Multisecret Sharing Immune against Cheating

Josef Pieprzyk and Xian-Mo Zhang
Department of Computing
Macquarie University
Sydney , NSW 2109, AUSTRALIA
E-mail: josef,xianmo@ics.mq.edu.au

February 23, 2003

Abstract

Cheating in multisecret sharing is considered. Multisecret sharing is defined by a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$ that provides a generic model. In this model, we propose nonlinear multisecret sharing that is immune against cheaters. Two cheating strategies are considered. In the first one, all cheaters always submit their invalid shares and they collectively know their own valid shares. In the second one, some cheaters may submit their valid shares while again sharing their knowledge about their valid shares. The combiner (or recovery algorithm) interacts with shareholders by collecting shares from them and distributing the recovered secrets back to active participants. Two different scenarios are considered when the combiner recreates all secrets (this is simultaneous recovery) or gradually (so called sequential recovery). Probabilities of successful cheating are derived and constructions for cheating immune multisecret sharing are given.
Keywords: Secret Sharing, Multisecret Secret Sharing, Cheating Immune Secret Sharing

1 Introduction

Cheating prevention in secret sharing and group oriented cryptography becomes one of the central security issues. Roughly saying, secret sharing is cheater-immune if a cheater is not better off than a participant who follows the protocol honestly. Tompa and Woll [8] demonstrated how Shamir secret sharing can be subject to cheating so after the recovery phase, honest participants are left with an invalid secret while cheaters are able to compute the valid one.

The problem of cheating prevention was investigated in [6]. It was shown that secret sharing can be constructed in such a way that cheaters after revealing an invalid secret by the combiner (or recovery algorithm), are getting no information about the valid secret. In a sense, the knowledge about the valid secret of honest and dishonest participants is the same with an obvious exception that cheaters know that the recovered secret is invalid while the honest ones will learn about this fact later when the recovered secret fails to trigger the intended action.

Multisecret sharing was probably first discussed in [5]. General formulation of the problem for the case when m different secrets are shared among participants with a single access structure was studied in [1]. Some further works can be found in [3, 4, 2].

Clearly, cheating participants in multisecret sharing schemes have more possibilities to deviate during the reconstruction of secrets depending on how the combiner who collects shares is working and also how the secrets are reconstructed. To make our considerations explicit we assume a simple multisecret sharing model in which every n participants can recover the secrets. The combiner who reconstructs the secrets can return all secrets (parallel reconstruction) or secret by secret (sequential reconstruction) where secrets are recreated in a some publicly known order. ¿From now on we assume that the combiner is implemented in such a way that it accepts shares and after getting the appropriate number of them, reveals the

reconstructed secret to all active participants (shares are never revealed by the combiner). This of course, does not restrict dishonest participants who may reveal their shares to each other.

2 Notations

Multisecret sharing is defined by a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. F is called the defining mapping (or distribution rule) and is publicly accessible. Each vector $\alpha \in GF(p^t)^n$ determines a collection of n shares held by n participants and the vector $F(\alpha) \in GF(p^t)^m$ specifies a collection of m secrets. In particular, when $m = 1$, the defining mapping becomes the defining function that was studied in [6].

We consider two basic cheating strategies that are possible for dishonest participants to undertake. The strategies characterise the way the combiner works:

• simultaneous recovery of all secrets – in this case dishonest participants can modify all their shares or perhaps, they can collectively decide that some portion of their valid shares will be submitted to the combiner (those two scenarios will be considered). Note that the knowledge of cheaters is restricted to the shares they hold,

• sequential recovery of secrets – again dishonest participants submit a collection of invalid shares to the combiner who returns a single secret. The recovery process of a single secret is independent as dishonest participants can deliver a different collection of invalid shares for each recovery. Observe that the knowledge of cheaters changes after each recovery as they obtain a secret returned by the combiner.

We assume that the combiner is honest and returns the secret corresponding to the submitted shares and after the recovery it "forgets" all shares and secrets.

Let $GF(p^t)$ denote a finite field with p^t elements where p is a prime number and t is a positive integer. We write $GF(p^t)^n$ to denote the vector space of n tuples of elements from $GF(p^t)$. Then each vector $\alpha \in GF(p^t)^n$ can be expressed as $\alpha = (a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in GF(p^t)$. The *Hamming weight* of a vector $\alpha \in GF(p^t)^n$, denoted by $HW(\alpha)$, is the number of nonzero coordinates of α.

We consider a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$ written either $F(x)$ or $F(x_1, \ldots, x_n)$ where $x = (x_1, \ldots, x_n)$ and each $x_j \in GF(p^t)$. F is said to be *regular* if $F(x)$ takes each vector in $GF(p^t)^m$ precisely $p^{t(n-m)}$ times while x goes through each vector in $GF(p^t)^n$ once. A regular mapping $GF(p^t)^n \longrightarrow GF(p^t)^m$ exists only when $n \geq m$. A mapping f: $GF(p^t)^n \longrightarrow GF(p^t)$ is called a *function* on $GF(p^t)^n$. A regular function f is also called a *balanced* function. A mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$ can be expressed as $F = (f_1, \ldots, f_m)$ or $F(x) = (f_1(x), \ldots, f_m(x))$, where each coordinate f_j is a function on $GF(p^t)^n$ and $x \in GF(p^t)^n$.

Let $x = (x_1, \ldots, x_n)$ and $\delta = (\delta_1, \ldots, \delta_n)$ be two vectors in $GF(p^t)^n$. Define a vector $x_\delta^+ \in GF(p^t)^n$, whose j-th coordinate is x_j if $\delta_j \neq 0$, or 0 if $\delta_j = 0$. In addition, we define a vector $x_\delta^- \in GF(p^t)^n$, whose j-th coordinate is 0 if $\delta_j \neq 0$, or x_j if $\delta_j = 0$. Clearly $(\beta+\gamma)_\delta^+ = \beta_\delta^+ + \gamma_\delta^+$, $(\beta+\gamma)_\delta^- = \beta_\delta^- + \gamma_\delta^-$ and $\beta_\delta^+ + \beta_\delta^- = \beta$ hold for any $\beta, \gamma \in GF(p^t)^n$, also $\delta_\delta^+ = \delta$, $\delta_\delta^- = 0$. Let $\tau = (\tau_1, \ldots, \tau_n)$ and $\delta = (\delta_1, \ldots, \delta_n)$ be two vectors in $GF(p^t)^n$. We write $\tau \preceq \delta$ to denote the property that if $\tau_j \neq 0$ then $\delta_j \neq 0$. In addition, we write $\tau \prec \delta$ to denote the property that $\tau \preceq \delta$ and $HW(\tau) < HW(\delta)$. Clearly if $\tau \preceq \delta$ then $\tau + \delta \preceq \delta$. In particular, if $\delta' \preceq \delta$ and $HW(\delta') = HW(\delta)$ we write $\delta \bowtie \delta'$. It is easy to verify that $\delta \bowtie \delta' \Longleftrightarrow \delta' \preceq \delta$ and $\delta \preceq \delta' \Longleftrightarrow$ both $x_\delta^+ = x_{\delta'}^+$ and $x_\delta^- = x_{\delta'}^-$ hold for any $x \in GF(p^t)^n$, where $\Longleftrightarrow$ denotes "if and only if".

3 Simultaneous Recovery of Secrets with Cheaters using Invalid Shares only

3.1 Probability of Successful Cheating

In this work we use a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$ that defines a multisecret sharing. Let δ be a nonzero vector in $GF(p^t)^n$, $\tau \preceq \delta$ and $\mu \in GF(p^t)^m$. F can be equivalently represented in the form of table $\mathcal{T}$ with rows containing $(\alpha, F(\alpha))$. Set $R_F(\delta, \tau, \mu) = \{x_\delta^- \mid F(x_\delta^- + \tau) = \mu\}$. We also simply write $R_F(\delta, \tau, \mu)$ as $R(\delta, \tau, \mu)$ if no confusion occurs. The following statement can be formulated.

Lemma 1 *Let δ be a nonzero vector in $GF(p^t)^n$, $\tau \in GF(p^t)^n$, $\tau \preceq \delta$, and $\mu \in GF(p^t)^m$. Then for any given*

mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$, (i) $R(\delta,\tau,\mu) = R(\delta',\tau,\mu)$ if $\delta \bowtie \delta'$, (ii) $R(\delta,\alpha_\delta^+,\mu) = R(\delta,\gamma_\delta^+,\mu)$ for any $\alpha,\gamma \in GF(p^t)^n$ with $\alpha_\delta^+ = \gamma_\delta^+$, (iii) there exists some $\mu \in GF(p^t)^m$ such that $R(\delta,\tau,\mu) \neq \emptyset$, where $\emptyset$ denotes the empty set.

Given a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. We introduce the following notations:

• Let $\alpha \in GF(p^t)^n$ be the sequence of n shares held by the group $\mathcal{P} = \{P_1,\ldots,P_n\}$ of n participants and the multisecret $\mu = F(\alpha)$.

• The collection of cheaters is determined by the sequence $\delta = (\delta_1,\delta_2,\ldots,\delta_n)$ where P_i is a cheater $\Longleftrightarrow$ δ_i is nonzero.

• At the pooling time, the cheaters submit their shares. It is assumed that the cheaters always submit invalid shares. The honest participants always submit their valid shares. We consider the vector $\alpha+\delta$. From the properties of α_δ^+ and α_δ^-, we can write that $\alpha+\delta = \alpha_\delta^- + \alpha_\delta^+ + \delta$. Thus the combiner obtains $\alpha+\delta$ that splits into two parts: α_δ^- – the part submitted by honest participants, and $\alpha_\delta^+ + \delta$ – the part submitted by the cheaters. The combiner (or recovery algorithm) returns an invalid multisecret $\mu^* = F(\alpha+\delta)$. Note that the cheaters always change their shares. We assume that there exists at least one cheater, in other words, δ is nonzero or $HW(\delta) > 0$.

• α_δ^+ determines valid shares held by the cheaters. The set $R(\delta,\alpha_\delta^+,\mu)$, or $\{x_\delta^- | F(x_\delta^- + \alpha_\delta^+) = \mu\}$, determines a collection of rows of $\mathcal{T}$ with the correct multisecret μ and valid shares held by the cheaters.

• The set $R(\delta,\alpha_\delta^+ + \delta,\mu^*)$, or $\{x_\delta^- | F(x_\delta^- + \alpha_\delta^+ + \delta) = \mu^*\}$, represents the view of the cheaters after getting back μ^* from the combiner.

In this work the *cheating* means the action of cheaters by submitting incorrect shares, and *successful cheating* means the case that the cheaters not only submit incorrect shares but also guess the correct secret.

The mapping F is called the *defining mapping* as it determines the multisecret sharing. The nonzero vector $\delta = (\delta_1,\ldots,\delta_n)$ is called a *cheating vector*, α is called an *original vector*. The value of $\rho_{\delta,\alpha} = \#(R(\delta,\alpha_\delta^+ + \delta,\mu^*) \cap R(\delta,\alpha_\delta^+,\mu))/\#R(\delta,\alpha_\delta^+ + \delta,\mu^*)$, expresses the probability of successful cheating with respect to δ and α, where $\#X$ denotes the number of elements in the set X. As an original vector α is always in $R(\delta,\alpha_\delta^+ + \delta,\mu^*) \cap R(\delta,\alpha_\delta^+,\mu)$, the probability of successful cheating always satisfies $\rho_{\delta,\alpha} > 0$. Clearly the number of cheaters is equal to $HW(\delta)$.

Theorem 1 *Given a multisecret sharing scheme with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Let $\delta \in GF(p^t)^n$ with $0 < HW(\delta) < n$ be a cheating vector and α be an original vector in $GF(p^t)^n$. If $\rho_{\delta,\alpha} < p^{-tm}$ then there exists a vector $\gamma \in GF(p^t)^n$ such that $\rho_{\delta,\gamma} > p^{-tm}$.*

Proof Let $F(\alpha) = \mu$ and $F(\alpha+\delta) = \mu^*$. By definition, $R(\delta,\alpha_\delta^+,\mu) = \{x_\delta^- | F(x_\delta^- + \alpha_\delta^+) = \mu\}$ and $R(\delta,\alpha_\delta^+ + \delta,\mu^*) = \{x_\delta^- | F(x_\delta^- + \alpha_\delta^+ + \delta) = \mu^*\}$. We partition $R(\delta,\alpha_\delta^+ + \delta,\mu^*)$ into p^{tm} parts: $R(\delta,\alpha_\delta^+ + \delta,\mu^*) = \cup_{\lambda \in GF(p^t)^m} Q_\lambda$ where $Q_\lambda = R(\delta,\alpha_\delta^+ + \delta,\mu^*) \cap R(\delta,\alpha_\delta^+,\lambda+\mu)$. Clearly

$$\#R(\delta,\alpha_\delta^+ + \delta,\mu^*) = \sum_{\lambda \in GF(p^t)^m} \#Q_\lambda \qquad (1)$$

Note that $R(\delta,\alpha_\delta^+ + \delta,\lambda^*) \cap R(\delta,\alpha_\delta^+,\lambda) = Q_0$. Therefore

$$\begin{aligned}&\rho_{\delta,\alpha} = \\ &\#(R(\delta,\alpha_\delta^+ + \delta,\mu^*) \cap R(\delta,\alpha_\delta^+,\mu))/\#R(\delta,\alpha_\delta^+ + \delta,\mu^*) \\ &= \#Q_0/\#R(\delta,\alpha_\delta^+ + \delta,\mu^*) \qquad (2)\end{aligned}$$

Since $\rho_{\delta,\alpha} < p^{-tm}$, from (2), $\#Q_0/\#R(\delta,\alpha_\delta^+ + \delta,\mu^*) < p^{-tm}$. It follows that

$$\#Q_0 < p^{-tm}\#R(\delta,\alpha_\delta^+ + \delta,\mu^*) \qquad (3)$$

¿From (1) and (3), we know that $\sum_{\lambda \in GF(p^t)^m, \lambda \neq 0} \#Q_\lambda > (1-p^{-tm})\#R(\delta,\alpha_\delta^+ + \delta,\mu^*)$. Thus there exists some $\lambda' \in GF(p^t)^m$ with $\lambda' \neq 0$ such that $\#Q_{\lambda'} > p^{-tm}\#R(\delta,\alpha_\delta^+ + \delta,\mu^*)$. By definition, $Q_{\lambda'} = \{x_\delta^- | F(x_\delta^- + \alpha_\delta^+ + \delta) = \mu^*, F(x_\delta^- + \alpha_\delta^+) = \lambda' + \mu\}$. Then there exists a vector $\beta_\delta^- \in Q_\nu$ and then $F(\beta_\delta^- + \alpha_\delta^+ + \delta) = \mu^*$, $F(\beta_\delta^- + \alpha_\delta^+) = \lambda' + \mu$. Set $\gamma = \beta_\delta^- + \alpha_\delta^+$. Thus $F(\gamma+\delta) = \mu^*$ and $F(\gamma) = \lambda' + \mu$. Clearly $\gamma_\delta^+ = \alpha_\delta^+$ and $\gamma_\delta^- = \beta_\delta^-$. Next we choose γ as an original vector. Due to $R(\delta,\gamma_\delta^+ + \delta,\mu^*) = \{x_\delta^- | F(x_\delta^- + \gamma_\delta^+ + \delta) = \mu^*\}$, $R(\delta,\gamma_\delta^+,\lambda' + \mu) = \{x_\delta^- | F(x_\delta^- + \gamma_\delta^+) = \lambda' + \mu\}$ and $\gamma_\delta^+ = \alpha_\delta^+$, we know that $R(\delta,\gamma_\delta^+ + \delta,\mu^*) \cap R(\delta,\gamma_\delta^+,\lambda' + \mu) = Q_{\lambda'}$ and $\rho_{\delta,\gamma} = \#(R(\delta,\gamma_\delta^+ + \delta,\mu^*) \cap R(\delta,\gamma_\delta^+,\lambda' + \mu))/\#R(\delta,\gamma_\delta^+ + \delta,\mu^*) = \#Q_{\lambda'}/\#R(\delta,\gamma_\delta^+ + \delta,\mu^*) = \#Q_{\lambda'}/\#R(\delta,\alpha_\delta^+ + \delta,\mu^*) > p^{-tm}$.

Corollary 1 *Given a multisecret sharing scheme with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Then $\max\{\rho_{\delta,\alpha} | \alpha \in GF(p^t)^n\} \geq p^{-tm}$ for any fixed nonzero vector $\delta \in GF(p^t)^n$.*

3.2 k-Cheating Immune Multisecret Sharing

Given a multisecret sharing with its defining mapping F on $GF(p^t)^n$. For a fixed nonzero $\delta \in GF(p^t)^n$, due to Theorem 1, it is desirable that $\rho_{\delta,\alpha} = p^{-tm}$ holds for every $\alpha \in GF(p^t)^n$. A multisecret sharing is said to be *k-cheating immune* if $\rho_{\delta,\alpha} = p^{-tm}$ holds for every $\delta \in GF(p^t)^n$ with $1 \leq HW(\delta) \leq k$ and every $\alpha \in GF(p^t)^n$.

Theorem 2 *Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Then the multisecret sharing is k-cheating immune $\Longleftrightarrow$ for any integer l with $1 \leq l \leq k$, any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, any $\tau \preceq \delta$ and any $\mu, \nu \in GF(p^t)^m$, the following conditions hold simultaneously: (i) $\#R(\delta, \tau, \nu) = p^{t(n-l-m)}$, (ii) $\#(R(\delta, \tau, \nu) \cap R(\delta, \tau + \delta, \mu)) = p^{t(n-l-2m)}$.*

The proof is given in the Appendix.

Theorem 3 *Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Then the following statements are equivalent: (i) the multisecret sharing is k-cheating immune, (ii) for any integer l with $1 \leq l \leq k$, any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, any $\tau \preceq \delta$ and any $\mu, \nu \in GF(p^t)^m$, we have $\#(R(\delta, \tau, \nu) \cap R(\delta, \tau + \delta, \mu)) = p^{t(n-l-2m)}$, (iii) for such l, δ, τ, μ and ν mentioned in (ii), the system of equations: $\begin{cases} F(x_\delta^- + \tau + \delta) = \mu \\ F(x_\delta^- + \tau) = \nu \end{cases}$ has precisely $p^{t(n-l-2m)}$ solutions on x_δ^-.*

Proof Clearly (ii) $\Longleftrightarrow$ (iii). Due to Theorem 2, (i) $\Longrightarrow$ (ii). To complete the proof, we only need prove that (ii) $\Longrightarrow$ (i). Assume that (ii) holds. Thus $\#(R(\delta, \tau, \nu) \cap R(\delta, \tau + \delta, \mu)) = p^{t(n-l-2m)}$ for every $\mu, \nu \in GF(p^t)^m$. Note that $R(\delta,\tau,\nu) = \cup_{\mu \in GF(p^t)^m} R(\delta, \tau, \nu) \cap R(\delta, \tau + \delta, \mu)$ and then $\#R(\delta, \tau, \nu) = \sum_{\mu \in GF(p^t)^m} \#(R(\delta, \tau, \nu) \cap R(\delta, \tau + \delta, \mu))$. This proves that $\#R(\delta, \tau, \nu) = p^{t(n-l-m)}$. Using Theorem 2, we have proved that (i) holds.

Corollary 2 *Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. If the multisecret sharing is k-cheating immune, then (i) $n \geq 2m + k$, (ii) F is regular.*

Proof Let $l = k$ in Theorem 2, we have $\#(R(\delta, \tau, \nu) \cap R(\delta, \tau + \delta, \mu)) = p^{t(n-k-2m)} \geq 1$. This proves that $n \geq 2m + k$. Again from Theorem 2 we have $\#R(\delta, \tau, \nu) = p^{t(n-k-m)}$, for any $\tau \preceq \delta$ and any $\nu \in GF(p^t)^m$. This means that for each fixed τ with $\tau \preceq \delta$, the mapping $F(x_\delta^- + \tau)$ is regular. Thus the mapping F is regular.

Due to Corollary 2, a k-cheating immune multisecret sharing, defined by a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$, exists only when $n \geq 2m + k$.

4 Simultaneous Recovery of Secrets with Cheaters using Valid and Invalid Shares

4.1 Probability of Successful Cheating

Given a mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. We introduce the following notations. As before we can see F as a table $\mathcal{T}$ with rows containing $(\delta, F(\delta))$. We also assume that the combiner returns all secrets (or the multisecret for short).

• Let $\alpha \in GF(p^t)^n$ be the sequence of shares held by the group $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants and the secret $\mu = F(\alpha)$.

• The collection of cheaters is determined by the sequence $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$ where P_i is a cheater $\Longleftrightarrow$ if $\delta_i \neq 0$.

• 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. The collection of cheaters who submit invalid shares is determined by the sequence $\tau = (\tau_1, \ldots, \tau_n)$ where $\tau_j = 0 \Longleftrightarrow P_j$ is honest or P_j is a cheater who submits a valid share, in other words, $\tau_j \neq 0 \Longleftrightarrow P_j$ is a cheater who submits an invalid share. 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 $\alpha + \tau$. Due to the properties of operations α_δ^+ and α_δ^-, we can write $\alpha + \tau = \alpha_\delta^- + \alpha_\delta^+ + \tau$. The combiner obtains $\alpha + \tau$ that splits into two parts: α_δ^-

– the part submitted by honest participants and $\alpha_\delta^+ + \tau$ the part submitted by cheaters. The combiner returns an invalid multisecret $\mu^* = F(\alpha + \tau)$.

• $R(\delta, \alpha_\delta^+ + \tau, \mu^*)$, or $\{x_\delta^- | F(x_\delta^- + \alpha_\delta^+ + \tau) = \mu^*\}$, where α_δ^+ determines valid shares held by the cheaters, represents the view of the cheater after getting back μ^* from the combiner.

• The set $R(\delta, \alpha_\delta^+, \mu)$, or $\{x_\delta^- | f(x_\delta^- + \alpha_\delta^+) = \mu\}$, determines a collection of rows of $\mathcal{T}$ with the correct multisecret μ and valid shares held by the cheaters.

As mentioned in Section 3, the cheating means the action of cheaters by submitting incorrect shares, and successful cheating means the case when cheaters are able to guess the correct secret.

In generalised model of cheating, τ is used to determine how to cheat while δ is only used to determine which participants are dishonest, therefore we can define δ as a $(0, 1)$-vector in $GF(p^t)^n$. However, in basic model of cheating, δ is not only used to determine which participants are dishonest but also used to determine how to cheat, thus δ has a more general form.

The mapping F is called the *defining mapping* of multisecret sharing. We assume that the combiner returns multisecrets (all secrets). The nonzero vector $\delta = (\delta_1, \ldots, \delta_n)$ is called a *cheating vector*, the nonzero vector $\tau \preceq \delta$ is called an *active cheating vector*, α is called an *original vector*. The value of $\rho_{\delta,\tau,\alpha} = \#(R(\delta, \alpha_\delta^+ + \tau, \mu^*) \cap R(\delta, \alpha_\delta^+, \mu))/\#R(\delta, \alpha_\delta^+ + \tau, \mu^*)$ expresses the probability of successful cheating with respect to δ, τ and α. As an original vector α is always in $R(\delta, \alpha_\delta^+ + \tau, \mu^*) \cap R(\delta, \alpha_\delta^+, \mu)$, 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 basic model of cheating.

4.2 Strictly k-cheating Immune Multisecret Sharing

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

Theorem 4 *Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Let $\delta \in GF(p^t)^n$; $0 < HW(\delta) < n$, be a cheating vector, let $\tau \preceq \delta$; $\tau \neq 0$, be an active cheating vector, and let $\alpha \in GF(p^t)^n$ be an original vector (representing valid shares). If $\rho_{\delta,\tau,\alpha} < p^{-tm}$ then there exists a vector $\gamma \in GF(p^t)^n$ such that $\rho_{\delta,\tau,\gamma} > p^{-tm}$.*

Corollary 3 *Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Then $\max\{\rho_{\delta,\tau,\alpha} \mid \alpha \in GF(p^t)^n\} \geq p^{-tm}$ for any fixed δ and τ with $\tau \preceq \delta$ and $\tau \neq 0$.*

For the same reason mentioned in Section 3.2, we introduce the concept of k-cheating immunity. Given a secret sharing with its defining mapping F on $GF(p^t)^n$. Let k be an integer with $1 \leq k \leq n-1$. The secret sharing is said to be *strictly k-cheating immune* if the probability of successful cheating satisfies $\rho_{\delta,\tau,\alpha} = p^{-tm}$ for every $\delta \in GF(p^t)^n$ and any $\tau \preceq \delta$ with $1 \leq HW(\tau) \leq HW(\delta) \leq k$ and every $\alpha \in GF(p^t)^n$. The following theorem establishes a relationship between the two models of cheating immunity.

Theorem 5 *Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Then the multisecret sharing is strictly k-cheating immune $\Longleftrightarrow$ for any integer r with $0 \leq r \leq k-1$, any subset $\{j_1, \ldots, j_r\}$ of $\{1, \ldots, n\}$ and any $a_1, \ldots, a_r \in GF(p^t)$, the mapping $F(x_1, \ldots, x_n)|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$, with the variables $x_{i_1}, \ldots, x_{i_{n-r}}$, where $\{i_1, \ldots, i_{n-r}\} \cup \{j_1, \ldots, j_r\} = \{1, \ldots, n\}$, is the defining mapping of a $(k-r)$-cheating immune secret sharing.*

Proof Assume that the multisecret sharing is strictly k-cheating immune (model in Section 4.1). Denote $F(x_1, \ldots, x_n)|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$ by G. Then G is a mapping: $GF(p^t)^{n-r} \longrightarrow GF(p^t)^m$. Comparing the model in Section 3.1 with the model in Section 4.1, we know that G is the defining mapping of $(k-r)$-cheating immune secret sharing (model in Section 3.1). This proves the necessity. By definition, we can prove the sufficiency by inverting the above reasoning.

5 Secret Sharing versus Multisecret Sharing

We regard $GF(p^{tm})$ as a simple extension of $GF(p^t)$ and then there exists an element $\epsilon \in GF(p^{tm})$ such that

each element in $GF(p^{tm})$ can be uniquely expressed as $b_1 + b_2\epsilon + \cdots + b_m\epsilon^{m-1}$ where each $b_j \in GF(p^t)$. Let f be a function on $GF(p^{tm})^n$, i.e., a mapping: $GF(p^{tm})^n \longrightarrow GF(p^{tm})$, and ψ be a nonzero linear mapping: $GF(p^{tm}) \longrightarrow GF(p^t)$. ¿From f and ψ, we now define a mapping $F_{f,\psi}$: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $F_{f,\psi}(a_1, \ldots a_n) = (b_1, \ldots, b_m)$, where each $a_j, b_i \in GF(p^t)$, $\Longleftrightarrow f(c_1, \ldots c_n) = c$, where $a_j = \psi(c_j)$, $j = 1, \ldots, n$, and $c = b_1 + b_2\epsilon + \cdots + b_m\epsilon^{m-1}$.

Theorem 6 *Given a secret sharing with its defining function f on $GF(p^{tm})^n$. Let ψ be a nonzero linear mapping from $GF(p^{tm})$ to $GF(p^t)$. If the secret sharing is k-cheating immune then the mapping $F_{f,\psi}$: $GF(p^t)^n \longrightarrow GF(p^t)^m$ is the defining mapping a k-cheating immune multisecret sharing.*

Proof Let δ be any vector in $GF(p^t)^n$ with $HW(\delta) = l$, where $1 \leq l \leq k$, and τ be any vector in $GF(p^t)^n$ with $\tau \preceq \delta$. Consider the system of equations:

$$\begin{cases} F_{f,\psi}(x_\delta^- + \tau + \delta) = (a_1, \ldots, a_m) \\ F_{f,\psi}(x_\delta^- + \tau) = (b_1, \ldots, b_m) \end{cases} \tag{4}$$

where each $a_j, b_j \in GF(p^t)$, and

$$\begin{cases} f(x_\delta^- + \tau + \delta) = a_1 + a_2\epsilon + \cdots + a_m\epsilon^{m-1} \\ f(x_\delta^- + \tau) = b_1 + b_2\epsilon + \cdots + b_m\epsilon^{m-1} \end{cases} \tag{5}$$

Due to Theorem 3, Equations (5) have precisely $p^{tm(n-l-2)}$ solutions. Note that for each element $a \in GF(p^t)$, there precisely exist $p^{t(m-1)}$ elements $c \in GF(p^{tm})$ such that $\psi(c) = a$. Therefore for each vector $(a_1, \ldots, a_{n-l}) \in GF(p^t)^{n-l}$, there precisely exist $p^{t(m-1)(n-l)}$ vectors $(c_1, \ldots, c_{n-l}) \in GF(p^{tm})^{n-l}$ such that $(\psi(c_1), \ldots, \psi(c_{n-l})) = (a_1, \ldots, a_{n-l})$. Summarising the above, we know that Equations (4) have precisely $p^{tm(n-l-2)}/p^{t(m-1)(n-l)} = p^{t(n-l-2m)}$ solutions. Due to Theorem 3, we have proved that the mapping $F_{f,\psi}$: $GF(p^t)^n \longrightarrow GF(p^t)^m$ is the defining mapping a k-cheating immune multisecret sharing.

Combining Theorems 5 and 6, we can prove the following statement.

Corollary 4 *Given secret sharing with its defining function f on $GF(p^{tm})^n$. Let ψ be a nonzero linear mapping from $GF(p^{tm})$ to $GF(p^t)$. If the secret sharing is strictly k-cheating immune then the mapping $F_{f,\psi}$: $GF(p^t)^n \longrightarrow GF(p^t)^m$ is the defining mapping of a strictly k-cheating immune multisecret sharing.*

The construction of a k-cheating immune secret sharing defined by a function has been studied [6]. Therefore applying Theorems 6 and 4, we can construct a k-cheating immune secret sharing defined by a mapping from a k-cheating immune secret sharing defined by a function. Using Corollary 4 and construction given in [6], we can obtain strictly cheating immune secret sharing defined by a mapping. The constructions will be shown in Examples 1 and 2.

Theorem 7 *Let F be a mapping: $GF(p^t)^n \longrightarrow GF(p^t)^m$. Write $F(x) = (f_1(x), \ldots, f_m(x))$ where each f_j is a function on $GF(p^t)^n$ and $x \in GF(p^t)^n$. Let s be an integer with $1 \leq s \leq m$ and $\{j_1, \ldots, j_s\} \subseteq \{1, \ldots, n\}$. Define a mapping H: $GF(p^t)^n \longrightarrow GF(p^t)^s$ such that $H(x) = (f_{j_1}(x), \ldots, f_{j_s}(x))$. If F is the defining mapping of a k-cheating immune multisecret sharing, so is H.*

Proof Without loss of generality, we only prove the theorem in the special case that $j_1 = 1, \ldots, j_s = s$. Consider the system of equations:

$$\begin{cases} H(x_\delta^- + \tau + \delta) = \omega \\ H(x_\delta^- + \tau) = \sigma \end{cases} \tag{6}$$

where $\omega, \sigma \in GF(p^t)^s$.

Since F is the defining mapping of a k-cheating immune multisecret sharing, due to Theorem 3, for any integer l with $1 \leq l \leq k$, any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, any $\tau \preceq \delta$ and any $\mu, \nu \in GF(p^t)^m$, the system of equations: $\begin{cases} F(x_\delta^- + \tau + \delta) = \mu \\ F(x_\delta^- + \tau) = \nu \end{cases}$ has precisely $p^{t(n-l-2m)}$ solutions on x_δ^-. On the other hand, there precisely exist $p^{t(m-s)}$ vectors $\mu \in GF(p^t)^m$ satisfying $\mu = (\omega, y)$ where $y \in GF(p^t)^{m-s}$ and there precisely exist $p^{t(m-s)}$ vectors $\nu \in GF(p^t)^m$ satisfying $\nu = (\sigma, z)$ where $z \in GF(p^t)^{m-s}$. It is easy to see that the system of equations (6) has precisely $p^{t(n-l-2m)} \cdot p^{2t(m-s)} = p^{t(n-l-2s)}$ solutions on x_δ^-. Applying Theorem 3 to H, we have proved that H is the defining mapping of a k-cheating immune multisecret sharing.

The above theorem can be rephrased to the following statement.

Theorem 8 *Let F be a mapping: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $F(x) = (f_1(x), \ldots, f_m(x))$ where each f_j is a function on $GF(p^t)^n$ and $x \in GF(p^t)^n$. If F is the defining mapping of a k-cheating immune multisecret sharing then each f_j is the defining function of a k-cheating immune secret sharing.*

Applying Theorem 5 to Theorem 8, we obtain

Corollary 5 *Let F be a mapping: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $F(x) = (f_1(x), \ldots, f_m(x))$ where each f_j is a function on $GF(p^t)^n$ and $x \in GF(p^t)^n$. If F is the defining mapping of a strictly k-cheating immune multisecret sharing then each f_j is the defining function of a strictly k-cheating immune sharing.*

Theorem 9 *Let F be a mapping: $GF(p^t)^n \longrightarrow GF(p^t)^m$ and B is a nonsingular $m \times m$ matrix over $GF(p^t)$. Define another mapping G: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $G(x) = (F(x))B$. If F is the defining mapping of a k-cheating immune multisecret sharing, so is G.*

Proof For any integer l with $1 \leq l \leq k$, any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, any $\tau \preceq \delta$ and any $\mu, \nu \in GF(p^t)^m$, consider the system of equations: $\begin{cases} G(x_\delta^- + \tau + \delta) = \mu \\ G(x_\delta^- + \tau) = \nu \end{cases}$ that is equivalent to

$$\begin{cases} F(x_\delta^- + \tau + \delta) = \mu B^{-1} \\ F(x_\delta^- + \tau) = \nu B^{-1} \end{cases} \quad (7)$$

Since F is the defining mapping of a k-cheating immune multisecret sharing, due to Theorem 3, (7) has precisely $p^{t(n-l-2m)}$ solutions on x_δ^-. Therefore G has precisely $p^{t(n-l-2m)}$ solutions on x_δ^-. Again using Theorem 3, G is also the defining mapping of a k-cheating immune multisecret sharing.

Theorem 10 *Let F be a mapping: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $F(x) = (f_1(x), \ldots, f_m(x))$ where each f_j is a function on $GF(p^t)^n$ and $x \in GF(p^t)^n$. If F is the defining mapping of a k-cheating immune multisecret sharing then any nonzero linear combination of $f_1, \ldots, f_m$, i.e., $b_1 f_1 + \cdots + b_m f_m$ where each $b_j \in GF(p^t)$ and $(b_1, \ldots, b_m) \neq (0, \ldots, 0)$, is the defining function of a k-cheating immune secret sharing.*

Proof Let $(b_1, \ldots, b_m)$ be a nonzero vector in $GF(p^t)^m$. Let B be a nonsingular $m \times m$ matrix over $GF(p^t)$, whose first column is $(b_1, \ldots, b_m)^T$ where X^T denote the transpose of the matrix X. Set $G(x) = (g_1(x), \ldots, g_m(x)) = (f_1(x), \ldots, f_m(x))B$. Using Theorem 9, we know that G is the defining mapping of a k-cheating immune multisecret sharing. Applying Theorem 8 to G, we know that g_1 is the defining function of a k-cheating immune secret sharing. Since $g_1 = b_1 f_1 + \cdots + b_m f_m$, we have proved that $b_1 f_1 + \cdots + b_m f_m$ is the defining function of a k-cheating immune secret sharing.

Applying Theorem 5 to Theorem 10, we obtain

Corollary 6 *Let F be a mapping: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $F(x) = (f_1(x), \ldots, f_m(x))$ where each f_j is a function on $GF(p^t)^n$ and $x \in GF(p^t)^n$. If F is the defining mapping of a strictly k-cheating immune multisecret sharing then any nonzero linear combination of $f_1, \ldots, f_m$ is the defining function of a strictly k-cheating immune secret sharing.*

Due to Theorem 10 (Corollary 6), we have $f_1, \ldots, f_m$ that are m coordinate functions of the mapping F. Denote the set of all the nonzero linear combinations of $f_1, \ldots, f_m$, by $\Omega = \{g_1, \ldots, g_{p^{tm}-1}\}$. Then each g_j is the defining function of a (strictly) k-cheating immune secret sharing. Clearly $g_j \pm g_i \in \Omega$ for $j \neq i$, and thus $g_j \pm g_i$ is the defining function of a (strictly) k-cheating immune secret sharing. Due to Corollary 2, $g_j \pm g_i$ is balanced. This means that any f_j does not give any information on any other f_i with $i \neq j$ as balance means unbiased for every element in $GF(p^t)$. Note that $\Omega \cup \{0\}$, where 0 denotes the zero function on $GF(p^t)^n$ form an m-dimensional linear space over $GF(p^t)$.

6 Constructions

The following two examples indicate how to construct a multisecret sharing mentioned in Theorem 10 and Corollary 6.

Example 1 *Define a function χ_{2k+1} on $GF(p^{tm})^{2k+1}$ by $\chi_{2k+1}(x_1, \ldots, x_{2k+1}) = x_1x_2 + x_2x_3 + \cdots + x_{2k}x_{2k+1} + x_{2k+1}x_1$ and then define a function χ_{4k+2} on $GF(p^{tm})^{4k+2}$ by $\chi_{4k+2}(x_1, \ldots, x_{4k+2}) = \chi_{2k+1}(x_1, \ldots, x_{2k+1}) + \chi_{2k+1}(x_{2k+2}, \ldots, x_{4k+2})$.*

Let k and s be positive integers with $s \geq k+1$, $n_1, \ldots, n_s = 4k+1$ or $4k+2$, and $n = n_1 + \cdots + n_s$. Define a function on $GF(p^{tm})^n$ such as $f(x) = \chi_{n_1}(y) + \cdots + \chi_{n_s}(z)$ where $x = (y, \ldots, z)$, $y \in GF(p^{tm})^{n_1}, \ldots, z \in GF(p^{tm})^{n_s}$, and $\chi_{n_1}, \ldots, \chi_{n_s}$ have disjoint variables mutually. ¿From [6], the secret sharing with the defining function f is k-cheating immune. Let ψ be a nonzero linear mapping: $GF(p^{tm}) \longrightarrow GF(p^t)$. Due to Theorem 6, the mapping $F_{f,\psi}$: $GF(p^t)^n \longrightarrow GF(p^t)^m$ is the defining mapping a k-cheating immune multisecret sharing.

Example 2 *Let $\lambda_{n,p}$ be a function on $GF(p^{tm})^n$ ($n \geq 2p^2+p$) defined by $\lambda_{n,p}(x_1, \ldots, x_n) = x_1 + \sum_{j=1}^{n}(x_j x_{[j+1]_{(n)}} + x_j x_{[j+2]_{(n)}} + \cdots + x_j x_{[j+p]_{(n)}})$ where $[i]_{(n)}$ denotes the integer j such that $1 \leq j \leq n$ and $j \equiv i \bmod n$ (we replace i by $[i]_{(n)}$ as i is possibly greater than n). Let s be an integer with $s \geq 2p$, $n_1, \ldots, n_s = 2p^2+p$ or $2p^2+p+1$, and $n = n_1 + \cdots + n_s$. Define a function on $GF(p^{tm})^n$ such as $f(x) = \lambda_{n_1,p}(y) + \cdots + \lambda_{n_s,p}(z)$ where $x = (y, \ldots, z)$, $y \in GF(p^{tm})^{n_1}, \ldots, z \in GF(p^{tm})^{n_s}$, and $\lambda_{n_i,p}, \ldots, \lambda_{n_j,p}$ have disjoint variables if $i \neq j$. From [6], the secret sharing with the defining function f is strictly p-cheating immune. Let ψ be a nonzero linear mapping: $GF(p^{tm}) \longrightarrow GF(p^t)$. Due to Corollary 4, the mapping $F_{f,\psi}$: $GF(p^t)^n \longrightarrow GF(p^t)^m$ is the defining mapping a strictly p-cheating immune multisecret sharing.*

7 Sequential Recovery of Secrets

Given a multisecret sharing with its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$ such that $F = (f_1, \ldots, f_m)$ where each f_j is a function on $GF(p^t)^n$. In the multisecret sharing schemes mentioned in Sections 3 and 4, we stipulate that the multisecret as a vector $(b_1, \ldots, b_m)$ that determines m secrets. We assume that those secrets are recovered simultaneously.

In this section, we consider a scenario where the combiner will recover single secrets (instead of the multisecret) in a some order (perhaps imposed by the participants) and return the recovered secrets to active participants. We will study two basic cheating strategies

• cheaters use the same cheating vector and the same original vector for all recoveries – this case is equivalent to the simultaneous recovery of secrets,

• cheaters modify their cheating vectors depending on the returned secrets.

Assume that the participants sequentially perform m secret sharing schemes with defining functions $f_1, \ldots, f_m$ by taking cheating vectors $\delta_1, \ldots, \delta_m \in GF(p^t)^n$ and original vectors. $\beta_1, \ldots, \beta_m \in GF(p^t)^n$ and original vectors. Since the secret of each secret sharing defined by f_j is independent to the secret of secret sharing defined by f_i if $i \neq j$, the probability of successful cheating is identical with $\rho_{\delta_1,\beta_1} \cdots \rho_{\delta_m,\beta_m}$, where ρ_{δ_i,β_i} denotes the probability of successful cheating of the secret sharing defined by f_i with respect to the cheating vector δ_i and the original vector β_i. We notice that each ρ_{δ_i,β_i} can be calculated by the definition of probability of successful cheating. Obviously the probability of successful cheating of sequentially recovery is invariable under a permutation on the order of participants. In particular, $F = (f_1, \ldots, f_m)$ is the mapping of a k-th immune secret sharing, then using Theorem 10, we conclude that $\rho_{\delta_1,\beta_1} = \cdots = \rho_{\delta_m,\beta_m} = p^{-t}$. Therefore the probability of successful cheating is identical with p^{-tm}.

As for the model that cheaters submit a mixture of valid and invalid shares, using the same arguments, we conclude that the probability of successful cheating is identical with $\rho_{\delta_1,\beta_1} \cdots \rho_{\delta_m,\beta_m}$. In particular, $F = (f_1, \ldots, f_m)$ is the mapping of a k-th immune secret sharing, then using Theorem 10, we conclude that $\rho_{\delta_1,\beta_1} = \cdots = \rho_{\delta_m,\beta_m} = p^{-t}$. Therefore the probability of successful cheating is identical with p^{-tm}.

8 Conclusions and Remarks

We define a multisecret sharing by its defining mapping F: $GF(p^t)^n \longrightarrow GF(p^t)^m$. For n participants, each vector $\alpha \in GF(p^t)^n$ is a share and the vector $F(\alpha) \in GF(p^t)^m$ is the multisecret corresponding to the share α. It has been proven that the probability of recovery of correct multisecret by cheaters is can be made as small as p^{-tm}. Clearly, cheaters who are interested in getting a single secret may get it with the probability no smaller than p^{-t}. In a sense each recovered invalid secret provides no information about the valid secret but also gives no help in gaining information about other secrets.

We have investigated two models of k-cheating im-

mune secret sharing defined by a mapping. A relationship between defining mappings and functions has been examined and constructions of k-cheating immune multisecret sharing have been given. We have shown how k-cheating immune multisecret sharing relates to a linear space defined over k-cheating immune secret sharing schemes. We have also demonstrated that k-cheating immunity guarantees that multisecret sharing can be used for simultaneous and sequential recovery without any impact on the probability of guessing of valid secrets by cheaters.

References

[1] C. Blundo, A. De Santis, and U. Vaccaro. Efficient sharing of many secrets. In K.W. Wagner P. Enjalbert, A. Finkel, editor, *Proceedings of STACS93, 10th Symposium on Theoretical Aspects of Computer Science*, pages 692–703. Springer, 1993. LNCS No. 665.

[2] Carlo Blundo, Alfredo De Santis, Giovanni Di Crescenzo, Antonio Giorgio Gaggia, and Ugo Vaccaro. Multi-secret sharing schemes. In *Advances in Cryptology - CRYPTO'94*, LNCS No. 839. pages 150–163. Springer-Verlag, 1994.

[3] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. Multisecret threshold schemes. In Douglas R. Stinson, editor, *CRYPTO93*, pages 126–135. Springer, 1994. LNCS No. 773.

[4] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. On sharing many secrets. In J. Pieprzyk and R. Safavi-Naini, editors, *ASIACRYPT'94*, pages 42–54. Springer, 1995. LNCS No. 917.

[5] E.D. Karnin, J.W. Greene, and M.E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, IT-29:35–41, 1983.

[6] J. Pieprzyk and X. M. Zhang. Cheating prevention in immune secret sharing over $GF(p^t)$, In *Indocrypt 2001*, LNCS No. 2247, pages 79–91. Springer-Verlag, 2001.

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

[8] 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.

Appendix: the Proof of Theorem 2

Proof Assume that the secret sharing is k-cheating immune. Choose δ as a cheating vector and any vector $\alpha \in GF(p^t)^n$ as an original vector. Due to Lemma 1, there exist $\mu', \nu' \in GF(p^t)^m$ such that $R(\delta, \alpha_\delta^+ + \delta, \mu') \neq \emptyset$ and $R(\delta, \alpha_\delta^+, \nu') \neq \emptyset$. Note that $R(\delta, \alpha_\delta^+ + \delta, \mu')$ can be partitioned into p^t parts:

$$R(\delta, \alpha_\delta^+ + \delta, \mu') = \bigcup_{\nu \in GF(p^t)^m} R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu) \quad (8)$$

Assume that $R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu) \neq \emptyset$ for some $\nu \in GF(p^t)^m$. Then there exists a vector $\beta_\delta^- \in R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu)$. Set $\gamma = \beta_\delta^- + \alpha_\delta^+$. Since the secret sharing is k-cheating immune, $\#(R(\delta, \gamma_\delta^+ + \delta, \mu') \cap R(\delta, \gamma_\delta^+, \nu))/\#R(\delta, \gamma_\delta^+ + \delta, \mu') = \rho_{\delta,\gamma} = p^{-tm}$, where $\gamma_\delta^+ = \alpha_\delta^+$. Thus

$$\#R(\delta, \alpha_\delta^+ + \delta, \mu') = p^{tm} \#(R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu)) \quad (9)$$

whenever $R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu) \neq \emptyset$. ¿From (8),

$$\#R(\delta, \alpha_\delta^+ + \delta, \mu') = \sum_{\nu \in GF(p^t)^m} \#(R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu)) \quad (10)$$

Combing (9) and (10), we know that $R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu) \neq \emptyset$ for every $\nu \in GF(p^t)^m$ and thus

$$\#(R(\delta, \alpha_\delta^+ + \delta, \mu') \cap R(\delta, \alpha_\delta^+, \nu)) = p^{-tm} \#R(\delta, \alpha_\delta^+ + \delta, \mu') \quad (11)$$

for every $\nu \in GF(p^t)^m$. Replacing $\alpha, \delta,$ by $\alpha+\delta, (p-1)\delta$ respectively, due to the same arguments for (11), we have

$$\#(R((p-1)\delta, \alpha_\delta^+ + p\delta, \nu') \cap R((p-1)\delta, \alpha_\delta^+ + \delta, \mu)) = p^{-tm} \#R((p-1)\delta, \alpha_\delta^+ + p\delta, \nu')$$

for every $\mu \in GF(p^t)^m$. Since the characteristic of the finite field $GF(p^t)$ is p, $pe = 0$ for every $e \in GF(p^t)$. It follows that $\#(R((p-1)\delta, \alpha_\delta^+, \nu') \cap R((p-1)\delta, \alpha_\delta^+ + \delta, \mu')) = p^{-tm} \#R((p-1)\delta, \alpha_\delta^+, \nu')$ for every $\mu \in GF(p^t)^m$. Using Lemma 1, we obtain

$$\begin{aligned} &\#(R(\delta, \alpha_\delta^+, \nu') \cap R(\delta, \alpha_\delta^+ + \delta, \mu)) \\ &= p^{-tm} \#R(\delta, \alpha_\delta^+, \nu') \end{aligned} \tag{12}$$

for every $\mu \in GF(p^t)^m$. Recall that $R(\delta, \alpha_\delta^+ + \delta, \mu') \neq \emptyset$ and $R(\delta, \alpha_\delta^+, \nu') \neq \emptyset$. Therefore (11) and (12) imply that $R(\delta, \alpha_\delta^+, \nu) \neq \emptyset$ and $R(\delta, \alpha_\delta^+ + \delta, \mu) \neq \emptyset$ for every $\mu, \nu \in GF(p^t)^m$. Due to the same reasoning for (11) and (12), we have

$$\begin{aligned} &\#(R(\delta, \alpha_\delta^+ + \delta, \mu) \cap R(\delta, \alpha_\delta^+, \nu)) \\ &= p^{-tm} \#R(\delta, \alpha_\delta^+ + \delta, \mu) \end{aligned} \tag{13}$$

$$\begin{aligned} &\#(R(\delta, \alpha_\delta^+, \nu) \cap R(\delta, \alpha_\delta^+ + \delta, \mu)) \\ &= p^{-tm} \#R(\delta, \alpha_\delta^+, \nu) \end{aligned} \tag{14}$$

for every $\mu, \nu \in GF(p^t)^m$. Comparing (14) with (13), we conclude that $\#R(\delta, \alpha_\delta^+ + \delta, \mu) = \#R(\delta, \alpha_\delta^+, \nu)$ for every $\mu, \nu \in GF(p^t)^m$. Therefore both $\#R(\delta, \alpha_\delta^+ + \delta, \mu)$ and $\#R(\delta, \alpha_\delta^+, \nu)$ are constant. Note that $\sum_{\nu \in GF(p^t)^m} \#R(\delta, \alpha_\delta^+, \nu) = p^{t(n-l)}$. We have proved that

$$\#R(\delta, \alpha_\delta^+, \nu) = p^{t(n-l-m)} \tag{15}$$

for any $\nu \in GF(p^t)^m$. From (15) and (14), we have proved that

$$\#(R(\delta, \alpha_\delta^+ + \delta, \mu) \cap R(\delta, \alpha_\delta^+, \nu)) = p^{t(n-l-2m)} \tag{16}$$

for every $\mu, \nu \in GF(p^t)^m$. For any $\tau \preceq \delta$, choose $\alpha \in GF(p^t)^n$ such that $\alpha_\delta^+ = \tau$. Due to (15) and (16), both conditions (i) and (ii) hold.

Conversely assume the defining mapping F satisfies conditions (i) and (ii). Choose any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, where $1 \leq l \leq k$, as a cheating vector and any α as an original vector. Set $F(\alpha) = \mu$ and $F(\alpha + \delta) = \mu^*$. By definition, $\rho_{\delta,\alpha} = \#(R(\delta, \alpha_\delta^+ + \delta, \mu^*) \cap R(\delta, \alpha_\delta^+, \mu)) / \#R(\delta, \alpha_\delta^+ + \delta, \mu^*)$. Due to conditions (i) and (ii), $\rho_{\delta,\alpha} = p^{-tm}$. Thus we have proved that the secret sharing is k-cheating immune.