Cheating-Immune Secret Sharing Schemes from Maiorana-McFarland Boolean Functions

Romar B. dela Cruz[1](✉) and Say Ol[2]

[1] Institute of Mathematics, University of the Philippines Diliman,
Quezon City, Philippines
rbdelacruz@math.upd.edu.ph

[2] Teacher Education College, Phnom Penh, Cambodia
say_ol@yahoo.com

Abstract. We consider cheating-immune secret sharing schemes proposed by Pieprzyk and Zhang. This type of secret sharing scheme keeps dishonest participants from having a better chance (over the honest ones) of knowing the secret using their incorrect shares. We show that the class of Maiorana-McFarland Boolean functions can be used to construct such schemes. Consequently, new cheating-immune secret sharing schemes are presented.

Keywords: Secret sharing scheme · Boolean function · Error-correcting code

1 Introduction

A *secret sharing scheme* (SSS) is a technique of allocating access to a secret among a set of participants in such a way that only certain subsets are allowed to determine the secret. It was introduced independently by Shamir [30] and Blakley [1] for the protection of cryptographic keys. It is now a fundamental primitive as it is used to construct cryptographic protocols such as for secure multiparty computation [12] and oblivious transfer [32].

In general, an SSS starts with the *share distribution* phase followed by the *secret reconstruction* phase. In the share distribution phase, there is a dealer who produces the shares to be given to the participants. In the secret reconstruction phase, a subset of participants attempt to determine the secret using their shares. We consider the setting wherein the participants submit their shares to a trusted combiner who reconstructs the secret. We assume that the dealer and combiner are honest but the participants can cheat during secret reconstruction.

Tompa and Woll [33] showed that if a secret sharing scheme is linear, then it can be subjected to an attack from dishonest participants. During the secret reconstruction phase, the cheaters can submit invalid shares to the combiner. As a result, the combiner returns an invalid secret and the cheaters are able to

K. Lee (Ed.): ICISC 2018, LNCS 11396, pp. 233–247, 2019.
https://doi.org/10.1007/978-3-030-12146-4_15

compute the valid secret using their valid shares and the invalid secret. This attack also prevents the honest participants from knowing the valid secret. Several approaches to counter this attack can be found in the literature (for instance see [2,6,11,19,21,25,29]). The survey article by Martin [24] is a comprehensive analysis of the different types of SSS that handle dishonest participants, dealers and combiners.

This work deals with *cheating-immune secret sharing schemes* proposed by Pieprzyk and Zhang [28]. This type of SSS is capable of preventing the dishonest participants of gaining an advantage over the honest ones in the attack described above. In a cheating-immune scheme, the cheaters will not be able to determine the secret even if they submit invalid shares during reconstruction. If we compare with the other SSS that deal with cheating, there is no detection or identification of cheaters in a cheating-immune scheme. There is also no correction of the submitted invalid shares which means that the honest participants also do not recover the secret. A nice property of cheating-immune schemes is that the share size is the same as the secret size (in other schemes, either we have large shares or the recovery of the secret requires more than the minimum number of shares). The main problem in the theory of cheating-immune schemes is the construction of such schemes for any access structure. Properties and constructions of such schemes are studied in [4,13,14,22,23,26,27].

In this paper, we show that the class of Maiorana-McFarland Boolean functions can be used to construct cheating-immune schemes and we present new schemes. We used the techniques in the work of Carlet [9]. Our method of construction can be seen as a generalization of the method in [14]. This paper is organized as follows. Section 2 contains the definition and model of binary cheating-immune schemes. In Sect. 3, we present the relation between cheating-immune schemes and Boolean functions. Sections 4, 5 and 6 contain the main results of the paper. We summarize the work in the last section.

2 Cheating-Immune Secret Sharing Schemes

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of n participants. The set of all authorized or qualified subsets $\Gamma \subseteq 2^{\mathcal{P}}$ is called the *access structure.*

Definition 1. *A secret sharing scheme realizing an access structure Γ is a method to distribute shares of a secret K such that*

i. if a subset of participants $A \in \Gamma$ then A can reconstruct the secret K
ii. if a subset of participants $B \notin \Gamma$ then B cannot reconstruct the secret K.

We say that a secret sharing scheme is *perfect* if unauthorized subsets obtain no information about the secret. Otherwise, the scheme is *non-perfect*, that is, it is possible for an unauthorized subset to obtain partial information about the secret. A measure of efficiency of a secret sharing scheme is the so-called *information rate* which is the ratio of the size of the secret and the size of the shares. We assume that the dealer selects the secrets uniformly at random.

We use the model of a cheating-immune (n,n)-SSS over $\mathbb{F}_2$ introduced in [26]. The scheme is represented by a *defining function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ that maps each possible vector of shares $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ to a secret K. All participants must submit their shares to the combiner in order to reconstruct the secret. Let $\alpha, \beta \in \mathbb{F}_2^n$. We say that β *covers* α, denoted by $\alpha \preceq \beta$, if whenever $\alpha_i \neq 0$ then $\beta_i \neq 0$, $1 \leq i \leq n$. The *Hamming weight* of a vector α will be denoted by $wt(\alpha)$.

We represent the cheaters by a *cheating vector* δ with $\delta_i = 1$ if P_i is a cheater and 0 otherwise. Hence, $wt(\delta)$ gives the number of cheaters. Given two vectors x and δ, we distinguish the shares of the cheaters from the honest participants using the following vectors:

i. $x_\delta^+ = (x_1^+, \ldots, x_n^+)$ with $x_i^+ = x_i$ if $\delta_i = 1$ and $x_i^+ = 0$ if $\delta_i = 0$
ii. $x_\delta^- = (x_1^-, \ldots, x_n^-)$ with $x_i^- = x_i$ if $\delta_i = 0$ and $x_i^- = 0$ if $\delta_i = 1$

The vector x_δ^+ represents the cheaters' valid shares while x_δ^- represents the honest participants' shares.

Recall that when cheaters submit invalid shares during reconstruction, they will use the secret (sent by the combiner) to determine the true secret. Consider now the following sets of shares:

$$R(\delta, \alpha_\delta^+, K) = \{x_\delta^- \mid f(x_\delta^- \oplus \alpha_\delta^+) = K\}$$
$$R(\delta, \alpha_\delta^+ \oplus \delta, K^*) = \{x_\delta^- \mid f(x_\delta^- \oplus \alpha_\delta^+ \oplus \delta) = K^*\}$$

The set $R(\delta, \alpha_\delta^+, K)$ consists of all possible shares of honest participants such that combined with the cheaters' valid shares, will produce the original secret K. On the other hand, the set $R(\delta, \alpha_\delta^+ \oplus \delta, K^*)$ contains all the possible shares of honest participants such that combined with the cheaters' incorrect shares, will produce the secret K^*. The *probability of successful cheating with respect to* δ, α is given by

$$\rho_{\delta,\alpha} = |R(\delta, \alpha_\delta^+ \oplus \delta, K^*) \cap R(\delta, \alpha_\delta^+, K)| / |R(\delta, \alpha_\delta^+ \oplus \delta, K^*)|.$$

We now define a k-cheating-immune (n,n)-SSS or k-CI (n,n)-SSS. Note that we assume that all cheaters submit invalid shares during reconstruction.

Definition 2. *An (n,n)-SSS over $\mathbb{F}_2$ is k-cheating-immune if for every $\alpha, \delta \in \mathbb{F}_2^n$ with $1 \leq wt(\delta) \leq k$, we have $\rho_{\delta,\alpha} = 1/2$.*

The general case where not all cheaters submit invalid shares is handled by the so-called *strictly cheating-immune secret sharing schemes*. In this type of scheme, we use two vectors $\delta, \tau \in \mathbb{F}_2^n$ such that δ represents the cheaters while τ represents the cheaters who submitted fake shares. Note that $\tau \preceq \delta$. The value

$$\rho_{\delta,\tau,\alpha} = |R(\delta, \alpha_\delta^+ \oplus \tau, K^*) \cap R(\delta, \alpha_\delta^+, K)| / |R(\delta, \alpha_\delta^+ \oplus \tau, K^*)|$$

is the *probability of successful cheating with respect to* δ, τ, α.

Definition 3. *An (n,n)-SSS over $\mathbb{F}_2$ is strictly k-cheating-immune if, for every $\alpha, \delta, \tau \in \mathbb{F}_2^n$ such that $1 \leq wt(\delta) \leq k$ and $\tau \preceq \delta$, we have that $\rho_{\delta,\tau,\alpha} = 1/2$.*

3 Cheating-Immune Schemes and Boolean Functions

We now describe the connection between Boolean functions and cheating-immune secret sharing schemes. The defining function of an (n, n)-SSS over $\mathbb{F}_2$ is a Boolean function on $\mathbb{F}_2^n$. We recall some basic concepts in the theory of Boolean functions (for reference, see [8,10]).

A Boolean function f is *affine* if $f(x_1, x_2, \ldots, x_n) = a_1x_1 \oplus a_1x_2 \oplus \ldots \oplus a_nx_n \oplus c$. The affine function f is *linear* if $c = 0$. We say that f is *balanced* on $\mathbb{F}_2^n$ if $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$. A nonconstant affine function is balanced.

A Boolean function f is said to be *k-resilient* if for every subset $\{j_1, j_2, \ldots, j_k\}$ of $\{1, 2, \ldots, n\}$ and every $(a_1, a_2, \ldots, a_k) \in \mathbb{F}_2^k$, the restricted function

$$f(x_1, x_2, \ldots, x_n)|_{x_{j_1}=a_1, x_{j_2}=a_2, \ldots, x_{j_k}=a_k}$$

is balanced on $\mathbb{F}_2^{n-k}$. We note that if f is k-resilient then it is also l-resilient for $0 \leq l \leq k$.

We say that a Boolean function f satisfies the *strengthened propagation of degree* k or $SP(k)$ if for any $\delta \in \mathbb{F}_2^n$ such that $1 \leq wt(\delta) \leq k$, and for any $\tau \preceq \delta$, the function $f(x_{\delta}^{-} \oplus \tau) \oplus f(x_{\delta}^{-} \oplus \tau \oplus \delta)$ is balanced. A function f satisfying $SP(k)$ also satisfies $SP(l)$ for $1 \leq l \leq k$.

The following theorems characterize cheating-immune (n, n)-SSS:

Theorem 1 ([27]). *An (n, n)-SSS over $\mathbb{F}_2$ with defining function f is k-CI if and only if f is k-resilient and satisfies $SP(k)$.*

Theorem 2 ([27]). *An (n, n)-SSS over $\mathbb{F}_2$ with defining function f is strictly k-CI if and only if the following conditions are satisfied:*

1. *f is k-resilient.*
2. *For any integer l with $0 \leq l \leq k-1$, every function obtained from f by fixing any l input variables satisfies $SP(k-l)$.*

A bound on the number of cheaters is given by the following result:

Theorem 3 ([4]). *An (n, n)-SSS over $\mathbb{F}_2$ with defining function f can be k-cheating-immune only if $2k \leq n-2$.*

4 Cheating-Immune SSS from Maiorana-McFarland Boolean Functions

Theorem 1 states that constructing a k-CI (n, n)-SSS over $\mathbb{F}_2$ is equivalent to constructing a Boolean function satisfying resiliency and strengthened propagation. In this section, we will show that a class of *Maiorana-McFarland* Boolean functions can be used to construct cheating-immune SSS. The Maiorana-McFarland Boolean functions are well-studied and these functions are used to build Boolean functions with cryptographic properties.

Let s, t be positive integers and ϕ be a vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_2^s$, or a (t, s)-vectorial function given by

$$\phi(x_1, x_2, \ldots, x_t) = (\phi_1(x_1, x_2, \ldots, x_t), \phi_2(x_1, x_2, \ldots, x_t), \ldots, \phi_s(x_1, x_2, \ldots, x_t))$$

where its coordinate functions $\phi_1, \phi_2, \ldots, \phi_s$ are t-variable Boolean functions. Let g be a t-variable Boolean function. An $(s+t)$-variable Boolean function f defined by

$$f(x, y) = x \cdot \phi(y) \oplus g(y),$$

where $x \in \mathbb{F}_2^s, y \in \mathbb{F}_2^t$ is said to be of *Maiorana-McFarland* form. We call f an *MM function* for short.

The next theorem gives a condition under which a Maiorana-McFarland function satisfies resiliency.

Theorem 4 **([7]).** *An MM function $f(x, y) = x \cdot \phi(y) \oplus g(y)$ is k-resilient if for every $y \in \mathbb{F}_2^t$, we have $wt(\phi(y)) \geq k + 1$.*

We now show that this class of functions also satisfies strengthened propagation criterion. We will use the following lemma.

Lemma 1. *A Boolean function f is balanced on $\mathbb{F}_2^n$ if there exists a subset $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ such that for every $a = (a_1, a_2, \ldots, a_k) \in \mathbb{F}_2^k$, the restricted function f_a obtained from f by substituting $x_{i_1} = a_1, x_{i_2} = a_2, \ldots, x_{i_k} = a_k$ is balanced.*

Proof. For every $a \in \mathbb{F}_2^k$, by assumption, f_a is balanced on $\mathbb{F}_2^{n-k}$. Hence, we have $|f_a^{-1}(0)| = |f_a^{-1}(1)| = 2^{n-k-1}$. Since there are 2^k possibilities for a, then $|f^{-1}(0)| = |f^{-1}(1)| = 2^k \times 2^{n-k-1} = 2^{n-1}$. Thus, f is balanced on $\mathbb{F}_2^n$.

A modification of the construction of Boolean functions satisfying propagation criterion using *Maiorana-McFarland* Boolean functions considered by [9] gives us a construction of Boolean functions satisfying strengthened propagation.

Theorem 5. *An MM function $f(x, y) = x \cdot \phi(y) \oplus g(y)$ satisfies $SP(k)$ if the following conditions are satisfied:*

1. *For any $a \in \mathbb{F}_2^s$ such that $1 \leq wt(a) \leq k$, the function $a \cdot \phi(y)$ is balanced on $\mathbb{F}_2^t$.*
2. *For any $y, z \in \mathbb{F}_2^t$ such that $wt(y \oplus z) \geq 1$, we have $wt(\phi(y) \oplus \phi(z)) \geq k$.*

Proof. Let $z = (x, y) = (x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_t)$. For any $\delta, \tau \in \mathbb{F}_2^{s+t}$ such that $1 \leq wt(\delta) \leq k$ and $\tau \preceq \delta$, we denote by $\delta = (\delta^x, \delta^y)$ and $\tau = (\tau^x, \tau^y)$ where $\delta^x = (\delta_1, \delta_2, \ldots, \delta_s), \tau^x = (\tau_1, \tau_2, \ldots, \tau_s), \delta^y = (\delta_{s+1}, \delta_{s+2}, \ldots, \delta_{s+t})$ and $\tau^y = (\tau_{s+1}, \tau_{s+2}, \ldots, \tau_{s+t})$.

Define $h(z_{\bar{\delta}}) = f(z_{\bar{\delta}} \oplus \tau) \oplus f(z_{\bar{\delta}} \oplus \tau \oplus \delta)$. Then,

$$\begin{aligned} h(z_{\bar{\delta}}) &= f(x_{\bar{\delta^x}} \oplus \tau^x, y_{\bar{\delta^y}} \oplus \tau^y) \oplus f(x_{\bar{\delta^x}} \oplus \tau^x \oplus \delta^x, y_{\bar{\delta^y}} \oplus \tau^y \oplus \delta^y) \\ &= a(y_{\bar{\delta^y}}) \cdot x_{\bar{\delta^x}} \oplus b(y_{\bar{\delta^y}}) \end{aligned}$$

where

$$
\begin{aligned}
a(y^-_{\delta^y}) &= \phi(y^-_{\delta^y} \oplus \tau^y) \oplus \phi(y^-_{\delta^y} \oplus \tau^y \oplus \delta^y)\\
b(y^-_{\delta^y}) &= \tau^x \cdot \phi(y^-_{\delta^y} \oplus \tau^y) \oplus (\tau^x \oplus \delta^x) \cdot \phi(y^-_{\delta^y} \oplus \tau^y \oplus \delta^y) \oplus\\
&\quad\; g(y^-_{\delta^y} \oplus \tau^y) \oplus g(y^-_{\delta^y} \oplus \tau^y \oplus \delta^y)
\end{aligned}
$$

Case 1. If $\delta^y = 0$ then $\tau^y = 0, y^-_{\delta^y} = y$ and $wt(\delta^x) = wt(\delta)$. Hence, $h(z^-_\delta) = \delta^x \cdot \phi(y)$ is balanced by the first condition.

Case 2. If $\delta^y \neq 0$ then $0 \leq wt(\delta^x) \leq k-1$. In other words, the number of constant coordinates of $x^-_{\delta^x}$ is less than or equal to $k-1$. For every substitution of $t - wt(\delta^y)$ variables in $y^-_{\delta^y}$, by the second condition, $wt(a(y^-_{\delta^y})) \geq k$. Hence, the function obtained from $h(z^-_\delta)$ by the substitution is a non-constant affine function which is balanced. Therefore, $h(z^-_\delta)$ is balanced by Lemma 1.

In conclusion, the function f satisfies $SP(k)$.

5 Construction of CI-SSS Using Binary Systematic Codes

Similar to what was done on [9], we use binary systematic codes to come up with concrete examples of functions satisfying the conditions in Theorems 4 and 5. This method of construction is a generalization of [14] which uses linear codes. The technique used here allows us to use nonlinear codes. We start with a discussion of some basic concepts on binary codes (the reader is referred to [18,20] for a complete treatment of codes).

A nonempty subset $C \subseteq \mathbb{F}_2^n$ is called a *binary code* of length n. The *Hamming distance* between two vectors $x, y \in \mathbb{F}^n$, denoted by $d(x, y)$, is the number of positions where x and y differ. The *minimum distance* of C is defined as

$$d(C) = \min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

A binary code of length n having M codewords and minimum distance d is called an *(n, M, d)-code*. The distance from a vector $\alpha \in \mathbb{F}_2^n$ to a code C is given by $d(\alpha, C) = \min\{d(\alpha, c) \,|\, c \in C\}$. The *covering radius* of C is defined to be $\rho = \max\{d(x, C) \,|\, x \in \mathbb{F}_2^n\}$.

Definition 4. *A binary code C is said to be k-systematic if there exists k positions $i_1, \ldots, i_k$ such that every element of $\mathbb{F}_2^k$ appears in exactly one codeword of C in the specified positions. The set $\{i_1, i_2, \ldots, i_k\}$ is called an information set of C.*

Let C be a binary k-systematic code. It follows from the definition that C has 2^k codewords. Let $c = (c_1, c_2, \ldots, c_n) \in C$. The coordinates $c_{i_1}, c_{i_2}, \ldots, c_{i_k}$ are called *information bits* and the remaining coordinates are called *parity-check bits*. Hence, if all of the parity-check bits of a binary k-systematic code are deleted, we obtain the code $\mathbb{F}_2^k$.

A *binary linear code* C is a k-dimensional subspace of $\mathbb{F}_2^n$. A binary linear code of length n, dimension k and minimum distance d is called an $[n, k, d]$-code.

A $k \times n$ matrix whose rows form a basis of C is called a *generator matrix.* The *dual code* of C is its $(n-k)$-dimensional dual space $C^{\perp} = \{x \in \mathbb{F}_2^n \,|\, c \cdot x = 0, \forall c \in C\}$. Note that a binary linear code is k-systematic.

Let C be an (n, M, d) binary code and let

$$B_i = \frac{1}{|C|} \sum_{c \in C} |\{x \in C \,|\, d(c, x) = i\}|.$$

The list $B_1, B_2, \ldots, B_n$ is called the *distance distribution* of C. The homogeneous polynomial $D_C(x, y) = \sum_{i=0}^{n} B_i x^{n-i} y^i$ is called the *distance enumerator* of C. The *dual distance* of an (n, M, d) binary code C is the smallest positive integer d' such that the coefficient of $x^{n-d'} y^{d'}$ of $D_C(x+y, x-y)$ is nonzero. In the case that C is linear, the dual distance is the same as the minimum distance of $C^{\perp}$.

Due to the notion of equivalence of codes, we can assume that the information set of a given systematic code is the set $\{1, \ldots, k\}$. We also assume that the generator matrix of a given linear code is in standard form, i.e. $[I_k \mid A]$ where I_k is the identity matrix of order k and A is a $k \times (n-k)$ binary matrix.

We now proceed with the construction of cheating-immune schemes using binary systematic codes.

Lemma 2 **([9]).** *Let C be a binary code of length s with dual distance d'. Then, for every $a \in \mathbb{F}_2^s$ such that $1 \leq wt(a) \leq d' - 1$, the s-variable Boolean function $\psi(x) = a \cdot x$ is still balanced when its domain is restricted to C.*

Theorem 6. *An MM function $f(x, y) = x \cdot \phi(y) \oplus g(y)$ satisfies $SP(k)$ if the (t, s)-vectorial function ϕ is injective and the code $\phi(\mathbb{F}_2^t)$ has minimum distance $d \geq k$ and dual distance $d' \geq k + 1$.*

Proof. We will show that the conditions of Theorem 5 are satisfied. For any $a \in \mathbb{F}_2^s$ such that $1 \leq wt(a) \leq k$, the s-variable Boolean function $\psi(x) = a \cdot x$ is balanced on $\phi(\mathbb{F}_2^t)$ (because $k \leq d' - 1$) thanks to Lemma 2. Since ϕ is injective, for any $z \in \phi(\mathbb{F}_2^t)$, there is a unique $y \in \mathbb{F}_2^t$ such that $z = \phi(y)$. Thus, the composition $(\psi \circ \phi)(y) = a \cdot \phi(y)$ is balanced on $\mathbb{F}_2^t$. For any $y, z \in \mathbb{F}_2^t$ with $wt(y \oplus z) \geq 1$, $wt(\phi(y) \oplus \phi(z)) \geq k$ because ϕ is injective and $\phi(\mathbb{F}_2^t)$ has minimum distance $d \geq k$.

Theorem 7. *Let C be an $(s, 2^t, d)$ binary t-systematic code with dual distance d' and covering radius ρ. Let $k = \min\{d, d' - 1, \rho - 1\}$ and $\alpha \in \mathbb{F}_2^s$ such that $d(\alpha, C) \geq k + 1$. Define the (t, s)-vectorial function $\phi(x) = \alpha \oplus (x, u(x))$ where $u(x)$ is vector of $(s - t)$ parity-check bits of a codeword of C whose t information bits are represented by the vector x. Let g be an arbitrary t-variable Boolean function. Then the MM function $f(x, y) = x \cdot \phi(y) \oplus g(y)$ defines a k-CI $(s + t, s + t)$-SSS.*

Proof. For every $y \in \mathbb{F}_2^t$, $wt(\phi(y)) \geq d(\alpha, C) = k + 1$. By Theorem 4, f is k-resilient. The code $\phi(\mathbb{F}_2^t) = \alpha \oplus C$ has the same minimum distance $d \geq k$ and the same dual distance $d' \geq k + 1$ as C. By Theorem 5, f satisfies $SP(k)$. Due to Theorem 1, the $(s + t, s + t)$-SSS defined by f is k-CI.

We present examples of schemes obtained using the preceding theorem. The computations were performed using Magma [5]. In case that C is linear with generator matrix G, the function ϕ can be written as $\phi(y) = \alpha \oplus yG$. Then the defining function f will be $f(x, y) = x \cdot (\alpha \oplus yG) \oplus g(y)$.

Example 1 **(a new scheme)**. Let C be the $[12, 5, 4]$ binary linear code with dual distance $d' = 4$, covering radius $\rho = 4$ and generator matrix

$$G = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1 \\ 0\,1\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1 \\ 0\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0\,1 \\ 0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0 \end{bmatrix}.$$

Using $\alpha = (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$ with $d(\alpha, C) = 4$, we obtain a 3-CI $(17, 17)$-SSS.

Example 2 **(using some classes of linear codes)**

a. 1-CI $(m + 1, m + 1)$-SSS: For $m \geq 4$, let $C = \mathcal{R}_m$, the $[m, 1, m]$ binary repetition code with dual distance $d^{\perp} = 2$ and covering radius $\rho = \lfloor \frac{n}{2} \rfloor$. Choose α such that $d(\alpha, C) = 2$.
b. 2-CI $(2^m + m - 1, 2^m + m - 1)$-SSS: For $m \geq 3$, let $C = \mathcal{S}_m$, the $[2^m - 1, m, 2^{m-1}]$ binary *Simplex* code with dual distance $d^{\perp} = 3$ and covering radius $\rho = 2^{m-1} - 1$. Choose α such that $d(\alpha, C) = 3$.
c. 3-CI $(2^m + m + 1, 2^m + m + 1)$-SSS: For $m \geq 4$, let $C = \mathcal{R}(1, m)$, the $[2^m, m + 1, 2^{m-1}]$ first-order *Reed-Muller* code with dual distance $d^{\perp} = 4$ and covering radius $2^{m-1} - 2^{\lceil m/2 \rceil - 1} \leq \rho \leq 2^{m-1} - 2^{m/2-1}$ [17]. Choose α such that $d(\alpha, C) \geq 4$.

Example 3 **(using nonlinear codes)**. For even integer $m \geq 4$, there exists two well-known classes of binary nonlinear systematic codes [20]:

i. $(2^m, 2^{2m}, 2^{m-1} - 2^{\frac{m}{2}-1})$ *Kerdock* code $\mathcal{K}(m)$ with dual distance 6 and covering radius $2^{m-1} - 2^{\frac{m}{2}-1}$
ii. $(2^m, 2^{2^m - 2m}, 6)$ *Preparata* code $\mathcal{P}(m)$ with dual distance $2^{m-1} - 2^{\frac{m}{2}-1}$ and covering radius 3.

We use these codes to obtain the following schemes:

a. 2-CI $(2^{m+1} - 2m, 2^{m+1} - 2m)$-SSS: For even integer $m \geq 4$, let $C = \mathcal{P}(m)$ and choose $\alpha \in \mathbb{F}_2^m$ such that $d(\alpha, \mathcal{P}(m)) = 3$.
b. 5-CI $(2^m + 2m, 2^m + 2m)$-SSS: For even integer $m \geq 6$, let $C = \mathcal{K}(m)$ and choose $\alpha \in \mathbb{F}_2^m$ such that $d(\alpha, \mathcal{K}(m)) = 6$.

6 Strictly Cheating-Immune SSS

Here we consider the construction of strictly cheating-immune SSS from the class of Maiorana-McFarland Boolean functions. The goal is to construct functions satisfying the conditions given by Theorem 2. The next theorem talks about the strengthened propagation property.

Theorem 8. *Let $f(x, y) = x \cdot \phi(y) \oplus g(y)$ be an MM function satisfying the following conditions:*

1. *for any $a \in \mathbb{F}_2^s$ with $1 \leq wt(a) \leq k$, the function $a \cdot \phi(y)$ on $\mathbb{F}_2^t$ is $(k-1)$-resilient;*
2. *for any $y, z \in \mathbb{F}_2^t$ if $1 \leq wt(y \oplus z) \leq k$, we have $wt(\phi(y) \oplus \phi(z)) \geq k$.*

Then, for any integer l with $0 \leq l \leq k-1$, every function obtained from f by keeping any l input variables constant satisfies $SP(k-l)$.

Proof. Let $z = (x, y)$. For any integer l with $0 \leq l \leq k-1$, we denote by $\underline{x}$ and $\underline{y}$ the vectors obtained from x and y by fixing u and v coordinates constant such that $u + v = l$. If we let $\underline{z} = (\underline{x}, \underline{y})$ then $f(\underline{z})$ is the $(s+t-l)$-variable Boolean function obtained from f by fixing l input variables.

Now we show that $f(\underline{z})$ satisfies $SP(k-l)$. Let $\delta, \tau \in \mathbb{F}_2^n$, $n = s+t$, such that $\tau \preceq \delta, 1 \leq wt(\delta) \leq k-l$ and the set of nonzero coordinates of δ is a subset of the nonconstant coordinates of $\underline{z}$. We write $\delta = (\delta^{\underline{x}}, \delta^{\underline{y}})$ and $\tau = (\tau^{\underline{x}}, \tau^{\underline{y}})$ where $\delta^{\underline{x}}$ and $\tau^{\underline{x}}$ are the first s coordinates of δ and τ, and $\delta^{\underline{y}}$ and $\tau^{\underline{y}}$ are the remaining t coordinates of δ and τ, respectively.

Define $h(\underline{z_{\delta}}^{-}) = f(\underline{z_{\delta}}^{-} \oplus \tau) \oplus f(\underline{z_{\delta}}^{-} \oplus \tau \oplus \delta)$. Then $h(\underline{z_{\delta}}^{-}) = \underline{x_{\delta^{\underline{x}}}}^{-} \cdot a(\underline{y_{\delta^{\underline{y}}}}^{-}) \oplus b(\underline{y_{\delta^{\underline{y}}}}^{-})$ where

$$\begin{aligned} a(\underline{y_{\delta^{\underline{y}}}}^{-}) &= \phi(\underline{y_{\delta^{\underline{y}}}}^{-} \oplus \tau^{\underline{y}}) \oplus \phi(\underline{y_{\delta^{\underline{y}}}}^{-} \oplus \tau^{\underline{y}} \oplus \delta^{\underline{y}}) \\ b(\underline{y_{\delta^{\underline{y}}}}^{-}) &= \tau^{\underline{x}} \cdot \phi(\underline{y_{\delta^{\underline{y}}}}^{-} \oplus \tau^{\underline{y}}) \oplus (\tau^{\underline{x}} \oplus \delta^{\underline{x}}) \cdot \phi(\underline{y_{\delta^{\underline{y}}}}^{-} \oplus \tau^{\underline{y}} \oplus \delta^{\underline{y}}) \oplus \\ &\qquad g(\underline{y_{\delta^{\underline{y}}}}^{-} \oplus \tau^{\underline{y}}) \oplus g(\underline{y_{\delta^{\underline{y}}}}^{-} \oplus \tau^{\underline{y}} \oplus \delta^{\underline{y}}) \end{aligned}$$

Case 1. If $\delta^{\underline{y}} = 0$ then $\underline{y_{\delta^{\underline{y}}}}^{-} = \underline{y}, \tau^{\underline{y}} = 0$ and $1 \leq wt(\delta^{\underline{x}}) = wt(\delta) \leq k-l \leq k$. By the first condition, $\delta^{\underline{x}} \cdot \phi(y)$ is $(k-1)$-resilient. In addition, $v = l-u \leq l \leq k-1$. Hence, $h(\underline{z_{\delta}}^{-}) = \delta^{\underline{x}} \cdot \phi(\underline{y})$ is balanced because it is obtained from the function $\delta^{\underline{x}} \cdot \phi(y)$ by fixing v input variables constant.

Case 2. If $\delta^{\underline{y}} \neq 0$ then $0 \leq wt(\delta^{\underline{x}}) < wt(\delta) \leq k-l$. Hence, the number of constant coordinates of $\underline{x_{\delta^{\underline{x}}}}^{-}$ is $u + wt(\delta^{\underline{x}}) \leq l + (k-l-1) = k-1$. For every substitution of the $t - v - wt(\delta^{\underline{y}})$ variables in $\underline{y_{\delta^{\underline{y}}}}^{-}$, by the second condition, $wt(a(\underline{y_{\delta^{\underline{y}}}}^{-})) \geq k$. Hence, the function obtained from $h(\underline{z_{\delta}}^{-})$ by the substitution is a non-constant affine function which is balanced. Therefore, $h(\underline{z_{\delta}}^{-})$ is balanced by Lemma 1.

In conclusion, the function $f(\underline{z})$ satisfies $SP(k-l)$.

An (s, t)-vectorial function ϕ is balanced if for every $y \in \mathbb{F}_2^t$, $|\phi^{-1}(y)| = 2^{s-t}$. The function ϕ is said to be k-resilient if it is balanced and every function obtained from ϕ by keeping k input variables constant is balanced.

Lemma 3 **([3]).** *Let ϕ be a (t,r)-vectorial k-resilient function and ψ be an (r,s)-vectorial balanced function. Then the (t,s)-vectorial function $\psi \circ \phi$ is k-resilient.*

We now look at the construction of a function ϕ satisfying the conditions of Theorem 8. Similar to [9], we split ϕ into a composition of two simpler vectorial functions.

Theorem 9. *Suppose that $\phi = \phi_2 \circ \phi_1$ where ϕ_1 is a (t,r)-vectorial function and ϕ_2 is an (r,s)-vectorial function with the following properties:*

1. (a) ϕ_1 is $(k-1)$-resilient;
(b) for any $y,z \in \mathbb{F}_2^t$ with $1 \leq wt(y \oplus z) \leq k$, we have $wt(\phi_1(y) \oplus \phi_1(z)) \geq 1$;
2. (a) for any $a \in \mathbb{F}_2^s$ with $1 \leq wt(a) \leq k$, the function $a \cdot \phi_2(y)$ is balanced;
(a) for any $y,z \in \mathbb{F}_2^r$ with $wt(y \oplus z) \geq 1$, we have $wt(\phi_2(y) \oplus \phi_2(z)) \geq k$.

Then ϕ satisfies the condition of Theorem 8.

Proof. From $1(a)$ and $2(a)$, for any $a \in \mathbb{F}_2^s$ with $1 \leq wt(a) \leq k$, $a \cdot \phi(y) = a \cdot (\phi_2 \circ \phi_1)(y) = (a \cdot \phi_2) \circ \phi_1(y)$ is $(k-1)$-resilient thanks to Lemma 3. Hence, the first condition of Theorem 8 is satisfied. The $1(b)$ and $2(b)$ trivially imply the second condition of Theorem 8.

Next, we use binary systematic codes to construct ϕ_1 and ϕ_2. First we recall a connection between codes and orthogonal arrays. A *binary (n,k,λ)-orthogonal array* is a $\lambda 2^k \times n$ array such that for any k columns, every element of $\mathbb{F}_2^k$ appears in exactly λ rows. A binary orthogonal array is said to be simple if no two rows are identical. A *large set of binary (n,k,λ)-orthogonal arrays* is a set of $2^{n-k}/\lambda$ simple (n,k,λ)-orthogonal arrays such that every element of $\mathbb{F}_2^n$ appears in exactly one of the (n,k,λ)-orthogonal arrays in the set.

Lemma 4 [15]**.** *An $(n,2^k,d)$-binary k-systematic code C with dual distance d' is also a binary $(n,d'-1,2^{k-d'+1})$-orthogonal array.*

A relation between resilient functions and orthogonal arrays is given by the following lemma:

Lemma 5 [31]**.** *A k-resilient (t,r)-vectorial function is equivalent to a large set of binary $(t,k,2^{t-r-k})$-orthogonal arrays.*

The next two results concern the functions ϕ_1 and ϕ_2.

Theorem 10. *Let C_1 be a $(t,2^{t-r},d_1)$-binary $(t-r)$-systematic code with $d_1 \geq k+1$ and dual distance $d_1' \geq k$. Let $\phi_1(x,y) = u(x) \oplus y$ be a (t,r)-vectorial function where $x \in \mathbb{F}_2^{t-r}, y \in \mathbb{F}_2^r$ and $u(x)$ is vector of parity-check bits of a codeword of C_1 whose information bits are represented by the vector x. Then ϕ_1 has the following properties:*

1. ϕ_1 is $(k-1)$-resilient; and
2. for any $y,z \in \mathbb{F}_2^t$ with $1 \leq wt(y \oplus z) \leq k$, we have $wt(\phi_1(y) \oplus \phi_1(z)) \geq 1$.

Proof. For any $z \in \mathbb{F}_2^r$, consider $\phi_1^{-1}(z) = \{(x, y) \,|\, \phi_1(x, y) = z, x \in \mathbb{F}^{t-r}$ and $y \in \mathbb{F}^r\}$. Since $\phi_1(x, y) = z \Leftrightarrow y = u(x) \oplus z$, we get $\phi_1^{-1}(z) = \{(x, u(x) \oplus z) \,|\, x \in \mathbb{F}_2^{t-r}\}$. Let $\mathbf{0} \in \mathbb{F}_2^{t-r}$ be the zero vector of length $t-r$. Then $\phi_1^{-1}(z) = (\mathbf{0}, z) \oplus C_1$ is a $(t, 2^{t-r}, d_1)$-binary $(t-r)$-systematic code with dual distance d_1'. By Lemma 4, $\phi_1^{-1}(z)$ is a binary $(t, d_1' - 1, 2^{t-r-d_1'+1})$-orthogonal array. It is also a binary $(t, k-1, 2^{t-r-k+1})$-orthogonal array since $k \le d_1'$. By Lemma 5, ϕ_1 is $(k-1)$-resilient.

For any $y, z \in \mathbb{F}_2^t$ with $1 \le wt(y \oplus z) \le k$, suppose that $wt(\phi_1(y) \oplus \phi_1(z)) = 0$. It follows that $y, z \in \phi_1^{-1}(w)$ for some $w \in \mathbb{F}_2^r$. Since $\phi_1^{-1}(w) = (\mathbf{0}, w) \oplus C_1$ has minimum distance $d_1 \ge k+1$, we obtain $wt(y \oplus z) \ge k+1$, a contradiction. Consequently, $wt(\phi_1(y) \oplus \phi_1(z)) \ge 1$.

Theorem 11. *Let C_2 be an $(s, 2^r, d_2)$-binary r-systematic code with $d_2 \ge k$ and dual distance $d_2' \ge k+1$. Let $\phi_2(y) = \alpha \oplus (y, v(y))$ where $y \in \mathbb{F}_2^r, \alpha \in \mathbb{F}_2^s$ and $v(y)$ is a vector of parity-check bits of a codeword of C_2 whose information bits are represented by the vector y. Then ϕ_2 has the following properties:*

1. *for any $a \in \mathbb{F}_2^s$ with $1 \le wt(a) \le k$, the function $a \cdot \phi_2(y)$ is balanced; and*
2. *for any $y, z \in \mathbb{F}_2^r$ with $wt(y \oplus z) \ge 1$, we have $wt(\phi_2(y) \oplus \phi_2(z)) \ge k$.*

Proof. For an arbitrary $\alpha \in \mathbb{F}_2^s$, ϕ_2 is injective (see the proof of Theorem 6).

We now present a construction of strictly cheating-immune schemes from Maiorana-McFarland functions.

Theorem 12. *Let $C_1 = \{(x, u(x)) \,|\, x \in \mathbb{F}_2^{t-r}\}$ be a $(t, 2^{t-r}, d_1)$-binary $(t-r)$-systematic code with dual distance d_1' and let $\phi_1(x, y) = u(x) \oplus y$ be a (t, r)-vectorial function where $x \in \mathbb{F}_2^{t-r}, y \in \mathbb{F}_2^r$. Suppose that $C_2 = \{(x, v(x)) \,|\, x \in \mathbb{F}_2^r\}$ is an $(s, 2^r, d_2)$-binary r-systematic code with dual distance d_2' and covering radius ρ. Let $k = \min\{d_1 - 1, d_1' d_2, d_2' - 1, \rho - 1\}$ and let $\phi_2(y) = \alpha \oplus (y, v(y))$ be a (r, s)-vectorial function where $y \in \mathbb{F}_2^r, \alpha \in \mathbb{F}_2^s$ such that $d(\alpha, C_2) \ge k+1$. Define $\phi = \phi_2 \circ \phi_1$ and $f(x, y, z) = x \cdot \phi(y, z) \oplus g(y, z)$ where $x \in \mathbb{F}_2^s$ and g is an arbitrary t-variable Boolean function. Then the MM function f defines a k-CI $(s+t, s+t)$-SSS.*

Proof. Since $\phi(\mathbb{F}_2^t) = \alpha \oplus C_2$ then for any $(y, z) \in \mathbb{F}_2^t$ we must have $wt(\phi(y, z)) \ge k+1$. By Theorem 4, f is k-resilient. The functions ϕ_1 and ϕ_2 satisfy the conditions of Theorems 10 and 11 respectively. Hence, they also satisfy the conditions of Theorem 9. Thus, ϕ satisfies the conditions of Theorem 8. Due to Theorem 2, the $(s+t, s+t)$-SSS defined by f is k-CI.

If C_1 and C_2 are linear codes with generator matrices $G_1 = [I_{t-r} \mid A]$ and G, respectively, then $\phi_1(y, z) = yA \oplus z$ and $\phi_2(y) = yG$. Thus, the defining function f can be written as $f(x, y, z) = x \cdot (\alpha \oplus (yA \oplus z)G) \oplus g(y, z)$.

Example 4 **(new schemes)**

a. Strictly 2-CI $(13, 13)$-SSS: Let C_1 be a $[6, 3, 3]$ binary self-dual code and C_2 be the $[7, 3, 4]$ binary Simplex code with $d_2^{\perp} = 3$ and covering radius $\rho = 3$. Consider a generator matrix $G_1 = [I_3 \mid A]$ of C_1 and a generator matrix G of C_2 where

$$A = \begin{bmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&1 \end{bmatrix} \text{ and } G = \begin{bmatrix} 1&0&0&0&1&1&1 \\ 0&1&0&1&0&1&1 \\ 0&0&1&1&1&0&1 \end{bmatrix}.$$

Choose $\alpha = (0, 0, 1, 0, 1, 1, 0)$, then $d(\alpha, C_2) = 3$.

b. Strictly 3-CI $(21, 21)$-SSS: Let C_1 be a $[9, 4, 4]$ binary linear code with $d_1^{\perp} = 3$ and C_2 be a $[12, 5, 4]$ binary linear code with $d_2^{\perp} = 4$ and covering radius $\rho = 4$. We use generator matrices $G_1 = [I_4 \mid A]$ and G where

$$A = \begin{bmatrix} 0&1&1&1&1 \\ 1&1&0&0&1 \\ 1&1&0&1&0 \\ 1&1&1&0&0 \end{bmatrix} \text{ and } G = \begin{bmatrix} 1&0&0&0&0&0&1&1&0&1&1&1 \\ 0&1&0&0&0&1&0&1&1&0&1&1 \\ 0&0&1&0&0&1&1&0&1&1&0&1 \\ 0&0&0&1&0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0 \end{bmatrix}.$$

Choose $\alpha = (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$, then $d(\alpha, C_2) = 4$.

c. Strictly 3-CI $(22, 22)$-SSS: Let C_1 be a $[10, 5, 4]$ binary self-dual code and C_2 be a $[12, 5, 4]$ binary linear code with $d_2^{\perp} = 4$ and covering radius $\rho = 4$. We use generator matrices $G_1 = [I_5 \mid A]$ and G where

$$A = \begin{bmatrix} 0&1&1&1&1 \\ 1&0&1&1&1 \\ 1&1&0&1&0 \\ 1&1&1&0&0 \\ 1&1&0&0&1 \end{bmatrix} \text{ and } G = \begin{bmatrix} 1&0&0&0&0&0&1&1&0&1&1&1 \\ 0&1&0&0&0&1&0&1&1&0&1&1 \\ 0&0&1&0&0&1&1&0&1&1&0&1 \\ 0&0&0&1&0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0 \end{bmatrix}.$$

Choose $\alpha = (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$, then $d(\alpha, C_2) = 4$.

d. Strictly 3-CI $(23, 23)$-SSS: Let C_1 be an $[11, 6, 4]$ binary linear code with $d_1^{\perp} = 3$ and generator matrix $G_1 = [I_6 \mid A]$ and C_2 be a $[12, 5, 4]$ binary linear code with $d_2^{\perp} = 4$, covering radius $\rho = 4$ and generator matrix G where

$$A = \begin{bmatrix} 0&0&1&1&1 \\ 0&1&0&1&1 \\ 0&1&1&0&1 \\ 1&0&1&1&0 \\ 1&1&0&1&0 \\ 1&1&1&0&0 \end{bmatrix} \text{ and } G = \begin{bmatrix} 1&0&0&0&0&0&1&1&0&1&1&1 \\ 0&1&0&0&0&1&0&1&1&0&1&1 \\ 0&0&1&0&0&1&1&0&1&1&0&1 \\ 0&0&0&1&0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0 \end{bmatrix}.$$

Choose $\alpha = (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$, then $d(\alpha, C_2) = 4$.

Example 5 **(using nonlinear codes)**

a. Strictly 2-CI $(2^{m+1}, 2^{m+1})$-SSS: For even integer $m \geq 4$, let $C_1 = \mathcal{K}(m)$ and $C_2 = \mathcal{P}(m)$. Choose $\alpha \in \mathbb{F}_2^m$ such that $d(\alpha, C_2) = 3$.
b. Strictly 5-CI $(2^{m+1}, 2^{m+1})$-SSS: For even integer $m \geq 6$, let $C_1 = \mathcal{P}(m)$ and $C_2 = \mathcal{K}(m)$. Choose $\alpha \in \mathbb{F}_2^m$ such that $d(\alpha, C_2) \geq 6$.

7 Concluding Remarks

We showed that cheating-immune secret sharing schemes can be obtained from the class of Maiorana-MacFarland Boolean functions. We presented one new cheating-immune scheme, $k = 3$ for $n = 17$ and four new strictly cheating-immune schemes, $k = 2$ for $n = 13$ and $k = 3$ for $n = 21, 22, 23$. We also gave constructions of (strictly) cheating-immune secret sharing schemes from some well-known classes of binary nonlinear codes. There are still open cases in the construction of (n, n) cheating-immune secret sharing schemes. Another open problem is the construction of cheating-immune schemes for other access structures.

Acknowledgments. The authors would like to thank the reviewers for their comments and suggestions. The first author would like to thank the University of the Philippines Diliman for the financial support. The second author's work is supported by CIMPA and IMU.

References

1. Blakley, G.: Safeguarding cryptographic keys. In: Proceedings of AFIPS 1979 National Computer Conference, New York, vol. 48, pp. 313–317 (1979)
2. Bellare, M., Rogaway, P.: Robust computational secret sharing and a unified account of classical secret-sharing goals. In: ACM Conference on Computer and Communications Security, pp. 172–184. ACM (2007)
3. Bierbrauer, J., Gopalakrishnan, K., Stinson, D.R.: Bounds for resilient functions and orthogonal arrays. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 247–256. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48658-5_24
4. Braeken, A., Nikov, V., Nikova, S.: On cheating immune secret sharing. In: Proceedings of 25th Symposium on Information Theory in the Benelux, pp. 113–120 (2004)
5. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
6. Cabello, S., Padró, C., Sáez, G.: Secret sharing schemes with detection of cheaters for general access structures. Des. Codes Cryptogr. **25**, 175–188 (2002)
7. Camion, P., Carlet, C., Charpin, P., Sendrier, N.: On Correlation-immune functions. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 86–100. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_6

8. Carlet, C.: Boolean functions for cryptography and error-correcting codes. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications), pp. 257–397. Cambridge University Press (2010)
9. Carlet, C.: On the propagation criterion of degree l and order k. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 462–474. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054146
10. Carlet, C.: Vectorial Boolean functions for cryptography. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications), pp. 398–470. Cambridge University Press (2010)
11. Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults. In: FOCS 1985, pp. 383–395 (1985)
12. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_22
13. D'Arco, P., Kishimoto, W., Stinson, D.: Properties and constraints of cheating-immune secret sharing schemes. Discret. Appl. Math. **154**, 219–233 (2006)
14. dela Cruz, R., Wang, H.: Cheating-immune secret sharing schemes from codes and cumulative arrays. Cryptogr. Commun. **5**, 67–83 (2013)
15. Delsarte, P.: Four fundamental parameters of a code and their combinatorial significance. Inf. Control **23**, 407–438 (1973)
16. Guo-Zhen, X., Massey, J.: A spectral characterization of correlation-immune combining functions. IEEE Trans. Inf. Theory **34**(3), 569–571 (1988)
17. Helleseth, T., Klove, T., Mykkeltveit, J.: On the covering radius of binary codes. IEEE Trans. Inf. Theory **24**(5), 627–628 (1978)
18. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
19. Kurosawa, K., Obana, S., Ogata, W.: t-Cheater identifiable (k, n) threshold secret sharing schemes. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 410–423. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-44750-4_33
20. MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
21. McEliece, R., Sarwate, D.: On sharing secrets and Reed-Solomon codes. Commun. ACM **24**, 583–584 (1981)
22. Ma, W.P., Lee, M.H.: New methods to construct cheating immune functions. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 79–86. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24691-6_7
23. Ma, W.P., Zhang, F.T.: New methods to construct cheating-immune multisecret sharing scheme. In: Feng, D., Lin, D., Yung, M. (eds.) CISC 2005. LNCS, vol. 3822, pp. 384–394. Springer, Heidelberg (2005). https://doi.org/10.1007/11599548_33
24. Martin, K.: Challenging the adversary model in secret sharing schemes. In: Coding and Cryptography II, Proceeidngs of the Royal Flemish Academy of Belgium for Science and the Arts, pp. 45–63 (2008)
25. Ogata, W., Kurosawa, K., Stinson, D.: Optimum secret sharing scheme secure against cheating. SIAM J. Discret. Math. **20**, 79–95 (2006)
26. Pieprzyk, J., Zhang, X.-M.: Cheating Prevention in Secret Sharing over $GF(p^t)$. In: Rangan, C.P., Ding, C. (eds.) INDOCRYPT 2001. LNCS, vol. 2247, pp. 79–90. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45311-3_8

27. Pieprzyk, J., Zhang, X.-M.: Constructions of cheating-immune secret sharing. In: Kim, K. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 226–243. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45861-1_18
28. Pieprzyk, J., Zhang, X.M.: On cheating immune secret sharing. Discret. Math. Theor. Comput. Sci. **6**, 253–264 (2004)
29. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of 21st ACM Symposium on Theory of Computing, pp. 73–85 (1989)
30. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
31. Stinson, D., Massey, J.: An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. J. Cryptol. **8**(3), 167–173 (1995)
32. Tassa, T.: Generalized oblivious transfer by secret sharing. Des. Codes Cryptogr. **58**(1), 11–21 (2011)
33. Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptol. **1**, 133–138 (1988)
34. Wei, Y., Hu, Y.: New Construction of resilient functions with satisfying multiple cryptographic criteria. In: Proceedings of the 3rd International Conference on Information Security InfoSecu 2004, pp. 175–180. ACM (2004)