New Methods to Construct Cheating Immune Multisecret Sharing Scheme*

Wen Ping Ma[1] and Fu Tai Zhang[2]

[1] Key Laboratory of Computer Network and Information Security, Ministry of Education, Xidian University, Xi'an 710071, P.R. China
wp_ma@mail.xidian.edu.cn
[2] The School of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097, P.R. China
zhangfutai@njnu.edu.cn

Abstract. In this paper, the constructions of cheating immune secret sharing and multisecret sharing are studied. Based on the theories of matrix and linear block codes over finite field, some new methods to construct cheating immune secret sharing, strictly cheating immune secret sharing and multisecret sharing immune against cheating are proposed. Some cryptographic properties of the constructed secret sharing are analyzed as well.

Keywords: Quadratic Function, Secret Sharing, Cheating Immune Function, Multisecret Secret Sharing.

1 Introduction

Secret sharing is an indispensable tool in key management, multiparty computation, group cryptography and distributed cryptography. Unfortunately, many existing secret sharing systems are easily subjected to cheat by dishonest participants in the process of reconstruction. In such secret sharing systems the dishonest participants may submit fake shares to the combiner so that the combiner cannot reconstruct the original shared secret, but the dishonest participants may find the original shared secret in some way. Tompa and Woll [1]discussed the problem of cheating prevention in secret sharing in 1988. Since then, a considerable effort has been put into the investigation of cheating prevention in secret sharing systems. A notable work in this line of study is the research on cheating immune secret sharing systems initiated by Josef Pipprzyk and Xian Mo Zhang [4]. They studied the problem of cheating prevention and the construction of cheating immune secret sharing schemes in [4, 5, 6, 7].

Cheating immune secret sharing schemes are divided into two classes, i.e., the computational secure schemes and unconditional secure ones. In computational secure cheating immune secret sharing schemes, the combiner checks the

* This work was supported by the National Science Foundation of China under the grant No.60373104 and Key Project of Jiangsu education bureau, China, under grant number 03KJA520066.

D. Feng, D. Lin, and M. Yung (Eds.): CISC 2005, LNCS 3822, pp. 384–394, 2005.

validity of the shares submitted by the participants before he reconstructs the shared secret, so any false shares may probably be found out in this stage and the cheaters are likely to be detected. One solution for computational secure cheating immune secret sharing is publicly verifiable secret sharing. M.Stadler et. al considered this problem in [8, 9, 10]. Josef Pieprzyk and Xian-Mo Zhang [4] pointed out that cheating by dishonest participants can also be prevented without using the method of public key cryptography. The prevention here is meant that the dishonest participants cannot derive the original shared secret correctly from the invalid secret computed by the combiner, furthermore, the invalid secret reveals no information about the original shared secret.

Multisecret sharing was probably first discussed in [2]. The problem of cheating prevention in this type of secret sharing schemes was also first considered by Josef Pieprzyk and Xian Mo Zhang [5]. They gave the fundamental concepts of multisecret sharing immune against cheating and some ideas to construct multisecret sharing immune against cheating.

In this paper, we further study the problem of cheating prevention in secret sharing systems. Based on quadratic function over finite field, the cheating immune secret sharing, strictly cheating immune secret sharing and multisecret sharing immune against cheating are constructed. Some cryptographic properties of these secret sharing schemes are also analyzed.

2 Secret Sharing System Immune Against Cheating

2.1 Basic Model of Cheating Immune Secret Sharing Scheme [4]

Let $GF(p)$ denote a finite field with p elements, where p is a prime number or a power of a prime number. We use $GF(p)^n$ to denote the vector space of dimension n over $GF(p)$.

For vectors $x = (x_1, x_2, \cdots, x_n), \delta = (\delta_1, \delta_2, \cdots, \delta_n)$ in $GF(p)^n$, define vectors $x_\delta^+ \in GF(p)^n$, $x_\delta^- \in GF(p)^n$ as follows :

$$(x_\delta^+)_j = \begin{cases} x_j, \text{ if } \delta_j \neq 0 \\ 0, \text{ if } \delta_j = 0 \end{cases}$$

$$(x_\delta^-)_j = \begin{cases} 0, \text{ if } \delta_j \neq 0 \\ x_j, \text{ if } \delta_j = 0 \end{cases}$$

where $j = 1, 2, \cdots, n$.

Let $\tau = (\tau_1, \tau_2, \cdots, \tau_n)$, $\delta = (\delta_1, \delta_2, \cdots, \delta_n)$ be two vectors in $GF(p)^n$. By the notation $\tau \leq \delta$ we mean that $\tau_i \neq 0$ implies $\delta_i \neq 0$, for all $i \in \{1, 2, ..., n\}$. We use $\tau < \delta$ to denote $\tau \leq \delta$ and the Hamming weight $HW(\tau)$ of τ (the number of nonzero coordinates of τ) is less than the Hamming weight $HW(\delta)$ of δ. If $\delta^/ \leq \delta$, and $HW(\delta^/) = HW(\delta)$, we write $\delta^/ \approx \delta$. For $\tau, \delta \in GF(p)^n, \delta \neq 0, \tau \leq \delta$, $u \in GF(p)$, and a mapping f from $GF(p)^n$ to $GF(p)$, define

$$R_f(\delta, \tau, u) = \{x_\delta^- | f(x_\delta^- + \tau) = u\}.$$

We also simply write $R(\delta, \tau, u)$ in place of $R_f(\delta, \tau, u)$ if no confusion occurs.

Now, we consider a secret sharing system. Suppose the secret to be shared is randomly chosen from $GF(p)$, namely the secret space is $GF(p)$. There are n participants(or share-holders) $P_1, P_2, \cdots, P_n$, a dealer D and a combiner in the system. Denote $P = \{P_1, P_2, \cdots, P_n\}$. Two phases are involved in a secret sharing scheme. One is share distribution, and the other is reconstruction. In the share distribution phase, the dealer D randomly splits a secret K into n shares in $GF(p)$, and distributes in secret each participant one share.In reconstruction phase, all participants submit their shares to the combiner who computes the shared secret using a function f from $GF(p)^n$ to $GF(p)$. The function f is called the defining function as it determines the secret sharing.

Let $\alpha = (s_1, s_2, \cdots, s_n) \in GF(p)^n$ be the share vector, i.e., s_j is the share distributed to participant P_j by the dealer, $K = f(\alpha)$ be the shared secret.

Let $\alpha + \delta$ be the vector whose coordinates are *shares* submitted to the combiner by the participants. We call $\delta = (\delta_1, \delta_2, \cdots, \delta_n) \in GF(p)^n$ a cheating vector, and P_i is a cheater if and only if $\delta_i \neq 0$. The collection of cheaters is determined by the vector $\delta = (\delta_1, \delta_2, \cdots, \delta_n)$ uniquely.

It is assumed that in pooling phase, dishonest participants always submit invalid shares, and honest participants always submit their valid shares. We also suppose the dishonest participants change their *shares* from time to time, and there is at least one cheater in the system, this implies $\delta \neq 0$.

Consider the vector $\alpha + \delta$. It is obvious that $\alpha + \delta = \alpha_\delta^- + \alpha_\delta^+ + \delta$, here α_δ^- is submitted by the honest participants (or we can say the nonzero coordinates of α_δ^- are shares submitted to the combiner by the honest participants), and $\alpha_\delta^+ + \delta$ by the dishonest ones (the nonzero coordinates of α_δ^+ are shares held by the dishonest participants). In this case, the combiner will output an invalid secret $K^* = f(\alpha + \delta)$.

For the defining function f, share vector α and cheating vector $\delta = (\delta_1, \delta_2, \cdots, \delta_n)$, the number

$$\rho_{\delta,\alpha} = \frac{\sharp(R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K))}{\sharp R(\delta, \alpha_\delta^+ + \delta, K^*)}$$

is the probability of successful cheating by dishonest participants with respect to δ, α, where $\sharp X$ denotes the number of elements in the set X.

It is obvious that $\rho_{\delta,\alpha} > 0$ since the share vector α is always in the set $(R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K))$ and the number of cheaters is equal to $HW(\delta)$. It was proved in [4] that $max\{\rho_{\delta,\alpha} | \alpha \in GF(p)^n\} \geq p^{-1}$ for arbitrary $\alpha \in (GF(p))^n$ and nonzero $\delta \in GF(p)^n$.

Definition 1. A secret sharing is said to be k-cheating immune if $\rho_{\delta,\alpha} = p^{-1}$ for every $\delta \in GF(p)^n$ with $1 \leq HW(\delta) \leq k < n$ and every $\alpha \in GF(p)^n$.

Let f be a quadratic function, if $f(x_\delta^- + \tau + \delta) - f(x_\delta^- + \tau)$ is a non-constant affine function for arbitrary $\delta, \tau \in GF(p)^n$ with $1 \leq HW(\delta) \leq k$ and $\tau \leq \delta$, we call f has property $B(k)$.

Let f be the defining function, $\delta = (\delta_1, \delta_2, \cdots, \delta_n)$ be a nonzero vector, α be an original vector, the nonzero vector τ, $\tau \leq \delta$ be an active cheating vector, the number

$$\rho_{\delta,\tau,\alpha} = \frac{\sharp(R(\delta, \alpha_\delta^+ + \tau, K^*) \cap R(\delta, \alpha_\delta^+, K))}{\sharp R(\delta, \alpha_\delta^+ + \tau, K^*)}$$

expresses the probability of cheaters' success with respect to δ, τ and α.

Definition 2. A secret sharing is said to be strictly k-cheating immune if $\rho_{\delta,\tau,\alpha} = p^{-1}$ for every $\delta \in GF(p)^n$ with $1 \leq HW(\delta) \leq k < n$, every $\alpha \in GF(p)^n$ and any nonzero vector τ, $\tau \leq \delta$.

Next, we will study how to use quadratic functions over finite field to construct cheating immune secret sharing.

A function f from $GF(p)^n$ to $GF(p)$ is said balanced if

$\sharp\{\alpha : \alpha \in GF(p)^n, f(\alpha) = b, \forall b \in GF(p)\} = p^{(n-1)}$

For quadratic functions, the following theorem can be easily proved.

Theorem 1. *Let* $Q(x_1, x_2, \cdots, x_n) = \sum_{i,j=1, i\leq j}^{n} a_{ij}x_ix_j + \sum_{i=1}^{n} a_ix_i$ *be a quadratic function over finite field* $GF(q)$ *with characteristic not equal to* 2*, then the function* $Q(x_1, x_2, \cdots, x_n)$ *is balanced if and only if there exists* $\omega \in GF(q)^n$ *such that* $Q(x + \omega) - Q(x)$ *equals to a constant, and* $Q(\omega) \neq 0$.

2.2 A New Construction of Cheating Immune Secret Sharing

Let $\alpha = (a_1, a_2, \cdots, a_m)$ be a nonzero vector over $GF(p)$ with characteristic not equal to 2, and $\Sigma_{i=1}^{m} a_i = 0$, $b_0, b_1, \cdots, b_{n-1} \in GF(p)$, and $\Sigma_{i=0}^{n-1} b_i \neq 0$. Define a function $\lambda_{n,m}$ on $GF(p)^n$ as:

$$\begin{aligned}
&\lambda_{n,m}(x_0, x_1, \cdots, x_{n-1}) \\
&= \Sigma_{i=0}^{n-1} b_i x_i + (x_0, x_1, \cdots, x_{n-1}) A(\alpha, n) (x_0, x_1, \cdots, x_{n-1})^T \\
&= \Sigma_{i=0}^{n-1} b_i x_i + \Sigma_{j=0}^{n-1} x_j (a_1 x_{[j+1]_{(n)}} + a_2 x_{[j+2]_{(n)}} + \cdots + a_m x_{[j+m]_{(n)}})
\end{aligned}$$

where $j = i_{(n)}$ iff $j = i \bmod n$.

$A(\alpha, n)$ is an $n \times n$ matrix over $GF(p)$ determined by the vector $\alpha = (a_1, a_2, \cdots, a_m)$ as follows:

$$A(\alpha, n) = \begin{pmatrix}
0 & a_1 & a_2 & \cdots & a_m & 0 & \cdots & 0 \\
0 & 0 & a_1 & \cdots & a_{m-1} & a_m & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
a_m & 0 & 0 & \cdots & 0 & 0 & \cdots & a_{m-1} \\
a_{m-1} & a_m & 0 & \cdots & 0 & 0 & \cdots & a_{m-2} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a_2 & a_3 & a_4 & \cdots & \cdots & \cdots & \cdots & a_1 \\
a_1 & a_2 & a_3 & \cdots & 0 & 0 & \cdots & 0
\end{pmatrix}$$

Theorem 2. *1.* $\lambda_{n,m}(x_0, x_1, \cdots, x_{n-1})$*is balanced.*

2. If $n \geq km + k + 1$*, then the function* $\lambda_{n,m}(x_0, x_1, \cdots, x_{n-1})$ *satisfies the property* $B(k)$.

Proof. 1. Because $\lambda_{n,m}(1,1,\cdots,1) = \Sigma_{i=0}^{n-1} b_i \neq 0$, we have $\lambda_{n,m}(x_0+1, x_1+1,\cdots,x_{n-1}+1) - \lambda_{n,m}(x_0,x_1,\cdots,x_{n-1}) = \Sigma_{i=0}^{n-1} b_i = \text{constant}$. From theorem 1, $\lambda_{n,m}(x_0,x_1,\cdots,x_{n-1})$ is balanced.

2. Let $\delta \in GF(p)^n$, with $HW(\delta) \leq k$, and $\tau \leq \delta$. Suppose $HW(\delta) = k$, write $\delta = (0,\cdots,\delta_{i_1},\cdots,\delta_{i_2},\cdots,\delta_{i_k},\cdots,0)$ where $0 \leq i_1, i_2,\cdots,i_k \leq n-1$, $\delta_{i_1} \neq 0, \delta_{i_2} \neq 0,\cdots,\delta_{i_k} \neq 0$. If $n \geq km+k+1$, then there exists at least one element $k \in \{0,1,2,\cdots,n-1\}$ such that k belongs to just one of the classes

$\{\{(i_j-1) \bmod \text{n}, (i_j-2) \bmod \text{n}, \cdots,$

$(i_j-m) \bmod \text{n}, (i_j+1) \bmod \text{n}, (i_j+2) \bmod \text{n}, \cdots, (i_j+m) \bmod \text{n}\}, 1 \leq j \leq k\}$,

thus $f(x_\delta^- + \delta + \tau) - f(x_\delta^- + \tau)$ contains the term ax_k, $a \in GF(p)$, $a \neq 0$. This implies that the function $\lambda_{n,m}(x_0,x_1,\cdots,x_{(n-1)})$ satisfies the property $B(k)$.

Theorem 3 ([4]). *Let k, s be two positive integers satisfying $s \geq (k+1)$, h_i be a balanced quadratic function with property $B(k)$ on $GF(p)^{n_i}$ for each $i = 1,2,\cdots,s$. Set $n = n_1 + n_2 + \cdots + n_s$. Defining the function f on $GF(p)^n$ as $f(x) = h_1(y_1) + h_2(y_2) + \cdots + h_s(y_s)$, where $x = (y_1, y_2, \cdots, y_s)$, h_i and h_j have disjoint variables if $i \neq j$. Then the secret sharing with defining function f is k-cheating immune.*

3 The Construction of Multisecret Sharing Immune Against Cheating

3.1 Basic Model of Multisecret Sharing Immune Against Cheating [2, 5]

The multisecret sharing system is defined by a mapping $F : GF(p)^n \to GF(p)^m$. The function F is equivalent to the following function group :

$$\begin{cases} f_1 : GF(p)^n \to GF(p) \\ f_2 : GF(p)^n \to GF(p) \\ \cdots \\ f_m : GF(p)^n \to GF(p) \end{cases}$$

We denote this function group by $[f_1, f_2, \cdots, f_m]$, and call it the defining function of the multisecret sharing.

Let δ be a nonzero vector in $GF(p)^n$, $\tau \leq \delta$, and $\mu \in GF(p)^m$, set

$$R_f(\delta,\tau,\mu) = \{x_\delta^- : f(x_\delta^- + \tau) = \mu\}.$$

We simply denote $R_f(\delta,\tau,\mu)$ as $R(\delta,\tau,\mu)$ if no confusion occurs.

Let $u^* = f(\alpha+\delta)$, the number

$$\rho_{\delta,\alpha} = \frac{\sharp(R(\delta,\alpha_\delta^+ + \delta, u^*) \cap R(\delta,\alpha_\delta^+, u))}{\sharp R(\delta,\alpha_\delta^+ + \delta, u^*)}$$

expresses the probability of successful cheating with respect to δ and α.

A multisecret sharing is said to be k-cheating immune if $\rho_{\delta,\alpha} = p^{-m}$ hold for every $\delta \in GF(p)^n$, with $1 \le HW(\delta) \le k$, and every $\alpha \in GF(p)^n$.

We call the nonzero vector $\delta = (\delta_1, \delta_2, \cdots, \delta_n)$ a cheating vector, nonzero vector $\tau \le \delta$ an active cheating vector, α the original vector, then the value

$$\rho_{\delta,\tau,\alpha} = \frac{\sharp(R(\delta, \alpha_\delta^+ + \tau, u^*) \cap R(\delta, \alpha_\delta^+, u))}{\sharp R(\delta, \alpha_\delta^+ + \tau, u^*)}$$

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

A multisecret sharing is said to be strictly k-cheating immune if the the probability of successful cheating satisfies $\rho_{\delta,\tau,\alpha} = p^{-m}$ for every nonzero $\delta \in GF(p)^n$ with $1 \le HW(\delta) \le k < n$, any $\alpha \in GF(p)^n$, and any nonzero vector $\tau \le \delta$.

Definition 3. Let $[f_1, f_2, \cdots, f_m]$ be the defining function of a multisecret sharing, k a positive integer, and $k < n$. $[f_1, f_2, \cdots, f_m]$ is said satisfying the property $B(k)$ if there exists $a_1, a_2, \cdots, a_m \in GF(p)$ such that $\Sigma_{i=1}^m a_i[f_i(x_\delta^- + \tau + \delta) - f_i(x_\delta^- + \tau)]$ is a non-constant affine function, where $(a_1, a_2, \cdots, a_m) \ne (0, 0, \cdots, 0)$, $1 \le HW(\delta) \le k, \tau \le \delta$.

Thus $[f_1, f_2, \cdots, f_m]$ satisfies the property $B(k)$ iff any nonzero linear combination of $f_1, f_2, \cdots, f_m$, i.e., $\Sigma_{i=1}^m a_i f_i$ satisfies the property $B(k)$, where a_1, a_2, $\cdots, a_m \in GF(p)$, and $(a_1, a_2, \cdots, a_m) \ne (0, 0, \cdots, 0)$.

3.2 The New Construction of Multisecret Sharing Immune Against Cheating

Let $GF(p)$ be a finite field whose characteristic is not equal to 2. Set

$$\Delta = \{(x_1, x_2, \cdots, x_m) : x_i \in GF(p), i = 1, 2, \cdots, m, \Sigma_{i=1}^m x_i = 0\},$$

then Δ is a linear subspace of dimension $m-1$ of vector space $GF(p)^m$.

A set of base of linear subspace Δ is:

$\alpha_1 = (a_{11}, a_{12}, \cdots, a_{1m})$,
$\alpha_2 = (a_{21}, a_{22}, \cdots, a_{2m})$,
$\cdots$
$\alpha_{m-1} = (a_{(m-1)1}, a_{(m-1)2}, \cdots, a_{(m-1)m})$.

For each $i \in \{1, 2, \cdots, m-1\}$, we construct an $n \times n$ matrix

$$A(\alpha_i, n) = \begin{pmatrix} 0 & a_{i1} & a_{i2} & \cdots & a_{im} & 0 & \cdots & 0 \\ 0 & 0 & a_{i1} & \cdots & a_{i(m-1)} & a_{im} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & a_{im} \\ a_{im} & 0 & 0 & \cdots & 0 & 0 & \cdots & a_{i(m-1)} \\ a_{i(m-1)} & a_{im} & 0 & \cdots & 0 & 0 & \cdots & a_{i(m-2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i2} & a_{i3} & a_{i4} & \cdots & \cdots & \cdots & \cdots & a_{i1} \\ a_{i1} & a_{i2} & a_{i3} & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Let $\lambda(\alpha_i, n) = (x_1, x_2, \cdots, x_n)A(\alpha_i, n)(x_1, x_2, \cdots, x_n)^T$,

$f_{11}(x_1, x_2, \cdots, x_n) = x_1 + \lambda(\alpha_1, n)$,
$f_{21}(x_1, x_2, \cdots, x_n) = x_2 + \lambda(\alpha_2, n)$,$f_{22}(x_1, x_2, \cdots, x_n) = 2x_2 + \lambda(\alpha_2, n)$
$\cdots$
$f_{(m-1)1}(x_1, x_2, \cdots .x_n) = x_{m-1} + \lambda(\alpha_{m-1}, n)$,
$f_{(m-1)2}(x_1, x_2, \cdots, x_n) = 2x_{m-1} + \lambda(\alpha_{m-1}, n)$.

From theorem 1, each function constructed above is balanced.
Let $(x_1, x_2, \cdots, x_{nm}) \in GF(p)^{nm}$, we can write

$(x_1, x_2, \cdots, x_{mn}) = (y_1, y_2, \cdots, y_m)$, $y_i \in GF(p)^n, i = 1, 2, \cdots, n$.

Now we construct the following functions:

$f_1(x_1, x_2, \cdots, x_{mn}) = f_{11}(y_1) + f_{11}(y_2) + \cdots + f_{11}(y_m)$,
$f_2(x_1, x_2, \cdots, x_{mn}) = f_{21}(y_1) + f_{22}(y_2) + f_{21}(y_3) + \cdots + f_{21}(y_m)$,
$\cdots$
$f_{m-1}(x_1, x_2, \cdots, x_{mn}) = f_{(m-1)1}(y_1) + f_{(m-1)1}(y_2) + \cdots + f_{(m-1)2}(y_{m-1}) + f_{(m-1)1}(y_m)$.

Namely, the $i'th$ term of $f_i(x_1, x_2, \cdots, x_{mn})$ is f_{i2}, and the other terms of $f_i(x_1, x_2, \cdots, x_{nm})$ are f_{i1}, $i = 2, \cdots, (m-1)$.

Theorem 4. *If $n \geq km + k + 1$, then the function group:*

$$\begin{cases} f_1(x_1, x_2, \cdots, x_{nm}) \\ f_2(x_1, x_2, \cdots, x_{nm}) \\ \cdots \\ f_{m-1}(x_1, x_2, \cdots, x_{nm}) \end{cases}$$

is a balanced function from $GF(p)^{nm}$ to $GF(p)^{m-1}$, and satisfies the property $B(k)$.

Proof. We use the fact that a function group $[g_1, g_2, \cdots, g_{m-1}]$ is balanced iff for any nonzero linear combination of $g_1, g_2, \cdots, g_{m-1}$, i.e,$\Sigma_{i=1}^{m-1} a_i g_i$ is balanced, where $a_1, a_2, \cdots, a_{m-1} \in GF(p)$, and $(a_1, a_2, \cdots, a_{m-1}) \neq (0, 0, \cdots, 0)$. Now, for the function group $[f_1, f_2, \cdots, f_{(m-1)}]$, we have

$a_1 f_1 + a_2 f_2 + \cdots + a_{m-1} f_{m-1}$
$=[(a_1 x_1 + a_2 x_2 + \cdots + a_{m-1} x_{m-1}) + y_1 \Sigma_{i=1}^{m-1} a_i \lambda(\alpha_i, n) y_1^T]$
$+[(a_1 x_{n+1} + 2a_2 x_{n+2} + \cdots + a_{m-1} x_{n+m-1}) + y_2 \Sigma_{i=1}^{m-1} a_i \lambda(\alpha_i, n) y_2^T] + \cdots +$
$[(a_1 x_{(m-2)n+1} + a_2 x_{(m-2)n+2} + \cdots + 2a_{m-1} x_{(m-2)n+m-1}) +$
$y_{m-1} \Sigma_{i=1}^{m-1} a_i \lambda(\alpha_i, n) y_{m-1}^T]$
$+[(a_1 x_{(m-1)n+1} + a_2 x_{(m-1)n+2} + \cdots + a_{m-1} x_{(m-1)n+m-1}) +$
$y_m \Sigma_{i=1}^{m-1} a_i \lambda(\alpha_i, n) y_m^T]$.
$\Sigma_{i=1}^{m-1} a_i \lambda(\alpha_i, n) = \lambda(\Sigma_{i=1}^{m-1}(a_i \alpha_i), n)$

Since $a_1, a_2, \cdots, a_{m-1} \in GF(p)$ are not all zero, thus there exists at least a nonzero element in $a_1 + a_2 + \cdots + a_{m-1}, a_1 + 2a_2 + \cdots + a_{m-1}, \cdots, a_1 + a_2 + \cdots +$

$2a_{m-1}$, hence we know from theorem 1, the function $a_1f_1+a_2f_2+\cdots+a_{m-1}f_{m-1}$ is balanced. This proves the function group $[f_1, f_2, \cdots, f_{m-1}]$ is balanced.

For each $i \in \{1, 2, \cdots, m-1\}$, the function $\lambda(\alpha_i, n)$ satisfies the property $B(k)$, so we know from the theorem 2, $\lambda(\Sigma_{i=1}^{m-1} a_i\alpha_i, n)$ satisfies the property $B(k)$ when $n \geq mk + k + 1$ and $a_1, a_2, \cdots, a_{m-1} \in GF(p)$, with $(a_1, a_2, \cdots, a_{m-1}) \neq (0, 0, \cdots, 0)$. This implies the function group $\lambda(\alpha_i, n), i = 1, 2, \cdots, m-1$ satisfies the property $B(k)$, namely $[f_1, f_2, \cdots, f_{m-1}]$ satisfies the property $B(k)$.

The following theorem can be proved using the similar way as in [4].

Theorem 5. *Let k, s be two positive integers satisfying $s \geq q(k+1)$, h_i be a balanced function with property $B(k)$ from $GF(p)^{n_i}$ to $GF(p)^m$ for each $i = 1, 2, \cdots, s$. Set $n = n_1 + n_2 + \cdots + n_s$. Defining the function f from $GF(p)^n$ to $GF(p)^m$ as $f(x) = h_1(y_1) + h_2(y_2) + \cdots + h_s(y_s)$, where $x = (y_1, y_2, \cdots, y_s)$, h_i and h_j have disjoint variables if $i \neq j$, then the multisecret sharing with defining function f is k-cheating immune.*

4 On the Construction of Strictly Cheating Immune Multisecret Sharing

Theorem 6. *Given a multisecret sharing defining function $f : GF(p)^n \longrightarrow GF(p)^m$, the following statements are equivalent:*

(1) the multisecret sharing is strictly $k-$cheating immune,

(2) *For any integer l with $1 \leq l \leq k$, any $\delta \in GF(p)^n$ with $HW(\delta) = l$, any $\tau_1 \leq \delta, \tau_2 \leq \delta, 0 \leq HW(\tau_2)$, and any $\mu, \nu \in GF(p)^m$, we have*

$$\sharp(R(\delta, \tau_1, \nu) \cap R(\delta, \tau_1 + \tau_2, \mu)) = p^{n-l-2m},$$

(3) *The system of equations:*

$$\begin{cases} f(x_\delta^- + \tau_1 + \tau_2) = \mu \\ f(x_\delta^- + \tau_1) = \upsilon \end{cases}$$

has precisely $p^{(n-l-2m)}$ solutions on x_δ^-, for any $\tau_1 \leq \delta, \tau_2 \leq \delta, 0 < HW(\tau_2)$, and any $\mu, \nu \in GF(p)^m$.

The proof is similar to the proof of theorem 3 in [5].

If $m = 1$, the multisecret sharing with its defining mapping $f : GF(p)^n \longrightarrow GF(p)^m$is a secret sharing. Thus the theorem is also right for ordinary secret sharing.

Definition 4. The function f of degree two is said to have the strict property $B(k)$ if for any $\delta \in GF(p)^n, 1 \leq HW(\delta) \leq k$, any $\tau_1 \leq \delta$, any $\tau_2 \leq \delta$ and $0 < HW(\tau_2)$, $f(x_\delta^+ + \tau_1 + \tau_2) - f(x_\delta^+ + \tau_1)$ is a non-constant affine function.

Similar to theorem 4, the function f of degree two which satisfies the strictly property $B(k)$ can be used to construct the strictly cheating immune secret sharing.

In the following, a method to construct strictly cheating immune multisecret sharing will be given.

Theorem 7. *[5] Given a multisecret sharing with its defined mapping* $f : GF(p)^n \to GF(p)^m$*, then the multisecret sharing is strictly* $k-$*cheating immune iff for any integer* r *with* $0 \le r \le k-1$*, any subset* $\{j_1, j_2, \cdots, j_r\}$ *of* $\{1, 2, \cdots, n\}$ *and any* $a_1, a_2, \cdots, a_r \in GF(p)$*, the mapping*

$$f(x_1, x_2, \cdots, x_n)|_{x_{j_1}=a_{j_1}, x_{j_2}=a_{j_2}, \cdots, z_{j_r}=a_{j_r}}$$

is the defining mapping of a $(k-r)$ *cheating immune secret sharing.*

Let $GF(p)$ be a finite field whose characteristic is not equal to 2. Suppose $C^{/}$ is a $(n^{/}, k^{/}, d)$linear cyclic codes over $GF(p)$ such that for every codeword $\alpha = (a_1, a_2, \cdots, a_m) \in C^{/}$, such that $\Sigma_{i=1}^{m} a_i = 0$, and $k^{/} \ge d, n^{/} - k^{/} \ge d$. Let C be $(n^{/} - d, k^{/} - d, \ge d)$ shortened cyclic codes, rewrite the parameter $(n^{/} - d, k^{/} - d, \ge d)$ as $(m, k, \ge d)$.

Let $\alpha = (a_1, a_2, \cdots, a_m) \in C$ be a nonzero code of the code C, b_0, b_1, $b_2, \cdots, b_{n-1} \in GF(p)$, such that $\Sigma_{i=0}^{n-1} b_i \ne 0$, $\lambda_{n,m}$ be a function on $GF(p)^n$ defined by :

$\lambda_{n,m}(x_0, x_1, \cdots, x_{n-1}) =$
$\Sigma_{i=0}^{n-1} b_i x_i + (x_0, x_1, \cdots, x_{n-1}) A(\alpha, n)(x_0, x_1, \cdots, x_{n-1})^T$

Theorem 8. *1.* $\lambda_{n,m}(x_0, x_1, \cdots, x_{n-1})$ *is balanced.*
2. If $n \ge 2m^2 + m + 1$*, the function satisfies strict property* $B(d)$*.*

Proof. 1), From the theorem 1, it is easy to prove that $\lambda_{n,m}(x_0, x_1, \cdots, x_{n-1})$ is balanced.

2),Let $h(x_{i_1}, x_{i_2}, \cdots, x_{i_{n-r}}) = \lambda_{n,m}(x_0, x_1, \cdots, x_{n-1})|_{x_{j_1}=a_1, \cdots, x_{j_r}=a_r}, 0 \le r < d$, $x_{i_1} = y_1, x_{i_2} = y_2, \cdots, x_{i_{n-r}} = y_{n-r}$.

Consider the function $h(y_1, y_2, \cdots, y_{n-r})$. Recall that for each j, $1 \le j \le n-r$, x_j appears precisely in $2m$ quadratic terms of

$$\lambda_{n,m}(x_0, x_2, \cdots, x_{n-1}) : x_j x_{[j+i]_{(n)}}, x_j x_{[j-i]_{(n)}}, i = 1, 2, \cdots, m.$$

Let $\delta \in GF(p)^{n-r}$ be an cheating vector with $HW(\delta) = l, 1 \le l \le m, \tau \le \delta$ be an active cheating vector. Write $\delta = (\delta_1, \delta_2, \cdots, \delta_{n-r})$,

$J = \{j | \delta_j \ne 0, 1 \le j \le n-r\}$, $\sharp J = HW(\delta) = l \le d - r$, if i, j do not belong to J, the term $y_i y_j$ does not appear in $h(y_\delta^- + \delta + \tau) - h(y_\delta^- + \tau)$.
Since $n - r > n - m > 2m^2 + 1$, $\lceil \frac{n-r}{m-r} \rceil \ge 2m + 1$, there exist $j_0 \in J$ and l_1 such that $l_1 \ge 2m + 1$, we have

$$[j_0 + l_1]_{(n-r)} \in J, \{[j_0 + 1]_{(n-r)}, [j_0 + 2]_{(n-r)}, \cdots, [j_0 + l_1 - 1]_{(n-r)}\} \cap J = \varnothing.$$

Let $[j_{l-1}]_{(n-r)}, [j_{l-2}]_{(n-r)}, \cdots, j_0$ be all elements of J, and $[j_0 + l_1 - 1]_{(n-r)} = [j_{(l-1)}]_{(n-r)}$.

Because every codeword in $C^{/}$ has minimum weight not smaller than d, there exists some element $[i_0]_{(n-r)} \in \{[j_0+1]_{(n-r)}, [j_0+2]_{(n-r)}, \cdots, [j_0+m]_{(n-r)}\}$ such that $a x_{[i_0]_{(n-r)}}$ $(a \ne 0)$ appears in $\Sigma_{s=0}^{l-1} \delta_s (a_1 x_{(j_s+1)} + a_2 x_{(j_s+2)} + \cdots + a_m x_{(j_s+m)})$,

thus $ax_{[i_0]_{(n-r)}}, (a \neq 0)$ appears in $h(y_\delta^+ + \tau + \delta) - h(y_\delta^+ + \tau)$. This proves that h has the property $B(d-r)$.

Suppose a set of base of the codes C is

$\alpha_1 = (a_{11}, a_{12}, \cdots, a_{1m})$,

$\alpha_2 = (a_{21}, a_{22}, \cdots, a_{2m})$,

$\cdots$

$\alpha_k = (a_{k1}, a_{k2}, \cdots, a_{km})$.

To construct matrix $A(\alpha_i, n), i = 1, 2, \cdots, k$.

let $\lambda(\alpha_i, n) = (x_1, x_2, \cdots, x_n)A(\alpha_i, n)(x_1, x_2, \cdots, x_n)^T$,

$f_{11}(x_1, x_2, \cdots, x_n) = x_1 + \lambda(\alpha_1, n)$,

$f_{21}(x_1, x_2, \cdots, x_n) = x_2 + \lambda(\alpha_2, n)$, $f_{22}(x_1, x_2, \cdots, x_n) = 2x_2 + \lambda(\alpha_2, n)$,

$\cdots$

$f_{k1}(x_1, x_2, \cdots .x_n) = x_k + \lambda(\alpha_k, n)$, $f_{k2}(x_1, x_2, \cdots, x_n) = 2x_k + \lambda(\alpha_k, n)$.

From theorem 1, each function constructed above is balanced.

Let $(x_1, x_2, \cdots, x_{nk}) \in GF(p)^{nk}$. Write $(x_1, x_2, \cdots, x_{kn}) = (y_1, y_2, \cdots, y_k)$, $y_i \in GF(p)^n, i = 1, 2, \cdots, n$.

Now, we construct the following functions:

$f_1(x_1, x_2, \cdots, x_{kn}) = f_{11}(y_1) + f_{11}(y_2) + \cdots + f_{11}(y_k)$,

$f_2(x_1, x_2, \cdots, x_{kn}) = f_{21}(y_1) + f_{22}(y_2) + f_{21}(y_3) + \cdots + f_{21}(y_k)$,

$\cdots$

$f_k(x_1, x_2, \cdots, x_{kn}) = f_{k1}(y_1) + f_{k1}(y_2) + \cdots + f_{k2}(y_k)$.

The $i'th$ term of $f_i(x_1, x_2, \cdots, x_{kn})$ is f_{i2}, and the other terms of $f_i(x_1, x_2, \cdots, x_{nk})$ are f_{i1}, $i = 2, \cdots, k$.

Theorem 9. *If $n \geq 2m^2 + m + 1$, then the function group:*

$$\begin{cases} f_1(x_1, x_2, \cdots, x_{nk}) \\ f_2(x_1, x_2, \cdots, x_{nk}) \\ \cdots \\ f_k(x_1, x_2, \cdots, x_{nk}) \end{cases}$$

is a balanced function form $GF(p)^{kn}$ to $GF(p)^k$, and satisfies the strict property $B(d)$.

The proof is similar to that of the theorem (4) and (8).

Similar to theorem 5, the construction of strictly cheating immune multisecret sharing can be given easily by the construction above.

5 Conclusions

In this paper, we have presented some methods to construct the cheating immune secret sharing functions, strictly cheating immune secret sharing and multisecret sharing immune against cheating, some cryptographic properties of related schemes are analyzed as well.

Acknowledgements

We would like to thank the anonymous referees for their helpful comments and suggestions.

References

1. M.Tompa and H.Woll. How to Share a Secret with cheaters. Journal of Cryptology, Vol.1, No.2, pp.133-138, 1988.
2. Wen-Ai Jackson, Keith M.Martin and Christine M.OKeefe. Multisecret Threshold Schemes. Advance in Cryptology-Crypto' 93, Lecture Notes in Computer Science, 773, pp. 126-135, Springer-verlag, 1994.
3. Kaisa Nyberg and Lars Ramkilde Knudsen. Provable Security against Differential Cryptanalysis. Advance in CryptologyCrypto' 92, Lecture Notes in Computer Science, 740, pp. 566-574, Springer-verlag, 1992.
4. Josef Pieprzyk and Xian-Mo Zhang. Cheating Prevention in Secret sharing over $GF(p)$. INDOCRYPT 2001, Lecture Notes in Computer Science, 2247, pp. 226-243, Springer-Verlag, 2001.
5. Josef Pieprzyk and Xian-Mo Zhang. Multisecret Sharing Immune against cheating. Informatica-An International Journal of Computing and Informatics, Volume 26, Number 3, 271-278, 2002.
6. Josef Pieprzyk, Xian-Mo Zhang. Construction of cheating immune secret sharing. ICISC2001, Lecture Note in Computer Science, 2288, 226-243, Springer-Verlag2002.
7. Hossein Ghodosi, Josef Piepreyk. Cheating prevention in secret sharing. ACISP2000, Lecture Notes in Computer Science, 1841, 328-341, Springer-Verlag, 2000.
8. M. Stadler. Publicly verifiable secret sharing[A]. In Advances in cryptology. EUROCRYPT' 96[C], LNCS 1070, 190-199, Springer-Verlag, Berlin, 1996.
9. Fujisaki E, T. Okamoto. A practical and provably secure scheme for publicly verifiable secret sharing and its applications[A]. Advances in Cryptology, EUCRYPTO' 98[C], 32-47, Springer-Verlag, Berlin, 1998.
10. B. Schoenmakers. A simple publicly verifiably secret sharing scheme and its application to electronic voting[A]. CRYPTO' 99[C], 148-164, Springer-Verlag, Berlin, 1999.
11. R, J. McEliece. Finite fields for computer scientists and engineers. Kluwer Academic, 1987.
12. Wen Ping Ma, Moon Ho Lee. New methods to construct cheating immune functions. Information Security and Cryptology -ICISC2003, LNCS 2971, 79-86, Springer-Verlag, Berlin, 2003.