高效的强 (n, t, n) 可验证秘密共享方案

吴春英^{1,2} 李顺东¹

(陕西师范大学计算机科学学院 西安 710062)¹ (青海师范大学计算机学院 西宁 810008)²

摘要 2010 年, Harn 和 Lin 提出了强 t -一致的概念, 并设计了一个强 (n, t, n) 可验证的秘密共享方案, 但该方案的效率较低。提出一个基于范德蒙行列式性质的高效的强 (n, t, n) 可验证的秘密共享方案, 该方案可以抵抗并检验出 Harn 方案中出现的欺诈行为。同时, 新方案无须选取 Harn 方案中的 kn 个子多项式, 在保证秘密份额满足强 t -一致定义的前提下具有较低的计算复杂度。

关键词 秘密共享, 范德蒙行列式, 强 t -一致, 可验证秘密共享方案

中图分类号 TP309 **文献标识码** A

Efficient Strong (n, t, n) Verifiable Secret Sharing Scheme

WU Chun-ying^{1,2} LI Shun-dong¹

(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)¹

(School of Computer, Qinghai Normal University, Xining 810008, China)²

Abstract In 2010, Harn and Lin proposed the conception of strong t -consistency and designed a strong (n, t, n) verifiable secret sharing scheme, but the scheme has a low efficiency. This paper proposed an efficient strong (n, t, n) verifiable secret sharing scheme. Based on the property of Vandermonde determinant, the scheme can resist and verify the fraud proposed in Harn scheme. Meanwhile, our scheme doesn't need to select the kn sub-polynomials. The new scheme with strong t -consistency has the advantage of a low computational complexity.

Keywords Secret sharing, Vandermonde determinant, Strong t -consistency, Verifiable secret sharing scheme

1 引言

秘密共享是当前密码学的主要研究课题之一。1979 年, Shamir 提出了 (t, n) 门限秘密共享方案^[1]。其中, 任意 t 个或 t 个以上的参与者可以共同恢复出秘密, 而小于 t 个参与者的集合得不到关于秘密的任何信息。之后, 门限秘密共享方案得到了大量的研究^[2-4, 7]。1991 年, Pederson 提出了一个 (n, t, n) 秘密共享方案^[5]。方案没有可信第三方, 即每个参与者都是分发者。参与者 P_i 选取秘密 S_i , 定义主秘密

$$S = \sum_{i=1}^n S_i = S_1 + S_2 + \dots + S_n$$

同时, 由于该方案是基于 Shamir 门限秘密共享方案所设计的, 因此方案中秘密份额的长度与主秘密的长度相等。但是该方案不能抵抗以下两种欺诈行为: (a) 不诚实的参与者选取次数小于 $t-1$ 的多项式, 使得小于 t 个参与者可以重构主秘密; (b) 不诚实的参与者选取次数大于 $t-1$ 的多项式, 使得任意 t 个或 t 个以上的参与者所恢复的主秘密不相同, 从而导致方案失败。

2010 年, Harn 和 Lin 提出强 t -一致和强可验证性的概念, 并设计了一个强 (n, t, n) 可验证秘密共享方案^[6]。该方案要求所有参与者可以共同验证其秘密份额是 t -一致的 (即任

意 t 个参与者所重构的主秘密必须相同), 但该方案的效率较低。即参与者为了使方案具有防欺诈性, 选取了较多的子多项式, 从而增加了方案的运算量。

为了克服以上方案的不足, 本文提出一个高效的强 (n, t, n) 可验证秘密共享方案。我们将长度一定的秘密分割成长度相同的 n 份, 同时, 通过构造 n 个新的多项式使得这些多项式的系数所组成的行列式恰好为范德蒙行列式, 因此, 方案可以抵抗和检验出 Harn 方案中出现的欺诈行为。另外, 新方案无须选取 Harn 方案中的 kn 个子多项式, 在保证秘密份额满足强 t -一致定义的前提下具有较小的计算复杂度。

2 预备知识

这一节主要回顾引言中提到的 3 个基本的门限秘密共享方案。

2.1 Shamir (t, n) 门限秘密共享方案的回顾

Shamir (t, n) 门限方案是基于拉格朗日插值多项式构造的, n 个参与者集合记作 $\{P_1, \dots, P_n\}$, D 是分发者。方案^[8]构造如下:

1. 秘密份额生成算法: 分发者 D 首先选取一个 $t-1$ 次多项式 $f(x)$, 其中 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$ 使得 $s = a_0$, 这里, 多项式的系数 $a_0, a_1, \dots, a_{t-1} \in F_p$ (p 是一个大素数), D

到稿日期: 2012-11-09 返修日期: 2013-01-26 本文受国家自然科学基金(61070189, 61272435)资助。

吴春英(1972-), 女, 博士生, 主要研究领域为安全多方计算、隐私保护、数据挖掘, E-mail: wuandli2012@126.com; 李顺东(1964-), 男, 博士, 教授, 博士生导师, 主要研究领域为信息安全。

计算 $s_i = f(x_i)$, 并将 s_i 秘密地发送给参与者 P_i 。

2. 秘密重构算法:任意 t 个参与者集合 $\{P_{i_1}, P_{i_2}, \dots, P_{i_t}\}$ 可以利用拉格朗日插值公式重构秘密 S 。

2.2 Pederson(n, t, n)秘密共享方案回顾

Pederson 方案中没有分发者 D , 每个参与者都充当了分发者的角色, 且每个参与者 P_i 选取一个子秘密 S_i , 利用 Shamir 秘密份额生成算法与其他参与者共享该子秘密。方案设计如下:

1. 主秘密生成算法: 每个参与者 P_i 选取一个子秘密 S_i , 定义整个方案的主秘密 $S = \sum_{i=1}^n S_i = S_1 + S_2 + \dots + S_n$;

2. 子份额生成算法: 每个参与者 $P_i (1 \leq i \leq n)$ 选取一个 $t-1$ 次多项式 $f_i(x)$, 使得 $S_i = f_i(0)$, P_i 计算 $s_{ij} = f_i(x_j)$, 并将 s_{ij} 秘密地发送给参与者 $P_{j_i} (1 \leq j \leq n \text{ 且 } j \neq i)$;

3. 主份额生成算法: 每个参与者 P_i 计算各自的主份额 $s_i = \sum_{j=1}^n s_{ji} = s_{1i} + s_{2i} + \dots + s_{ni}$, 即 P_i 在最后只需持有主份额 s_i 即可;

4. 主秘密的重构算法: 任意 t 个参与者集合可以利用拉格朗日插值公式和同态加的性质恢复主秘密 S (具体重构算法见文献[6])。

2.3 Harn(n, t, n)秘密共享方案回顾

2.3.1 强 t -一致性

Harn 在 Pederson(n, t, n)秘密共享方案的基础上给出 t -一致的定义。

定义 1 n 个共享 $s_1, s_2, \dots, s_n$ 称作是 t -一致的, 如果其中任意 t 个共享可以恢复出相同的秘密。

主秘密 $S = \sum_{i=1}^n f_i(0)$, 因此, 如果多项式 $F(x) = \sum_{i=1}^n f_i(x)$ 的次数小于 $t-1$, 则大于等于 t 个参与者即可恢复主秘密 S , 共享集合可以称作是 t -一致的。

定义 2 n 个共享 $s_1, s_2, \dots, s_n$ 称作是强 t -一致的, 如果满足:

- 任意 t 个或 t 个以上的参与者可以恢复出相同的秘密;
- 任意 $t-1$ 个或少于 $t-1$ 个参与者无法恢复出主秘密。

定义 3 如果秘密共享方案的所有共享可以被验证满足强 t -一致的定义, 则称该秘密共享方案是强可验证的。

2.3.2 强(n, t, n)可验证秘密共享方案

Harn 强(n, t, n)可验证秘密共享方案构造如下:

- 每个参与者 P_i 完成 Pederson 方案中的前 3 个步骤。
- 参与者 P_i 选取 k 个 $t-1$ 次多项式, $f_l^i(x) (l=1, 2, \dots, k)$ 并计算子份额 $r_{ij}^l = f_l^i(x_j)$, 将其发送给其它参与者 $P_j (1 \leq j \leq n, j \neq i)$ 。同时, P_j 计算验证子份额 $r_i^l = \sum_{j=1}^n r_{ji}^l = r_{1i}^l + \dots + r_{ni}^l (l=1, 2, \dots, k)$, 即 P_i 需持有 k 个验证子份额 $R = r_i^l (l=1, 2, \dots, k)$ 。

3. 每个参与者 P_i 公开验证子份额子集 U_i , 其中 $|U_i| = k/2$ 。

4. 所有参与者共同验证上一步中公布的验证子份额是否是由 $t-1$ 次多项式所得出, 并且验证其是否具有 t -一致性, 如果验证结果为“是”, 则能够以很高的概率确保子多项式是

$t-1$ 次的。

5. 每个参与者 P_i 公开 $s_i + r_i^l$, 其中 $r_i^l \in R - U_i$ 。所有参与者共同验证这些数据是否是由 $t-1$ 次多项式所得出, 并且验证其是否具有 t -一致性, 如果验证结果为“是”, 则能够确定多项式 $F(x) = \sum_{i=1}^n f_i(x)$ 是 $t-1$ 次的。

3 本文方案

这一节提出一个高效的强(n, t, n)可验证秘密共享方案。已知 Shamir 门限方案以及(n, t, n)秘密共享方案均是在有限域 $GF(p)$ 上实现的, 这里, p 是一个二进制表示的 128 位的大素数。现在设 $P = \{P_1, P_2, \dots, P_n\}$ 是参与者集合, 且设 $q \approx p/n$ 是一个安全素数。构造分为如下两个阶段:

3.1 秘密分发阶段

1. 每个参与者 P_i 在 F_q 上选取一个 $t-1$ 次多项式 $f_i(x)$, 使得 $s_i = f_i(0)$, P_i 计算 $s_{ij} = f_i(x_j)$, 并将 s_{ij} 秘密地发送给参与者 $P_j (i=1, 2, \dots, n; j=1, 2, \dots, n)$;

2. 所有参与者共同选取并公开 n 个不同的元素, 记作 $w_1, w_2, \dots, w_n \in F_q$;

3. 方案的主秘密 $S = S_1 \parallel \dots \parallel S_l \parallel \dots \parallel S_n$ (符号“ $\parallel$ ”表示串联), 其中 $S_l = 1 \cdot s_{1l} + w_l \cdot s_{2l} + w_l^2 \cdot s_{3l} + \dots + w_l^{t-1} \cdot s_{nl} (l=1, 2, \dots, n)$;

4. 参与者 P_i 计算 $k_i^l = 1 \cdot s_{1i} + w_l \cdot s_{2i} + w_l^2 \cdot s_{3i} + \dots + w_l^{t-1} \cdot s_{ni} (l=1, 2, \dots, n)$ 且公开 k_i^n 。参与者 P_i 的主份额为 $K^i = k_i^1 \parallel \dots \parallel k_i^l \parallel \dots \parallel k_i^n$ 。

3.2 验证阶段

1. 共享持有者 $\{P_1, P_2, \dots, P_n\}$ 共同选取并公开 n 个不同的元素, 记作 $w_1, w_2, \dots, w_n \in F_q$;

2. 每个参与者 P_i 计算 $k_i^l = 1 \cdot s_{1i} + w_l \cdot s_{2i} + w_l^2 \cdot s_{3i} + \dots + w_l^{t-1} \cdot s_{ni} (l=1, 2, \dots, n)$ 且公开 k_i^l ;

3. 所有共享持有者用 n 个公开的可行的共享份额计算 $F_{w_l}(x) = 1 \cdot f_1(x) + w_l \cdot f_2(x) + w_l^2 \cdot f_3(x) + \dots + w_l^{t-1} \cdot f_n(x)$, 如果 $F_{w_l}(x)$ 多项式的最高系数是 $t-1$ 次的, n 个主共享是强 t -一致的 (具体见定理 2 和定理 3 的证明)。

3.3 秘密重构阶段

主秘密的重构可以利用拉格朗日插值公式及同态加的性质完成。对于任意 t 或 t 以上参与者子集可以共同恢复出主秘密。不妨设参与者子集 $A = \{P_{i_1}, P_{i_2}, \dots, P_{i_t}\}$, 即 $|A| = t$ 。参与者 P_{i_d} 出示其主份额 $K^{i_d} = k_{i_d}^1 \parallel \dots \parallel k_{i_d}^d \parallel \dots \parallel k_{i_d}^n$, A 中参与者利用各自的第 l 个子份额 $k_{i_d}^l (d=1, \dots, t)$ 共同计算 $S_l = F_A(k_{i_1}^l \parallel \dots \parallel k_{i_t}^l) (l=1, \dots, n)$, 其中 $F_A(k_{i_1}^l, \dots, k_{i_t}^l, \dots, k_{i_t}^l)$ 表示针对 t 个函数对 $(k_{i_d}^l, k_{i_d}^l) (d=1, \dots, t)$ 的拉格朗日插值公式。于是, 主秘密 $S = S_1 \parallel \dots \parallel S_l \parallel \dots \parallel S_n$ (方案秘密重构算法的正确性见定理 1)。

4 分析与讨论

4.1 方案的正确性分析

这一节主要给出方案秘密重构算法的正确性证明。

定理 1 方案中的主份额由以上算法生成, 则任意 t 或 t 以上参与者子集可以共同恢复出主秘密。

证明:不妨设参与者子集 $A = \{P_{i_1}, \dots, P_{i_d}, \dots, P_{i_t}\}$, 即 $|A| = t$ 。主秘密 $S = S_1 \parallel \dots \parallel S_t \parallel \dots \parallel S_n$ 。因为 $s_i = f_i(0)$ 且 $S_l = 1 \cdot s_1 + w_l \cdot s_2 + w_l^2 \cdot s_3 + \dots + w_l^{l-1} \cdot s_n$ ($l=1, 2, \dots, n$), 设 $g_{w_l}(x) = 1 \cdot f_1(x) + w_l \cdot f_2(x) + \dots + w_l^{l-1} \cdot f_n(x)$, 则有 $g_{w_l}(0) = S_l$ 。同时, 由 3.1 节 4 可知, $g_{w_l}(x_{i_d}) = k_l^{i_d}$ ($d=1, \dots, t$)。故由拉格朗日插值公式及同态加的性质可计算

$$\begin{aligned} S_l &= 1 \cdot s_1 + w_l \cdot s_2 + w_l^2 \cdot s_3 + \dots + w_l^{l-1} \cdot s_n \\ &= 1 \cdot F_A(s_{1i_1}, \dots, s_{1i_t}) + w_l \cdot F_A(s_{2i_1}, \dots, s_{2i_t}) + \dots + \\ &\quad w_l^{l-1} \cdot F_A(s_{ni_1}, \dots, s_{ni_t}) \\ &= 1 \cdot F_A(s_{1i_1}, \dots, s_{1i_t}) + w_l \cdot F_A(s_{2i_1}, \dots, s_{2i_t}) + \dots + \\ &\quad w_l^{l-1} \cdot F_A(s_{ni_1}, \dots, s_{ni_t}) \\ &= F_A(g_{w_l}(x_{i_1}), \dots, g_{w_l}(x_{i_d}), \dots, g_{w_l}(x_{i_t})) \\ &= F_A(k_l^{i_1}, \dots, k_l^{i_d}, \dots, k_l^{i_t}) \quad (l=1, \dots, n) \end{aligned}$$

其中, $F_A(s_{1i_1}, \dots, s_{1i_t}) = \prod_{d=1}^t s_{1i_d} \cdot \prod_{1 \leq r < d \leq t, r \neq d} \frac{(x - x_r)}{(x_{i_d} - x_{i_r})}$ 表示用于恢复 S_1 的拉格朗日插值公式。

4.2 方案的安全性分析

如果方案中的所有参与者均为诚实参与者, 则根据 Shamir(t, n) 门限方案的安全性可以保证本文方案的安全性。Harn 指出, 当方案中存在不诚实的参与者时, 以下两种情况会导致方案的安全隐患。

情况 1 不诚实的参与者选取次数小于 $t-1$ 的多项式使得小于 t 个参与者可以重构主秘密;

情况 2 不诚实的参与者选取次数大于 $t-1$ 的多项式使得任意 t 个或 t 个以上的参与者所恢复的主秘密不相同。

本文的方案可以抵抗并检验这两种攻击。针对情况 1 和情况 2, 给出相应的证明(定理 2 和定理 3)。

定理 2 如果本文的方案至少有一个诚实的参与者选取次数是 $t-1$ 的多项式, 则小于 t 个参与者无法重构主秘密。

证明: 设 d_i ($1 \leq i \leq n$) 是多项式 $f_i(x)$ 的 $t-1$ 次项 x^{t-1} 的系数, a_l ($1 \leq l \leq n$) 是多项式 g_{w_l} 的 $t-1$ 次项的系数。由于方案至少有一个诚实的参与者 P_i 选取次数是 $t-1$ 的多项式, 因此多项式 $f_i(x)$ 相应的 $t-1$ 次项系数 $d_i \neq 0$ 。从方案的构造可得方程组

$$\begin{pmatrix} 1 & w_1 & w_1^2 & \dots & w_1^{t-1} \\ 1 & w_2 & w_2^2 & \dots & w_2^{t-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & w_n & w_n^2 & \dots & w_n^{t-1} \end{pmatrix} \cdot \begin{pmatrix} d_1 \\ d_2 \\ \dots \\ d_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix} \quad (1)$$

因式(1)中的 $d_1, \dots, d_n$ 不全为 0, 且 $w_1, \dots, w_n$ 是两两不同的元素, 则由范德蒙行列式的性质可知, 式(1)中的 $a_1, \dots, a_n$ 不全为 0, 故重构秘密 S_l 时至少需要 t 个参与者, 因此新方案可以保证小于 $t-1$ 个参与者无法恢复整个方案的主秘密 $S = S_1 \parallel \dots \parallel S_t \parallel \dots \parallel S_n$ 。

针对情况 2, 我们给出定理 3, 即可以利用公开份额 k_i ($i=1, \dots, n$) 来检验方案中是否存在不诚实的参与者。

定理 3 给定已知方案中的 $w_1, \dots, w_n \in F_q$, 则多项式 $g_{w_n}(x) = 1 \cdot f_1(x) + w_n \cdot f_2(x) + w_n^2 \cdot f_3(x) + \dots + w_n^{n-1} \cdot f_n(x)$ 次数是 $t-1$ 次的概率为 $1/q$ 。

证明: 不妨设不诚实的参与者选取了 t 次多项式 $f_i(x)$, d'_i 是多项式 $f_i(x)$ 的 t 次项 x^t 的系数。令 $g_{w_n}(x)$ 的 t 次项

系数为

$$1 \cdot d'_1 + w_n \cdot d'_2 + w_n^2 \cdot d'_3 + \dots + w_n^{n-1} \cdot d'_n = 0 \quad (2)$$

由于 $d'_1 \dots d'_n$ 是参与者在 F_q 上随机选取的, 因此式(2)成立的概率为 $q^{n-1}/q^n = 1/q$ 。

由定理 3 可知, 不诚实的参与者选取 $d'_i \neq 0$ 使得 $g_{w_n}(x)$ 的 t 次项系数为 0 的概率小于 $1/q$ (可以忽略不计), 即所有参与者能够以 $(q-1)/q$ 的概率验证出欺诈行为。

4.3 方案的复杂性分析

存储空间: 从方案的构造过程来看, 每个参与者 P_i ($1 \leq i \leq n$) 收到的共享的长度与主密钥的长度相等, 与利用 l 分解以及单调布尔电路所构造的秘密共享方案^[9] 相比, 从比例上看, 本文方案中参与者的共享所占用的存储空间较小。事实上, l 分解以及单调布尔电路所构造的秘密共享方案的信息率大多数都小于 1, 即参与者收到的共享的长度要比主密钥的长度大。

计算复杂度: 由于方案是基于 Shamir 门限体制范德蒙行列式所设计的, 因此方案中只用到了基本的线性运算, 避免了复杂度高的运算, 如方幂运算、hash 函数值的计算等。

结束语 本文提出一个高效的强 (n, t, n) 可验证秘密共享方案。基于范德蒙行列式的性质, 方案可以抵抗和验证 Harn 方案中出现的欺诈行为。同时, 新方案无须选取 Harn 方案中的 kn 个子多项式, 因此, 方案在保证秘密份额满足强 t -一致定义的前提下具有较低的计算复杂度, 是一个高效的秘密共享方案。

参考文献

- [1] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613
- [2] Yang Chou-chen, Chang Ting-yi, Hwang Min-Shiang. A (t, n) multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151(2): 483-490
- [3] Qin Hua-wang, Dai Yue-wei, Wang Zhi-quan. A secret sharing based on (t, n) threshold and adversary structure [J]. Int. J. Inf. Secur., 2009(8): 379-385
- [4] Shao Jun, Cao Zhen-fu. A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme [J]. Applied Mathematics and Computation, 2005, 168(1): 135-140
- [5] Pedersen P. A threshold cryptosystem without a trusted party [C] // Advances in Cryptology, Proceedings of the Eurocrypt'91. Brighton, UK, LNCS, vol. 547, Berlin: Springer-Verlag, 1991: 522-526
- [6] Harn L, Lin Chang-lu. Strong (n, t, n) verifiable secret sharing scheme [J]. Information Sciences, 2010(180): 3059-3064
- [7] Chang T Y, Hwang M S, Yang W P. An improvement on the Lin-Wu (t, n) threshold verifiable multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2005, 163(1): 169-178
- [8] Stinson D R. 密码学原理与实践 (第二版) [M]. 冯登国, 译. 北京: 电子工业出版社, 2003: 138-139
- [9] 刘木兰, 张志芳. 秘密共享体制和安全多方计算 [M]. 北京: 电子工业出版社, 2008