Security Analysis of a Multi-secret Sharing Scheme with Unconditional Security

Min Xiao[1] and Zhe Xia[1,2](✉)

[1] School of Computer Science, Wuhan University of Technology,
Wuhan 430070, China
xiazhe@whut.edu.cn

[2] Guizhou Key Laboratory of Public Big Data,
Guizhou University, Guiyang 550025, China

Abstract. Harn has introduced a (t, n) threshold secret sharing scheme recently, in which shareholders' shares are not disclosed in the secret reconstruction phase. The benefit is that the outside adversary cannot learn the secret even if it is recovered by more than t shareholders. Moreover, Harn has further extended this scheme into a multi-secret sharing scheme so that multiple secrets can be recovered individually at different stagies. Both schemes are claimed to achieve the perfectness property using heuristic arguments. However, in this paper, we show that the above claim is false and these schemes are not perfect. In the first scheme, the coalition of $t-1$ shareholders can conclude that the secret is not uniformly distributed. And in the multi-secret sharing scheme, when the public parameters satisfy some special conditions, the coalition of $t-1$ shareholders can even use the recovered secrets to preclude some possible values for the unrecovered secrets.

Keywords: Threat analysis · Multi-secret sharing · Unconditional security

1 Introduction

Secret sharing is an fundamental building block in information security and cryptography. Over the last few decades, great efforts have devoted to designing various secret sharing schemes [1,3,14].

In traditional (t, n) threshold secret sharing schemes [4,5,11–13], the dealer first generates the shares and sends each share to a shareholder. Afterwards, the secret can be recovered if t or more than t of these shareholders reveal their shares. However, one drawback of these schemes is that when there are more than t shareholders in the secret reconstruction, the outside adversary may impersonate to be a shareholder, contribute an invalid share or even do not contribute any share, and learn the secret after the other shareholders have

G. Wang et al. (Eds.): SpaCCS 2020, LNCS 12383, pp. 533–544, 2021.
https://doi.org/10.1007/978-3-030-68884-4_44

revealed their shares. Obviously, this is not ideal for many applications where the secret should only be recovered among the legitimate shareholders. The problem can be solved if some proper authentication mechanism is added on top of the secret sharing scheme, but this will introduce additional complexity, because most of the user authentication schemes authenticate one user at a time.

In order to solve the above problem, Harn has proposed an interesting solution in [10]. To recover the secret in Harn's scheme, each shareholder uses her share as well as a value u (where $t \leq u \leq n$) to compute a shadow, where u is the expected number of shareholders participated in the secret reconstruction. Afterwards, each shareholder reveals this shadow instead of her share. The secret can be reconstructed if and only if there are exactly u shadows and all these shadows are correctly computed. Therefore, the outside adversary cannot use the same strategy to learn the secret, because she cannot compute a shadow without the knowledge of a valid share. Another appealing feature of this scheme is that the shadow will not disclose the corresponding share. And Harn has used this property to further extend the scheme into a multi-secret sharing scheme, in which the shareholders can reuse their shares to recover multiple secrets individually at different stagies. Note that both these schemes are not relying on any computational assumption, and the shareholders or the outside adversary are allowed to have unlimited computational power.

It was claimed in [10] that these two schemes both satisfy the perfectness property. Informally, this means that in the single secret sharing scheme, the coalition of $t-1$ shareholders cannot learn any information of the secret, and in the multi-secret sharing scheme, $t-1$ colluded shareholders cannot learn any information of the unrecovered secret even if some secrets have already been recovered. The above claims are argued based on the following reasons. Because the number of equations obtained by the $t-1$ shareholders and the outside adversary is less than the number of unknown values, the system of equations cannot be solved and the unkonwn values cannot be retrieved. Therefore, no information about the secret can be learned either by the colluding shareholders or by the outside adversary[1].

Our Contributions. In this paper, we demonstrate that Harn's schemes in [10] are not perfect. Firstly, we extend Ghodosi's results [8] to prove that Harn's single secret sharing scheme is not perfect. Although $t-1$ colluded shareholders can neither recover the secret nor preclude some possible values for the secret, they are able to conclude that the secret is not uniformly distributed. Secondly, we introduce a new method to analyse secret sharing schemes based on hyperplane geometry, and we use it to illustrate that in Harn's multi-secret sharing scheme, the coalition of $t-1$ shareholders can conclude that the secret is not uniformly distributed as well. Our method is more versatile than Ghodosi's one [8] and it may have some independent interests. Moreover, we show that when the public parameters satisfy some special conditions, these colluding shareholders also can

[1] Note that similar technique has been used in [9] and this scheme was attacked by a novel cryptanalysis, called linear subspace attack [2]. But our work is different from the existing attack and it illustrates some other weaknesses of Harn's work.

use the recovered secrets to preclude some possible values for the unrecovered secrets. Because both Harn's schemes have been claimed to achieve the perfectness property using heuristic arguments, our results provide some evidences that heuristic arguments may not be adequate to analyse the perfectness properties of secret sharing schemes. In order to carry out proper security analysis, formal methods should be used instead.

Outline of the Paper. The rest of this paper is organised as follows: some prelimilaries are outlined in Sect. 2. Harn's proposed secret sharing schemes are reviewed in Sect. 3. And in Sect. 4, we describe why both Harn's schemes fail to achieve the perfectness property, and how to make them perfect. Finally, we conclude in Sect. 5.

2 Prelimilaries

In this section, we describe some prelimilaries relate to the perfectness property of secret sharing schemes, including its definitions, the necessary conditions for lower bounds on the length of each share, and Ghodosi's results on perfectness.

2.1 Perfectness in Single Secret Sharing Schemes

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of n shareholders, and let $\mathcal{K}, \mathcal{S}$ be the secret set and the share set respectively. Let $\varGamma$ be a collection of authorised subsets of $2^{\mathcal{P}}$, called the access structure. In the share distribution phase, to share a secret $s \in \mathcal{K}$, each shareholder $P_i \in \mathcal{P}$ receives a share $\mathsf{sh}_i \in \mathcal{S}$ from the dealer. In the secret reconstruction phase, any authorised subset $\mathcal{A} \in \varGamma$ of shareholders can use their shares to recover the secret. But any non-authorised subset $\mathcal{B} \notin \varGamma$ of shareholders can learn no information about the secret.

The above two requirements can be formalised using the entropy $\mathsf{H}(\cdot)$ of random variables in information theory. Denote S as the random variable associated to the secret, SH_i as the random variable associated to P_i's share, and $\mathsf{SH}_{\mathcal{A}}$ as the vector of random variables associated to the shares belonging to the shareholders in the subset $\mathcal{A} \subset \mathcal{P}$. The perfect secret sharing scheme should satisfy the following two requirements:

- *Correctness:* Given the subset of shares $\{\mathsf{sh}_i\}_{P_i \in \mathcal{A}}$, we have $\mathsf{H}(\mathsf{S}|\mathsf{SH}_{\mathcal{A}}) = 0$ for any subset $\mathcal{A} \in \varGamma$.
- *Secrecy:* Given the subset of shares $\{\mathsf{sh}_i\}_{P_i \in \mathcal{B}}$, we have $\mathsf{H}(\mathsf{S}|\mathsf{SH}_{\mathcal{B}}) = \mathsf{H}(\mathsf{S})$ for any subset $\mathcal{B} \notin \varGamma$.

For any threshold secret sharing scheme that achieves the perfectness property, Brickell [7] has given the lower bounds on the length of each share: the equation $\mathsf{H}(\mathsf{SH}_i) \geq \mathsf{H}(\mathsf{S})$ needs to be hold for every shareholder $P_i \in \mathcal{P}$. In other words, the length of each share has to be equal or larger than the length of the secret.

2.2 Perfectness in Multi-secret Sharing Schemes

Let $s_1, s_2, \ldots, s_h \in \mathcal{K}$ be h secrets shared at the same time, and $\Gamma_1, \Gamma_2, \ldots, \Gamma_h \subset 2^{\mathcal{P}}$ be the corresponding access structures. In the share distribution phase, the dealer distributes the secrets according to their access structures. Each shareholder $P_i \in \mathcal{P}$ receives a share $\mathsf{sh}_i \in \mathcal{S}$. In the secret reconstruction phase, given a subset of shares and an index $j \in \{1, 2, \ldots, h\}$, the expected output is the j-th secret s_j. Denote S_j as the random variable associated to the secret s_j. The perfect multi-secret sharing scheme should satisfy the following two requirements:

- *Correctness:* Given the subset of shares $\{\mathsf{sh}_i\}_{P_i \in \mathcal{A}}$ and an index j, we have $\mathsf{H}(\mathsf{S}_j|\mathsf{SH}_{\mathcal{A}}) = 0$ for any subset $\mathcal{A} \in \Gamma_j$.
- *Secrecy:* Denote $\mathsf{T} \subset \{s_1, s_2, \ldots s_h\} \backslash \{s_j\}$ as the set of recovered secrets in the previous stagies. Given the subset of shares $\{\mathsf{sh}_i\}_{P_i \in \mathcal{B}}$ and an index j, we have $\mathsf{H}(\mathsf{S}_j|\mathsf{SH}_{\mathcal{B}}, \mathsf{T}) = \mathsf{H}(\mathsf{S}_j|\mathsf{T})$ for any subset $\mathcal{B} \notin \Gamma_j$.

For any threshold multi-secret sharing scheme that satisfies the perfectness property, Blundo et al. [6] have given the lower bounds on the length of each share: the equation $\mathsf{H}(\mathsf{SH}_i) \geq \sum_{j=1}^{h} \mathsf{H}(\mathsf{S}_j)$ needs to be hold for every shareholder $P_i \in \mathcal{P}$. In other words, the length of each share has to be equal or larger than the total length of the secrets.

2.3 Ghodosi's Results on Perfectness

In [13], Shamir has proposed a perfect (t, n) threshold secret sharing schemes, in which at least t shareholders can recover the secret. In other words, the access structure is $\Gamma = \{\mathcal{A} \subset \mathcal{P} : |\mathcal{A}| \geq t\}$. The secret set $\mathcal{K}$ is a finite field. To share a secret $s \in \mathcal{K}$, a random polynomial $f(x) \in \mathcal{K}[x]$ with degree *at most* $t - 1$ is generated by the dealer, such that $f(0) = s$. Then every shareholder $P_i \in \mathcal{P}$ receives the share $\mathsf{sh}_i = f(x_i)$, where $x_i \in \mathcal{K} \backslash \{0\}$ are publicly known and pairwise different values. In the secret reconstruction phase, any subset of t or more shares can recover the secret through polynomial interpolation, but less than t shares can derive no information of the secret.

Note that many papers in the literature have misused Shamir's secret sharing by requiring the dealer to randomly select the polynomial $f(x)$ of degree $t - 1$. In this case, although the length of each shareholder's share still satisfies the lower bounds given by Brickell, Ghodosi et al. [8] have pointed out that if the degree of $f(x)$ was known to be $t-1$, then Shamir's secret sharing scheme is not perfect. The consequence is that any coalition of $t-1$ shareholders can preclude a possible value for the secret using the following strategy.

Denote $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$ with $a_{t-1} \neq 0$. Then, $t - 1$ colluded shareholders can interpolate a $t - 2$ degree polynomial $g(x) = b_0 + b_1 x + \cdots + b_{t-2} x^{t-2}$, such that $f(x_i) = g(x_i)$ for $1 \leq i \leq t - 1$. This leads the system of equations:

$$\begin{cases} (a_0 - b_0) + (a_1 - b_1)x_1 + \cdots + (a_{t-2} - b_{t-2}){x_1}^{t-2} + a_{t-1}{x_1}^{t-1} & = 0 \\ (a_0 - b_0) + (a_1 - b_1)x_2 + \cdots + (a_{t-2} - b_{t-2}){x_2}^{t-2} + a_{t-1}{x_2}^{t-1} & = 0 \\ & \vdots \\ (a_0 - b_0) + (a_1 - b_1)x_{t-1} + \cdots + (a_{t-2} - b_{t-2}){x_{t-1}}^{t-2} + a_{t-1}{x_{t-1}}^{t-1} & = 0 \end{cases}$$

By contradiction, if we assume that $a_0 = b_0$, then the above system of equations with $t - 1$ equations and $t - 1$ unknown values $\{a_1, a_2, \ldots, a_{t-1}\}$ will have a unique solution. This is because the determinant of a Vandermonde matrix is not 0. Hence, the solution must be $a_1 = b_1, a_2 = b_2, \ldots, a_{t-2} = b_{t-2}$, and $a_{t-1} = 0$. This contradicts the assumption that $a_{t-1} \neq 0$. Therefore, any $t - 1$ shareholders can preclude b_0 as a possible value of the secret.

3 Review of Harn's Schemes

In this section, we review Harn's secret sharing schemes [10] and briefly explain why it is claimed that they can satisfy the perfectness property.

3.1 Models

The system model, communication model and adversary model used in Harn's schemes are as follows:

System Model. The players include a trusted dealer $\mathcal{D}$, n shareholders $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ and some insider or outsider adversaries. It is assumed that all these players have unlimited computational resources. Among these shareholders, it is assumed that at least t of them are honest, where $t > n/2$. Note that this setting prevents the dishonest shareholders from learning the secret even if they all collude. Here, the word "dishonest" means honest-but-curious. That is, these dishonest shareholders will follow the protocol, but they may try to learn information that should remain private.

Communication Model. It is assumed that there exists a secure channel between the dealer and every shareholder, so that the shares can be securely distributed to the shareholders. Moreover, it is assumed that every player is connected to a common authenticated broadcast channel $\mathcal{C}$. Any message sent through $\mathcal{C}$ can be heard by the other players. The adversary can neither modify messages sent by an honest player through $\mathcal{C}$, nor she can prevent honest players from receiving messages from $\mathcal{C}$. Note that these are standard assumptions widely used in existing secret sharing schemes.

Adversary Model. Two types of adversaries are considered in Harn's secret sharing schemes:

- *Inside adversary* is a legitimate shareholder who owns a valid share generated by the dealer. An insider adversary may work alone or collude with some other inside adversaries in order to learn the secrets before they are reconstructed. The restriction is that the maximum number of colluded inside adversaries is $t - 1$.

- *Outside adversary* is an attacker who does not own any valid share. But she may participate in the secret reconstruction phase, impersonate to be a shareholder, and learn the secret after the other shareholders have revealed their shares.

3.2 The Single Secret Sharing Scheme

- **Share distribution phase.**
  1. The dealer $\mathcal{D}$ selects k random polynomials $f_l(x)$ over $\mathbb{F}_p$ for $l = 1, 2, \ldots, k$, having degree $t-1$ each. Here, p is a prime that satisfies $p > n$.
  2. Then, $\mathcal{D}$ generates the shares $\mathsf{sh}_i = f_l(x_i) \pmod p$ for $i = 1, 2, \ldots, n$, and sends each share to the corresponding shareholder through the secure channel. The values $x_i \in \mathbb{F}_p \backslash \{0\}$ are publicly known and pairwise different. In the rest of this paper, we assume that all equations are modulo p unless otherwise stated.
  3. To share the secret $s \in \mathbb{F}_p$, the dealer finds integers $w_l, d_l \in \mathbb{F}_p$ for $l = 1, 2, \ldots, k$, such that $s = \sum_{l=1}^{k} d_l f_l(w_l)$. The values w_l need to be pairwise different, and the intersection of the two sets $\{x_1, x_2, \ldots, x_n\}$ and $\{w_1, w_2, \ldots, w_k\}$ needs to be empty. The dealer $\mathcal{D}$ makes these integers w_l, d_l publicly known for $l = 1, 2, \ldots, k$.
- **Secret reconstruction phase.**
  1. Suppose u shareholders participate in the secret reconstruction phase, where $t \leq u \leq n$. Each shareholder P_i uses her share sh_i and the value u to compute the shadow c_i as:

$$c_i = \sum_{l=1}^{k} d_l f_l(x_i) \prod_{v=1, v \neq i}^{u} \frac{w_l - x_v}{x_i - x_v}$$

     And then, P_i sends the shadow c_i to the authenticated broadcast channel.
  2. After receiving all the shadows c_i for $i = 1, 2, \ldots, u$, every shareholder can compute the secret as $s = \sum_{i=1}^{u} c_i$.

To prove that the above scheme is perfect, it needs to show that both the correctness and secrecy requirements (introduced in Sect. 2) are satisfied. It is easy to see that the correctness requirement holds, because we have

$$\begin{aligned} s = \sum_{i=1}^{u} c_i &= \sum_{i=1}^{u} \sum_{l=1}^{k} (d_l f_l(x_i) \prod_{v=1, v \neq i}^{u} \frac{w_l - x_v}{x_i - x_v}) \\ &= \sum_{l=1}^{k} (d_l \sum_{i=1}^{u} (f_l(x_i) \prod_{v=1, v \neq i}^{u} \frac{w_l - x_v}{x_i - x_v})) \\ &= \sum_{l=1}^{k} d_l f_l(w_l) \end{aligned}$$

Harn has claimed that if $kt > n-1$, then the secrecy requirement also holds. Considering the worst case that n players are involved to recover the secret and the outside adversary is the last one to reveal her shadow. Then, the outside adversary can obtain at most $n-1$ equations. But because the number of unkonwn values kt is larger than the number of equations, the outside adversary cannot learn any information of the secret. Moreover, the coalition of $t-1$ shareholders can obtain at most $k(t-1)$ equations, which is smaller than the number kt of unkonwn values. Hence, the inside adversaries cannot learn any information of the secret neither. Therefore, it is concluded that the secrecy requirement holds, and this scheme is perfect with unconditional security.

3.3 The Multi-secret Sharing Scheme

- **Share distribution phase.**
  1. To share h secrets $\{s_1, s_2, \ldots, s_h\}$, the dealer $\mathcal{D}$ first selects k random polynomials $f_l(x)$ over $\mathbb{F}_p$ for $l = 1, 2, \ldots, k$, having degree $t-1$ each.
  2. Then, $\mathcal{D}$ generates the shares $\mathsf{sh}_i = f_l(x_i)$ for $i = 1, 2, \ldots, n$, and distributes them to the corresponding shareholders through the secure channel. Similarly, the values $x_i \in \mathbb{F}_p \backslash \{0\}$ need to be publicly known and pairwise different.
  3. The dealer $\mathcal{D}$ finds some integers $w_l \in \mathbb{F}_p$ for $l = 1, 2, \ldots, k$, such that they are pairwise different and $w_l \notin \{x_1, x_2, \ldots, x_n\}$. For every secret s_j, where $j \in \{1, 2, \ldots, h\}$, the dealer $\mathcal{D}$ also finds some integers $d_{j,l} \in \mathbb{F}_p$ for $l = 1, 2, \ldots, k$, such that $s_j = \sum_{l=1}^{k} d_{j,l} f_l(w_l)$. Moreover, it is required that all the vectors $< d_{j,1}, d_{j,2}, \ldots, d_{j,k} >$ are linearly independent. The dealer $\mathcal{D}$ makes these integers $w_l, d_{j,l}$ publicly known.
- **Secret reconstruction phase.**
  1. Suppose u shareholders participate to recover the secret s_j, where $t \leq u \leq n$ and $j \in \{1, 2, \ldots, h\}$. Each shareholder P_i uses her share sh_i as well as the values u and j to compute the shadow $c_{j,i}$ as:

     $$c_{j,i} = \sum_{l=1}^{k} d_{j,l} f_l(x_i) \prod_{v=1, v \neq i}^{u} \frac{w_l - x_v}{x_i - x_v}$$

     Then, P_i sends this shadow $c_{j,i}$ to the authenticated broadcast channel.
  2. After receiving all the shadows $c_{j,i}$ for $i = 1, 2, \ldots, u$, every shareholder can calculate the secret as $s_j = \sum_{i=1}^{u} c_{j,i}$.

Similar as in the above secret sharing scheme, the multi-secret sharing scheme also satisfies the correctness requirement. In order to achieve the secrecy requirement, Harn has imposed the restriction that all the vectors $< d_{j,1}, d_{j,2}, \ldots, d_{j,k} >$ are linearly independent. Because these vectors are public parameters, and they satisfy the following condition:

$$\begin{bmatrix} d_{1,1} & d_{1,2} & \ldots & d_{1,k} \\ d_{2,1} & d_{2,2} & \ldots & d_{2,k} \\ \vdots & \vdots & & \\ d_{h,1} & d_{h,2} & \ldots & d_{h,k} \end{bmatrix} \cdot \begin{bmatrix} f_1(w_1) \\ f_2(w_2) \\ \vdots \\ f_k(w_k) \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_h \end{bmatrix}$$

If there exists some linear relationship among these vectors, anyone may learn some uncovered secret using the linear combination of previously recovered secrets. Moreover, the parameters need to satisfy $kt > h(n+1) - 2$ and $k > (h-1)(n-t+2)$ as well. This ensures that even in the worst case, neither the outside adversary nor the coalition of $t-1$ shareholders can obtain enough equations to learn the polynomials' coefficients. Therefore, Harn has also claimed that this multi-secret sharing scheme is perfect with unconditional security.

4 Threat Analysis of Harn's Schemes

In this section, we revisit Harn's schemes in [10], demonstrating that both his schemes fail to achieve the perfectness property. Because we have already shown in Sect. 3 that the correctness requirement holds, our focus is only to prove that Harn's schemes fail to satisfy the secrecy requirement. Then, we explain how to modify Harn's schemes to be perfect.

4.1 Analysis of the Single Secret Sharing Scheme

We first analyse whether Brickell's lower bounds on the length of each share are satisfied in Harn's single secret sharing scheme. If not, it can be simply concluded that this scheme is not perfect. Recall that in the threshold secret sharing scheme, the threshold value t has to be in the range $n/2 < t \leq n$. Then, $kt > n-1$ implies that $k \geq 1$. Hence, each shareholder's share is at least one value $f_l(x_i)$ in $\mathbb{F}_p$. Moreover, since the dealer $\mathcal{D}$ is assumed to be trusted, she will randomly generate the polynomial $f_l(x)$ over $\mathbb{F}_p$. The value $f_l(x_i)$ is randomly distributed in $\mathbb{F}_p$. Therefore, we have $\mathsf{H}(\mathsf{SH}_i) \geq \mathsf{H}(\mathsf{S})$ for every shareholder $P_i \in \mathcal{P}$, and Brickell's lower bounds on the length of each share are satisfied.

Now, we extend Ghodosi's results [8] to prove that Harn's single secret sharing scheme fails to satisfy the secrecy requirement. Without loss of generality, suppose the first $t-1$ shareholders $\{P_1, P_2, \ldots, P_{t-1}\}$ are colluding.

1. Firstly, based on Harn's description that "the dealer $\mathcal{D}$ selects k random polynomials $f_l(x) = a_{l,0} + a_{l,1}x + \ldots + a_{l,t-1}x^{t-1}$ over $\mathbb{F}_p$ for $l = 1, 2, \ldots, k$, having degree $t-1$ each", these colluded shareholders can apply Ghodosi's results (introduced in Sect. 2.3) to preclude one possible value for every $a_{l,0}$.
2. Secondly, we show that these shareholders also can preclude one possible value for every $f_l(w_l)$:

$$f_l(w_l) = a_{l,0}\lambda_{l,0} + \sum_{i=1}^{t-1} f_l(x_i)\lambda_{l,i}$$

where

$$\lambda_{l,0} = \prod_{j=1}^{t-1} \frac{x_j - w_l}{x_j}, \quad \text{and} \quad \lambda_{l,i} = \prod_{j=0, j\neq i}^{t-1} \frac{w_l - x_j}{x_i - x_j}$$

Because the values $x_i \in \mathbb{F}_p \backslash \{0\}$ and $w_l \notin \{x_1, x_2, \ldots, x_n\}$ for $l = 1, 2, \ldots, k$, we have $\gcd(\lambda_{l,0}, p) = 1$. The function $f_l(w_l)$ is bijective when treating $a_{l,0}$

as the unknown value. Hence, every different value of $a_{l,0}$ will result a unique value of $f_l(w_l)$.

3. Finally, recall that the secret is $s = \sum_{l=1}^{k} d_l f_l(w_l)$. Since one possible value for every $f_l(w_l)$ have been precluded, every $d_l f_l(w_l) \in \mathbb{F}_p$ can have only $p-1$ possible values if $d_l \neq 0$, and $d_l f_l(w_l) = 0$ if $d_l = 0$. Denote k' as the number of d_l values that equal to 0. Obviously, $k' = k$ is meaningless, because the secret s will be fixed as 0 in this case. Before the modulo p operation, the secret s will have $(p-1)^{k-k'}$ possible values. Since p does not divide $(p-1)^{k-k'}$, after the modulo p operation, the secret s cannot be uniformly distributed within $\mathbb{F}_p$. Therefore, for the subset of shares $\{\mathsf{sh}_i\}_{P_i \in \mathcal{B}}$, we have $\mathsf{H}(\mathsf{S}|\mathsf{SH}_{\mathcal{B}}) < \mathsf{H}(\mathsf{S})$ for any set $|\mathcal{B}| = t-1$. In other words, the secrecy requirement does not hold, and this secret sharing scheme is not perfect.

4.2 Analysis of the Multi-secret Sharing Scheme

We first analyse whether Blundo's lower bounds on the length of each share are satisfied in Harn's multi-secret sharing scheme. When they are not satisfied, we can easily conclude that the scheme is not perfect. Since $n/2 < t \leq n$, and Harn has required that $kt > h(n+1) - 2$ and $k > (h-1)(n-t+2)$, we have $k \geq h$. Each shareholder's share is k values of $f_l(x_i)$ for $l = 1, 2, \ldots, k$ that are randomly distributed in $\mathbb{F}_p$. Therefore, we have $\mathsf{H}(\mathsf{SH}_i) \geq \sum_{j=1}^{h} \mathsf{H}(\mathsf{S}_j)$ for every shareholder $P_i \in \mathcal{P}$, and Blundo's lower bounds on the length of each share are satisfied.

Now, we introduce a new method to analyse secret sharing schemes based on hyperplane geometry, and we use it to illustrate that Harn's multi-secret sharing scheme fails to satisfy the secrecy requirement. For each polynomial $f_l(x) = a_{l,0} + a_{l,1}x + \cdots + a_{l,t-1}x^{t-1}$ randomly selected by the dealer $\mathcal{D}$, we have

$$\begin{bmatrix} 1 & x_1 & \ldots & {x_1}^{t-1} \\ 1 & x_2 & \ldots & {x_2}^{t-1} \\ \vdots & \vdots & & \\ 1 & x_n & \ldots & {x_n}^{t-1} \end{bmatrix} \cdot \begin{bmatrix} a_{l,0} \\ a_{l,1} \\ \vdots \\ a_{l,t-1} \end{bmatrix} = \begin{bmatrix} f_l(x_1) \\ f_l(x_2) \\ \vdots \\ f_l(x_n) \end{bmatrix}$$

Hence, the vector $< a_{l,0}, a_{l,1}, \ldots, a_{l,t-1} >$ can be considered as the coordinates of some point $\mathbb{P}$ in the t dimensional space $\mathbb{S}$. Each shareholder's share $f_l(x_i)$ can be considered as a t dimensional plane in $\mathbb{S}$ that passes through the point $\mathbb{P}$. The Vandermonde matrix ensures that all these n planes intersect uniquely at the point $\mathbb{P}$. The coalition of $t-1$ shareholders can use their planes to derive a line $\mathbb{L}$ in the space $\mathbb{S}$. Based on Harn's description, the polynomial $f_l(x)$ is konwn to have degree $t-1$, so that $a_{l,t-1} \neq 0$. Now, all the points with the coordinate $a_{l,t-1} = 0$ will form another plane in the space $\mathbb{S}$, and this plane will intersect the line $\mathbb{L}$ by a point $\mathbb{P}'$. Then, we can conclude that $\mathbb{P}$ and $\mathbb{P}'$ are not the same point. Note that this method is very versatile. For example, in one hand, if we know that the coordinates satisfy some linear relationship, we can use this relationship to form a plane to derive the point $\mathbb{P}$. In the other hand, if we can exclude some linear relationship for these coordinates, we can also use this relationship to form a plane to derive a point $\mathbb{P}'$ and conclude that $\mathbb{P}$ and $\mathbb{P}'$ are not the same point.

Using this new method, the $t-1$ colluded shareholders can also preclude one possible value for every $a_{l,0}$ in the polynomials $f_l(x)$ for $l = 1, 2, \ldots, k$. Then, they can adapt the same strategy in Sect. 4.1 to preclude one possible value for every $f_l(w_l)$. Hence, they can conclude that the secret are not uniformly distributed within $\mathbb{F}_p$. This proves that the multi-secret sharing scheme fails to be perfect.

Moreover, we further show that compared with the single version of secret sharing, its multiple version may leak more information about the secret. In some special circumstances, when the public parameters satisfy some conditions, the colluded shareholders can even use the recovered secrets to preclude some possible values for the unrecovered secrets. Assume that two secrets s_i and s_j are recovered in different stagies. Without loss of generality, we assume s_i is already recovered but s_j is yet to be recovered. The vectors $< d_{i,1}, d_{i,2}, \ldots, d_{i,k} >$ and $< d_{j,1}, d_{j,2}, \ldots, d_{j,k} >$ are their corresponding public vectors, respectively. Moreover, we assume that the colluding shareholders already know that $f_v(w_v) \neq 0$ for some $v \in \{1, 2, \ldots, k\}$, and these two vectors happen to satisfy the following conditions:

- For all $u \in \{1, 2, \ldots, k\} \backslash \{v\}$, we have $d_{j,u} = \alpha \cdot d_{j,u}$.
- But for v, we have $d_{j,v} = \alpha d_{i,v} + \beta$.

where $\alpha, \beta \in \mathbb{F}_p \backslash \{0\}$. Note that in this case, the two vectors are linearly independent, and all the h vectors could still be linearly independent. However, if the secret s_i is recovered, the value of the unrecovered secret s_j cannot be $\alpha \cdot s_i$, and this is because $\beta \neq 0$. Therefore, the colluding shareholders can preclude one possible values for s_j.

4.3 Making Harn's Schemes Perfect

Harn's two secret sharing schemes can be easily modified to be perfect. The only required change is that the dealer $\mathcal{D}$ selects k random polynomials $f_l(x) = a_{l,0} + a_{l,1}x + \ldots + a_{l,t-1}x^{t-1}$ over $\mathbb{F}_q$ with degree *at most* $t-1$. Here, we only describe why such change can make the single secret sharing scheme to be perfect. And similar reasons also can be applied to the multi-secret sharing scheme.

If the polynomial is randomly generated with degree at most $t-1$, for every polynomial $f_l(x)$, the colluded shareholders only have $t-1$ points $(x_i, f_l(x_i))$ for $i = 1, 2, \ldots, t-1$. Because the colluded shareholders' view of $a_{l,0}$ is uniformly distributed in $\mathbb{F}_p$, every additional point $(0, a_{l,0})$ can interpolate $f_l(x)$ into a different polynomial with equal probability. Hence, every value $f_l(w_l)$ will be uniformly distributed in $\mathbb{F}_p$. This also implies that these shareholders' view of the secret $s = \sum_{l=1}^{k} d_l f_l(w_l)$ will be uniformly distributed in $\mathbb{F}_p$. Therefore, the secrecy requirement will hold, since for any subset of shares $\{\mathsf{sh}_i\}_{P_i \in \mathcal{B}}$, we have $\mathsf{H}(\mathsf{S}|\mathsf{SH}_{\mathcal{B}}) = \mathsf{H}(\mathsf{S})$ for any set $|\mathcal{B}| \leq t-1$.

5 Conclusion

In this paper, we have revisited Harn's secret sharing schemes introduced in [10]. We have demonstrated that both Harn's schemes fail to achieve the perfectness property. In the single secret sharing scheme, if it was known that all the random polynomials are with degree $t-1$, the coalition of $t-1$ shareholders can conclude that the secret is not uniformly distributed. In the multi-secret sharing scheme, when the public parameters satisfy some special conditions, the colluding $t-1$ shareholders may use the recovered secrets to preclude some possible values for the unrecovered secrets. We have also introduced a new method to analyse secret shairng schemes. Compared with Ghodosi's method in the literature, this new method is more versatile and it could be used in more circumstances. Moreover, this paper is another demonstration that formal security analyses [15,16] are crucial for secret sharing schemes.

Acknowledgement. This work was partially supported by the Guizhou Key Laboratory of Public Big Data (Grant No. 2019BDKFJJ005).

References

1. Aggarwal, D., et al.: Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 510–539. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_18
2. Ahmadian, Z., Jamshidpour, S.: Linear subspace cryptanalysis of Harn's secret sharing-based group authentication scheme. IEEE Trans. Inf. Forensics Secur. **13**(2), 502–510 (2017)
3. Applebaum, B., Beimel, A., Farràs, O., Nir, O., Peter, N.: Secret-sharing schemes for general and uniform access structures. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 441–471. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17659-4_15
4. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inf. Theory **29**(2), 208–210 (1983)
5. Blakley, R.: Safeguarding cryptographic keys. In: Proceedings of American Federation of Information Processing Societies (AFIPS'79), vol. 48, pp. 313–317 (1979)
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). https://doi.org/10.1007/3-540-48658-5_17
7. 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). https://doi.org/10.1007/3-540-46885-4_45
8. Ghodosi, H., Pieprzyk, J., Safavi-Naini, R.: Remarks on the multiple assignment secret sharing scheme. In: Han, Y., Okamoto, T., Qing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 72–80. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0028463
9. Harn, L.: Group authentication. IEEE Trans. Comput. **62**(9), 1893–1898 (2012)

10. Harn, L.: Secure secret reconstruction and multi-secret sharing schemes with unconditional security. Secur. Commun. Netw. **7**(3), 567–573 (2014)
11. Harn, L., Xia, Z., Hsu, C., Liu, Y.: Secret sharing with secure secret reconstruction. Inf. Sci. **519**, 1–8 (2020)
12. Mignotte, M.: How to share a secret. In: Beth, T. (ed.) EUROCRYPT 1982. LNCS, vol. 149, pp. 371–375. Springer, Heidelberg (1983). https://doi.org/10.1007/3-540-39466-4_27
13. Shamir, A.: How to share a secret. In: Proceedings of 22nd Communication of ACM, pp. 612–613 (1979)
14. Srinivasan, A., Vasudevan, P.N.: Leakage resilient secret sharing and applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 480–509. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_17
15. Xia, Z., Yang, B., Zhou, Y., Zhang, M., Shen, H., Mu, Y.: Provably secure proactive secret sharing without the adjacent assumption. In: Steinfeld, R., Yuen, T.H. (eds.) ProvSec 2019. LNCS, vol. 11821, pp. 247–264. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31919-9_14
16. Xia, Z., Yang, Z., Xiong, S., Hsu, C.-F.: Game-based security proofs for secret sharing schemes. In: Yang, C.-N., Peng, S.-L., Jain, L.C. (eds.) SICBS 2018. AISC, vol. 895, pp. 650–660. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-16946-6_53