High Security Frequency/Time Hopping Sequence Generators

Yun-Pyo Hong

The Graduate School

Yonsei University

Department of Electrical and Electronic Engineering

High Security Frequency/Time Hopping Sequence Generators

by

Yun-Pyo Hong

A Dissertation Submitted to the

Graduate School of Yonsei University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

Supervised by

Professor Hong-Yeop Song, Ph.D.

Department of Electrical and Electronic Engineering
The Graduate School

YONSEI University

December 2007

Contents

List of Figures

ABSTRACT

High Security Frequency/Time Hopping Sequence Generators

Yun-Pyo Hong
Department of Electrical and Electronic Eng.
The Graduate School
Yonsei University

We discuss some methods of constructing frequency/time hopping (FH/TH) sequences over $\mathbb{F}_{p^k}$ by taking successive k-tuples of given sequences over $\mathbb{F}_p$. We are able to characterize those p-ary sequences whose k-tuple versions now over $\mathbb{F}_{p^k}$ have the maximum possible linear complexities (LCs). Then, we consider FH/TH sequence generators composed of a combinatorial function generator and some registers. We are able to characterize the generators whose output FH/TH sequences over $\mathbb{F}_{p^k}$ have the maximum possible LCs for the given algebraic normal form to resist a Berlekamp-Massey (BM) attack.

Next, we consider the cryptographic properties of p-ary functions, that is the combinatorial functions of the FH/TH sequence generators, to resist other cryptographic attacks than the BM attack for high security. We are able to construct balanced p-ary functions by compositions. We are able to construct balanced p-ary functions which satisfy the propagation for the most of nonzero vectors and balanced functions which satisfy

the propagation of high degree. We are able to derive a necessary condition such that p-ary functions are correlation-immune by the Fourier transforms and show that some of nonlinearity criteria are invariant under cryptographically weak transformations.

Finally, we note a ultra-wide bandwidth (UWB) impulse radio (IR) as the example of commercial TH spread spectrum communication systems. We consider a coded N-ary pulse position modulated UWB-IR, which exploits the chaotic inter-pulse intervals in the framed-time structure and the polarity randomization for the coexistence with conventional narrow bandwidth wireless communication systems. We show that the proposed system has noise-like spectrum, that is line spectrum free, by calculating its power spectral density function. We discuss its multi-user system with its line spectrum property. Then, we confirm the bit error rate performance of the proposed system by simulation based on the UWB indoor channel model.

Key words : Frequency/time hopping sequence, linear complexity, balancedness, propagation, correlation-immunity, nonlinearity, p-ary function, ultra-wide bandwidth, line spectrum, polarity randomization, convolutional code

Chapter 1

Introduction

1.1 Motivation

In a peer-to-peer frequency/time hopping (FH/TH) spread spectrum communication system, an attacker may try to synthesize the entire FH/TH pattern from some frequency/time slots successively observed. When the attacker observes successive twice frequency/time slots as the linear complexity (LC) [1] [2] [3] [4] of the pattern, he can successfully synthesize the next frequency/time slots. Thus, from the view point of the system designers, the LCs of the FH/TH sequences in use should be as large as possible. Note that FH/TH communication systems using a few hundreds, or even a few thousands frequency/time slots are common in practice. Therefore, it is necessary to design non-binary sequences (i) with "large" LCs, and (ii) over "large" alphabets, but (iii) with "little" increase in the hardware complexity.

We consider the simple way of constructing a (p^k-ary) FH/TH sequence T over a large alphabet from a given (p-ary) sequence S over a small alphabet, simply reading its successive k-tuples. We believe that this method makes no significant increase in the complexity in actual hardware design. Thus, this method satisfies the last two conditions

listed in the previous paragraph. We interpret the terms of T, that is k-tuples over $\mathbb{F}_p$, as elements of $\mathbb{F}_{p^k}$ by using some but fixed basis over $\mathbb{F}_p$. We try to

- rule out any possibility that the decrease in its LC using some other basis than that used in the design might help the attacker to track the FH/TH sequence.

Given any one basis, it is clear that the LC of T is at most that of S. Therefore, it is worthy to

- characterize those p-ary sequences S whose k-tuple versions T have the same LCs as S (that is the maximum possible) for any choice of basis.

In addition, We consider FH/TH sequence generators composed of a combinatorial function generator [5] and some registers. Then, it is necessary to

- characterize the generators whose output FH/TH sequences have the maximum possible LCs.

However, we note that the above characterization is for resistance to the only Berlekamp-Massey (BM) attack [6]. So, we consider desired cryptographic properties [5] of combinatorial functions, i.e. p-ary functions, of the FH/TH sequence generators to resist other cryptographic attacks than the BM attack for high security. The relevance of these properties is based on information theoretic grounds or on specific cryptographic attacks that have their own attack scenarios. Unfortunately, it is clear that no function can satisfy all these properties. So, it is necessary to

- characterize the p-ary functions with a corresponding cryptographic property for each possible attack on a case by case basis.

And these cryptographic properties of Boolean functions have been intensively studied in many literatures. Thus, it is natural to

- extend the cryptographic properties of Boolean functions to those of p-ary cases.

Recently, a ultra-wide bandwidth (UWB) impulse radio (IR) has been intensively studied for short range multiple-access communications in dense multipath environments because of its fine time resolution properties [7]. We note the UWB-IR as the example of commercial TH spread spectrum communication systems because this radio adopt a TH binary pulse position modulation (PPM) for multi-user communications.

Because of its extremely large bandwidth, the UWB-IR and conventional narrow bandwidth wireless communication systems cannot help giving interference to each other, and furthermore, a UWB-IR signal accompanies line spectrums giving large interference to the conventional systems. Therefore, the reduction and management of the line spectrums of the UWB-IR signal is an essential problem to be solved for coexistence with the conventional narrow bandwidth systems. We believe that a possible solution is to make the UWB-IR work in lower signal to noise ratio at the same data rate and bit error rate (BER). So, we consider a coded N-ary PPM UWB-IR, which exploits the chaotic inter-pulse intervals in the framed-time structure and the polarity randomization for the coexistence. Then, we try to

- show that the proposed system has noise-like spectrum, that is line spectrum free by calculating its power spectral density function.

The performance analyses of the UWB-IR in multipath environments are usually based on narrowband channel models or straightforward extensions to finer delay resolutions

that, however, markedly differ from empirical UWB-IR channels in the distribution of path gains. Thus, it is essential to

- confirm the BER performance of the proposed system by simulation based on UWB indoor channel models given in [8].

1.2 Overview

In chapter 2, we characterize those p-ary sequences whose k-tuple versions now over $\mathbb{F}_{p^k}$ have the maximum possible LCs. Then, we propose FH/TH sequence generators and characterize the generators whose output FH/TH sequences have the maximum possible LCs for the given algebraic normal form.

In chapter 3, we construct balanced p-ary functions by compositions. We construct balanced p-ary functions which satisfy the propagation for the most of nonzero vectors and balanced functions which satisfy the propagation of high degree. Then, we derive a necessary condition such that p-ary functions are correlation-immune by the Fourier transforms and show that some of nonlinearity criteria are invariant under cryptographically weak transformations.

Finally, in chapter 4 we propose a coded N-ary PPM UWB-IR for the coexistence with conventional narrow bandwidth wireless communication systems. We show that the proposed system has noise-like spectrum, that is line spectrum free, and discuss its multi-user system. Then, we confirm the bit error rate performance of the proposed system by simulation based on the UWB indoor channel model.

Chapter 2

Frequency/Time Hopping Sequences with Large Linear Complexities

We discuss some methods of constructing frequency/time hopping (FH/TH) sequences over $\mathbb{F}_{p^k}$ by taking successive k-tuples of given sequences over $\mathbb{F}_p$. We are able to characterize those p-ary sequences whose k-tuple versions now over $\mathbb{F}_{p^k}$ have the maximum possible linear complexities (LCs). Next, we consider FH/TH sequence generators composed of a combinatorial function generator and some registers. We are able to characterize the generators whose output FH/TH sequences over $\mathbb{F}_{p^k}$ have the maximum possible LCs for the given algebraic normal form.

2.1 Detailed Motivation

In a peer-to-peer frequency/time hopping (FH/TH) spread spectrum communication system, an attacker may try to synthesize the entire FH/TH pattern from some frequency/time slots successively observed. That is, the attacker may try to synthesize the linear feed-

back shift register (LFSR) [1] [2] [3] [4] that can generate the next slots of the FH/TH pattern using Berlekamp-Massey (BM) algorithm [6] over a finite field.

Let L be the linear complexity (LC) [1] [2] [3] [4] of an FH/TH sequence. When the attacker observes successive $2L$ frequency/time slots, he can successfully synthesize the next frequency/time slots as long as the same FH/TH sequence is used. Therefore, from the view point of the system designers, the system should change from one FH/TH sequence to another before $2L$ slots of the sequence are used, and the LCs of the FH/TH sequences in use should be as large as possible.

Note that any FH/TH sequences are non-binary in general since there are usually more than 2 frequency/time slots available. In fact, FH/TH communication systems using a few hundreds, or even a few thousands frequency/time slots are common in practice. It is well-known that the number of frequency/time slots affects directly the processing gain [4] of the FH/TH spread spectrum communication systems, at the price of the hardware complexity. Therefore, it is necessary to design non-binary sequences (i) with "large" LCs, and (ii) over "large" alphabets, but (iii) with "little" increase in the hardware complexity.

In this chapter, we consider the simple way of constructing a non-binary (p^k-ary) sequence T over a large alphabet from a given (p-ary) sequence S over a small alphabet, simply reading its successive k-tuples. By increasing the parameter k, one may obtain a sequence over as large alphabet as one wishes. We believe that this method is so simple to construct a p^k-ary sequence compared with a construction over $\mathbb{F}_{p^k}$ because the multiplications over $\mathbb{F}_{p^k}$ are much more complex than those over $\mathbb{F}_p$ in the LFSR constructions which is general methods in the hardware systems. In this view point, there

will be no significant increase in the complexity in actual hardware design. Therefore, this method satisfies the last two conditions listed in the previous paragraph.

On the other hand, we have to be very careful in analyzing the LCs of the new sequences, including the definition of the LC of T over k-tuples over $\mathbb{F}_p$ which is not a field any more. One way to solve this problem is to interpret the k-tuples over $\mathbb{F}_p$ as elements of $\mathbb{F}_{p^k}$. In this case, it is not much surprising to observe that two different basis may result in two different LCs of T (now over $\mathbb{F}_{p^k}$), and hence, the LC of T depends on the choice of basis (of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$).

We are here trying to rule out any possibility that the decrease in its LC using some other basis than that used in the design might help the intercepter to track the FH/TH sequence, assuming that the FH/TH sequence T with its LC equal to L (using the basis used in the design process) is used for the duration of $2L-1$ slots.

Given any one basis, it is clear that the LC of T is at most that of S. We are able to characterize those p-ary sequences S whose k-tuple versions T now over $\mathbb{F}_{p^k}$ have the same minimal polynomials [1] [2] [3] [4] as S, and therefore, the same LCs as S (that is the maximum possible), for any choice of basis of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$. This leads to the construction of p^k-ary sequences with minimal polynomials essentially over $\mathbb{F}_p$.

We apply the above characterization into two sequences with as large as possible period when the number of registers, r, is given: binary de Bruijn sequences of period 2^r [9] and p-ary *m*-sequences of period p^r-1.

We consider FH/TH sequence generators composed of a combinatorial function generator [5] and some registers. We are able to characterize the FH/TH sequence generators which guarantee that a combinatorial function sequences, S, over $\mathbb{F}_p$ have the maximum

possible LCs for the given algebraic normal form and that k-tuple versions T of S now over $\mathbb{F}_{p^k}$ have the same minimal polynomials as S, and therefore, the same LCs as S (that is the maximum possible) for any choice of basis of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$.

2.2 Preliminaries

The LC of a sequence is the size of the shortest LFSR which can generate the sequence [1] [2] [3] [4]. Obviously, it means the difficulty of generating and perhaps analyzing the sequence from some symbols of the sequence successively observed and must be an important design criteria in the field of security (that is stream cipher systems, military FH/TH spread spectrum communication systems, etc.).

Let $\mathbb{F}_q$ be the finite field with q elements and p be a prime. Assume that the linear recurrence relation of an LFSR that generates a sequence $S = \{s_n | n = 0, 1, 2, ...\}$ over $\mathbb{F}_p$ is given by

$$s_n = \sum_{i=1}^{L} c_i s_{n-i}, \tag{2.1}$$

where $c_i,\ i = 1, 2, \ldots, L$, is a connection coefficient over $\mathbb{F}_p$. Then, the characteristic polynomial of S is given by [1] [2] [3] [4]

$$C(x) = x^L - \sum_{i=1}^{L} c_i x^{L-i}. \tag{2.2}$$

The minimal polynomial of S corresponds to the characteristic polynomial of the minimum degree [1] [2] [3] [4]. Note that the degree of minimal polynomial is the LC of S. Figure 2.1 shows the LFSR whose linear recurrence relation is given in (2.1).

BM algorithm regards the symbol of a sequence as the element of some finite field and synthesizes the minimal polynomial of the sequence over the field [6].

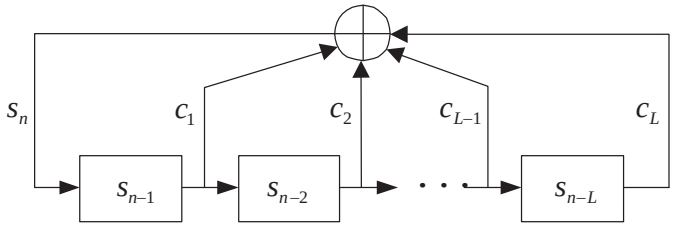


Figure 2.1: LFSR whose linear recurrence relation is given in (2.1).

2.3 Sequences over $\mathbb{F}_{p^k}$ with Minimal Polynomials over $\mathbb{F}_p$

Consider a given sequence $S = \{s_n | n = 0, 1, 2, ...\}$ over $\mathbb{F}_p$. Let k be a positive integer, and define a new sequence (an FH/TH sequence) $T(k, S) = \{t_n | n = 0, 1, 2, ...\}$ based on S by the following:

$$t_n = (s_n,\ s_{n-1},\ \ldots,\ s_{n-k+1})\ . \tag{2.3}$$

Then, it is clear that the sequence $T(k, S)$ is over $\mathbb{F}_p^k$, the k-tuple vector space over $\mathbb{F}_p$. By using some but fixed basis such as a simple polynomial basis given by

$$\{\alpha^{k-1},\ \alpha^{k-2},\ \ldots,\ \alpha,\ 1\}, \tag{2.4}$$

where α is a primitive element of $\mathbb{F}_{p^k}$, one can regard the sequence $T(k, S)$ being over a field $\mathbb{F}_{p^k}$. This is a straightforward and simple way of enlarging the size of alphabet over which a sequence is.

Proposition 2.1 The LFSR that generates a sequence $S = \{s_n\}$ over $\mathbb{F}_p$ also generates $T(k, S)$ over $\mathbb{F}_{p^k}$ as defined in (2.3) regardless of the choice of basis. The converse holds provided that the characteristic polynomial that generates T over $\mathbb{F}_{p^k}$ is essentially over $\mathbb{F}_p$.

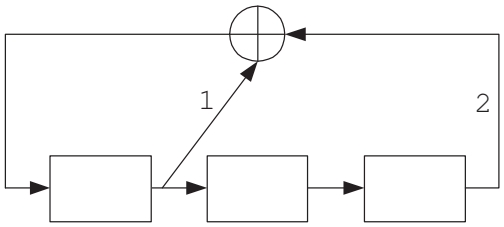


Figure 2.2: LFSR generating S and T's of Example 2.1.

Example 2.1 A ternary sequence S with period 26 is given by

$$0\,0\,1\,1\,1\,0\,2\,1\,1\,2\,1\,0\,1\,0\,0\,2\,2\,2\,0\,1\,2\,2\,1\,2\,0\,2\,0\,0\ \ldots\ .$$

Then the sequences $T(3,S)$ and $T(4,S)$ according to (2.3) are given by the following:

$$\begin{aligned} T(3,S) &= 000\ \ 000\ \ 100\ \ 110\ \ 111\ \ 011\ \ 201\ \ 120\ \ 112\ \ 211\ \ \ldots, \\ T(4,S) &= 0002\ \ 0000\ \ 1000\ \ 1100\ \ 1110\ \ 0111\ \ 2011\ \ 1201\ \ 1120\ \ 2112\ \ \ldots\ . \end{aligned}$$

Note that both T's as well as S are generated by the LFSR shown in Figure 2.2 with connection coefficients over $GF(3)$.

Proposition 2.1 does not guarantee that the LFSR for $T(k,S)$ over $\mathbb{F}_{p^k}$, $k \geq 2$, is necessarily the shortest possible even if it is the shortest for S over $\mathbb{F}_p$, but that the LC of $T(k,S)$ is at most that of S. In fact, the shortest LFSR for $T(k,S)$ over $\mathbb{F}_{p^k}$, $k \geq 2$, (and hence the LC of T) cannot be uniquely determined unless a basis of $\mathbb{F}_{p^k}$ is fixed. Following example shows this.

Example 2.2 (a) A binary sequence S_1 with period 63 is given by

$$1100100000111111101010010010011010101110110110111010011111110010\ldots\ .$$

The LC of S_1 over $GF(2)$ is 62, but that of $T(3, S_1)$ over $GF(2^3)$ is 60 with respect to any polynomial basis as in (2.4). (b) A binary sequence S_2 with period 63 is given by

$$0101111111001100000110111111010100111111000110011101001010010 11 \ldots .$$

The LC of $T(3, S_2)$ over $GF(2^3)$ is 55 or 53 with respect to the polynomial basis as in (2.4) using $x^3 + x + 1$ or $x^3 + x^2 + 1$, respectively.

A question at this point is the following: is it possible that the shortest LFSR that generates S over $\mathbb{F}_p$ is indeed the shortest LFSR that generates $T(k, S)$ over $\mathbb{F}_{p^k}$ with respect to some basis of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ for $k \geq 2$? If it is possible to characterize such p-ary sequences S, then $T(k, S)$ over $\mathbb{F}_{p^k}$ has the same minimal polynomial as S and hence it is over $\mathbb{F}_p$.

Lemma 2.1 [1] (i) The minimal polynomial of a sequence over $GF(q)$ divides any characteristic polynomial of the LFSR that generates the sequence over $GF(q)$. Therefore, it is uniquely determined up to the multiplication by a constant. (ii) An irreducible polynomial over $GF(q)$ of degree d remains irreducible over $GF(q^k)$ if and only if k and d are relatively prime.

Theorem 2.1 [10] Let the minimal polynomial $C(x)$ of $S = \{s_n\}$ over $\mathbb{F}_p$ be given by $C(x) = \prod_{i \in I}(f_i(x))^{m_i}$ for some irreducible polynomials $f_i(x)$ of degree d_i over $\mathbb{F}_p$, some positive integers m_i, and some index set I. Let $T(k, S)$ over $\mathbb{F}_{p^k}$ be defined as in (2.3) with respect to some but fixed basis for $k \geq 1$. Then, (i) the shortest LFSR that generates S is also the shortest LFSR that generates $T(k, S)$ over $\mathbb{F}_{p^k}$, and therefore, their LCs are same, if k and d_i are relatively prime for all $i \in I$. Furthermore, (ii) it is

also the shortest LFSR of $T(k, S)$ over $GF(p^m)$, and therefore, their LCs are same, for any $m \geq k$ such that m and d_i are relatively prime for all $i \in I$.

Proof: (i) The LFSR with $C(x)$ also generate $T(k, S)$ over $\mathbb{F}_{p^k}$ by Proposition 2.1. Suppose that the degree of $C(x)$ is not the least for $T(k, S)$. Then the shortest LFSR with characteristic polynomial $C'(x)$ exists and $C'(x)$ divides $C(x)$ by Lemma 2.1(i). $C'(x) = \prod_{i \in I}(f_i(x))^{s_i}$, where s_i is a non-negative integer, $0 \leq s_i \leq m_i$ for all $i \in I$, and $\sum_{i \in I} s_i < \sum_{i \in I} m_i$ by Lemma 2.1(ii). On the other hand, the polynomial $C'(x) = \prod_{i \in I}(f_i(x))^{s_i}$ is over $\mathbb{F}_p$, and Proposition 2.1 (the converse part) implies that $C'(x)$ is also a characteristic polynomial for S over $\mathbb{F}_p$ which is a desired contradiction. (ii) Furthermore, if we regard each term of $T(k, S)$ over $GF(p^m)$ for any $m \geq k$ such that m and d_i are relatively prime by inserting so many 0's at some fixed positions, all the previous arguments will be similarly applied. ■

The converse of Theorem 2.1 is not generally true. We are able to construct p^k-ary FH/TH sequences as in Theorem 2.1 whose LCs are the same as the originals (that is the maximum possible) with respect to any basis from p-ary sequences. Thus, if the p-ary sequences have large LCs, the resulting FH/TH sequences have the same large LCs as the originals with respect to any basis. We would like to emphasize the following two cases to which Theorem 2.1 applies.

Corollary 2.1 [10] (i) For a p-ary m-sequence S of period $p^r - 1$ with p a prime, the shortest LFSR that generates S is also the shortest LFSR that generates $T(k, S)$ over $\mathbb{F}_{p^k}$ as defined in (2.3) with respect to any basis if k is relatively prime to r. Furthermore, it is also the shortest LFSR of $T(k, S)$ over $GF(p^m)$ for any $m \geq k$ which is relatively

prime to r. (ii) If a binary sequence S has a period 2^r (for example, binary de Bruijn sequences), then the shortest LFSR that generates S is also the shortest LFSR that generates $T(k, S)$ over $GF(2^k)$ as defined in (2.3) for any positive integer k. Furthermore, it is also the shortest LFSR of $T(k, S)$ over $GF(2^m)$ for any $m \geq k$.

Proof: (i) Obvious. (ii) We note that the minimal polynomial $C(x)$ of a binary sequence S with period 2^r is of the form $(1 + x)^\tau$ for some positive integer τ [9]. ■

For a binary de Bruijn sequence, S, with period 2^r and large LC which is at least $2^{r-1} + r$ [9], $T(k, S)$ over $GF(2^k)$ as defined in (2.3) has the same large LC as S by Corollary 2.1(ii). In addition, the symbol distribution of the $T(k, S)$ in one period is uniform, that is any symbol of the $T(k, S)$ appears exactly 2^{r-k} times, $r \geq k$, in one period. In reality, the finite field of characteristic 2 would be a good choice for the algebraic structure of FH/TH sequences because the computations over characteristic 2 are most efficiently implemented as hardware systems and the usual practice follows this idea. In above three points, $T(k, S)$ from binary de Bruijn sequences would be good candidates for FH/TH sequences in a peer-to-peer FH/TH spread spectrum communication system.

Example 2.3 A binary sequence S with period 16 is given by

$$0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ \ldots .$$

An 8-ary sequence $T(3, S)$ with $k = 3$ over $GF(8)$ becomes

$$000\ \ 000\ \ 000\ \ 000\ \ 100\ \ 010\ \ 101\ \ 110\ \ 111\ \ 111\ \ 111\ \ 111\ \ \ldots .$$

An 8-ary sequence $T'(3, S)$ over $GF(16)$ becomes

$$0000\ \ 0000\ \ 0000\ \ 0000\ \ 0100\ \ 0010\ \ 0101\ \ 0110\ \ 0111\ \ 0111\ \ 0111\ \ 0111\ \ \ldots .$$

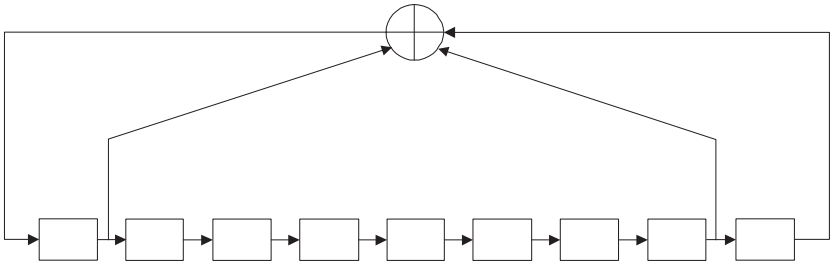


Figure 2.3: Shortest LFSR generating S and three T's of Example 2.3.

Here, the symbol 0 is padded at the leftmost position of the every term of $T(3, S)$, and the resulting 4-tuples are regarded as the elements of $GF(16)$. A 16-ary sequence $T(4, S)$ becomes

$$0001\ \ 0000\ \ 0000\ \ 0000\ \ 1000\ \ 0100\ \ 1010\ \ 1101\ \ 1110\ \ 1111\ \ 1111\ \ 1111\ \ \ldots\ .$$

All these sequences have the same minimal polynomial and the corresponding LFSR is shown in Figure 2.3.

Remark 2.1 Some interesting discussions are given in [11] and [12] which are methods of constructing p^k-ary m-sequences using several p-ary m-sequences of the same period. We note that the resulting m-sequences over $\mathbb{F}_{p^k}$ do not have the same minimal polynomial as the component p-ary m-sequences. In [12], for example, if the minimal polynomial $C(x)$ of the component p-ary m-sequence over $\mathbb{F}_p$ has degree kn, then the minimal polynomial of resulting p^k-ary m-sequence over $\mathbb{F}_{p^k}$ has degree n, and in fact, it is a factor of $C(x)$ over $\mathbb{F}_{p^k}$.

Remark 2.2 Some interesting discussions are given in [13] which establish a lower bound on the LC of a multisequence over $GF(q^k)$ in terms of the joint LC of its k

element sequences of period N over $GF(q)$. We note that he characterize the period, N, of which the LC of a multisequence is the same as the joint LC of element sequences.

Now, let $U = \{u_n | n = 0, 1, 2, ...\}$ be a p-ary k-tuple FH/TH sequence in general. In order to determine its minimal polynomial and therefore, LC of U over $\mathbb{F}_{p^k}$, we need to fix one basis for BM algorithm. Following theorem characterizes those U which do not need this.

Theorem 2.2 [10] Let $U = \{u_n | n = 0, 1, 2, ...\}$ be a p-ary k-tuple sequence in general, where $u_n = (u_n^{(1)}, u_n^{(2)}, \ldots, u_n^{(k)})$. Let a basis of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ be fixed, and the minimal polynomial $C(x)$ of U over $\mathbb{F}_{p^k}$ using BM algorithm be determined to be of the form $\prod_{i \in I}(f_i(x))^{m_i}$, where $f_i(x)$ are irreducible polynomials of degree d_i over $\mathbb{F}_p$, m_i are positive integers, and I is some index set. Then, $C(x)$ is a uniquely determined minimal polynomial of U over $\mathbb{F}_{p^k}$ regardless of the choice of basis, if k and d_i are relatively prime for all $i \in I$. Furthermore, $C(x)$ is the unique minimal polynomial of U over $GF(p^m)$ for any $m \geq k$ using any basis such that m and d_i are relatively prime for all $i \in I$.

Proof: Suppose $C'(x)$ is the corresponding minimal polynomial of U now over $\mathbb{F}_{p^k}$ with respect to another basis. Then, $C'(x)$ must divide $C(x)$ over $\mathbb{F}_{p^k}$ by Lemma 2.1(i), since $C(x)$ also generates U over $\mathbb{F}_{p^k}$ with respect to another basis. Using the same arguments as in the proof of Theorem 2.1, we have a contradiction unless $C'(x) = C(x)$.

■

2.4 Frequency/Time Hopping Sequence Generators for Large Linear Complexities

We pay attention to the construction of S over $\mathbb{F}_p$ with large LC. When $S^{(i)} = \{s_n^{(i)} | n = 0, 1, 2, ...\},\ i = 1, 2, \ldots, N$, are sequences over $\mathbb{F}_p$, a termwise product sequence $S = \prod_{i=1}^{N} S^{(i)} = \{s_n | n = 0, 1, 2, ...\}$ over $\mathbb{F}_p$ based on $S^{(i)},\ i = 1, 2, \ldots, N$, is defined as

$$s_n = \prod_{i=1}^{N} s_n^{(i)} \ \ (multiplication\ in\ \mathbb{F}_p)\ . \tag{2.5}$$

It is well-known that the LC of a termwise product sequence defined above is at most the product of the LCs of multiplied sequences.

Lemma 2.2 [2] Let $Y = \{y_n\}$ and $Z = \{z_n\}$ be sequences over $\mathbb{F}_p$ with some irreducible minimal polynomials $C_Y(x)$ and $C_Z(x)$ of degree l and m, respectively. If l and m are relatively prime, then $S = YZ$ over $\mathbb{F}_p$ as defined in (2.5) has the irreducible minimal polynomial of degree $l \times m$.

Corollary 2.2 [10] Let $S = YZ$ be a sequence over $\mathbb{F}_p$ as constructed in Lemma 2.2. If $l \times m$ and k are relatively prime, then $T(k, S)$ over $\mathbb{F}_{p^k}$ as defined in (2.3) has the same minimal polynomial as S.

Proof: It is obvious by Lemma 2.2 and Theorem 2.1. ■

Example 2.4 The irreducible minimal polynomial of Y and Z over $GF(2)$ is $C_Y(x) = x^4 + x + 1$ and $C_Z(x) = x^3 + x + 1$, respectively. The irreducible minimal polynomial of $S = YZ$ over $GF(2)$ as defined in (2.5) is $x^{12} + x^9 + x^5 + x^4 + x^3 + x + 1$ whose degree is $12 = 3 \times 4$ because $gcd(3, 4) = 1$. $T(k, S)$ over $GF(2^k)$ as defined in (2.3) has the same minimal polynomial as S for k relatively prime to 12.

We consider the general case of Lemma 2.2, that is the case of termwise product sequences based on arbitrary number of sequences with general minimal polynomials composed of irreducible factors.

Lemma 2.3 [2] Let $S^{(i)},\ i = 1, 2, \ldots, N$, be sequence over $\mathbb{F}_p$ with a minimal polynomial $C_{S^{(i)}}(x)$ of degree $M^{(i)}$, that divides $x^{p^{m^{(i)}}-1} - 1$ for some $m^{(i)}$ and contains no linear factor. For any pair of distinct roots, α and β, of $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, $\alpha\beta^{-1} \notin \mathbb{F}_p$. If $m^{(i)},\ i = 1, 2, \ldots, N$, are pairwise relatively prime, then $S = \prod_{i=1}^{N} S^{(i)}$ over $\mathbb{F}_p$ as defined in (2.5) has the minimal polynomial of degree $M = \prod_{i=1}^{N} M^{(i)}$.

The above lemma characterizes those LFSRs whose termwise product sequence has the maximum possible LC, that is the product of the LCs of multiplied sequences. We note that $\alpha\beta^{-1}$ never be in $\mathbb{F}_p$ for any pair of distinct roots, α and β, of a minimal polynomial $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, for the case of $p = 2$.

Corollary 2.3 [10] Let $S = \prod_{i=1}^{N} S^{(i)}$ be a sequence over $\mathbb{F}_p$ as constructed in Lemma 3.4. If $\prod_{i=1}^{N} m^{(i)}$ and k are relatively prime, then $T(k, S)$ over $\mathbb{F}_{p^k}$ as defined in (2.3) has the same minimal polynomial as S.

Proof: Let $C_S(x)$ be the minimal polynomial of S, then the degree of any irreducible factor of $C_S(x)$ is of the form $\prod_{i=1}^{N} r^{(i)}$, where $r^{(i)} | m^{(i)}$, by Lemma 3.4 and Theorem 2.1 completes the proof. ∎

Example 2.5 The minimal polynomial of Y over $GF(2)$ is $C_Y(x) = x^3 + x^2 + 1$ that divides $x^{2^3-1} - 1$ and $C_Y(1) = 1$. The minimal polynomial of Z over $GF(2)$ is $C_Z(x) = x^6 + x^3 + x^2 + x + 1$ that divides $x^{2^4-1} - 1$ and $C_Z(1) = 1$. The minimal

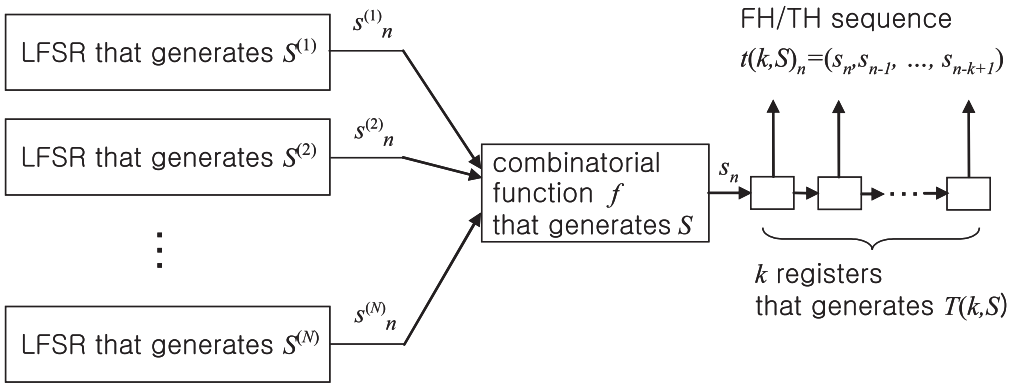


Figure 2.4: Frequency/Time hopping sequence generator for large linear complexity.

polynomial of $S = YZ$ over $GF(2)$ as defined in (2.5) is $x^{18}+x^{14}+x^{12}+x^{11}+x^{10}+x^9+x^6+x^4+x^3+x^2+1$ whose degree is $18 = 3 \times 6$ because $gcd(3,4) = 1$. $T(k,S)$ over $GF(2^k)$ as defined in (2.3) have the same minimal polynomial as S for k relatively prime to 3×4.

Now, we consider the FH/TH sequence generator composed of a combinatorial function generator [5] and k registers shown in Figure 2.4. The combinatorial function generator is a natural device to generate sequences with large LCs and called a filtering generator when the LFSRs are same. We note that we are only concerned with the case that all LFSRs are different. Let a combinatorial function sequence, S, over $\mathbb{F}_p$ by a combinatorial function, f, (that would make S have large LC) be represented in the algebraic normal form given by

$$\begin{aligned} s_n &= f(s_n^{(1)}, s_n^{(2)}, \ldots, s_n^{(N)}) \\ &= a_0 + \sum_{i=1}^{N} a_i s_n^{(i)} + \sum_{i=1}^{N} \sum_{j=i+1}^{N} a_{ij} s_n^{(i)} s_n^{(j)} + \ldots + a_{12\ldots N} s_n^{(1)} s_n^{(2)} \ldots s_n^{(N)}, \end{aligned} \tag{2.6}$$

where $S^{(i)},\ i = 1, 2, \ldots, N$, are sequences over $\mathbb{F}_p$ and the coefficients of f are elements of $\mathbb{F}_p$. We note that the algebraic normal form defined in (2.6) cannot represent all combinatorial functions. The maximum possible LC of a combinatorial function sequence, S, for the given algebraic normal form is given by [14]

$$M = F(M^{(1)}, M^{(2)}, \ldots, M^{(N)}), \tag{2.7}$$

where $F(M^{(1)}, M^{(2)}, \ldots, M^{(N)})$ is defined as (2.6) with a coefficient being 0 if it is 0 or 1 otherwise and $M^{(i)}$ is the LC of $S^{(i)},\ i = 1, 2, \ldots, N$, and operations of F are over the integers.

R. A. Rueppel characterize those LFSRs such that a combinatorial function sequence, S, has the maximum possible LC for the given algebraic normal form [2]. In Theorem 2.1, we characterize those p-ary sequences, S, whose k-tuple versions, $T(k, S)$, now over $\mathbb{F}_{p^k}$ have the maximum possible LCs. In this view point, we focus on the relations between the above two characterizations. We are able to characterize those LFSRs such that a resulting k-tuple sequence (an FH/TH sequence), $T(k, S)$, has the maximum possible LC, M as defined in (2.7). That is, we are able to construct FH/TH sequences with large LCs by the generators shown in Figure 2.4.

Lemma 2.4 [2] Let $S^{(i)},\ i = 1, 2, \ldots, N$, be sequences over $\mathbb{F}_p$ with minimal polynomials $C_{S^{(i)}}(x)$ of degree $M^{(i)}$, that divide $x^{p^{m^{(i)}}-1} - 1$ for some $m^{(i)}$ and contain no linear factor. For any pair of distinct roots, α and β, of $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, $\alpha\beta^{-1} \notin \mathbb{F}_p$. If $m^{(i)},\ i = 1, 2, \ldots, N$ are pairwise relatively prime, then S over $\mathbb{F}_p$ as defined in (2.6) has the minimal polynomial of degree M as defined in (2.7) for the given algebraic normal form, f.

Corollary 2.4 [10] Let S be a sequence over $\mathbb{F}_p$ as constructed in Lemma 3.6. If $\prod_{i=1}^{N} m^{(i)}$ and k are relatively prime, then $T(k, S)$ over $\mathbb{F}_{p^k}$ as defined in (2.3) has the same minimal polynomial as S.

Proof: Let $C_S(x)$ be the minimal polynomial of S, then the degree of any irreducible factor of $C_S(x)$ is of the form $\prod_{i=1}^{N} r^{(i)}$, where $r^{(i)}|m^{(i)}$, by Lemma 3.6 and Theorem 2.1 completes the proof. ■

Example 2.6 The minimal polynomial of X, Y, Z over $GF(2)$ is $C_X(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $C_Y(x) = x^6 + x^3 + x^2 + x + 1$, $C_Z(x) = x^{10} + x^8 + x^7 + x^5 + x^3 + x^2 + 1$ that divides $x^{2^3-1} - 1$, $x^{2^4-1} - 1$, $x^{2^5-1} - 1$ respectively and contains no linear factor. The minimal polynomial of S over $GF(2)$ defined by $s_n = f(x_n, y_n, z_n) = 1 + x_n + y_n + z_n + x_n y_n + y_n z_n + z_n x_n + x_n y_n z_n$ as (2.6) is of degree $539 = M(6, 6, 10) = 1 + 6 + 6 + 10 + 6 \cdot 6 + 6 \cdot 10 + 10 \cdot 6 + 6 \cdot 6 \cdot 10$ as defined in (2.7) because 3, 4, and 5 are pairwise relatively prime. $T(k, S)$ over $GF(2^k)$ as defined in (2.3) have the same minimal polynomial as S for k relatively prime to $3 \cdot 4 \cdot 5$. For example, $T(7, S)$ is a 128-ary FH/TH sequence whose LC is 539.

We believe that FH/TH sequences as constructed in Corollary 2.4 must be a good candidates of FH/TH patterns in a peer-to-peer FH/TH spread spectrum communication system for the following good reasons: (i) with "large" LCs, and (ii) over "large" alphabets, but (iii) with "little" increase in the hardware complexity. Furthermore, for multi-user FH/TH communication systems, a sequence as constructed in Corollary 2.4 can be $\prod_{i=1}^{N}(p^{M^{(i)}} - 1)$ multi-user FH/TH sequences by changing the initial states of the LFSRs.

2.5 Remarks

We believe that the finite field of characteristic 2 would be a good choice for the algebraic structure of FH/TH sequences because the computations over characteristic 2 are most efficiently implemented as hardware systems and the usual practice follows this idea.

We have tried several other options but failed to extract any further reasonable behavior of non-binary FH/TH sequences over $\mathbb{F}_{p^k}$ whose minimal polynomials and therefore, LCs are uniquely determined regardless of the choice of basis other than those given in Theorem 2.1. Theorem 2.2 is slightly more general in that the p-ary k-tuple FH/TH sequences are not necessarily constructed as a k-tuple version of a p-ary sequence.

We note that Corollary 2.4 characterize those FH/TH sequence generators such that a combinatorial function sequence, S, and a resulting k-tuple sequence (an FH/TH sequence), $T(k, S)$, has the maximum possible LC for any given algebraic normal form, f, to resist the only BM attack. So, it is proper that we use the algebraic normal form, f, that has desired cryptographic properties [5] to resist other attacks than the BM attack. These cryptographic properties of a combinatorial function, i.e. a p-ary function, are discussed in the next chapter.

We note that the sequence terms of $T(k, S)$ are highly correlated with each other because t_n is the right shifted version of t_{n-1} with the only new leftmost component. This correlation between consecutive terms must be a vulnerable point to some other attacks. But, Theorem 2.1 and all corollaries in this chapter also apply equally well to $T(k, S)$ defined by

$$t_n = (s_{n-\sigma(0)}, s_{n-\sigma(1)}, \ldots, s_{n-\sigma(k-1)}), \tag{2.8}$$

where σ is any permutation on $\{0, 1, \ldots, k-1\}$. A further generalization is also possible by using any integers instead of $\sigma(i)$ for each i. Therefore, we are able to solve the correlation problem between consecutive terms by the above method.

Chapter 3

High Security p-ary Functions

We consider the cryptographic properties of p-ary functions, that is the combinatorial functions of the frequency/time hopping sequence generators proposed in the previous chapter. We are able to construct balanced p-ary functions by compositions. We are able to construct balanced p-ary functions which satisfy the propagation for the most of nonzero vectors and balanced functions which satisfy the propagation of high degree. We are able to derive a necessary condition such that p-ary functions are correlation-immune by the Fourier transforms and show that some of nonlinearity criteria are invariant under cryptographically weak transformations.

3.1 Detailed Motivation

In a frequency/time hopping (FH/TH) spread spectrum communication, an attacker may try several attacks such as a Berlekamp-Massey (BM) attack [6], a jamming [4], a linear attack [15], and a correlation attack [16] based on his information about the system. In the previous chapter, we considered the FH/TH sequence generator composed of a combinatorial function generator and some registers shown in Figure 2.4. We charac-

terized the generator whose output FH/TH sequence has the maximum possible linear complexity (LC) for the given algebraic normal form to resist the only BM attack. So, we need to characterize the algebraic normal form that has desired cryptographic properties such as the balancedness [17], the nonlinearity [18], the propagation [19], and the correlation-immunity [16] to resist other cryptographic attacks than the BM attack for high security. The relevance of these properties is based on information theoretic grounds or on specific cryptographic attacks that have their own attack scenarios. Unfortunately, it is clear that no function can satisfy all these properties. So, we consider a corresponding cryptographic property for each possible attack on a case by case basis. These cryptographic properties of Boolean functions have been intensively studied but the combinatorial function of the generator is a p-ary function, where p is a prime. Thus, we focus on the extensions of the cryptographic properties of Boolean functions to those of p-ary cases.

3.2 Jamming and Balancedness

The attacker may jam an FH communication by radiating a Gaussian noise in the partial band or a Gaussian (multi) tone. And he does not need to care about the structure of the FH sequence generator. When some of frequency slots are more probable than the others the attacker more efficiently jam the system by concentrating the limited jamming power on these slots. Intuitively, a balanced function increases the randomness, and therefore the security, of the outputs in response to random inputs. The balancedness is explicitly identified as one of the desired cryptographic properties of data encryption schemes that rely on permutations and substitutions. For example, the S-boxes of the data en-

cryption standard [20] are designed such that all their Boolean functions are balanced. Let the outputs, $s_n^{(i)},\ n = 1, 2, \ldots$, of the linear feedback shift register (LFSR) in the FH/TH sequence generator shown in Figure 2.4 be independent identically distributed (iid) discrete uniform random variables (RVs) and $s_n^{(i)},\ i = 1, 2, \ldots, N$, be mutually independent. Note that when the combinatorial function, f, is balanced the outputs, $s_n,\ n = 1, 2, \ldots$, are iid discrete uniform RVs, and therefore the FH/TH sequence, T, is balanced. It means that we have the balanced FH/TH sequence which is resistent to the partial band and (multi) tone jamming.

We extend the general theory of balanced Boolean functions given in [17]. We are able to derive a necessary condition such that a p-ary function is balanced by a bijection on the set of input vectors. We examine the composition properties of balanced p-ary functions. We are able to construct a balanced p-ary function by the disjunctive composition of balanced functions by a balanced function. We are able to characterize non-disjunctive compositions which produce balanced p-ary functions. A disjunctive composition is the composition of functions such that the arguments of the functions are disjoint. For example, the composition $f(\overline{X}) = g(f_1(\overline{X}_1),\ f_2(\overline{X}_2)) = g(f_1(X_1,\ X_2),\ f_2(X_3,\ X_4))$ is disjunctive since $\overline{X}_1 \cap \overline{X}_2 = \emptyset$. The composition $f(\overline{X}) = g(f_1(\overline{X}_2),\ f_2(\overline{X}_3)) = g(f_1(X_3,\ X_4),\ f_2(X_4,\ X_5))$ is non-disjunctive since $\overline{X}_2 \cap \overline{X}_3 = \{X_4\} \neq \emptyset$. Note that we regard a vector as the set of arguments and use the set operations.

Remind that $\mathbb{F}_q$ is the finite field with q elements and p be a prime. Let $f(\overline{X})$ be a p-ary function of a vector over $\mathbb{F}_p$. Let $|f^r|$ denote the number of input vectors, $\overline{X}$, such that $f(\overline{X}) = r$, where $r \in \mathbb{F}_p$.

Definition 3.1 A p-ary function with N arguments, $f(\overline{X})$, is balanced if and only if $|f^r| = p^{N-1}$ for all $r \in \mathbb{F}_p$.

Proposition 3.1 A p-ary function $f(\overline{X}) = X_1 + X_2 + \cdots + X_N$ is balanced and $f(\overline{X}) = X_1 X_2 \cdots X_N$ is not balanced.

The above proposition is immediate. We derive a necessary condition such that a p-ary function is balanced by a bijection on the set of input vectors, as follows.

Theorem 3.1 If a p-ary function with N arguments, $f(\overline{X})$, is balanced, then there exists a bijection, h, on the set of input vectors such that for all input vectors, $\overline{X}$, $f(\overline{X}) \neq f(h(\overline{X}))$.

Proof: Let $S_r = \{\overline{X} \in \mathbb{F}_p^N |\ f(\overline{X}) = r\}$, where $r \in \mathbb{F}_p$. Then, $|S_r| = |f^r| = p^{N-1}$. We can define a bijection h as follows: $h(\overline{X}_r) = \overline{X}_{r+1}$, where $\overline{X}_r \in S_r$, $\overline{X}_{r+1} \in S_{r+1}$, and the addition of the subscripts is over $\mathbb{F}_p$. ■

Now, we examine the composition properties of balanced p-ary functions. First, we consider disjunctive compositions and then extend the results to non-disjunctive compositions.

Proposition 3.2 A p-ary function with N arguments $f(U, \overline{X})$ is balanced if $|f(u, \overline{X})^r| = p^{N-2}$ for all pair $r,\ u \in \mathbb{F}_p$.

We construct a balanced p-ary function by the disjunctive composition of balanced functions by a balanced function.

Theorem 3.2 Let $f(\overline{X}) = g(f_1(\overline{X}_1),\ f_2(\overline{X}_2),\ \ldots,\ f_K(\overline{X}_K),\ \overline{X}_{K+1})$, where $\overline{X} = (\overline{X}_1,\ \overline{X}_2,\ \ldots,\ \overline{X}_{K+1})$ and $\overline{X}_i \cap \overline{X}_j = \emptyset$ for $1 \leq i,\ j \leq K+1$ and $i \neq j$. If p-ary functions $f_i(\overline{X}_i),\ i = 1, 2, \ldots, K$, and $g(U_1,\ U_2,\ \ldots,\ U_K,\ \overline{X}_{K+1})$ are balanced, then $f(\overline{X})$ is also balanced.

Proof: Let $|\overline{X}_i| = m_i,\ i = 1, 2, \ldots, K$, and $|\overline{X}_{K+1}| = N$. For all $r \in \mathbb{F}_p$, we have $|f_i^r| = p^{m_i - 1},\ i = 1, 2, \ldots, K$, and $|g^r| = p^{K+N-1}$. We claim that for all $r \in \mathbb{F}_p$, $|f^r| = p^{m_1+m_2+\cdots+m_K+N-1}$. Let $N^{g^r}_{U_1^{d_1}, U_2^{d_2}, \ldots, U_K^{d_K}} = |g(d_1,\ d_2,\ \ldots,\ d_K,\ \overline{X}_{K+1})^r|$.

$$\begin{aligned} |f^r| &= \sum_{d_1,d_2,\ldots,d_K} N^{g^r}_{U_1^{d_1}, U_2^{d_2}, \ldots, U_K^{d_K}} |f_1^{d_1}||f_2^{d_2}| \cdots |f_K^{d_K}| \\ &= p^{m_1+m_2+\cdots+m_K-K} \sum_{d_1,d_2,\ldots,d_K} N^{g^r}_{U_1^{d_1}, U_2^{d_2}, \ldots, U_K^{d_K}} \\ &= p^{m_1+m_2+\cdots+m_K-K}|g^r| \\ &= p^{m_1+m_2+\cdots+m_K+N-1}. \end{aligned} \tag{3.1}$$

■

Next, we characterize non-disjunctive compositions which produce balanced p-ary functions. We consider the non-disjunctive composition of p-ary functions $f_1(\overline{X}_1)$ and $g(U,\ \overline{X}_2)$ such that $\overline{X}_1 \cap \overline{X}_2 = \{X_1,\ X_2,\ \ldots,\ X_K\} \neq \emptyset$.

Theorem 3.3 Let $f(\overline{X}) = g(f_1(\overline{X}_1),\ \overline{X}_1 \cap \overline{X}_2,\ \overline{X}_2 - \overline{X}_1)$, where $f_1(\overline{X}_1)$ is a p-ary function, $\overline{X} = \overline{X}_1 \cup \overline{X}_2$, $\overline{X}_2 - \overline{X}_1 \neq \emptyset$, and $|\overline{X}_2| = N$. For any combination $\overline{d}$ of $\overline{X}_1 \cap \overline{X}_2$ and $r \in \mathbb{F}_p$, $|g(s,\ \overline{d},\ \overline{X}_2 - \overline{X}_1)^r|$ is constant for $s \in \mathbb{F}_p$. Then, $f(\overline{X}_1 \cup \overline{X}_2)$ is balanced if and only if $|g(s,\ \overline{X}_2)^r| = p^{N-1}$ for all $r,\ s \in \mathbb{F}_p$.

Proof: Let $|\overline{X}_1| = m$ and $\overline{d} = (d_1,\ d_2,\ \ldots,\ d_K)$. We have constant $N^{g^r}_{U^s, X_1^{d_1}, X_2^{d_2}, \ldots, X_K^{d_K}}$

for $s \in \mathbb{F}_p$. Then,

$$\begin{aligned} |f^r| &= \sum_{d_1,d_2,\ldots,d_K} \sum_{s} N^{g^r}_{U^s,X_1^{d_1},X_2^{d_2},\ldots,X_K^{d_K}} N^{f_1^s}_{X_1^{d_1},X_2^{d_2},\ldots,X_K^{d_K}} \\ &= \sum_{d_1,d_2,\ldots,d_K} N^{g^r}_{U^0,X_1^{d_1},X_2^{d_2},\ldots,X_K^{d_K}} \sum_{s} N^{f_1^s}_{X_1^{d_1},X_2^{d_2},\ldots,X_K^{d_K}} \\ &= p^{m-K} \sum_{d_1,d_2,\ldots,d_K} N^{g^r}_{U^0,X_1^{d_1},X_2^{d_2},\ldots,X_K^{d_K}} \\ &= p^{m-K} N^{g^r}_{U^0}. \end{aligned} \tag{3.2}$$

$f(\overline{X}_1 \cup \overline{X}_2)$ is balanced if and only if $|f^r| = p^{m+N-K-1}$. ■

In the previous theorem, we note that if $f(\overline{X}_1 \cup \overline{X}_2)$ is balanced, then $g(U,\ \overline{X}_2)$ is also balanced by Proposition 3.2. The following corollary is easily proved by the theorem.

Corollary 3.1 Let $f_2(\overline{X}_2)$ be a p-ary linear function. Then, $f(\overline{X}) = f_1(\overline{X}_1) + f_2(\overline{X}_2)$ is balanced if $\overline{X}_2 - \overline{X}_1 \neq \emptyset$.

Note that Theorem 3.3 and Corollary 3.1 are also hold when $\overline{X}_1 \cap \overline{X}_2 = \emptyset$, which is the disjunctive case. Thus, we are able to construct a balanced p-ary function by simply adding a linear function with disjoint arguments by Corollary 3.1.

3.3 Linear Attack and Propagation

When the attacker knows the structure of the FH/TH sequence generator shown in Figure 2.4 except the p-ary function, i.e. combinatorial function, he may try a linear attack which is performed by obtaining the linear approximate expression of the p-ary function.

The nonlinearity characteristics of a cryptographic function are crucial since a linear system is easily breakable by the linear attack. A perfect nonlinear Boolean function

is optimum with respect to both the minimum distance to affine functions and therefore a resistance to the linear attack [18]. And this function was generalized to a perfect nonlinear p-ary function in [21], which coincides with a p-ary bent function defined in [22]. Unfortunately, a perfect nonlinear p-ary function is not be compatible with other desired cryptographic properties, e.g. the balancedness. The perfect nonlinearity of a p-ary function is generalized to a propagation [19], which is the randomness measure of the differences of outputs for the differences of inputs. It is one of the most important nonlinearity criteria because the differential cryptanalysis [23], which is one of the successful attacks, utilizes the bias of the distribution of the difference of outputs and the difference of inputs. Furthermore, some p-ary functions satisfy both the propagation and the balancedness. The propagation characteristics of a balanced Boolean function were discussed in [24]. We are able to define the propagation of a p-ary function by the Fourier transform. We are able to construct a balanced p-ary function which satisfies the propagation for the most of nonzero vectors. Furthermore, We are able to construct a balanced p-ary function which satisfies the propagation of high degree.

Let $f(\overline{X})$ be a p-ary function with N arguments. Let $W(\overline{A})$ denote the number of the nonzero components of $\overline{A}$, i.e. the Hamming weight of $\overline{A}$. The autocorrelation function of $f(\overline{X})$ is defined as follows [21]

$$r(\overline{A}) = \sum_{\overline{X} \in \mathbb{F}_p^N} \sigma^{f(\overline{X}+\overline{A})-f(\overline{X})}, \tag{3.3}$$

where $\sigma = e^{i\frac{2\pi}{p}}$, i.e. the primitive p-th root of unity in the complex field.

Definition 3.2 A p-ary function $f(\overline{X})$ satisfies the propagation of degree l if for all

vector $\overline{A}$ with $1 \leq W(\overline{A}) \leq l$

$$f(\overline{X} + \overline{A}) - f(\overline{X}) \tag{3.4}$$

is balanced, that is $r(\overline{A}) = 0$.

Thus, the strict avalanche criterion [25] is the propagation of degree one and the perfect nonlinearity is the propagation of degree N. The Fourier transform of $\sigma^{f(\overline{X})}$ is defined as follows [21]

$$F(\overline{\omega}) = \sum_{\overline{X} \in \mathbb{F}_p^N} \sigma^{f(\overline{X}) - \overline{\omega} \cdot \overline{X}}. \tag{3.5}$$

We define the propagation of a p-ary function by the Fourier transform. The strict avalanche criterion version for the binary case is given in [25].

Theorem 3.4 A p-ary function $f(\overline{X})$ satisfies the propagation of degree l if and only if for all vector $\overline{A}$ with $1 \leq W(\overline{A}) \leq l$

$$\sum_{\overline{\omega} \in \mathbb{F}_p^N} |F(\overline{\omega})|^2 \sigma^{\overline{\omega} \cdot \overline{A}} = 0 \tag{3.6}$$

Proof: The Fourier transform of the autocorrelation function of $f(\overline{X})$ is given by

$$R(\overline{\omega}) = |F(\overline{\omega})|^2. \tag{3.7}$$

Thus, its inverse Fourier transform and Definition 3.2 completes the proof. ■

Corollary 3.2 If a p-ary function $f(\overline{X})$ satisfies the propagation of degree l then $g(\overline{X}) = f(\pi(\overline{X}) + \overline{A})$ also satisfies it for a permutation operator π and $\overline{A} \in \mathbb{F}_p^N$.

Now, we construct a balanced p-ary function which satisfies the propagation for the most of nonzero vectors from the bent function which is not balanced. Let g be the p-ary bent function, i.e. perfect nonlinear function, with N arguments and f be given by

$$f(X_1,\ X_2,\ \ldots,\ X_{N+2}) = a_1X_1 + a_2X_2 + a_3g(X_3,\ X_4,\ \ldots,\ X_{N+2}), \tag{3.8}$$

where a_1, a_2, and a_3 are nonzero elements in $\mathbb{F}_p$.

Theorem 3.5 A p-ary function $f(\overline{X})$ with $N+2$ arguments defined in (3.8) is balanced and satisfies the propagation for all nonzero vectors $\overline{A} \in \mathbb{F}_p^{N+2}$ with $\overline{A} \neq (c_1,\ c_2,\ 0,\ 0,\ \ldots,\ 0)$.

Next, let f be given by

$$f(X_1,\ X_2,\ \ldots,\ X_{N+1}) = a_1X_1 + a_2g(X_2,\ X_3,\ \ldots,\ X_{N+1}), \tag{3.9}$$

where a_1 and a_2 are nonzero elements in $\mathbb{F}_p$.

Theorem 3.6 A p-ary function $f(\overline{X})$ with $N+1$ arguments defined in (3.9) is balanced and satisfies the propagation for all nonzero vectors $\overline{A} \in \mathbb{F}_p^{N+1}$ with $\overline{A} \neq (c,\ 0,\ 0,\ \ldots,\ 0)$.

The proofs of Theorem 3.5 and Theorem 3.6 are analogous to those of the binary cases given in [26]. When $p = 2$ the lower bounds of the minimum distances to affine functions of the constructed functions in the above two theorems are given in [26]. We note that the p-ary bent function with odd arguments does not exist for $p = 2$. Thus, Theorem 3.5 construct the function with even arguments and Theorem 3.6 with odd arguments for the binary case. We construct a balanced p-ary function with $N+1$ arguments which satisfies the propagation of degree N from the bent function. Let f^* be given by

$$\begin{aligned} f^*(X_1,\ X_2,\ \ldots,\ X_{N+1}) = a_1X_1 + g(&a_2X_1 + b_2X_2,\ a_3X_1 + b_3X_3,\\ &\ldots,\ a_{N+1}X_1 + b_{N+1}X_{N+1}), \end{aligned} \tag{3.10}$$

where a_i and $b_i,\ i = 1, 2, \ldots, N$, are nonzero elements in $\mathbb{F}_p$ and $a_i + b_i = 0$.

Corollary 3.3 A p-ary function $f^*(\overline{X})$ with $N+1$ arguments defined in (3.10) is balanced and satisfies the propagation of degree N.

Proof: Consider $f(\overline{X})$ defined in (3.9) for $a_1 = a_2 = 1$, then $f^*(\overline{X}) = f(\overline{X}\mathbf{M})$, where $\mathbf{M}$ is a nonsingular matrix given by

$$\mathbf{M} = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{2h+1} \\ 0 & b_2 & 0 & \cdots & 0 \\ 0 & 0 & b_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_{2h+1} \end{bmatrix} \tag{3.11}$$

$f^*(\overline{X})$ is balanced since $\overline{X}\mathbf{M}$ is the bijection on $\mathbb{F}_p^{N+1}$ and $f(\overline{X})$ is balanced by Theorem 3.6.

$$f^*(\overline{X} + \overline{A}) - f^*(\overline{X}) = f(\overline{X}\mathbf{M} + \overline{A}\mathbf{M}) - f(\overline{X}\mathbf{M}) \tag{3.12}$$

The above function is balanced when $\overline{A}\mathbf{M} \neq (c,\ 0,\ 0,\ \ldots,\ 0)$, where $c \neq 0$ by Theorem 3.6. Thus, $f^*(\overline{X})$ satisfies the propagation for all nonzero vectors $\overline{A} \in \mathbb{F}_p^{N+1}$ with $\overline{A} \neq (c,\ c,\ \ldots,\ c)$ ■

We are able to construct a p-ary function which satisfies both the balancedness and the propagation of high degree by Corollary 3.3. Note that Corollary 3.3 holds when $g(\cdot)$ in (3.10) is multiplied by a nonzero constant since $f(\overline{X})$ such that $f^*(\overline{X}) = f(\overline{X}\mathbf{M})$ always exists.

3.4 Correlation Attack and Correlation-Immunity

Assume that the structure of the FH/TH sequence generator shown in Figure 2.4 is known except a key $K^{(i)},\ i = 1, 2, \ldots, N$, which determines the initial state of an i-th LFSR. Then, the attacker may try a correlation attack which is performed by correlating the combinatorial function sequence S with the i-th LFSR's sequence $S^{(i)}$ to choose $K^{(i)}$. In some cases, there may be no correlation between any $S^{(i)}$ and S but correlation between the combination of $S^{(i)},\ i = 1, 2, \ldots, N$ and S. In this case, a high order correlation attack is still possible. Thus, to make the generator resistent to the correlation attack we must use a p-ary function, i.e. combinatorial function, which guarantees that there is no correlation between any combination of LFSRs' sequences and the combinatorial function sequence.

Since Siegenthaler introduced the concept of correlation-immune Boolean functions in [16], many results have been presented on the various aspects of the correlation-immunity. The recursive constructions of correlation-immune functions were proposed in [16], [27], and [28]. Especially, the constructions proposed in [28] are for a q-ary correlation-immune function. The equivalent definition of a correlation-immune Boolean function by the Fourier transform was proposed in [29]. Another equivalent definition by orthogonal arrays was proposed in [27] and generalized in [30].

We examine the general relation between a correlation-immune p-ary function and the Fourier transform. We are able to derive a necessary condition such that a p-ary function is correlation-immune by the Fourier transform. We are able to characterize a first order correlation-immune function by its balancedness property.

Let $Z = f(\overline{X})$ be a discrete RV produced by f, where $\overline{X} = (X_1, , X_2, \ \ldots, \ X_N)$ and $X_i, \ i = 1, 2, \ldots, N$, be mutually independent discrete uniform RVs.

Definition 3.3 [16] A p-ary function $f(\overline{X})$ is m-th order correlation-immune if $Z = f(\overline{X})$ is independent of every subset of m random variables chosen from $X_1, \ X_2, \ \ldots, \ X_N$.

Definition 3.4 [30] A balanced m-th order correlation-immune function is called m-th order resilient.

The following lemma is well known as the linear combination lemma.

Lemma 3.1 [30] A discrete random variable Y is independent of m mutually independent random variables $Y_1, \ Y_2, \ \ldots, \ Y_m$ if and only if Y is independent of the sum $\lambda_1 Y_1 + \lambda_2 Y_2 + \cdots + \lambda_m Y_m$ for every choice of $\lambda_1, \ \lambda_2, \ \ldots, \ \lambda_m$ with not all zeros in $\mathbb{F}_p$, that is Y is independent of any non-trivial linear combination of the m variables.

Because all p^{N-1} values $\overline{x}$ of $\overline{X}$ such that $\overline{\omega} \cdot \overline{x} = b \in \mathbb{F}_p$ are equally likely,

$$P_{Z|\overline{\omega}\cdot\overline{X}}(a|b) = \frac{N_{f=a,\overline{\omega}\cdot\overline{X}=b}(\overline{\omega})}{p^{N-1}}, \tag{3.13}$$

where $N_{f=a,\overline{\omega}\cdot\overline{X}=b}(\overline{\omega})$ denotes the number of $\overline{X}$ such that $f(\overline{X}) = a$ and $\overline{\omega} \cdot \overline{X} = b$. Now, we derive a necessary condition such that a p-ary function is correlation-immune by the Fourier transform.

Theorem 3.7 If a p-ary function $f(\overline{X})$ is m-th order correlation-immune, then the Fourier transform of $\sigma^{f(\overline{X})}$ satisfies $F(\overline{\omega}) = 0$ for $1 \leq W(\overline{\omega}) \leq m$.

Proof: By Definition 3.3, $f(\overline{X})$ is m-th order correlation-immune if and only if Z is independent of every subset of m or fewer RVs chosen from $X_1, \ X_2, \ \ldots, \ X_N$. By

Lemma 3.1, it follows that $f(\overline{X})$ is m-th order correlation-immune if and only if Z is independent of every $\overline{\omega} \cdot \overline{X}$ for $1 \leq W(\overline{\omega}) \leq m$. Equation (3.13) shows that Z is independent of $\overline{\omega} \cdot \overline{X}$ just when $N_{f=a,\overline{\omega}\cdot\overline{X}=b}(\overline{\omega})$ is constant for b. Thus, $f(\overline{X})$ is m-th order correlation-immune if and only if $N_{f=a,\overline{\omega}\cdot\overline{X}=b}(\overline{\omega})$ is constant for b, where $1 \leq W(\overline{\omega}) \leq m$. By this necessary and sufficient condition, if $f(\overline{X})$ is m-th order correlation-immune, then

$$\begin{aligned} F(\overline{\omega}) &= \sum_{\overline{X}\in\mathbb{F}_p^N} \sigma^{f(\overline{X})-\overline{\omega}\cdot\overline{X}} \\ &= \sum_{a\in\mathbb{F}_p} \sum_{b\in\mathbb{F}_p} N_{f=a,\overline{\omega}\cdot\overline{X}=b}(\overline{\omega})\sigma^{a-b} \\ &= \sum_{a\in\mathbb{F}_p} N_{f=a}(\overline{\omega}) \sum_{b\in\mathbb{F}_p} \sigma^{a-b} \\ &= \sum_{a\in\mathbb{F}_p} N_{f=a}(\overline{\omega}) \cdot 0 \\ &= 0, \end{aligned} \tag{3.14}$$

where $1 \leq W(\overline{\omega}) \leq m$. ■

We note that the converse of Theorem 3.7 holds provided that $p = 2$ [29]. We characterize a first order correlation-immune function by the following balancedness property. Remind notations given in Section 3.2.

Definition 3.5 [17] A p-ary function, $f(\overline{X})$, is balanced with respect to X_i if and only if $|f(X_1,\ \ldots,\ X_{i-1},\ b,\ X_{i-1},\ \ldots,\ X_N)^a| = \frac{1}{p}|f^a|$ for all pair $a,\ b \in \mathbb{F}_p$.

Proposition 3.3 A p-ary function, $f(\overline{X})$, is first order correlation-immune if and only if it is balanced with respect to all $X_i,\ i = 1, 2, \ldots, N$.

Proof: Equation (3.13) for $W(\overline{\omega}) = 1$ completes the proof. ■

We have tried to generalize the several construction methods of a correlation-immune Boolean function to those of p-ary cases, but unfortunately failed.

3.5 Invariant Nonlinearity Criteria

Recent progress in cryptanalysis, especially the discovery of a linear attack [15], has highlighted the nonlinearity characteristics of Boolean functions. Well-known nonlinearity criteria include the minimum distance to affine functions [18] [31], the minimum distance to Boolean functions with linear structures [18], the nonlinear order [18], the strict avalanche criterion [19], the propagation [19], and the correlation-immunity [16]. In cryptography, a function is considered weak when it can be turned into a cryptographically weak function by means of simple (e.g. linear or affine) transformations. From this viewpoint, a useful nonlinearity criterion should be invariant under the large group of transformations. For many applications this symmetry group should contain the group of all affine transformations. Thus, it is worthy to characterize nonlinearity criteria which are invariant under the group of all affine transformations.

We extend the result given in [18] to those of p-ary cases regarding invariant nonlinearity criteria. We are able to show that the minimum distance to affine functions, the minimum distance to functions with linear structures, the minimum distance to functions of nonlinear order k, and the nonlinear order of a p-ary function are invariant under the group of all affine transformations.

We note that the lemmas and corollaries of this section are presented without proofs since they are direct extensions of the results given in [18] to those of p-ary cases. First, we examine the minimum distance to affine functions of a p-ary function. Remind that

$f(\overline{X})$ is a p-ary function with N arguments. Let $A(N)$ denote the set of all p-ary affine functions $L(\overline{X}) = c_0 + c_1X_1 + c_2X_2 + \ldots + c_NX_N$, where $L(\overline{X}) \in \mathbb{F}_p$ and $c_i \in \mathbb{F}_p,\ i = 0, 1, \ldots,\ N$. Let $d(f,\ L)$ denote the Hamming distance, that is the number of differences, between f and L.

Definition 3.6 [18] The minimum distance, $\delta(f)$, to affine functions of a p-ary function, $f(\overline{X})$, is given by

$$\delta(f) = \min_{L \in A(N)} d(f,\ L). \tag{3.15}$$

$\delta(f)$ is generally called the nonlinearity of f. Let $\Omega(N)$ denote the group of all invertible transformations, i.e. bijections, on $\mathbb{F}_p^N$, $AGL(N)$ denote the subgroup with all affine transformations of $\Omega(N)$, and $\Phi(N)$ denote the set of all p-ary functions, $f(\overline{X})$. The operation of the group $\Omega(N)$ on the set $\Phi(N)$ is defined as

$$\alpha(f(\overline{X})) = f(\alpha(\overline{X})), \tag{3.16}$$

where $\alpha \in \Omega(N)$ and $f(\overline{X}) \in \Phi(N)$. Any design criterion is connected with a function D, given by

$$D :\ \Phi(N) \to V, \tag{3.17}$$

where V is the set of suitable values for the criterion. f is considered to be good if the value $D(f)$ belong to the desired subset of V. It must be essential for the criterion that $D(f)$ is invariant under those transformations of $\Omega(N)$ which are considered cryptographically weak. This guarantees that a good function cannot be made worse by means of weak transformations. For nonlinearity criteria, weak transformations usually include affine transformations. For any design criterion, it is of interest to introduce the largest

subgroup $I(D)$ which leaves D invariant, given by

$$I(D) = \{\alpha \in \Omega(N) |\ D(\alpha(f)) = D(f)\ for\ all\ f \in \Phi(N)\}. \tag{3.18}$$

We call $I(D)$ the symmetry group of D. It must be essential that $I(D)$ is large. Let H be the subset of $\Phi(N)$ and $d_H(f)$ be the minimum distance of f to the set H, where $f \in \Phi(N)$. Moreover, let

$$\Omega(N)^H = \{\alpha \in \Omega(N) |\ \alpha(h) \in H\ for\ all\ h \in H\}, \tag{3.19}$$

which is called the symmetry group of the set H. This terminology is justified by the following theorem.

Theorem 3.8 For any subset H of $\Phi(N)$ the symmetry group of d_H coincides with the symmetry group of H, i.e.

$$I(d_H) = \Omega(N)^H. \tag{3.20}$$

We show that the minimum distance to affine functions of a p-ary function is invariant under all operations of the affine group $AGL(N)$.

Corollary 3.4 The symmetry group, $I(\delta)$, of the minimum distance to affine functions, δ, is the affine group, $AGL(N)$.

Now, we consider the minimum distance to p-ary functions with linear structures. In certain applications the class of affine functions has to be extended to another class of cryptographically weak functions. The definition of these functions is motivated by the fact that for an affine p-ary function $L(\overline{X} + \overline{A})$ and $L(\overline{X})$ always have the same difference for all $\overline{X}$, where $\overline{A}$ is fixed. However, note that many functions except all

affine functions have this property, which is termed a linear structure [32]. The linear structure of a p-ary function can be identified with a vector $\overline{A}$ such that the expression

$$f(\overline{X} + \overline{A}) - f(\overline{X}) \tag{3.21}$$

has the same value for all $\overline{X}$ [18]. Let $LS(N)$ denote the set of p-ary functions which have linear structures. Observe that $LS(N)$ properly contains the set of all affine functions, $A(N)$.

Definition 3.7 [18] The minimum distance, $\eta(f)$, to functions with linear structures of a p-ary function, $f(\overline{X})$, is given by

$$\eta(f) = \min_{S \in LS(N)} d(f,\ S). \tag{3.22}$$

We show that the minimum distance to functions with linear structures of a p-ary function is invariant under all operations of the affine group, $AGL(N)$.

Corollary 3.5 The symmetry group, $I(\eta)$, of the minimum distance to functions with linear structures, η, contains the affine group, $AGL(N)$.

Now, we consider a polynomial whose argument is $X_1,\ X_2,\ \ldots,\ X_N$, that is the generalized algebraic normal form. Any p-ary function can be represented as this generalized algebraic normal form.

Definition 3.8 [18] The nonlinear order, $\zeta(f)$, of a p-ary function, $f(\overline{X})$, is the degree of the highest order term in its generalized algebraic normal form.

The following theorem shows that the nonlinear order of a p-ary function is invariant under all operations of the affine group, $AGL(N)$.

Theorem 3.9 The symmetry group, $I(\zeta)$, of the nonlinear order, ζ, is the affine group, $AGL(N)$.

Let $\delta_k(f)$ denote the minimum distance to functions of nonlinear order k. Note that $\delta(f) = \delta_1(f)$. Then, the following theorem shows that the minimum distance to functions of nonlinear order k is invariant under all operations of the affine group, $AGL(N)$.

Theorem 3.10 The symmetry group, $I(\delta_k)$, of the minimum distance to functions of nonlinear order k, δ_k, contains the affine group, $AGL(N)$.

3.6 Remarks

In chapter 2, we proposed the FH/TH generators which are resistent to the only BM attack. So, we considered the desired cryptographic properties of p-ary functions, that is the combinatorial functions of the generator, to resist other cryptographic attacks than the BM attack for high security. These cryptographic properties of Boolean functions have been intensively studied. Thus, we considered the extensions of the cryptographic properties of Boolean functions to those of p-ary cases.

On the same assumption as that of the correlation attack, an attacker may try an efficient algebraic attack by multiplying the combinatorial function f by a well-chosen multivariate polynomial [33]. If we increase the order of F_p, the monomials of linear equations to be solved will considerably increase and so the FH/TH sequence generator may be more resistent to the algebraic attack.

We have tried but failed to extend the several other properties of Boolean functions.

We note that it is mainly due to the fact that the p-ary field is more mathematically difficult to characterize than the binary field.

Chapter 4

Coded N-ary Pulse Position Modulated Ultra-Wide Bandwidth Impulse Radios

We consider a coded N-ary pulse position modulated ultra-wide bandwidth (UWB) impulse radio, which exploits the chaotic inter-pulse intervals in the framed-time structure and the polarity randomization for the coexistence with conventional narrow bandwidth wireless communication systems. We show that the proposed system has noise-like spectrum, that is line spectrum free, by calculating its power spectral density function. We discuss its multi-user system with its line spectrum property. Then, we confirm the bit error rate performance of the proposed system by simulation based on the UWB indoor channel model.

4.1 Detailed Motivation

There have been large interests in recent years in exploiting chaotic signals in communications [34]. The main premise in these studies is that broad-band signals gen-

erated by simple deterministic systems with chaotic dynamics can potentially replace pseudo-random carrier signals widely used in modern spread-spectrum communication systems. A chaotic pulse position modulation (CPPM) was proposed in [35], which encodes the information in a pulse train by the alteration of the time positions of pulses. This system avoids the difficulties, e.g. sensitivities to distortions and noise, of most other chaos-based communication schemes by using chaotically (aperiodically) timed pulse sequences rather than continuous chaotic waveforms.

And it belongs to the general class of time hopping (TH) ultra-wide bandwidth (UWB) impulse radio (IR) communications, which has been intensively studied for short range multiple-access communications in dense multipath environments because of its fine time resolution properties [7]. This radio has some other attractive advantages compared with conventional narrow bandwidth wireless communication systems, such as low hardware complexity, low power consumption, and multi-user capability than immunity to multipath fading. We note the UWB-IR as the example of commercial TH spread spectrum communication systems because this radio adopt a TH binary pulse position modulation (PPM) for multi-user communications. This radio communicates with the baseband pulses of ultra short duration ($<$1ns), i.e. impulses, thereby spreading the energy of the radio signal very thinly from d.c. to several gigahertz. Because of this extremely large bandwidth, the UWB-IR and conventional narrow bandwidth systems cannot help giving interference to each other, and furthermore, a UWB-IR signal accompanies line spectrums giving large interference to the conventional systems. Therefore, the reduction and management of the line spectrums of the UWB-IR signal is an essential problem to be solved for coexistence with the conventional narrow bandwidth systems.

Some analyses of the power spectral density (PSD) function and line spectrums of the UWB-IR signal resulted in some criteria for the reduction of line spectrums depending on TH sequences and modulation schemes [7] [36] [37] [38] [39].

We note that a possible solution is to make the UWB-IR work in lower signal to noise ratio (SNR) at the same data rate and bit error rate (BER). A coded N-ary PPM UWB-IR was proposed in [40], which uses the convolutional codes of low complexities for coding gains, but the line spectrum properties of the system have not been analyzed. A pseudo chaotic time hopping (PCTH) UWB-IR was proposed in [41], which combines the chaotically varying spacing between pulses like the CPPM with the framed-time structure. And its structure is an N-ary PPM UWB-IR combined with a PCTH code based on the symbolic dynamics of a chaotic map. This radio intends to coexist with conventional narrow bandwidth systems by both working in lower SNR at the same data rate and BER due to the code and having the enhanced spread-spectrum characteristics, that is the reduced number of line spectrums, rather than conventional TH UWB-IRs due to a chaotic (aperiodic) TH sequence removing periodic structures from the signal. As an alternative to the PCTH, an interleaved convolutional time hopping UWB-IR was discussed in [42]. This radio replaces the PCTH code by an optimum convolutional code (from the viewpoint of free distances) to improve a BER performance preserving the line spectrum properties. Unfortunately, this radio does not have a coding gain compared to the uncoded system because of using not the soft but the hard Viterbi decoder.

In this chapter, we also consider a coded N-ary PPM UWB-IR, which exploits the chaotic inter-pulse intervals in the framed-time structure like the PCTH and the polarity randomization discussed in [39] for the coexistence. We show that the proposed system

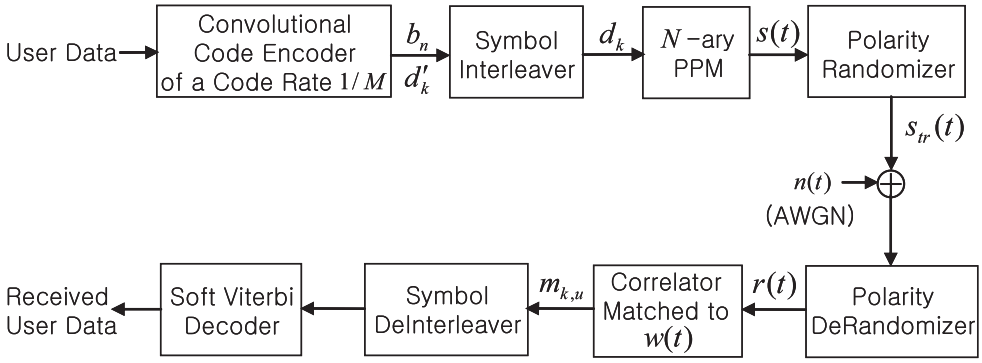


Figure 4.1: Coded N-ary PPM UWB-IR.

has noise-like spectrum, that is line spectrum free, by calculating its PSD function. We discuss its multi-user system, which assigns a user signature sequence [43] to each user as a multi-user sequence, with its line spectrum property. Then, we confirm the BER performance of the proposed system by simulation based on the UWB-IR indoor channel model given in [8].

4.2 System Structure

We consider the coded N-ary PPM UWB-IR shown in Figure 4.1. This radio uses a convolutional code whose outputs' linear equations are linearly independent. We can improve a BER performance by using a good convolutional code rather than the PCTH code. Note that $N = 2^M$ and $T_f = N \times T_s$, where T_f is a frame time and T_s is a slot time. The symbol, $d'_k \in \{0,\ 1,\ \ldots,\ N-1\}$, can be determined by reading each successive M output bits, b_n, in decimal as follows

$$d'_k = \sum_{i=0}^{M-1} b_{Mk+i} 2^i. \tag{4.1}$$

We assume that the user data are independent identically distributed (iid) discrete uniform random variables (RVs). Then, d'_k given in (4.1) are not iid because of a correlation between successive terms but uniform to improve the security by the linear independence of output bits. The time slot index, d_k, can be iid discrete uniform RVs by interleaving d'_k. Thus, a pulse is purely randomly distributed in T_f and a spacing between pulses varies chaotically, that is a chaotic time hopping. The transmitted signal is given by

$$s_{tr}(t) = \sum_{i=-\infty}^{\infty} p_i \times w(t - iT_f - d_i T_s), \tag{4.2}$$

where $p_i \in \{-1,\ 1\}$ is a polarity randomization sequence and $w(t)$ is a transmit pulse. In this paper, we use the second derivative of the Gaussian function for $w(t)$. The output of the correlator in the receiver for a u-th time slot in a k-th frame time is given by

$$m_{k,u} = \int_{kT_f+(u-\frac{1}{2})T_s}^{kT_f+(u+\frac{1}{2})T_s} r(t) \times w(t - kT_f - uT_s)\, dt. \tag{4.3}$$

A vector $\overline{m}_k = (m_{k,0},\ m_{k,1},\ \ldots,\ m_{k,N-1})$ is deinterleaved and $m_{k,u}$ is used as the soft branch metric of a branch whose output is u in decimal in the following soft Viterbi decoder. We note that not the hard but the soft Viterbi decoding has a coding gain in the coded N-ary PPM UWB-IR.

4.3 Line Spectrum Properties

Without the polarity randomizer, the line spectrums of the transmitted signal, $s(t)$, would exist at every $1/T_s$ Hz [44]. These are the same line spectrum properties as those of the PCTH UWB-IR and these sparse lines can be set to fall outside the useful bandwidth by design [41]. Though, signals that cause line spectrums are highly undesirable since they

have a high peak PSD function. They hardly guarantee the low probability of detection (LPD) and have to back off the average power until the peak of the spectrum complies with the spectral mask established by the Federal Communication Commission (FCC) [45]. We are able to eliminate these lines by using the polarity randomization discussed in [39]. After the polarity randomization, the transmitted signal, $s_{tr}(t)$, is similar to that of joint PPM/pulse amplitude modulation (PAM) but the sign of the transmit pulse does not bear any information. The PSD function of an N-ary modulated signal with an iid input sequence is given by [46]

$$\begin{aligned}\Phi(f) =& \frac{1}{T^2}\sum_{n=-\infty}^{\infty}\left\{\left|\sum_{i=0}^{N-1} P_i \cdot S_i\left(\frac{n}{T}\right)\right|^2 \delta\left(f-\frac{n}{T}\right)\right\} \\ &+ \frac{1}{T}\left\{\sum_{i=0}^{N-1} P_i \cdot |S_i(f)|^2 - \left|\sum_{i=0}^{N-1} P_i \cdot S_i(f)\right|^2\right\},\end{aligned} \tag{4.4}$$

where T is a symbol period, $S_i(f)$ is the Fourier transform of an i-th symbol, $s_i(t)$, of the constellation, P_i is the marginal probability of the i-th symbol, and $\delta(\cdot)$ is the Kronecker delta function. We assume that the polarity randomization sequence, which is actually a long pseudorandom sequence, is iid uniform RVs. Then, the transmitted signal, $s_{tr}(t)$, can be treated as a pulse train with equiprobable $2N$ antipodal symbols. From (4.4), the PSD function of $s_{tr}(t)$ is as follows

$$\begin{aligned}\Phi_{s_{tr}}(f) &= \frac{1}{T}\sum_{i=0}^{2N-1} P_i \cdot |S_i(f)|^2 \\ &= \frac{1}{N\cdot T}\sum_{i=0}^{N-1} |S_i(f)|^2 \\ &= \frac{1}{T_f}|W(f)|^2,\end{aligned} \tag{4.5}$$

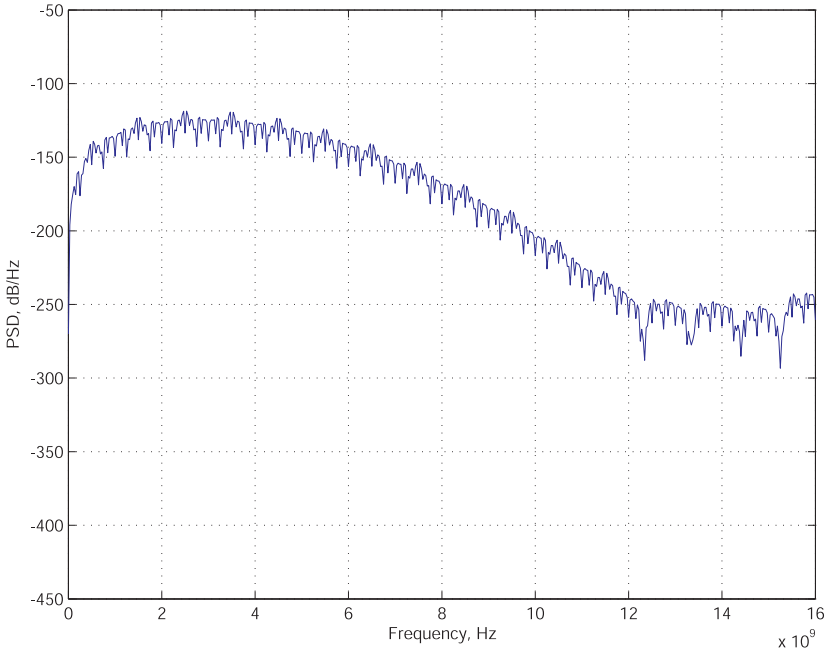


Figure 4.2: Actual PSD function for $N = 32$, $T_f = 32$ns, $T_s = 1$ns, and $E_s = 1$W/Hz.

where $T = T_f$, $s_i(t) = w(t - iT_s)$, $s_{i+N}(t) = -s_i(t)$, $i = 0,\ 1,\ \ldots,\ N - 1$, and $W(f)$ is the Fourier transform of $w(t)$. Thus, the proposed system has no line spectrums and the shape of its PSD function is determined by the transmit pulse, $w(t)$. When T_s is fixed, we can get lower PSD function by increasing N, that is increasing T_f. This results in the compliance with the FCC mask, an improved LPD, and an improved BER performance in the case of orthogonal PPM. Figure 4.2 shows the actual PSD of the system by Matlab.

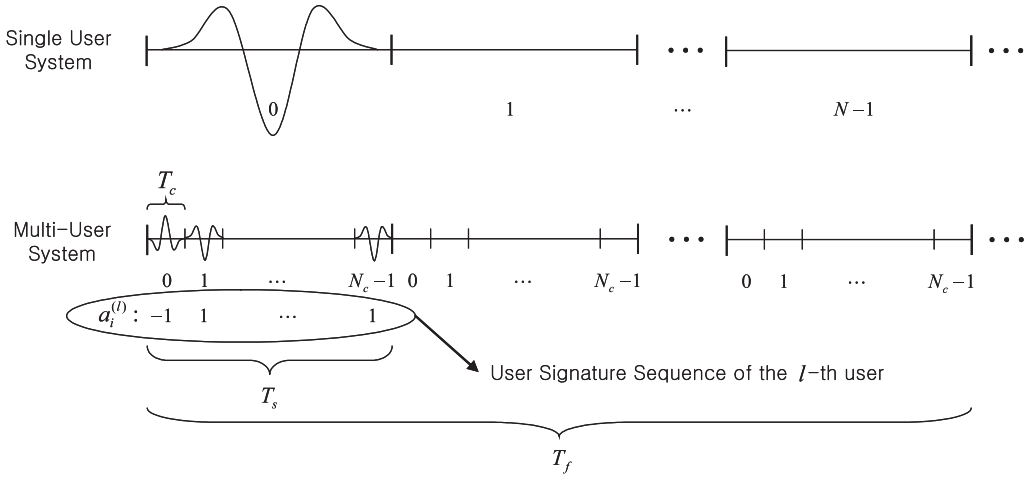


Figure 4.3: Transmitted signals of the proposed systems.

4.4 Multi-User System

In multi-user communications, an l-th user uses his own sequence of pulses for the transmit pulse like in code division multiple access schemes, given by

$$w^{(l)}(t) = \sum_{i=0}^{N_c-1} a_i^{(l)} \times w(t - iT_c), \tag{4.6}$$

where $a_i^{(l)} \in \{1, \ -1\}$, $i = 0, \ 1, \ \ldots, \ N_c - 1$, is the user signature sequence [43] of the l-th user and T_c is a chip time. Then, the transmitted signal of the l-th user is given by

$$s_{tr}^{(l)}(t) = \sum_{i=-\infty}^{\infty} p_i \times w^{(l)}(t - iT_f - d_i^{(l)} T_s), \tag{4.7}$$

where $d_i^{(l)}$ is a time slot index in an i-th frame time. Figure 4.3 shows the transmitted signals of the single user and the multi-user system. A receiver structure for the l-th user is the same as that of the single user system except that the correlator is matched to

$w^{(l)}(t)$ given in (4.6) not $w(t)$. The PSD function of the transmitted signal can calculated similarly to the case of the single user system as follows

$$\begin{aligned}\Phi_{s_{tr}^{(l)}}(f) &= \frac{1}{T_f}\left|W^{(l)}(f)\right|^2 \\ &= \frac{1}{T_f}\left|W(f)\right|^2 C^{(l)}(f),\end{aligned} \tag{4.8}$$

where $W^{(l)}(f)$ is the Fourier transform of $w^{(l)}(t)$ and

$$C^{(l)}(f) = \left|\sum_{i=0}^{N_c-1} a_i^{(l)} \exp[-j2\pi f i T_c]\right|^2 \tag{4.9}$$

which is dependent on the user signature sequence. The multi-user system also has no line spectrums and the shape of its PSD function is dependent on both the basic pulse and the user signature sequence.

Considering the multi-user interferences of the other users, the BER performance of the system mainly depends on the crosscorrelation properties of user signature sequences. A Hadamard matrix [47], $\mathbf{H}$, of order n is a square matrix with all entries in $\{1, -1\}$ such that

$$\mathbf{H}\mathbf{H}^t = n\mathbf{I_n}, \tag{4.10}$$

where $\mathbf{H}^t$ is the transpose of $\mathbf{H}$ and $\mathbf{I_n}$ is the identity matrix of order n. This implies that any two rows of $\mathbf{H}$ are orthogonal. Therefore, the rows of Hadamard matrix can be good candidates for the user signature sequences. When the slot time is synchronized (not necessarily frame time), that is the case of a forward link, the BER performance of the system is the same as that of the single user system by the optimum crosscorrelation properties of the sequences given in (4.10). By the way, when the slot time is not synchronized but the chip time is synchronized, that is the case of a reverse link, the rows

of Hadamard matrix do not guarantee the same good BER performance. In this case, the user signature sequences with optimal aperiodic crosscorrelation properties are necessary. A Welch-optimum family that is optimized with respect to mean-square aperiodic correlations [48] can be a good candidate.

4.5 UWB-IR Indoor Channel

The channels of personal wireless communications which are important application areas for UWB-IRs are dense multipath channels. The performance analyses of the UWB-IRs in multipath environments are usually based on narrowband channel models or straightforward extensions to finer delay resolutions that, however, markedly differ from empirical UWB-IR channels in the distribution of path gains. To confirm the BER performance, we use the UWB-IR indoor channel model given in [8] by the statistical analysis of UWB-IR channel data obtained from an extensive measurement in a typical modern office environment. A path loss, PL, is the function of a distance, d, between a transmitter and a receiver, given by

$$PL = \begin{cases} 20.4 \times \log_{10} d & \text{if } d \leq 11\text{m} \\ -56 + 74 \times \log_{10} d & \text{if } d > 11\text{m} \end{cases}. \tag{4.11}$$

A total power gain, G_t, is lognormally distributed with a mean $-PL$ and a standard deviation 4.3, denoted by

$$G_t = L_N(-PL,\ 4.3) \tag{4.12}$$

A decay constant, ε, and a power ratio, r, are also lognormal RVs, given by

$$\varepsilon = L_N(16.1,\ 1.27) \tag{4.13}$$

$$r = L_N(-4,\ 3) \tag{4.14}$$

The power delay profile, $g(\tau)$, of the channel is given by

$$\begin{aligned} g(\tau) = & \frac{G_t}{1 + rF(\varepsilon)} \\ & \times \left\{ \delta(\tau - \tau_1) + \sum_{k=2}^{N_{bin}} r \exp\left[-(\tau_k - \tau_2)/\varepsilon\right] \delta(\tau - \tau_k) \right\}, \end{aligned} \tag{4.15}$$

where

$$F(\varepsilon) = \frac{1}{1 - \exp[-\Delta\tau/\varepsilon]}, \tag{4.16}$$

a bin width $\Delta\tau = 2$ns, a delay $\tau_k = (k-1)\Delta\tau$, and N_{bin} is the total number of bins in an observation window whose width is 5ε.

4.6 Simulation Results

Figure 4.4 and Figure 4.5 show the BER performance of the proposed single user system. The proposed system uses the optimum convolutional code, whose outputs' linear equations are linearly independent, of the same code rate $1/5$ and constraint length 5 as those of the PCTH code of the 32-ary PCTH UWB-IR, respectively. An uncoded system transmits a pulse 5 times for each time slot index and uses the majority vote decoding for the same data rate, R_d, as that of a coded system. Figure 4.4 shows the BER performance in the additive white Gaussian noise (AWGN) channel. The proposed system and the PCTH UWB-IR have the almost same BER curve and about 3dB gain at BER=10^{-6} in the AWGN channel. Figure 4.5 shows the BER performance in the UWB-IR indoor channel described in the previous section. The figure (a) and (b) shows the performance when a distance between a transmitter and a receiver is 7 and 15 meters, respectively. A rake receiver with 50 bins is used and the perfect channel estimation is assumed. A

guard interval, T_g, is inserted between time frames to obtain meaningful BER curves by decreasing serious intersymbol interferences of the channel. Though inserting T_g, the PSD function given in (4.5) remains except for the increase of T_f by T_g. The proposed system has a lower error floor below BER=10^{-5} rather than the PCTH UWB-IR in the UWB-IR indoor channel. When d varies the BER curves are correspondingly shifted and the error floors of the proposed system and the PCTH UWB-IR are preserved.

4.7 Remarks

We considered the coded N-ary PPM UWB-IR which exploits the chaotic time hopping and the polarity randomization. We believe that the proposed system is a possible solution for the coexistence problem of the UWB-IR by the following reasons. First, the system works lower SNR at the same data rate and the same BER by the code. Second, the system has the line spectrum free PSD function by the polarity randomization.

We note that the PSD functions given in (4.5) and (4.8) is also applicable to any other linear code whose outputs' equations are linearly independent.

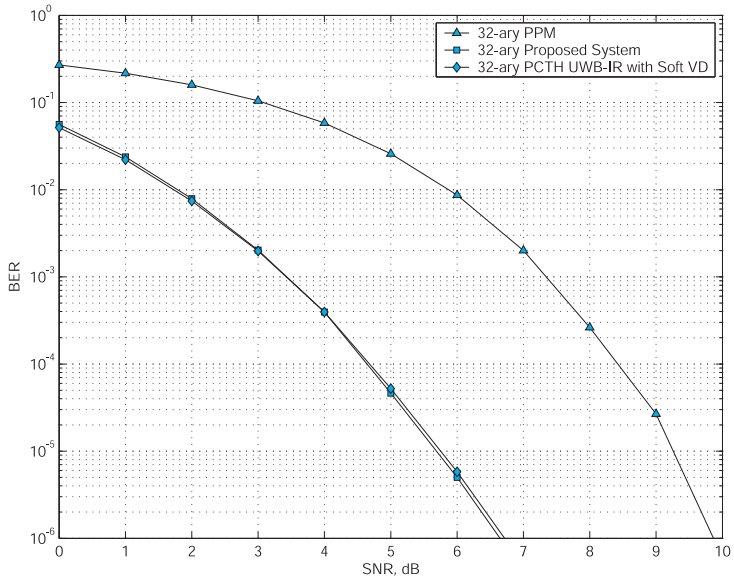
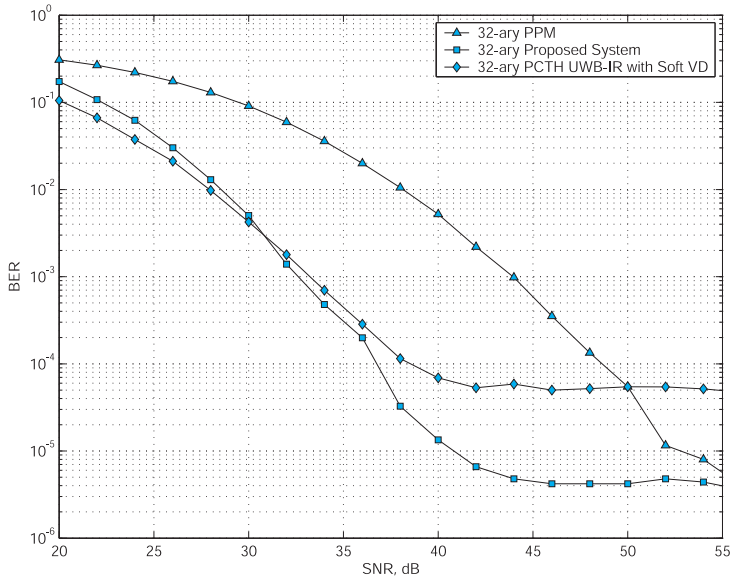
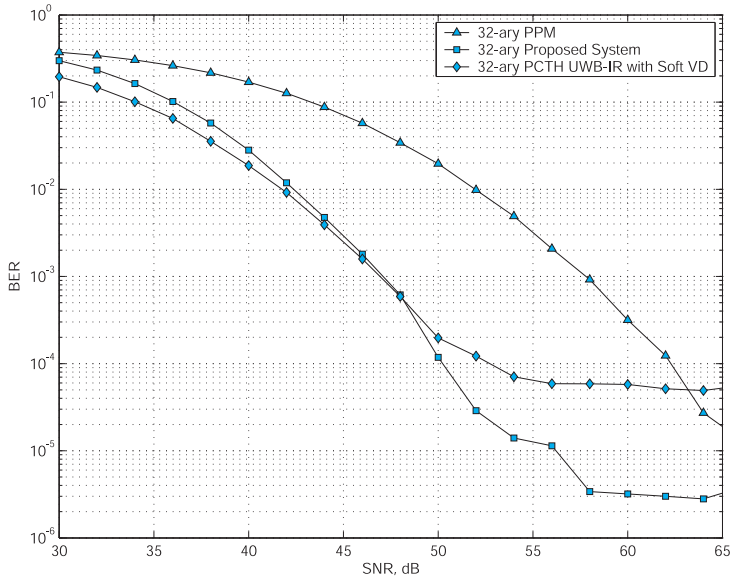


Figure 4.4: BER in the AWGN channel ($N = 32$, $T_f = 32$ns, $T_s = 1$ns, $R_d = 31.25$Mbps, $T_g = 0$ns).



(a) $d = 7$m



(b) $d = 15$m

Figure 4.5: BER in the UWB-IR indoor channel ($N = 32$, $T_f = 32$ns, $T_s = 1$ns, $R_d = 7.58$Mbps, and $T_g = 100$ns).

Chapter 5

Concluding Remarks

5.1 Summary

In this dissertation, we considered high security frequency/time hopping (FH/TH) sequence generators and ultra-wide bandwidth (UWB) impulse radios (IRs), which are commercial TH spread spectrum communication systems.

In chapter 2, we discussed some methods of constructing FH/TH sequences by taking successive k-tuples of given sequences. These methods can generate FH/TH sequences over large alphabets but with little increase in the hardware complexity. So, we focused on the linear complexities (LCs) of the FH/TH sequences, which is the only left design criterion for FH/TH sequences. We characterized those p-ary sequences whose k-tuple versions now over $\mathbb{F}_{p^k}$ have the maximum LCs. Then, we considered FH/TH sequence generators composed of a combinatorial function generator and some registers. We proposed the generators whose output FH/TH sequences have the maximum possible LCs for the given algebraic normal form to resist a Berlekamp-Massey (BM) attack.

In chapter 3, we considered the cryptographic properties of p-ary functions, that is

the combinatorial functions of the proposed FH/TH sequence generators, to resist other cryptographic attacks than the BM attack for high security. We constructed balanced p-ary functions by compositions. We constructed balanced p-ary functions which satisfy the propagation for the most of nonzero vectors and balanced functions which satisfy the propagation of high degree. Then, we derived a necessary condition such that p-ary functions are correlation-immune by the Fourier transforms and showed that some of nonlinearity criteria are invariant under cryptographically weak transformations.

Finally, in chapter 4 we considered a ultra-wide bandwidth UWB-IR as the example of commercial TH spread spectrum communication systems. We proposed a coded N-ary pulse position modulated (PPM) UWB-IR, which exploits the chaotic inter-pulse intervals in the framed-time structure and the polarity randomization for the coexistence with conventional narrow bandwidth wireless communication systems. We showed that the proposed system has noise-like spectrum, that is line spectrum free, by calculating its power spectral density function. We discussed its multi-user system with its line spectrum property. Then, we confirmed the bit error rate performance of the proposed system by simulation based on the UWB indoor channel model.

5.2 Future Directions and Open problems

Throughout this dissertation, we considered high security FH/TH sequence generators and coded N-ary PPM UWB-IRs. In further research, the following unsolved problems are desired to be studied.

1. For multi-user FH/TH communication systems, an FH/TH sequence constructed by the proposed generator in chapter 2 can be multi-user sequences by changing

the initial states of the linear feedback shift registers. We need to characterize the correlation properties of these multi-user sequences to verify their performance.

2. We need to verify that perfect nonlinear p-ary functions, i.e. p-ary bent functions, discussed in chapter 3 are optimum with respect to the minimum distance to affine functions and the minimum distance to functions with linear structures.

3. In chapter 4, we discussed the multi-user system of the proposed coded N-ary PPM UWB-IR. For the case of a reverse link, we need the user signature sequences with optimal aperiodic crosscorrelation properties.

Bibliography

[1] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., ser. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1997, vol. 20.

[2] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Springer-Verlag, 1986.

[3] S. W. Golomb, *Shift Register Sequences*, revised ed. Laguna Hills, CA 92654, USA: Aegean Park Press, 1982.

[4] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, revised ed. McGraw-Hill, Inc., 1994.

[5] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[6] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[7] M. Z. Win and R. A. Scholtz, "Impulse radio: how it works," *IEEE Communications Letters*, vol. 2, no. 2, pp. 36–38, Feb. 1998.

[8] D. Cassioli, M. Z. Win, and A. F. Molisch, "The ultra-wide bandwidth indoor

channel: from statistical model to simulations," *IEEE Journal on Selected Areas in Communicaitons*, vol. 20, no. 6, pp. 1247–1257, Aug. 2002.

[9] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *Journal of Combinatorial Theory*, vol. Series A 33, pp. 233–246, 1982.

[10] Y.-P. Hong and H.-Y. Song, "Frequency/time hopping sequences with large linear complexities," *Lecture Notes in Computer Science*, vol. 3969, pp. 386–396, 2006.

[11] W. J. Park and J. J. Komo, "Relationships between m-sequences over $GF(q)$ and $GF(q^m)$," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 183–186, Jan. 1989.

[12] G. Gong and G. Z. Xiao, "Synthesis and uniqueness of m-sequences over $GF(q^n)$ as n-phase sequences over $GF(q)$," *IEEE Transactions on Communications*, vol. 42, no. 8, pp. 2501–2505, Aug. 1994.

[13] W. Meidl, "Discrete Fourier transform, joint linear complexity and generalized joint linear complexity of multisequences," *Lecture Notes in Computer Science*, vol. 3486, pp. 101–112, Mar. 2005.

[14] N. Zierler and W. H. Mills, "Products of linear recurring sequences," *Journal of Algebra*, vol. 27, pp. 147–157, 1973.

[15] M. Matsui, "Linear cryptanalysis method for des cipher," *Lecture Notes in Computer Science*, vol. 765, pp. 386–397, 1994.

[16] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” *IEEE Transactions on Information Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.

[17] K. Chakrabarty and J. P. Hayes, “Balanced Boolean functions,” *IEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 1, pp. 52–62, Jan. 1998.

[18] W. Meier and O. Staffelbach, “Nonlinearity criteria for cryptographic functions,” *Lecture Notes in Computer Science*, vol. 434, pp. 549–562, 1990.

[19] B. Preneel, W. V. Leekwijck, and L. V. Linden, “Propagation characteristics of Boolean functions,” *Lecture Notes in Computer Science*, vol. 473, pp. 161–173, 1990.

[20] National Institute of Standards and Technology, “Data encryption standard,” FIPS Pub. 46-3, U. S. Department of Commerce, Oct. 1999.

[21] K. Nyberg, “Constructions of bent functions and difference sets,” *Lecture Notes in Computer Science*, vol. 473, pp. 151–160, 1991.

[22] P. V. Kumar, R. A. Scholtz, and L. R. Welch, “Generalized bent functions and their properties,” *Journal of Combinatorial Theory*, vol. Series A 40, pp. 90–107, 1985.

[23] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 1993.

[24] S. Hirose and K. Ikeda, “Propagation characteristics of Boolean functions and their

balancedness," *IEICE Transactions on Fundamentals*, vol. E78-A, no. 1, pp. 11–18, Jan. 1995.

[25] R. Forre, "The strict avalanche criterion: spectral properties of boolean functions and an extended definition," *Lecture Notes in Computer Science*, vol. 403, pp. 450–468, 1990.

[26] J. Seberry, X. M. Zhang, and Y. Zheng, "Highly nonlinear balanced Boolean functions satisfying high degree propagation criterion," *Tech. Rep. The Univ. Wollongong*, vol. tr–93–1, 1993.

[27] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," *Lecture Notes in Computer Science*, vol. 576, pp. 86–100, 1992.

[28] M. Liu, P. Lu, and G. L. Mullen, "Correlation-immune functions over finite fields," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1273–1276, May 1998.

[29] X. Guo-Zhen and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Transactions on Information Theory*, vol. 34, no. 3, pp. 569–571, May 1988.

[30] K. Gopalakrishnan and D. R. Stinson, "Three characterizations of non-binary correlation-immune and resilient functions," *Designs, Codes and Cryptography*, vol. 5, no. 3, pp. 241–251, 1995.

[31] Y. Zheng, X.-M. Zhang, and H. Imai, "Restriction, terms and nonlinearity of Boolean functions," *Theoretical Computer Science*, vol. 226, pp. 207–223, 1999.

[32] J.-H. Evertse, “Linear structures in block ciphers,” *Lecture Notes in Computer Science*, vol. 304, pp. 249–266, 1988.

[33] N. T. Courtois and W. Meier, “Algebraic attacks on stream ciphers with linear feedback,” *Lecture Notes in Computer Science*, vol. 2656, pp. 345–359, 2003.

[34] *Special Issue in Noncoherent Chaotic Communications, IEEE transactions on circuits and systems-I: fundamental theory and applications*, vol. 47, no. 12, pp. 1661–1764, Dec. 2000.

[35] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, “Digital communication using chaotic-pulse-position modulation,” *IEEE transactions on circuits and systems-I: fundamental theory and applications*, vol. 48, no. 12, pp. 1436–1444, Dec. 2001.

[36] M. Z. Win, “A unified spectral analysis of generalized time-hopping spread-spectrum signals in the presence of timing jitter,” *IEEE Journal on Selected Areas in Communicaitons*, vol. 20, no. 9, pp. 1664–1676, Dec. 2002.

[37] R. A. Scholtz, P. V. Kumar, and C. J. Corrada-Bravo, “Signal design for ultra-wideband radio,” in *Proceedings of Sequences and Their Applications 2001*, pp. 72–87.

[38] J. Romme and L. Piazzo, “On the power spectral density of time-hopping impulse radio,” in *Proceedings of IEEE Conference on Ultra Wideband Systems and Technologies 2002*, pp. 241–244.

[39] Y. P. Nakache and A. F. Molish, “Spectral shaping of uwb signals for time-hopping impulse radio,” *IEEE Journal on Selected Areas in Communicaitons*, vol. 24, no. 4, pp. 738–744, Apr. 2006.

[40] A. R. Forouzan and M. Abtahi, “Application of convolutional error correcting codes in ultrawideband M-ary PPM signaling,” *IEEE Microwave and Wireless Components Letters*, vol. 13, no. 8, pp. 308–310, Aug. 2003.

[41] G. M. Maggio, N. Rulkov, and L. Reggiani, “Pseudo-chaotic time hopping for UWB impulse radio,” *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1424–1435, Dec. 2001.

[42] D. Laney, G. M. Maggio, F. Lehmann, and L. Larson, “Ber performance and spectral properties of interleaved convolutional time hopping for UWB impulse radio,” in *Proceedings of IEEE Global Telecommunications Conference 2003*, vol. 4, Dec., pp. 1994–1998.

[43] D. C. Laney, G. M. Maggio, F. Lehmann, and L. Larson, “Multiple access for UWB impulse radio with pseudochaotic time hopping,” *IEEE Journal on Selected Areas in Communicaitons*, vol. 20, no. 9, pp. 1692–1700, Dec. 2002.

[44] Y. P. Hong and H. Y. Song, “Line apectrum analysis of impulse radio uwb systems using a pulse position modulation,” in *Proceedings of IEEE international conference on communications 2005*, vol. 5, May, pp. 2877–2880.

[45] “First report and order in the matter of revision of part 15 of the commission’s

rules regarding ultra-wideband transmission systems," FCC, released, ET Docket 98-153, FCC 02-48, Apr. 22 2002.

[46] S. G. Wilson, *Digital Modulation and Coding*. Upper Saddle River, New Jersey 07458, USA: Prentice-Hall. Inc., Simon & Schuster/A Viacom Company.

[47] S. S. Agaian, *Hadamard Matrices and Their Applications*, ser. Lecture Notes in Mathematics. Springer-Verlag, 1985, vol. 1168.

[48] H. D. Schotten, H. Elders-Boll, and A. Busboom, "Optimization of spreading-sequences for ds-cdma systems and frequency-selective fading channels," in *Proceedings of IEEE international symposium on spread spectrum techniques and applications 1998*, vol. 1, Sept., pp. 33–37.

국 문 요 약

높은 보안성을 갖는 주파수/시간 도약 수열 생성기

본 논문에서는 주어진 $\mathbb{F}_p$상의 수열을 연속적으로 k-터플(tuple)씩 읽음으로써 $\mathbb{F}_{p^k}$상의 주파수/시간 도약 수열을 생성하는 방법에 대해 논의하였으며 자신의 k-터플 수열의 선형 복잡도(linear complexity)가 최대 값을 갖는 p진 수열의 조건을 기술하였다. 또한 조합 함수 생성기(combinatorial function generator)와 레지스터(register)들로 구성된 주파수/시간 도약 수열 생성기를 제안하고 Berlekamp-Massey (BM) 공격에 대한 저항성을 위해 최대 선형 복잡도를 갖는 도약 수열을 생성하는 주파수/시간 도약 수열 생성기의 조건을 기술하였다.

다음으로, 위에서 언급한 BM 공격이외의 다른 공격에 대해서도 저항성을 갖는 보다 높은 보안성을 갖기 위해, 제안된 주파수/시간 도약 수열 생성기의 조합 함수인 p진 함수의 암호학적 특성을 고려하였다. 함수의 합성(composition)에 의해 균등(balanced) p진 함수를 생성하였으며 영 벡터가 아닌 대부분의 벡터에 대해 확산(propagation)을 만족하는 균등 p진 함수와 높은 단계의 확산을 만족하는 균등 p진 함수를 생성하였다. p진 함수가 상관 면역(correlation-immune)하기 위한 필요조건을 푸리에(Fourier) 변환을 통해 유도하였고 몇가지 비선형성 (nonlinearity) 기준들이 암호학적으로 간단한 변환에 대해 불변이라는 것을 보였다.

마지막으로, 시간 도약 대역 확산 통신 시스템의 상업적인 예로서 초 광대역 무선 전송 기법(ultra-wide bandwidth impulse radio)을 주목하여 기존 협대역 무선 통

신 시스템과의 공존을 위해 프레임 구조를 갖는 시간축에서의 무질서한(chaotic) 펄스 간격과 극성 난수화(polarity randomization)를 이용하는 채널 부호화된 N진 펄스 위치 변조 초 광대역 무선 전송 시스템을 제안하였다. 전력 밀도 함수를 계산함으로써 제안된 시스템이 선 스텍트럼이 없는 잡음 형태의 주파수 스펙트럼을 가짐을 보였고 제안된 시스템의 다중 사용자 시스템과 그것의 선 스펙트럼 특성에 대해 논의하였으며 초 광대역 무선 전송 실내 채널에서의 모의 실험을 통하여 제안된 시스템의 비트 오류율을 검증하였다.

핵심되는 말: 주파수/시간 도약 수열, 선형 복잡도, 균등, 확산, 상관 면역, 비선형성, 초 광대역, 선 스펙트럼, 극성 난수화, 길쌈 부호