Remarks on-An ideal multi-secret sharing scheme based on MSP *

Zhi-hui Li ⋆, Jing Li

College of Mathematics and Information Science, Shaanxi Normal University, 710062, Xi'an, P. R. China

Abstract— In 2010, C.- F. Hsu, Q.Cheng, X.M.Tang and B.Zeng proposed an ideal linear multi-secret sharing scheme based on monotone span programs (for short HCTZ scheme). This paper mainly makes an analysis about the problems in HCTZ scheme. Meanwhile, we presents an efficient ideal multi-secret sharing scheme based on monotone span programs for a family of access structures. The new scheme effectively overcomes the deficiency of HCTZ scheme, and has the advantage of small calculation cost.

Keywords— multi-secret sharing ; monotone span programs; a family of access structures; small calculation cost

1 Introduction

Secret sharing is a method, mainly used to solve key management. Since 1979, threshold secret sharing schemes were first described by Shamir and Blakley based on Lagrange Polynomial interpolation and projective geometry theory, respectively, according to the various practical needs, people have studied many meaningful secret sharing schemes[3]. However, very little is known about how to devise ideal secret sharing scheme for general access structures.

In 2010, C.- F. Hsu, Q.Cheng, X.M.Tang and B.Zeng proposed an ideal linear multi-secret sharing scheme based on Monotone Span Programs(MSP) for a family of access structures[1]. But, in general, this scheme is not feasible. According to the distribution phase described in HCTZ scheme, to find the vector $\vec{r}$, which meets the given conditions, is equivalent to solve a system of a linear equations. Namely, the existence of $\vec{r}$ is equivalent to the solvability of the system of linear equations. However, the corresponding linear equations is not solvable in most cases. Hence, the feasibility of the whole scheme would be limited.

*This work was supported by the National Natural Science Foundation of China (Grant No. 60873119)

⋆ Corresponding author. E-mail: snnulzh@yahoo.com.cn

This paper firstly analyzes the deficiency of the access structures in HCTZ scheme . Then we propose an ideal linear multi-secret sharing scheme based on monotone span programs for a new family of access structures.

2 HCTZ scheme

This section briefly reviews the HCTZ scheme, and more detailed information can be read in cf.[1].

2.1 Definition of the access structures

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of participants and Ω be the collection of all nonempty subsets of $\mathcal{P}$ with $|\Omega| = m = 2^{|\mathcal{P}|} - 1$. Suppose that $\varphi : \{1, 2, \ldots, m\} \to \Omega$ be a bijection which associates each element in Ω with a number in $\{1, 2, \ldots, m\}$. Seeing that each element in Ω carries different target secret, there are all m secrets $s_1, s_2, \ldots, s_m$ such that for any $1 \leqslant j \leqslant m$, each secret s_j is associated with an access structure Γ_j on $\mathcal{P}$. Define such an m-tuple $\vec{\Gamma} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$ of access structures as follows:

$$(\Gamma_j)_{min} = \{\varphi(j)\}, (1 \leqslant j \leqslant m) \tag{1}$$

2.2 The construction of HCTZ scheme

2.2.1 The setup phase

Let $S_1 \times S_2 \times \ldots \times S_m$ be the set from which the secrets are chosen (that is, s_j to be shared is chosen in S_j, $1 \leqslant j \leqslant m$). Let $S_1 = S_2 = \ldots = S_m = \kappa$ be a finite field, and $\overline{\mathrm{V}} = \kappa$ be the n dimensional linear space over κ Given a basis $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ of $\overline{\mathrm{V}}$, consider the mapping $\mathbf{v} : \kappa \to \overline{\mathrm{V}}$ defined by $\mathbf{v}(x) = \sum_{i=1}^{n} x^{i-1}\vec{e}_i$. Observe that the vectors $\mathbf{v}(x)$ have Vandermonde coordinates with respect to the given basis of $\overline{\mathrm{V}}$. This implies that every set of at most n vectors of the form $\mathbf{v}(x)$ is linearly independent. For any $1 \leq i \leq n$, let $\vec{u}_i \in \{\mathbf{v}(x) : x \in \kappa\}$ be the n-dimensional vector associated with the participant P_i and $V_i \in \mathrm{span}\{\vec{\mathrm{u}}_\mathrm{i}\}$, where $\vec{u}_i \neq \vec{u}_j$ for $i \neq j$.

Let $\vec{v}_j = \sum_{\substack{P_i \in \varphi(j) \\ x_i \in \kappa}} x_i \cdot \vec{u}_i$ $(1 \leq i \leq n)$be the m target vectors and $\vec{u}_i$ be the row vector distributed to participant P_i for $1 \leq i \leq n$. Based on the monotone span programs(cf.[2]), build a $n \times n$ matrix M over κ, with the ith row vector $\vec{u}_i$, that is, $\psi(i) = P_i$ for $1 \leq i \leq n$.

2.2.2 The distribution phase

The dealer first randomly selects a vector $\vec{r} \in \kappa^n$ such that the inner product $(\vec{v}_j, \vec{r}) = s_j$, $1 \leq j \leq m$. Then he computes $M \cdot \vec{r}^{\tau}$, and transmits $M_i \cdot \vec{r}^{\tau}$ to participant P_i $(1 \leq i \leq n)$, where "$\vec{r}^{\tau}$" is the transpose of $\vec{r}$ and M_i denotes the matrix M restricted to the row i (that is, $M_i = \vec{u}_i$). Thus, each participant P_i $(1 \leq i \leq n)$ gets the share $M_i \cdot \vec{r}^{\tau}$.

2.2.3 The reconstruction phase

For any $A \in \Gamma_j$ $(1 \leq j \leq m)$, since $\vec{v}_j = \sum_{\substack{P_i \in \varphi(j) \\ x_i \in \kappa}} x_i \cdot \vec{u}_i$ and $\varphi(j) \subseteq A$, hence $\vec{v}_j \in \sum_{P_i \in A} V_i$, there exists a vector $\vec{w}$ such that $\vec{v}_j = \vec{w} \cdot M_A$. So $s_j = (\vec{v}_j, \vec{r}) = \vec{v}_j \cdot \vec{r}^{\tau} = (\vec{w} \cdot M_A) = \vec{w} \cdot (M_A \cdot \vec{r}^{\tau})$. That is, the participants in A can reconstruct the secret s_j by computing a linear combination of their shares.

2.3 Infeasibility of HCTZ scheme

In the distribution phase of HCTZ scheme, the dealer randomly selects a vector $\vec{r} \in \kappa^n$ such that the inner product $(\vec{v}_j, \vec{r}) = s_j$ for $1 \leq j \leq m$. In fact, to find the vector $\vec{r} = (r_1, r_2, \ldots, r_n)$ is equivalent to solve a system of linear equations about $r_1, r_2, \ldots, r_n$:

$$\begin{cases} c_{11}r_1 + c_{12}r_2 + \cdots + c_{1n}r_n = s_1 \\ \cdots \\ c_{n1}r_1 + c_{n2}r_2 + \cdots + c_{nn}r_n = s_n \\ \cdots \\ c_{m1}r_1 + c_{m2}r_2 + \cdots + c_{mn}r_n = s_m \end{cases} \tag{2}$$

where $m = 2^n - 1 > n$, and $(c_{j1}, c_{j2}, \ldots, c_{jn}) = \vec{v}_j (1 \leq j \leq m)$. Due to the fact that $\vec{u}_1, \ldots, \vec{u}_n$ is linearly independent, the maximum of the rank of the coefficient matrix above can only reach n. We can select a maximal independent set$\{\vec{v}_{j_1}, \ldots, \vec{v}_{j_n}\}$ that is equivalent to $\{\vec{u}_1, \ldots, \vec{u}_n\}$, where $\vec{v}_{j_1}, \ldots, \vec{v}_{j_n}$ is from the m target vectors. Since $\vec{v}_j = \sum_{\substack{P_i \in \varphi(j) \\ x_i \in \kappa}} x_i \cdot \vec{u}_i$, so $\vec{v}_j (j \neq j_1, \ldots, j_n)$ can be represented linearly, that is, the pre-selected secret $s_j (j \neq j_1, \ldots, j_n)$ must be the linear combination of $s_{j_1}, \ldots, s_{j_n}$. Otherwise, the system of equations (2) has no solutions, so HCTZ scheme is not feasible. Thus the multiplicity of access structures in HCTZ scheme can only reach n.

According to the examples in cf.[1], $n = 3$, $m = 7$,and the three target vectors are $\vec{v}_1 = (1, 2, 3)$, $\vec{v}_2 = (2, 2, 4)$, $\vec{v}_3 = (3, 4, 4)$, $\vec{v}_4 = (3, 0, 3)$. Let $s_1 = 1$, $s_2 = 2$, $s_3 = 3$, $s_4 = 4$. We construct a new system of equations by intercepting the first four equations of the system of equations (2):

$$\begin{cases} 1r_1 + 2r_2 + 3r_3 = 1 \\ 2r_1 + 2r_2 + 4r_3 = 2 \\ 3r_1 + 4r_2 + 4r_3 = 3 \\ 3r_1 + 0r_2 + 3r_3 = 4 \end{cases} \tag{3}$$

It is easily verified that the system of equation (3) has no solution in Z_5

2.4 The deficiency of the family of access structures

In HCTZ scheme, the family of access structures is $\vec{\Gamma} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$. For $1 \leq i \leq n$, $(\Gamma_i)_{min} = \{\{P_i\}\}$. This means that each participant can individually carry one master secret, which is against with the thought of secret sharing, since it aims to " share". Thus, to design a general secret sharing scheme does not allow that each participant can recover one of master secrets.

3 Our scheme

3.1 Definition of the access structures

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of participants. We can define an m-tuple $\vec{\Gamma} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$ of access structures as follows:

$$(\Gamma_k)_{min} = \{\{P_{i_{k-1}}, P_{i_{k-1}+1}, \ldots, P_{i_k}\}\}(1 \leqslant k \leqslant m) \tag{4}$$

where $i_k = t_1 + t_2 + \cdots + t_k - (k-1)(1 \leqslant k \leqslant m)$, let $i_0 = 1$, t_k denotes the number of minimal access structure $(\Gamma_k)_{min}$, $2 \leq t_k \leq n$, and $t_1 + t_2 + \cdots + t_m - (m-1) = n$, particularly $i_m = n$.

Observe that, there is only one minimal authorized subset in $(\Gamma_k)_{min}$, denoted by $A_k (1 \leq k \leq m)$, namely $|A_k| = t_k$.

Example 1 Let $n = 7$, $\mathcal{P} = \{P_1, P_2, \ldots, P_7\}$, consider that $m = 3$, $t_1 = 4$, $t_2 = 2$, $t_3 = 3$, then $(\Gamma_1)_{min} = \{\{P_1, P_2, P_3, P_4\}\}$, $(\Gamma_2)_{min} = \{\{P_4, P_5\}\}$, $(\Gamma_3)_{min} = \{\{P_5, P_6, P_7\}\}$, and the corresponding minimal authorized subsets are $A_1 = \{P_1, P_2, P_3, P_4\}$, $A_2 = \{P_4, P_5\}$, $A_3 = \{P_5, P_6, P_7\}$, respectively.

3.2 Construction of our scheme

Let $S_1 \times S_2 \times \cdots \times S_m$ be the set from which the secrets are chosen (that is, s_k to be shared is chosen in S_k, $1 \leqslant k \leqslant m$),Let $S_1 = S_2 = \cdots = S_m = \kappa$, where κ is a finite field. Based on MSPM(κ, M, ψ), our scheme consists of three phases:

3.2.1 The setup phase

We construct a $n \times n$ upper triangular matrix M over κ, whose (i, j) entry is a_{ij} $(i = 1, \ldots, n; j = 1, \ldots, n)$. When $i > j$, $a_{ij} = 0$; when $i \leq j$, we can define a_{ij} as follows:

(i) if $i = 1$, $a_{1j} = b_j$, where $b_j \in \kappa$ and $b_j \neq 0$;

(ii) if $i_k + 1 \leq i \leq i_{k+1}$ and $0 \leq k \leq m - 1$,

$$a_{ij} = \begin{cases} \frac{a_{i_k,j}}{j-i_k} & \text{if } i_k + 1 \leq j \leq i_{k+1} \\ \frac{a_{i_k,j}}{t_{k+1}-1} & \text{if } i_{k+1} + 1 \leq j \leq n \end{cases}$$

For any $1 \leq i \leq n$, let $V_i = \text{span}\{M_i\}$, where M_i denotes the matrix M restricted to the row i. Let $\vec{v}_k = (0, \ldots, 0, 1, 0, \ldots, 0) \in \kappa^n$, $1 \leq k \leq m$, be the m target vector where the $i_{k-1}th$ coordinator is 1, and 0 elsewhere.

Example 2 (Following Example 1) Suppose that M be a $n \times n$ upper triangular matrix constructed as above:

$$M = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ 0 & b_2 & \frac{b_3}{2} & \frac{b_4}{3} & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & \frac{b_3}{2} & \frac{b_4}{3} & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & 0 & \frac{b_4}{3} & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & 0 & 0 & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{b_6}{3} & \frac{b_7}{6} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{b_7}{6} \end{pmatrix}$$

The three target vectors are $\vec{v}_1 = (1, 0, 0, 0, 0, 0, 0)$, $\vec{v}_2 = (0, 0, 0, 1, 0, 0, 0)$, $\vec{v}_3 = (0, 0, 0, 0, 1, 0, 0)$. Obviously, $\vec{v}_1 = b_1^{-1} \cdot [M_1 - (M_2 + M_3 + M_4)]$, $\vec{v}_2 = (\frac{b_4}{3})^{-1} \cdot (M_4 - M_5)$, $\vec{v}_3 = (\frac{b_5}{3})^{-1} \cdot [M_5 - (M_6 + M_7)]$. In fact, according to the definition of the access structures and matrix M, $\vec{v}_k = a_{i_{k-1},i_{k-1}}^{-1} \cdot [M_{i_{k-1}} - (M_{i_{k-1}+1} + \cdots + M_{i_k})]$ for $1 \leq k \leq m$.

3.2.2 The distribution phase

The dealer first secretly selects n elements $r_1, r_2, \ldots, r_n$ with $r_{i_{k-1}} = s_k$, $1 \leq k \leq m$ are the m master secrets, constructing a n-dimensional vector:

$$\vec{s} = (r_1, r_2, \ldots, r_n) = (s_1, r_2, \ldots, r_{i_1-1}, s_2, \ldots, s_m, r_{i_{m-1}+1}, \ldots, r_{i_m-1}, r_n),$$

he computes $M_i \cdot \vec{s}^{\tau}$, and transmits it to participant $P_i (1 \leq i \leq n)$.

3.2.3 The reconstruction phase

For any $A \in \Gamma_k (1 \leq k \leq m)$, note that, $A_k \subseteq A$. According to remark 1, $\vec{v}_k \in \sum_{P_i \in A_k} V_i$, it is easy to find a t_k-dimensional vector $\vec{w}$ such that $\vec{v}_k = \vec{w} \cdot M_{A_k}$, where

the $t_k \times n$ matrix M_{A_k} consists of the rows i of M with $P_i \in A_k$, then $s_k = \vec{v}_k \cdot \vec{s}^{\tau} = (\vec{w} \cdot M_{A_k}) \cdot \vec{s}^{\tau} = \vec{w} \cdot (M_{A_k} \cdot \vec{s}^{\tau})$. Hence, the participants in $A_k \subseteq A$ can reconstruct the secret s_k by computing a linear combination of their shares, that is, the participants in A can recover the secret s_k.

Example 3 (Following Example 2) The dealer secretly selects 7 elements $r_1, r_2, r_3, r_4, r_5, r_6, r_7$, where $r_1 = s_1$, $r_4 = s_2$, $r_5 = s_3$, each secret $s_k (k = 1, 2, 3)$ is associated with an access structure Γ_k, and $\vec{s} = (s_1, r_2, r_3, s_2, s_3, r_6, r_7) \in \kappa^7$, and each participant $P_i (1 \leq i \leq 7)$ gets the shares $M_i \cdot \vec{s}^{\tau}$. When $A \in \Gamma_1$, we have $A_1 \subseteq A$, due to $\vec{v}_1 = b_1^{-1} \cdot [M_1 - (M_2 + M_3 + M_4)] = b_1^{-1} M_1 - b_1^{-1} M_2 - b_1^{-1} M_3 - b_1^{-1} M_4$, then $\vec{v}_1 \in \sum_{P_i \in A_1} V_i$, thus, there exists a vector $\vec{w}$ such that $\vec{v}_1 = \vec{w} \cdot M_{A_1}$. Observe that $\vec{w} = (b_1^{-1}, -b_1^{-1}, -b_1^{-1}, -b_1^{-1})$, $s_1 = \vec{v}_1 \cdot \vec{s}^{\tau} = (\vec{w} \cdot M_{A_1}) \cdot \vec{s}^{\tau} = \vec{w} \cdot (M_{A_1} \cdot \vec{s}^{\tau})$. Besides, the case $A \in \Gamma_2$ or $A \in \Gamma_3$ can be similarly analyzed.

4 Analysis and discussion

4.1 The security of our scheme

The security of our scheme means that, for the access structure Γ_k, $1 \leq k \leq m$, any unauthorized subset of participants cannot recover the secret s_k, which is equivalent to $\vec{v}_k \notin \bigcup_{B \in (\mathcal{A}_k)_{\max}} \sum_{P_i \in B} V_i$, where $(\mathcal{A}_k)_{\max}$ denotes the maximum adversary structure, and the unauthorized subset denoted by B.

Proposition 1 Suppose that $\vec{\Gamma} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$ be defined by (4), and κ, M_i, V_i, $1 \leq i \leq n$ are given as above. For any $1 \leq k \leq m$, it holds that $\vec{v}_k \notin \bigcup_{B \in (\mathcal{A}_k)_{\max}} \sum_{P_i \in B} V_i$.

Proof. Due to the fact that the determinant of the upper triangular matrix M is nonzero, we can obtain that the row vectors $M_1, \ldots, M_n$ of matrix M are linearly independent. Furthermore, observe that $V_i = \text{span}\{M_i\}$ for $A_k \notin (\mathcal{A}_k)_{\max}$ for any $1 \leq k \leq m$. These imply that for any $B \in (\mathcal{A}_k)_{\max}$, there does not exist a linear combination of the vector $\vec{v}_k$ in $\sum_{P_i \in B} V_i$. Otherwise, $\vec{v}_k = \sum_{\substack{P_i \in B \\ x_i \in \kappa}} x_i \cdot M_i$, and $\vec{v}_k = a^{-1}_{i_{k-1}, i_{k-1}} \cdot [M_{i_{k-1}} - (M_{i_{k-1}+1} + \cdots + M_{i_k})]$, these implies that $M_1, M_2, \ldots, M_n$ are linearly dependent, which is a contradiction, Thus $\vec{v}_k \notin \sum_{P_i \in B} V_i$. Hence $\vec{v}_k \notin \bigcup_{B \in (\mathcal{A}_k)_{\max}} \sum_{P_i \in B} V_i$ for any $1 \leq k \leq m$.

4.2 The feasibility of our scheme

Compared with HCTZ scheme, in the distribution phase of our scheme, the dealer transmits $M_i \cdot \vec{s}^{\tau}$ to the participant $P_i(1 \leq i \leq n)$, where the vector $\vec{s}$ is secretly pre-selected , without solving a system of equations. Therefore, this scheme can effectively save the calculations for solving the system of linear equations, in particular, to avoid infeasible troubles caused by unsolvable system of equations.

4.3 The parameters analysis of our scheme

According to the description of 3.2, when $t_1 = t_2 = \ldots = t_m = 2$, the multiplicity of access structures can reach its maximum $n-1$, the family of access structures is $(\Gamma_k)_{min} = \{\{P_k, P_{k+1}\}\}$, namely, $(\Gamma_1)_{min} = \{\{P_1, P_2\}\}$, $(\Gamma_2)_{min} = \{\{P_2, P_3\}\}$, $\ldots$, $(\Gamma_{n-1})_{min} = \{\{P_{n-1}, P_n\}\}$.

5 Conclusions

This paper mainly makes an analysis about the problems an ideal linear multi-secret sharing scheme proposed by C.- F. Hsu. Meanwhile, we presents a new ideal multi-secret sharing scheme based on monotone span programs. The new scheme effectively avoids the steps of the system of linear equations, so it has the advantage of small calculation cost.

References

[1] C.F.Hsu, Q.Chang, X.M.Tang, B.Zeng, An ideal multi-secret sharing scheme based on MSP, Information Sciences 181(7)(2011) 1403-1409.

[2] L.L.Xiao, M.L.Liu, Linear multi-secret sharing schemes, Science in China Series F Information Sciences 48(1) (2005) 125-136.

[3] M.Liu, ZF.Zhang, Secret sharing schemes and secure multi-party computation, Beijing, Publishing House of electronics industry, 2008.