Ideal Secret Sharing Schemes with Share Selectability

Keita Emura[1], Atsuko Miyaji[2], Akito Nomura[3], Mohammad Shahriar Rahman[2], and Masakazu Soshi[4]

[1] Center for Highly Dependable Embedded Systems Technology, Japan Advanced Institute of Science and Technology (JAIST), Japan
[2] School of Information Science, JAIST, Japan
[3] Institute of Science and Engineering, Kanazawa University, Japan
[4] Graduate School of Information Sciences, Hiroshima City University, Japan
{k-emura,miyaji,mohammad}@jaist.ac.jp, anomura@t.kanazawa-u.ac.jp, soshi@hiroshima-cu.ac.jp

Abstract. In this paper, we investigate a new concept, called *share selectable secret sharing*, where no unauthorized set can obtain information of the secret (in the information-theoretic sense) even if shares are selectable as arbitrary values which are independent of the secret. We propose two totally selectable (i.e., all users' shares are selectable) secret sharing schemes with unanimous structure. We also propose a quasi-selectable (i.e., a part of each user's share is selectable) secret sharing scheme with certain hierarchical structures which contains special cases of the hierarchical threshold structures introduced by Tamir Tassa in TCC2004 (or its full version (J. Cryptology2007)). If all selectable shares are randomly chosen, then our schemes are perfect. Finally, we discuss the effect of the leakage information of the secret if a weak secret is indicated as a selectable share.

1 Introduction

1.1 Cryptography with Information-Theoretic Security

In cryptography, security models are classified roughly according to computational security and unconditional security (or information-theoretic security). An adversary is modeled as a probabilistic polynomial time algorithm in computational security, whereas it is defined as an infinitely powerful adversary in unconditional security. Nowadays, unconditional secure protocols have become more noticeable as one of the post-quantum cryptographic schemes. Many unconditional secure protocols have been proposed so far. Secret sharing is one of the most popular schemes among such primitives. Briefly, the flow of secret sharing is described as follows. Each user is given a piece of the secret called *share*, and an authorized set of users can recover the secret value by using their shares. On the contrary, unauthorized set can obtain information of the secret. Until now, several kind of research issues of secret sharing have been proposed,

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 143–157, 2011.

e.g., realizing flexible access structures [9,24,25,41,42,44], multi secret sharing [6], dynamic secret sharing [5], information rate (which indicates the lower bound of the share size in the case of corresponding access structure[1]) [10,12,31], rational secret sharing [18,20,23,27,32] (i.e., with game-theoretic analyses), and so on. In addition, for the purpose of establishing secret sharing with shorter share size, computational secure secret sharing also have been proposed [3,28]. As one of such schemes, computational secure on-line secret sharing schemes have been proposed [11,22,35,40], where an auxiliary public value is opened to abridge the secret and the shares. Secret sharing is used in other cryptographic primitive as a building tool, e.g., attribute-based encryption [2,34,45], threshold encryption [7,14,36], and so on. In this paper, we attempt to revisit secret sharing from a perspective different from previous works above.

1.2 Research Background

Recently, construction of cryptographic protocols from weak secrets (e.g., a short human selected password with low Shannon's entropy) has been considered. Some examples are, password-based authenticated key exchange (where cryptographically strong key can be exchanged even user has a very weak secret) [16,17,26,30,38,46], distributed public-key cryptography (where even if each group member holds a small secret password only, they can associate to a public-key cryptosystem) [1,8], and symmetric-key cryptography from weak secrets (where two users share a secret key which might not be uniformly random) [15], and so on. However, to the best of our knowledge, there is no proposal of unconditional secret sharing with such attempt so far (here, we exclude computational secure secret sharing which can treat such weak secrets under the computational security). Moreover, no consideration has been made about the cases where a dealer can "select" shares independently with the secret. As a simple example, in the Shamir's secret sharing scheme [37], a share is a random value on a randomly-chosen polynomial (with the condition that the constant value equals the secret value). That is, it is impossible to select the values of shares as particular values (for certain purposes) in the Shamir's secret sharing scheme.

1.3 Our Contribution

In this paper, we innovate a new concept, called *share selectable secret sharing*, where

- Shares are selectable as arbitrary values.
  - The word "arbitrary" means that shares are independent of the secret.
- No unauthorized set can obtain information of the secret even if shares are selectable.

[1] Note that unconditionally secure secret sharing requires that every qualified user should have a share at least as large as the secret itself. Secret sharing is said to be *ideal* if and only if the size of share is the same as that of the secret (i.e., the corresponding information rate is 1).

Of course, it is impossible to reconstruct the secret only from shares which are independently selected of the secret. Therefore, we introduce an auxiliary public value which works as a bridge between the secret and the shares. That is, it is required that even if unauthorized set of users obtain the auxiliary public value, it is not possible to obtain any information on the secret.

Briefly, we investigate ρ_s-quasi selectable secret sharing, where ρ_s is the selectability ratio estimating the number of users' shares that are selectable (i.e., ρ_s=(|Share selectable users|/|All users|), and selectable secret sharing is said to be totally selectable if and only if $\rho_s = 1$. In this paper, we propose two (n, n)-threshold totally selectable secret sharing schemes, where n is the total number of users. We also propose a $(1 - \frac{\ell}{n})$-quasi selectable secret sharing scheme with certain hierarchical structures, where ℓ $(0 \leq \ell \leq n-2, \ell \neq 1)$ is the number of users who have un-selectable shares. Briefly speaking, these hierarchical structures contain special cases of the hierarchical threshold structures of Tassa [41] (or its full version [42]). Note that Tassa [41,42] (and [43] also) applies polynomial derivatives and Birkhoff interpolation for achieving hierarchical structures, whereas we apply the classical Lagrange interpolation technique only. That is, our quasi scheme implements hierarchical threshold structures by different methodology from that of Tassa's constructions.

Remark1: Trivial Non-ideal Share Selectable Secret Sharing with Flexible Access Structures: Ito, Saito, and Nishizeki [24] proposed a secret sharing scheme with general access structure from any (n, n) secret sharing scheme. Since a (n, n)-threshold totally selectable secret sharing scheme can be constructed easily (e.g., protocol 1 in Section 2), we also realize a totally selectable secret sharing scheme with general access structure. However, this totally selectable scheme is not ideal (i.e., the size of share is larger than that of the secret). We make it clear that the main objective of this paper is to construct "ideal" secret sharing schemes (i.e., the size of share is the same as that of the secret) with share selectability, and we stick resolutely to such ideal schemes in this paper.

Remark2: The Csirmaz-Tardos On-line Secret Sharing: To the best of our knowledge, the case that shares are independently selected with the secret to be distributed has not been considered except in the following scheme proposed by Csirmaz and Tardos. Very recently, Csirmaz and Tardos proposed on-line secret sharing [13] for graph based access structures (which is totally different from the computational on-line ones [11,22,35,40]). In the Csirmaz-Tardos on-line secret sharing scheme, the dealer *assigns* shares in the order the participants show up knowing only those qualified subsets whose all members she have seen. Users form a queue in the on-line share distribution, and they receive their shares in the order they appear. The users receive their shares one by one and the assigned share cannot be changed later on. Csirmaz and Tardos insist that their on-line scheme is useful when the set of users is not fixed in advance. Since their purpose and construction method are totally different from ours, we do not discuss their on-line secret sharing anymore although there might be somewhat relationships

between share selectable secret sharing and the Csirmaz-Tardos on-line secret sharing. There is space for argument on this point.

1.4 Requirement of Shannon's Entropy of Selected Shares

Here, we clarify the requirement of selectable shares, especially, the difference between selectable shares and weak secrets with low entropy. For achieving "perfect" secret sharing (i.e., no information can revealed from any unauthorized set of users), we cannot assume that a low entropy value (e.g., a human selected password) is indicated as a share. That is, we can say that:

- If selectable shares are randomly chosen, then our schemes are perfect.
  - I.e., we assume that the guessing probability of each share is smaller than that of the secret itself, namely $H(S) \leq H(W_i)$ holds, where $H(\cdot)$ is the Shannon's entropy, S and W_i are the random variables induced by the secret s and a share ω_i. We explain other notations in Section 2.
- If a weak secret is indicated as a selectable share, then users gain some information by guessing the share of uncorrupted users.
  - This setting is essentially the same as that of ramp secret sharing [4,29].

From the above considerations, first, we propose selectable secret sharing schemes. We also prove that these schemes are perfect if selectable shares are randomly chosen (Appendix). Finally, we discuss the effect of the leakage information of the secret if a weak secret is indicated as a selectable share (Section 4).

1.5 Another Significance of the Share Selectability

Although our research starts with mainly mathematical interests, cryptographic applications of share selectable secret sharing are also expected. For example, in cryptographic schemes, where secret sharing approach is used, secret keys are computed by using shares of the master key. That is, if a decryptor has legitimate secret keys, then she can decrypt the corresponding ciphertext by combining the secret keys in the secret sharing manner (e.g., applying Lagrange interpolations). In this case, each share is also changed if access structures are changed. Hence the secret keys of users need to be updated as well. For example, in access trees (e.g., [19]), first a secret value of the root node is chosen, and next a polynomial is defined with the condition that the constant value is equal to the root secret, and a secret value of a child node is set as a value on the polynomial. So, a secret value of the leaf node is computed at the end. Therefore, if the structure of the access tree is changed, these procedures must be executed again. On the contrary, each share can be independently selected under the share selectability. So, it is expected that access structures can be updated by applying share selectable secret sharing without changing secret keys of users. In an opposite manner, secret keys might be updated without changing access structures and the master key (which is the same motivation of proactive secret sharing [21,33,39]). Since we mainly focus on the share selectability, we do not argue on updating the access structures or shares anymore.

2 Preliminaries

Throughout this paper, we use the following notations. Let $n \in \mathbb{N}$ be the number of participants, p be a prime number of $p > n$ (and $ID \bmod p \neq 0$ for all public identity), $H(X)$ be Shannon's entropy of a random variable X, $H(X|Y)$ be conditional Shannon's entropy of random variables X and Y, $|\mathcal{X}|$ be the number of elements of a finite set $\mathcal{X}$, and $2^{\mathcal{X}}$ be the family of all subsets of $\mathcal{X}$. Operations are done over the field $\mathbb{F}_p$.

2.1 Share Selectable Secret Sharing

Here, we define share selectable secret sharing (notations are referred by [29]). Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a set of participants, and $D \notin \mathcal{P}$ be a dealer who selects a secret $s \in \mathcal{S}$, computes the corresponding auxiliary public value $u \in \mathcal{U}$, and gives a share $\omega_i \in \mathcal{W}_i$ to $P_i \in \mathcal{P}$ for $i \in [1, n]$, where $\mathcal{S}$ denotes the set of secrets, $\mathcal{U}$ denotes the set of auxiliary public values, and $\mathcal{W}_i$ denotes the set of possible shares that P_i might receive. The access structure $\Gamma \subset 2^{\mathcal{P}}$ is a family of subsets of $\mathcal{P}$.

Definition 1 (Share selectable secret sharing). *Let S, U, and W_i be the random variables induced by s, u, and ω_i, respectively, and $\mathcal{V}_A = \{W_i | P_i \in A\}$ be the set of random variable of shares given to every participant $P_i \in A \subset \mathcal{P}$. Let* SSGen *be a selectable-share generation algorithm, which takes as an input the description of the underlying group $\mathbb{G}$ (in our schemes, $\mathbb{G} = \mathbb{Z}_p$), and returns a share $\omega \in \mathbb{G}$. A share selectable secret sharing scheme is said to be perfect if the following holds.*

$$H(S|\mathcal{V}_A, U) = \begin{cases} 0 & (A \in \Gamma) \\ H(S) & (A \notin \Gamma) \end{cases}$$

Our major argument is the secret s is not included in the input of the SSGen algorithm. That is, a share $\omega \leftarrow \mathsf{SSGen}(\mathbb{G})$ is totally independent with the secret s, and is called selectable. Therefore, for a selectable share ω,

$$H(S|\mathcal{V}) = H(S)$$

holds, where $\mathcal{V} \subset \mathcal{W} := \bigcup_{i=1}^{n} \mathcal{W}_i$ be a random variable of shares induced by ω.

As a remark, we definitely distinguish the equation $H(S|\mathcal{V}) = H(S)$ above and the case that $H(S|\mathcal{V}_A) = H(S)$ for $A \notin \Gamma$ in conventional perfect secret sharing manner. That is, in share selectable secret sharing, even if all selectable shares are collected (i.e., A might be in Γ), there is no way to recover the secret. Therefore, if all shares are selectable, then some auxiliary public value $u \in \mathcal{U}$ is indispensable for reconstructing the secret s. Note that if a part of shares are non-selectable, then there is room for reconstructing the secret s without using any auxiliary public value $u \in \mathcal{U}$.

Next, we define the selectability ratio which estimates the number of users' shares that are selectable.

Definition 2 (The Selectability Ratio). *Let $0 \leq n_s \leq n$ be the number of users who have a selectable share. The selectabilty ratio ρ_s is defined as $\rho_s = n_s/n$.*

Definition 3 (Quasi Selectability and Total Selectability). *A secret sharing is said to be ρ_s-quasi selectable secret sharing if its selectability ratio ρ_s is $0 < \rho_s < 1$. A secret sharing is said to be totally selectable if its selectability ratio ρ_s is 1.*

The case $\rho_s = 0$ represents the conventional secret sharing schemes. Note that there have been secret sharing schemes having $\rho_s > 0$. For example, for a secret $s \in \mathbb{Z}_p$, the dealer D selects $\omega_i \in \mathbb{Z}_p$ for all $i \in [1, n-1]$ (so, these shares are selectable, since these can be selected independently with s), sets $\omega_n := s - \sum_{i=1}^{n-1} \omega_i$ (so, ω_n is unselectable), and gives ω_i to P_i for all $i \in [1, n]$. s can be reconstructed by $\sum_{i=1}^{n} \omega_i$. Then, obviously this scheme is a $(1 - \frac{1}{n})$-quasi selectable (n, n)-threshold secret sharing scheme, and is perfect.

3 Proposed Schemes

In this section, we propose two totally selectable (n, n)-threshold secret sharing schemes, and a $(1 - \frac{\ell}{n})$-quasi selectable secret sharing scheme with certain hierarchical structures (ℓ $(0 \leq \ell \leq n-2, \ell \neq 1)$ is defined in the third scheme). The first construction (protocol 1) is somewhat trivial since it is a simple modification of the $(1 - \frac{1}{n})$-quasi selectable (n, n)-threshold secret sharing scheme introduced in the previous section. However, this scheme is easy-to-understand due to its simple structure. In our all schemes, the $\mathsf{SSGen}(\mathbb{Z}_p)$ algorithm simply returns $\omega \in \mathbb{Z}_p$.

Protocol 1 (The first scheme: A totally selectable (n,n)-threshold secret sharing scheme).

Distribution Phase:

1. *The dealer D selects the secret $s \in \mathbb{Z}_p$*
2. *D selects a share $\omega_i \in \mathbb{Z}_p$ for all $i \in [1, n]$ such that $\omega_i \leftarrow \mathsf{SSGen}(\mathbb{Z}_p)$.*
3. *D sets $u := s - \sum_{i=1}^{n} \omega_i$.*
4. *D gives ω_i to P_i for all $i \in [1, n]$, and opens u as the auxiliary public value.*

Reconstruction Phase: *Compute $s = u + \sum_{i=1}^{n} \omega_i$.*

Next, we propose a polynomial-based totally selectable (n, n)-threshold secret sharing scheme. This second scheme can be seen as a special case of our quasi one (protocol 3). Let ID_i be the (public) identity of $P_i \in \mathcal{P}$ and $\Gamma = \{P_1, P_2, \ldots, P_n\}$, namely, Γ is a (n, n)-threshold structure. We require $ID_i \neq ID_j$ $(i \neq j)$.

Protocol 2 (The second scheme: A polynomial-based totally selectable (n,n)-threshold secret sharing scheme).

Distribution Phase:

1. *The dealer D selects the secret $s \in \mathbb{Z}_p$.*
2. *D selects a share $\omega_i \in \mathbb{Z}_p$ for all $i \in [1,n]$ such that $\omega_i \leftarrow \mathsf{SSGen}(\mathbb{Z}_p)$.*
3. *Let $f(x)$ be a polynomial of degree at most n such that $f(ID_i) = \omega_i$ ($P_i \in \Gamma$) and $f_j(0) = s$. D chooses $ID_D \in \mathbb{Z}_p$ such that $ID_D \notin \{ID_i\}_{i=1}^n$, and computes $u = f(ID_D)$.*
4. *D gives ω_i to P_i for all $i \in [1,n]$, and opens u as the auxiliary public value.*

Reconstruction Phase: *By using Lagrange interpolation, $f(x)$ can be reconstructed from (ID_D, u) and all $\{(ID_i, \omega_i)\}_{i=1}^n$, and $s = f(0)$ can be computed.*

Next, we propose a $(1 - \frac{\ell}{n})$-quasi selectable secret sharing scheme, which is the most interesting construction in this paper. First, we define the access structures of this quasi scheme.

Definition 4 (Hierarchical access structures realized in our quasi scheme). *Let ℓ $(0 \le \ell \le n-2, \ell \ne 1)$ be the number of users who have an unselectable share, and set $\mathcal{P}^\ell := \{U_{j_1}, U_{j_2}, \ldots, U_{j_\ell}\}$ as the set of such ℓ users. Let $n' := n - \ell$ be the number of user who have a selectable share, and set $\mathcal{P}' := \{U_{i_1}, U_{i_2}, \ldots, U_{i_{n'}}\}$ as the set of such n' users. We require $\mathcal{P} = \mathcal{P}^\ell \cup \mathcal{P}'$ and $\mathcal{P}^\ell \cap \mathcal{P}' = \emptyset$. Let $\Gamma' \subset 2^{\mathcal{P}'}$ is a family of subsets of $\mathcal{P}'$, and $m = |\Gamma'|$. For $A_j \in \Gamma'$ $(j \in [1,m])$, set $|A_j| = n_j$. Let $\Gamma^\ell := \{A \in 2^{\mathcal{P}^\ell} : |A| \ge k\}$, where $k \in \mathbb{N}$ be the threshold value and $2 \le k \le \ell$. The actual access structure Γ is defined as follows.*

$$\Gamma := \{A : A = A^\ell \cup A' \text{ such that } A^\ell \in \Gamma^\ell \wedge A' \in \Gamma'\}$$

As one exception, if $\ell = 0$, then Γ' is restricted as the (n,n)-threshold structure only.

Note that the restriction case ($\ell = 0$) is exactly the second construction, and therefore the second scheme is a special case of the third scheme. In addition, Γ contains special cases of the hierarchical threshold structures [41,42][2]. For example, let Γ' be (n', n')-threshold structure, then $\Gamma = \{A \subset \mathcal{P} : |A \cap \mathcal{P}'| = n' \wedge |A \cap |\mathcal{P}' \cup \mathcal{P}^\ell|| \ge n' + k\}$ holds. This is a special case of the hierarchical threshold structures with $k_0 = n'$, $k_1 = n' + k$, $\mathcal{P}_0 = \mathcal{P}'$, and $\mathcal{P}_1 = \mathcal{P}^\ell$. In addition to this hierarchical threshold structure, the above Γ can represent any kind of access structure for $\mathcal{P}'$ (not $\mathcal{P}$). More precisely, we can achieve general access structures [24,25,44] for $\mathcal{P}'$ although our scheme is ideal. Note that our result

[2] In the hierarchical threshold structures, a set of users $\mathcal{P}$ is divided as N hierarchy $\mathcal{P} := \cup_{i=1}^N \mathcal{P}_i$ such that $\mathcal{P}_i \cap \mathcal{P}_j = \emptyset$ for $0 \le i < j \le N$. Let $\mathbf{k} = (k_0, k_1, \ldots, k_N)$ be monotonically increasing sequence of integers $0 < k_0 < \cdots < k_N$. $(\mathbf{k}, n)$ hierarchical threshold structure is defined as $\Gamma = \{A \subset \mathcal{P} : |A \cap \big(\cup_{i=0}^N \mathcal{P}_i\big)| \ge k_i \ \forall i \in [0,N]\}$.

does not contradict with certain impossible results (e.g., there exist families of special access structures with n participants where the size of some shares increases unboundedly as $n \to \infty$, i.e., at least about $n/\log n$ times the secret size [12]), since access structures are restricted as threshold ones for $\mathcal{P}^\ell$ (that is, for $\mathcal{P} = \mathcal{P}^\ell \cup \mathcal{P}'$, our access structure is not general).

Here, we give our quasi scheme. We omit the case $\ell = 0$ in the following scheme, since it has already been shown as the second scheme.

Protocol 3 (The third scheme : A (1-$\frac{\ell}{n}$)-quasi selectable secret sharing scheme).

Distribution Phase:

1. *The dealer D selects the secret $s \in \mathbb{Z}_p$.*
2. *D selects a share $\omega_i \in \mathbb{Z}_p$ for all $P_i \in \mathcal{P}'$ such that $\omega_i \leftarrow \mathsf{SSGen}(\mathbb{Z}_p)$.*
3. *D chooses $ID_{\mathcal{A}_j} \in \mathbb{Z}_p$ for all $j \in [1, m]$ such that $ID_{\mathcal{A}_j} \notin \{ID_i\}_{i=1}^n$ and $ID_{\mathcal{A}_i} \neq ID_{\mathcal{A}_j}$ $(i \neq j)$.*
4. *For each $A_j \in \Gamma'$ $(j \in [1, m])$, let $f_j(x)$ be a polynomial of degree at most n_j such that $f_j(ID_i) = \omega_i$ $(U_i \in A_j)$ and $f_j(0) = s$. Set $D_j := (ID_{\mathcal{A}_j}, f_j(ID_{\mathcal{A}_j}))$.*
5. *Let $g(x)$ be a polynomial of degree at most $m-1$ such that $g(ID_{\mathcal{A}_j}) = f_j(ID_{\mathcal{A}_j})$ for all $j \in [1, m]$.*
6. *For all $P_i \in \mathcal{P}^\ell$, D computes $\omega_i := g(ID_i)$ (we make it clear that this step is NOT for users $P_i \in \mathcal{P}'$, their shares $\{\omega_i\}_{P_i \in \mathcal{P}'}$ have been "selected" in Step 2).*
7. *D randomly chooses $(m-k)$ coordinates on the polynomial $g(x)$, excluding all D_j and $(ID_i, g(ID_i))$ for all $P_i \in \mathcal{P}^\ell$, and sets these $(m-k)$ coordinates as u. If $k \geq m$, then $u = \emptyset$.*
8. *D gives ω_i to P_i for all $i \in [1, n]$, and opens u as the auxiliary public value.*

Reconstruction Phase:

1. *As in the Shamir (k, ℓ)-threshold secret sharing, by using Lagrange interpolation, $g(x)$ is reconstructed from all ω_i of $P_i \in \mathcal{P}^\ell$ (and u if $k < m$).*
2. *By using Lagrange interpolation, $f_j(x)$ can be reconstructed from $(ID_{\mathcal{A}_j}, g(ID_{\mathcal{A}_j}))$ and (ID_i, ω_i) for all $P_i \in A_j \in \Gamma'$, and $s = f_j(0)$ can be computed.*

The first and second schemes are totally selectable (n, n)-threshold secret sharing schemes, and the third scheme is a $(1 - \frac{\ell}{n})$-quasi selectable secret sharing scheme realizing Γ defined in Definition 4. Security proofs are given in the Appendix.

4 Share Selectable Secret Sharing with Weak Shares

In this Section, we discuss the effect of the leakage information of the secret when a weak secret (e.g., a short human selected password with low Shannon's entropy) is indicated as a selectable share. To give the maximum information to

an unauthorized set of users A, we consider the situation where (1) A will be an authorized set if only one more user (who has a share ω) is added to A, (2) ω is a selectable share, and (3) ω is the weakest share in the underlying system (i.e., for the random variables W induced by ω, $H(W) = \min\{H(W_i) : H(W_i) < H(S)\}$ holds). Note that ω is a independent value of the secret s. Therefore, the mutual information between s and ω is 0 since $I(S;W) := H(S) + H(W) - H(S,W) = H(S)+H(W)-H(S)-H(W) = 0$. It is thus easy to conclude that $H(S|\mathcal{V}_A, U) = H(W) < H(S)$ holds.

5 Conclusion and Future Work

In this paper, we investigate the new concept *share selectable secret sharing*, where a dealer D can select shares independent of the secret. We propose two totally selectable (i.e., all users' share are selectable) secret sharing schemes with unanimous structure, and a quasi-selectable (i.e., a part of users' share are selectable) secret sharing scheme with certain hierarchical structures which contains special cases of the hierarchical threshold structures [41,42]. Our quasi scheme can be seen as an ideal secret sharing with flexible hierarchical structures which has not been done before to the best of our knowledge, and is of independent interest.

Although our research resorts mainly on the mathematical interest, applications of share selectable secret sharing are also realizable (as discussed in Section 1.5). As future work, it might be interesting to update access structures (resp. shares) without changing shares (resp. access structures).

References

1. Abdalla, M., Boyen, X., Chevalier, C., Pointcheval, D.: Distributed Public-key Cryptography from Weak Secrets. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 139–159. Springer, Heidelberg (2009)
2. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive Key-policy Attribute-based Encryption with Constant-size Ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 90–108. Springer, Heidelberg (2011)
3. Béguin, P., Cresti, A.: General Short Computational Secret Sharing Schemes. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 194–208. Springer, Heidelberg (1995)
4. Blakley, G.R., Meadows, C.: Security of Ramp Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 242–268. Springer, Heidelberg (1985)
5. Blundo, C., Cresti, A., De Santis, A., Vaccaro, U.: Fully dynamic secret sharing schemes. Theor. Comput. Sci. 165(2), 407–440 (1996)
6. Blundo, C., De Santis, A., Di Crescenzo, G., Gaggia, A.G., Vaccaro, U.: Multi-secret Sharing Schemes. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 150–163. Springer, Heidelberg (1994)
7. Boneh, D., Boyen, X., Halevi, S.: Chosen Ciphertext Secure Public Key Threshold Encryption without Random Oracles. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 226–243. Springer, Heidelberg (2006)

8. Boyen, X., Chevalier, C., Fuchsbauer, G., Pointcheval, D.: Strong Cryptography from Weak Secrets. In: Bernstein, D.J., Lange, T. (eds.) AFRICACRYPT 2010. LNCS, vol. 6055, pp. 297–315. Springer, Heidelberg (2010)
9. Brickell, E.F.: Some Ideal Secret Sharing Schemes. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 468–475. Springer, Heidelberg (1990)
10. Brickell, E.F., Stinson, D.R.: Some improved bounds on the information rate of perfect secret sharing schemes. J. Cryptology 5(3), 153–166 (1992)
11. Cachin, C.: On-line secret sharing. In: IMA Conf., pp. 190–198 (1995)
12. Csirmaz, L.: The size of a share must be large. J. Cryptology 10(4), 223–231 (1997)
13. Csirmaz, L., Tardos, G.: On-line secret sharing. Cryptology ePrint Archive, Report 2011/174 (2011), http://eprint.iacr.org/
14. Desmedt, Y., Frankel, Y.: Threshold Cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1990)
15. Dodis, Y., Wichs, D.: Non-malleable extractors and symmetric key cryptography from weak secrets. In: STOC, pp. 601–610 (2009)
16. Gennaro, R.: Faster and Shorter Password-authenticated Key Exchange. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 589–606. Springer, Heidelberg (2008)
17. Gentry, C., MacKenzie, P.D., Ramzan, Z.: Password authenticated key exchange using hidden smooth subgroups. In: ACM Conference on Computer and Communications Security, pp. 299–309 (2005)
18. Gordon, S.D., Katz, J.: Rational Secret Sharing, Revisited. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 229–241. Springer, Heidelberg (2006)
19. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
20. Halpern, J.Y., Teague, V.: Rational secret sharing and multiparty computation: extended abstract. In: STOC, pp. 623–632 (2004)
21. Herzberg, A., Jarecki, S., Krawczyk, H., Yung, M.: Proactive Secret Sharing or: How to Cope with Perpetual Leakage. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 339–352. Springer, Heidelberg (1995)
22. Hwang, R.-J., Chang, C.-C.: An on-line secret sharing scheme for multi-secrets. Computer Communications 21(13), 1170–1176 (1998)
23. Isshiki, T., Wada, K., Tanaka, K.: A rational secret-sharing scheme based on RSA-OAEP. IEICE Transactions 93-A(1), 42–49 (2010)
24. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. In: Proceedings IEEE Globecom 1987, pp. 99–102 (1987)
25. Iwamoto, M., Yamamoto, H., Ogawa, H.: Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures. IEICE Transactions 90-A(1), 101–112 (2007)
26. Katz, J., Ostrovsky, R., Yung, M.: Efficient Password-authenticated Key Exchange using Human-memorable Passwords. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 475–494. Springer, Heidelberg (2001)
27. Kol, G., Naor, M.: Games for exchanging information. In: STOC, pp. 423–432 (2008)
28. Krawczyk, H.: Secret Sharing Made Short. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 136–146. Springer, Heidelberg (1994)
29. Kurihara, J., Kiyomoto, S., Fukushima, K., Tanaka, T.: A fast (k, L, n)-threshold ramp secret sharing scheme. IEICE Transactions 92-A(8), 1808–1821 (2009)
30. MacKenzie, P.D., Shrimpton, T., Jakobsson, M.: Threshold password-authenticated key exchange. J. Cryptology 19(1), 27–66 (2006)

31. Martí-Farré, J., Padró, C.: Secret sharing schemes on access structures with intersection number equal to one. Discrete Applied Mathematics 154(3), 552–563 (2006)
32. Micali, S., Shelat, A.: Purely Rational Secret Sharing (Extended Abstract). In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 54–71. Springer, Heidelberg (2009)
33. Nikov, V., Nikova, S.: On Proactive Secret Sharing Schemes. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 308–325. Springer, Heidelberg (2004)
34. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden ciphertext policies. IEICE Transactions 92-A(1), 22–32 (2009)
35. Oba, T., Ogata, W.: Provably secure on-line secret sharing scheme. IEICE Transactions 94-A(1), 139–149 (2011)
36. Qin, B., Wu, Q., Zhang, L., Domingo-Ferrer, J.: Threshold Public-key Encryption with Adaptive Security and Short Ciphertexts. In: Soriano, M., Qing, S., López, J. (eds.) ICICS 2010. LNCS, vol. 6476, pp. 62–76. Springer, Heidelberg (2010)
37. Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979)
38. Shin, S., Kobara, K., Imai, H.: Security analysis of two augmented password-authenticated key exchange protocols. IEICE Transactions 93-A(11), 2092–2095 (2010)
39. Stinson, D.R., Wei, R.: Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures. In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, pp. 200–214. Springer, Heidelberg (2000)
40. Sun, H.-M.: On-line multiple secret sharing based on a one-way function. Computer Communications 22(8), 745–748 (1999)
41. Tassa, T.: Hierarchical Threshold Secret Sharing. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 473–490. Springer, Heidelberg (2004)
42. Tassa, T.: Hierarchical threshold secret sharing. J. Cryptology 20(2), 237–264 (2007)
43. Tassa, T., Dyn, N.: Multipartite secret sharing by bivariate interpolation. J. Cryptology 22(2), 227–258 (2009)
44. Tochikubo, K.: Efficient secret sharing schemes realizing general access structures. IEICE Transactions 87-A(7), 1788–1797 (2004)
45. Yamada, S., Attrapadung, N., Hanaoka, G., Kunihiro, N.: Generic Constructions for Chosen-ciphertext Secure Attribute Based Encryption. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 71–89. Springer, Heidelberg (2011)
46. Yoneyama, K.: Does secure password-based authenticated key exchange against leakage of internal states exist? IEICE Transactions 92-A(1), 113–121 (2009)

Appendix: Security Proofs

Here, we give security proofs of our schemes. As a reminder, we do not assume that a weak share is indicated as a selectable share (such weak cases has been considered in Section 4).

Theorem 1. *The first scheme is a totally selectable (n, n)-threshold secret sharing scheme.*

Proof. The condition $H(S|\mathcal{V}_A, U) = 0$ is clear when $A = \mathcal{P}$, since s can be reconstructed by computing $s = u + \sum_{i=1}^{n} \omega_i$. In addition, the condition $H(S|\mathcal{V}) = H(S)$ holds since each ω_i is independently chosen with the secret s. W.l.o.g., we set $\mathcal{V}_A := (P_1, \ldots, P_{n-1})$ as the unqualified set of users. Then, since the secret s is independent from $(u, \omega_1, \ldots, \omega_{n-1})$, $H(S|\mathcal{V}_A, U) = H(S)$ holds. □

Theorem 2. *The second scheme is a totally selectable (n, n)-threshold secret sharing scheme.*

Since the second scheme is a special case of the third scheme, we give the security proof of Theorem 2 with the proof of Theorem 3.

Theorem 3. *The third scheme is a $(1-\frac{\ell}{n})$-quasi selectable secret sharing scheme realizing Γ defined in Definition 4.*

As in Theorem 1, the condition $H(S|\mathcal{V}_A, U) = 0$ $(A \in \Gamma)$ and $H(S|\mathcal{V}) = H(S)$ hold, where $\mathcal{V} \subset \mathcal{W} := \bigcup_{i=1}^{n'} \mathcal{W}_i$ be a random variable of shares of users in $\mathcal{P}'$. So, the remaining part is $H(S|\mathcal{V}_A, U) = H(S)$ if $A \notin \Gamma$. Before giving the proof, we prove the following Proposition and Lemmas. Below in this proposition, the notation (M, N) represents the numbers of rows and columns, respectively.

Proposition 1. *Let A be an $M \times N$ matrix over a field, and the first column of A is $\boldsymbol{C} = [c_1, c_2, \ldots, c_M]^T$, where $A = [\ \boldsymbol{C} \mid B\ ]$. Then the first component of the solution for simultaneous equation $A\boldsymbol{x} = \boldsymbol{s}$ is not unique if and only if $rank(A) = rank(B)$.*

Proof. Let $W_A = \{\boldsymbol{x} | A\boldsymbol{x} = \boldsymbol{0}\}$. Then $\dim W_A = N - rank(A)$. We assume that $\boldsymbol{u}$ is a solution for $A\boldsymbol{x} = \boldsymbol{s}$. Then we can express the general solution for $A\boldsymbol{x} = \boldsymbol{s}$ as $\boldsymbol{x} = \boldsymbol{u} + \boldsymbol{x'}$, where $\boldsymbol{x'}$ satisfies $A\boldsymbol{x'} = \boldsymbol{0}$. We further assume that $\boldsymbol{x''}$ satisfies $B\boldsymbol{x''} = \boldsymbol{0}$. Then,

$$
\begin{aligned}
&\text{The first component of } \boldsymbol{x}, \text{ which is the solution for } A\boldsymbol{x} = \boldsymbol{s}\ , \text{ is unique.} \\
\iff\ & \boldsymbol{x'} = [0, \boldsymbol{x''}]^T. \\
\iff\ & \dim W_A = \dim W_B \\
\iff\ & N - rank(A) = N - 1 - rank(B) \\
\iff\ & rank(A) = rank(B) + 1
\end{aligned}
$$

Since $rank(A)$ is equal to $rank(B)$ or $rank(B) + 1$, then the first component of the solution for simultaneous equation $A\boldsymbol{x} = \boldsymbol{s}$ is not unique if and only if $rank(A) = rank(B)$. □

Next, we prove the following Lemma. For simplicity, we assume that $g(x)$ is a polynomial of degree at most $m - 1$ which passes through m coordinates $(ID_{\mathcal{A}_j}, f_j(ID_{\mathcal{A}_j}))$. Let P_s be an "imaginary" participant who has $g(x)$ as P_s's share, and $\mathcal{P}'$ be the set of users. Note that, here $\mathcal{P}^\ell$ is not considered, since P_s can be seen as $\mathcal{P}^\ell$ by using the Shamir (k, ℓ)-threshold scheme for the secret $g(x)$. Let $\mathcal{C}$ be the set of malicious participants such that they know the shares of one another.

Lemma 1. *We assume that the number of malicious participants be t $(n'+1 \geq t)$ in n' participants and one imaginary participant P_s. We calculate simultaneous equations for coefficient polynomial f_j $(j = 1, 2, \ldots, m)$ and shares of $n' + 1 - t$ honest participants. Let $V(n'+1, m, t)$ be the number of unknown quantities and*

$R(n'+1, m, t)$ be the number of simultaneous equations for malicious participants. Then $V(n'+1, m, t)$ and $R(n'+1, m, t)$ satisfy the following:

$$V(n'+1, m, t) = \begin{cases} R(n'+1, m, t) + (n' - t + 1) & (P_s \notin \mathcal{C}) \\ R(n'+1, m, t) + (n' - t - m + 2) & (P_s \in \mathcal{C}) \end{cases}$$

Proof.

The case of $P_s \notin \mathcal{C}$: W.l.o.g., we assume that P_i $(i = 1, 2, \ldots, t)$ are malicious participants. Let $\mathcal{C} = \{P_1, P_2, \ldots, P_t\} \notin \Gamma$ be the set of malicious participants. A polynomial of degree at most n_j is made for each qualified set A_j. So, the number of coefficients of the polynomial (except the secret value s) is n_j. We add the share of $n' - t$ honest participants, the share of a special participant P_s (i.e., a polynomial $g(x)$) and the secret value s to this, $V(n'+1, m, t) = 1 + n' - t + m + \sum_{j=1}^{m} n_j$. Now we assume that $P_i \in A_{k_j}$ $(j = 1, 2, \ldots, r_i)$, i.e., r_i is the number of qualified sets P_i belongs to. Then we can obtain r_i simultaneous equations. More specifically, $\omega_i = f_{k_1}(ID_i) = f_{k_2}(ID_i) = \cdots = f_{k_{r_i}}(ID_i)$. Moreover, we add a condition such that each polynomial f_j passes through coordinate $(ID_{\mathcal{A}_j}, f_j(ID_{\mathcal{A}_j}))$, $R(n'+1, m, t) = m + \sum_{i=1}^{n'} r_i$ holds. Then $\sum_{i=1}^{n'} r_i = \sum_{j=1}^{m} n_j$ holds, and therefore $\sum_{i=1}^{n'} r_i = \sum_{j=1}^{m} n_j = V(n'+1, m, t) - (m + n' - t + 1) = R(n'+1, m, t) - m$ holds.

The case of $P_s \in \mathcal{C}$: W.l.o.g., we assume that P_i $(i = 1, 2, \ldots, t-1)$ are malicious participants. Let $\mathcal{C} = \{P_s, P_1, P_2, \ldots, P_{t-1}\} \notin \Gamma$ represents the set of malicious participants. Similar to the case of $P_s \notin \mathcal{C}$, the number of coefficients of the polynomial (except the secret value s) is n_j. We add the share of $n' - (t-1)$ honest participants and the secret value s to this, $V(n'+1, m, t) = 1 + n' - (t-1) + \sum_{j=1}^{m} n_j$ holds. Moreover, $R(n'+1, m, t) = m + \sum_{i=1}^{n'} r_i$ holds. So $\sum_{i=1}^{n'} r_i = \sum_{j=1}^{m} n_j = V(n'+1, m, t) - (n' - t + 2) = R(n'+1, m, t) - m$ holds. □

Lemma 2. *We assume that $P_s \notin \mathcal{C}$. In this situation, the secret value s cannot be determined with $R(n'+1, m, n')$ simultaneous equations.*

Proof. Let $\Gamma'' = \{A' = A \cup \{U_s\} : A \in \Gamma\}$. For any $B_j \in \Gamma''$, let $f_j(x) = s + a_{j_1}x + a_{j_2}x^2 + \cdots + a_{j_{n_j}}x^{n_j}$ be the polynomial associated with $B_j = \{P_s, P_{j_1}, P_{j_2}, \ldots, P_{j_{n_j}}\}$. Note that $f_j(ID_{\mathcal{A}_j}) = g(ID_{\mathcal{A}_j})$. So, simultaneous equations for s, a_{j_1}, $a_{j_2}, \ldots, a_{j_n}, g(ID_{\mathcal{A}_j})$ are (1)

$$N_j = \begin{bmatrix} 1 & 0 & ID_{j_1} & {ID_{j_1}}^2 & \cdots & {ID_{j_1}}^{n_j} \\ 1 & 0 & ID_{j_2} & {ID_{j_2}}^2 & \cdots & {ID_{j_2}}^{n_j} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & ID_{j_{n_j}} & {ID_{j_{n_j}}}^2 & \cdots & {ID_{j_{n_j}}}^{n_j} \\ 1 & -1 & x_{d,j} & {x_{d,j}}^2 & \cdots & {x_{d,j}}^{n_j} \end{bmatrix} \text{ and } N_j \begin{bmatrix} s \\ g(ID_{\mathcal{A}_j}) \\ a_{j_1} \\ a_{j_2} \\ \vdots \\ a_{j_{n_j}} \end{bmatrix} = \begin{bmatrix} \omega_{j_1} \\ \omega_{j_2} \\ \vdots \\ \omega_{j_{n_j}} \\ 0 \end{bmatrix} \tag{1}$$

Moreover, we define that $\boldsymbol{C} = [\ \overbrace{1, 1, \ldots, 1}^{1+m+\sum_{j=1}^{m} n_j}\ ]^T$,

$$M_j = \begin{bmatrix} 0 & ID_{j_1} & {ID_{j_1}}^2 & \cdots & {ID_{j_1}}^{n_j} \\ 0 & ID_{j_2} & {ID_{j_2}}^2 & \cdots & {ID_{j_2}}^{n_j} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & ID_{j_{n_j}} & {ID_{j_{n_j}}}^2 & \cdots & {ID_{j_{n_j}}}^{n_j} \\ -1 & ID_{\mathcal{A}_j} & {ID_{\mathcal{A}_j}}^2 & \cdots & {ID_{\mathcal{A}_j}}^{n_j} \end{bmatrix} \text{ and } M' = \begin{bmatrix} & & 0 \cdots 0 & 0 \cdots 0 \\ & M_1 & \vdots \ddots \vdots & \ddots \vdots \\ & & 0 \cdots 0 & 0 \cdots 0 \\ 0 \cdots 0 & & & 0 \cdots 0 \\ \vdots \ddots \vdots & & & \ddots & 0 \cdots 0 \\ 0 \cdots 0 & & & & 0 \cdots 0 \\ 0 \cdots 0 & 0 \cdots 0 & & & \\ \vdots \ddots \vdots & \vdots \ddots \vdots & & & M_m \\ 0 \cdots 0 & 0 \cdots 0 & & & \end{bmatrix}$$

Then, all simultaneous equations are as follows:

$$[\boldsymbol{C} \mid M'] \begin{bmatrix} s \\ g(ID_{\mathcal{A}_1}) \\ a_{1_1} \\ \vdots \\ a_{1_{n_1}} \\ g(ID_{\mathcal{A}_2}) \\ a_{2_1} \\ \vdots \\ \vdots \\ g(ID_{\mathcal{A}_m}) \\ a_{m_1} \\ \vdots \\ a_{m_{n_m}} \end{bmatrix} = \begin{bmatrix} * \\ * \\ * \\ \vdots \\ * \\ * \\ * \end{bmatrix}$$

Here, we prove that matrices $M_1, M_2, \ldots, M_m$ are regular. Let $\boldsymbol{a}_h$ $(h = 1, 2, \ldots, n_j+1)$ be column vectors and $c_h \in \mathbb{F}_p$ be scalars on M_j. Then $c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_{n_j+1}\boldsymbol{a}_{n_j+1} = 0$ holds. Let M'_j be the matrix which is M_j except the first column and the $(n_j + 1)$'th row. Then M'_j is regular, since it is a Vandermonde matrix. We can obtain that $c_2 = c_3 = \ldots = c_{n_j+1} = 0$ since $\boldsymbol{a}_1 = [0, 0, \ldots, 0, -1]^T$. Therefore $-c_1 = 0$ holds (and so $c_1 = 0$). That is, M_j is regular.

Let $\boldsymbol{C}_j = [1, 1, \ldots, 1]^T$ $(j = 1, \ldots, m)$ which is the first column of N_j. Then, there exist $\alpha_i \in \mathbb{F}_p$ such that $\boldsymbol{C}_j = \sum_{i=1}^{n_j+1} \alpha_i \boldsymbol{a}_i$. Since this condition is satisfied for all j $(j = 1, 2, \ldots, m)$, $rank([\boldsymbol{C} \mid N]) = rank(N)$ holds. By Proposition 1, an unqualified set cannot compute any information about s. □

Similar to the above, we prove Corollary 1. The notion was defined in the proof of Lemma 2.

Corollary 1. *We assume that $P_s \notin \mathcal{C}$. In this situation, $g(ID_{\mathcal{A}_j})$ $(j = 1, 2, \ldots, m)$ cannot be determined from $R(n' + 1, m, n')$ simultaneous equations.*

Proof. Similar to Lemma 2, let $\boldsymbol{C}_j = [1, 1, \ldots, 1]^T$ which is the first column of N_j. Then, there exist $\alpha_i \in \mathbb{F}_p$ such that $\boldsymbol{C}_j = \sum_{i=1}^{n_j+1} \alpha_i \boldsymbol{a}_i$. Then also $[\boldsymbol{C}_j \mid \boldsymbol{a}_2\ \boldsymbol{a}_3\ \cdots\ \boldsymbol{a}_{n_j+1}]$ is a Vandermonde matrix. Then, there exist β_i $(i = 1, 2, \ldots, n_j + 1)$ such that $\boldsymbol{a}_1 = \beta_1 \boldsymbol{C}_j + \sum_{i=2,}^{n_j+1} \beta_i \boldsymbol{a}_i$. By Proposition 1, an unqualified set cannot compute any information about $g(ID_{\mathcal{A}_j})$. We previously assumed that $ID_{\mathcal{A}_i} \neq ID_{\mathcal{A}_j}$. Therefore $g(ID_{\mathcal{A}_j})$ only appear on N_j, and an unqualified set cannot compute any information about $g(ID_{\mathcal{A}_j})$ $(j = 1, 2, \ldots, m)$. □

By Lemma 2 and Corollary 3, Theorem 3 is proven by regarding as the share of P_s, $g(x)$, is distributed by using the Shamir (k, ℓ)-threshold secret sharing.

Next, we assume that $P_s \in \mathcal{C}$, i.e., malicious participants can obtain a polynomial $g(x)$. We can obtain the corollary as follows:

Corollary 2. *We assume that an access structure for n' participants and one special participant P_s is unanimous, i.e., $(n'+1, n'+1)$ threshold structure. Then $V(n'+1, m, t) > R(n'+1, m, t)$.*

Proof. The case $P_s \notin \mathcal{C}$, obviously hold. We assume that $P_s \in \mathcal{C}$. Then the number of participants that can collude is n' ($n'-1$ participants and P_s). Therefore $V(n'+1, m, t) = R(n'+1, m, t) + (n' - t - m + 2) > R(n'+1, m, t) + (n' - n' - 1 + 2) = R(n'+1, m, t) + 1$ holds. □

Lemma 3. *We assume that an access structure for n' participants and one special participant P_s is unanimous, i.e., $(n'+1, n'+1)$ threshold structure. Then the secret value s cannot be determined from $R(n'+1, m, n')$ simultaneous equations.*

Proof. Let $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{n'} x^{n'}$ be the polynomial associated with $B = \{P_s, P_1, P_2, \ldots, P_{n'}\}$. W.l.o.g., we assume P_1 to be the honest participant. So, malicious participants can obtain simultaneous equation as follows (2):

$$N' = \begin{bmatrix} 1 & -1 & ID_1 & ID_1^2 & \cdots & ID_1^{n'} \\ 1 & 0 & ID_2 & ID_2^2 & \cdots & ID_2^{n'} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & ID_{n'} & ID_{n'}^2 & \cdots & ID_{n'}^{n'} \\ 1 & 0 & ID_D & {ID_D}^2 & \cdots & {ID_D}^{n'} \end{bmatrix} \text{ and } N' \begin{bmatrix} s \\ \omega_1 \\ a_1 \\ a_2 \\ \vdots \\ a_{n'} \end{bmatrix} = \begin{bmatrix} 0 \\ \omega_2 \\ \omega_3 \\ \vdots \\ \omega_{n'} \\ g(ID_D) \end{bmatrix} \tag{2}$$

Similar to Lemma 2, the $(n'+1) \times (n'+1)$ matrix which is N' except the first column is Vandermonde. Moreover, the $(n'+1) \times (n'+1)$ matrix which is N' except the second column is also Vandermonde. By Proposition 1, the set of malicious participants cannot determine the secret value s and the shares of honest participants. □

By Lemma 3, Theorem 2 is proven by regarding as the share of P_s, i.e., $g(ID_D) = f(ID_D)$, is publicly opened as u.