On Cheating-Immune Secret Sharing

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 Combinatorics and Optimization
University of Waterloo, N2L 3G1, Waterloo Ontario, Canada
email: wkishimoto@cacr.math.uwaterloo.ca

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

Abstract

Cheating-immune secret sharing schemes are secret sharing schemes where dishonest participants, during the reconstruction phase, have *no advantage* in submitting incorrect shares (i.e., cheating), compared to honest participants. In particular, they get no information at all on the *true secret* that would be reconstructed if they submit correct shares. In this paper we study properties and constraints holding for 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 tolerated cheaters in such schemes, and we propose a modified version of an existing construction to realize cheating-immune secret sharing schemes. Finally, we discuss some open problems.

1 Introduction

Secret sharing schemes are a fundamental primitive in Cryptography. In the basic model, a secret sharing scheme is a protocol divided in two phases: *Share* and *Reconstruct*. During *Share*, a dealer distributes a secret among a set of participants by sending each of them a piece of information, called a *share*. Then, during *Reconstruct*, some subsets of participants, called *qualified*, can reconstruct the secret either by pooling together their shares or by sending their shares to a *combiner* that collects the shares, reconstructs the secret, and sends it back to these participants; while, some other subsets, called *forbidden*, do not learn any information about the secret. In such a model, dealer and participants are *supposed to be* honest.

However, many applications have to deal with the case of dishonest participants and, possibly, of a dishonest dealer. Tompa and Woll in [9], showed that secret sharing schemes

* 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.

where the function for reconstructing the secret is *linear* (e.g., Shamir's scheme) can be subject to the following attack: some dishonest participants, during *Reconstruct*, can submit fake shares. Hence, the reconstructed secret is different from the original one. But, from this secret and their true shares, these dishonest users can recover the original secret.

In order to design secret sharing schemes that keep working even in hostile environments, the concept of *verifiability* was introduced in [3]. With this approach, some *extra information* is used to enable users to detect a dishonest dealer, who sends inconsistent shares during *Share*, and to verify that during *Reconstruct* each user submits a correct share. A lot of research has been done along this line for both unconditionally secure and computationally secure verifiable secret sharing schemes.

A different approach was suggested last year in [10, 5, 6]. The dealer is *assumed to be honest*: Only participants can cheat during *Reconstruct*, by submitting incorrect shares, in order to gain some advantage upon honest users. In this setting, the secret sharing scheme is said to be *cheating-immune* if cheaters have *no advantage at all* in submitting incorrect shares. As it has been pointed out in [10, 5, 6], this property strongly depends on the *structure* of the reconstruction function used in the secret sharing scheme. In this paper we continue the study of such a model, showing some new results.

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 [5], and in Section 4 we recall a characterization for such schemes; while, in Section 5, we point out a relation with resilient functions, which enable us to prove an upper bound on the number of possible cheaters in any (n, N) threshold scheme. Finally, in Section 6, we describe a new construction for cheating-immune secret sharing schemes, and in Section 7 we state some result for the case of ramp schemes.

2 Perfect Secret Sharing Scheme

Secret sharing were introduced in 1979 by Blakley [1] and Shamir [7]. The reader can find an introduction and references to the literature in [8].

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[1], 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 $H(\mathbf{S}|\mathbf{A}) = H(\mathbf{S})$.

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

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 participant gets absolutely no information about the secret. When 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 [8].

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 for $\mathcal{A}$. Secret sharing schemes with information rate equal to one, which is the maximum possible value of this parameter (i.e., secret and 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* the shares held by n participants are required to reconstruct the secret. The model and the notation are the same used in [5].

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 the Share. The secret sharing scheme Σ is represented by a *defining* function,

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

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,

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

The first set represents the possible shares held by honest participants, enabling the reconstruction of the true secret K, if cheaters behave 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 *[5] 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* cheaters submit fake shares. A more general definition takes into account the possibility that *some* 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 *[5] An (n, n)-SSS with shares and values in $GF(p^t)$ is said to be strictly k-cheating-immune if, for any vector $\delta \in GF(2)^n$, for any $\tau \in GF(p^t)^n)$, such that $\tau \preceq \delta$, $1 \leq HW(\delta) \leq HW(\tau) \leq k$, and every $\alpha \in GF(p^t)^n$, 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 a secret sharing scheme with access structure $\mathcal{A}$ on the set of participants $\mathcal{P}$. If Σ is perfect, then Σ cannot be cheating-immune.*

Proof. For simplicity, assume that Σ is an (n,n)-SSS, and the set of 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 $1 \Leftrightarrow b$. 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. The same argument can be used for the case in which the set of shares and secrets is $GF(p^t)$, and when considering a general access structure $\mathcal{A}$ defined over $\mathcal{P}$. ■

The structure of the defining function f of a cheating-immune secret sharing scheme can be precisely characterized. The following result was shown in [5]. We recall it[2].

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

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 [6, 10]. We use it to state an upper bound on the number of possible cheaters 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 $K \in GF(p^t)$*

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

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

[2] In the full version of the paper we will propose a slightly simplified proof, compared to the one given in [5], of this characterization.

Notice that, if $f : GF(p^t)^n \rightarrow GF(p^t)$ is the defining function of an (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.

About k-cheating-immune secret sharing schemes, from Theorem 4.2, the next corollary easily follows:

Corollary 5.3 *Let Σ be an (n,n)-SSS, and let $f : GF(p^t)^n \rightarrow GF(p^t)$ 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 $f : GF(p^t)^n \rightarrow GF(p^t)$ be the defining function of Σ. If Σ is k-cheating-immune, then f cannot be $(n \Leftrightarrow k)$-resilient.*

Proof. Omitted from this extended abstract, due to lack of space.

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

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

Proof. Notice that a k-resilient function is also s-resilient, for any $1 \leq s < k$. This observation, Theorem 5.4, and Corollary 5.3, imply the result. ■

The above upper bound on the number of cheaters holds even for the case of strictly k-cheating-immune secret sharing. Indeed, in the worst case a strictly k-cheating-immune secret sharing is exactly a k-cheating-immune secret sharing (i.e., when all the 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 [5]. Basically, we use of *a new* function μ as a building block for the scheme, instead of the function λ therein described [3].

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 $a \in GF(p^t)^n$, $b_p^+ a$ ($b_p^- a$, 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 *[5] 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 $h(x_\delta^- + \delta + \tau) \Leftrightarrow h(x_\delta^- + \tau)$ is a non-constant affine function.*

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

Lemma 6.2 *[5] Let a function f of degree two on $GF(P^t)^n$ do not have a nonzero constant term; in other words, $f(0,\ldots,0) = 0$, where 0 denotes the zero element in $GF(p^t)^n$. Then, f is balanced $\Leftrightarrow$ there exists a nonzero vector $\alpha \in GF(p^t)^n$ such that $f(x+\alpha) \Leftrightarrow f(x)$ is constant and $f(\alpha) \neq 0$.*

[3] Unfortunately, the function λ proposed in [5] is not balanced, as the construction requires.

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

Lemma 6.3 *Let $n \geq 2k+1$, and let $\mu_{n,p} : GF(p^t)^n \rightarrow GF(p^t)$ 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 $g = \mu_{n,p} \Leftrightarrow x_1$. 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 $\lceil n/2 \rceil \cdot p$ 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, $g(x + \alpha) \Leftrightarrow g(x)$ produces $2p$ single x_1 terms. Therefore, it is easy to verify $g(x + \alpha) \Leftrightarrow g(x) = 0$. Hence, $\mu_{n,p}(x + \alpha) \Leftrightarrow \mu_{n,p}(x) = 1$, 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 $X_i = \{[i \Leftrightarrow 1]_{(n)}, i, [i+1]_{(n)}\}$. It can be easily seen that no quadratic term exists in $\mu_{n,p}(x_\delta^+ + \tau + \delta) \Leftrightarrow \mu_{n,p}(x_\delta^+ + \tau)$. 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 $\mu_{n,p}(x_\delta^+ + \tau + \delta) \Leftrightarrow \mu_{n,p}(x_\delta^+ + \tau)$. To this aim notice that, since $n \geq 2k+1$, there exists an i such that $X_i \cap J = \{[i \Leftrightarrow 1]_{(n)}\}$. Let i_0 be such that $X_{i_0} \cap J = \{[i_0 \Leftrightarrow 1]_{(n)}\}$. Then $\delta_{[i_0-1]_{(n)}} \neq 0$, and $\delta_{i_0} = \delta_{[i_0+1]_{(n)}} = 0$. Hence, in $\mu_{n,p}(x_\delta^+ + \tau + \delta) \Leftrightarrow \mu_{n,p}(x_\delta^+ + \tau)$, 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, $\mu_{n,p}(x_\delta^+ + \tau + \delta) \Leftrightarrow \mu_{n,p}(x_\delta^+ + \tau)$ includes a linear term x_{i_0}, which ensures that $\mu_{n,p}$ has the property $B(k)$.

■

According to the strategy defined by Lemma 5 and Theorem 5 in [5], using μ as a building block, we can construct a k-cheating-immune secret sharing scheme.

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 [4], 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 $f : GF(p^t)^n \rightarrow GF(p^t)$ can be k-cheating-immune only if $k < n \Leftrightarrow t_1$.*

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 revised 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 the honest participants infer (i.e., no advantage for the cheaters compared to the honest users).

References

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

[2] G.R. Blakley and C. Meadows, *Security of Ramp Schemes*, CRYPTO 1984, LNCS 196, pp. 242-268, 1984.

[3] B. Chor, S. Goldwasser, S. Micali, and B. Awerbach. *Verifiable Secret Sharing and Achieving Simultaneity in Presence of Faults*, Proc. of the 26-th Annual Symposium on the Foundations of Computer Science, IEEE, pp. 383–395, 1985.

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

[5] J. Pieprzyk and X. M. Zhang, *Cheating Prevention in Secret Sharing over $GF(P^t)$*, INDOCRYPT 2001, LNCS 2247, pp. 79–90, 2001.

[6] J. Pieprzyk and X. M. Zhang, *Constructions of Cheating Immune Secret Sharing* ICISC 2001, LNCS 2288, pp. 226–243, 2001.

[7] A. Shamir, *How to Share a Secret* Communications of ACM, vol. 22, n. 11, pp. 612–613, 1979.

[8] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Designs, Codes and Cryptography, Vol. 2, pp. 357-390, 1992.

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

[10] X. M. Zhang and J. Pieprzyk *Cheating Immune Secret Sharing*, ICICS 2001, LNCS 2229, pp. 144–149, 2001.

A Entropy Function

This appendix briefly recalls some elements of information theory (the reader is referred to [4] 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

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

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

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

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

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

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, once given $\mathbf{Y}$.