Constructions of Cheating Immune Secret Sharing

Josef Pieprzyk[1] and Xian-Mo Zhang[2]

[1] Department of Computing
Macquarie University
Sydney , NSW 2109, AUSTRALIA
josef@ics.mq.edu.au
[2] School of IT and CS, University of Wollongong
Wollongong NSW 2522, AUSTRALIA
xianmo@cs.uow.edu.au

Abstract. The work addresses the problem of cheating prevention in secret sharing. Two cheating scenarios are considered. In the first one, the cheaters always submit invalid shares to the combiner. In the second one, the cheaters collectively decide which shares are to be modified so the combiner gets a mixture of valid and invalid shares from the cheaters. The secret scheme is said to be k-cheating immune if any group of k cheaters has no advantage over honest participants. The paper investigates cryptographic properties of the defining function of secret sharing so the scheme is k-cheating immune. Constructions of secret sharing immune against k cheaters are given.

1 Introduction

Secret sharing is the basic cryptographic tool that allows to define an environment in which the active entity is a group. A (t, n) threshold secret sharing scheme permits any group of t or more participants to access the secret. Any group of $t-1$ or less participants cannot recover the secret. The group operation is normally performed by a trusted combiner who collects shares from participants, computes the result and communicates it to the members of the active group. Tompa and Woll [20] showed that a dishonest participant can cheat by providing an invalid share to the combiner. If the secret sharing in use is linear then the cheater is able to recover the valid secret from an invalid secret returned by the combiner. In effect, the cheater holds the secret while other (honest) participants are left with an invalid secret.

Cheating prevention becomes a major challenge in the distributed environment. Ideally, one would expect that a cheater should gain no advantage over honest participants. The problem can be addressed by forcing the combiner to check validity of shares before they are used to recover the secret. In the conditionally secure setting, shares can be checked using verifiable secret sharing (see [4, 8, 17, 13]). In the unconditionally secure secret sharing, shares can be verified

using a system of linear equations (see [11, 2, 1]). Note that share verification requires the combiner to be able to access the additional information (which also needs to be authenticated). This introduces extra complexity in the design and maintenance of secret sharing.

An alternative approach removes the main incentive for cheating. If one or more shares are invalid, then the invalid secret recovered by the combiner provides no information about the valid secret. In a sense, the cheaters position is similar to that of the honest participants except that the cheater knows that the recovered secret is invalid (in practice, the honest participants will learn about this with some delay when they try to use the invalid secret with a predictable failure).

The work in this paper covers the case where shares and the secret are binary. The non-binary case when shares are from $GF(p^t)$, was considered in [9]. Note that for the binary case, functions display some "special" characteristics not found when $p > 2$. In effect, constructions for binary case do not follow those for the case when shares are drawn from $GF(p^t)$. Moreover, design of strictly cheating immune secret sharing over $GF(p^t)$ is in general easier than over $GF(2)$.

This work uses a different concept of cheating prevention by removing the main incentive for cheating. The secret sharing is design in such a way that the group of cheaters has no advantage over honest participants. In the case of cheating, all participants (honest and dishonest) end up with an invalid secret and both honest and dishonest participants have the same probability of guessing the valid secret. This differentiate our approach from others (such as that in [3]) in which cheating prevention is done by share verification. In other words, the combiner will return secret only when all shares submitted are valid.

The work is structured as follows. Binary sequences are introduced in Section 2. An initial model of cheating is introduced in Section 3 and a lower bound on the probability of successful cheating is derived. The strengthened propagation is defined and its basic properties are investigated in Section 3.1. Secret sharing immune against k cheaters is studied in Section 3.2 and such secret sharing is constructed in Section 3.3. A generalised model of cheating where cheaters may submit a mixture of their valid and invalid shares, is considered in Section 4. Properties of secret sharing immune against the generalised cheating are examined in Section 4.1 and construction for such secret sharing is given in Section 4.2. In this paper we provide all proofs in the Appendix.

2 Binary Sequences

Let $GF(2)$ denote the binary field and V_n denote the vector space of n tuples of elements from $GF(2)$. Then each vector α can be expressed as $\alpha = (a_1, \ldots, a_n)$ where each $a_j \in GF(2)$. We consider a mapping f from V_n to $GF(2)$. f can be written as $f(x)$ or $f(x_1, \ldots, x_n)$, where $x = (x_1, \ldots, x_n)$ and each $x_j \in GF(2)$. f is also called a *function* on V_n. The *truth table* of f is a sequence defined by $(f(\alpha_0),\ f(\alpha_1), \ldots,\ f(\alpha_{2^n-1}))$, where $\alpha_0 = (0, \ldots, 0, 0)$, $\alpha_1 = (0, \ldots, 0, 1)$, $\ldots$, $\alpha_{2^n-1} = (1, \ldots, 1, 1)$. 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 $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $\oplus$ denotes the addition in $GF(2)$, $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$. It is easy to verify that any nonzero affine function is balanced.

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.

Let f be a function on V_n. We say that f satisfies the *propagation criterion with respect to* $\alpha \in V_n$ 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 [10]. Note that the *SAC (strict avalanche criterion)* [19] is the same as the propagation criterion of degree one.

Due to Lemma 3 of [22], we can give a k-resilient function an equivalent definition. A function f on V_n is said to be k-resilient if 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}. Additionally using Corollary 2 of [22], we can say that f is k-resilient if it is also t-resilient for any $t = 0, 1, \ldots, k$.

A vector $\alpha \in V_n$ is called a *linear structure* of f if $f(x) \oplus f(x \oplus \alpha)$ is a constant. For any function f, the zero vector on V_n is a linear structure. It is easy to verify that the set of all linear structures of a function f form a linear subspace of V_n, whose dimension is called the *linearity of* f.

Bent functions create a special class of functions. The class can be defined differently but all definitions are equivalent [12]. A function f on V_n is said to be *bent* 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.

3 Initial Model of Cheating

We see secret sharing as a set of distribution rules combined into a single table $\mathcal{T}$ (see [18]) with binary entries. We also assume that we are dealing with (n, n) threshold scheme where any n participants are able to determine a single entry from $\mathcal{T}$ which indicates the secret. Being more specific, the sequence of shares is $x = (x_1, \ldots, x_n)$ and the secret is $f(x)$ where $f : V_n \to \{0, 1\}$.

Our considerations are restricted to the case of (n, n) secret sharing. The general case of (n, N) secret sharing can be seen as a concatenation of (n, n) secret sharing with a system of N "consistent" linear equations. Shares are generated for N participants using the linear equations. Any n participants can get a system of linear equations with a unique solution which points out the unique row of the table $\mathcal{T}$.

Let $x = (x_1, \ldots, x_n)$ and $\delta = (\delta_1, \ldots, \delta_n)$ be two vectors in V_n. Define a vector in V_n, denoted by x^+_δ, whose j-th coordinate is x_j if $\delta_j = 1$, or 0 if $\delta_j = 0$. In addition, we denote a vector by x^-_δ, whose j-th coordinate is 0 if $\delta_j = 1$, or x_j if $\delta_j = 0$. For example, let $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, and $\delta = (0, 1, 0, 1, 1, 0, 0)$ then $x^+_\delta = (0, x_2, 0, x_4, x_5, 0, 0)$ and $x^-_\delta = (x_1, 0, x_3, 0, 0, x_6, x_7)$.

It is easy to verify the properties of operations x^+_δ and x^-_δ: (i) $(\beta \oplus \gamma)^\pm_\delta = \beta^\pm_\delta \oplus \gamma^\pm_\delta$ holds for any two vectors β and γ in V_n, (ii) $\delta^+_\delta = \delta$, $\delta^-_\delta = 0$, (iii) $\beta^+_\delta \oplus \beta^-_\delta = \beta$ holds for any $\beta \in V_n$.

Given a function f on V_n. We introduce the following notations:

- Let $\alpha \in V_n$ be the sequence of shares held by the group $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants and the secret $K = f(\alpha)$.
- The collection of cheaters is determined by the sequence $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$ where P_i is a cheater if and only if $\delta_i = 1$.
- At the pooling time, the cheaters submit their shares. It is assumed that cheaters always submit invalid shares. The honest participants always submit their valid shares. We consider the vector $\alpha \oplus \delta$. From the properties of x^+_δ and x^-_δ,
$$\alpha \oplus \delta = \alpha^-_\delta \oplus \alpha^+_\delta \oplus \delta$$
Thus the combiner obtains $\alpha \oplus \delta$ that splits into two parts: α^-_δ – the part submitted by honest participants, and $\alpha^+_\delta \oplus \delta$ – the part submitted by cheaters. The combiner returns an invalid secret $K^* = f(\alpha \oplus \delta)$. Note that the cheaters always change their shares.
- Let
$$\Omega^*_{\delta,\alpha} = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta \oplus \delta) = K^*\}$$
where α^+_δ determines valid shares held by the cheaters. The set $\Omega^*_{\delta,\alpha}$ represents the view of the cheater after getting back K^* from the combiner. The set clearly includes also the vector α of all valid shares.
- The set
$$\Omega_{\delta,\alpha} = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta) = K\}$$
determines a collection of rows of $\mathcal{T}$ with the correct secret K and valid shares held by the cheaters.

Example 1. Let $n = 7$, f be a function on V_7 and $\delta = (0, 1, 0, 1, 1, 0, 0)$. Furthermore let $\alpha = (a_1, a_2, a_3, a_4, a_5, a_6, a_7)$. Then $\alpha \oplus \delta = (a_1, 1 \oplus a_2, a_3, 1 \oplus a_4, 1 \oplus a_5, a_6, a_7)$. Let $K = f(\alpha)$ and $K^* = f(\alpha \oplus \delta)$. Write $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$. Clearly $x^-_\delta \oplus \alpha^+_\delta = (x_1, a_2, x_3, a_4, a_5, x_6, x_7)$ and $x^-_\delta \oplus \alpha^+_\delta \oplus \delta = (x_1, 1 \oplus a_2, x_3, 1 \oplus a_4, 1 \oplus a_5, x_6, x_7)$. Therefore $\Omega^*_{\delta,\alpha} = \{(x_1, 0, x_3, 0, 0, x_6, x_7) \mid f(x_1, 1 \oplus a_2, x_3, 1 \oplus a_4, 1 \oplus a_5, x_6, x_7) = K^*\}$ and $\Omega_{\delta,\alpha} = \{(x_1, 0, x_3, 0, 0, x_6, x_7) \mid f(x_1, a_2, x_3, a_4, a_5, x_6, x_7) = K\}$. In this example, P_2, P_4 and P_5 are cheaters and they all submit invalid shares.

The function f is called the *defining function* as it determines the secret sharing. The nonzero vector $\delta = (\delta_1, \ldots, \delta_n)$ is called the *cheating vector*, α is called the *original vector*, and $\alpha \oplus \delta$ is called the *failure vector*. The value of

$\rho_{\delta,\alpha} = \#(\Omega^*_{\delta,\alpha} \cap \Omega_{\delta,\alpha})/\#\Omega^*_{\delta,\alpha}$ expresses the probability of successful cheating with respect to δ and α. As the original vector α is always in $\Omega^*_{\delta,\alpha} \cap \Omega_{\delta,\alpha}$, the probability of successful cheating always satisfies $\rho_{\delta,\alpha} > 0$. Clearly the number of cheaters is equal to $HW(\delta)$.

Theorem 1. *Given secret and its defining function f on V_n. Then for any cheating vector $\delta \in V_n$ with $0 < HW(\delta) < n$ and any vector $\alpha \in V_n$, there exists a vector $\gamma \in V_n$ such that $\rho_{\delta,\alpha} + \rho_{\delta,\gamma} = 1$ otherwise $\rho_{\delta,\alpha} = 1$.*

3.1 Strengthened Propagation

We introduce the concept of strengthened propagation that is useful further in the paper. Let $\tau = (t_1, \ldots, t_n)$ and $\delta = (\delta_1, \ldots, \delta_n)$ be two vectors in V_n. We write $\tau \preceq \delta$ to denote the property that if $t_j = 1$ then $\delta_j = 1$. In addition, we write $\tau \prec \delta$ to denote the property that $\tau \preceq \delta$ and $\tau \neq \delta$. For example, $(0,1,0,0,1) \preceq (1,1,0,0,1)$ or precisely $(0,1,0,0,1) \prec (1,1,0,0,1)$. Clearly if $\tau \preceq \delta$ then $\tau \oplus \delta \preceq \delta$.

A function f on V_n is said to satisfy the *strengthened propagation* with respect to a nonzero vector $\delta \in V_n$ if for any vector τ with $\tau \preceq \delta$, $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$ is balanced. If f satisfies the strengthened propagation with respect to every $\delta \in V_k$ with $0 < HW(\delta) \leq k$ then f is said to satisfy the *strengthened propagation of degree k*.

We now illustrate the strengthened propagation. Let f be a function on V_4 such that $f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4 \oplus x_1x_3$. Let $\delta = (1,1,0,0)$. Choose $\tau = (0,0,0,0)$. Then $f(x_\delta^- \oplus \tau) = f(0,0,x_3,x_4) = x_3x_4$ and $f(x_\delta^- \oplus \tau \oplus \delta) = f(1,1,x_3,x_4) = 1 \oplus x_3x_4 \oplus x_3$. Thus $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta) = 1 \oplus x_3$ is balanced. Next we choose $\tau = (0,1,0,0)$. Then $f(x_\delta^- \oplus \tau) = f(0,1,x_3,x_4) = x_3x_4$ and $f(x_\delta^- \oplus \tau \oplus \delta) = f(1,0,x_3,x_4) = x_3x_4 \oplus x_3$. Thus $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta) = x_3$ is balanced. We have proved that f satisfies the strengthened propagation with respect to $\delta = (1,1,0,0)$.

Proposition 1. *Let f be a function on V_n. If f satisfies the strengthened propagation of degree k then f satisfies the propagation criterion of degree k.*

It should be noticed that the converse of Proposition 1 does not hold when $k \geq 2$. For example, $f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4$ is a bent function on V_4 thus f satisfies the propagation criterion of degree 4. But f does not satisfy the strengthened propagation of degree 2. This can be seen from the following: $f(0,0,x_3,x_4) = x_3x_4$ and $f(1,1,x_3,x_4) = 1 \oplus x_3x_4$, and $f(0,0,x_3,x_4) \oplus f(1,1,x_3,x_4) = 1$. Therefore f does not satisfy the strengthened propagation with respect to $\delta = (1,1,0,0)$. However we can state as follows.

Proposition 2. *A function f on V_n satisfies the strengthened propagation of degree 1 if and only if f satisfies the propagation criterion of degree 1 (the SAC).*

Lemma 1. *If a function f on V_n satisfies the strengthened propagation of degree k then $f \oplus \psi$ also satisfies the strengthened propagation of degree k where ψ is any affine function on V_n.*

Lemma 2. *Let f_1 and f_2 be two functions on V_p and V_q respectively. Set $f(x) = f_1(y) \oplus f_2(z)$ where $x = (y, z)$, $y \in V_p$ and $z \in V_q$. Then (i) f is balanced if f_1 or f_2 is balanced, (ii) f satisfies the strengthened propagation of degree k if both f_1 and f_2 satisfy the strengthened propagation of degree k.*

3.2 k-Cheating Immune Secret Sharing Scheme

.

Clearly it is desirable that $\max\{\rho_{\delta,\alpha} | \delta \in V_n,\ \delta \neq 0,\ \alpha \in V_n\}$ is as small as possible. However if $\rho_{\delta,\alpha} < \frac{1}{2}$ for a nonzero vector δ and a vector $\alpha \in V_n$, from Theorem 1, there exists a vector $\gamma \in V_n$ such that $\rho_{\delta,\alpha} + \rho_{\delta,\gamma} = 1$ and then $\rho_{\delta,\gamma} > \frac{1}{2}$. This indicates that the case of $\min\{\rho_{\delta,\alpha} | \delta \in V_n,\ \delta \neq 0,\ \alpha \in V_n\} < \frac{1}{2}$ is not desirable. For this reason we introduce the concept of k-cheating immune secret sharing scheme.

Given secret sharing with its defining function f on V_n. Let k be an integer with $1 \leq k \leq n-1$. The secret sharing is said to be *k-cheating immune* if $\rho_{\delta,\alpha} = \frac{1}{2}$ holds for every $\delta \in V_n$ with $1 \leq HW(\delta) \leq k$ and every $\alpha \in V_n$. The integer k is called the *order of cheating immunity* of the secret sharing.

1-cheating immune secret sharing is also called cheating immune secret sharing in [21]. The following is a characterisation of 1-cheating immune secret sharing [21]:

Theorem 2. *Given secret sharing with its defining function f on V_n. Then this secret sharing is 1-cheating immune if and only if f is 1-resilient and satisfies the SAC.*

The following result provides a relationship between k-cheating immune secret sharing and $(k-1)$-cheating immune secret sharing:

Lemma 3. *Given secret sharing with its defining function f on V_n. Let this secret sharing be $(k-1)$-cheating immune. Then it is k-cheating immune if and only if the following two conditions are satisfied simultaneously: (i) f satisfies the strengthened propagation with respect to every vector in V_n with Hamming weight k, (ii) for any vector $\alpha \in V_n$ with $HW(\delta) = k$ and any vector $\tau \in V_n$ with $\tau \preceq \delta$, $f(x_\delta^- \oplus \tau)$ is balanced.*

Theorem 3. *Given secret sharing with its defining function f on V_n. Then the secret sharing is k-cheating immune if and only if f is k-resilient and satisfies the strengthened propagation of degree k.*

3.3 Constructions of k-cheating Immune Secret Sharing Scheme

Due to Theorem 3, to construct a k-cheating immune secret sharing, we need k-resilient functions satisfying the strengthened propagation of degree k. In particular we consider quadratic functions with such properties.

Proposition 3. *Let $f(x_1, \ldots, x_n)$ be a quadratic function on V_n. Let $\delta = (\delta_1, \ldots, \delta_n)$ be a nonzero vector in V_n. Set $J_\delta = \{j \mid \delta_j \neq 0,\ 1 \leq j \leq n\}$. For each integer i with $1 \leq i \leq n$ and $i \notin J_\delta$, define*
$D_\delta(i) = \{j \mid j \in J_\delta$ and $x_i x_j$ is a term of $f\}$. Then f satisfies the strengthened propagation with respect to δ if and only if there exists some i_0 with $1 \leq i_0 \leq n$ and $i_0 \notin J_\delta$ such that $\#D_\delta(i_0)$ is odd.

The following will be used in constructions of desirable functions.

Corollary 1. *Let $f(x_1, \ldots, x_n)$ be a quadratic function on V_n. Then*

(i) f satisfies the strengthened propagation with respect to $\delta = (0, \ldots, 0, 1, 0, \ldots, 0)$ where only the j-th coordinate is nonzero, if and only if there exists some s with $1 \leq s \leq n$ and $s \neq j$ such that $x_s x_j$ is a term of f,
(ii) f satisfies the strengthened propagation with respect to $\delta = (0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$ where only the j-th and i-th coordinates are nonzero, if and only if there exists some s with $1 \leq s \leq n$ and $s \neq j, i$ such that $x_s x_j$ is a term of f and $x_s x_i$ does not appear in f.

The following is a restatement of a lemma in [7]:

Lemma 4. *Let a quadratic function f on V_n do not have a nonzero constant term, in other words, $f(0, \ldots, 0) = 0$. Then f is balanced if and only if there exists a nonzero linear structure $\alpha \in V_n$ such that $f(\alpha) \neq 0$.*

The following Lemma can be found in [22]:

Lemma 5. *Let f_j be a t_j-resilient function on V_{n_j}, $j = 1, \ldots, s$. Then $f_1(y) \oplus \cdots \oplus f_s(z)$ is an $(s - 1 + t_1 + \cdots + t_s)$-resilient function on $V_{n_1 + \cdots + n_s}$, where f_i and f_j have disjoint variables if $i \neq j$.*

Lemma 6. *Define two functions as follows*

$$\chi_{2k+1}(x_1, \ldots, x_{2k+1}) = x_1 x_2 \oplus x_2 x_3 \oplus \cdots \oplus x_{2k} x_{2k+1} \oplus x_{2k+1} x_1 \quad (1)$$

$$\chi_{2k}(x_1, \ldots, x_{2k}) = x_1 \oplus x_1 x_2 \oplus x_2 x_3 \oplus \cdots \oplus x_{2k-1} x_{2k} \oplus x_{2k} x_1 \quad (2)$$

Then

(i) χ_{2k+1} is balanced, satisfies the strengthened propagation of degree k,
(ii) χ_{2k} is balanced, satisfies the strengthened propagation of degree $(k - 1)$.

Due to Theorem 3, the following constructions enable us to construct k-cheating immune secret sharing scheme.

Theorem 4. *Let k and s be positive integers with $s \geq k + 1$. Let $n_1, \ldots, n_s = 2k + 1$ or $2k + 2$, and $n = n_1 + \cdots + n_s$. Define a function on V_n such as $f(x) = \chi_{n_1}(y) \oplus \cdots \oplus \chi_{n_s}(z)$ where $x = (y, \ldots, z)$, $y \in V_{n_1}, \ldots, z \in V_{n_s}$, each χ_{n_j} has been defined in (1) or (2), and $\chi_{n_1}, \ldots, \chi_{n_s}$ have disjoint variables mutually. Then the secret sharing with the defining function f is k-cheating immune.*

Note that $n = n_1 + \cdots + n_s$, defined in Theorem 4, can be expressed as $n = (2k+1)r + (2k+2)q$ where $r \geq 0$ and $q \geq 0$ are integers. Since $2k+1$ and $2k+2$ are relatively prime, any integer can also be written as $(2k+1)r+(2k+2)q$ where r and q are integers. Furthermore it is easy to verify that any integer n with $n \geq (2k+1)^2$ can be expressed as $n = (2k+1)r + (2k+2)q$ where $r, q \geq 0$. Since $n \geq (2k+1)^2$, it is easy to verify that $s = r + q > k+1$ where s was mentioned in Theorem 4. Using Theorem 4, we can construct k-cheating immune secret sharing with n participants where $n \geq (2k+1)^2$.

4 Generalised Model of Cheating

As before secret sharing is considered to be a set of distribution rules combined into a single table $\mathcal{T}$ (see [18]) with binary entries. We also assume that we are dealing with (n, n) threshold scheme where any n participants are able to determine a single entry from $\mathcal{T}$ which indicates the secret.

Given a function f on V_n. We introduce the following notations:

- Let $\alpha \in V_n$ be the sequence of shares held by the group $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants and the secret $K = f(\alpha)$.
- The collection of cheaters is determined by the sequence $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$ where P_i is a cheater if and only if $\delta_i = 1$.
- At the pooling time, the cheaters submit their shares. This time it is assumed that cheaters may submit a mixture of valid and invalid shares. The honest participants always submit their valid shares. Define $\tau = (\tau_1, \ldots, \tau_n)$ such that

$$\tau_j = \begin{cases} 0, \text{ if } P_j \text{ is honest or } P_j \text{ is a cheater who submits a valid share} \\ 1, \text{ if } P_j \text{ a cheater who submits an invalid share} \end{cases}$$

  Clearly $\tau \preceq \delta$. We assume that there exists at least one cheater who submits invalid share, in other words, we only consider the case that τ is nonzero or $HW(\tau) > 0$.
  We consider the vector $\alpha \oplus \tau$. Due to the properties of operations x_δ^+ and x_δ^-,

$$\alpha \oplus \tau = \alpha_\delta^- \oplus \alpha_\delta^+ \oplus \tau$$

  The combiner obtains $\alpha \oplus \tau$ that splits into two parts: α_δ^- – the part submitted by honest participants and $\alpha_\delta^+ \oplus \tau$ the part submitted by cheaters. The combiner returns an invalid secret $K^* = f(\alpha \oplus \tau)$.
- Let

$$\Omega^*_{\delta,\tau,\alpha} = \{x_\delta^- \mid f(x_\delta^- \oplus \alpha_\delta^+ \oplus \tau) = K^*\}$$

  where α_δ^+ determines valid shares held by the cheaters. The set $\Omega^*_{\delta,\tau,\alpha}$ represents the view of the cheater after getting back K^* from the combiner. The set clearly includes also the vector α of all valid shares.

– The set

$$\Omega_{\delta,\tau,\alpha} = \{x_\delta^- \mid f(x_\delta^- \oplus \alpha_\delta^+) = K\}$$

determines a collection of rows of $\mathcal{T}$ with the correct secret K and valid shares held by the cheaters.

Example 2. Let $n = 7$, f be a function on V_7 and $\delta = (0,1,0,1,1,0,0)$ and $\tau = (0,0,0,1,1,0,0)$. Furthermore let $\alpha = (a_1, a_2, a_3, a_4, a_5, a_6, a_7)$. Then $\alpha \oplus \tau = (a_1, a_2, a_3, 1 \oplus a_4, 1 \oplus a_5, a_6, a_7)$. Let $K = f(\alpha)$ and $K^* = f(\alpha \oplus \tau)$. Write $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$. Clearly $x_\delta^- \oplus \alpha_\delta^+ = (x_1, a_2, x_3, a_4, a_5, x_6, x_7)$ and $x_\delta^- \oplus \alpha_\delta^+ \oplus \tau = (x_1,\ a_2,\ x_3,\ 1 \oplus a_4,\ 1 \oplus a_5,\ x_6, x_7)$. Therefore $\Omega^*_{\delta,\tau,\alpha} = \{(x_1, 0, x_3,\ 0, 0,\ x_6, x_7) \mid f(x_1, a_2, x_3, 1 \oplus a_4, 1 \oplus a_5, x_6, x_7) = K^*\}$ and $\Omega_{\delta,\tau,\alpha} = \{(x_1, 0, x_3,\ 0, 0,\ x_6, x_7) | f(x_1, a_2, x_3,\ a_4, a_5, x_6, x_7) = K\}$. In this example P_2, P_4 and P_5 are cheaters but P_2 submits valid share.

From Examples 1 and 2, we can find a main difference between initial and generalised models of cheating. Clearly P_2, P_4 and P_5 are cheaters in both examples. However P_2, P_4 and P_5 all submit invalid shares in Example 1 while P_4, P_5 submit invalid shares and P_2 submits valid share in Example 2.

The function f is called the *defining function* as it determines the secret sharing. The nonzero vector $\delta = (\delta_1, \ldots, \delta_n)$ is called the *cheating vector*, the nonzero vector $\tau \preceq \delta$ is called *active cheating vector*, α is called the *original vector*, and $\alpha \oplus \tau$ is called the *failure vector*. The value of $\rho_{\delta,\tau,\alpha} = \#(\Omega^*_{\delta,\tau,\alpha} \cap \Omega_{\delta,\tau,\alpha})/\#\Omega^*_{\delta,\tau\alpha}$ expresses the probability of successful cheating with respect to δ, τ and α. As the original vector α is always in $\Omega^*_{\delta,\tau,\alpha} \cap \Omega_{\delta,\tau,\alpha}$, the probability of successful cheating always satisfies $\rho_{\delta,\tau,\alpha} > 0$. Clearly the number of cheaters is equal to $HW(\delta)$ and the number of active cheaters is equal to $HW(\tau)$. In particular, if $\tau = \delta$, we regain the initial scheme. Therefore the initial model of cheating is a special case of the generalised model of cheating. From now, we consider secret sharing in the generalised model.

4.1 Strictly k-cheating Immune Secret Sharing Scheme

By using the same arguments as in the proof of Theorem 1, we can prove

Theorem 5. *Given secret sharing with its defining function f on V_n. Then for any cheating vector $\delta \in V_n$, any active cheating vector $\tau \preceq \delta$ with $1 \le HW(\tau) \le HW(\delta) < n$, and any vector $\alpha \in V_n$, there exists a vector $\gamma \in V_n$ such that $\rho_{\delta,\tau,\alpha} + \rho_{\delta,\tau,\gamma} = 1$ otherwise $\rho_{\delta,\tau,\alpha} = 1$.*

For the same reason mentioned in Section 3.2, we introduce the concept of k-cheating immune secret sharing scheme.

Given secret sharing with its defining function f on V_n. Let k be an integer with $1 \le k \le n-1$. The secret sharing is said to be *strictly k-cheating immune* if the probability of successful cheating satisfies $\rho_{\delta,\tau,\alpha} = \frac{1}{2}$ for every $\delta \in V_n$ and any $\tau \preceq \delta$ with $1 \le HW(\tau) \le HW(\delta) \le k$ and every $\alpha \in V_n$. The integer k is called the *order of strict cheating immunity* of the secret sharing.

Lemma 7. *Given secret sharing with its defining function f on V_n. Then the secret sharing is strictly k-cheating immune if and only if for any integer t with $0 \leq t \leq k-1$, any subset $\{j_1, \ldots, j_t\}$ of $\{1, \ldots, n\}$ and any $a_1, \ldots, a_t \in GF(2)$, $f(x_1, \ldots, x_n)|_{x_{j_1}=a_1, \ldots, x_{j_t}=a_t}$, as a function on V_{n-t} with the variables x_{i_1}, ..., $x_{i_{n-t}}$, where $\{i_1, \ldots, i_{n-t}\} \cup \{j_1, \ldots, j_t\} = \{1, \ldots, n\}$, is $(k-t)$-resilient and satisfies the strengthened propagation of degree $(k-t)$.*

Theorem 6. *Given secret sharing with its defining function f on V_n. Then the secret sharing is strictly k-cheating immune if and only if the following conditions are satisfied simultaneously: (i) f is k-resilient, (ii) for any integer t with $0 \leq t \leq k-1$, any subset $\{j_1, \ldots, j_t\}$ of $\{1, \ldots, n\}$ and any $a_1, \ldots, a_t \in GF(2)$, $f(x_1, \ldots, x_n)|_{x_{j_1}=a_1, \ldots, x_{j_t}=a_t}$, as a function on V_{n-t} with the variables $x_{i_1}, \ldots, x_{i_{n-t}}$, where $\{i_1, \ldots, i_{n-t}\} \cup \{j_1, \ldots, j_t\} = \{1, \ldots, n\}$, satisfies the strengthened propagation of degree $(k-t)$.*

We indicate that the condition (ii) in Theorem 6 is more restrictive than the strengthened propagation of degree k. For example, due to Lemma 6, χ_{13} satisfies the strengthened propagation of degree 6. However χ_{13} does not satisfy the condition (ii) in Theorem 6 with $k = 3$ and $t = 2$. This can be seen from the following: $\chi_{13}(0, x_2, 0, x_4, \ldots x_{13}) = x_4x_5 \oplus x_5x_6 \oplus \cdots \oplus x_{12}x_{13}$, as a function on V_{11} with the variables $x_2, x_4, x_5, \ldots, x_{13}$, does not contain x_2. From (i) of Corollary 1, $\chi_{13}(0, x_2, 0, x_4, \ldots x_{13})$, as a function on V_{11} with the variables $x_2, x_4, x_5, \ldots, x_{13}$, does not satisfy the strengthened propagation of degree 1. Therefore χ_{13} does not satisfy the condition (ii) in Theorem 6 with $k = 3$ and $t = 2$.

4.2 Construction of Strictly k-cheating Immune Secret Sharing Scheme

If f in Theorem 6 is quadratic, Theorem 6 can be simplified as follows:

Theorem 7. *Given secret sharing with its defining function f on V_n. Let f be quadratic. Then the secret sharing is strictly k-cheating immune if and only if the following two conditions are satisfied simultaneously: (i) f is k-resilient, (ii) for any integer t with $0 \leq t \leq k-1$ and any subset $\{j_1, \ldots, j_t\}$ of $\{1, \ldots, n\}$, $f(x_1, \ldots, x_n)|_{x_{j_1}=0, \ldots, x_{j_t}=0}$, as a function on V_{n-t} with the variables x_{i_1}, ..., $x_{i_{n-t}}$, where $\{i_1, \ldots, i_{n-t}\} \cup \{j_1, \ldots, j_t\} = \{1, \ldots, n\}$, satisfies the strengthened propagation of degree $(k-t)$.*

Construction of Strictly 2-cheating Immune Secret Sharing Scheme

Let $s \geq 3$ be an integer, $n_1, \ldots, n_s = 5, 6$ and $n = n_1 + \cdots + n_s$. Define a function on V_n such as $f(x) = \chi_{n_1}(y) \oplus \cdots \oplus \chi_{n_s}(z)$ where $x = (y, \ldots, z)$, each χ_{n_j} has been defined in (1) or (2), and χ_{n_i}, χ_{n_j} have disjoint variables if $i \neq j$. Due to Theorem 4, the secret sharing with the defining function f is $(s-1)$-cheating immune, where $s-1 \geq 2$, and thus from Theorem 3, f is $(s-1)$-resilient and satisfies the strengthened propagation of degree $s-1$. Therefore f satisfies the condition (i) of Theorem 7 with $k = 2$.

Next we verify that f satisfies the condition (ii) of Theorem 7 with $k = 2$. Let $t = 0$ in the condition (ii) of Theorem 7 with $k = 2$. Due to Lemma 6 and Lemma 2, we know that f satisfies the strengthened propagation of degree 2. Let $t = 1$ in the condition (ii) of Theorem 7 with $k = 2$. Fix any j_0 with $1 \leq j_0 \leq n$. Note that each $1 \leq i \leq n$, x_i appears in two quadratic terms in f thus for any i with $1 \leq i \leq n$ and $i \neq j_0$, x_i appears in at least one quadratic term in $f(x)|_{x_{j_0}=0}$. From (i) of Corollary 1, we know that $f(x)|_{x_{j_0}=0}$ satisfies the strengthened propagation of degree 1.

We have proved that f satisfies the condition (ii) of Theorem 7 with $k = 2$. Therefore if we place f as the defining function of a secret sharing and then by Theorem 7 we conclude that this secret sharing is 2-cheating immune.

Note that 5 and 6 are relatively prime thus any integer can also be written as $5p + 6q$ where p and q are integers. Furthermore it is easy to verify that any integer $n \geq 20$ can be expressed as $n = 5p + 6q$ where $p \geq 0$ and $q \geq 0$ are integers. As for $n \leq 19$, n can be expressed as $n = 5p + 6q$ where $p \geq 0$ and $q \geq 0$ are integers when $n = 5, 6, 11, 12, 15, 16, 17$ and 18.

Therefore we can construct 2-cheating immune secret sharing with n participants where $n \geq 20$ or $n = 5, 6, 11, 12, 15, 16, 17$ and 18.

Construction of Strictly 3-cheating Immune Secret Sharing Scheme

Set

$$\begin{aligned}
&h_9(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \\
&= x_1 \oplus \chi_9(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \\
&\oplus \chi_3(x_1, x_4, x_7) \oplus \chi_3(x_2, x_5, x_8) \oplus \chi_3(x_3, x_6, x_9)
\end{aligned}$$

where each χ_j has been defined in (1) or (2).

Since $(1,1,1,1,1,1,1,1,1) \in V_9$ is a nonzero linear structure of h_9 and $h_9(1,1,1,1,1,1,1,1,1) \neq 0$, from Lemma 4, we know that h_9 is balanced.

Set

$$\begin{aligned}
&h_{10}(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) \\
&= x_1 \oplus \chi_{10}(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) \\
&\oplus \chi_{10}(x_1, x_4, x_7, x_{10}, x_3, x_6, x_9, x_2, x_5, x_8)
\end{aligned}$$

Since $(1,1,1,1,1,1,1,1,1,1) \in V_{10}$ is a nonzero linear structure of h_{10} and $h_{10}(1,1,1,1,1,1,1,1,1,1) \neq 0$, from Lemma 4, we know that h_{10} is balanced.

Let $s \geq 4$ be an integer, $n_1, \ldots, n_s = 9, 10$ and $n = n_1 + \cdots + n_s$. Define a function on V_n such as $f(x) = h_{n_1}(y) \oplus \cdots \oplus h_{n_s}(z)$ where h_{n_i} and h_{n_j} have disjoint variables if $i \neq j$.

Since both h_9 and h_{10} are balanced, from Lemma 5, f is $(s-1)$-resilient. Therefore f satisfies the condition (i) of Theorem 7 with $k = 3$.

Next we verify that f satisfies the condition (ii) of Theorem 7 with $k = 3$. Let $t = 0$ in the condition (ii) of Theorem 7 with $k = 3$. Using a straightforward verification, we know that h_9 (h_{10}) satisfies the condition mentioned in

Proposition 3 for every $\delta \in V_9$ ($\delta \in V_{10}$) with $HW(\delta) = 1, 2, 3$. Thus both h_9 and h_{10} satisfy the strengthened propagation of degree 3. Due to Lemma 2, f satisfies the strengthened propagation of degree 3. Let $t = 1$ in the condition (ii) of Theorem 7 with $k = 3$. Fix any j_0 with $1 \leq j_0 \leq n$, it is easy to verify that $f(x)|_{x_{j_0}=0}$ satisfies the condition mentioned in (ii) of Corollary 1, and thus $f(x)|_{x_{j_0}=0}$ satisfies the strengthened propagation of degree 2. Let $t = 2$ in the condition (ii) of Theorem 7 with $k = 3$. Fix any j_0 and i_0 with $1 \leq j_0 < i_0 \leq n$. Note that each $1 \leq i \leq n$, x_i appears in four quadratic terms in f thus for any i with $1 \leq i \leq n$ and $i \neq j_0, i_0$, x_i appears in at least two quadratic terms in $f(x)|_{x_{j_0}=0, x_{i_0}=0}$. From (i) of Corollary 1, we know that $f(x)|_{x_{j_0}=0, x_{i_0}=0}$ satisfies the strengthened propagation of degree 1.

We have proved that f satisfies Theorem 7 with $k = 3$. Therefore if we place f as the defining function of a secret sharing and then by Theorem 7, we conclude that this secret sharing is 3-cheating immune.

Note that 9 and 10 are relatively prime thus any integer can also be written as $9p + 10q$ where p and q are integers. Furthermore it is easy to verify that any integer $n \geq 72$ can be expressed as $n = 9p + 10q$ where $p \geq 0$ and $q \geq 0$ are integers. As for $n \leq 71$, n can also be expressed as $n = 9p + 10q$ where $p \geq 0$ and $q \geq 0$ are integers when $n = 9, 10, 18, 19, 20, 27, 28, 29, 30, 36, 37, 38, 39, 40, 45, 46, 47, 48, 49, 50, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70$. Therefore we can construct 3-cheating immune secret sharing with n participants where $n \geq 72$ or $n = 9, 10, 18, 19, 20, 27, 28, 29, 30, 36, 37, 38, 39, 40, 45, 46, 47, 48, 49, 50, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70$.

Based on Theorem 7 and Proposition 3, we can continue to construct strictly k-cheating immune secret sharing scheme, $k = 4, 5, \ldots$. Due to the page limitation, this will be completed in the full paper.

5 Conclusions and Remarks

We have considered secret sharing and its resistance against cheating by a group of k dishonest participants. We have proved that the probability of successful cheating is always higher than $\frac{1}{2}$ if the participants hold binary shares. The secret scheme is said to be k-cheating immune if the probability of successful cheating is $\frac{1}{2}$ for any group of k or less participants. We have characterised k-cheating immune secret sharing scheme by examining its defining function. This characterisation enables us to construct k-cheating immune secret sharing scheme. Being more precise, we have studied two cases. In the first case, the group of cheaters always submit invalid shares. While in the second case, the group is more flexible as they collectively decide which of their shares should be modified and which should be submitted in their original form.

Acknowledgements

The first author was supported by the Large ARC Grant A00103078. The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. M. Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes and Cryptography*, 5(3):183–187, 1995.
2. M. Carpentieri, A. De Santis, and U. Vaccaro. Size of shares and probability of cheating in threshold schemes. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93*, LNCS No 765, pages 118–125. Springer-Verlag, 1993.
3. C. Ding, D. Pei and A Salomaa. Chinese remainder theorem: applications in computing, coding and cryptography. World Scientific, Singapore, 1996
4. P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pages 427–437. IEEE, 1987.
5. F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland, Amsterdam, 1977.
6. K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*, LNCS No 658, pages 92–98. Springer-Verlag, 1993.
7. K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, LNCS No 740, pages 566–574. Springer-Verlag, 1993.
8. T.P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO'91*, LNCS No 576, pages 129–140. Springer-Verlag, 1992.
9. J. Pieprzyk and X. M. Zhang. Cheating prevention in secret sharing over $GF(p^t)$. to appear in Indocrypt 2001.
10. B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, LNCS No 437, pages 155–165. Springer-Verlag, 1991.
11. 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, 1989.
12. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (A)*, 20:300–305, 1976.
13. B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In M. Wiener, editor, *Advances in Cryptology - CRYPTO'99*, LNCS No 1666, pages 148–164. Springer-Verlag , 1999.
14. J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93*, LNCS No 765, pages 181–199. Springer-Verlag, 1994.
15. J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.
16. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30 No. 5:776–779, 1984.
17. M. Stadler. Publicly verifiable secret sharing. In U. Maurer, editor, *Advances in Cryptology - EUROCRYPT'96*, LNCS No 1070, pages 190–199. Springer-Verlag, 1996.
18. D.R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.
19. A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, LNCS No 219, pages 523–534. Springer-Verlag, 1986.

20. Martin Tompa and Heather Woll. How to share a secret with cheaters. In A.M. Odlyzko, editor, *Advances in Cryptology - CRYPTO'86*, LNCS No 263, pages 261–265. Springer-Verlag, 1987.
21. X. M. Zhang and J. Pieprzyk, Cheating immune secret sharing. to appear in *The Third International Conference on Information and Communication Security (ICICS)* 2001.
22. X. M. Zhang and Y. Zheng. Cryptographically resilient functions. *IEEE Transactions on Information Theory*, 43(5):1740–1747, 1997.

Appendix: Proofs of Propositions, Lemmas and Theorems

The Proof of Theorem 1 Let $f(\alpha) = K$ and $f(\alpha \oplus \delta) = K^*$. Set $\Omega^*_{\delta,\alpha} = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta \oplus \delta) = K^*\}$ and $\Omega_{\delta,\alpha} = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta) = K\}$.

We partition $\Omega^*_{\delta,\alpha}$ into two parts: $\Omega^*_{\delta,\alpha} = \Omega^*_1 \cup \Omega^*_2$ where

$$\Omega^*_1 = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta \oplus \delta) = K^*,\ f(x^-_\delta \oplus \alpha^+_\delta) = K\}$$

and

$$\Omega^*_2 = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta \oplus \delta) = K^*,\ f(x^-_\delta \oplus \alpha^+_\delta) = K \oplus 1\}$$

Note that $\Omega^*_{\delta,\alpha} \cap \Omega_{\delta,\alpha} = \Omega^*_1$. Therefore

$$\rho_{\delta,\alpha} = \#(\Omega^*_{\delta,\alpha} \cap \Omega_{\delta,\alpha})/\#\Omega^*_{\delta,\alpha} = \#\Omega^*_1/\#\Omega^*_{\delta,\alpha} \tag{3}$$

There exist two cases to be considered: $\Omega^*_2 \neq \emptyset$, where $\emptyset$ denotes the empty set, and $\Omega^*_2 = \emptyset$.

Case 1: $\Omega^*_2 \neq \emptyset$. Then there exists a vector $\beta \in \Omega^*_2$. Thus

$$f(\beta^-_\delta \oplus \alpha^+_\delta \oplus \delta) = K^*,\ f(\beta^-_\delta \oplus \alpha^+_\delta) = K \oplus 1 \tag{4}$$

Set $\gamma = \beta^-_\delta \oplus \alpha^+_\delta$. Therefore (4) can be rewritten as $f(\gamma \oplus \delta) = K^*,\ f(\gamma) = K \oplus 1$. Clearly $\gamma^+_\delta = \alpha^+_\delta$ and $\gamma^-_\delta = \beta^-_\delta$.

Next we choose γ as the original vector. Therefore $\Omega^*_{\delta,\gamma} = \{x^-_\delta \mid f(x^-_\delta \oplus \gamma^+_\delta \oplus \delta) = K^*\}$ and $\Omega_{\delta,\gamma} = \{x^-_\delta \mid f(x^-_\delta \oplus \gamma^+_\delta) = K \oplus 1\}$. Since $\gamma^+_\delta = \alpha^+_\delta$, we have $\Omega^*_{\delta,\gamma} = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta \oplus \delta) = K^*\}$ and $\Omega_{\delta,\gamma} = \{x^-_\delta \mid f(x^-_\delta \oplus \alpha^+_\delta) = K \oplus 1\}$. Clearly $\Omega^*_{\delta,\gamma} \cap \Omega_{\delta,\gamma} = \Omega^*_2$. Note that $\Omega^*_{\delta,\gamma}$ is identified with $\Omega^*_{\delta,\alpha}$. Therefore

$$\rho_{\delta,\gamma} = \#(\Omega^*_{\delta,\gamma} \cap \Omega_{\delta,\gamma})/\#\Omega^*_{\delta,\gamma} = \#\Omega^*_2/\#\Omega^*_{\delta,\gamma} = \#\Omega^*_2/\#\Omega^*_{\delta,\alpha} \tag{5}$$

Combining (3) and (5), and noticing $\#\Omega^*_{\delta,\alpha} = \#\Omega^*_1 + \#\Omega^*_2$, we have $\rho_{\delta,\alpha} + \rho_{\delta,\gamma} = 1$.

Case 2: $\Omega^*_2 = \emptyset$. Then $\Omega^*_{\delta,\alpha} = \Omega^*_1$. From (3), we have $\rho_{\delta,\alpha} = 1$. We have proved the theorem.

The Proof of Proposition 1 Fix any $\delta \in V_n$ with $0 < HW(\delta) \leq k$. Let $\tau \preceq \delta$. Since f satisfies the strengthened propagation of degree k, $f(x^-_\delta \oplus \tau) \oplus f(x^-_\delta \oplus$

$\tau \oplus \delta$) is balanced. Since τ is an arbitrary vector with $\tau \preceq \delta$, $x_\delta^- \oplus \tau$ runs through every vector in V_n while τ and x_δ^- are as changed as possible. Therefore $f(x) \oplus f(x \oplus \delta)$ is balanced, i.e., f satisfies the propagation criterion with respect to δ. Since δ is an arbitrary vector in V_n with $0 < HW(\delta) \leq k$, we have proved that f satisfies the propagation criterion of degree k.

The Proof of Proposition 2 The necessity is true due to Proposition 1. We now prove the sufficiency. Assume that f satisfies the SAC. Fix j with $1 \leq j \leq n$ and set

$$\begin{aligned} &g(x_1, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_n) \\ &= f(x_1, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_n) \oplus f(x_1, \ldots, x_{j-1}, x_j \oplus 1, x_{j+1}, \ldots, x_n) \end{aligned}$$

Obviously $g(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n) = g(x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n)$. Since f satisfies the SAC, $g(x_1, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_n)$ is balanced. Thus both $g(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$ and $g(x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n)$ are balanced. This proves that f satisfies the strengthened propagation of degree 1.

The Proof of Lemma 1 In fact, since ψ is affine, $\psi(x_\delta^- \oplus \tau) \oplus \psi(x_\delta^- \oplus \tau \oplus \delta)$ is constant, where δ is any nonzero vector in V_n and τ is any vector in V_n with $\tau \preceq \delta$. Thus the lemma holds.

The Proof of Lemma 2 The part (i) can be found from Lemma 12 of [15]. By using (i) of the Lemma, we can verify the part (ii) of the lemma.

The Proof of Lemma 3 Let $\delta \in V_n$ be the cheating vector with $HW(\delta) = k$. Let τ be a vector in V_n with $\tau \preceq \delta$. Clearly $\delta_\delta^+ = \delta$, $\tau_\delta^+ = \tau$ and $\tau \oplus \delta_\delta^+ = \tau \oplus \delta$.

Write $x = (x_1, \ldots, x_n)$. Set

$$\begin{aligned} R_0 &= \{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 0, f(x_\delta^- \oplus \tau \oplus \delta) = 0\} \\ R_1 &= \{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 0, f(x_\delta^- \oplus \tau \oplus \delta) = 1\} \\ R_2 &= \{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 1, f(x_\delta^- \oplus \tau \oplus \delta) = 0\} \\ R_3 &= \{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 1, f(x_\delta^- \oplus \tau \oplus \delta) = 1\} \end{aligned} \tag{6}$$

Write $\#R_i = r_i$, $i = 0, 1, 2, 3$. Since $HW(\delta) = k$, it is easy to see that $r_1 + r_2 + r_3 + r_4 = 2^{n-k}$. By definition, it is easy to verify that

$$\rho_{\tau,\delta} = \begin{cases} \frac{r_0}{r_0+r_2} \text{ if } f(\tau \oplus \delta) = 0, f(\tau) = 0 \\ \frac{r_2}{r_0+r_2} \text{ if } f(\tau \oplus \delta) = 0, f(\tau) = 1 \\ \frac{r_1}{r_1+r_3} \text{ if } f(\tau \oplus \delta) = 1, f(\tau) = 0 \\ \frac{r_3}{r_1+r_3} \text{ if } f(\tau \oplus \delta) = 1, f(\tau) = 1 \end{cases} \tag{7}$$

Similarly,

$$\rho_{\tau\oplus\delta,\delta} = \begin{cases} \frac{r_0}{r_0+r_1} \text{ if } f(\tau) = 0, f(\tau \oplus \delta) = 0 \\ \frac{r_1}{r_0+r_1} \text{ if } f(\tau) = 0, f(\tau \oplus \delta) = 1 \\ \frac{r_2}{r_2+r_3} \text{ if } f(\tau) = 1, f(\tau \oplus \delta) = 0 \\ \frac{r_3}{r_2+r_3} \text{ if } f(\tau) = 1, f(\tau \oplus \delta) = 1 \end{cases} \tag{8}$$

Assume that the secret sharing is k-cheating immune. Let δ be the cheating vector and τ be the original vector. Since the scheme is k-cheating immune and $HW(\delta) = k$, we have $\rho_{\tau,\delta} = \frac{1}{2}$. Due to (7), $\frac{r_0}{r_0+r_2} = \frac{r_2}{r_0+r_2}$ and $\frac{r_1}{r_1+r_3} = \frac{r_3}{r_1+r_3}$. It follows that $r_0 = r_2$ and $r_1 = r_3$. On the other hand, since $\rho_{\tau\oplus\delta,\delta} = \frac{1}{2}$, due to (8), $\frac{r_0}{r_0+r_1} = \frac{r_1}{r_0+r_1}$ and $\frac{r_2}{r_2+r_3} = \frac{r_3}{r_2+r_3}$. It follows that $r_0 = r_1$ and $r_2 = r_3$. Therefore we have proved that $r_0 = r_1 = r_2 = r_3$.

Note that $\#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta) = 0\} = r_0 + r_3$ and $\#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta) = 1\} = r_1 + r_2$. Thus

$$\begin{aligned} &\#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta) = 0\} \\ &= \#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta) = 1\} \end{aligned} \tag{9}$$

From (9), $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$ is balanced. Since τ is an arbitrary vector in V_n with $\tau \preceq \delta$, f satisfies the strengthened propagation with respect to δ, where δ is an arbitrary vector in V_n with $HW(\delta) = k$. This proves that the condition (i) is satisfied.

We now consider the condition (ii). Note that $\#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 0\} = r_0 + r_1$ and $\#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 1\} = r_2 + r_3$. Since $r_0 = r_1 = r_2 = r_3$, we have $\#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 0\} = \#\{x_\delta^- \mid f(x_\delta^- \oplus \tau) = 1\}$. This proves that $f(x_\delta^- \oplus \tau)$ is balanced, where δ is an arbitrary vector in V_n and τ is any vector in V_n with $\tau \preceq \delta$. Therefore the condition (ii) is satisfied.

Conversely assume that f satisfies (i) and (ii).

From the condition (i), for any vector $\delta \in V_n$ with $HW(\delta) = k$ and any vector $\tau \in V_n$ with $\tau \preceq \delta$, $f(x_\delta^- \oplus \tau)$ is balanced, thus we have $r_0 + r_3 = r_1 + r_2$.

From the condition (ii), $f(x_\delta^- \oplus \tau)$ is balanced, thus $r_0 + r_1 = r_2 + r_3$. By the same reasoning, $f(x_\delta^- \oplus \tau \oplus \delta)$ is also balanced, thus $r_0 + r_2 = r_1 + r_3$.

Therefore we conclude that $r_0 = r_1 = r_2 = r_3$. Due to (7), it follows that

$$\rho_{\tau,\delta} = \frac{1}{2} \tag{10}$$

Next we prove that $\rho_{\delta,\alpha} = \frac{1}{2}$ for every $\alpha \in V_n$. Clearly $\alpha_\delta^+ \preceq \delta$, $\alpha_\delta^+ \oplus \delta \preceq \delta$. Replacing τ and $\tau \oplus \delta$ by α_δ^+ and $\alpha_\delta^+ \oplus \delta$ in (6) respectively, and using the same arguments for (10), we can prove that $\rho_{\delta,\alpha} = \frac{1}{2}$.

The Proof of Theorem 3 We prove the theorem by induction on k. Due to Theorem 2, the theorem is true when $k = 1$. Assume that the theorem is true when $1 \le k \le s-1$. Consider the case of $k = s$.

We now prove the necessity. Assume that the secret sharing is s-cheating immune. Then it is also $(s-1)$-cheating immune. Due to the assumption that the theorem is true when $1 \le k \le s-1$, f is $(s-1)$-resilient and satisfies the strengthened propagation of degree $(s-1)$. Since the secret sharing is s-cheating immune, from the condition (i) of Lemma 3, f satisfies the strengthened propagation with respect to any vector in V_n with Hamming weight s. Therefore f satisfies the strengthened propagation of degree s. On the other hand, due to the condition (ii) of Lemma 3, for any vector $\alpha \in V_n$ with $HW(\delta) = k$ and any

vector $\tau \in V_n$ with $\tau \preceq \delta$, $f(x_\delta^- \oplus \tau)$ is balanced. Combing this property and the fact that f is $(s-1)$-resilient, we conclude that f is s-resilient.

Conversely assume that f is s-resilient and satisfies the strengthened propagation of degree s. Due to the assumption that the theorem is true when $1 \leq k \leq s-1$, the secret sharing is $(s-1)$-cheating immune. Since f satisfies the conditions (i) and (ii), due to Lemma 3, the secret sharing is s-cheating immune. We have proved the theorem when $k = s$. The proof is completed.

The Proof of Proposition 3 We generalise the notations J_δ and $D_\delta(i)$. For any $\tau = (\tau_1, \ldots, \tau_n) \preceq \delta$, set $J_\tau = \{j \mid \tau_j \neq 0,\ 1 \leq j \leq n\}$. For any i with $1 \leq i \leq n$ and $i \notin J_\delta$, define $D_\tau(i) = \{j \mid j \in J_\tau \text{ and } x_i x_j \text{ is a term of } f\}$.

It is easy to see that $x_j x_i$ is a quadratic term of $f(x_\delta^- \oplus \tau)$ if and only if $x_j x_i$ is a quadratic term of f with $j, i \notin J_\delta$. Similarly $x_j x_i$ is a quadratic term of $f(x_\delta^- \oplus \tau \oplus \delta)$ if and only if $x_j x_i$ is a quadratic term of f with $j, i \notin J_\delta$. Therefore $f(x_\delta^- \oplus \tau)$ and $f(x_\delta^- \oplus \tau \oplus \delta)$ have the same quadratic terms. Thus $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$ does not contain any quadratic term and thus we only need to consider affine terms in $f(x_\delta^- \oplus \tau)$ and $f(x_\delta^- \oplus \tau \oplus \delta)$.

First we assume that there exists some i_0 with $1 \leq i_0 \leq n$ and $i_0 \notin J_\delta$ such that $\#D_\delta(i_0)$ is odd. Since $i_0 \notin J_\delta$, we know that $i_0 \notin J_\tau$ and $i_0 \notin J_{\tau \oplus \delta}$. Note that x_{i_0} appears linearly in $f(x_\delta^- \oplus \tau)$ if and only if $\#D_\tau(i_0)$ is odd. Similarly x_{i_0} appears linearly in $f(x_\delta^- \oplus \tau \oplus \delta)$ if and only if $\#D_{\tau \oplus \delta}(i_0)$ is odd. Note that for $i_0 \notin J_\delta$, we have $\#D_\tau(i_0) + \#D_{\tau \oplus \delta}(i_0) = \#D_\delta(i_0)$. Since $\#D_\delta(i_0)$ is odd, x_{i_0} must appear linearly in $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$. This proves that $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$ is non-constant affine and then balanced. We have proved the sufficiency.

Conversely assume that f satisfies the strengthened propagation with respect to δ. We now prove the necessity by contradiction. Assume that $\#D_\delta(i)$ is even for each $i \notin J_\delta$. From the proof of the sufficiency, for each $i \notin J_\delta$, x_j cannot appear in $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$. This implies that $f(x_\delta^- \oplus \tau) \oplus f(x_\delta^- \oplus \tau \oplus \delta)$ is constant and then unbalanced. This contradicts the assumption that assume that f satisfies the strengthened propagation with respect to δ. The contradiction proves the necessity.

The Proof of Lemma 6 (i) Since $(1, \ldots, 1) \in V_{2k+1}$ is a nonzero linear structure of χ_{2k+1} and $\chi_{2k+1}(1, \ldots, 1) \neq 0$, from Lemma 4, we know that χ_{2k+1} is balanced. Let δ be a nonzero vector in V_{2k+1} with $0 < HW(\delta) \leq k$. Since $1 \leq \#J_\delta = HW(\delta) \leq k$, where J_δ has been defined in Proposition 3, there must exist an integer s with $1 \leq s \leq 2k+1$ such that $s \in J_\delta$ and $s+1, s+2 \notin J_\delta$ (if $s = 2k$ then $s+2 = 2k+2$ is regarded as 1, and if $s = 2k+1$ then $s+1 = 2k+2$ and $s+2 = 2k+3$ are regarded as 1 and 2 respectively). Clearly $\#D_\delta(s+1) = 1$. From Proposition 3, we know that χ_{2k+1} satisfies the strengthened propagation respect to δ. Since δ is an arbitrary nonzero vector in V_{2k+1} with $0 < HW(\delta) \leq k$. We have proved the part (i) of the lemma.

(ii) Since $(1,\ldots,1) \in V_{2k}$ is a nonzero linear structure of χ_{2k} and $\chi_{2k}(1,\ldots,1) \neq 0$, from Lemma 4, we know that χ_{2k} is balanced. Using the same arguments in the proof of the part (i), we complete the proof of the part (ii).

The Proof of Theorem 4 Due to Lemma 6, each χ_{n_j} is balanced. From Lemma 2, f is $(s-1)$-resilient, where $s-1 \geq k$. Using Lemma 6 and Lemma 2, we know that f satisfies the strengthened propagation of degree k. Using Theorem 3, we have proved that the secret sharing is k-immune.

The Proof of Lemma 7 Assume that the secret sharing is strictly k-cheating immune. Let g be a function on V_{n-t} given by $g = f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$. Since f is the defining function on V_n of a strictly k-cheating immune secret sharing in generalised model of cheating, we know that g is the defining function on V_{n-t} of a $(k-t)$-cheating immune secret sharing in initial model of cheating. Applying Theorem 3 to g, we conclude that g is $(k-t)$-resilient and satisfies the strengthened propagation of degree $(k-t)$. We have proved the necessity. Comparing generalised model of cheating with initial model of cheating, we can invert the above reasoning and then prove the sufficiency.

The Proof of Theorem 6 Comparing Theorem 6 with Lemma 7, due to a definition of k-resilient functions mentioned in Section 2, it is easy to see the equivalence between Theorem 6 and Lemma 7.

The Proof of Theorem 7 Due to Theorem 6, we only need to prove the following lemma called Lemma (C): "let f be a quadratic function on V_n, t be an integer with $0 \leq t < n$ and $\{j_1,\ldots,j_t\}$ be a subset of $\{1,\ldots,n\}$. Then for any $a_1,\ldots,a_t \in GF(2)$, $f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$, as a function on V_{n-t} with the variables $x_{i_1},\ldots,x_{i_{n-t}}$, where $\{i_1,\ldots,i_{n-t}\} \cup \{j_1,\ldots,j_t\} = \{1,\ldots,n\}$, satisfies the strengthened propagation of degree s if and only if $f(x_1,\ldots,x_n)|_{x_{j_1}=0,\ldots,x_{j_t}=0}$ satisfies the strengthened propagation of degree s".

Since the necessity is obvious, we only need to prove the sufficiency. It is easy to verify that x_jx_i is a quadratic term of $f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$ if and only if x_jx_i is a quadratic term of f with $j,i \notin \{j_1,\ldots,j_t\}$. Similarly x_jx_i is a quadratic term of $f(x_1,\ldots,x_n)|_{x_{j_1}=0,\ldots,x_{j_t}=0}$ if and only if x_jx_i is a quadratic term of f with $j,i \notin \{j_1,\ldots,j_t\}$. Then $f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$ and $f(x_1,\ldots,x_n)|_{x_{j_1}=0,\ldots,x_{j_t}=0}$ have the same quadratic terms. Therefore $f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$ can be expressed as

$$f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t} = f(x_1,\ldots,x_n)|_{x_{j_1}=0,\ldots,x_{j_t}=0} \oplus \psi(x_{i_1},\ldots,x_{i_{n-t}})$$

where ψ is an affine function on V_{n-t}.

Assume that $f(x_1,\ldots,x_n)|_{x_{j_1}=0,\ldots,x_{j_t}=0}$, as a function on V_{n-t} with the variables $x_{i_1},\ldots,x_{i_{n-t}}$, where $\{i_1,\ldots,i_{n-t}\} \cup \{j_1,\ldots,j_t\} = \{1,\ldots,n\}$, satisfies the strengthened propagation of degree s. By using Lemma 1, we conclude that $f(x_1,\ldots,x_n)|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$, satisfies the strengthened propagation of degree s. We have proved Lemma (C) and thus the theorem is true.