Discrete Mathematics and Theoretical Computer Science **6**, 2004, 253–264

On Cheating Immune Secret Sharing

Josef Pieprzyk and Xian-Mo Zhang

Centre for Advanced Computing – Algorithms and Cryptography
Department of Computing, Macquarie University
Sydney , NSW 2109, Australia
Email: josef,xianmo@ics.mq.edu.au

received Nov 14, 2003, *accepted Mar 23, 2004*.

The paper addresses the cheating prevention in secret sharing. We consider secret sharing with binary shares. The secret also is binary. This model allows us to use results and constructions from the well developed theory of cryptographically strong boolean functions. In particular, we prove that for given secret sharing, the average cheating probability over all cheating vectors and all original vectors, i.e., $\frac{1}{n} \cdot 2^{-n} \sum_{c=1}^{n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$, denoted by $\overline{\rho}$, satisfies $\overline{\rho} \geq \frac{1}{2}$, and the equality holds if and only if $\rho_{c,\alpha}$ satisfies $\rho_{c,\alpha} = \frac{1}{2}$ for every cheating vector δ_c and every original vector α. In this case the secret sharing is said to be cheating immune. We further establish a relationship between cheating-immune secret sharing and cryptographic criteria of boolean functions. This enables us to construct cheating-immune secret sharing.

Keywords: Secret Sharing, Cheating Prevention, Cheating Immune

1 Introduction

Since its invention in 1978 by Blakley (Bla79) and Shamir (Sha79), secret sharing has evolved dramatically. Initially, it was designed to facilitate a distributed storage for a secret in an unreliable or insecure environment. Later, however, secret sharing has been incorporated into public key cryptography giving rise to the well-known concept of group or society oriented cryptography (see (Des88)). Now secret sharing is one of the basic cryptographic tools with variety of very interesting schemes based on algebraic or geometric structures.

Tompa and Woll (TW88) observed that Shamir secret sharing can be subject to cheating by dishonest participants who, at the recovery stage, may submit invalid shares to the combiner. Clearly, the combiner reconstructs an invalid secret and passes it to currently active participants. The honest participants are left with the invalid secret while the cheaters are able to recover the valid secret from the invalid one. This observation is true for all linear secret sharing. The cheating attack can also be extended for geometrical secret sharing.

Cheating prevention can be considered in the context of conditionally and unconditionally secure secret sharing. We focus our attention on unconditionally secure secret sharing. In this setting, cheating can be thwarted by

- share verification by the combiner – all invalid shares are identified and discarded. The key recovery goes ahead only if there are enough valid shares to recover the valid secret (see (Car95; CSV93; RBO89)),
- discouraging cheaters from sending invalid shares to the combiner – this argument works if the cheater gains no advantage over honest participants. In other words, sending invalid share will result with recovery of an invalid secret which gives no clues to the cheater as to the value of the valid secret. This paper investigates this case of cheater prevention.

We intend to consider a class of secret sharing for which, a cheating participant is no better off than a participant who tries simply to guess a secret. Ideally, the probability of successful cheating should be equal to the probability of guessing the secret by a participant. To make our considerations explicit, we assume that secret and shares are binary. For this case we prove that there is a secret sharing, further in the work called *cheating immune*, that gives no advantage to a cheater making it, in a sense, immune against cheating. The cheating immunity was considered in (PZ01) and this paper continues this line of the study by investigating the connection between secret sharing and cryptographically strong boolean functions.

The work is structured as follows. Section 2 introduces secret sharing in terms of its notions and notations. Section 3 gives necessary background for boolean functions. In Section 4, we describe a model which is further used to characterise cheating in secret sharing. The main results are given in Section 5. Section 6 explores the problem of constructing cheating-immune secret sharing. Section 7 concludes the work.

2 Background

Secret sharing allows a group of participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ to collectively hold a secret $K \in \mathcal{K}$, where $\mathcal{K}$ is a set of elements from which the secret is drawn. Secret sharing is created by a trusted algorithm called a *dealer* who for a given secret, generates a collection of shares $s_i \in \mathcal{S}$, where $\mathcal{S}$ is a set of shares. Note that s_i is given to P_i, $i = 1, \ldots, n$. The collective ownership of the secret is defined by the access structure of secret sharing. The access structure Γ is a collection of subgroups of $\mathcal{P}$ that are authorised to recover the secret.

An authorised group of participants $\mathcal{A} \in \Gamma$ is able to reconstruct the secret by invoking a trusted algorithm called *combiner*. The combiner always returns the valid secret if the group $\mathcal{A}$ submits their valid shares. If the group, however, is too small, i.e. $\mathcal{A} \notin \Gamma$, then the algorithm returns a value which is not the valid secret (with an overwhelming probability).

In this work, we describe a secret sharing by a set of *distribution rules* (Sti95), where a distribution rule is a function $f : \mathcal{P} \to \mathcal{S}$ that represents possible distribution of shares to the participants. In other words, secret sharing is a set

$$\mathcal{F} = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K$$

where $\mathcal{F}_K$ is a distribution rule corresponding to the secret K. Equivalently, $\mathcal{F}$ can be presented in the form of *distribution table* $\mathcal{T}$. The table has $(n+1)$ columns – the first one includes secrets and the other n ones list shares assigned to participants $(P_1, \ldots, P_n)$, respectively. Each row of the distribution table specifies the secret for a collection of shares held by $\mathcal{P}$. Note that $\mathcal{F}_K$ can be seen as a part of the distribution table with rows whose first entry is K. This table is denoted by $\mathcal{T}_K$.

Most of practical secret sharing schemes are linear and therefore subject to an attack observed by Tompa and Woll (TW88). The attack permits a dishonest participant who at the pooling stage submits an invalid share, to recover the valid secret from an invalid one returned by the combiner.

3 Binary Sequences

We consider a mapping f from V_n to $GF(2)$ where V_n is the vector space of n tuples of elements from $GF(2)$. f is also called a *function* on V_n. The *truth table* of a mapping f is a sequence defined by $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$, where $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, …, $\alpha_{2^n-1} = (1,\ldots,1,1)$. Each α_j is said to be the *binary representation* of integer j, $j = 0,1,\ldots,2^n-1$. A function f is said to be *balanced* if its truth table contains an equal number of zeros and ones.

An *affine* function f on V_n is a function that takes the form of $f(x_1,\ldots,x_n) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $\oplus$ denotes the addition in $GF(2)$, $a_j, c \in GF(2)$, $j = 1,2,\ldots,n$. The function f is called a *linear* function if $c = 0$. It is easy to verify that any nonzero affine function is balanced. Let $\langle,\rangle$ denote the scalar product of two vectors. There precisely exist 2^n linear functions on V_n. We can denote all the 2^n linear functions by $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$, where $\varphi_j(x) = \langle\alpha_j, x\rangle$.

The *Hamming weight* of a vector $\alpha \in V_n$, denoted by $HW(\alpha)$, is the number of nonzero coordinates of α. The Hamming weight of a function f, denoted by $HW(f)$, is the number of nonzero terms in the truth table of f.

The *nonlinearity* of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e.,

$$N_f = \min_{i=1,2,\ldots,2^{n+1}} HW(f \oplus \psi_i)$$

where ψ_1, ψ_2, …, $\psi_{2^{n+1}}$ are all the affine functions on V_n. High nonlinearity can be used to resist a linear attack. We know that $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$ (MS78).

Let f be a function on V_n. We say that f satisfies the *propagation criterion with respect to* α if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, where $x = (x_1,\ldots,x_n) \in V_n$ and $\alpha = (a_1,\ldots,a_n) \in V_n$. Furthermore f is said to satisfy the *propagation criterion of degree k* if it satisfies the propagation criterion with respect to every nonzero vector α whose Hamming weight is not larger than k. (PLL$^+$91). The propagation properties were employed in selecting the S-boxes used in the cipher, which contributed to the strength of the cipher against various attacks including differential (BS91) and linear (Mat94) attacks. Note that the *strict avalanche criterion (SAC)* (WT86) is the same as the propagation criterion of degree one.

The concept of correlation immune functions was introduced by Siegenthaler (Sie84). Xiao and Massey gave an equivalent definition (CCCS91; XM88). A function f on V_n is called a *k-th order correlation immune function* if $\sum_{x\in V_n} f(x)(-1)^{\langle\beta,x\rangle} = 0$ for all $\beta \in V_n$ with $1 \leq HW(\beta) \leq k$, where $f(x)$ and $\langle\beta,x\rangle$ are regarded as real-valued functions. Correlation immune functions are used in the design of running-key generators in stream ciphers to resist a correlation attack. A balanced kth-order correlation immune function is also called a *k-resilient function*. Due to Lemma 3 of (ZZ97), we can give a k-resilient function an equivalent definition: a function f is said to be k-resilient if f satisfies the property: for every subset $\{j_1,\ldots,j_k\}$ of $\{1,\ldots,n\}$ and every $(a_1,\ldots,a_k) \in V_k$,

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

is a balanced function on V_{n-k}.

A special class of functions is called bent. There exist equivalent definitions of bent functions (Rot76). For example, a function f on V_n is said to be *bent* if and only if f satisfies the propagation criterion with respect to every nonzero vector in V_n. The sum of any bent function on V_n and any affine function on V_n is bent. Bent functions are not balanced and bent functions on V_n exist only when n is even. Furthermore, it is well known that any bent function f on V_n achieves the maximum nonlinearity, i.e., $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$.

4 Model of Cheating

Given (n,n) threshold secret sharing defined by its distribution table $\mathcal{T}$. We define a function $f : V_n \to \{0,1\}$ and fix an integer c; $1 \le c \le n$, which points to the position (column) of the cheater P_c in $\mathcal{T}$. The vector $\delta_c = (0,\ldots,0,1,0,\ldots,0) \in V_n$ represents the cheating vector introduced by the cheater. Note that the cheater P_c can only change his share on the c-th position (other positions are not changed assuming that other participants are honest). Let $\rho_{c,\alpha}$ be the probability of successful cheating by P_c, where α is a row of $\mathcal{T}$ indicating the secret and shares currently in use. A precise expression of $\rho_{c,\alpha}$ will be given in next two paragraphs. In the work (PZ01), it was shown that for an arbitrary α, there is a vector $\alpha' \in V_n$ such that either $\rho_{c,\alpha} + \rho_{c,\alpha'} = 1$ or $\rho_{c,\alpha} = 1$. This implies that the maximum cheating probability is always larger than or equal to $\frac{1}{2}$. Naturally one would expect that (a) $\max\{\rho_{c,\alpha} | \alpha \in V_n,\ 1 \le c \le n\}$ is as small as possible, and (b) $\overline{\rho} = \frac{1}{n} \cdot 2^{-n} \sum_{c=1}^{n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$ is as small as possible (ideally, the both probabilities are equal to $\frac{1}{2}$). In this paper we identify conditions for which (a) and (b) hold and as the result we introduce the concept of *cheating-immune* secret sharing. Furthermore we characterise cheating-immune secret sharing using cryptographic properties of boolean functions. Thus we are able to construct cheating-immune secret sharing that gives no advantage to a cheater over honest participants.

We introduce the following notations:

- $\alpha = (s_1,\ldots,s_n)$ is the sequence of shares held by $\mathcal{P}$ and the secret $K = f(\alpha)$,
- $\alpha^* = (s_1,\ldots,s_{c-1},1 \oplus s_c,s_{c+1},\ldots,s_n)$ is the sequence of shares submitted to the combiner where P_c modified her share. The sequence
  $\delta_c = (0,\ldots,0,1,0,\ldots,0)$ contains all zero except the c-th position and represents modification done by the cheater, $K^* = f(\alpha^*)$ is the invalid secret returned by combiner,
- $\Omega^*_\alpha = \{(x_1,\ldots,x_{c-1},s_c,x_{c+1},\ldots,x_n) | f(x_1,\ldots,x_{c-1},1 \oplus s_c,x_{c+1},\ldots,x_n) = K^*\}$ is the set of all shares taken from rows of $\mathcal{T}$ containing α and K which are consistent with the invalid secret returned by the combiner. The set determines the view of the cheater after getting back K^* from the combiner,
- $\Omega_\alpha = \{(x_1,\ldots,x_{c-1},s_c,x_{c+1},\ldots,x_n) | f(x_1,\ldots,x_{c-1},s_c,x_{c+1},\ldots,x_n) = K\}$ is the set of rows which contain the current share of P_c and the valid secret K.

The function f is called *defining function*. To prevent cheaters from finding the correct secret (and effectively discourage them from cheating), one would wish to obtain Ω^*_α as big as possible for any α, while $\Omega^*_\alpha \cap \Omega_\alpha$ as small as possible. The nonzero vector $\delta_c = (0,\ldots,0,1,0,\ldots,0)$, where only the c-th coordinate is nonzero, is called the *cheating vector*. $\alpha = (s_1,\ldots,s_n)$ is called the *original vector*. The value of $\rho_{c,\alpha} = \#(\Omega^*_\alpha \cap \Omega_\alpha)/\#\Omega^*_\alpha$, where $\#X$ denotes the the number of elements in the set X, expresses the probability of cheater success with respect to $\alpha = (s_1,\ldots,s_n)$. As the original vector $\alpha = (s_1,\ldots,s_n)$ is always in $\Omega^*_\alpha \cap \Omega_\alpha$, the probability of successful cheating is always nonzero or $\rho_{c,\alpha} > 0$.

The following result can be found in (PZ01):

Theorem 1 *Given secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n. Let c be any integer with $1 \le c \le n$ and $\alpha = (s_1, \ldots, s_n)$ be any vector in V_n. Then there exists a vector $\alpha' \in V_n$ such that $\rho_{c,\alpha} + \rho_{c,\alpha'} = 1$ otherwise $\rho_{c,\alpha} = 1$.*

Theorem 1 implies that the maximum probability of successful cheating is always higher than or equal to $\frac{1}{2}$.

Given secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n. The value of

$$\rho_c = 2^{-n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$$

is the average cheating probability over all original vectors in V_n for a fixed cheating vector. The value of

$$\overline{\rho} = \frac{1}{n} \sum_{c=1}^{n} \rho_c = \frac{1}{n} \cdot 2^{-n} \sum_{c=1}^{n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$$

is the average cheating probability over all cheating vectors (with Hamming weight one) and all original vectors in V_n.

It should be noticed that the definition of $\overline{\rho}$ depends on a particular defining function f.

Theorem 2 *Given secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n. Then for each fixed integer c with $1 \le c \le n$, we have $\rho_c \ge \frac{1}{2}$ where the equality holds if and only if $\rho_{c,\alpha} = \frac{1}{2}$ for each $\alpha \in V_n$.*

Proof 1 *Write $y = (x_1, \ldots, x_{c-1})$ and $z = (x_{c+1}, \ldots, x_n)$. Set*

$$\begin{aligned} R_1 &= \{(y,z) | f(y,1,z) = 1, \quad f(y,0,z) = 1\} \\ R_2 &= \{(y,z) | f(y,1,z) = 1, \quad f(y,0,z) = 0\} \\ R_3 &= \{(y,z) | f(y,1,z) = 0, \quad f(y,0,z) = 1\} \\ R_4 &= \{(y,z) | f(y,1,z) = 0, \quad f(y,0,z) = 0\} \end{aligned} \tag{1}$$

and $\#R_i = r_i$, $i = 1,2,3,4$. Obviously $r_1 + r_2 + r_3 + r_4 = 2^{n-1}$.

Let $\beta_1 \in V_{c-1}$, $\beta_2 \in V_{n-c}$ and $\alpha = (\beta_1, 0, \beta_2)$ or $\alpha = (\beta_1, 1, \beta_2)$. Due to the definition of $\rho_{c,\alpha}$, it is easy to verify that

$$\rho_{c,\alpha} = \begin{cases} \frac{r_1}{r_1+r_2} & \text{if } \alpha = (\beta_1,0,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_1 \\ \frac{r_2}{r_1+r_2} & \text{if } \alpha = (\beta_1,0,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_2 \\ \frac{r_3}{r_3+r_4} & \text{if } \alpha = (\beta_1,0,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_3 \\ \frac{r_4}{r_3+r_4} & \text{if } \alpha = (\beta_1,0,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_4 \\ \frac{r_1}{r_1+r_3} & \text{if } \alpha = (\beta_1,1,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_1 \\ \frac{r_3}{r_1+r_3} & \text{if } \alpha = (\beta_1,1,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_3 \\ \frac{r_2}{r_2+r_4} & \text{if } \alpha = (\beta_1,1,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_2 \\ \frac{r_4}{r_2+r_4} & \text{if } \alpha = (\beta_1,1,\beta_2), \text{ where } (\beta_1,\beta_2) \in R_4 \end{cases} \tag{2}$$

There exist two cases to be considered: $R_j \cup R_i \neq \emptyset$*, where* $\emptyset$ *denotes the empty set, for each* $(j,i) \in \{(1,2),(3,4),(1,3),(2,4)\}$*, and* $R_{j_0} \cup R_{i_0} = \emptyset$ *for some* $(j_0,i_0) \in \{(1,2),(3,4),(1,3),(2,4)\}$.

Case 1: $R_j \cup R_i \neq \emptyset$ *for each* $(j,i) \in \{(1,2),(3,4),(1,3),(2,4)\}$. *In this case* $r_j + r_i \neq 0$ *for each* $(j,i) \in \{(1,2),(3,4),(1,3),(2,4)\}$. *Therefore we can compute* ρ_c*:*

$$\begin{aligned}\rho_c &= 2^{-n}\sum_{\alpha\in V_n}\rho_{c,\alpha} = 2^{-n}\Big(\frac{r_1^2}{r_1+r_2}+\frac{r_2^2}{r_1+r_2}+\frac{r_3^2}{r_3+r_4} \\ &\quad +\frac{r_4^2}{r_3+r_4}+\frac{r_1^2}{r_1+r_3}+\frac{r_3^2}{r_1+r_3}+\frac{r_2^2}{r_2+r_4}+\frac{r_4^2}{r_2+r_4}\Big) \qquad (3)\end{aligned}$$

It is easy to see that $(a-b)^2 \geq 0$ *or equivalently* $\frac{a^2+b^2}{a+b} \geq \frac{1}{2}(a+b)$ *for any two real numbers with* $a,b \geq 0$ *and* $a+b>0$ *where the equality holds if and only if* $a=b$. *Using the same arguments on (3), we conclude that*

$$\begin{aligned}\rho_c &\geq 2^{-n}\Big(\frac{1}{2}(r_1+r_2)+\frac{1}{2}(r_3+r_4)+\frac{1}{2}(r_1+r_3)+\frac{1}{2}(r_2+r_4)\Big) \\ &= 2^{-n}(r_1+r_2+r_3+r_4) = \frac{1}{2} \qquad (4)\end{aligned}$$

where the equality holds if and only if $r_1=r_2=r_3=r_4$. *From (2),* $r_1=r_2=r_3=r_4$ *if and only if* $\rho_{c,\alpha}=\frac{1}{2}$ *for each* $\alpha \in V_n$. *Therefore, in Case 1,* $\rho_c \geq \frac{1}{2}$ *where the equality holds if and only if* $\rho_{c,\alpha}=\frac{1}{2}$ *for each* $\alpha \in V_n$.

Case 2: $R_{j_0} \cup R_{i_0} = \emptyset$ *for some* $(j_0,i_0) \in \{(1,2),(3,4),(1,3),(2,4)\}$. *Without loss of generality we assume that* $R_1 \cup R_2 = \emptyset$. *In this case* $r_1=r_2=0$ *and thus* $r_3+r_4=2^{n-1}$.

There exist two cases to be considered: $R_j \cup R_i \neq \emptyset$ *for each* $(j,i) \in \{(3,4),(1,3),(2,4)\}$*, and* $R_{j_1} \cup R_{i_1} = \emptyset$ *for some* $(j_1,i_1) \in \{(3,4),(1,3),(2,4)\}$.

Case 2.1: $R_j \cup R_i \neq \emptyset$ *for each* $(j,i) \in \{(3,4),(1,3),(2,4)\}$. *In this case* $r_j+r_i \neq 0$ *for each* $(j,i) \in \{(3,4),(1,3),(2,4)\}$.

We can compute ρ_c*:*

$$\rho_c = 2^{-n}\sum_{\alpha\in V_n}\rho_{c,\alpha} = 2^{-n}\Big(\frac{r_3^2}{r_3+r_4}+\frac{r_4^2}{r_3+r_4}+\frac{r_3^2}{r_1+r_3}+\frac{r_4^2}{r_2+r_4}\Big)$$

Since $r_1=r_2=0$*, we have* $\rho_c = 2^{-n}\sum_{\alpha\in V_n}\rho_{c,\alpha} = 2^{-n}(\frac{r_3^2+r_4^2}{r_3+r_4}+r_3+r_4)$. *Note that* $\frac{r_3^2+r_2^4}{r_3+r_4} \geq \frac{1}{2}(r_3+r_4)$ *and* $r_3+r_4=2^{n-1}$. *Thus we conclude that* $\rho_c \geq 2^{-n}(\frac{1}{2}(r_3+r_4)+r_3+r_4) = \frac{3}{4}$.

Case 2.2: $R_{j_1} \cup R_{i_1} = \emptyset$ *for some* $(j_1,i_1) \in \{(3,4),(1,3),(2,4)\}$. *Recall that* $r_3+r_4=2^{n-1}$. *Thus* $(j_1,i_1) \neq (3,4)$. *Without loss generality we assume that* $(j_1,i_1)=(1,3)$. *In other words,* $R_1 \cup R_3 = \emptyset$. *Thus* $r_3=0$. *Since* $r_1=r_2=r_3=0$*, we know that* $r_4=2^{n-1}$. *We compute* ρ_c*:*

$$\rho_c = 2^{-n}\sum_{\alpha\in V_n}\rho_{c,\alpha} = 2^{-n}\Big(\frac{r_4^2}{r_3+r_4}+\frac{r_4^2}{r_2+r_4}\Big)$$

Since $r_2=r_3=0$*, we have* $\rho_c = 2^{-n}(r_4+r_4)=1$.

Summarising Cases 1 and 2, we have proved that $\rho_c \geq \frac{1}{2}$ *where the equality holds if and only if* $\rho_{c,\alpha}=\frac{1}{2}$ *for each* $\alpha \in V_n$. □

Theorem 3 *Given secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n. Then $\overline{\rho} \geq \frac{1}{2}$ where the equality holds if and only if $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$.*

Proof 2 *By using Theorem 2, we have*

$$\overline{\rho} = \frac{1}{n}\sum_{c=1}^{n} \rho_c \geq \frac{1}{2} \tag{5}$$

Hence we have proved inequality in the theorem.

Assume $\overline{\rho} = \frac{1}{2}$. From $\overline{\rho} = \frac{1}{2}$ and $\rho_c \geq \frac{1}{2}$, $c = 1,\ldots,n$, we know that $\rho_c = \frac{1}{2}$, $c = 1,\ldots,n$. By using Theorem 2, we know that $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$. We have proved the necessity. The sufficiency is obvious. Hence we proved the theorem. □

5 Cheating-Immune Secret Sharing Scheme

Secret sharing resists cheating if either $\max\{\rho_{c,\alpha} | \alpha \in V_n,\ 1 \leq c \leq n\}$ is as small as possible, or $\overline{\rho}$ is as small as possible. As mentioned in Section 4, the maximum cheating probability is always larger than or equal to $\frac{1}{2}$. Due to Theorem 1, if $\overline{\rho} = \frac{1}{2}$ then the maximum cheating probability is equal to $\frac{1}{2}$. We now prove the converse. Assume that the maximum cheating probability is equal to $\frac{1}{2}$. We next prove that $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$. Assume for contradiction that $\rho_{c,\alpha} < \frac{1}{2}$ for some integer c with $1 \leq c \leq n$ and some $\alpha \in V_n$. According to Theorem 1, there exists another vector $\alpha' \in V_n$ such that $\rho_{c,\alpha} + \rho_{c,\alpha'} = 1$ then $\rho_{c,\alpha'} > \frac{1}{2}$. This contradicts the assumption that the maximum cheating probability is equal to $\frac{1}{2}$. The contradiction proves $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$. In this case, clearly, $\overline{\rho} = \frac{1}{2}$.

Due to Theorems 2 and 3, we conclude

Corollary 1 *Given secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n. Then the following statements are equivalent:*

(i) $\overline{\rho} = \frac{1}{2}$,

(ii) $\rho_c = \frac{1}{2}$ *for each integer c with $1 \leq c \leq n$,*

(iii) $\rho_{c,\alpha} = \frac{1}{2}$ *for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$.*

A secret sharing is said to be *cheating immune* if it satisfies (i) or (ii) or (iii) of Corollary 1.

Cheating immunity of secret sharing can be investigated in the context of well-known characteristics of the defining function f such as correlation immunity and SAC.

Theorem 4 *Given secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n. Then the secret sharing is cheating immune if and only if f is 1-resilient and satisfies the SAC.*

Proof 3 *We keep using the notations as in the proof of Theorem 2. Assume that the secret sharing is cheating immune. Let c be an integer with $1 \leq c \leq n$. Using Corollary 1, $\rho_{c,\alpha} = \frac{1}{2}$ for each $\alpha \in V_n$. Therefore, from the proof of Theorem 2, we have $r_1 = r_2 = r_3 = r_4$. From $r_1 + r_2 = r_3 + r_4$, we conclude that*

$f(x_1,\dots,x_n)|_{x_c=1}$ is balanced. Similarly from the fact $r_1+r_3=r_2+r_4$, we conclude that $f(x_1,\dots,x_n)|_{x_c=0}$ is balanced. Since c is arbitrarily in $\{1,\dots,n\}$, we have proved that f is 1-resilient.

We now consider $f(x)\oplus f(x\oplus\delta_c)$ where $\delta_c=(0,\dots,0,1,0,\dots,0)$ has been defined in Section 4.

Let $x=(y,x_c,z)$ where $y\in V_{c-1}$, $z\in V_{n-c}$ and $x_c\in GF(2)$. ¿From (1),

$$f(x)\oplus f(x\oplus\delta_c)=\begin{cases}0 & \text{if } (y,z)\in R_1 \text{ or } (y,z)\in R_4\\ 1 & \text{if } (y,z)\in R_2 \text{ or } (y,z)\in R_3\end{cases} \tag{6}$$

Since $r_1=r_2=r_3=r_4$, from (6), it is clear that $f(x)\oplus f(x\oplus\delta_c)$ is balanced. Note that c is an arbitrarily integer with $1\le c\le n$. Thus we have proved that f satisfies the SAC.

Conversely assume that f is 1-resilient and satisfies the SAC. Let c be an integer with $1\le c\le n$. Due to the 1-resilience, $f(x_1,\dots,x_n)|_{x_c=1}$ is balanced and thus $r_1+r_2=r_3+r_4$. Similarly $f(x_1,\dots,x_n)|_{x_c=0}$ is balanced and thus $r_1+r_3=r_2+r_4$.

On the other hand, since f satisfies the SAC, $f(x)\oplus f(x\oplus\delta_c)$ is balanced. From (6), we have $r_1+r_4=r_2+r_3$. Combing $r_1+r_2=r_3+r_4$, $r_1+r_3=r_2+r_4$ and $r_1+r_4=r_2+r_3$, we conclude that $r_1=r_2=r_3=r_4$. From the proof of Theorem 2, we have proved that $\rho_{c,\alpha}=\frac{1}{2}$ for each $\alpha\in V_n$. Since c is an arbitrarily integer with $1\le c\le n$, we have proved that the secret sharing is cheating immune. □

Since resilient functions are balanced, the defining function of any cheating immune secret sharing must be balanced.

6 Construction of Cheating-Immune Secret Sharing Scheme

Based on Theorem 4, to construct an cheating-immune secret sharing scheme, we need a 1-resilient function on V_n satisfying the SAC.

The following result can be found from the proof of Theorem 17 of the reference (SM00), that is an article on boolean functions with cryptographic properties.

Lemma 1 *Let h be a bent function on V_{n-2} (n is even). Set*

$$g(x_1,\dots,x_{n-1})=(1\oplus x_{n-1})h(x_1,\dots,x_{n-2})\oplus x_{n-1}(1\oplus h(x_1\oplus a_1,\dots,x_{n-2}\oplus a_{n-2}))$$

where $HW(a_1,\dots,a_{n-2})=\frac{1}{2}n-1$. Set

$$f(x_1,\dots,x_n)=(1\oplus x_n)g(x_1,\dots,x_{n-1})\oplus x_n g(x_1\oplus 1,\dots,x_{n-1}\oplus 1)$$

Then

(i) *f is 1-resilient,*

(ii) *f satisfies the propagation criterion of degree $\frac{1}{2}n-1$,*

(iii) *f has a nonlinearity $2^{n-1}-2^{\frac{1}{2}n}$.*

If we apply the function mentioned in Lemma 1 to Theorem 4, then we obtain an cheating-immune secret sharing with defining function whose nonlinearity is $2^{n-1}-2^{\frac{1}{2}n}$. Therefore we have the following conclusion:

Theorem 5 *Let $n > 0$ be an even integer. Then there exists a secret sharing with its distribution table $\mathcal{T}$ and the defining function f on V_n such that*

(i) this secret sharing is cheating immune,

(ii) the nonlinearity N_f of f satisfies $2^{n-1} - 2^{\frac{1}{2}n}$.

For each secret sharing constructed in (PZ01), there always exists some integer c and some vector $\alpha \in V_n$ such that $\rho_{c,\alpha} > \frac{1}{2}$. Therefore each secret sharing in (PZ01) is not cheating immune.

Example 1 Let $n = 4$ in Lemma 1. Set $h(x_1, x_2) = x_1x_2$. It is easy to see that h is a bent function on V_2. Choose $(a_1, a_2) = (1, 0)$. Then $HW(a_1, a_2) = 1 = \frac{1}{2}n - 1$.

Set

$$g(x_1, x_2, x_3) = (1 \oplus x_3)h(x_1, x_2) \oplus x_3(1 \oplus h(1 \oplus x_1, x_2)) = x_1x_2 \oplus x_2x_3 \oplus x_3$$

We further set

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= (1 \oplus x_4)g(x_1, x_2, x_3) \oplus x_4 g(x_1 \oplus 1, x_2 \oplus 1, x_3 \oplus 1) \\ &= x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_3 \oplus x_4 \end{aligned}$$

Due to Lemma 1, f is 1-resilient and satisfies the propagation criterion of degree 1 (SAC). Due to Theorem 4, this secret sharing is cheating immune. Let the group $\mathcal{P}$ include four participants and the defining function

$$f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_3 \oplus x_4$$

It is easy to find the truth table of f which is

$$0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0$$

The secret sharing can be described as the following table:

f	S_1	S_2	S_3	S_4
0	0	0	0	0
1	0	0	0	1
1	0	0	1	0
1	0	0	1	1
0	0	1	0	0
1	0	1	0	1
0	0	1	1	0
0	0	1	1	1
0	1	0	0	0
0	1	0	0	1
1	1	0	1	0
0	1	0	1	1
1	1	1	0	0
1	1	1	0	1
1	1	1	1	0
0	1	1	1	1

Using Theorem 4 or by a straightforward verification, we get that $N_f = 4 = 2^{n-1} - 2^{\frac{1}{2}n}$ where $n = 4$.

Assume that the dealer fixed the shares $\alpha = (1,0,1,0) \in V_4$ and the secret $K = f(1,0,1,0) = 1$. Our cheater is P_3. Thus $\delta_3 = (0,0,1,0)$ and $c = 3$. The combiner obtains the sequence $\alpha^* = (1,0,0,0)$ with the third share changed by the cheater and returns the invalid secret $K^* = f(1,0,0,0) = 0$. On receiving K^*, the cheater can identify the set

$$\Omega^*_\alpha = \{(x_1,x_2,1,x_4) | f(x_1,x_2,0,x_4) = 0\}$$

which is $\Omega^*_\alpha = \{(0,0,1,0),(0,1,1,0),(1,0,1,0),(1,0,1,1)\}$. The set

$$\Omega_\alpha = \{(x_1,x_2,1,x_4) | f(x_1,x_2,1,x_4) = 1\}$$

becomes $\Omega_\alpha = \{(0,0,1,0),(0,0,1,1),(1,0,1,0),(1,1,1,0)\}$.

The intersection $\Omega^*_\alpha \cap \Omega_\alpha = \{(0,0,1,0),(1,0,1,0)\}$ and the probability of successful cheating is $\rho_{3,\alpha} = \#(\Omega^*_\alpha \cap \Omega_\alpha)/\#\Omega^*_\alpha = \frac{1}{2}$.

7 Conclusions

We have proved an interesting property of secret sharing. For given secret sharing, the average cheating probability over all cheating vectors and all original vectors, denoted by $\overline{\rho}$, satisfies $\overline{\rho} \geq \frac{1}{2}$, and the equality holds if and only if the cheating probability $\rho_{c,\alpha}$ satisfies $\rho_{c,\alpha} = \frac{1}{2}$ for every cheating vector δ_c and every original vector α. In this case the secret sharing is said to be cheating immune. We have found a relationship between cheating immune secret sharing and cryptographic criteria of boolean functions, and then we have successfully constructed cheating immune secret sharing using a highly nonlinear defining function. For simplicity, in this work we have considered cheating immune secret sharing where there is a single dishonest participant (or cheater). However this concept can be generalised for the case where there are many colluding cheaters. Future works include also the design of cheating immune secret sharing for a given access structure.

Acknowledgements

The work was in part supported by Australian Research Council grant A00103078 and DP0345366. The authors thank the anonymous referees for helpful comments.

References

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of AFIPS 1979 National Computer Conference*, pages 313–317, 1979.

[BS91] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.

[Car95] M. Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes and Cryptography*, 5(3):183–187, 1995.

[CCCS91] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[CSV93] M. Carpentieri, A. De Santis, and U. Vaccaro. Size of shares and probability of cheating in threshold schemes. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 118–125. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[Des88] Y. Desmedt. Society and group oriented cryptography: A new concept. In *Advances in Cryptology - CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 120–127. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

[Mat94] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[MS78] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.

[PLL+91] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437 of *Lecture Notes in Computer Science*, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[PZ01] J. Pieprzyk and X. M. Zhang. Nonlinear secret sharing immune against cheating. In Knowledge Systems Institute, editor, *Proceedings of 2001 International Workshop on Cryptology and Network Security, parallel to The Seventh International Conference on Distributed Multimedia Systems*, pages 154–161. DMS, 2001.

[RBO89] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In Proceedings of 21st ACM Symposium on Theory of Computing, pages 73–85. Springer-Verlag, Berlin, Heidelberg, New York, 1989.

[Rot76] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[Sie84] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30 No. 5:776–779, 1984.

[SM00] P. Sarkar and S. Maitra. Highly nonlinear balanced boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[Sti95] D.R. Stinson. Cryptography: Theory and practice. CRC Press, 1995.

[TW88] M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1(2):133–138, 1988.

[WT86] A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219 of *Lecture Notes in Computer Science*, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.

[XM88] G. Z. Xiao and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.

[ZZ97] X. M. Zhang and Y. Zheng. Cryptographically resilient functions. *IEEE Transactions on Information Theory*, 43(5):1740–1747, 1997.