Period Distribution of Generalized Discrete Arnold Cat Map for $N = p^e$

Fei Chen, Kwok-Wo Wong, Xiaofeng Liao, and Tao Xiang

***Abstract*—In this paper, we analyze the period distribution of the generalized discrete cat map over the Galois ring $(Z_{p^e}, +, \times)$ where $p > 3$ is a prime. The sequences generated by this map are modeled as 2-dimensional *LFSR* sequences. Employing the generation function and the Hensel lifting approaches, full knowledge of the detail period distribution is obtained analytically. Our results not only characterize the period distribution of the cat map, which gives insights to various applications, but also demonstrate some approaches to deal with the period of a polynomial in the Galois ring.**

***Index Terms*—Dynamical system, Galois ring, generalized cat map, Hensel lift, *LFSR*, period distribution.**

I. Introduction

In RECENT years, there are considerable attempts to study the behavior of general dynamical systems such as chaotic systems or maps. Chaotic systems are ergodic in the whole phase space, mixing, and sensitive to initial conditions. These properties are analogue to the confusion and diffusion nature required in cryptosystems and have attracted research interest to apply chaotic systems in various cryptographic applications such as encryption [1]–[8] and watermarking [9]. Among these applications, the Arnold cat map is often employed as a major building block [3], [5], [9].

The original Arnold cat map [10] is a chaotic map with the form

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \bmod 1 \qquad (1)$$

where $x(n), y(n) \in [0, 1]$. To make it appropriate for digital applications, the following discretized and generalized form is often employed [3]:

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \bmod N \qquad (2)$$

where $a, b, x(n), y(n) \in Z_N$. When this map is used for watermarking or image encryption, $[x(0), y(0)]^{\mathbf{T}}$ usually denotes the initial position of a pixel in an image while $[x(n), y(n)]^{\mathbf{T}}$ denotes the position of the pixel after the n-th iteration of the map. In private-key and public-key cryptosystems, partial or the whole $[x(0), y(0)]^{\mathbf{T}}$ and n play the role of the secret key.

The discretization of the continuous cat map leads to the consequence that the cat map must have a period T, i.e., $[x(n + T), y(n + T)]^{\mathbf{T}} = [x(n), y(n)]^{\mathbf{T}}$, which has a great impact on practical applications. Although different applications have their own requirements on the period, a long period is often required for cryptographic purpose. If the period is not sufficiently long, the algorithms presented in [7]–[9] are vulnerable to attacks. Therefore, the full knowledge of the detail period distribution of the cat map is useful in system design and analysis. This knowledge also contributes to chaos theory in understanding the unstable rational periodic orbits of (1). The reason is that if a rational point $[\frac{x_0}{N}, \frac{y_0}{N}]^{\mathbf{T}}$ is a periodic point of (1), then $[x_0, y_0]^{\mathbf{T}}$ is also a periodic point of (2) and vice versa.

The sequence generated by (2) is essentially a 2-dimensional linear feedback shift register (*LFSR*) sequence which is the foundation of many traditional stream ciphers [11]–[15]. The property of the sequence varies substantially as N changes because $(Z_N, +, \times)$ is a Galois field when N is a prime, a Galois ring when N is a power of a prime and just a commutative ring when N is a common composite. Employing the LFSR model, Chen *et al.* analyzed the period distribution of the cat map (2) when $(Z_N, +, \times)$ forms a Galois field, i.e., N is a prime, and full knowledge on the period distribution was obtained [16]. Here, we further investigate the period distribution for the case $N = p^e$ where $p > 3$ is a prime, i.e., to make exact statistics about the period of the cat map when a and b traverse all elements in Z_{p^e}. However, the structure of $(Z_{p^e}, +, \times)$, which is a Galois ring, is more complicated than that of a Galois field. Our contributions are described as follows. The full results for the period distribution are obtained by combining the generation function and the Hensel lifting approaches. These results not only characterize the period distribution of the cat map but also demonstrate some methods to deal with the period of polynomials in $Z_{p^e}[t]$, the latter is also an interesting problem in the analysis of sequences and cyclic codes over Galois rings [17]–[21].

Manuscript received August 07, 2010; revised July 1, 2011; accepted July 26, 2011. Date of current version January 06, 2012. This work was supported in part by the Research Grants Council of the Hong Kong Special Administrative Region, China under Grant Project CityU 123009; in part by the Fundamental Research Funds for the Central Universities (No. CDJXS10182215); in part by the National Natural Science Foundation of China (No. 60973114, 60703035); in part by the Natural Science Foundation Project of CQ CSTC (No. 2009BA2024, 2008BB2193), and State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University (No. 2007DA10512709207); in part by the Natural Science Foundation Project of CQ CSTC (No. 2008BB2193); in part by the Fundamental Research Funds for the Central Universities (No. CDJZR10180020); and in part by the Post-doctoral Science Foundation of China (No.20100470817).

F. Chen, X. Liao, and T. Xiang are with the College of Computer Science, Chongqing University, Chongqing, 400044, China (e-mail: chenfeiorange@163.com; xfliao@cqu.edu.cn; txiang@cqu.edu.cn).

K.-W. Wong is with the Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong (e-mail: itkwwong@cityu.edu.hk).

Communicated by M. G. Parker, Associate Editor for Sequences.

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/TIT.2011.2171534

This paper is organized as follows. Section II introduces the concept of period distribution and the basic idea to address this problem. Sections III and IV present the detail analysis of period distribution of the cat map in two cases. The full results on period distribution are presented in Table II at the end of Section IV, followed by some implications of our results. Finally, a conclusion is drawn in Section V.

II. Problem Definition and Basic Idea

This section introduces some concepts and notations employed in our analysis. For the knowledge of basic number theory and abstract algebra, please refer to [22]–[24]. Let the cat map be

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \bmod p^e \quad (3)$$

where $x(n), y(n) \in [0, p^e - 1]$ and $a, b \in Z_{p^e}$. Let $\mathbf{A} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix}$.

Firstly, the period distribution problem is stated. Let $\mathbf{x}(0) = [x(0), y(0)]^{\mathbf{T}}$ be an initial point of the cat map (3) and $\mathbf{x}(n) = [x(n), y(n)]^{\mathbf{T}}$ be the point after n iterations of the cat map from $\mathbf{x}(0)$. If there exists an integer T such that $\mathbf{x}(T) = \mathbf{x}(0)$ for all initial points in $Z_{p^e}^2$, T is called the period of the cat map. Since $\det(\mathbf{A}) = 1$, the period must exist. The period distribution analysis is defined as finding all possible periods of the cat map (3) and then counting the number of cat maps possessing a specific period when a and b traverse all possible values in Z_{p^e}. Throughout this paper, p is a prime larger than 3 and e is an integer, $e \geq 2$. The reason for $p > 3$ is stated in Section IV. The period distribution when $N = 2^e$ and $N = 3^e$ need special analysis.

Secondly, the approach adopted is described. Generally, the sequence generated by (3) is considered as a LFSR sequence and the algebraic theory handling with recurrent equations is employed to characterize the period distribution. Here $(Z_{p^e}, +, \times)$ forms a Galois ring where addition and multiplication are all modular operations. Let (a, b) and $[a, b]$ denote the greatest common divisor and the least common multiple of a and b, respectively. $a \,|\, b$ means that a is a divisor of b. $\varphi(n)$, i.e., Euler's totient function, denotes the number of positive integers which are both less than or equal to the positive integer n and coprime with n. Suppose that $f(t)$ is a polynomial in $Z_{p^e}[t]$ and $f(0)$ is a unit in $(Z_{p^e}, +, \times)$, the period of $f(t)$, denoted as $\mathrm{per}(f)$, is defined as the smallest integer such that $f(t) \,|\, x^{\mathrm{per}(f)} - 1$ where all the arithmetical operations are in $Z_{p^e}[t]$.

Let $x(n)_{n\geq 0}, y(n)_{n\geq 0}$ be the sequences generated by (3) and $X(t)$ and $Y(t)$ be their generation functions, respectively. Then it holds that $X(t) = \sum_{n=0}^{\infty} x(n)t^n = x_0 + tX(t) + atY(t)$ and $Y(t) = y_0 + btX(t) + (ab+1)tY(t)$ which result in

$$X(t) = \frac{g_x(t)}{f(t)} \quad (4)$$

and

$$Y(t) = \frac{g_y(t)}{f(t)} \quad (5)$$

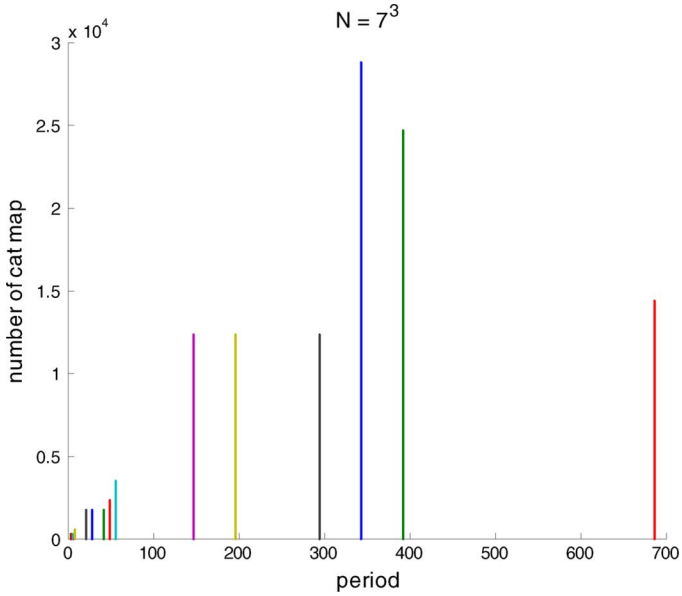

Fig. 1. Period distribution when $N = 7^3$.

where

$$f(t) = t^2 - (ab+2)t + 1, \quad (6)$$

$g_x(t) = (y_0 a - x_0(ab+1))t + x_0$ and $g_y(t) = (x_0 b - y_0)t + y_0$. It is easy to verify that the period of the cat map is the least common multiple of $X(t)$ and $Y(t)$ for all initial points and it must be a divisor of $\mathrm{per}(f)$. For a special initial point $\mathbf{x}(0) = [x(0), y(0)]^{\mathbf{T}}$, if $g_x(t)$ or $g_y(t)$ is coprime with $f(t)$, the period of this point is $\mathrm{per}(f)$ [23]. Observing that if a is coprime with p, the point $[1, a^{-1}(ab+1)]^{\mathbf{T}}$ is special since $g_x(t) = 1$ which is coprime with $f(t)$ and the period of this point is $\mathrm{per}(f)$. If b is coprime with p, the point $[b^{-1}, 1]^{\mathbf{T}}$ is also special since $g_y(t) = 1$ which is also coprime with $f(t)$ and the period of this point is $\mathrm{per}(f)$. However, when a and b both have a common factor with p, i.e., a and b are both divisible by p, such a point cannot be found.

It can be concluded that if a and$b$ are not both divisible by p, the period of the cat map must be $\mathrm{per}(f)$. Otherwise, it only holds that the period must be a divisor of $\mathrm{per}(f)$. The two situations are totally different and need to be analysed separately. Therefore, it is natural to divide the analysis into these two cases. The analysis in each case is composed of two steps. First is the period analysis step which finds all possible periods of the cat map. It is followed by the counting step which counts the number of cat maps having a specific period.

It would be better if we have an impression on what the period distribution looks like. Fig. 1 is a plot of the period distribution when $N = 7^3$. It shows that the periods distribute very sparsely, some periods exist but some do not. There are also many small periods in this example. It is worthy noting that small periods are not desirable in security applications but they may be needed in other applications. In the following sections, the period distribution rules will be worked out analytically.

III. Period Distribution if a and b Are Not Both Divisible by p

Let $f(t) = t^2 - (ab+2)t + 1$ and the period of the cat map be T. In this case, $T = \mathrm{per}(f)$ and $(Z_{p^e}, +, \times)$ forms a Galois ring with a unique maximal ideal (p). There are some zero divisors in this ring which make the analysis more complicated than that in the Galois field.

The analysis goes into two ways: (i) $f(t) = t^2 - (ab+2)t + 1$ can be factorized in $Z_{p^e}[t]$, and (ii) $f(t)$ cannot be factorized in $Z_{p^e}[t]$ but can be factorized in its extension ring $Z_{p^e}[t]/(f(t))$. In either case, $f(t)$ can be written as $f(t) = (t-\alpha)(t-\alpha^{-1})$. When N is a prime, $(Z_N, +, \times)$ forms a Galois field and $\mathrm{per}(f) = \mathrm{ord}(\alpha)$ if $(t-\alpha)$ and $(t-\alpha^{-1})$ are coprime, i.e., $\alpha \neq \alpha^{-1}$. This also means $(t-\alpha)(t-\alpha^{-1}) \,|\, t^{\mathrm{ord}(\alpha)} - 1$ and $\mathrm{ord}(\alpha)$ is the smallest positive integer for such relationship to hold. However, when $N = p^e$, this is not always the case for the Galois ring $(Z_{p^e}, +, \times)$ because there are some zero divisors in it. This point is illustrated as follows.

Suppose $\alpha \neq \alpha^{-1}$. Notice that $\mathrm{ord}(\alpha) = \mathrm{ord}(\alpha^{-1})$, then we have

$$t - \alpha \,|\, t^{\mathrm{ord}(\alpha)} - 1 \tag{7}$$

and

$$t - \alpha^{-1} \,|\, t^{\mathrm{ord}(\alpha)} - 1. \tag{8}$$

The expression (7) implies $t^{\mathrm{ord}(\alpha)} - 1 = (t-\alpha)g(t)$ for some $g(t) \in Z_N[t]$. It is easy to observe that α^{-1} is also a root of $t^{\mathrm{ord}(\alpha)} - 1$. Therefore,

$$(\alpha^{-1} - \alpha)g(\alpha^{-1}) = 0 \tag{9}$$

in Z_N. If $g(\alpha^{-1}) = 0$, which means $g(t) = (t-\alpha^{-1})h(t)$ for some $h(t) \in Z_N[t]$, then it leads to

$$(t-\alpha)(t-\alpha^{-1}) \mid t^{\mathrm{ord}(\alpha)} - 1 \tag{10}$$

and $\mathrm{per}(f) = \mathrm{ord}(\alpha)$. This is always true in a Galois field since $\alpha^{-1} - \alpha$ must be a unit and there is only one zero divisor which is the trivial zero element in the Galois field, i.e., N is a prime. However, if $g(\alpha^{-1}) \neq 0$, it holds that $(t-\alpha)(t-\alpha^{-1}) \nmid t^{\mathrm{ord}(\alpha)} - 1$ and $\mathrm{per}(f) > \mathrm{ord}(\alpha)$ in a general ring with composite N. It occurs in $Z_{p^e}[t]$ when $\alpha^{-1} - \alpha$ is a zero divisor, i.e., $p \,|\, \alpha^{-1} - \alpha$ in Z_{p^e}. To have a more detailed illustration, let $\alpha = 1 + p^{e-1}$ and so $\alpha^{-1} = 1 + (p-1)p^{e-1}$ in Z_{p^e}. It is easy to verify that $\mathrm{ord}(\alpha) = p$ and $t^p - 1 = (t-\alpha)g(t)$ where $g(t) = t^{p-1} + \alpha t^{p-2} + \cdots + \alpha^{p-2}t + \alpha^{p-1}$. It holds that $\alpha^{-1} - \alpha = (p-2)p^{e-1}$ and $g(\alpha^{-1}) \neq 0$ in Z_{p^e} but $p \,|\, g(\alpha^{-1})$, thus (9) also holds. Now it is clear that (7) and (8) are both valid but (10) does not hold. As a result, $\mathrm{per}(f) > \mathrm{ord}(\alpha)$. Notice that α and α^{-1} are expressed in p-adic representation which is common in the study of the Galois ring and is useful in our analysis, as shown later.

Now we face a problem that (10) cannot be used directly as in the Galois field. Thus an in-depth investigation is needed. From the discussion above, if $\alpha^{-1} - \alpha$ is not a zero divisor, i.e., $p \nmid \alpha^{-1} - \alpha$ or $\alpha^{-1} - \alpha$ is an unit, then (10) still holds. This leaves the case when $\alpha^{-1} - \alpha$ is a zero divisor which we will discuss separately. Therefore the period distribution of the cat map is analyzed in the following three cases. The first case is that $f(t)$ is reducible in $Z_{p^e}[t]$ with its roots satisfying $p \nmid \alpha^{-1} - \alpha$. The second is that $f(t)$ is irreducible in $Z_{p^e}[t]$ but can be factorized in its extension ring $Z_{p^e}[t]/(f(t))$ with its roots satisfying $p \nmid \alpha^{-1} - \alpha$. The third case is $\alpha^{-1} - \alpha$ being a zero divisor.

A. Case 1: $f(t)$ Is Reducible in $Z_{p^e}[t]$ and $p \nmid \alpha^{-1} - \alpha$

Denote the multiplicative group of the Galois ring $(Z_{p^e}, +, \times)$ as $Z_{p^e}^{\times}$. Its structure is first reviewed. By number theory [22], $Z_{p^e}^{\times}$ is a cyclic group with generator g and $\mathrm{ord}(g) = p^e - p^{e-1}$. Suppose $\alpha \in Z_{p^e}$, then it can be represented in the p-adic form as $\alpha = \sum_{i=0}^{e-1} a_i p^i$ where $a_i \in Z_p$ which is a Galois field. If $a_0 = 0$, α is a zero divisor in Z_{p^e}. Otherwise, α is a unit in Z_{p^e}. Although the structure of $Z_{p^e}^{\times}$ is quite simple, it is interesting and useful to consider the order of $\alpha = \sum_{i=0}^{e-1} a_i p^i$ with $a_0 \neq 0$. Suppose the order of a_0 in Z_p is $\mathrm{ord}(a_0)$. Then $\alpha^{\mathrm{ord}(a_0)} = (\sum_{i=0}^{e-1} a_i p^i)^{\mathrm{ord}(a_0)} = 1 + \sum_{i=1}^{e-1} a_i' p^i$ in Z_{p^e}. Take power p at both sides repeatedly gives $\alpha^{p^t \mathrm{ord}(a_0)} = 1$ for some t in Z_{p^e}. In this case, $f(t)$ can be factorized as $f(t) = (t-\alpha)(t-\alpha^{-1})$ where $\alpha \in Z_{p^e}^{\times}$. Then it holds that

$$ab + 2 = \alpha + \alpha^{-1}. \tag{11}$$

Let

$$\alpha = \sum_{i=0}^{e-1} a_i p^i \tag{12}$$

and

$$\alpha^{-1} = \sum_{i=0}^{e-1} b_i p^i \tag{13}$$

where $a_0, b_0 \in Z_p^{\times}, a_i, b_i \in Z_p$ for $1 \leq i \leq e-1$. Then $\alpha^{-1} - \alpha = \sum_{i=0}^{e-1} (b_i - a_i) p^i$ and $p \nmid \alpha^{-1} - \alpha$ means $a_0 \neq b_0$. As $\alpha\alpha^{-1} = 1$ in Z_{p^e}, $a_0 b_0 = 1$ in Z_p. If $a_0 = b_0$, it must hold that $a_0 = b_0 = 1$ or $a_0 = b_0 = p-1$ because $(Z_p, +, \times)$ is a Galois field and its multiplicative group is a cyclic group. Thus if $a_0 \neq 1, p-1$, then $p \nmid \alpha^{-1} - \alpha$ must hold. Now we are ready to present our results on the period distribution of the cat map for this case.

Proposition 1: Suppose $f(t)$ can be factorized in $Z_{p^e}[t]$ as $f(t) = (t-\alpha)(t-\alpha^{-1})$ where $\alpha \in Z_{p^e}^{\times}$. Let α, α^{-1} be the expressions given by (12) and (13), respectively, with $a_0 \neq 1, p-1$. $\mathrm{per}(f)$ traverses the set $\{k : k = k_1 k_2, k_1 > 2, k_1 | p-1, k_2 | p^{e-1}\}$. For each k, there are $\frac{\varphi(k)}{2}(p^e - 1)$ cat maps of period k.

Proof: Period analysis.

$f(t) = (t-\alpha)(t-\alpha^{-1})$. $\alpha\alpha^{-1} = 1$ gives $a_0 b_0 = 1 \bmod p$. Since $a_0 \neq 1, p-1$, $\alpha^{-1} - \alpha = \sum_{i=0}^{e-1} (b_i - a_i) p^i$ must be a unit as $b_0 - a_0 \neq 0$ in Z_p. Thus (7), (8) and (10) all hold and $f(t) \,|\, t^{\mathrm{ord}(\alpha)} - 1$. By the property of the order, i.e., $\mathrm{ord}(\alpha)$ is the smallest positive integer such that $t - \alpha \,|\, t^{\mathrm{ord}(\alpha)} - 1$, it holds that $\mathrm{per}(f) = \mathrm{ord}(\alpha)$.

Let α traverses all elements in $Z_{p^e}^{\times}$ with $a_0 \neq 1, p-1$. Considering that $Z_{p^e}^{\times}$ is a cyclic group, then $\mathrm{ord}(\alpha)$ traverses the set $\{k : k = k_1 k_2, k_1 > 2, k_1 | p-1, k_2 | p^{e-1}\}$, so does $\mathrm{per}(f)$.

Counting.

From (11), $ab = \alpha + \alpha^{-1} - 2$ in Z_{p^e}, i.e., $ab \equiv \alpha + \alpha^{-1} - 2 \bmod p^e$. Notice $a, b \in Z_{p^e}$.

First, we check whether ab is uniquely determined by α's. If there are two $\alpha, \beta \in Z_{p^e}^{\times}$ such that $\alpha + \alpha^{-1} - 2 = \beta + \beta^{-1} - 2$, simplifying this expression gives

$$(\alpha - \beta)(\alpha\beta - 1) = 0. \tag{14}$$

Let $\alpha = \sum_{i=0}^{e-1} a_i p^i$ and $\beta = \sum_{i=0}^{e-1} b_i p^i$ where $a_0, b_0 \neq 1, p-1$ as assumed in this proposition. Obviously, $\alpha = \beta$ and $\alpha\beta = 1$ are two solutions for (14). If there are some more solutions, we must have $p \,|\, \alpha - \beta$ and $p \,|\, \alpha\beta - 1$. The former means $a_0 = b_0$ and the latter implies $a_0 b_0 = 1$ in Z_p. This leads to $a_0 = b_0 = 1$ or $a_0 = b_0 = p - 1$ which contradicts with the assumption of this proposition. As a result, there are only two solutions for (14). Since $Z_{p^e}^{\times}$ is a cyclic group, there are $\varphi(k)$ elements in $Z_{p^e}^{\times}$ whose order is k. Combining the discussions on the solutions of (14), there are $\frac{\varphi(k)}{2}$ different values for $\alpha + \alpha^{-1} - 2$ with $\mathrm{ord}(\alpha) = k$.

Now we check whether $\alpha + \alpha^{-1} - 2$ is a unit or a zero divisor which will affect the choices of a and b. Let $\alpha + \alpha^{-1} - 2 = \sum_{i=0}^{e-1} c_i p^i$. It is obvious that $c_0 = a_0 + b_0 - 2 = a_0 + a_0^{-1} - 2 \bmod p$. From $a_0 \neq 1, p-1$, $c_0 \neq 0 \bmod p$, $\alpha + \alpha^{-1} - 2$ is a unit, so is ab. This is the criterion for choosing a and b.

The choices for a are $p^e - p^{e-1}$. Once a is chosen, b is uniquely determined by $b = (a)^{-1}(\alpha + \alpha^{-1} - 2) \bmod p^e$. Thus, for each k, there are $\frac{\varphi(k)}{2}(p^e - p^{e-1})$ cat maps of period k. ∎

Remark 2: From the above discussion, it is clear that $p \nmid \alpha^{-1} - \alpha$ means $a_0 \neq 1, p-1$ when $f(t)$ is reducible in $Z_{p^e}[t]$. In other words, when $f(t)$ is considered as a polynomial in $Z_p[t]$, $f(t) = t^2 - (\alpha + \alpha^{-1})t + 1 \neq t^2 - 2t + 1$ corresponding to $a_0 \neq 1$ and $f(t) \neq t^2 + 2t + 1$ implies $a_0 \neq p - 1$. This is very important when we discuss the period distribution in the special case of $p \mid \alpha^{-1} - \alpha$.

B. Case 2: $f(t)$ Is Irreducible in $Z_{p^e}[t]$ and $p \nmid \alpha^{-1} - \alpha$

Although $f(t)$ is irreducible in $Z_{p^e}[t]$, it can be factorized in its extension ring $Z_{p^e}[t]/(f(t))$. Indeed, it can be expressed as $f(t) = (t - \alpha)(t - \alpha^{-1})$ where $\alpha, \alpha^{-1} \in Z_{p^e}[t]/(f(t))$ and $\alpha, \alpha^{-1} \notin Z_{p^e}$. The following equality thus holds:

$$ab + 2 = \alpha + \alpha^{-1}. \tag{15}$$

Firstly, we will review the structure of $Z_{p^e}[t]/(f(t))$. In general, $f(t)$ is irreducible in $Z_p[t]$ if it is a basic irreducible polynomial in $Z_{p^e}[t]$. Let the degree of $f(t)$ be m. Then $Z_{p^e}[t]/(f(t))$, denoted as $GR(p^e, m)$, is a Galois ring with the unique maximal ideal $pGR(p^e, m)$ composed of all zero divisors in $GR(p^e, m)$. Please refer to [21] and [24] for more about the Galois ring. There is an element ξ in its multiplicative group with $\mathrm{ord}(\xi) = p^m - 1$. It generates a cyclic group with order $p^m - 1$. Let $X = \{0, 1, \xi, \cdots, \xi^{p^m - 2}\}$. Then $\forall r \in GR(p^e, m)$, r can be expressed as

$$r = \sum_{i=0}^{e-1} a_i p^i \tag{16}$$

where $a_i \in X$ for $0 \leq i \leq e - 1$. This can be considered as a generalized p-adic representation of an element in the Galois ring. r is a unit if and only if $a_0 \neq 0$. Thus there are $p^{me} - p^{m(e-1)}$ units in $GR(p^e, m)$ and $p^{m(e-1)}$ zero divisors. The multiplicative group of $GR(p^e, m)$ can be represented as

$$GR^{\times}(p^e, m) = (\xi) \times \varepsilon \tag{17}$$

where (ξ) is the cyclic group generated by ξ and $\varepsilon = \{1 + a_1 p + \cdots + a_{e-1} p^{e-1}\}$ with $a_i \in X$ for $1 \leq i \leq e - 1$. It should be noticed that the order of any element in (ξ) is a divisor of $p^m - 1$ while the order of any element in ε is a divisor of p^{e-1}. It is easy to verify that all elements in Z_{p^e} can also be found in $GR(p^e, m)$ with the same order as in Z_{p^e}.

A further investigation in $Z_{p^e}[t]/(f(t))$ reveals what exactly ξ looks like. It is easy to check that $f(t)$ splits in $Z_{p^e}[t]/(f(t))$. This is because $f(t)$ splits in the Galois field $Z_p[t]/(f(t))$ and the result in this field can be lifted into $Z_{p^e}[t]/(f(t))$ using Hensel lifting [21] and [24]. Let η be a root of $f(t)$ in $Z_{p^e}[t]/(f(t))$. Then $Z_{p^e}[t]/(f(t))$ can be expressed as

$$\{a_0 + a_1\eta + \cdots + a_{m-1}\eta^{m-1}, a_i \in Z_{p^e}, 0 \leq i \leq m - 1\}. \tag{18}$$

Note that a_i can also be expressed in its p-adic form as

$$a_i = \sum_{j=0}^{e-1} a_{ij} p^j \tag{19}$$

where $a_{ij} \in Z_p$. Combining (16), (18) and (19), we have

$$r = \sum_{i=0}^{e-1} \left(\sum_{j=0}^{m-1} a_{ij} \eta^j \right) p^i \tag{20}$$

$\forall r \in GR(p^e, m)$ and $a_{ij} \in Z_p$. However, (20) does not mean all elements in (ξ) are of the form $\sum_{j=0}^{m-1} a_{ij}\eta^j$. This representation helps a lot in our analysis.

The unique maximal idea in $GR(p^e, m)$ is $pGR(p^e, m)$ which implies that $GR(p^e, m)/pGR(p^e, m)$ is a Galois field. Denote the natural homomorphism between $GR(p^e, m)$ and $GR(p^e, m)/pGR(p^e, m)$ as ψ. Then $\forall r \in GR(p^e, m)$, $r = \sum_{i=0}^{e-1} (\sum_{j=0}^{m-1} a_{ij}\eta^j) p^i$ and

$$\psi(r) = \sum_{j=0}^{m-1} a_{0j}\eta^j + pGR(p^e, m) \tag{21}$$

in the Galois field $GR(p^e, m)/pGR(p^e, m)$ which is isomorphic to $GF(p^m)$.

It is important to make clear what $p \nmid \alpha^{-1} - \alpha$ means in this case when $f(t)$ is irreducible in $Z_{p^e}[t]$. The degree of $f(t)$ is 2 since $f(t) = (t - \alpha)(t - \alpha^{-1})$. If $p \,|\, \alpha^{-1} - \alpha$, making use of the natural homomorphism ψ between $GR(p^e, 2)$ and $GR(p^e, 2)/pGR(p^e, 2)$, it holds that $\psi(\alpha^{-1} - \alpha) = \psi(\alpha^{-1}) - \psi(\alpha) = \psi(\alpha)^{-1} - \psi(\alpha) = 0$. Thus $\psi(\alpha)^{-1} = \psi(\alpha)$ in the Galois field $GR(p^e, 2)/pGR(p^e, 2)$. Since this Galois field is isomorphic with $GF(p^2)$, it must hold that $\psi(\alpha) = 1 + pGR(p^e, m)$ or $\psi(\alpha) = p - 1 + pGR(p^e, m)$. Thus either $\alpha = 1 + px_1$, $\alpha^{-1} = 1 + py_1$ for some $x_1, y_1 \in GR(p^e, 2)$ or $\alpha = p-1+px_2$, $\alpha^{-1} = p-1+py_2$ for some $x_2, y_2 \in GR(p^e, 2)$ should hold. Then $f(t) = t^2 - 2t + 1$ or $f(t) = t^2 + 2t + 1$ in Z_p. This is the same as Remark 2.

Now all preparation work has been done, it is time to present our results on the period distribution of the cat map over Z_{p^e} for this case. Our analysis is basically the same as that performed in Section III-A, except that the technique used here is more advanced.

Proposition 3: Suppose $f(t)$ can be factorized in $Z_{p^e}[t]/(f(t))$ as $f(t) = (t-\alpha)(t-\alpha^{-1}), \alpha \notin Z_{p^e}$ and $p \nmid \alpha^{-1} - \alpha$. $\mathrm{per}(f)$ transverses the set $\{k : k = k_1 k_2, k_1 > 2, k_1 | p+1, k_2 | p^{e-1}\}$. For each k, there are $\frac{\varphi(k)}{2}(p^e - p^{e-1})$ cat maps of period k.

Proof: Period analysis.

As $p \nmid \alpha^{-1} - \alpha$ and $f(t) = (t-\alpha)(t-\alpha^{-1})$, $\alpha^{-1} - \alpha$ must be a unit in $GR(p^e, m)$. Thus (7), (8) and (10) all hold. Then $f(t) \,|\, t^{\mathrm{ord}(\alpha)} - 1$ and $\mathrm{per}(f) = \mathrm{ord}(\alpha)$.

By (17), α can also be expressed as $\alpha = xy$ where $x \in (\xi)$ and $y \in \varepsilon$. Let $\mathrm{ord}(x) = k_1$ and $\mathrm{ord}(y) = k_2$, it is easy to verify that $k_1 | p^2 - 1, k_2 | p^{e-1}$ and $\mathrm{ord}(\alpha) = k_1 k_2$. Notice that $\alpha, \alpha^{-1} \in Z_{p^e}[t]/(f(t))$ and $\alpha, \alpha^{-1} \notin Z_{p^e}$. $Z_{p^e} \subseteq Z_{p^e}[t]/(f(t))$ implies that all units in Z_{p^e} are contained in $Z_{p^e}[t]/(f(t))$ which means $k_1 \nmid p-1$. Now let α traverse the units in $Z_{p^e}[t]/(f(t))$ such that $k_1 \nmid p-1$, then $\mathrm{ord}(\alpha)$ traverses the set $\{k : k = k_1 k_2, k_1 > 2, k_1 | p+1, k_2 | p^{e-1}\}$, so does $\mathrm{per}(f)$.

Counting.

From (15), $ab = \alpha + \alpha^{-1} - 2$ in Z_{p^e}, i.e., $ab \equiv \alpha + \alpha^{-1} - 2 \mathrm{mod} p^e$ with $a, b \in Z_{p^e}$.

First, we check whether ab is uniquely determined by α's. If there are two $\alpha, \beta \in Z_{p^e}^{\times}$ such that $\alpha + \alpha^{-1} - 2 = \beta + \beta^{-1} - 2$, then simplifying this expression leads to

$$(\alpha - \beta)(\alpha\beta - 1) = 0. \tag{22}$$

Obviously, $\alpha = \beta$ and $\alpha\beta = 1$ are two solutions of (22). If there are more solutions, it must hold that $p \mid \alpha - \beta$ and $p \mid \alpha\beta - 1$. Let $\alpha = \sum_{i=0}^{e-1}(\sum_{j=0}^{m-1} a_{ij}\eta^j)p^i$ and $\beta = \sum_{i=0}^{e-1}(\sum_{j=0}^{m-1} b_{ij}\eta^j)p^i$ where $a_{ij}, b_{ij} \in Z_p$. Then $p \,|\, \alpha - \beta$ means $\sum_{j=0}^{m-1} a_{0j}\eta^j = \sum_{j=0}^{m-1} b_{0j}\eta^j$ which gives $\psi(\alpha) = \psi(\beta)$. Moreover, $p \,|\, \alpha\beta - 1$ means $\psi(\alpha\beta - 1) = \psi(\alpha)\psi(\beta) - 1 = \psi(\alpha)^2 - 1 = 0$. Thus $\psi(\alpha) = 1$ or $\psi(\alpha) = p-1$, which implies that either $\alpha = 1 + px_1$, $\alpha^{-1} = 1 + py_1$ for some $x_1, y_1 \in GR(p^e, 2)$ or $\alpha = p-1+px_2, \alpha^{-1} = p-1+py_2$ for some $x_2, y_2 \in GR(p^e, 2)$ holds. This contradicts with the assumption $p \nmid \alpha^{-1} - \alpha$. Thus $\alpha = \beta$ and $\alpha\beta = 1$ are the only two solutions of (22) if $f(t)$ is irreducible in $Z_{p^e}[t]$ and $p \nmid \alpha^{-1} - \alpha$, as assumed in this proposition. This result identifies the number of distinct values for $\alpha + \alpha^{-1} - 2$ when α traverse the units in $Z_{p^e}[t]/(f(t))$ such that $k_1 \nmid p-1$. From the Frobenius map [25] of the Galois ring, it can be easily deduced that there are $\frac{\varphi(k)}{2}$ elements whose order is k and $\alpha + \alpha^{-1} \in Z_{p^e}$.

Now we check whether $\alpha + \alpha^{-1} - 2$ is a unit or a zero divisor which will affect the selection of a and b. It holds that $\psi(\alpha + \alpha^{-1} - 2) = \psi(\alpha)^{-1}[\psi(\alpha) - 1]^2 \neq 0$ in $GR(p^e, 2)/pGR(p^e, 2)$ since $\psi(\alpha) \neq 1$. Then $\alpha + \alpha^{-1} - 2$ must be a unit in Z_{p^e}, so is ab. This is the criterion for choosing a and b.

The number of choices for a is $p^e - p^{e-1}$. Once a is fixed, b is determined by $b = (a)^{-1}(\alpha + \alpha^{-1} - 2) \mathrm{mod} p^e$. Thus for each k, there are $\frac{\varphi(k)}{2}(p^e - p^{e-1})$ cat maps of this period. ■

Remark 4: From the discussion for the case that $f(t)$ is irreducible in $Z_{p^e}[t]$, we know that $p \nmid \alpha^{-1} - \alpha$ also means $f(t) \neq t^2 - 2t + 1$ and $f(t) \neq t^2 + 2t + 1$ when $f(t)$ is considered as a polynomial in $Z_p[t]$.

C. $\alpha^{-1} - \alpha$ Is a Zero Divisor

As we mentioned in Remarks 2 and 4, the case of $\alpha^{-1} - \alpha$ being a zero divisor means that $f(t) = t^2 - 2t + 1$ or $f(t) = t^2 + 2t + 1$ when $f(t)$ is considered as a polynomial in $Z_p[t]$. First be sure that $f(t) = t^2 - (ab+2)t + 1$ in $Z_{p^e}[t]$ and it can be reducible or irreducible. The Hensel lifting approach gives some useful results but does not provide the whole period distribution. Here we still adopt the approach used in the previous analyses, i.e., analyze the period of the roots of $f(t)$, and, at the same time, combine the Hensel lifting approach as a subsidiary tool. Let T and T' be the period of $f(t)$ in $Z_{p^e}[t]$ and $Z_p[t]$, respectively. Our results are presented as follows.

1) $f(t) = t^2 - 2t + 1$ in $Z_p[t]$: In this case, $ab + 2 \equiv 2 \mathrm{mod} p$ and $p \,|\, ab$. If $f(t)$ can be factorized in $Z_{p^e}[t]$, α and α^{-1} must be in Z_{p^e}. Otherwise, it must split in its extension ring $Z_{p^e}[t]/(f(t))$ denoted as R. Now α and α^{-1} are in R. It should be noticed that this ring is not a Galois ring. Its structure is described as follows. The zero divisors form a maximal ideal generated by p and $t-1$ which is $(p, t-1)$ denote as I. The quotient ring R/I is a Galois field. Similar to the p-adic representation in Galois ring, we can also express the elements of R/I in the form of p and $t-1$ which can be considered as a generalization to the traditional p-adic representation. This form helps in computing the order in its multiplicative group and plays an important role in our analysis.

Proposition 5: If $f(t) = t^2 - 2t + 1$ in $Z_p[t]$, $\mathrm{per}(f) = p^e$ and there are $2p^{2e-2}(p-1)$ cat maps having this period.

Proof: Period analysis.

We have $f(t) = t^2 - (ab+2)t + 1 = (t-\alpha)(t-\alpha^{-1})$. When it is considered as a polynomial over $Z_p[t]$, $f(t) = t^2 - 2t + 1$. By finite field theory [23], it is easy to verify $\mathrm{per}(f) = p$. Using the Hensel lifting method [21] and [24], it holds that $T = T'p^k$ where $0 \leq k \leq e-1$. Therefore the period of $f(t)$ must be in the form of $T = p^k$ where $1 \leq k \leq e$. Actually, T has the maximal value $T = p^e$. This can be shown in two cases: α is in Z_{p^e}, and α is in $Z_{p^e}[t]/(f(t))$.

Case 1: α is in Z_{p^e}

Let $\alpha = 1 + \sum_{j=1}^{e-1} a_j p^j$ where $a_j \in Z_p$. Suppose $\alpha \neq 1$ and $i \in [1, e-1]$ is the smallest integer such that $a_i \neq 0$, then it is easy to check $\mathrm{ord}(\alpha) = p^{e-i}$ just by taking the powers to p at each side for $e - i$ times. $f(t) \,|\, t^T - 1$ gives $t - \alpha \,|\, t^T - 1$ and thus $\mathrm{ord}(\alpha) \,|\, T$. Let $T = \mathrm{ord}(\alpha)p^l$ where $0 \leq l \leq i$. Then it holds that

$$\begin{aligned} t^T - 1 &= t^{\mathrm{ord}(\alpha)p^l} - 1 \\ &= t^{\mathrm{ord}(\alpha)p^l} - \alpha^{\mathrm{ord}(\alpha)p^l} \\ &= (t-\alpha)g(t) \end{aligned}$$

where $g(t) = \sum_{i=0}^{\mathrm{ord}(\alpha)p^l - 1} t^{\mathrm{ord}(\alpha)p^l - 1 - i}\alpha^i$. From $(t-\alpha)(t-\alpha^{-1}) \,|\, t^T - 1$, it is valid that $t - \alpha^{-1} \,|\, g(t)$ which is equivalent to $g(\alpha^{-1}) = 0$. Our scheme makes use of this relation to find

the proper value of T. Now $g(\alpha^{-1})$ can be computed directly as

$$\begin{aligned} g(\alpha^{-1}) &= \sum_{i=0}^{\mathrm{ord}(\alpha)p^l-1} (\alpha^{-1})^{\mathrm{ord}(\alpha)p^l-1-i}\alpha^i \\ &= \sum_{i=0}^{\mathrm{ord}(\alpha)p^l-1} \alpha^{i+1-\mathrm{ord}(\alpha)p^l}\alpha^i \\ &= \sum_{i=0}^{\mathrm{ord}(\alpha)p^l-1} \alpha^{2i+1}. \end{aligned}$$

Notice that $\mathrm{ord}(\alpha)$ is odd. Then $\sum_{i=0}^{\mathrm{ord}(\alpha)-1}\alpha^{2i+1} = \alpha^1+\alpha^3+\cdots+\alpha^{\mathrm{ord}(\alpha)}+\alpha^2+\alpha^4+\cdots+\alpha^{\mathrm{ord}(\alpha)-1} = \sum_{i=1}^{\mathrm{ord}(\alpha)}\alpha^i$. This leads to $g(\alpha^{-1}) = p^l h(\alpha^{-1})$ where

$$h(\alpha^{-1}) = \sum_{i=1}^{\mathrm{ord}(\alpha)} \alpha^i. \tag{23}$$

Multiplying both sides of (23) with α gives

$$\alpha h(\alpha^{-1}) = \sum_{i=2}^{\mathrm{ord}(\alpha)} \alpha^i + \alpha^{\mathrm{ord}(\alpha)+1}. \tag{24}$$

Subtract (23) by (24) gets $(1-\alpha)h(\alpha^{-1}) = \alpha - \alpha^{\mathrm{ord}(\alpha)+1}$. Obviously, $\alpha - \alpha^{\mathrm{ord}(\alpha)+1} = 0$ and so $(1-\alpha)h(\alpha^{-1}) = 0$. Since $1-\alpha$ is a zero divisor in Z_{p^e} and $p^i \,|\, 1-\alpha$, it must hold that $p^{e-i} \,|\, h(\alpha^{-1})$. Now we check this in more detail to verify whether $p^{e-i+1} \,|\, h(\alpha^{-1})$ which is important in the analysis of the period.

We have $\alpha = 1+\sum_{j=i}^{e-1} a_j p^j$ and $1-\alpha = \sum_{j=i}^{e-1} a_j p^j$. Now compute $\alpha^{\mathrm{ord}(\alpha)+1}$ directly. As $p>3$, it holds that

$$\begin{aligned} \alpha^p &= \left(1+\sum_{j=i}^{e-1} a_j p^j\right)^p \\ &= 1 + p^{i+1}\sum_{j=i}^{e-1} a_j p^{j-i} + \binom{p}{2} p^{2i}\left(\sum_{j=i}^{e-1} a_j p^{j-i}\right)^2 + \cdots \\ &\quad + \binom{p}{p} p^{pi}\left(\sum_{j=i}^{e-1} a_j p^{j-i}\right)^p \\ &= 1 + p^{i+1}\sum_{j=i}^{e-1} a_j p^{j-i} + p^{2i+1}\left(\sum_{j=i}^{e-1} a_j p^{j-i}\right) m \end{aligned}$$

where $m \in Z$. Continue in this way gives $\alpha^{\mathrm{ord}(\alpha)} = \alpha^{p^{e-i}} = 1 + p^e\sum_{j=i}^{e-1} a_j p^{j-i} + p^{e+i}(\sum_{j=i}^{e-1} a_j p^j)m'$ for some $m' \in Z$. This leads to $\alpha - \alpha^{\mathrm{ord}(\alpha)+1} = \alpha[p^e\sum_{j=i}^{e-1} a_j p^{j-i} + p^{e+i}(\sum_{j=i}^{e-1} a_j p^j)m']$. Therefore, in Z, $h(\alpha^{-1}) = \frac{\alpha-\alpha^{\mathrm{ord}(\alpha)+1}}{1-\alpha} = \alpha[p^{e-i} + p^e m']$ which shows $h(\alpha^{-1}) = \alpha p^{e-i}$ in Z_{p^e} and $p^{e-i+1} \nmid h(\alpha^{-1})$.

The relationship $g(\alpha^{-1}) = p^l h(\alpha^{-1}) = \alpha p^{e-i+l} = 0$ gives $l = i$. Thus the period of $f(t)$ is $T = \mathrm{ord}(\alpha)p^l = p^{e-i}p^i = p^e$. If $\alpha = 1$, we have $T = p^e$ by the same argument.

Therefore $T = p^e$.

Case 2: α is in $Z_{p^e}[t]/(f(t))$

In this case, $f(t)$ is irreducible in $Z_{p^e}[t]$. Moreover, α is a root of $f(t)$ and all elements in $Z_{p^e}/(f(t))$ can be expressed as $b_1 + b_2\times\alpha$ where $b_1, b_2 \in Z_{p^e}$. Since $T = p^k$ where $1 \le k \le e$, $\mathrm{ord}(\alpha)$ must be some powers of p. Notice that $\alpha - 1$ is a zero divisor since $(\alpha-1)\times p^{e-1}(\alpha-1) = p^{e-1}\times ab\times\alpha = 0$. Then $p \,|\, (\alpha-1)^2$. Now the order of α can be calculated directly as:

$$\begin{aligned} \alpha^p &= [1+(\alpha-1)]^p \\ &= 1 + p(\alpha-1) + \sum_{i=2}^{p}\binom{p}{i}(\alpha-1)^i. \end{aligned} \tag{25}$$

Since $p>3$, (25) can be written as $\alpha^p = 1 + p(\alpha-1) + p^2 c$ where $c \in Z_{p^e}/(f(t))$. Continue in the same manner leads to $\mathrm{ord}(\alpha) = p^e$.

From $\mathrm{ord}(\alpha) \,|\, T$ and $T = p^k$, where $1 \le k \le e$, it must hold that $T = p^e$.

Combining Cases 1 and 2, it can be concluded that $T = p^e$.

Counting.

In this case $ab + 2 \equiv 2 \bmod p$, i.e., $p \,|\, ab$. Notice also that $a, b \in Z_{p^e}$ and a, b are not both divisible by p.

If $(a,p) = 1$, p must divide b. There are $\varphi(p^e) = p^e - p^{e-1}$ choices for a and p^{e-1} for b. In this situation, there are $p^{2e-2}(p-1)$ cat maps.

If $(b,p) = 1$, p must divide a. Based on the same argument, there are also $p^{2e-2}(p-1)$ cat maps. Therefore the total number of cat maps of period p^e is $2p^{2e-2}(p-1)$. ■

2) $f(t) = t^2 + 2t + 1$ in $Z_p[t]$: In this case, $ab + 2 \equiv p - 2 \bmod p$. The analysis for this case is the same as for the previous case $f(t) = t^2 - 2t + 1$ in $Z_p[t]$. When $f(t)$ is irreducible in $Z_{p^e}[t]$, the ring $Z_{p^e}[t]/(f(t))$ is again not a Galois ring. Its zero divisors form a maximal ideal generated by p and $t+1$ which is $(p, t+1)$. The quotient ring R/I is a Galois field.

We present our result as follows without proof because the proof is the same as that for Proposition 5.

Proposition 6: If $f(t) = t^2+2t+1$ in $Z_p[t]$, then $\mathrm{per}(f(t)) = 2p^e$ and there are $p^{2e-2}(p-1)$ cat maps having this period.

Now combining Propositions 1, 3, 5, and 6, we summarize the results in the following theorem.

Theorem 7: Let T be the period of the cat map over Z_{p^e}. If a and$b$ are not both divisible by p, the possible periods and the number of distinct cat maps corresponding to each period are given by Table I.

TABLE I
PERIOD DISTRIBUTION IF a AND b ARE NOT BOTH DIVISABLE BY p

Period	Number of cat maps
$T = 1$	1
$T = p^e$	$2p^{2e-2}(p-1)$
$T = 2p^e$	$p^{2e-2}(p-1)$
For each T in $\{k : k = k_1k_2, k_1 > 2, k_1 \mid p-1, k_2 \mid p^{e-1}\}$	$\frac{\varphi(k)}{2}(p^e - p^{e-1})$
For each T in $\{k : k = k_1k_2, k_1 > 2, k_1 \mid p+1, k_2 \mid p^{e-1}\}$	$\frac{\varphi(k)}{2}(p^e - p^{e-1})$

IV. PERIOD DISTRIBUTION IF a AND b ARE BOTH DIVISIBLE BY p

In this case, $a \,|\, p$ and $b \,|\, q$. If $a = 0$ and $b = 0$, it is trivial to verify that the period of the cat map is 1. Therefore, we assume as least one of a and b is non-zero in the following analysis. The period of the cat map may not equal to $\mathrm{per}(f)$. Here we adopt another way to deal with this problem. Rewrite the cat

map (3) as $\mathbf{x}(n+1) = \mathbf{A}\mathbf{x}(n) \bmod N$. Suppose its period is T, then $\mathbf{x}(T) = \mathbf{A}\mathbf{x}(T-1) = \cdots = \mathbf{A}^T\mathbf{x}(0)$. Since T is the period of cat map, $\mathbf{x}(T) = \mathbf{x}(0)$ holds and it follows that $(\mathbf{A}^T - \mathbf{I})\mathbf{x}(0) = \mathbf{0}$ in Z_N for all possible initial points in Z_N^2 where $\mathbf{I}$ is the identity matrix and $\mathbf{0}$ is the zero vector. Then it must hold that T is the smallest integer such that $\mathbf{A}^T = \mathbf{I}$ in Z_N. This suggests another way to compute the period of the cat map.

Generally, this approach is difficult and the carry problem in the arithmetic operations needs to be solved. However, if $a \,|\, p$ and $b \,|\, q$ as in this case, The Hensel lifting method can give satisfactory results. Let the p-adic expansion of a and b be $a = a_0 + a_1 \times p + \cdots + a_{e-1} \times p^{e-1}$ and $b = b_0 + b_1 \times p + \cdots + b_{e-1} \times p^{e-1}$, respectively, with $a_i, b_i \in Z_p$. Then the p-adic expansion of $\mathbf{A}$ is

$$\begin{aligned}\mathbf{A} &= \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \\ &= \mathbf{I} + p\begin{pmatrix} 0 & a_1 \\ b_1 & r_1 \end{pmatrix} + \cdots + p^{e-1}\begin{pmatrix} 0 & a_{e-1} \\ b_{e-1} & r_{e-1} \end{pmatrix}.\end{aligned}$$

Let $\mathbf{A}_i = \begin{pmatrix} 0 & a_i \\ b_i & r_i \end{pmatrix}$ and rewrite $\mathbf{A}$ as

$$\mathbf{A} = \mathbf{I} + \mathbf{A}_1 \times p + \cdots + \mathbf{A}_{e-1} \times p^{e-1}. \tag{26}$$

Now we can use (26) to compute the n-th power of $\mathbf{A}$.

Proposition 8: For the cat map (3) with $\mathbf{A}$ given by (26), its period T traverses the set $\{p^i, 1 \le i \le e-1\}$ and there are $(p^2-1)p^{2i-2}$ cat maps corresponding to period p^i.

Proof: Period analysis.

Suppose $\mathbf{A}_i (1 \le i \le e-1)$ is the first term in (26) whose elements are not all zeros. In this situation, it holds that $r_i = 0$ since $ab+1 = (\sum_{j=i}^{e-1} a_j p^j)(\sum_{j=i}^{e-1} b_j p^j) + 1$ and the i-th term in its p-adic expansion must be 0.

From the expression $\mathbf{A} = \mathbf{I} + \mathbf{A}_i \times p^i + \cdots + \mathbf{A}_{e-1} \times p^{e-1}$, taking power p at both sides gets $\mathbf{A}^p = \mathbf{I} + \mathbf{A}'_{i+1} \times p^{i+1} + \cdots + \mathbf{A}'_{e-1} \times p^{e-1}$ where $\mathbf{A}'_{i+1} = \mathbf{A}_i$. Continuing in this fashion gives $\mathbf{A}^{p^{e-i}} = \mathbf{I}$ in Z_{p^e} and p^{e-i} is the smallest integer for such an equality to hold. Then the period T of the cat map is also p^{e-i}. Therefore T traverses the set $\{p^i, 1 \le i \le e-1\}$ when i changes from 1 to $e-1$.

Counting.

Let $T = p^{e-i}$ where $1 \le i \le e-1$ and $\mathbf{A}_i$ be the first term in (26) whose elements are not all zeros.

If $a_i \ne 0$, the number of choices for a_i is $p-1$ and there are p choices for a_j where $j > i$. Then the total number of choices for a and b are $(p-1)p^{e-1-i}$ and p^{e-i}, respectively. As a result, there are $(p-1)p^{2(e-i)-1}$ cat maps.

If $a_i = 0$, b_i must be non-zero. The number of choices for a is p^{e-1-i} and there are $(p-1)p^{e-1-i}$ possible values for b. The number of cat maps falling into this category is $(p-1)p^{2(e-i)-2}$.

To summarize, there are $(p-1)p^{2(e-i)-1} + (p-1)p^{2(e-i)-2}$ cat maps of period p^{e-i}, where $1 \le i \le e-1$. Equivalently, there are $(p^2-1)p^{2i-2}$ cat maps of period p^i, where $1 \le i \le e-1$. ∎

Now we have discussed all cases for analysing the period distribution of the cat map. Combining Theorem 7, Proposition 8 and the trivial case $a = b = 0$, the overall results are summarized in the following theorem.

TABLE II
PERIOD DISTRIBUTION FOR $N = p^e, p > 3$

Period	Number of cat maps
$T = 1$	1
$T = p^e$	$2p^{2e-2}(p-1)$
$T = 2p^e$	$p^{2e-2}(p-1)$
For each T in $\{p^k : 1 \le k \le e-1\}$	$(p^2-1)p^{2k-2}$
For each T in $\{k : k = k_1k_2, k_1 > 2, k_1 \mid p-1, k_2 \mid p^{e-1}\}$	$\frac{\varphi(k)}{2}(p^e - p^{e-1})$
For each T in $\{k : k = k_1k_2, k_1 > 2, k_1 \mid p+1, k_2 \mid p^{e-1}\}$	$\frac{\varphi(k)}{2}(p^e - p^{e-1})$

TABLE III
EXPERIMENTAL RESULTS FOR $N = 7^3$

period	1	3	4	6	7	8
number of cat maps	1	294	294	294	48	588
period	21	28	42	49	56	147
number of cat maps	1764	1764	1764	2352	3528	12348
period	196	294	343	392	686	
number of cat maps	12348	12348	28812	24696	14406	

Theorem 9: Let $N = p^e$ where $p > 3, e \ge 2$ and T be the period of the cat map over Z_{p^e}. The possible periods and the number of cat maps possessing each period are listed in Table II.

Remark 10: There are p^{2e} cat maps in Z_{p^e} which implies that the summation of the last column of Table II should be p^{2e}. Now we check for this. It holds that

$$\sum_{k=1}^{e-1}(p^2-1)p^{2k-2} = p^{2e-2} - 1$$

and

$$\begin{aligned}&\sum_{k=k_1k_2, k_1>2, k_1 \mid p-1, k_2 \mid p^{e-1}} \frac{\varphi(k)}{2}(p^e - p^{e-1}) \\ &= \sum_{k \,|\, (p-1)p^{e-1}} \frac{\varphi(k)}{2}(p^e - p^{e-1}) - \sum_{k \mid p^{e-1}} \frac{\varphi(k)}{2}(p^e - p^{e-1}) \\ &\quad - \sum_{k \,|\, p^{e-1}} \frac{\varphi(2k)}{2}(p^e - p^{e-1}) \\ &= \frac{(p^e - p^{e-1})}{2}[(p-1)p^{e-1} - p^{e-1} - p^{e-1}] \\ &= \frac{(p-3)}{2}p^{e-1}(p^e - p^{e-1}).\end{aligned}$$

Similarly, $\sum_{k=k_1k_2, k_1>2, k_1 \,|\, p+1, k_2 \mid p^{e-1}} \frac{\varphi(k)}{2}(p^e - p^{e-1}) = \frac{(p-1)}{2}p^{e-1}(p^e - p^{e-1})$. As a result, adding all entries in the last column of Table II gives p^{2e} which verifies the correctness of our analysis. We also remind that $p > 3$ is needed in the proof of Proposition 5.

Example 11: An example is given here to compare the theoretical and experimental results. A computer program has been written to exhaust all possible cat maps over Z_{7^3} to find the period by brute force. The results are listed in Table III.

It is easy to check that the maximal period is $2 \times 7^3 = 686$. The number of cat maps of this period is $7^{2\times 3-2} \times (7-1) = 14406$. The search outputs are consistent with our theoretical results.

Table II lists the complete result we have obtained. It provides full information on the period distribution of the cat map. The maximal period is $2p^e$ while the minimal period is 1. The mean value of the periods varies a lot, depending on p. The analysis process also indicates how to choose the parameters a and b such that the period of the cat map fits a specific application. In security applications, a long period is often required which limits the choice for a and b, and hence the size of the key space.

The period distribution for the cases $p = 2$ and $p = 3$ needs special analyses. They can be solved simply by adopting the Hensel lifting approach and we are now working toward this. It is easy to observe that once this is done, the period distribution for general composite $N = p_1^{e_1} \cdots p_l^{e_l}$ is also revealed. This is because the overall period equals to the least common multiple of the periods of the cat maps on $Z_{p_i^{e_i}}$.

V. Conclusion

The period distribution of the cat map on the Galois ring Z_{p^e} for prime $p > 3$ has been analyzed. Full knowledge on the distribution is obtained by combining the generation function and Hensel lifting method. The results help in various system designs and analyses. The analysis process also illustrates how to compute the period of some polynomials in the Galois ring.

Acknowledgment

The first author is grateful to Dr. Qunxiong Zheng and Dr. Xiutao Feng for wonderful discussions on sequences over rings when he was an intern at the *State Key Laboratory of Information Security*, Chinese Academy of Science.

References

[1] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaoticmaps," *IEEE Trans. Circuits Syst. I, Fundam. Theory \Appl.*, vol. 48, no. 2, pp. 163–169, 2001.
[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, pp. 1259–1284, 1998.
[3] G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons, Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
[4] Y. Zhang, Y. Wang, and X. Shen, "A chaos-based image encryption algorithm using alternate structure," *Sci. China Series F: Inf. Sci.*, vol. 50, no. 3, pp. 334–341, 2007.
[5] Z. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, no. 1–3, pp. 153–157, 2005.
[6] L. Kocarev and Z. Tasev, "Public-key encryption based on chebyshev maps," in *Proc. Int. Symp. Circuits Syst. (ISCAS'03)*, vol. 3, no. 25–28, pp. III-28–III-31, Vol. 3.
[7] L. Kocarev, M. Sterjev, A. Fekete, and G. Vattay, "Public-key encryption with chaos," *Chaos*, vol. 14, p. 1078, 2004.
[8] R. Bose, "Novel public key encryption technique based on multiple chaotic systems," *Phys. Rev. Lett.*, vol. 95, no. 9, p. 98702, 2005.
[9] D. Lou and C. Sung, "A steganographic scheme for secure communications based on the chaos and Euler theorem," *IEEE Trans. Multimedia*, vol. 6, no. 3, pp. 501–509, 2004.
[10] V. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics*. New York: Benjamin, 1968.
[11] E. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 732–736, Nov. 1976.
[12] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. New York, NY: Springer-Verlag, 1986.
[13] R. Rueppel and O. Staffelbach, "Products of linear recurring sequences with maximum complexity," *IEEE Trans. Inf. Theory*, vol. IT-33, no. 1, pp. 124–131, 1987.
[14] S. Blackburn, "The linear complexity of the self-shrinking generator," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2073–2077, 1999.
[15] A. Canteaut, "Fast correlation attacks against stream ciphers and related open problems," in *Proc. IEEE Inf. Theory Workshop Theory Practice Inf.-Theor. Security*, 2005, pp. 49–54.
[16] F. Chen, K. Wong, X. Liao, and H. Zheng, "Period distribution of generalized discrete arnold cat map for prime N," *IEEE Trans. Circuits Syst. I, Reg. Papers*, 2010, submitted for publication.
[17] S. Fan and W. Han, "Random properties of the highest level sequences of primitive sequences over Z_{2^e}," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1553–1557, 2003.
[18] X. Zhu and W. Qi, "Further result of compressing maps on primitive sequences modulo odd prime powers," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2985–2990, 2007.
[19] V. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over Z_4," *IEEE Trans. Inf. Theory*, vol. 42, no. 5, pp. 1594–1600, 1996.
[20] P. Sole and V. Sison, "Quaternary convolutional codes from linear block codes over galois rings," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2267–2270, 2007.
[21] Z. Wan, *Quaternary Codes*. Singapore: World Scientific, 1997.
[22] G. Hardy, E. Wright, D. Heath-Brown, and J. Silverman, *An Introduction to the Theory of Numbers*. Gloucestershire, U.K.: Clarendon, 1960.
[23] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, U.K.: Cambridge Univ. Press, 1994.
[24] Z. Wan, *Lectures on Finite Fields and Galois Rings*. Singapore: World Scientific, 2003.
[25] Wiki, Frobenius Endomorphism [Online]. Available: http://en.wikipedia.org/wiki/Frobenius_endomorphism

Fei Chen received the B.S. and M.S. degrees in computer science and engineering from Chongqing University, China. He is now pursuing the Ph.D. degree in The Chinese University of Hong Kong. His research interests include cryptology and network security.

Kwok-Wo Wong (SM'03) received the B.Sc. degree in electronic engineering from the Chinese University of Hong Kong and the Ph.D. degree from the City University of Hong Kong, where he is currently an associate professor in the Department of Electronic Engineering. His current research interests include chaos, cryptography, and neural networks. He has published more than 100 papers in 25 international mathematics, physics, and engineering journals in the fields of nonlinear dynamics, cryptography, neural networks, and optics. He is a senior member of the IEEE. He is also a chartered engineer and a member of the Institution of Engineering and Technology (IET).

Xiaofeng Liao received the B.S. and M.S. degrees in mathematics from Sichuan University, Chengdu, China, in 1986 and 1992, respectively, and the Ph.D. degree in circuits and systems from the University of Electronic Science and Technology of China in 1997. From 1999 to 2001, he was involved in postdoctoral research at Chongqing University, where he is currently a professor. From November 1997 to April 1998, he was a research associate at the Chinese University of Hong Kong. From October 1999 to October 2000, he was a research associate at the City University of Hong Kong. From March 2001 to June 2001 and March 2002 to June 2002, he was a senior research associate at the City University of Hong Kong. From March 2006 to April 2007, he was a research fellow at the City University of Hong Kong. He has published more than 150 international journal and conference papers. His current research interests include neural networks, nonlinear dynamical systems, bifurcation and chaos, and cryptography.

Tao Xiang received the B.S., M.S. and Ph.D. degrees in computer science from Chongqing University, China, in 2003, 2005, and 2008, respectively. He is currently an Associate Professor of Chongqing University. His research interests include multimedia security, chaotic cryptography, and particle swarm optimization. He has published more than 30 papers on international journals and conferences. He also served as a referee for numerous international journals.