP attack is $O(1) + \max(H, W)$ with an overwhelming probability.

B. Cryptanalysis of Norouzi and Yang's Cryptosystems

Applying the analysis presented in Section V-B, it is readily to conclude that Norouzi 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 $\boldsymbol{P}_1$, $\boldsymbol{P}_2$, and $\boldsymbol{P}_3$ whose 1D formats have the form $[0, 0, 0, \ldots, 0, 0, 0, 1]$, $[0, 0, 0, \ldots, 0, 0, 1, 0]$ and $[0, 0, 0, \ldots, 0, 1, 0, 0]$. According to (11)–(13), their corresponding cipher-images $\boldsymbol{C}_1$, $\boldsymbol{C}_2$, and $\boldsymbol{C}_3$ satisfy the following two conditions: 1) there are two distinct ciphertext elements between $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ and 2) there are three distinct ciphertext elements between $\boldsymbol{C}_3$ and $\boldsymbol{C}_1$ (or $\boldsymbol{C}_2$). Comparing $\boldsymbol{C}_1$, $\boldsymbol{C}_2$, and $\boldsymbol{C}_3$, the location of $c_1(H, W-2)$ can be identified. Fig. 7 sketches the rules involved in this procedure. Repeating this test to the last row and column of $\boldsymbol{P}_1$, the equivalent permutation key streams $\boldsymbol{U}$ and $\boldsymbol{V}$ can be fully recovered at the data complexity[6] $O(H+W)$ 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 and Yang's cryptosystems is to group several pixels as a single element to enlarge the real key space. For example, combining 15 pixels together will make the key space grows to 2^{120} and frustrate the KP attack presented in Section V-B. However, Norouzi 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.

[6]The permutation for the last two pixels can be retrieved by brute force search.

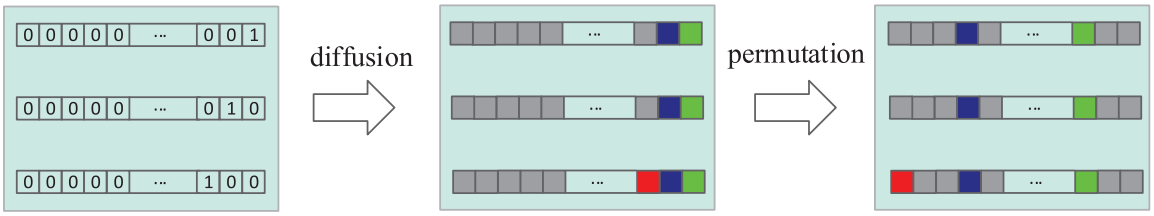


Fig. 7. Illustration of the CP attack on Yang's cryptosystem to recover the equivalent secret key used for permutation.

TABLE III
VALUES OF $\tilde{y}_{i+1}$ CORRESPONDING TO THE VALUES OF α_i, β_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)

Regarding the widely usage of the diffusion equation (8), 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 crytosystems, 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 (5).

VII. CONCLUSION

Considering the three cryptosystems proposed in [19], [22], and [23] as case studies, we have studied the security properties of equations: 1) $(\alpha \dot{+} k) \oplus (\beta \dot{+} k) = y$ and 2) $(\alpha \dot{+} k) \oplus g(\beta, k) = y$. The underlying theory of the key scheduling process employed in these example cryptosystems ranges 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 1) under the KP attack scenario. The relationship of our result and the existing ones under CP attack assumption [21], [54], [55] is also investigated. The algorithms provided and the extensive numerical experiments confirm that both equations 1) and 2) 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. This paper can be extended to investigate diffusion equations which involve more complex cryptographic primitives, such as modulo multiplication [35].

APPENDIX
PROOF OF THEOREM 2

Let us consider the equivalent form of (3), that is

$$\tilde{y} = (\alpha \dot{+} k) \oplus (\beta \dot{+} k) \oplus \alpha \oplus \beta. \tag{19}$$

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

$$\begin{cases} \tilde{y}_{i+1} = c_{i+1} \oplus \tilde{c}_{i+1} \\ c_{i+1} = k_i\alpha_i \oplus k_i c_i \oplus \alpha_i c_i \\ \tilde{c}_{i+1} = k_i\beta_i \oplus k_i\tilde{c}_i \oplus \beta_i\tilde{c}_i \end{cases} \tag{20}$$

where c_i is the carry bit at the ith bit plane of $(\alpha \dot{+} k)$ and $\tilde{c}_i = \tilde{y}_i \oplus c_i$. Table III lists the values of $\tilde{y}_{i+1}$ that computed from (20) under all the possible values of α_i, β_i, $\tilde{y}_i$, k_i, and c_i.

Table III indicates that k_i can be determined if $(\alpha_i, \beta_i, \tilde{y}_i)$ falls in {Col(2), Col(3), Col(5), 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 $(0 \le i \le n-2)$. 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 the fact

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

Hence, the theorem is proved for the case $i = 0$. Assume that it is valid for $i = m$ $(m \le n-3)$, i.e., all the m LSBs of k are confirmed when $y = \sum_{j=0}^{m-1} 2^m$ and thus all the c_i and $\tilde{c}_i$ can

be derived by (20) 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 (19) and (20). When computing y_{m+2} by (20), we have

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

Observing that α_{m+1}, β_{m+1}, and $\tilde{y}_{m+2}$ are known parameters in our KP attack scenario, and c_{m+1} and $\tilde{c}_{m+1}$ are the results 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 and E. B. Barker, *NIST Special Publication 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2012.

[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Heidelberg, Germany: Springer, 2002.

[3] F. Liu and H. Koenig, "A survey of video encryption algorithms," *Comput. Security*, vol. 29, no. 1, pp. 3–15, 2010.

[4] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol. 48, no. 8, pp. 2439–2451, Aug. 2000.

[5] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 2, pp. 214–223, Feb. 2007.

[6] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital image and video," in *Multimedia Encryption and Authentication Techniques and Applications*. Boca Raton, FL, USA: Auerbach, 2006, pp. 129–164.

[7] H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," *J. Cryptol.*, vol. 9, no. 1, pp. 1–19, 1996.

[8] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[9] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[10] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[11] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Phys. Lett. A*, vol. 372, no. 15, pp. 2645–2652, 2008.

[12] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, 2011.

[13] W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," *Commun. Nonlin. Sci. Numer. Simulat.*, vol. 18, no. 3, pp. 584–600, 2013.

[14] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-gray code for image systems," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 515–529, Apr. 2013.

[15] M. Zanin and A. N. Pisarchik, "Gray code permutation algorithm for high-dimensional data encryption," *Inf. Sci.*, vol. 270, pp. 288–297, Jun. 2014.

[16] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, 2012.

[17] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011.

[18] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[19] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools Appl.*, vol. 75, no. 17, pp. 10631–10648, 2016.

[20] H. Zhu, C. Zhao, X. Zhang, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," *Optik Int. J. Light Electron Opt.*, vol. 125, no. 22, pp. 6672–6677, 2014.

[21] X. Wang, D. Luan, and X. Bao, "Cryptanalysis of an image encryption algorithm using Chebyshev generator," *Digit. Signal Process.*, vol. 25, pp. 244–247, Feb. 2014.

[22] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools Appl.*, vol. 71, no. 3, pp. 1469–1497, 2014.

[23] Y.-G. Yang, Q.-X. Pan, S.-J. Sun, and P. Xu, "Novel image encryption based on quantum walks," *Sci. Rep.*, vol. 5, no. 7, 2015, Art. no. 7784.

[24] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[25] H. Chen, X. Du, Z. Liu, and C. Yang, "Color image encryption based on the affine transform and gyrator transform," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 768–775, 2013.

[26] Z. Liu, Y. Zhang, H. Zhao, M. A. Ahmad, and S. Liu, "Optical multi-image encryption based on frequency shift," *Optik Int. J. Light Electron Opt.*, vol. 122, no. 11, pp. 1010–1013, 2011.

[27] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, 2014.

[28] B. Javidi *et al.*, "Roadmap on optical security," *J. Opt.*, vol. 18, no. 8, pp. 1–39, 2016.

[29] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.*, vol. 31, no. 8, pp. 1044–1046, 2006.

[30] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.*, vol. 30, no. 13, pp. 1644–1646, 2005.

[31] Z. Liu, C. Shen, J. Tan, and S. Liu, "A recovery method of double random phase encoding system with a parallel phase retrieval," *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–7, Feb. 2016.

[32] W. Li, Y. Yan, and N. Yu, "Breaking row-column shuffle based image cipher," in *Proc. 20th ACM Int. Conf. Multimedia*, Nara, Japan, 2012, pp. 1097–1100.

[33] Y. Wu *et al.*, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

[34] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," *AMC Trans. Math. Softw.*, vol. 33, no. 4, pp. 22–40, 2007.

[35] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, and K.-W. Wong, "Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure," *Nonlin. Dyn.*, vol. 84, no. 4, pp. 2241–2250, 2016.

[36] E. Solak, C. Çokal, O. T. Yildiz, and T. Biyikoğlu, "Cryptanalysis of Fridrich's chaotic image encryption," *Int. J. Bifurcation Chaos*, vol. 20, no. 5, pp. 1405–1413, 2010.

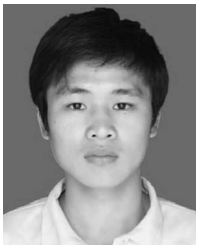
[37] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, and G. Chen, "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure," *J. Syst. Softw.*, vol. 85, no. 9, pp. 2077–2085, 2012.

[38] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Process. Image Commun.*, vol. 23, no. 3, pp. 212–223, 2008.

[39] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 235–246, Feb. 2016.

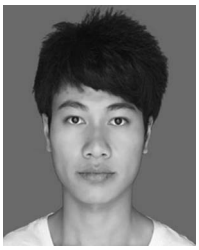
[40] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold cat map for $N = p^e$," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 445–452, Jan. 2012.

[41] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of the generalized discrete Arnold cat map for $N = 2^e$," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 3249–3255, May 2013.
[42] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold cat map," *Theor. Comput. Sci.*, vol. 552, pp. 13–25, Oct. 2014.
[43] N. Ferguson *et al.*, "Helix: Fast encryption and authentication in a single cryptographic primitive," in *Fast Software Encryption*. Heidelberg, Germany: Springer, 2003, pp. 330–346.
[44] N. Ferguson *et al. The Skein Hash Function Family, Submission to NIST (Round 3)*. Accessed on Apr. 7, 2016. [Online]. Available: http://www.skein-hash.info/sites/default/files/skein1.3.pdf
[45] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Advances in Cryptology-EUROCRYPT'91*. Heidelberg, Germany: Springer, 1991, pp. 17–38.
[46] J. Wallén, "On the differential and linear properties of addition," Lab. Theor. Comput. Sci., Helsinki Univ. Technol., Espoo, Finland, Tech. Rep. A84, 2003.
[47] O. Staffelbach and W. Meier, "Cryptographic significance of the carry for ciphers based on integer addition," in *Advances in Cryptology-CRYPTO'90*. Heidelberg, Germany: Springer, 1990, pp. 602–614.
[48] K. A. McKay and P. L. Vora, "Pseudo-linear approximations for ARX ciphers: With application to threefish," in *Proc. 2nd SHA-3 Candidate Conf.*, Santa Barbara, CA, USA, 2010, p. 282.
[49] S. Paul and B. Preneel, "Solving systems of differential equations of addition," in *Proc. 10th Aust. Conf. Inf. Security Privacy*, Brisbane, QLD, Australia, 2005, pp. 75–88.
[50] S. Paul and B. Preneel, "Near optimal algorithms for solving differential equations of addition with batch queries," in *Progress in Cryptology-INDOCRYPT'05*. Heidelberg, Germany: Springer, 2005, pp. 90–103.
[51] S. Paul, "Cryptanalysis of stream ciphers based on arrays and modular addition," *IACR Cryptol. ePrint Archive*, vol. 2007, p. 54, Feb. 2007.
[52] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108–3114, Jun. 2012.
[53] Z. Ni *et al.*, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 4, pp. 497–509, Apr. 2008.
[54] C. Li, M. Z. Q. Chen, and K.-T. Lo, "Breaking an image encryption algorithm based on chaos," *Int. J. Bifurcation Chaos*, vol. 21, no. 7, pp. 2067–2076, 2011.
[55] C. Li, Y. Liu, L. Y. Zhang, and M. Z. Q. Chen, "Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation," *Int. J. Bifurcation Chaos*, vol. 23, no. 4, pp. 1–12, 2013.
[56] C. Gangadhar and K. D. Rao, "Hyperchaos based image encryption," *Int. J. Bifurcation Chaos*, vol. 19, no. 11, pp. 3833–3839, 2010.
[57] K. D. D. Rao and C. Gangadhar, "Modified chaotic key-based algorithm for image encryption and its VLSI realization," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Cardiff, U.K., 2007, pp. 439–442.
[58] N. Yujun, W. Xingyuan, W. Mingjun, and Z. Huaguang, "A new hyperchaotic system and its circuit implementation," *Commun. Nonlin. Sci. Numer. Simulat.*, vol. 15, no. 11, pp. 3518–3524, 2010.



Leo Yu Zhang (S'14–M'17) received the bachelor's and master's degrees in computational mathematics from Xiangtan University, Xiangtan, China, in 2009 and 2012, respectively, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2016.

He is a Post-Doctoral Fellow for a joint program initiated with the Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY, USA, the Department of Computer Science, City University of Hong Kong, and the College of Information Science and Technology, Jinan University, Guangzhou, China. He held various research positions with the City University of Hong Kong, the University of Macau, Macau, China, the University of Ferrara, Ferrara, Italy, and the University of Bologna, Bologna, Italy. His current research interests include cloud security, multimedia security, and compressed sensing.



Yuansheng Liu received the bachelor's and master's degrees in computer science from Xiangtan University, Xiangtan, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with the University of Technology Sydney, Ultimo, NSW, Australia.

In 2015, he was a Research Assistant with the Department of Electronic Engineering, City University of Hong Kong, Hong Kong, for one month and as a Research Assistant with the Dalian University of Technology, for five months. His current research interest include signal processing techniques for bioinformatics and multimedia security.

Fabio Pareschi (S'05–M'08) received the Dr.Eng. (Hons.) degree in electronic engineering from the University of Ferrara, Ferrara, Italy, in 2001, and the Ph.D. degree in information technology under the European Doctorate Project from the University of Bologna, Bologna, Italy, in 2007.

He is currently an Assistant Professor with the Department of Engineering, University of Ferrara. He is also a Faculty Member with the ARCES, University of Bologna. His current research interests include analog and mixed-mode electronic circuit design, statistical signal processing, random number generation and testing, and electromagnetic compatibility.

Dr. Pareschi was a recipient of the Best Paper Award at ECCTD 2005 and the Best Student Paper Award at EMC Zurich 2005. He served as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART II from 2010 to 2013.

Yushu Zhang received the B.S. degree from the Department of Mathematics, North University of China, Taiyuan, China, in 2010, and the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014.

Since 2015, he has been an Associate Professor with the School of Electronics and Information Engineering, Southwest University, Chongqing. He held various research positions with the City University of Hong Kong, Hong Kong, and the University of Macau, Macau, China. His current research interests include multimedia coding and security, multimedia cloud security, and compressive sensing security.

Kwok-Wo Wong (S'93–M'95–SM'03) was born in 1968. He received the B.Sc. degree in electronic engineering from the Chinese University of Hong Kong, Hong Kong, in 1990, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 1994.

Since 1994, he was a Faculty Member with the City University of Hong Kong until his death. He has published over 100 papers in 25 international mathematics, physics, and engineering journals in the fields of nonlinear dynamics, cryptography, neural networks, and optics.

Dr. Wong was a Chartered Engineer and a member of the Institution of Engineering and Technology.

Riccardo Rovatti (M'99–SM'02–F'12) received the M.S. degree in electronic engineering and the Ph.D. degree in electronics, computer science, and telecommunications from the University of Bologna, Bologna, Italy, in 1992 and 1996, respectively.

He is currently a Full Professor of Electronics with the University of Bologna. He has authored approximately 300 technical contributions to international conferences and journals, and of two volumes. His current research interests include mathematical and applicative aspects of statistical signal processing and on the application of statistics to nonlinear dynamical systems.

Dr. Rovatti was a recipient of the 2004 IEEE CAS Society Darlington Award, the 2013 IEEE CAS Society Guillemin-Cauer Award, the Best Paper Award at ECCTD 2005, and the Best Student Paper Award at EMC Zurich 2005 and ISCAS 2011.

Gianluca Setti (S'89–M'91–SM'02–F'06) received the Ph.D. degree in electronic engineering and computer science from the University of Bologna, Bologna, Italy, in 1997.

Since 1997, he has been with the School of Engineering, University of Ferrara, Ferrara, Italy, where he is currently a Professor of Circuit Theory and Analog Electronics and is also a permanent Faculty Member of ARCES, University of Bologna. His current research interests include nonlinear circuits, implementation and application of chaotic circuits and systems, electromagnetic compatibility, statistical signal processing, and biomedical circuits and systems.

Dr. Setti was a recipient of the 2013 IEEE CAS Society Meritorious Service Award and a co-recipient of the 2004 IEEE CAS Society Darlington Award, the 2013 IEEE CAS Society Guillemin-Cauer Award, the Best Paper Award at ECCTD 2005, and the Best Student Paper Award at EMC Zurich 2005 and at ISCAS 2011. He held several editorial positions and served, in particular, as the Editor-in-Chief for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART II from 2006 to 2007 and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART I from 2008 to 2009. He was the Technical Program Co-Chair at ISCAS 2007, ISCAS 2008, ICECS 2012, and BioCAS 2013, and the General Co-Chair of NOLTA 2006. He was a member of the Board of Governors of the IEEE CAS Society from 2005 to 2008, served as its 2010 President. He is a Distinguished Lecturer of CASS from 2015 to 2016. He held several other volunteer positions for the IEEE and from 2013 to 2014, he was the first non North-American Vice President of the IEEE for Publication Services and Products.