第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 安全技术 • 文章编号：1000—3428(2011)24—0100—03 文献标识码：A 中图分类号：TP309

基于向量空间的防欺诈秘密共享方案

雷 娟，李志慧，张倩倩

(陕西师范大学数学与信息科学学院，西安 710062)

摘 要：传统秘密共享方案在防止成员间的欺诈方面存在缺陷。为此，基于线性方程组理论，提出一种新的防欺诈秘密共享方案。新方案在秘密恢复前，需要分 2 步对授权子集中的参与者份额进行验证，并证明了凡是通过以上 2 步验证的参与者一定是诚实的。分析结果表明，与其他基于向量空间的秘密共享方案相比，该方案具有更高的安全性。

关键词：秘密共享；访问结构；授权子集；向量空间；黑盒子

Secret Sharing Scheme for Fraud Prevention Based on Vector Space

LEI Juan, LI Zhi-hui, ZHANG Qian-qian

(College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China)

【**Abstract**】The traditional secret sharing scheme has defects in preventing cheating between participants. Based on systems of linear equations, this paper proposes a new scheme. Before the recovery phase, the new scheme needs two steps in which authorized participants shares must be verified, and it is shown that any participant who has passed the verification in these two steps must be honest. The new scheme is more safer than the other vector space secret sharing schemes.

【**Key words**】secret sharing; access structure; authorized subset; vector space; black box

DOI: 10.3969/j.issn.1000-3428.2011.24.033

1 概述

自从文献[1-2]提出秘密共享的概念后，秘密共享开始成为密码学中一个非常重要的研究课题，同时在防欺诈方面也有了很大进展。文献[3]提出一种防欺诈的秘密共享方案。文献[4]利用平面差异集的有关理论提出一种防欺诈的秘密共享方案。文献[5]提出一种无条件安全性的防欺诈方案，它是 Shamir 门限方案的修改方案，并且仅把秘密的一部分作为其合法值。文献[6-9]提出向量空间上的防欺诈的秘密共享方案。方案灵活地使用黑盒子来重构秘密，但该方案在防止成员欺诈方面存在漏洞。本文指出文献[6]方案的缺陷，在原方案基础上，提出一种新的方案，该方案具有防欺诈功能，从而在理论上保证了其可行性。

2 原方案的介绍

2.1 系统初始化阶段

设 $P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参与者的集合，分发者 $D\notin P$，$K=GF(q)$，其中，q 为素数，$E=K^r$ 是有限域 K 上的 r 维向量空间。设 Γ 是一个访问结构，如果存在函数 $\psi:P\cup\{D\}\to E$ 使得 $A\in\Gamma\Leftrightarrow\psi(D)\in\langle\psi(P_i):P_i\in A\rangle$，则称 Γ 是向量空间 E 上的访问结构。

2.2 共享分发阶段

D 首先公开函数 ψ，然后对要共享的密钥 $k\in K$，D 随机选择 $\boldsymbol{v}_1,\boldsymbol{v}_2\in E$ 使得 $k=v_1\cdot x_0$ 且 $k^2=v_2\cdot x_0$，其中 $x_0=\psi(D)$，$x_i=\psi(P_i)$。D 计算：$s_i=\boldsymbol{v}_1\cdot x_i$，$t_i=\boldsymbol{v}_2\cdot x_i$，并把 (s_i,t_i) 作为共享发给 P_i ($i=1,2,\cdots,n$)，这里 $\boldsymbol{v}_1,\boldsymbol{v}_2$ v_2 是向量。

2.3 秘密重构阶段

设 $A=\{P_1,P_2,\cdots,P_l\}\in\Gamma$，则 $\psi(D)\in\langle\psi(P_i):P_i\in A\rangle$，即 $x_0=\sum_{i=1}^{l}\lambda_i x_i$，其中 $\lambda_i\in K$。秘密由黑盒子计算。具体如下：A 中的参与者把共享传给黑盒子，黑盒子计算：$k_1=\sum_{i=1}^{l}\lambda_i s_i$，$k_2=\sum_{i=1}^{l}\lambda_i t_i$。如果 $k_1^2=k_2$ 成立，则黑盒子返回 k_1 作为正确的秘密值。否则参与者被警告该授权子集存在欺诈者，同时黑盒子毁掉 k_1 和 k_2。值得注意的是，若黑盒子没有毁掉 k_1 和 k_2，则欺诈者可获得秘密 k_1 的真实值。原因如下：不妨设 P_j 为某个欺诈者，其出示的伪份额为 (s_j^*,t_j^*)，其中，$s_j^*=s_j+\varepsilon$，$t_j^*=t_j+\delta$，那么 $k_1^*=\lambda_1 s_1+\lambda_2 s_2+\cdots+\lambda_j s_j^*+\cdots+\lambda_l s_l$，$k_2^*=\lambda_1 t_1+\lambda_2 t_2+\cdots+\lambda_j t_j^*+\cdots+\lambda_l t_l$，即有 $k_1^*=k_1+\lambda_j\varepsilon$，$k_2^*=k_2+\lambda_j\delta$。这样 P_j 通过计算 $k_1=k_1^*-\lambda_j\varepsilon$ 或 $k_2=k_2^*-\lambda_j\delta$ 便可获得 k_1 的真实值。

3 原方案的安全漏洞

3.1 安全漏洞

原方案提出的防欺诈条件 $k_1^2=k_2$ 并不能有效防止成员之间的欺诈行为。

假设 A 中某一不诚实的成员 P_j 提交伪份额 (s_j^*,t_j^*) 给黑盒子，其中，$s_j^*=s_j+\varepsilon$，$t_j^*=t_j+\delta$。P_i 的共享为 (s_i,t_i)，$i=1,2,\cdots,j-1,j+1,\cdots,l$。

黑盒子计算：k_1^*,k_2^*,k_1,k_2，并且满足 $k_1^2=k_2$，从而有 $k_1^*=k_1+\lambda_j\varepsilon,k_2^*=k_2+\lambda_j\delta$，要使 $(k_1^*)^2=k_2^*$，只需 $\lambda_j^2\varepsilon^2+\lambda_j\delta-2\lambda_j\varepsilon k_1^*=0$，由于 P_j 知道 λ_j，因此任意选取 ε,δ 都可以欺骗其他参与者，并且 P_j 通过计算 $k_1=k_1^*-\lambda_j\varepsilon$ 便可获得真正的秘密 k。

基金项目：国家自然科学基金资助项目(60873119)；陕西师范大学优秀科技预研基金资助项目(GK200902051)

作者简介：雷 娟(1986－)，女，硕士研究生，主研方向：有限域，密码学；李志慧(通讯作者)，教授、博士；张倩倩，硕士研究生

收稿日期：2011-06-17 **E-mail**：snnulzh@yahoo.com.cn

3.2 举例说明

限于篇幅，这里选取部分数据罗列。设 $\Gamma=\{\{P_1,P_2,P_3\},\{P_1,P_2,P_4\},\{P_1,P_3,P_4\}\}$，$K=GF(3)$。函数 ψ 满足：$\psi(D)=(0,0,1)$；$\psi(P_2)=(1,0,1)$；$\psi(P_3)=(0,2,0)$；$\psi(P_4)=(1,2,1)$。

首先验证 Γ 是向量空间 K^3 上的访问结构。由访问结构的定义，只需证 $\psi(D)$ 可由任何授权子集的成员所持的份额线性表示。由访问结构的单调性只需证 $\psi(D)$ 能由任何最小授权子集的成员所持的份额线性表示即可。这里显然成立：

$$-\psi(P_1)+\psi(P_2)-\psi(P_3)=(0,0,1)$$
$$-\psi(P_1)+2\psi(P_2)-\psi(P_4)=(0,0,1)$$
$$-\psi(P_1)-2\psi(P_3)+\psi(P_4)=(0,0,1)$$

然后验证 $\psi(D)$ 不能由任何非授权子集线性表示。同理只需证 $\psi(D)$ 不能由任何最大非授权子集的成员所持的份额线性表示即可。Γ 的最大非授权子集有 4 个：$\{P_1,P_2\}$，$\{P_1,P_3\}$，$\{P_1,P_4\}$，$\{P_2,P_3,P_4\}$。对每种情况都可建立一个特定的线性方程组，并求得相应的线性方程组无解，即 $\psi(D)$ 不能由它们线性表示。

下面以 $\{P_1,P_2\}$ 为例。设：$(1,0,0)=a_1\psi(P_1)+a_2\psi(P_3)$，其中，$a_1,a_2\in K$，这等价于方程组 $\begin{cases}a_1=0\\a_1-a_2=0\\0=1\end{cases}$。容易看出，此方程组无解。其余 3 种情况同理。故 Γ 是向量空间 K^3 上的访问结构。用此方案来说明原方案存在的漏洞，这里不详细说明。

4 改进后的方案

4.1 系统初始化阶段

设 $P=\{P_1,P_2,\cdots,P_n\}$，$D\notin P$，$K=GF(q)$，q 为素数。$E=K^r$。D 选择 $\psi:P\cup\{D\}\to E$ 使得 Γ 是向量空间 E 上的访问结构，同时公开 ψ，$x_i=\psi(P_i)$ 线性无关，$i=1,2,\cdots,n$ $(n\leqslant r)$。

4.2 共享分发阶段

共享分发阶段如下：

(1) D 在 K 中随机选取 n 个不同的数 $d_1,d_2,\cdots,d_n$，并把 (x_i,d_i) 作为 P_i 的身份标识发给黑盒子，$i=1,2,\cdots,n$。

(2) D 首先秘密选取 $v_1\in K^r$，然后计算 $s_{1i}=v_1\cdot x_i$，$s_{ji}=d_i^{j-1}s_{1i}$，且 $s_{ji}=v_j\cdot x_i$，并把 $(s_{1i},s_{2i},\cdots,s_{ni})$ 作为共享发送给 P_i，$j=2,3,\cdots,n$。

(3)对要共享的秘密 $k\in K$ 及 D 秘密选取的 $v_1,v_2,\cdots,v_n$，D 计算 $k_1=v_1\cdot x_0$，$k_2=v_2\cdot x_0,\cdots,k_n=v_l\cdot x_0$，并把 $(k_1,k_2,\cdots,k_n)$ 发送给黑盒子。

4.3 秘密重构阶段

设 $A=\{P_{i_1},P_{i_2},\cdots P_{i_l}\}\in\Gamma$，则黑盒子重构秘密的具体操作如下：

(1)对参与者 P_{i_j} $(j=1,2,\cdots,l)$ 的共享 $(s_{1i_j},s_{2i_j},\cdots,s_{ni_j})$，黑盒子判断：$\frac{s_{2i_j}}{s_{1i_j}}=\frac{s_{3i_j}}{s_{2i_j}}=\cdots=\frac{s_{li_j}}{s_{l-1i_j}}=d_{i_j}$ 是否成立。若成立，则 P_{i_j} 进入下一步验证。否则，黑盒子认为 P_{i_j} 没有提供真实的共享。

(2)黑盒子利用 P_{i_j} $(j=1,2,\cdots,l)$ 的共享，验证以下 l 个等式 $k_j=\lambda_{i_1}s_{ji_1}+\lambda_{i_2}s_{ji_2}+\cdots+\lambda_{i_l}s_{ji_l}$ 是否成立，$j=1,2,\cdots,l$。若所有等式均成立，则 P_{i_j} 是诚实的，黑盒子进行下一步，否则，P_{i_j} 没有提供真实的共享。

(3)设 $x_0=\lambda_{i_1}x_{i_1}+\lambda_{i_2}x_{i_2}+\cdots+\lambda_{i_l}x_{i_l}$，黑盒子计算 $k_1=v_1\cdot x_0=\lambda_{i_1}s_{1i_1}+\lambda_{i_2}s_{1i_2}+\cdots+\lambda_{i_l}s_{1i_l}$，并返回 k_1 作为正确的秘密值。

5 方案分析

5.1 正确性分析

本节主要证明 D 选取的满足以下条件的 $v_1,v_2,\cdots,v_n$ 是存在的。

(1) $s_{j1}=v_j\cdot x_1,s_{j2}=v_j\cdot x_2,\cdots,s_{jn}=v_j\cdot x_n$，$j=1,2,\cdots,n$。

(2) $s_{2i}=d_i\cdot s_{1i},s_{3i}=d_i^2\cdot s_{1i},\cdots,s_{ni}=d_i^{n-1}\cdot s_{1i}$，$i=1,2,\cdots,n$。

设 D 随机选取 $v_1=(a_{11},a_{12},\cdots,a_{1r})\in K^r$，$x_i=(b_{i1},b_{i2},\cdots,b_{ir})$，$i=1,2,\cdots,n$。$D$ 计算：$s_{11}=v_1\cdot x_1,s_{12}=v_1\cdot x_2,\cdots,s_{1n}=v_1\cdot x_n$，则 $s_{21}=d_1\cdot s_{11},s_{22}=d_2\cdot s_{12},\cdots,s_{2n}=d_n\cdot s_{1n}$，它等价于方程组：

$$\begin{cases}v_2\cdot x_1=d_1\cdot s_{11}=d_1\cdot(a_{11}b_{11}+a_{12}b_{12}+\cdots+a_{1r}b_{1r})\\v_2\cdot x_2=d_2\cdot s_{12}=d_2\cdot(a_{11}b_{21}+a_{12}b_{22}+\cdots+a_{1r}b_{2r})\\\vdots\\v_2\cdot x_n=d_n\cdot s_{1n}=d_n\cdot(a_{11}b_{n1}+a_{12}b_{n2}+\cdots+a_{1r}b_{nr})\end{cases}\tag{1}$$

设 $v_2=(a_{21},a_{22},\cdots,a_{2r})$，则式(1)又等价于：

$$\begin{cases}a_{21}b_{11}+\cdots+a_{2r}b_{1r}=d_1s_{11}=d_1a_{11}b_{11}+\cdots+d_1a_{1r}b_{1r}\\a_{21}b_{21}+\cdots+a_{2r}b_{2r}=d_1s_{12}=d_2a_{11}b_{21}+\cdots+d_2a_{1r}b_{2r}\\\vdots\\a_{21}b_{n1}+\cdots+a_{2r}b_{nr}=d_1s_{1n}=d_na_{11}b_{n1}+\cdots+d_na_{1r}b_{nr}\end{cases}\tag{2}$$

由 $x_1,x_2,\cdots,x_n$ 线性无关可得式(2)有解，即 D 选取的满足条件(1)和条件(2)的 v_2 是存在的。同理 D 计算：$s_{j1}=d_1^{j-1}s_{11}$，$s_{j2}=d_2^{j-1}s_{12}$，$\cdots$，$s_{jn}=d_n^{j-1}s_{1n}$，j=3,4, $\cdots$,l。又 $s_{j1}=v_j\cdot x_1$，$s_{j2}=v_j\cdot x_2,\cdots,s_{jn}=v_j\cdot x_n$，则按照以上方法可验证 D 选取的满足条件(1)和条件(2)的 $v_3,v_4,\cdots,v_n$ 也存在。

5.2 可验证性分析

在秘密重构阶段，黑盒子实现了对参与者的身份验证，从而有效地防止了参与者的欺诈行为，以下从 2 个方面具体分析。

(1)黑盒子对参与者 P_{i_j} 进行身份验证时所用的算法。

1)实质为初步验证。因为 P_{i_j} 的共享 $(s_{1i_j},s_{2i_j},\cdots,s_{ni_j})$ 满足：$\frac{s_{2i_j}}{s_{1i_j}}=\frac{s_{3i_j}}{s_{2i_j}}=\cdots=\frac{s_{ni_j}}{s_{n-1i_j}}=d_{i_j}$，所以凡是不满足此条件的参与者一定为欺诈者。

2)实质为进一步验证。由于黑盒子知道 $k_1,k_2,\cdots,k_l$ 的值，即以下每个等式的左边为固定值，则黑盒子可通过验证这 l 个等式是否成立来判定 P_{i_j} 是否为欺诈者，这 l 个等式组成的方程组为：

$$\begin{cases}k_1=\lambda_{i_1}s_{1i_1}+\lambda_{i_2}s_{1i_2}+\cdots+\lambda_{i_l}s_{1i_l}\\k_2=\lambda_{i_1}s_{2i_1}+\lambda_{i_2}s_{2i_2}+\cdots+\lambda_{i_l}s_{2i_l}\\\vdots\\k_l=\lambda_{i_1}s_{li_1}+\lambda_{i_2}s_{li_2}+\cdots+\lambda_{i_l}s_{li_l}\end{cases}\tag{3}$$

(2)通过上面验证的参与者一定是诚实的。

由于 $s_{ji_1}=d_{i_1}^{j-1}s_{1i_1}$，$s_{ji_2}=d_{i_2}^{j-1}s_{1i_2}$，$\cdots$，$s_{ji_l}=d_{i_l}^{j-1}s_{1i_l}$，$j=2,3,\cdots,n$，因此式(3)等价于：

$$\begin{cases}k_1=\lambda_{i_1}s_{1i_1}+\lambda_{i_2}s_{1i_2}+\cdots+\lambda_{i_l}s_{1i_l}\\k_2=\lambda_{i_1}d_{i_1}s_{1i_1}+\lambda_{i_2}d_{i_2}s_{1i_2}+\cdots+\lambda_{i_l}d_{i_l}s_{1i_l}\\k_3=\lambda_{i_1}d_{i_1}^2s_{1i_1}+\lambda_{i_2}d_{i_2}^2s_{1i_2}+\cdots+\lambda_{i_l}d_{i_l}^2s_{1i_l}\\\vdots\\k_l=\lambda_{i_1}d_{i_1}^{l-1}s_{1i_1}+\lambda_{i_2}d_{i_2}^{l-1}s_{1i_2}+\cdots+\lambda_{i_l}d_{i_{l1}}^{l-1}s_{1i_l}\end{cases}\tag{4}$$

其系数矩阵的行列式为：

$$\begin{vmatrix} \lambda_{i_1} & \lambda_{i_2} & \cdots & \lambda_{i_l} \\ \lambda_{i_1}d_{i_1} & \lambda_{i_2}d_{i_2} & \cdots & \lambda_{i_l}d_{i_l} \\ \lambda_{i_1}d_{i_1}^2 & \lambda_{i_2}d_{i_2}^2 & \cdots & \lambda_{i_l}d_{i_l}^2 \\ \vdots & \vdots & & \vdots \\ \lambda_{i_1}d_{i_1}^{l-1} & \lambda_{i_2}d_{i_2}^{l-1} & \cdots & \lambda_{i_l}d_{i_l}^{l-1} \end{vmatrix} = \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_l} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ d_{i_1} & d_{i_2} & \cdots & d_{i_l} \\ d_{i_1}^2 & d_{i_2}^2 & \cdots & d_{i_l}^2 \\ \vdots & \vdots & & \vdots \\ d_{i_1}^{l-1} & d_{i_2}^{l-1} & \cdots & d_{i_l}^{l-1} \end{vmatrix}$$

由 d_{i_j} 互不相同知行列式不为零，故 $s_{1i_j}, s_{2i_j}, \cdots, s_{li_j}$ 是正确的，又 $s_{l+1i_j} = d_{i_j}s_{1i_j}$，$s_{l+2i_j} = d_{i_j}^2 s_{1i_j}$，$\cdots, s_{ni_j} = d_{i_j}^{n-1}s_{1i_j}$，$j = 1,2,\cdots,l$，故 P_{i_j} 出示的共享的所有分量都正确，即通过黑盒子两步验证的参与者一定是诚实的。

5.3 安全性分析

方案的安全性基于本文所讨论的线性方程组有唯一解这一结论。黑盒子首先对参与者的共享的前 l 个分量进行验证，再根据每个参与者的共享的 n 个分量之间的关系，即可完成对参与者所持共享的所有分量的验证，而且非授权子集中的参与者的联合无法重构秘密。故方案可有效地检测和识别出不诚实的参与者，从而提高了方案的实用性。

6 结束语

本文基于向量空间访问结构，提出一种防欺诈的秘密共享方案。根据本文中所讨论的线性方程组有唯一解这一结论，黑盒子实现了对授权子集中的参与者的身份验证，从而有效地防止了参与者的欺诈行为。今后还可从量的角度考虑方案的信息率，总的来说，新方案具有较强的安全性和实用性。

参考文献

[1] Shamir A. How to Share a Secret[J]. Communications of ACM, 1979, 22(11): 612-613.

[2] Blakley G R. Safeguarding Cryptographic Keys[D]. Rudder Tower, Texas, USA: Texas A&M University, 1979.

[3] Rima C. How to Avoid Cheaters Succeeding in the Key Sharing Scheme[J]. Designs, Codes and Cryptography, 1993, 3(3): 221-228.

[4] Ogata W, Kurosawa K. Optimum Secret Sharing Scheme Secure Against Cheating[C]//Proc. of EUROCRYPT'96. Berlin, Germany: [s. n.], 1996.

[5] Tompa M, Woll H. How to Share a Secret with the Cheaters[J]. Journal of Cryptology, 1988, 1(2): 133-139.

[6] Jorge L V. Detection of Cheaters in Vector Space Secret Sharing Schemes[J]. Designs, Codes and Cryptography, 1999, 16(1): 75-85.

[7] Brickell E F. Some Ideal Secret Sharing Schemes[C]//Proc. of EUROCRYPT'89. New York, USA: [s. n.], 1989.

[8] Simmons G J. How to Really Share a Secret[M]. Berlin, Germany: [s. n.], 1989.

[9] Simmons G J. An Introduction to Shared Secret and/or Shared Control Schemes and Their Applications[M]. Piscataway, USA: [s. n.], 1992.

编辑 陈 文

(上接第 99 页)

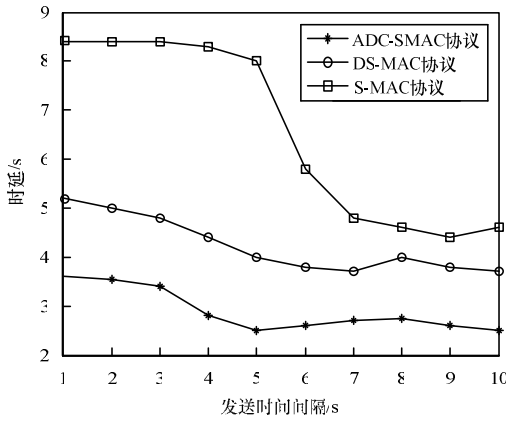

图 8 网状拓扑下平均延迟比较结果

5 结束语

无线传感器网络有各种不同的应用环境，有的只要求低能耗，有的只要求低时延，有的既要求低能耗也要求低时延。因此，本文提出 ADC-SMAC 来解决在不同应用背景下能耗与时延的均衡问题。为了解决这个问题，本文提出的机制主要为根据节点利用率、平均睡眠延时和占空比上下限等调节参数，动态地调节节点的占空比，目的是在一定程度上同时保证低能耗和低延时。在线性拓扑和网状拓扑下对 S-MAC、DS-MAC、ADC-SMAC 进行了对比实验，结果证明在这 2 种拓扑下，ADC-SMAC 的能耗和延时都比 S-MAC 和 DS-MAC 有了较大的改善。

参考文献

[1] 任丰源, 黄海宁, 林 闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282-1291.

[2] 丁 睿, 南建国. 无线传感器网络 MAC 协议的研究与分析[J]. 计算机工程, 2009, 35(19): 105-107.

[3] Ye Wei, Heidemann J, Estrin D. Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks[J]. IEEE/ACM Transactions on Networking, 2004, 12(3): 493-506.

[4] Zhang Dengyin, Jiang Juan, Anani A, et al. QoS-guaranteed Packet Scheduling in Wireless Networks[J]. Institute of Signal Processing and Transmission, 2009, 16(4): 63-67.

[5] Lu Gang, Sadagopan N, Krishnamachari B, et al. Delay Efficient Sleep Scheduling in Wireless Sensor Networks[C]//Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies. [S. 1.]: IEEE Press, 2005: 2470-2481.

[6] 刘希若, 袁康敏, 李院民. 无线传感器网络新型 MAC 协议研究[J]. 通信技术, 2008, 41(8): 160-165.

[7] 徐雷鸣, 庞 博, 赵 耀. NS 与网络模拟[M]. 北京: 人民邮电出版社, 2003.

编辑 索书志