Almost Security of Cryptographic Boolean Functions

Kaoru Kurosawa, *Member, IEEE,* and Ryutaroh Matsumoto, *Member, IEEE*

***Abstract*—The propagation criterion, PC (ℓ) of order k, is one of the most general cryptographic criteria of secure Boolean functions f. In this paper, we formalize its ε-almost version. The new definition requires that $f(X)+f(X+\Delta)$ is *almost* uniformly distributed while in the original definition, it must be *strictly* uniformly distributed. Better parameters are then obtained than the strict PC (ℓ) of order k functions. To construct ε-*almost* PC (ℓ) of order k functions, we introduce a notion of *domain distance*.**

***Index Terms*—Boolean functions, ε-almost version, PC (ℓ) of order k.**

I. INTRODUCTION

A. Overview

SEVERAL criteria of Boolean functions f have been developed to examine their cryptographic properties. However, the properties have shown to be contradictory in the sense that strict fulfillment in one criterion leads to less optimal fulfillment or complete failure with respect to another criterion. Previously, Kurosawa, Johansson, and Stinson introduced the notion of ε-almost k-resilience [9], which relaxes, in a controlled manner, the strict requirement of k-resilience.

The goal of this paper is to extend this approach to the propagation criterion PC (ℓ) of order k. That is, we formalize an ε-almost version of PC(ℓ) of order k. The new definition requires that $f(X)+f(X+\Delta)$ is *almost* uniformly distributed while in the original definition, it must be *strictly* uniformly distributed. Better parameters are then obtained than the strict PC(ℓ) of order k functions. To construct ε-*almost* PC(ℓ) of order k functions, we introduce a notion of *domain distance*.

B. PC(ℓ) of Order k and its Almost Version

PC(ℓ) of order k [19], [20] is one of the most general criteria among many cryptographic criteria which have been studied in order to design secure block ciphers.

A Boolean function $f(X)$ is said to satisfy PC(ℓ) if the output difference $f(X)+f(X+\Delta)$ is uniformly distributed for any input difference Δ with $1 \le \mathrm{wt}(\Delta) \le l$, where $\mathrm{wt}(\Delta)$ denotes the Hamming weight of Δ. Further suppose that $f(X)$ satisfies PC(ℓ) even if any k bits of $X=(x_1,\ldots,x_n)$ are fixed into any constants. Then we say that $f(X)$ satisfies PC(ℓ) of order k.

The famous strict avalanche criterion (SAC), which was introduced as a criterion of the security of S-boxes [21], is equivalent to PC(1). SAC (k) is equivalent to PC(1) of order k. Also, $f(X)$ is a bent function [11, Ch. 14] if and only if $f(X)$ satisfies PC(n) [19], where a bent function has the largest distance from the set of affine (linear) functions. (Hence, it is directly related to the linear attack.) PC(ℓ) of order k in general is directly related to the security against differential attacks.

Kurosawa *et al.* gave a general method to design PC(ℓ) of order k functions by using linear codes [10]. Carlet extended it to nonlinear codes [4].

Boolean functions, however, do not need to satisfy the strict definitions of cryptographic criteria in general. These definitions are sometimes stronger than what we want and may introduce other vulnerabilities. For example, cryptographic Boolean functions need to be balanced, but bent functions are never balanced. Therefore, it would be good if by relaxing the conditions, better parameters with respect to all known attacks could be obtained.

From this point of view, this paper introduces a notion of ε-almost PC(ℓ) of order k. It requires that $f(X)+f(X+\Delta)$ is *almost* uniformly distributed while in the original definition, it must be *strictly* uniformly distributed. We then show that indeed better parameters are obtained than the strict PC(ℓ) of order k functions.

We present a design method of ε-almost PC(ℓ) of order k functions using linear codes and an ε-biased sample spaces [13] which satisfy some property. To achieve our goal, we introduce a new notion of *domain distance*. Our construction offers smaller input length n than the strict PC(ℓ) of order k functions for the same (l,k). (The input size n of S-boxes can be smaller for the security level (l,k).) In other words, we can obtain larger (l,k) for the same input length n. (Higher security level (l,k) can be obtained for the same input size n of S-boxes.)

We also show that our ε-almost PC(ℓ) of order k functions have large nonlinearity, where the nonlinearity $N(f)$ of a Boolean function f is defined by a distance between f and the set of affine functions. $N(f)$ must be large to avoid linear attack.

We finally generalize our result to multiple output bit Boolean functions.

Remark 1.1: We compare our construction of ε-almost PC(ℓ) of order k with the strict PC(ℓ) of order k functions using linear codes [10] because it is the best known construction.

It will be further work to show that for any strict PC(ℓ) of order k function, there exists a better ε-almost PC(ℓ) of order k function.

C. Related Work

Suppose that $\phi(x_1,\ldots,x_n)=(y_1,\ldots,y_m)$ is uniformly distributed even if any k bits of $(x_1,\ldots,x_n)$ are fixed into any constant. We then say that ϕ is an (n,m,k)-resilient function. This

---

Manuscript received May 19, 2003; revised June 9, 2004.

K. Kurosawa is with the Department of Computer and Information Sciences, Ibaraki University 4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan (e-mail: kurosawa@cis.ibaraki.ac.jp).

R. Matsumoto is with the Department of Communications and Integrated Systems, Tokyo Institute of Technology, 2-12-1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan (e-mail: ryutaroh@it.ss.titech.ac.jp).

Communicated by T. Johansson, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2004.836684

notion has been studied by several researchers from the point of view of key renewal [6], [2], [8], [17], [3], [18]. Especially, a notion of ε-almost k-resilient functions was introduced in [9]. The authors presented its construction and showed that better parameters are obtained than the strict k-resilient functions. Dodis *et al.* improved it by showing a probabilistic construction [7].

Our work can be considered as an extension of [9]. Indeed, it is shown that an ε-almost PC(ℓ) of order k function is obtained from a linear code and an ε-almost k-resilient function with a special property. The special property is characterized by our new notion of *domain distance*. We then present how to construct such ε-almost k-resilient functions by extending the technique of [9].

D. Organization

This paper is organized as follows. Section II is for preliminaries. In Section III, we review almost resilient functions. Section IV formalizes a notion of ε-almost PC(ℓ) of order k functions and shows our basic theorem. Our construction is presented in Section V. Section VI shows a comparison with our construction with the strict PC(ℓ) of order k functions. In Section VII, we study the nonlinearity of our construction. Section VIII shows a generalization to multiple-output bits. In Section IX, we discuss t-systematic almost k-wise independent sample spaces.

II. PRELIMINARIES

We use f to denote a Boolean function $\{0,1\}^n \to \{0,1\}$, and ϕ to denote a function $\{0,1\}^n \to \{0,1\}^m$, where $m \le n$. We use X to denote $(x_1,\dots,x_n)$, where x_i is a binary variable.

We denote by $\mathrm{wt}(\Delta)$ the Hamming weight of a binary vector Δ. Let $\cdot$ denote the inner product of two binary vectors over GF(2). For a set A, $|A|$ denotes the cardinality of A.

Let a linear $[N,m,d]$-code denote a binary linear code C of length N, dimension m, and the minimum Hamming distance at least d. The dual code $C^\perp$ of a linear code C is defined as $C^\perp \triangleq \{u \mid u\cdot v = 0 \text{ for all } v \in C\}$. The dual minimum Hamming distance $d^\perp$ of C is defined as the minimum Hamming distance of $C^\perp$.

A. Resilient Functions

Definition 2.1: We say that $\phi : \{0,1\}^n \to \{0,1\}^m$ is an (n,m,k)-resilient function if $\phi(x_1,\dots,x_n)$ is uniformly distributed even if any k variables $x_{i_1},\dots,x_{i_k}$ are fixed into any constants. That is,

$$\Pr[\phi(x_1,\dots,x_n)=(y_1,\dots,y_m) \mid x_{i_1}x_{i_2}\cdots x_{i_k}=\alpha]=2^{-m}$$

for any k positions $i_1 < \cdots < i_k$, for any k-bit string $\alpha \in \{0,1\}^k$ and for any fixed $(y_1,\dots,y_m) \in \{0,1\}^m$, where the values x_j ($j \notin \{i_1,\dots,i_k\}$) are chosen independently at random.

Chor *et al.* showed that an (n,m,k)-resilient function can be obtained from a linear $[n,m,k+1]$-code [6].

Proposition 2.1: Let G be a generator matrix of a linear $[n,m,k+1]$-code C. Then $\phi(X) = G\cdot X$ is an (n,m,k)-resilient function.

Proof: Let $\phi(X) = (y_1,\dots,y_m)$. Then each y_i is a linear function of $X=(x_1,\dots,x_n)$. Further, each linear function has $k+1$ or more nonzero coefficients.

Now it is known that $\phi(X) = (y_1,\dots,y_m)$ is an (n,m,k)-resilient function if and only if

$$a_1y_1 + \cdots + a_my_m \tag{1}$$

is an $(n,1,k)$-resilient function for any $(a_1,\dots,a_m) \ne (0,\dots,0)$. (See [6].) In our case, expression (1) becomes the following:

$$(a_1,\dots,a_m)\cdot GX = (b_1,\dots,b_n)\cdot X$$

where $(b_1,\dots,b_n) = (a_1,\dots,a_m)\cdot G$. Note that

$$\mathrm{wt}(b_1,\dots,b_n) \ge k+1$$

because $(b_1,\dots,b_n)$ is a nonzero codeword of C. Then it is easy to see that $(b_1,\dots,b_n)\cdot X$ is k-resilient. Q.E.D.

We say that $f : \{0,1\}^n \to \{0,1\}$ is k-resilient if f is an $(n,1,k)$-resilient function.

B. PC(ℓ) of Order k

Define the derivative of $f : \{0,1\}^n \to \{0,1\}$ by

$$D_\triangle f = F(X) + f(X+\Delta)$$

for $\Delta \in \{0,1\}^n$.

Definition 2.2: [19], [20] We say that a Boolean function $f : \{0,1\}^n \to \{0,1\}$ satisfies PC(ℓ) of order k if $D_\triangle f$ is k-resilient for any $\Delta \in \{0,1\}^n$ with $1 \le \mathrm{wt}(\Delta) \le l$. (We also say that f is a PC(ℓ) of order k function.)

Kurosawa *et al.* gave a general method to design PC(ℓ) of order k functions by using two linear codes [10].

Proposition 2.2: Suppose that there exist

1) a linear $[n_1,m,k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell+1$ and
2) a linear $[n_2,m,k+1]$-code C_2 with the dual minimum Hamming distance at least $\ell+1$.

Then there exists a PC(ℓ) of order k function $f : \{0,1\}^n \to \{0,1\}$ such that $n = n_1+n_2$.

III. ALMOST RESILIENT FUNCTIONS

A. Almost k-Wise Independent Sample Space

Let ε be a constant such that $0 \le \varepsilon \le 1$. An ε-biased sample space is a subset $S_n \subseteq \{0,1\}^n$ which looks random. To formalize this notion, we consider that S_n is an $|S_n| \times n$ binary matrix and each row is randomly chosen.

Definition 3.1: S_n is ε-biased if

$$\left|\Pr_{X\in S_n}(X\cdot\alpha = 0) - \Pr_{X\in S_n}(X\cdot\alpha = 1)\right| \le \varepsilon$$

for any $\alpha \in \{0,1\}^n \setminus \{0^n\}$. We also say that S_n is an ε-biased sample space.

An almost k-wise independent sample space is a subset $S_N \subseteq \{0,1\}^N$ such that any k out of N bits look random. To formalize this notion, we consider that S_N is an $|S_N| \times N$ binary matrix and each row is randomly chosen.

Definition 3.2: (Almost k-wise independence). Suppose that $X = x_1 \cdots x_N$ is chosen randomly from S_N. Then we say that S_N is (ε, k)-independent if for any k positions $i_1 < i_2 < \cdots < i_k$ and any k-bit string α, we have

$$|\Pr[x_{i_1} x_{i_2} \cdots x_{i_k} = \alpha] - 2^{-k}| \le \varepsilon.$$

(We also say that S_N is an almost k-wise independent sample space.)

It is known that a large almost k-wise independent sample space S_N can be obtained from a small ε-biased sample space S_n, where $N > n$.

Proposition 3.1: [13] Suppose that S_n is ε-biased. Let H be a parity-check matrix of a $[N, N-n, k+1]$-linear code C. Define

$$S_N \triangleq S_n \cdot H. \tag{2}$$

Then S_N is $(\widetilde{\varepsilon}, k)$-independent, where

$$\widetilde{\varepsilon} = \left(1 - \frac{1}{2^k}\right) \cdot \varepsilon.$$

B. Almost Resilient Functions

Kurosawa, Johansson, and Stinson introduced a notion of ε-almost k-resilient functions [9]. It is an ε-almost version of (n, m, k)-resilient functions.

Definition 3.3: [9] We say that $\phi : \{0,1\}^n \to \{0,1\}^m$ is an *ε-almost (n, m, k)-resilient function* if

$$|\Pr[\phi(x_1, \ldots, x_n) = (y_1, \ldots, y_m) \mid x_{i_1} x_{i_2} \cdots x_{i_k} = \alpha] - 2^{-m}| \le \varepsilon$$

for any k positions $i_1 < \cdots < i_k$, for any k-bit string $\alpha \in \{0,1\}^k$, and for any fixed $(y_1, \ldots, y_m) \in \{0,1\}^m$, where the values x_j $(j \notin \{i_1, \ldots, i_k\})$ are chosen independently at random.

The authors presented its construction by using t-systematic (ε, k)-independent sample spaces [9].

Definition 3.4: [9] An (ε, k)-independent sample space S_N is called *t-systematic* if $|S_N| = 2^t$, and there exist t positions $i_1 < \cdots < i_t$ such that each t-bit string occurs in these positions for exactly one N-tuple in S_N.

t-systematic ε-biased sample spaces are defined similarly.

Proposition 3.2: [9, Theorem 4.4] If there exists a t-systematic (ε, k)-independent sample space S_N, then there exists a balanced δ-almost $(N, N-t, k)$-resilient function ϕ, where $\delta = \varepsilon / 2^{N-t-k}$.

Proof Sketch: Without loss of generality, assume that the first t positions in S_N run through all possible t-bit strings. We construct 2^{N-t} sample spaces E_α indexed by $\alpha = (\alpha_1, \ldots, \alpha_{N-t}) \in \{0,1\}^{N-t}$ by

$$E_\alpha = S_N + (\underbrace{0, 0, \ldots, 0}_{t}, \alpha_1, \ldots, \alpha_{N-t}).$$

Finally, define a function $\phi : \{0,1\}^N \to \{0,1\}^{N-t}$ by the rule

$$\phi(x_1, \ldots, x_N) = \alpha \text{ if and only if } (x_1, \ldots, x_N) \in E_\alpha. \tag{3}$$

Then ϕ is a δ-almost $(N, N-t, k)$-resilient function with $\delta = \varepsilon / 2^{N-t-k}$. Q.E.D.

TABLE I

DEFINITIONS OF PC(ℓ) AND ε-*ALMOST* PC(ℓ)

f	$PC(\ell)$ of order k	ε-*almost* $PC(\ell)$ of order k
$D_\Delta f$	$(n, 1, k)$-resilient function for any Δ with $1 \le wt(\Delta) \le l$	ε-*almost* $(n, 1, k)$-resilient function for any Δ with $1 \le wt(\Delta) \le l$

IV. ALMOST PC(ℓ) OF ORDER k

In this section, we formalize a notion of ε-almost PC(ℓ) of order k functions. It is an ε-almost version of PC(ℓ) of order k functions.

A. Definition

Definition 4.1: We say that $f : \{0,1\}^n \to \{0,1\}$ satisfies *ε-almost* PC(ℓ) *of order k* if its derivative $D_\Delta f$ is an *ε-almost $(n, 1, k)$-resilient function* for any $\Delta \in \{0,1\}^n$ with $1 \le \mathrm{wt}(\Delta) \le l$. (We also say that $f(X)$ is an *ε-almost* PC(ℓ) *of order k function*.)

The definitions of "PC(ℓ) of order k" and "*ε-almost* PC(ℓ) of order k" are summarized in Table I.

B. Basic Theorem

We show that an almost PC(ℓ) of order k function is obtained from a linear code and an ε-almost (n, m, k)-resilient function which satisfies some property. We first introduce a notion of *domain distance*.

Definition 4.2: For a function $\phi : \{0,1\}^n \to \{0,1\}^m$ and for any $\alpha \in \{0,1\}^m$, define

$$C_\alpha = \{X \mid \phi(X) = \alpha\}.$$

For nonempty C_α, let d_α be the minimum Hamming distance of the code C_α. Then we define the domain distance d_ϕ of ϕ by

$$d_\phi = \min d_\alpha$$

where the minimum is taken over all nonempty C_α.

Lemma 4.1: Suppose that a function $\phi : \{0,1\}^n \to \{0,1\}^m$ has the domain distance d_ϕ. Then

$$\phi(\beta) \ne \phi(\beta + \Omega)$$

for any $\beta \in \{0,1\}^n$ if $1 \le \mathrm{wt}(\Omega) \le d_\phi - 1$.

Proof: Suppose that

$$\alpha = \phi(\beta) = \phi(\beta + \Omega)$$

for some $\alpha \in \{0,1\}^m$, $\beta \in \{0,1\}^n$, and $\Omega \in \{0,1\}^n$ with $1 \le \mathrm{wt}(\Omega) \le d_\phi - 1$. Then $d_\alpha < d_\phi$, where d_α is the minimum Hamming distance of C_α. This is a contradiction. Q.E.D.

We next prove the following lemma.

Lemma 4.2: Let $\phi : \{0,1\}^n \to \{0,1\}^m$ be an ε-almost (n, m, k)-resilient function with $2^{m-1}\varepsilon \le 1$. Then $\phi(X) \cdot \Delta$ is a $(2^{m-1}\varepsilon)$-almost $(n, 1, k)$-resilient function for any $\Delta \ne (0, \ldots, 0)$, where $X = (x_1, \ldots, x_n)$.

Proof: For any $\Delta \ne (0, \ldots, 0)$, let

$$A_0 = \{Y \mid Y \cdot \Delta = 0\}, \; A_1 = \{Y \mid Y \cdot \Delta = 1\}.$$

Then $|A_0| = |A_1| = 2^{m-1}$. Therefore,

$$\begin{aligned}\Pr(\phi(X)\cdot\Delta = 0) &= \sum_{\alpha\in A_0}\Pr(\phi(X)=\alpha)\\ &\ge \sum_{\alpha\in A_0}(2^{-m}-\varepsilon)\\ &= 1/2 - 2^{m-1}\varepsilon.\end{aligned}$$

Similarly, we have

$$\Pr(\phi(X)\cdot\Delta = 0) \le 1/2 + 2^{m-1}\varepsilon.$$

Hence,

$$|\Pr(\phi(X)\cdot\Delta = 0) - 1/2| \le 2^{m-1}\varepsilon.$$

Similarly

$$|\Pr(\phi(X)\cdot\Delta = 1) - 1/2| \le 2^{m-1}\varepsilon. \qquad \text{Q.E.D.}$$

Then our basic theorem is stated as follows.

Theorem 4.1: Suppose that there exist

1) a linear $[n_1, m, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell + 1$ and
2) an ε-almost (n'_2, m, k)-resilient function ϕ with the domain distance $d_\phi \ge \ell + 1$.

Then there exists a δ-almost PC(ℓ) of order k function $f : \{0,1\}^n \to \{0,1\}$ such that $\delta = 2^{m-1}\varepsilon$ and $n = n_1 + n'_2$.

Proof: Let G_1 be a generator matrix of C_1. Define a Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $n = n_1 + n'_2$ as follows. For $X = (x_1, \ldots, x_{n_1})$ and $Y = (y_1, \ldots, y_{n'_2})$, let

$$f(X,Y) = \phi(Y)\cdot G_1 X + \pi(Y) \tag{4}$$

where $\pi : \{0,1\}^{n'_2} \to \{0,1\}$ is any Boolean function. We show that $f(X,Y)$ satisfies $(2^{m-1}\varepsilon)$-almost PC(ℓ) of order k. Define the derivative of f by

$$D_{(\Delta,\Omega)}f(X,Y) = f(X,Y) + f(X+\Delta, Y+\Omega).$$

Then

$$\begin{aligned}&D_{(\Delta,\Omega)}f(X,Y)\\ &\quad= (\phi(Y)+\phi(Y+\Omega))\cdot G_1X + \phi(Y+\Omega)\cdot G_1\Delta\\ &\qquad+ \pi(Y) + \pi(Y+\Omega).\end{aligned}$$

Case 1. Suppose that $\Omega = 0$ and $1 \le \mathrm{wt}(\Delta) \le l$. In this case

$$D_{(\Delta,\Omega)}f(X,Y) = \phi(Y)\cdot G_1\Delta.$$

Then $G_1\Delta \ne \mathcal{O}$ because Δ is not a codeword of $C_1^{\perp}$. Hence, $D_{(\Delta,\Omega)}f(X,Y)$ is $(2^{m-1}\varepsilon)$-almost k-resilient from Lemma 4.2.

Case 2. Suppose that $\Omega \ne 0$ and $1 \le \mathrm{wt}(\Delta) + \mathrm{wt}(\Omega) \le l$. Then for any β

$$D_{(\Delta,\Omega)}f(X,\beta) = (\phi(\beta)+\phi(\beta+\Omega))\cdot G_1X + \gamma$$

where $\gamma = \phi(\beta+\Omega)\cdot G_1\Delta + \pi(\beta) + \pi(\beta+\Omega)$ is a constant. Now

$$\phi(\beta) \ne \phi(\beta+\Omega)$$

because $d_\phi \ge \ell + 1$. Therefore, $D_{(\Delta,\Omega)}f(X,\beta)$ is k-resilient from the proof of Proposition 2.1.

This means that $D_{(\Delta,\Omega)}f(X,Y)$ is k-resilient.

Consequently, $f(X,Y)$ satisfies $2^{m-1}\varepsilon$-almost PC(ℓ) of order k. Q.E.D.

TABLE II
RELATIONSHIP BETWEEN PROPOSITION 2.2 AND THEOREM 4.1

	Proposition 2.2	Theorem 4.1
$\phi(Y)$	G_2Y ($[n_2, m, k+1]$-code)	ε-almost (n'_2, m, k)-resilient function
d_ϕ	dual minimum Hamming distance of C_2	domain distance of ϕ
ε	0	$\varepsilon > 0$
δ	0	$2^{m-1}\varepsilon$
n	$n_1 + n_2$	$n_1 + n'_2$

C. Discussion

Equation (4) gives a general formula of our δ-almost PC(ℓ) of order k function. Note that Proposition 2.2 can be seen as a corollary of Theorem 4.1.

Indeed, in (4), let $\phi(Y) = G_2Y$, where G_2 is a generator matrix of a linear $[n_2, m, k+1]$-code C_2. Then $\phi(Y)$ is an (n_2, m, k)-resilient function from Proposition 2.1. In this case, it is easy to see that the d_ϕ is equal to the dual minimum Hamming distance of C_2.

The relationship between Proposition 2.2 and Theorem 4.1 is summarized in Table II.

Now suppose that there exists a linear $[n_2, m, k+1]$-code with the dual minimum Hamming distance at least $\ell + 1$. In what follows, we show that there exists an ε-almost (n'_2, m, k)-resilient function with the domain distance at least $\ell + 1$ such that $n'_2 < n_2$.

This means that we can obtain smaller input length n for the same (l, k). In other words, we can obtain larger (l, k) for the same n.

V. CONSTRUCTION

A. Outline

From the proof of Theorem 4.1, we can construct a $(2^{m-1}\varepsilon)$-almost PC(ℓ) of order k function f by using a linear $[n_1, m, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell + 1$ and an ε-almost (n_2, m, k)-resilient function ϕ with the domain distance $d_\phi \ge \ell + 1$.

In this section, we show how to achieve the second condition, i.e., how to construct an ε-almost (n, m, k)-resilient function with the domain distance at least $\ell + 1$.

We define the domain distance of an (ε, k)-independent sample space S_N as follows.

Definition 5.1: For an (ε, k)-independent sample space S_N, let $C(S_N)$ be a nonlinear code such that each row of S_N is a codeword. Then we say that S_N has the domain distance d, where d is the minimum Hamming distance of $C(S_N)$.

It is easy to see that the domain distance d_ϕ of ϕ defined by (3) is equal to the minimum Hamming distance of $C(S_N)$. Therefore, it is reasonable to define the domain distance of an (ε, k)-independent sample space S_N as above.

Now our construction is outlined as follows.

Step 1. We first show that the second condition of Theorem 4.1 is satisfied if there exists a t-systematic (ε, k)-independent sample space S_N whose domain distance is at least $\ell + 1$.

Step 2. We next show that such S_N is obtained from a t-systematic ε-biased sample space S_n and a linear $[N, N-n, k+1]$-code with the dual minimum Hamming distance at least $\ell+1$.

Step 3. We finally show how to construct such S_n by using Weil–Carlitz–Uchiyama bound. (The same technique was used in [9] to construct a t-systematic (ε, k)-independent sample space S_N directly.)

B. Step 1–Step 3

We show Step 1–Step 3 of the previous subsection.

Theorem 5.1: Suppose that there exists a t-systematic (ε, k)-independent sample space S_N with the domain distance at least $\ell+1$. Then there exists a balanced δ-almost $(N, N-t, k)$-resilient function ϕ with the domain distance d_ϕ at least $\ell+1$, where $\delta = \varepsilon/2^{N-t-k}$.

Proof: Construct ϕ from S_N as shown in the proof of Proposition 3.2. Then the ϕ is a balanced δ-almost $(N, N-t, k)$-resilient function.

Next suppose that $d_\phi \le l$. That is, $\phi(\beta) = \phi(\beta+\Omega) = \alpha$ for some α, β, and Ω such that $1 \le \mathrm{wt}(\Omega) \le l$. Then we see that

$$\beta + (0, \dots, 0, \alpha) \in S_N \text{ and } \beta + \Omega + (0, \dots, 0, \alpha) \in S_N.$$

This means that there are two codewords with the distance l or less in S_N. However, this is a contradiction because S_N has the domain distance at least $\ell+1$. Q.E.D.

Theorem 5.2: Suppose that there exists a t-systematic ε-biased sample space S_n and a linear $[N, N-n, k+1]$-code C with the dual minimum Hamming distance at least $\ell+1$. Then there exists a t-systematic $(\tilde{\varepsilon}, k)$-independent sample space S_N with the domain distance at least $\ell+1$, where

$$\tilde{\varepsilon} = \left(1 - \frac{1}{2^k}\right) \cdot \varepsilon.$$

Proof: Let $H = (I_n, \tilde{H})$ be a parity-check matrix of C, where I_n is the $n \times n$ identity matrix. Let

$$S_N = S_n \cdot H. \tag{5}$$

Then S_N is $(\tilde{\varepsilon}, k)$-independent from Proposition 3.1, where

$$\tilde{\varepsilon} = \left(1 - \frac{1}{2^k}\right) \cdot \varepsilon.$$

Next it is easy to see that S_N is t-systematic if S_n is t-systematic.

Finally, we show that S_N has the domain distance at least $\ell+1$. From (5), we see that S_N is a subset of all codewords of $C^\perp$. Therefore, S_N has the domain distance at least $\ell+1$ because C has the dual distance at least $\ell+1$. Q.E.D.

We next show how to construct a t-systematic ε-biased sample space S_n by using Weil–Carlitz–Uchiyama bound. For $x \in \mathrm{GF}(2^t)$, let

$$\mathrm{Tr}(x) \triangleq x + x^2 + x^{2^2} + \cdots + x^{2^{t-1}}.$$

It is well-known that $\mathrm{Tr}(x) = 0$ or 1 and $\mathrm{Tr}(x_1 + x_2) = \mathrm{Tr}(x_1) + \mathrm{Tr}(x_2)$.

Proposition 5.1: (Weil–Carlitz–Uchiyama Bound) [11, Ch. 9, Theorem 19] Let

$$f(x) = \sum_{i=1}^{D} f_i x^i \in \mathrm{GF}(2^t)[x]$$

be a polynomial such that $f(x) \ne g(x)^2 - g(x) + \theta$ for any polynomial $g(x) \in \mathrm{GF}(2^t)[x]$ and for any constant $\theta \in F_{2^t}$. Then

$$\left| \sum_{\alpha \in \mathrm{GF}(2^t)} (-1)^{\mathrm{Tr}(f(\alpha))} \right| \le (D-1)\sqrt{2^t}.$$

Remark 5.1: It is easy to see that if $f(x)$ is an odd degree polynomial, then $f(x) \ne g(x)^2 - g(x) + \theta$ for any $g(x)$ and any θ.

Now for two positive integers t and D', let $n = tD'$ and $D = 2D' - 1$. Let g be a primitive element of $\mathrm{GF}(2^t)$ and $x_1, x_2, \dots, x_{2^t}$ be the elements of $\mathrm{GF}(2^t)$. For each $x_i \in \mathrm{GF}(2^t)$, let X_i be a string of length $n = tD'$ such that

$$X_i \triangleq (Z_{i,1}, Z_{i,2}, \dots, Z_{i,D'})$$

where

$$Z_{i,j} \triangleq (\mathrm{Tr}(x_i^{2j-1}), \mathrm{Tr}(g x_i^{2j-1}), \dots, \mathrm{Tr}(g^{t-1} x_i^{2j-1})).$$

The proposed ε-biased sample space is defined as

$$S_n = \begin{pmatrix} X_1 \\ \vdots \\ X_{2^t} \end{pmatrix}. \tag{6}$$

Theorem 5.3: The above $S_n \subseteq \{0,1\}^n$ is a t-systematic ε-biased sample space such that $n = tD'$, $|S_n| = 2^t$ and

$$\varepsilon = \frac{2(D'-1)}{\sqrt{2^t}}.$$

Proof: First it is a well known fact [9, p. 245] that

$$Y_x = (\mathrm{Tr}\,(x), \mathrm{Tr}\,(gx), \dots, \mathrm{Tr}\,(g^{t-1}x))$$

runs through $\{0,1\}^t$ when x runs through $\mathrm{GF}\,(2^t)$. Hence S_n is t-systematic.

Next consider $\alpha \in \{0,1\}^n \backslash \{0^n\}$. Let

$$\alpha = (\Lambda_1, \Lambda_2, \dots, \Lambda_{D'})$$

where

$$\Lambda_j = (\alpha_{0,2j-1}, \alpha_{1,2j-1}, \dots, \alpha_{t-1,2j-1}).$$

Then since $\alpha_{i,j}$ is binary, we have that

$$\begin{aligned} X_i \cdot \alpha &= \sum_{j=1}^{D'} (\alpha_{0,2j-1} \mathrm{Tr}(x_i^{2j-1}) + \cdots + \alpha_{t-1,2j-1} \mathrm{Tr}(g^{t-1} x_i^{2j-1})) \\ &= \sum_{j=1}^{D'} \mathrm{Tr}((\alpha_{0,2j-1} + \alpha_{1,2j-1} g + \cdots + \alpha_{t-1,2j-1} g^{t-1}) x_i^{2j-1}) \\ &= \mathrm{Tr}(a_1 x_j + a_3 x_i^3 + \cdots + a_D x_i^D) \end{aligned}$$

where

$$a_j \triangleq \alpha_{0,j} + \alpha_{1,j} g + \cdots + \alpha_{t-1,j} g^{t-1}.$$

Since g is a primitive element, $a_j = 0$ if and only if

$$(\alpha_{0,j}, \alpha_{1,j}, \ldots, \alpha_{t-1,j}) = (0, \ldots, 0).$$

This implies that $(a_1, \ldots, a_D) \neq (0, \ldots, 0)$ because $\alpha \neq 0$.

Now define

$$f_i(x) \triangleq a_1 x_i + a_3 x_i^3 + \cdots + a_D x_i^D.$$

Let

$$A_0 \triangleq \{x_i | \mathrm{Tr}(f(x_i)) = 0\},\ A_1 \triangleq \{x_i | \mathrm{Tr}(f(x_i)) = 1\}.$$

Then we see that

$$\begin{aligned} &|\Pr(X \cdot \alpha = 0) - \Pr(X \cdot \alpha = 1)| \\ &\quad = \left| \frac{|A_0|}{2^t} - \frac{|A_1|}{2^t} \right| \\ &\quad = \frac{1}{2^t} \left| \sum_{x_i \in \mathrm{GF}\,(2^t)} (-1)^{\mathrm{Tr}(f(x_i))} \right|. \end{aligned}$$

Finally, from the Weil–Carlitz–Uchiyama bound (see also Remark 5.1), we have

$$|\Pr(X \cdot \alpha = 0) - \Pr(X \cdot \alpha = 1)| \leq \frac{(D-1)\sqrt{2^t}}{2^t} = \frac{D-1}{\sqrt{2^t}}.$$

Hence,

$$\varepsilon = \frac{D-1}{\sqrt{2^t}} = \frac{2(D'-1)}{2^{t/2}}. \qquad \text{Q.E.D.}$$

C. Final Construction

Corollary 5.1: Suppose there exists a linear $[N, N-tD', k+1]$-code C with the dual distance at least $\ell+1$. Then there exists a balanced δ-almost $(N, N-t, k)$-resilient function with the domain distance at least $\ell+1$ such that

$$\delta = \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)\sqrt{2^t}}{2^{N-k}}.$$

Proof: From Theorems 5.1, 5.2, and 5.3. More precisely, it is illustrated as follows.

t-systematic ε-biased sample space S_n such that $n = tD'$, $|S_n| = 2^t$ and $\varepsilon = 2(D'-1)/\sqrt{2^t}$ (Theorem 5.3)

$$+$$

Linear $[N, N-tD', k+1]$-code C with the dual minimum Hamming distance at least $\ell+1$.

$$\Downarrow \text{ Theorem 5.2}$$

t-systematic $(\tilde{\varepsilon}, k)$-independent sample space S_N with the domain distance at least $\ell+1$, where

$$\tilde{\varepsilon} = \left(1 - \tfrac{1}{2^k}\right) \cdot \varepsilon.$$

$$\Downarrow \text{ Theorem 5.1.}$$

Balanced δ-almost $(N, N-t, k)$-resilient function ϕ with the domain distance d_ϕ at least $\ell+1$, where

$$\delta = \tilde{\varepsilon}/2^{N-t-k} = \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)\sqrt{2^t}}{2^{N-k}}. \qquad \text{Q.E.D.}$$

We finally obtain the following corollary.

Corollary 5.2: Suppose that there exist

1) a linear $[n_1, m, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell+1$ and
2) a linear $[n_2', m-(D'-1)t, k+1]$-code C_2' with the dual minimum Hamming distance at least $\ell+1$.

Then there exists a $\tilde{\delta}$-almost PC(ℓ) of order k function f: $\{0,1\}^{n'} \to \{0,1\}$ such that $n' = n_1 + n_2'$ and

$$\tilde{\delta} = \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)}{2^{(t/2)+1-k}}.$$

Proof: From Theorem 4.1 and Corollary 5.1. It is illustrated as follows.

Linear $[N, N-tD', k+1]$-code C_2 with the dual distance at least $\ell+1$.

$$\Downarrow \text{ (Corollary 5.1)}$$

Balanced δ-almost $(N, N-t, k)$-resilient function with the domain distance at least $\ell+1$, where

$$\delta = \left(1 - \tfrac{1}{2^k}\right) \tfrac{2(D'-1)\sqrt{2^t}}{2^{N-k}}.$$

$$+$$

Linear $[n_1, N-t, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell+1$.

$$\Downarrow \text{ (Theorem 4.1)}$$

$\tilde{\delta}$-almost PC(ℓ) of order k function $f: \{0,1\}^{n'} \to \{0,1\}$, where $n' = n_1 + n_2'$ and

$$\tilde{\delta} = 2^{m-1}\delta = 2^{m-1} \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)\sqrt{2^t}}{2^{N-k}}.$$

Finally, by letting $m = N-t$ and $n_2' = N$, we obtain this corollary. Q.E.D.

To summarize, a $\tilde{\delta}$-almost PC(ℓ) of order k function is constructed as follows.

1) Construct a t-systematic ε-biased sample space S_{n_0} with $n_0 = tD'$ by using Theorem 5.3, where

$$\varepsilon = \frac{2(D'-1)}{\sqrt{2^t}}.$$

2) Let H be a parity-check matrix of a linear $[N, N-tD', k+1]$-code C_2' with the dual minimum Hamming distance at least $l+1$. Define $S_N = S_{n_0} H$. Then S_N is a t-systematic $(\tilde{\varepsilon}, k)$-independent sample space with the domain distance at least $l+1$ from Theorem 5.2, where

$$\tilde{\varepsilon} = \left(1 - \frac{1}{2^k}\right) \cdot \varepsilon.$$

3) From S_N, construct a balanced δ-almost $(N, N-t, k)$-resilient function ϕ with the domain distance d_ϕ at least $l+1$ by using Theorem 5.1, where

$$\delta = \widetilde{\varepsilon}/2^{N-t-k} = \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)\sqrt{2^t}}{2^{N-k}}.$$

4) Let G_1 be a generator matrix of a linear $[n_1, N-t, k+1]$-code C_1 with the dual minimum Hamming distance at least $l+1$. Define

$$f(X,Y) = \phi(Y) \cdot G_1 X + \pi(Y)$$

where $\pi : \{0,1\}^N \rightarrow \{0,1\}$ is any Boolean function. Then $f(X,Y)$ is a $\widetilde{\delta}$-almost PC(ℓ) of order k function from Corollary 5.2, where the input length is $n = n_1 + N$ and

$$\widetilde{\delta} = \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)}{2^{(t/2)+1-k}}.$$

VI. COMPARISON

Proposition 2.2 can be seen as a corollary of Corollary 5.2. Indeed, let $D' = 1$ in Corollary 5.2. Then we obtain Proposition 2.2.

Now let us compare the parameters of ϵ-almost PC(ℓ) of order k functions (Corollary 5.2) with the strict PC(ℓ) of order k functions (Proposition 2.2).

- In Proposition 2.2, the dimension of C_2 is equal to m.
- In Corollary 5.2, the dimension of C_2' is equal to $m-(D'-1)t$.

Therefore, $n_2' < n_2$ because $m-(D'-1)t < m$. Hence, $n' < n$.

This shows that our construction has a smaller input length for the same (l,k). In other words, our construction has larger (l,k) for the same input length n. (From Corollary 5.2, we can also see that the larger t is, the smaller both $\widetilde{\delta}$ and $m-(D'-1)t$ are.)

As an example, first try to construct a PC(1) of order 2 function by using Proposition 2.2 from a linear $[n_1, m=40, k+1 \geq 3]$ code C_1 which has the dual minimum Hamming distance at least 2. Suppose that $n_2 = 41$. Then from Proposition 2.2, we need a linear $[41, m=40, k+1]$-code C_2. However, it is clear that $k \leq 1$ for $n_2 = 41$ and $m = 40$. Hence we cannot construct a PC(1) of order 2 function for C_1 and $n_2 = 41$.

Next consider to construct $\widetilde{\delta}$-almost a PC(1) of order 2 function by using Corollary 5.2 for the same C_1 and $n_2' = n_2 = 41$. Let $D' = 2$ and $t = 30$ in Corollary 5.2. Then we see that a linear $[41, 11, k+1]$-code C_2 with the dual minimum Hamming distance at least 2 is necessary.

As shown below, there exists a linear $[41, 11, 3]$-code C_2 with the dual minimum Hamming distance at least 2. Hence, we can construct a $\widetilde{\delta}$-almost PC(1) of order 2 function with the input length $n = n_1 + 41$, where

$$\widetilde{\delta} = \left(1 - \frac{1}{2^k}\right) \frac{1}{2^{15-k}} = \frac{3}{4} \times \frac{1}{2^{13}}.$$

We finally show that there exists a linear $[41, 11, 3]$-code. Consider a Bose–Chaudhuri–Hocquenghem (BCH) code C_1 whose generator polynomial $\tilde{g}(x)$ has g as a root, where g is a primitive element of GF(2^5). Then we obtain a linear $[31, 26, 3]$-code [11, p. 204]. Its dual code $C_1^{\perp}$ is also a cyclic code such that the generator polynomial $\tilde{g}^{\perp}(x)$ has 1 as a root [16, p. 227, eq. (2.10)]. Therefore, the parity-check matrix of $C_1^{\perp}$ includes a row of $(1, \ldots, 1)$ [11, p. 203, eq (19)]. This means that C_1 has $(1, \ldots, 1)$ as a codeword.

Let the basis of C_1 be $\vec{g}_1, \ldots, \vec{g}_{26}$, where

$$\vec{g}_1 = (1, 1, \ldots, 1).$$

Define

$$\begin{aligned} \vec{h}_1 &= (\vec{g}_1, 1, 1, \ldots, 1) \\ \vec{h}_i &= (\vec{g}_i, 0, 0, \ldots, 0) \end{aligned}$$

for $i \geq 2$, where $\vec{h}_i$ is a binary vector of length 41. Let C be a linear code such that $\vec{h}_1, \ldots, \vec{h}_{11}$ are the basis of C. Then C is a linear $[41, 11, 3]$-code which includes $(1, \ldots, 1)$ as a codeword. It implies that the minimum Hamming distance $d^{\perp}$ of the dual code $C^{\perp}$ is even. That is, $d^{\perp} \geq 2$.

VII. ON OTHER CRYPTOGRAPHIC CRITERIA

To simplify the notation, let $s = n_1$ and $u = n_2'$ in Corollary 5.2. Then our $\widetilde{\delta}$-almost PC(ℓ) of order k function $f : \{0,1\}^n \rightarrow \{0,1\}$ is written as

$$f(X,Y) = \phi(Y) \cdot G_1 X + \pi(Y) \tag{7}$$

from (4), where

- $X = (x_1, \ldots, x_s)$ and $Y = (y_1, \ldots, y_u)$;
- $\phi : \{0,1\}^u \rightarrow \{0,1\}^m$ is an ε-almost (u, m, k)-resilient function with the domain distance $d_\phi \geq \ell + 1$;
- G_1 is a generator matrix of a linear $[s, m, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell + 1$;
- $\pi : \{0,1\}^u \rightarrow \{0,1\}$ is any Boolean function.

A. Balance

We say that $f : \{0,1\}^n \rightarrow \{0,1\}$ is balanced if

$$|\{X \mid f(X) = 0\}| = |\{X \mid f(X) = 1\}| = 2^{n-1}.$$

In this subsection, we show that our f is balanced if π is chosen appropriately in (7).

Definition 7.1: For ϕ, define

$$ZERO_\phi = \{Y \mid \phi(Y) = (0, \ldots, 0)\}.$$

We say that π is balanced for ϕ if

$$\begin{aligned} &\left|\{Y \mid \pi(Y) = 0, Y \in ZERO_\phi\}\right| & (8) \\ &= \left|\{Y \mid \pi(Y) = 1, Y \in ZERO_\phi\}\right|. & (9) \end{aligned}$$

Theorem 7.1: Our f is balanced if π is balanced for ϕ in (7).

Proof: Substitute $Y = \alpha$ into (7), where $\alpha \in \{0,1\}^u$ is a constant. Then we have

$$f(X,\alpha) = \phi(\alpha) \cdot G_1 X + \pi(\alpha). \tag{10}$$

Case 1. If $\phi(\alpha) \neq (0, \ldots, 0)$, then the right-hand side of (10) is a nonconstant affine function on X. In this case, $f(X,\alpha)$ is balanced as a function on X.

Case 2. If $\phi(\alpha) = (0, \dots, 0)$, then we have

$$f(X, \alpha) = \pi(\alpha).$$

In this case, $f(X, \alpha) = 0$ for a half of $\alpha \in ZERO_\phi$ and $f(X, \alpha) = 1$ for the half of $\alpha \in ZERO_\phi$ because π is balanced for ϕ.

The above argument implies that f is balanced. Q.E.D.

We show that it is easy to find a π which is balanced for ϕ. A trivial way is to write down the truth table of π.

Another way is as follows. From the proofs of Theorem 5.1 and Proposition 3.2, we see that $\phi(Y) = (0, \dots, 0)$ if and only if $Y \in E_{(0,\dots,0)} = S_N$. Therefore, $ZERO_\phi = S_N$, where S_N is a t-systematic (ε, k)-independent sample space. Assume that the first t positions in S_N run through all possible t-bit strings. Define π by

$$\pi(y_1, \dots, y_u) = y_1.$$

Then it is easy to see that π is balanced for ϕ.

B. Nonlinearity

Define a distance between two Boolean functions f_1 and f_2 by

$$d(f_1, f_2) = |\{X \mid f_1(X) \neq f_2(X)\}|.$$

The nonlinearity of a Boolean function f, denoted by $N(f)$, is defined by a distance between f and the set of affine functions

$$N(f) = \min_{A(x)} |\{X \mid f(X) \neq A(X)\}|$$

where

$$A(X) = a_0 + a_1 x_1 + \cdots a_n x_n$$

is an affine function. $N(f)$ must be large to avoid linear attack.

In this subsection, we show that our f has large nonlinearity if π is chosen appropriately in (7). For $f : \{0,1\}^n \to \{0,1\}$, it holds that [15], [12]

$$N(f) \leq 2^{n-1} - 2^{(n/2)-1}.$$

If the equality is satisfied, then f is called a bent function. There exists a bent function if and only if $n =$ even [15], [12].

Theorem 7.2: In Corollary 5.2, let $s = n_1$ and $u = n_2'$. Then the $\widetilde{\delta}$-almost PC(ℓ) of order k function $f : \{0,1\}^n \to \{0,1\}$ has nonlinearity such that

$$\begin{aligned} N(f) &\geq 2^{n-m-1} - 2^{s+(u/2)-m-1}, && \text{if } u = \text{even} \\ N(f) &\geq 2^{n-m-1} - 2^{s+(u-1)/2-m}, && \text{if } u = \text{odd} \end{aligned}$$

where $n = s + u$ and m is given in Corollary 5.2.

Proof: Remember that f is expressed by (7).

If $u = even$, let $\pi : \{0,1\}^u \to \{0,1\}$ be a bent function. We compute the distance between this $f(X, Y)$ and an affine function $A(X, Y)$ as follows. For $\beta \in \{0,1\}^s$, define

$$\begin{aligned} f_\beta(Y) &= f(\beta, Y) = \phi(Y) \cdot G_1 \beta + \pi(Y) \\ A_\beta(Y) &= A(\beta, Y). \end{aligned}$$

Then

$$\begin{aligned} d(f, A) &= \sum_{\beta \in \{0,1\}^s} d(f_\beta, A_\beta) \\ &= \sum_{\beta \in \{0,1\}^s} d(\phi(Y) \cdot G_1 \beta + \pi(Y), A_\beta(Y)) \\ &= \sum_{\beta : G_1 \beta = (0,\dots,0)^T} d(\pi(Y), A_\beta(Y)) \\ &\quad + \sum_{\beta : G_1 \beta \neq (0,\dots,0)^T} d(\phi(Y) \cdot G_1 \beta + \pi(Y), A_\beta(Y)) \\ &\geq \sum_{\beta : G_1 \beta = (0,\dots,0)^T} d(\pi(Y), A_\beta(Y)) \\ &\geq 2^{s-m}(2^{u-1} - 2^{u/2-1}) \end{aligned}$$

because $A_\beta(Y)$ is an affine function and π is a bent function, where $N(\pi) = 2^{u-1} - 2^{u/2-1}$. Therefore,

$$\begin{aligned} N(f) = \min_A d(f, A) &\geq 2^{s-m}(2^{u-1} - 2^{u/2-1}) \\ &= 2^{n-m-1} - 2^{s+(u/2)-m-1} \end{aligned}$$

because $n = s + u$.

If $u =$ odd, let $\pi' : \{0,1\}^{u-1} \to \{0,1\}$ be a bent function and define $\pi(y_1, \dots, y_u) = \pi'(y_1, \dots, y_{u-1})$. Then we obtain that

$$\begin{aligned} N(f) &\geq 2^{s-m+1}(2^{t-2} - 2^{(u-1)/2-1}) \\ &= 2^{n-m-1} - 2^{s+(u-1)/2-m} \end{aligned}$$

because $N(\pi') = 2^{u-2} - 2^{(u-1)/2-1}$. Q.E.D.

Remark 7.1: For $\varphi : \{0,1\}^u \to \{0,1\}^s$ and $\pi : \{0,1\}^u \to \{0,1\}$, define

$$f(X, Y) = \varphi(Y) \cdot X + \pi(Y)$$

where $X = (x_1, \dots, x_s)$ and $Y = (y_1, \dots, y_u)$. Then f: $\{0,1\}^{s+u} \to \{0,1\}$ is a $(s + u, 1, k)$-resilient function for any π if the Hamming weight of $\varphi(a)$ is strictly greater than k for any $a \in \{0,1\}^u$ [5, Sec.2.1]. Carlet studied the nonlinearity of this type of resilient functions in [5].

Equation (7) can be expressed similarly to the preceding equation by letting $\varphi(Y) = \phi(Y)G$. However, we cannot apply the result of Carlet [5] because it is possible that $\phi(a) = (0, \dots, 0)$ for some $a \in \{0,1\}^u$ in (7).

VIII. GENERALIZATION TO MULTIPLE-OUTPUT BITS

In this section, we generalize our result to multiple-output Boolean functions.

Definition 8.1: We say that $F(X) = (f_1, \dots, f_m)$ satisfies ε-almost PC(ℓ) of order k if $a_1 f_1 + \cdots + a_m f_m$ satisfies ε-almost PC(ℓ) of order k for any $(a_1, \dots, a_m) \neq (0, \dots, 0)$.

Theorem 8.1: Suppose that there exist

1) a linear $[n_1, m, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell + 1$ and
2) a linear $[n_2, m - (D' - 1)t, k + 1]$-code C_2 with the dual minimum Hamming distance at least $\ell + 1$

Then there exists a δ-almost PC(ℓ) of order k function $F : \{0,1\}^n \to \{0,1\}^m$ such that $n = n_1 + n_2$, where

$$\delta = \left(1 - \frac{1}{2^k}\right) \frac{2(D'-1)}{2^{(t/2)+1-k}}.$$

Proof: Let G_1 be a generator matrix of a linear $[n_1, m, k+1]$-code C_1 with the dual minimum Hamming distance at least $\ell+1$. Let $\phi(Y)$ be an ε-almost (n_2, m, k)-resilient function with the domain distance $d_\phi \geq \ell + 1$.

Consider a linear feedback shift register of length m with a primitive feedback polynomial. Let S be the state transition matrix of such a shift register. Let $X = (x_1, \ldots, x_{n_1})$ and $Y = (y_1, \ldots, y_{n_2})$. For $i = 1, \ldots, m$, define

$$f_i(X,Y) \triangleq \phi(Y) \cdot S^{i-1} G_1 X + g_i(Y)$$

where $g_i(Y)$ is any Boolean function. Then we show that $F(X,Y) = (f_1, \ldots, f_m)$ satisfies $(2^{m-1}\varepsilon)$-almost PC(ℓ) of order k.

For $(a_1, \ldots, a_m) \neq (0, \ldots, 0)$, we have

$$a_1 f_1 + \cdots + a_m f_m = \phi(Y) \cdot (a_1 I + a_2 S + \cdots + a_m S^{m-1}) G_1 X + a_1 g_1(Y) + \cdots + a_m g_m(Y).$$

It is easy to see that $a_1 I + a_2 S + \cdots + a_m S^{m-1}$ is a permutation of the space $\{0,1\}^m$, as pointed out by Nyberg [14]. Therefore, this matrix is nonsingular. It implies that $(a_1 I + a_2 D + \cdots + a_m D^{m-1}) G_1$ is a generator matrix of the linear code C_1. Then from the proof of Theorem 4.1, we see that $a_1 f_1 + \cdots + a_m f_m$ satisfies $(2^{m-1}\varepsilon)$-almost PC(ℓ) of order k.

The rest of the proof is straightforward from Section V.

Q.E.D.

IX. On t-Systematic Almost k-Wise Independent Sample Space

In this section, we discuss on the previous construction of t-systematic almost k-wise independent sample spaces [9].

A. Previous Construction

Kurosawa, Johansson, and Stinson showed a construction of t-systematic (ϵ, k)-independent sample spaces S_N [9] as follows.

Definition 9.1: A polynomial $h(x) \in \mathrm{GF}(2^t)[x]$ is called a $(2^t, D)$-*polynomial* if h has degree at most D and $a_i = 0$ for all even i, where $h = \sum_{i=0}^{D} a_i x^i$. Define $\mathrm{Poly}(2^t, D, k)$ to be a set of $(2^t, D)$-polynomials such that any k polynomials in the set are independent over GF(2).

Proposition 9.1: Suppose that g is a primitive element of GF(2^t), and $\mathrm{Poly}(2^t, D, k)$ is chosen such that

$$\{x, gx, g^2 x, \ldots, g^{t-1} x\} \subseteq \mathrm{Poly}(2^t, D, k).$$

Then there exists a t-systematic (ϵ, k)-independent sample space S_N where $N = |\mathrm{Poly}(2^t, D, k)|$ and $\varepsilon = (D-1)/\sqrt{2^t}$.

Proof Sketch: Let $\mathrm{Poly}(2^t, D, k) = \{h_1, \ldots, h_N\}$. Construct a sample space S_N as follows: A binary string

$$\widetilde{X_i} = b_1 b_2 \cdots b_N \in S_N$$

is specified by

$$b_j = \mathrm{Tr}(h_j(x_i))$$

where $\mathrm{GF}(2^t) = \{x_1, \ldots, x_{2^t}\}$. Let

$$S_N = \begin{pmatrix} \widetilde{X_1} \\ \vdots \\ \widetilde{X_{2^t}} \end{pmatrix}.$$

Then S_N is a t-systematic (ϵ, k)-independent sample space with $\varepsilon = (D-1)/\sqrt{2^t}$.

Q.E.D.

The above $\mathrm{Poly}(2^t, D, k)$ can be constructed as follows. For a fixed (odd) degree D, we can express each polynomial as a linear combination of

$$x, gx, \ldots, g^{t-1}x, x^3, gx^3, \ldots, g^{t-1}x^3, \ldots, x^D, gx^D, \ldots, g^{t-1}x^D.$$

The polynomials in this set are clearly independent over GF(2). Indexing the polynomials in $\mathrm{Poly}(2^t, D, k)$ as $h_1, h_2, \ldots, h_N$ we obtain a binary $tD' \times N$ matrix, where $D' = (D+1)/2$

$$H = \begin{pmatrix} h_{1,1} & h_{1,2} & \ldots & h_{1,N} \\ h_{2,1} & h_{2,2} & \ldots & h_{2,N} \\ \vdots & \ddots & \ddots & \vdots \\ h_{tD',1} & h_{tD',2} & \ldots & h_{tD',N} \end{pmatrix}$$

where $h_i(x) = h_{1,i} x + h_{2,i} gx + \cdots + h_{tD',i} g^{t-1} x^D$. Any k polynomials are independent over GF(2) means that any k columns of the above matrix are linearly independent. Hence, the matrix corresponds to a parity-check matrix of an $[N, l, d]$ error-correcting code, a code of length $N = |\mathrm{Poly}(2^t, D, k)|$, dimension $N - l = tD'$, and minimum Hamming distance $d = k + 1$ [11].

In order to get a t-systematic sample space, we have already chosen the polynomials $h_1 = x, h_2 = gx, \ldots, h_t = g^{t-1}x$. But clearly, this is no restriction, since any parity-check matrix can be rewritten into such a form without changing the code parameters.

B. Relationship

We show that the previous S_N coincides with our S_N if we ignore the condition on the domain distance. Let

$$B(x) = (x, gx, \ldots, g^{t-1}x, x^3, gx^3, \ldots, g^{t-1}x^3, \ldots, x^D, gx^D, \ldots, g^{t-1}x^D).$$

Then

$$(h_1(x), \ldots, h_N(x)) = B(x)H. \tag{11}$$

From (11), it is easy to see that

$$\widetilde{X_i} = \mathrm{Tr}(h_1(x_i)) \cdots \mathrm{Tr}(h_N(x_i)) = \mathrm{Tr}(B(x_i))H$$

where

$$\mathrm{Tr}(B(x_i)) = (\mathrm{Tr}(x_i), \mathrm{Tr}(gx_i), \ldots, \mathrm{Tr}(g^{t-1}x_i^D)).$$

Therefore, by letting

$$S_n = \begin{pmatrix} \mathrm{Tr}(B(x_1)) \\ \vdots \\ \mathrm{Tr}(B(x_{2^t})) \end{pmatrix} \tag{12}$$

we obtain that

$$S_N = S_n H. \tag{13}$$

Here (13) is the same as (2), and (12) is equivalent to (6). Therefore, we can see that the previous construction coincides with our construction if we ignore the condition on the domain distance.

C. On the Domain Distance

However, it is essential that S_N has the domain distance at least $\ell + 1$ in the construction of ε-almost PC(ℓ) of order k functions. In the previous method [9], S_N is constructed directly from $\mathrm{Poly}(2^t, D, k)$. From that point of view, we have no idea on how to impose the domain distance condition on S_N.

On the other hand, our S_N is constructed from the equation $S_N = S_n H$. From this point of view, it is very easy to impose the condition on the domain distance through H. Indeed, it is enough that H is a parity-check matrix of a linear code with the dual minimum Hamming distance st least $\ell + 1$.

In [9], it was not shown that the S_n is an ε-biased sample space, neither.

REFERENCES

[1] N. Alon, O. Goldreich, J. Hastad, and R. Peralta, “Simple constructions of almost k-wise independent random variables,” *Random Structures and Algorithms*, vol. 3, pp. 289–304, 1992.

[2] C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy amplification by public discussion,” *SIAM J. Comput.*, vol. 17, pp. 210–229, 1988.

[3] J. Bierbrauer, K. Gopalakrishnan, and D. R. Stinson, “Bounds for resilient functions and orthogonal arrays,” in *Proc. CRYPTO ’94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 839, pp. 247–257.

[4] C. Carlet, “On the propagation criterion of degree l and order k,” in *Advances in Cryptology—Proc. EUROCRYPT ’98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1998, vol. 1403, pp. 462–474.

[5] ——, “A larger class of cryptographic boolean functions via a study of the Maiorana-McFarland construction,” in *Advances in Cryptology—Proc. CRYPTO’02 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 549–564.

[6] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, and R. Smolensky, “The bit extraction problem or t-resilient functions,” in *Proc. 26th IEEE Symp. Foundations of Computer Science*, 1985, pp. 396–407.

[7] Y. Dodis, A. Sahai, and A. Smith, “On perfect and adaptive security in exposure-resilient cryptography,” in *Proc. EUROCRYPT ’01 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2001, vol. 2045, pp. 301–324.

[8] J. Friedman, “On the bit extraction problem,” in *Proc. 33rd IEEE Symp. Foundations of Computer Science*, 1992, pp. 314–319.

[9] K. Kurosawa, T. Johansson, and D. Stinson, “Almost k-wise independent sample spaces and their cryptologic applications,” *J. Cryptol.*, vol. 14, no. 4, pp. 231–253, 2001.

[10] K. Kurosawa and T. Satoh, “Design of SAC/PC (l) of order k Boolean functions and three other cryptographic criteria,” in *Advances in Cryptology—Proc. EUROCRYPT ’97 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1233, pp. 434–449.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*: North-Holland, 1977.

[12] W. Meier and O. Staffelbach, “Nonlinearity criteria for cryptographic functions,” in *Advances in Cryptology—Proc. EUROCRYPT ’89 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1990, vol. 434, , pp. 549–562.

[13] J. Naor and M. Naor, “Small bias probability spaces: Efficient constructions and applications,” *SIAM J. Comput.*, vol. 22, pp. 838–856, 1993.

[14] K. Nyberg, “Perfect nonlinear S-boxes,” in *Advances in Cryptology—Proc. EUROCRYPT ’91 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 547, , pp. 378–386.

[15] O. S. Rothaus, “On bent functions,” *J. Comb. Theory (A)*, vol. 20, pp. 300–305, 1976.

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[17] D. R. Stinson, “Resilient functions and large set of orthogonal arrays,” *Congr. Numer.*, vol. 92, pp. 105–110, 1993.

[18] D. R. Stinson and J. L. Massey, “An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions,” *J. Cryptol.*, vol. 8, pp. 167–173, 1995.

[19] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, “Propagation characteristics of boolean functions,” in *Advances in Cryptology—Proc. EUROCRYPT ’90 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 473, , pp. 161–173.

[20] B. Preneel, R. Govaerts, and J. Vandewalle, “Boolean functions satisfying higher order propagation criteria,” in *Advances in Cryptology—Proc. EUROCRYPT ’91 (Lecture Notes in Computer Science)*, 1991, vol. 547, pp. 141–152.

[21] A. F. Webster and S. E. Tavares, “On the design of S-boxes,” in *Advances in Cryptology—Proc.CRYPTO ’85 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1986, vol. 218, pp. 523–534.