Properties and Constraints of Cheating-Immune Secret Sharing Schemes*

Paolo D'Arco[1]†, Wataru Kishimoto[2]‡, and Douglas R. Stinson[3]

[1] Dipartimento di Informatica ed Applicazioni
Università degli Studi di Salerno, Italy
email: paodar@dia.unisa.it

[2] Department of Information & Image Science
Chiba University, Chiba 263-8522, Japan
email: wkishi@faculty.chiba-u.jp

[3] School of Computer Science
University of Waterloo, N2L 3G1, Waterloo Ontario, Canada
e-mail: dstinson@cacr.math.uwaterloo.ca

December 3, 2003

Abstract

A secret sharing scheme is a cryptographic protocol by means of which a dealer shares a secret among a set of participants in such a way that it can be subsequently reconstructed by certain qualified subsets. The setting we consider is the following: in a first phase, the dealer gives in a secure way a piece of information, called a *share*, to each participant. Then, participants belonging to a qualified subset send in a secure way their shares to a trusted party, referred to as a *combiner*, who computes the secret and sends it back to the participants.

Cheating-immune secret sharing schemes are secret sharing schemes in the above setting where dishonest participants, during the reconstruction phase, have *no advantage* in sending incorrect shares to the combiner (i.e., cheating) as compared to honest participants. More precisely, a coalition of dishonest participants, by using their correct shares and the incorrect secret supplied by the combiner, have no better chance in determining the true secret (that would have been reconstructed if they submitted correct shares) than an honest participant.

In this paper we study properties and constraints of cheating-immune secret sharing schemes. We show that a perfect secret sharing scheme cannot be cheating-immune. Then, we prove an upper bound on the number of cheaters tolerated in such schemes. We also repair a previously proposed construction to realize cheating-immune secret sharing schemes. Finally, we discuss some open problems.

*An extended abstract of this paper was presented at the International Workshop on Coding and Cryptography (WCC 2003).

†This work was partially done while the author was a Post-Doc Fellow at the Department of Combinatorics and Optimization, University of Waterloo, Canada

‡Supported by the Telecommunications Advancement Foundation in Japan.

Keywords: Cryptography, Secret Sharing, Cheating, Resilient Functions.

1 Introduction

Secret sharing schemes are a fundamental primitive in cryptography. They were introduced in 1979 by Blakley [1] and Shamir [13]. The reader can find an introduction and references to the literature in [14].

In its basic form, a secret sharing scheme is a protocol divided into two phases: *Share* and *Reconstruct*. During *Share*, a dealer distributes a secret among a set of participants by sending in a secure way a piece of information to each of them, called a *share*. Then, during *Reconstruct*, some subsets of participants (called *qualified subsets*) can reconstruct the secret either by pooling together their shares, or by sending their shares in a secure way to a trusted party (called a *combiner*) who collects the shares, reconstructs the secret, and sends it back to these participants[1]. Other subsets (called *forbidden subsets*), even by pooling together and processing their shares, do not learn any information about the secret. In such a model, the dealer and participants are assumed to be honest.

However, many applications have to deal with the case of dishonest participants and (possibly) a dishonest dealer. Tompa and Woll in [16] showed that Shamir's threshold scheme can be subject to the following attack (which can be applied to all linear secret sharing schemes). A dishonest participant, during *Reconstruct*, can submit to the combiner an opportunely constructed fake share. Hence, the reconstructed secret is different from the original one. But, from this secret, the dishonest participant (and only he) can recover the original secret.

For example, consider the simple secret sharing scheme where the secret K is the modulo-q sum of three shares: $K = s_1 + s_2 + s_3 \bmod q$. If the first participant submits an incorrect share, say $s_1' \neq s_1$, then the combiner outputs the value $K' = s_1' + s_2 + s_3 \bmod q$. Given K', the first participant can compute the correct secret $K = K' + s_1 - s_1' \bmod q$. The second and third participants may not even know that the value K' is incorrect. In any event, they cannot compute K even if they do know that K' is incorrect.

Tompa and Woll showed in [16] how to modify Shamir's scheme to avoid such an attack. Other papers which deal with the model analysed by Tompa and Woll include [4, 5].

In order to design secret sharing schemes that keep working even in hostile environments, the concept of *verifiability* was introduced in [7]. With this more general approach, some extra information is used to enable participants to detect a dishonest dealer, who sends inconsistent shares during *Share*, and to verify during *Reconstruct* that each participant submits a correct share. A lot of research has been done for both unconditionally secure and computationally secure verifiable secret sharing schemes (see [3, 6, 9, 15, 12], to name a few papers). Verifiable secret sharing schemes have been widely used in multi-party computation and in other applications of secret sharing schemes.

However, the world of applications is quite varied and verifiable secret sharing schemes are not always necessary. Morever, the computation, communication, and round complexities of verifiable secret sharing schemes are considerably greater than in the basic model for secret sharing. Therefore, achieving some forms of limited protection against cheaters in the basic model remains an interesting research problem. Along this line, a different approach to deal with cheating in secret sharing schemes was suggested by Pieprzyk and Zhang in [17, 10, 11]. In the model therein considered, called *cheating-immune secret sharing*, the

[1] In this paper we deal only with the latter reconstruction mode.

dealer and combiner are assumed to be honest. Participants can cheat, during *Reconstruct*, by submitting incorrect shares to the combiner. Such a secret sharing scheme is said to be *cheating-immune* if cheaters, on submitting incorrect shares, have no advantage (as compared to honest users) in determining the true secret. Notice that the combiner will only hear from some qualified subset of participants, and some bounded number of these may be cheaters.

It is perhaps useful to point out that, despite some superficial resemblances, cheating-immune and verifiable secret sharing schemes are solving two different problems. A verifiable secret sharing scheme is one that tolerates incorrect shares, allowing the correct secret to be reconstructed even when certain shares are faulty, via a process of detection and/or correction of the faulty shares. A cheating-immune secret sharing scheme will not compute the correct secret if a submitted share is faulty. The objective is rather to prevent cheaters from being able to compute the secret when honest participants cannot do so.

Organization of the paper: In Section 2, we give some background on secret sharing schemes: we recall the concepts of *perfect* and *ideal* secret sharing schemes. In Section 3, we describe a model for cheating-immune secret sharing scheme, which is the same given in [10], and in Section 4 we recall a characterization for such schemes; while, in Section 5, we point out a relation with resilient functions, which enables us to prove an upper bound on the number of possible cheaters in any (n, n) threshold scheme. In Section 6, we repair a previously proposed construction for cheating-immune secret sharing schemes. Finally, in Section 7, we state some results for the case of ramp schemes.

2 Perfect Secret Sharing Scheme

In this section we briefly recall the definition and some properties of perfect secret sharing schemes.

Let $\mathcal{P}$ be a set of participants and let S be a set of possible secrets. The collection of subsets $\mathcal{A} \subseteq 2^{\mathcal{P}}$, qualified to reconstruct the secret, is usually referred to as the *access structure* of the secret sharing scheme. Denoting by $\mathbf{S}$ a random variable representing the choice of a secret in S, by $\mathbf{A}$ the shares received by a subset of participants $A \in \mathcal{A}$, and using the entropy function[2], we can state the following definition:

Definition 2.1 *A* perfect secret sharing scheme Σ *with secrets chosen in* S*, for the* access structure $\mathcal{A} \subseteq 2^{\mathcal{P}}$*, is a protocol consisting of a* Share *phase and a* Reconstruct *phase, satisfying two conditions:*

1. *Every qualified subset of participants can compute the secret:*
   Formally, for all $A \in \mathcal{A}$*, it holds that* $H(\mathbf{S}|\mathbf{A}) = 0$.
2. *Any forbidden subset of participants gets absolutely no information on the secret value:*
   Formally, for all $A \notin \mathcal{A}$*, it holds that* $H(\mathbf{S}|\mathbf{A}) = H(\mathbf{S})$.

Property 1. means that the value of the shares held by $A \in \mathcal{A}$ uniquely determines the secret $s \in S$. On the other hand, Property 2 means that the probability that the secret is equal to s given that the shares held by $A \notin \mathcal{A}$ are a, is the same as the *a priori* probability of the secret s. In other words, by pooling together their shares, a forbidden subset of

[2]The reader is referred to Appendix A for the definition of the entropy function and some basic properties.

participant gets absolutely no information about the secret. If Property 2. is not satisfied, i.e., $H(\mathbf{S}|\mathbf{A}) < H(\mathbf{S})$, then a secret sharing scheme Σ is said to be *not perfect*.

A secret sharing scheme Σ can be represented by a matrix M, where each row corresponds to a possible distribution of shares for a certain secret. More precisely, in this representation, the first column of M is indexed by the dealer D, and contains the possible secret values he may wish to share, and the remaining columns are indexed by the participants in $\mathcal{P}$, and represent the shares they can get for each secret. This model has been proposed in [14].

The *efficiency* of a secret sharing scheme is measured by means of an *information rate*, which relates the size of the secret to the size of the shares given to the participants. More precisely, given a secret sharing scheme Σ for the access structure $\mathcal{A}$, on the set of secrets S, and denoting by $K(P)$ the set of possible shares for participant P, we define the information rate $\rho(\Sigma, \mathcal{A}, S)$ as

$$\rho(\Sigma, \mathcal{A}, S) = \frac{\log |S|}{\max_{P \in \mathcal{P}} \log |K(P)|}$$

and the optimal information rate of $\mathcal{A}$ as

$$\rho(\mathcal{A}) = \sup \rho(\Sigma, \mathcal{A}, S)$$

where the sup is taken over the space of all possible sets of secrets S, such that $|S| \geq 2$, and all secret sharing schemes Σ for $\mathcal{A}$. Secret sharing schemes with information rate equal to one, which is the maximum possible value of this parameter (i.e., the secret and the shares have the same size), are called *ideal*.

3 Cheating-Immune Model

We consider ideal secret sharing schemes with shares and values in $GF(p^t)$. More precisely, we start by considering (n, n) secret sharing schemes ((n, n)-SSS, for short), i.e., schemes where *all* shares held by n participants are required to reconstruct the secret. The model and the notation are the same as in [10].

Let $GF(p^t)$ denote a finite field with p^t elements, where p is a prime number and t is a positive integer. Let $GF(p^t)^n$ be the vector space of n-tuples of elements from $GF(p^t)$. For each $\alpha = (\alpha_1, \ldots, \alpha_n) \in GF(p^t)^n$, we denote by $HW(\alpha)$ (Hamming Weight) the number of non-zero coordinates of α.

In our setting, a vector $\alpha \in GF(P^t)^n$ represents the shares the participants get from the dealer during *Share*. The secret sharing scheme Σ is represented by a *defining* function,

$$f : GF(p^t)^n \to GF(p^t),$$

which associates to each n-tuple of shares a secret value in $GF(p^t)$.

Cheaters are represented by a vector $\delta \in GF(p^t)^n$, called *cheating vector*: non-zero elements represent the change of the true shares performed by the cheaters. The number of cheaters is equal to the Hamming weight of δ. Moreover, given two vectors, x and δ, we denote by $x_\delta^+ \in GF(p^t)^n$ a vector such that $x_j^+ = x_j$ if $\delta_j \neq 0$, and $x_j^+ = 0$ otherwise. Conversely, we denote by $x_\delta^- \in GF(p^t)^n$ a vector such that $x_j^- = x_j$ if $\delta_j = 0$, and $x_j^- = 0$ otherwise. Finally, given two vectors τ and δ, we say that $\tau \preceq \delta$ if $\tau_j \neq 0$ implies $\delta_j \neq 0$. Using the above notation we further define the following sets:

$$R(\delta, \alpha_\delta^+, K) \quad = \quad \{x_\delta^- | f(x_\delta^- + \alpha_\delta^+) = K\}$$

and,

$$R(\delta, \alpha_\delta^+ + \delta, K^*) \quad = \quad \{x_{\bar{\delta}}^- | f(x_{\bar{\delta}}^- + \alpha_\delta^+ + \delta) = K^*\}.$$

where $K = f(\alpha)$ and $K^* = f(\alpha + \delta)$.

The first set represents the possible shares held by honest participants, enabling the reconstruction of the true secret K, if cheaters behaved honestly. The second one, represents the possible shares held by honest participants enabling the reconstruction of K^*, when the cheaters submit incorrect shares. Therefore, the value

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

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

Definition 3.1 *[10] An (n, n)-SSS with shares and values in $GF(p^t)$ is said to be* k-cheating-immune *if, for every $\alpha \in GF(p^t)^n$ and any $\delta \in GF(p^t)^n$, with $1 \leq HW(\delta) \leq k$, it holds that $\rho_{\delta,\alpha} = p^{-t}$.*

A 1-cheating-immune secret sharing scheme will be simply referred to as a cheating-immune secret sharing scheme. Notice that the above definition assumes that all the cheaters submit fake shares. When $k > 1$, a more general definition takes into account the possibility that some subset of the cheaters submit correct shares. The underlying idea that justifies such an extension of the model is that there could be a strategy by means of which a coalition of cheaters can gain more information if *only some* of them submit incorrect shares. More precisely, we use a binary vector δ to identify the cheaters and a vector $\tau \in GF(p^t)^n$ to specify how much they cheat and, for every $\tau \preceq \delta$, we define

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

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

Definition 3.2 *[10] An (n, n)-SSS with shares and values in $GF(p^t)$ is said to be* strictly k-cheating-immune *if, for every $\alpha \in GF(p^t)^n$, any vector $\delta \in GF(2)^n$, and any $\tau \in GF(p^t)^n$, such that $\tau \preceq \delta$, $1 \leq HW(\delta) \leq HW(\tau) \leq k$, it holds that $\rho_{\delta,\tau,\alpha} = p^{-t}$.*

4 Characterisation for k-Cheating-Immune Secret Sharing

In this section we show some results about cheating-immune secret sharing schemes. We start by proving that a perfect secret sharing scheme cannot be cheating-immune. More precisely, we can state the following:

Theorem 4.1 *Let Σ be an (n, n)-secret sharing scheme with shares and values in $GF(p^t)$. If Σ is perfect, then Σ cannot be cheating-immune.*

Proof. For simplicity, assume the set of shares and secrets is $GF(2)$. In this case, the defining function, f, is given by

$$f : GF(2)^n \to GF(2).$$

Moreover, assume that 0 and 1, the values the secret can assume, are uniformly distributed. For any subset of participants $A = \{i_1, \ldots, i_{n-1}\}$, Condition 2 of Definition 2.1, implies that 0 and 1 still have the same a-priori probabilities, once the users in A pool together their shares. From the point of view of user i_n, this means that his share determines the value of the function. In other words, assuming that the share he gets from the dealer is 0, if during the reconstruction phase he submits 1, and the reconstructed secret is b, then he knows that the real secret is $1 - b$. Hence, the cheating-immune property is not satisfied since $\rho_{\delta,\alpha} \neq \frac{1}{2}$ with respect to any α and $\delta = (0, \ldots, 0, 1, 0, \ldots 0)$, with a single one in position i_n. A similar argument can be used for the case in which the set of shares and secrets is $GF(p^t)$. ∎

Notice that, if Definition 3.1 is extended to the case of general (ideal) access structures $\mathcal{A}$, defined over the set of participants $\mathcal{P}$, the above result still holds. Indeed, the key point in the above proof is that Condition 2 of Definition 2.1 rules out, from the point of view of participant i_n, one possible secret; hence, $\rho_{\delta,\alpha} \neq \frac{1}{p^t}$.

A cheating-immune secret sharing scheme will satisfy property 1. of Definition 2.1, namely, a qualified subset of shares will determine the value of the secret. Therefore it follows from Theorem 4.1 that property 2. cannot be satisfied. Hence, in a cheating-immune secret sharing scheme, some forbidden subsets of participants will, in some circumstances, be able to determine some (partial) information about the secret by pooling their shares.

The structure of the defining function f of a cheating-immune secret sharing scheme can be precisely characterized. The following result was shown in [10]. We recall this characterization by giving a slightly simplified proof, compared to the one given in [10].

Theorem 4.2 *Let Σ be an (n, n)-SSS with shares and values in $GF(p^t)$. Then, Σ is k-cheating-immune $\Leftrightarrow$ for any integer ℓ, where $1 \leq \ell \leq k$, for any $\delta \in GF(p^t)^n$, such that $HW(\delta) = \ell$, for any $\tau \preceq \delta$, and for any $u, v \in GF(p^t)$, the following conditions hold simultaneously:*

(i) $|R(\delta, \tau, v)| = p^{t(n-\ell-1)}$,

(ii) $|(R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u))| = p^{t(n-\ell-2)}$.

Proof. The first implication is immediate: indeed, if (i) and (ii) hold, then the scheme is k-cheating immune. Hence, given a k-cheating immune secret sharing scheme, we have to show that (i) and (ii) hold. Let $HW(\delta) = \ell$. For any $\alpha, \delta \in GF(p^t)^n$, the family of subsets $\{R(\delta, \alpha_\delta^+ + \delta, K^*)\}_{K^* \in GF(p^t)}$ is a partition of the set $\{x_\delta^- | \delta \in GF(p^t)^n \text{ and } x_\delta^- \in GF(p^t)^n\} \subseteq GF(p^t)^n$. Since $|\{x_\delta^- | \delta \in GF(p^t)^n \text{ and } x_\delta^- \in GF(p^t)^n\}| = p^{t(n-\ell)}$, we have that

$$\sum_{K^* \in GF(p^t)} |R(\delta, \alpha_\delta^+ + \delta, K^*)| = p^{t(n-\ell)} \tag{1}$$

From the definition of a k-cheating immune secret sharing scheme, we also have

$$|R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K)| = \frac{1}{p^t} |R(\delta, \alpha_\delta^+ + \delta, K^*)|. \tag{2}$$

On the other hand, we can partition $R(\delta, \alpha_\delta^+, K)$ as follows:

$$R(\delta, \alpha_\delta^+, K) = \bigcup_{K^* \in GF(p^t)} \{R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K)\}$$

Therefore,

$$|R(\delta,\alpha_\delta^+,K)| = \sum_{K^*\in GF(p^t)} |R(\delta,\alpha_\delta^+ + \delta, K^*) \cap R(\delta,\alpha_\delta^+,K)|. \tag{3}$$

Then, substituting equation (2) in equation (3), we get

$$|R(\delta,\alpha_\delta^+,K)| = \sum_{K^*\in GF(p^t)} \frac{1}{p^t}|R(\delta,\alpha_\delta^+ + \delta, K^*)|,$$

and, by using equation (1),

$$|R(\delta,\alpha_\delta^+,K)| = \frac{1}{p^t}\sum_{K^*\in GF(p^t)} |R(\delta,\alpha_\delta^+ + \delta, K^*)| = p^{t(n-\ell-1)}. \tag{4}$$

Thus, property (i) is satisfied. At this point notice that, since (4) holds for *every pair* (δ,α_δ^+), using an appropriate β, we can always write $\alpha_\delta^+ = \beta_\delta^+ + \delta$. Therefore, we can replace α_δ^+ in $R(\delta,\alpha_\delta^+,K)$ in equation (4) with $\alpha_\delta^+ + \delta$. Hence

$$|R(\delta,\alpha_\delta^+ + \delta,K)| = p^{t(n-\ell-1)},$$

and, by using equation (2), we get

$$|R(\delta,\alpha_\delta^+ + \delta,K^*) \cap R(\delta,\alpha_\delta^+,K)| = \frac{1}{p^t}\cdot p^{t(n-\ell-1)} = p^{t(n-\ell-2)}.$$

Therefore, the result holds. ∎

5 k-Cheating-Immunity and k-Resilience

In this section we investigate the relation between k-cheating-immune secret sharing scheme over $GF(p^t)$ and resilient functions. Such a relation has already been pointed out for the binary case (k-cheating-immune secret sharing scheme over $GF(2)$) in [11, 17]. We use it to state an upper bound on the number of possible cheaters tolerated in a cheating-immune secret sharing scheme.

Definition 5.1 *A function $f : GF(p^t)^n \to GF(p^t)$ is said to be* balanced *if, for each $K \in GF(p^t)$, it holds that*

$$|\{x \in GF(p^t)^n | f(x) = K\}| = p^{t(n-1)}.$$

In other words, each value $f(x) \in GF(p^t)$ has the same number of pre-images x.

Definition 5.2 *A function $f : GF(p^t)^n \to GF(p^t)$ is said to be* k-resilient *if, for every subset $\{j_1,\ldots,j_k\} \subset \{1,\ldots,n\}$ and every $(a_1,\ldots,a_k) \in GF(p^t)^k$, the function*

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

is balanced over $GF(p^t)^{n-k}$.

Notice that, if $f : GF(p^t)^n \to GF(p^t)$ is the defining function of a perfect (n, n)-SSS where the secrets are chosen *uniformly at random*, then, *for any* $1 \leq k < n$, f is k-resilient. This property easily follows from Condition 2 of Definition 2.1.

The next corollary, concerning k-cheating-immune secret sharing schemes, easily follows from Theorem 4.2.

Corollary 5.3 *Let Σ be an (n, n)-SSS, and let $f : GF(p^t)^n \to GF(p^t)$ be the defining function of Σ. If Σ is k-cheating-immune, then f is k-resilient.*

On the other hand, we can prove the following result:

Theorem 5.4 *Let Σ be an (n, n)-SSS, and let $f : GF(p^t)^n \to GF(p^t)$ be the defining function of Σ. If Σ is k-cheating-immune, then f cannot be $(n-k)$-resilient.*

Proof. We need some notation and preliminary results.

- Let $1 \leq s \leq k$. For any subset of indices $\gamma = \{j_1, \ldots, j_s\} \subseteq \{1, \ldots, n\}$, let $\overline{\gamma} = \{i_1, \ldots, i_{n-s}\} = \{1, \ldots, n\} \setminus \{j_1, \ldots, j_s\}$ be the complementary subset. For any vector $x \in GF(p^t)^n$, let

$$u = (x_{j_1}, \ldots, x_{j_s}), \quad \text{and} \quad v = (x_{i_1}, \ldots, x_{i_{n-s}}).$$

  Then, we can write $f(x) = f(u, v)$. Moreover, let $\alpha = (\alpha_{j_1}, \ldots, \alpha_{j_s}) \in GF(p^t)^s$. This vector represents shares held by cheaters. If u and α have no common coordinates, that is, $\alpha_{j_i} \neq x_{j_i}$ for every $1 \leq i \leq s$, we say that they are totally distinct, and we write $u \not\simeq \alpha$.

- If Σ is k-cheating immune, Theorem 4.2 implies that, for any $K \in GF(p^t)$ and any $\alpha \in GF(p^t)^s$,

$$\left|\{v \in GF(p^t)^{n-s} | f(\alpha, v) = K\}\right| = p^{t(n-s-1)}.$$

  Let us fix $K \in GF(p^t)$ and $\alpha \in GF(p^t)^s$, and denote by

$$R_{K,\alpha} = \{v \in GF(p^t)^{n-s} | f(\alpha, v) = K\}.$$

  Then, $|R_{K,\alpha}| = p^{t(n-s-1)}$, and applying again Theorem 4.2, for any $K^* \in GF(p^t)$ and any $u \in GF(p^t)^s$, such that $u \not\simeq \alpha$, we have that

$$\begin{aligned} |\{v \in R_{K,\alpha} | f(u, v) = K^*\}| &= \left|R_{K,\alpha} \cap \{v \in GF(p^t)^{n-s} | f(u, v) = K^*\}\right| \\ &= p^{t(n-s-2)}. \end{aligned}$$

  The above relation holds even for $K = K^*$.

- Let

$$Q_{K,\alpha} = \{(u, v) | u \in GF(p^t)^s, u \not\simeq \alpha, v \in R_{K,\alpha}, f(u, v) = K\}.$$

It easily follows that

$$\begin{aligned}|Q_{K,\alpha}| &= \sum_{u \in GF(p^t)^s, u \not\simeq \alpha} |\{v \in R_{K,\alpha} | f(u,v) = K\}| \\ &= (p^t - 1)^s p^{t(n-s-2)}. \end{aligned} \tag{5}$$

Equation (5) holds for $1 \le s \le k$; while, when $s = 0$, we have

$$|Q_{K,\alpha}| = |\{v | v \in R_{K,\alpha}, f(v) = K\}| = |\{v | f(v) = K\}| = p^{t(n-1)}. \tag{6}$$

- For any subset $a \subseteq \{1, 2, \cdots, s\}$ and $\overline{a} = \{1, 2, \cdots, s\} \setminus a$, let

  $$S(\alpha, a) = \{u \in GF(p^t)^s | \forall i \in a, \quad u_{j_i} = \alpha_{j_i} \quad \text{and} \quad \forall i \in \overline{a}, \quad u_{j_i} \neq \alpha_{j_i}\}.$$

  Notice that if a and b are different subsets, then $S(\alpha, a) \cap S(\alpha, b) = \emptyset$. Moreover,

  $$S(\alpha, \emptyset) = \{u \in GF(p^t)^s | u \not\simeq \alpha\}, \quad \text{and} \quad S(\alpha, \{1, 2, \cdots, s\}) = \{\alpha\}.$$

  We can express
  $$GF(p^t)^s = \bigcup_{a \subseteq \{1,2,\cdots,s\}} S(\alpha, a).$$

At this point, we can start the real proof. Let us fix $K \in GF(p^t)$, $\alpha \in GF(p^t)^s$, and a k-subset of indices $\gamma = \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$. Let us consider the set

$$T_\alpha(u, v) = \{(u, v) | u \in GF(p^t)^s, v \in R_{K,\alpha}, f(u, v) = K\}.$$

The value

$$\begin{aligned} T &= \sum_{\alpha \in GF(p^t)^k} |T_\alpha(u, v)| \\ &= \sum_{\alpha \in GF(p^t)^k} |\{(u, v) | u \in GF(p^t)^k, v \in R_{K,\alpha}, f(u, v) = K\}| \\ &= \sum_{\alpha \in GF(p^t)^k} \sum_{a \subseteq \{1,2,\cdots,k\}} |\{(u, v) | u \in S(\alpha, a), v \in R_{K,\alpha}, f(u, v) = K\}| \\ &= \sum_{a \subseteq \{1,2,\cdots,k\}} \sum_{\alpha \in GF(p^t)^k} |\{(u, v) | u \in S(\alpha, a), v \in R_{K,\alpha}, f(u, v) = K\}|. \end{aligned}$$

We prove that f cannot be $n-k$-resilient by showing a contradiction on the value of T. First we compute the real value of T and, then, the one that we would get if f were $n-k$-resilient. Since the two values are different, we conclude that f cannot be $n-k$ resilient.
For any $a \subseteq \{1, 2, \ldots, k\}$, let

$$U^a = \sum_{\alpha \in GF(p^t)^k} |\{(u, v) | u \in S(\alpha, a), v \in R_{K,\alpha}, f(u, v) = K\}|.$$

By fixing an m-subset of indices $a = \{i_1, \ldots, i_m\} \subseteq \{1, 2, \ldots, k\}$, we can partition

$$GF(p^t)^k = \bigcup_{\beta \in GF(p^t)^{k-m}} \{\alpha | \alpha_{[a]} \in GF(p^t)^m, \alpha_{[\overline{a}]} = \beta\}.$$

where $\alpha_{[a]} = (\alpha_{i_1}, \ldots, \alpha_{i_m})$ and $\alpha_{[\overline{a}]} = (\alpha_{i_{m+1}}, \ldots, \alpha_{i_k})$. Then,

$$U^a = \sum_{\beta \in GF(p^t)^{k-m}} \sum_{\alpha_{[a]} \in GF(p^t)^m, \alpha_{[\overline{a}]} = \beta} |\{(u,v) | u \in S(\alpha, a), v \in R_{K,\alpha}, f(u,v) = K\}|.$$

Let us fix $\beta \in GF(p^t)^{k-m}$, and let

$$W^a(\beta) = \sum_{\alpha_{[a]} \in GF(p^t)^m, \alpha_{[\overline{a}]} = \beta} |\{(u,v) | u \in S(\alpha, a), v \in R_{K,\alpha}, f(u,v) = K\}|.$$

Moreover, let $\omega = \bigcup_{i \in a} \{j_i\}$, and $\eta = \gamma \setminus \omega$. Denoting with $y = x_{[\eta]}$, $z = x_{[\omega]}$, and $v = x_{[\overline{\gamma}]}$, we can re-write $f(x)$ as

$$f(x) = f(x_{[\gamma]}, x_{[\overline{\gamma}]}) = f(x_{[\eta]}, x_{[\omega]}, x_{[\overline{\gamma}]}) = f(y, z, v).$$

Notice that, $u = \alpha$ implies $y = \alpha_{[a]}$ and $z = \alpha_{[\overline{a}]}$. Therefore, we can rewrite $R_{K,\alpha}$ and $S(\alpha, a)$ as

$$\begin{aligned} R_{K,\alpha} &= \{v \in GF(p^t)^{n-k} | f(\alpha_{[\overline{a}]}, \alpha_{[a]}, v) = K\} \\ S(\alpha, a) &= \{(y,z) \in GF(p^t)^{k-m} \times GF(p^t)^m | y \not\preceq \alpha_{[\overline{a}]}, z = \alpha_{[a]}\} \end{aligned}$$

Using these expressions, we get

$$\begin{aligned} W^a(\beta) &= \sum_{\alpha_{[a]} \in GF(p^t)^m, \alpha_{[\overline{a}]} = \beta} |\{(y,z,v) | (y,z) \in S(\alpha, a), v \in R_{K,\alpha}, f(y,z,v) = K\}| \\ &= \sum_{\alpha_{[a]} \in GF(p^t)^m, \alpha_{[\overline{a}]} = \beta} |\{(y,z,v) | y \not\preceq \alpha_{[\overline{a}]}, y \in GF(p^t)^{k-m}, z = \alpha_{[a]}, \\ &\qquad\qquad f(\alpha_{[\overline{a}]}, \alpha_{[a]}, v) = K, f(y,z,v) = K\}| \\ &= \sum_{\alpha_{[a]} \in GF(p^t)^m} |\{(y,z,v) | y \not\preceq \beta, y \in GF(p^t)^{k-m}, z = \alpha_{[a]}, \\ &\qquad\qquad f(\beta, \alpha_{[a]}, v) = K, f(y,z,v) = K\}| \\ &= |\{(y,z,v) | y \not\preceq \beta, y \in GF(p^t)^{k-m}, f(\beta, z, v) = K, f(y,z,v) = K\}|. \end{aligned}$$

Since there is a natural one-to-one correspondence between $v' \in GF(p^t)^{n-k+m}$ and (z,v), we can treat $v' = (z,v)$. Then,

$$\begin{aligned} W^a(\beta) &= |\{(y,v') | y \not\preceq \beta, y \in GF(p^t)^{k-m}, f(\beta, v') = K, f(y,v') = K\}| \\ &= |\{(y,v') | y \not\preceq \beta, y \in GF(p^t)^{k-m}, v' \in R_{K,\beta}, f(y,v') = K\}| \\ &= |Q_{K,\beta}|. \end{aligned}$$

From equations (5) and (6), it follows that

$$W^a(\beta) = |Q_{K,\beta}| = \begin{cases} (p^t - 1)^{k-m} p^{t(n-k+m-2)} & \text{if } k > m, \\ p^{t(n-1)} & \text{if } k = m. \end{cases}$$

Therefore, we have that

$$T = \sum_{a \subseteq \{1,\ldots,k\}} U^a$$

$$
\begin{aligned}
&= \sum_{a\subseteq\{1,\ldots,k\}} \sum_{\beta\in GF(p^t)^{k-m}} W^a(\beta) \\
&= \sum_{a\subseteq\{1,\ldots,k\}} \sum_{\beta\in GF(p^t)^{k-m}} |Q_{K,\beta}| \\
&= \sum_{a\subset\{1,\ldots,k\},a\neq\{1,\ldots,k\}} \sum_{\beta\in GF(p^t)^{k-m}} |Q_{K,\beta}| + \sum_{a=\{1,\ldots,k\}} \sum_{\beta\in GF(p^t)^{k-m}} |Q_{K,\beta}| \\
&= \sum_{a\subset\{1,\ldots,k\},a\neq\{1,\ldots,k\}} \sum_{\beta\in GF(p^t)^{k-m}} (p^t-1)^{k-m}p^{t(n-k+m-2)} + p^{t(n-1)} \\
&= \sum_{a\subset\{1,\ldots,k\},a\neq\{1,\ldots,k\}} p^{t(k-m)}(p^t-1)^{k-m}p^{t(n-k+m-2)} + p^{t(n-1)} \\
&= \sum_{m=0}^{k-1} \binom{k}{m}(p^t-1)^{k-m}p^{t(n-2)} + p^{t(n-1)} \\
&= p^{t(n-2)}\{\sum_{m=0}^{k-1} \binom{k}{m}(p^t-1)^{k-m}+1\} - p^{t(n-2)} + p^{t(n-1)} \\
&= p^{t(n-2)} \sum_{m=0}^{k} \binom{k}{m}1^m(p^t-1)^{k-m} - p^{t(n-2)} + p^{t(n-1)} \\
&= p^{t(n-2)}(1+p^t-1)^k - p^{t(n-2)} + p^{t(n-1)} \\
&= p^{t(n+k-2)} - p^{t(n-2)} + p^{t(n-1)}. \qquad (7)
\end{aligned}
$$

On the other hand, if f were $n-k$-resilient, for any fixed $v \in GF(p^t)^{n-k}$, $f(u,v)$ would be balanced; that is, for each $K \in GF(p)^t$, it would be

$$|\{(u,v)|u \in GF(p^t)^k, f(u,v) = K\}| = p^{t(k-1)}.$$

Since, from Theorem 4.2, $|R_{K,\alpha}| = p^{t(n-k-1)}$, then for any $K \in GF(p^t)$ and any $\gamma \subseteq \{1,\cdots,n\}$ of size k, we have that

$$
\begin{aligned}
|T_\alpha(u,v)| &= |\{(u,v)|u \in GF(p^t)^k, v \in R_{K,\alpha}, f(u,v) = K\}| \\
&= |\bigcup_{v\in R_{K,\alpha}} \{(u,v)|u \in GF(p^t)^k, f(u,v) = K\}| \\
&= \sum_{v\in R_{K,\alpha}} |\{(u,v)|u \in GF(p^t)^k, f(u,v) = K\}| \\
&= p^{t(n-k-1)}p^{t(k-1)} \\
&= p^{t(n-2)}.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
T &= \sum_{\alpha\in GF(p^t)^k} |T_\alpha(u,v)| \\
&= \sum_{\alpha\in GF(p^t)^k} p^{t(n-2)} \\
&= p^{tk}p^{t(n-2)} \\
&= p^{t(n+k-2)}, \qquad (8)
\end{aligned}
$$

which clearly contradicts (7). Therefore, f cannot be $n-k$-resilient. ■

At this point, we can state the main result of this section.

Theorem 5.5 *A secret sharing scheme Σ defined by $f : GF(p^t)^n \to GF(p^t)$ can be k-cheating-immune only if $k < \frac{n}{2}$.*

Proof. A k-resilient function is also s-resilient, for any $1 \leq s < k$. This observation, together with Theorem 5.4 and Corollary 5.3, implies the result. ■

The above upper bound on the number of cheaters holds also for the case of strictly k-cheating-immune secret sharing. Indeed, a strictly k-cheating-immune secret sharing possibility that all k cheaters submit fake shares.

6 A Construction for k-Cheating-Immune Secret Sharing

We present a construction for k-cheating-immune secret sharing applying the ideas of the construction given in [10]. Basically, we use a new function μ as a building block for the scheme, instead of the function χ described (unfortunately, the function χ proposed is not balanced, as the construction requires).

In the following, if 1 denotes the identity in $GF(p^t)$, we indicate the sum of $\lceil p/2 \rceil$ elements equal to 1 by b_p^+, and the sum of $\lfloor p/2 \rfloor$ elements equal to 1 by b_p^-. Therefore, for any $a \in GF(p^t)^n$, the term $b_p^+ a$ ($b_p^- a$, resp.) is the sum of $\lceil p/2 \rceil$ ($\lfloor p/2 \rfloor$, resp.) elements equal to a. In order to show the properties of our new function, we need some results, that we briefly recall.

Definition 6.1 *[10] A function h of degree two is said to have the property $B(k)$ if, for any $\delta \in GF(p^t)^n$, with $1 \leq HW(\delta) \leq k$, and for any $\tau \preceq \delta$, the function $h(x_{\bar{\delta}}^- + \delta + \tau) - h(x_{\bar{\delta}}^- + \tau)$ is a non-constant affine function.*

The next lemma is used to prove that our function is balanced.

Lemma 6.2 *[10] Suppose a function f of degree two on $GF(p^t)^n$ does 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 vector $\alpha \in GF(p^t)^n$ such that $f(x+\alpha) - f(x)$ is constant and $f(\alpha) \neq 0$.*

The function μ we use in order to set up a k-cheating-immune secret sharing scheme is defined as follows:

Lemma 6.3 *Let $n \geq 2k+1$, and let $\mu_{n,p} : GF(p^t)^n \to GF(p^t)$ be a function defined by*

$$\mu_{n,p} = x_1 + \sum_{i=1}^{\lfloor n/2 \rfloor} \{ b_p^- x_{[2i-1]_{(n)}} x_{[2i]_{(n)}} + b_p^+ x_{[2i]_{(n)}} x_{[2i+1]_{(n)}} \} + \begin{cases} b_p^- x_n x_1 + b_p^+ x_1 x_1 & \text{if } n \text{ is odd,} \\ 0 & \text{otherwise,} \end{cases}$$

where $[i]_{(n)}$ denotes the integer j such that $1 \leq j \leq n$, and $j \equiv i \bmod n$. Then, (i) $\mu_{n,p}$ is balanced, and (ii) $\mu_{n,p}$ satisfies the property $B(k)$.

Proof. For any $2 \leq j \leq n$, by definition, $\mu_{n,p}$ has p quadratic terms including x_j, which consist of either b_p^+ terms $x_{[j-1]_{(n)}} x_j$ and b_p^- terms $x_j x_{[j+1]_{(n)}}$, or b_p^- terms $x_{[j-1]_{(n)}} x_j$ and b_p^+ terms $x_j x_{[j+1]_{(n)}}$ in $\mu_{n,p}$. Moreover, if n is even, there exist p quadratic terms including x_1, which consist of b_p^+ terms $x_n x_1$ and b_p^- terms $x_1 x_2$. Otherwise, there exist $p + b_p^-$ quadratic terms including x_1, which consist of b_p^- terms $x_n x_1$, b_p^- terms $x_1 x_2$, and b_p^+ terms $x_1 x_1$. Let g be a function defined as $g = \mu_{n,p} - x_1$. Then, g can be re-written as

$$g = \sum_{i=1}^{\lfloor n/2 \rfloor} x_{[2i]_{(n)}} \{ b_p^- x_{[2i-1]_{(n)}} + b_p^+ x_{[2i+1]_{(n)}} \} + \begin{cases} x_1 (b_p^- x_n + b_p^+ x_1) & \text{if } n \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Let $\alpha = (1, \ldots, 1)$, and assume n is odd. Since $pe = 0$ for any $e \in GF(p^t)^n$ (p is the characteristic of the finite field $GF(p^t)$), and there exist $\lceil n/2 \rceil p$ quadratic terms, then $g(\alpha) = 0$. Moreover, for $2 \leq j \leq n$, x_j appears in p quadratic terms, while x_1 appears in $2b_p^-$ quadratic terms with another term $x_k \neq x_1$, and in b_p^+ terms of the form $x_1 x_1$. Finally, since a term $(x_1+1)(x_1+1)$ produces two single x_1 terms, $g(x+\alpha) - g(x)$ produces $2p$ single x_1 terms. Therefore, it is easy to verify that $g(x+\alpha) - g(x) = 0$. Hence, $\mu_{n,p}(x+\alpha) - \mu_{n,p}(x) = 1$, and $\mu_{n,p}(\alpha) = 1$. Using Lemma 6.2, we can conclude that $\mu_{n,p}$ is balanced. When n is even, we can also show that $\mu_{n,p}$ is balanced, similarly.

To show that *(ii)* of the lemma holds, we can proceed as follows: Let $\delta = (\delta_1, \ldots, \delta_n) \in GF(p^t)^n$ be a cheating vector such that $HW(\delta) = \ell$, where $1 \leq \ell \leq k$. Moreover, let $\tau \preceq \delta$, and let $J = \{ j | \delta_j \neq 0, 1 \leq j \leq n \}$. Then, $|J| = HW(\delta) = \ell$. Each quadratic term that includes x_i consists of variables in $\{ x_{[i-1]_{(n)}}, x_i, x_{[i+1]_{(n)}} \}$. Let $X_i = \{ [i-1]_{(n)}, i, [i+1]_{(n)} \}$. It can be easily seen that no quadratic term exists in $\mu_{n,p}(x_{\bar{\delta}}^+ + \tau + \delta) - \mu_{n,p}(x_{\bar{\delta}}^+ + \tau)$. Therefore, to show that $\mu_{n,p}$ has the property $B(k)$, it is enough to show that there exists a linear term x_i in $\mu_{n,p}(x_{\bar{\delta}}^+ + \tau + \delta) - \mu_{n,p}(x_{\bar{\delta}}^+ + \tau)$. To this aim notice that, since $n \geq 2k+1$, there exists an i such that $X_i \cap J = \{ [i-1]_{(n)} \}$. Let i_0 be such that $X_{i_0} \cap J = \{ [i_0 - 1]_{(n)} \}$. Then $\delta_{[i_0-1]_{(n)}} \neq 0$, and $\delta_{i_0} = \delta_{[i_0+1]_{(n)}} = 0$. Hence, in $\mu_{n,p}(x_{\bar{\delta}}^+ + \tau + \delta) - \mu_{n,p}(x_{\bar{\delta}}^+ + \tau)$, either $\delta_{[i_0-1]_{(n)}} b_p^+ x_{i_0}$ or $\delta_{[i_0-1]_{(n)}} b_p^- x_{i_0}$ is the only term which includes x_{i_0}. Therefore, $\mu_{n,p}(x_{\bar{\delta}}^+ + \tau + \delta) - \mu_{n,p}(x_{\bar{\delta}}^+ + \tau)$ includes a linear term x_{i_0}, which ensures that $\mu_{n,p}$ has the property $B(k)$. ∎

Example 6.1 We provide an example of a function $\mu_{n,p}(x)$. Let $n = 3$, $p = 3$, and $k = 1$. Then, we have that $b_p^- = 1$ and $b_p^+ = 2$. According to the above lemma, the function $\mu_{3,3}$: $GF(3)^3 \to GF(3)$ is defined as follows:

$$\mu_{3,3}(x_1, x_2, x_3) = x_1 + x_1 x_2 + 2 x_2 x_3 + x_3 x_1 + 2 x_1 x_1.$$

It is not difficult to see that $\mu_{3,3}$ is balanced. Indeed, we have

x_1	x_2	x_3	S
0	0	0	0
1	0	0	0
2	0	0	1
0	1	0	0
1	1	0	1
2	1	0	0
0	2	0	0
1	2	0	2
2	2	0	2

x_1	x_2	x_3	S
0	0	1	0
1	0	1	1
2	0	1	0
0	1	1	2
1	1	1	1
2	1	1	1
0	2	1	1
1	2	1	1
2	2	1	2

x_1	x_2	x_3	S
0	0	2	0
1	0	2	2
2	0	2	2
0	1	2	1
1	1	2	1
2	1	2	2
0	2	2	2
1	2	2	0
2	2	2	2

Notice that $\mu_{3,3}(0,0,0) = 0$ and, for $\alpha = (1,1,1)$, it holds that $\mu_{3,3}(1,1,1) = 1$. Moreover, simple algebra shows that

$$\mu_{3,3}(x_1 + 1, x_2 + 1, x_3 + 1) - \mu_{3,3}(x_1, x_2, x_3) = 1.$$

We can also easily check that $\mu_{3,3}$ has property $B(1)$. Indeed, for each $\delta \in GF(3)^3$, with $HW(\delta) = 1$, and for any $\tau \preceq \delta$, we have that $\mu_{3,3}(x_{\bar{\delta}}^- + \delta + \tau) - \mu_{3,3}(x_{\bar{\delta}}^- + \tau)$ is given by:

δ	τ	$\mu_{3,3}(x_{\bar{\delta}}^- + \delta + \tau) - \mu_{3,3}(x_{\bar{\delta}}^- + \tau)$
$(1,0,0)$	$(0,0,0)$	$x_2 + x_3$
$(1,0,0)$	$(1,0,0)$	$1 + x_2 + x_3$
$(1,0,0)$	$(2,0,0)$	$2 + x_2 + x_3$
$(0,1,0)$	$(0,0,0)$	$x_1 + 2x_3$
$(0,1,0)$	$(0,1,0)$	$x_1 + 2x_3$
$(0,1,0)$	$(0,2,0)$	$x_1 + 2x_3$
$(0,0,1)$	$(0,0,0)$	$x_1 + 2x_2$
$(0,0,1)$	$(0,0,1)$	$x_1 + 2x_2$
$(0,0,1)$	$(0,0,2)$	$x_1 + 2x_2$

Therefore $\mu_{3,3}$ has property $B(1)$. ∎

According to the strategy defined by Lemma 5 and Theorem 5 in [10], using $\mu_{n,p}$ as a building block, we can construct a k-cheating-immune secret sharing scheme. More precisely, it is possible to show that the following lemma holds.

Lemma 6.4 *[10] Let f_1 and f_2 be two functions defined over $GF(p^t)^{n_1}$ and $GF(p^t)^{n_2}$, respectively. Let $f(x) = f_1(y) + f_2(z)$, where $x = (y, z)$, and $y \in GF(p^t)^{n_1}, z \in GF(p^t)^{n_2}$. Then,*

1. *f is balanced if f_1 or f_2 is balanced.*
2. *f has the property $B(k)$ if both f_1 and f_2 have the property $B(k)$.*

By setting $\chi_{2k+1} = \mu_{2k+1,p}$, and using the above result, the following lemma holds:

Lemma 6.5 *[10] Let $\chi_{4k+2}(x_1, \ldots, x_{4k+2}) = \chi_{2k+1}(x_1, \ldots, x_{2k+1}) + \chi_{2k+1}(x_{2k+2}, \ldots, x_{4k+2})$. Then, the function χ_{4k+2} is balanced and satisfies the property $B(k)$.*

Finally, a k-cheating-immune secret sharing scheme can be realized as follows:

Theorem 6.6 *[10] Let k and s be positive integers with $s \geq k+1$, and let $n_1, \ldots, n_s \in \{4k+1, 4k+2\}$, such that $n = n_1 + \cdots + n_s$. Let $f(x)$ be a function defined over $GF(p^t)^n$ by $f(x) = \chi_{n_1}(x_1) + \ldots + \chi_{n_s}(x_s)$, where $x = (x_1, \ldots, x_s)$, and, for $i = 1, \ldots, s$, the value $x_i \in GF(p^t)^{n_i}$. If each χ_{n_i} is constructed according to Lemma 6.3 or Lemma 6.5, and $\chi_{n_1}, \ldots, \chi_{n_s}$ have mutually disjoint variables, then the secret sharing scheme with defining function $f(x)$ is k-cheating-immune.*

Example 6.2 We give an example of an $(11, 11)$ cheating-immune secret sharing scheme. Let $k = 1$, $s = 2$, and $p = 5$. Moreover, let us set, according to Theorem 6.6, $n_1 = 5$ and $n_2 = 6$. It follows that $n = n_1 + n_2 = 11$. Let us start by constructing the functions $\mu_{5,5}$ and $\mu_{3,5}$. Since $p = 5$, we have that $b_p^- = 2$, and $b_p^+ = 3$. Hence:

$$\begin{aligned} \mu_{5,5}(x_1, x_2, x_3, x_4, x_5) &= x_1 + 2x_1x_2 + 3x_2x_3 + 2x_3x_4 + 3x_4x_5 + 2x_5x_1 + 3x_1x_1 \\ \mu_{3,5}(x_1, x_2, x_3) &= x_1 + 2x_1x_2 + 3x_2x_3 + 2x_3x_1 + 3x_1x_1. \end{aligned}$$

Then, let us define the functions $\chi_5(z_1)$ and $\chi_6(z_2)$, where $z_1 = (x_1, x_2, x_3, x_4, x_5)$ and $z_2 = (x_6, x_7, x_8, x_9, x_{10}, x_{11})$, as follows:

$$\begin{aligned} \chi_5(z_1) &= \mu_{5,5}(x_1, x_2, x_3, x_4, x_5) \\ &= x_1 + 2x_1x_2 + 3x_2x_3 + 2x_3x_4 + 3x_4x_5 + 2x_5x_1 + 3x_1x_1 \\ \chi_6(z_2) &= \mu_{3,5}(x_6, x_7, x_8) + \mu_{3,5}(x_9, x_{10}, x_{11}) \\ &= x_6 + 2x_6x_7 + 3x_7x_8 + 2x_8x_6 + 3x_6x_6 + x_9 + 2x_9x_{10} + 3x_{10}x_{11} \\ &\quad +2x_{11}x_9 + 3x_{11}x_{11} \end{aligned}$$

The defining function $f(x) : GF(5)^{11} \to GF(5)$ of the cheating-immune secret sharing scheme is given by:

$$f(x) = \chi_5(z_1) + \chi_6(z_2),$$

where $x = (z_1, z_2)$. By plugging in the above pieces, we get the explicit form:

$$\begin{aligned} f(x) &= f(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) \\ &= x_1 + 2x_1x_2 + 3x_2x_3 + 2x_3x_4 + 3x_4x_5 + 2x_5x_1 + 3x_1x_1 \\ &\quad +x_6 + 2x_6x_7 + 3x_7x_8 + 2x_8x_6 + 3x_6x_6 \\ &\quad +x_9 + 2x_9x_{10} + 3x_{10}x_{11} + 2x_{11}x_9 + 3x_{11}x_{11}. \end{aligned}$$

■

A construction for strictly k-cheating-immune secret sharing schemes, which basically generalises the above one, can be found in [10].

7 Ramp Secret Sharing Schemes

The idea of a ramp secret sharing scheme has been introduced in [2]. More precisely, a ramp secret sharing scheme ((t_1, t_2, n)-RS, for short) is a protocol by means of which a dealer distributes a secret s among a set of n participants $\mathcal{P}$ in such a way that subsets of $\mathcal{P}$ of size greater than or equal to t_2 can reconstruct the value of s; no subset of $\mathcal{P}$ of size less than or equal to t_1 can determine anything about the value of the secret; and a subset of size $t_1 < t < t_2$ can recover *some* information about the secret [2]. Using the entropy function [8], the three properties of a (linear) (t_1, t_2, n)-RS can be stated as follows. Assuming that A denotes both a subset of participants and the set of shares these participants receive from the dealer to share a secret $s \in S$, and denoting the corresponding random variables in bold, it holds that

- *Any subset of participants of size less than or equal to t_1 has no information on the secret value:* Formally, for each subset $A \subseteq \mathcal{P}$ of size $|A| \leq t_1$, $H(\mathbf{S}|\mathbf{A}) = H(\mathbf{S})$.

- *Any subset of participants of size $t_1 < |A| < t_2$ has some information on the secret value:* Formally, for each subset $A \subseteq \mathcal{P}$ of size $t_1 < |A| < t_2$, $H(\mathbf{S}|\mathbf{A}) = \frac{|A|-t_1}{t_2-t_1} H(\mathbf{S})$.
- *Any subset of participants of size greater than t_2 can compute the whole secret:* Formally, for each subset $A \subseteq \mathcal{P}$ of size $|A| \geq t_2$, $H(\mathbf{S}|\mathbf{A}) = 0$.

It can be easily seen that the defining function of a (t_1, t_2, n)-RS, where the secrets are chosen uniformly at random, is t_1-resilient. Applying the same arguments we have applied before, and using Theorem 5.4, we can show the following:

Theorem 7.1 *A (t_1, t_2, n)-ramp secret sharing scheme Σ defined by $f : GF(p^t)^n \to GF(p^t)$ can be k-cheating-immune only if $k < n - t_1$.*

8 Conclusions and Open Problems

We have studied some properties and constraints holding for cheating-immune secret sharing schemes. We have shown that a perfect secret sharing scheme cannot be cheating-immune, and we have given an upper bound on the number of tolerated cheaters in such schemes. Then, we have repaired an existing construction to realize cheating-immune secret sharing schemes. Interesting open problems are secret sharing constructions for threshold and general (ideal) access structures. Another interesting research line could be the generalization of the definition of cheating-immunity: at the moment, it is implicitly assumed that the secrets are chosen by the dealer *uniformly* at random. If the dealer chooses the secret according to a certain probability distribution on the space of secrets, we have to require that, when the cheaters submit fake shares, the probability distribution that they infer over the set of possible true secrets (once the incorrect secret has been reconstructed) must be the same as the one that the honest participants infer (i.e., there is no advantage for the cheaters compared to the honest users).

9 Acknowledgement

D. R. Stinson's research is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through grant RGPIN 203114-02.

References

[1] G. R. Blakley. Safeguarding Cryptographic keys, in *AFIPS Conference Proceedings*, vol. 48, 1979, pp. 313–317.

[2] G. R. Blakley and C. Meadows. Security of Ramp Schemes, *Lecture Notes in Computer Science* **196** (1985), 242–268 (CRYPTO '84).

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, in *Proceedings of STOC '88*, 1988, pp. 1–10.

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

[5] M. Carpentieri, A. De Santis, and U. Vaccaro. Size of shares and probability of cheating in threshold schemes, *Lecture Notes in Computer Science* **765** (1993), 118–125 (EUROCRYPT '93).

[6] D. Chaum. C. Crépeau, and I. Damgård. Multiparty Unconditionally Secure Protocols, in *Proceedings of STOC '88*, 1988, pp. 11–19.

[7] B. Chor, S. Goldwasser, S. Micali, and B. Awerbach. Verifiable Secret Sharing and Achieving Simultaneity in Presence of Faults, in *Proceedings of FOCS '85*, 1985, pp. 383–395.

[8] T. M. Cover and J. A. Thomas. *Elements of Information Theory*, John Wiley & Sons, 1991.

[9] P. Feldman. Non-interactive and Information Theoretic Secure Verifiable Secret Sharing, in *Proceedings of FOCS '87*, 1987, pp. 427–437.

[10] J. Pieprzyk and X. M. Zhang. Cheating Prevention in Secret Sharing over $GF(P^t)$, *Lecture Notes in Computer Science* **2247** (2001), 79–90 (INDOCRYPT '01).

[11] J. Pieprzyk and X. M. Zhang. Constructions of Cheating Immune Secret Sharing, *Lecture Notes in Computer Science* **2288** (2001), 226–243 (ICISC '01).

[12] T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority, in *Proceedings of STOC '89*, 1989, pp. 73–85.

[13] A. Shamir. How to Share a Secret, *Communications of the ACM* **22** (1979), 612–613.

[14] D. R. Stinson. An Explication of Secret Sharing Schemes, *Designs, Codes and Cryptography* **2** (1992), 357–390.

[15] D. R. Stinson and R. Wei. Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures. *Lecture Notes in Computer Science* **1758** (2000), 200–214 (SAC '99).

[16] M. Tompa and H. Woll. How to Share a Secret with Cheaters, *Journal of Cryptology* **1** (1988), 133–138.

[17] X. M. Zhang and J. Pieprzyk. Cheating Immune Secret Sharing, *Lecture Notes in Computer Science* **2229** (2001), 144–149 (ICICS '01).

A Entropy Function

This appendix briefly recalls some elements of information theory. However, the reader is encouraged to consult [8] for details.

Let $\mathbf{X}$ be a random variable taking values on a set X according to a probability distribution $\{P_{\mathbf{X}}(x)\}_{x\in X}$. The *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, is defined as

$$H(\mathbf{X}) = -\sum_{x\epsilon X} P_{\mathbf{X}}(x) \log P_{\mathbf{X}}(x),$$

where the logarithm is to the base 2. The entropy function satisfies the inequality

$$0 \leq H(\mathbf{X}) \leq \log |X|,$$

where $H(\mathbf{X}) = 0$ if and only if there exists $x_0 \in X$ such that $Pr(\mathbf{X} = x_0) = 1$; whereas, $H(\mathbf{X}) = \log |X|$ if and only if $Pr(\mathbf{X} = x) = 1/|X|$, for all $x \in X$. The entropy of a random variable is usually interpreted as

- a measure of the equidistribution of the random variable
- a measure of the amount of information given on average by the random variable.

Given two random variables $\mathbf{X}$ and $\mathbf{Y}$ taking values on sets X and Y, respectively, according to the joint probability distribution $\{P_{\mathbf{XY}}(x, y)\}_{x \in X, y \in Y}$ on their cartesian product, the *conditional entropy* $H(\mathbf{X}|\mathbf{Y})$ is defined as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y \in Y} \sum_{x \in X} P_{\mathbf{Y}}(y) P_{\mathbf{X}|\mathbf{Y}}(x|y) \log P_{\mathbf{X}|\mathbf{Y}}(x|y).$$

It is easy to see that

$$H(\mathbf{X}|\mathbf{Y}) \geq 0,$$

with equality if and only if X is a function of Y. The conditional entropy is a measure of the amount of information that $\mathbf{X}$ still has, given $\mathbf{Y}$.