基于向量空间上的无分发者的秘密共享方案 *

张倩倩, 李志慧, 雷 娟
(陕西师范大学 数学与信息科学学院, 西安 710062)

摘 要: 将 Harn 和 Lin 提出的(n,t,n)秘密共享方案的思想应用到向量空间秘密共享方案,利用向量空间秘密共享方案(+,+)同态性质,提出了一个基于向量空间上的无分发者的秘密共享方案。新方案中每个参与者也是分发者,主秘密由每个分发者的子秘密决定,避免了秘密由一个分发者选择、分发而造成分发者权利过大的问题;新方案适用于向量空间访问结构,较(n,t,n)秘密共享方案更具一般性,应用范围更广。

关键词: 秘密共享; 向量空间; 同态; 无分发者; 子秘密; 主秘密
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2011)06-2230-03
doi:10.3969/j.issn.1001-3695.2011.06.064

Secret sharing scheme without dealer in vector space

ZHANG Qian-qian, LI Zhi-hui, LEI Juan
(*College of Mathematics & Information Science, Shaanxi Normal University, Xi'an* 710062, *China*)

Abstract: The idea of (n,t,n) secret sharing scheme, which was proposed by Harn and Lin, was generalized to secret sharing scheme in vector space, and based on the (+,+) homomorphism property of secret sharing scheme in vector space, a secret sharing scheme without dealer in vector space was proposed. In this new scheme, each participant also acted as a dealer. This scheme avoided the problem that a secret was chosen and distributed by a dealer so that the dealer had too much powerful right. Furthermore, the scheme was suited to the vector space access structure. Compared with the (n,t,n) secret sharing scheme, the new scheme is more general and is applied more widely.

Key words: secret sharing; vector space; homomorphism; no dealer; sub-secret; master-secret

0 引言

秘密共享方案是在 n 个参与者中共享秘密的方法,即将秘密分成 n 个子秘密分别分发给 n 个参与者,使得任何参与者的授权子集能够恢复秘密,而参与者的非授权子集不能得到秘密的任何信息。自 1979 年 Shamir[1] 和 Blakley[2] 独自地提出了实现门限访问结构的秘密共享方案即门限方案以来,许多学者对秘密共享方法和具体实现进行了大量研究。文献[3]是动态秘密共享方案,解决了参与者的增加和删除问题;文献[4,5]是多秘密共享方案,方案中参与者可同时共享多个秘密;文献[6]提出层次秘密共享方案,实现了不同层次的参与者间的秘密共享;文献[7]是可验证的秘密共享方案,能有效地防止参与者之间的欺诈。在上述这些方案中都存在参与者之外的一个分发者 D。秘密由 D 单独选择、分发,这就造成了分发者权利过大;再者,D 有可能给参与者发送伪份额使得参与者无法恢复出有效的秘密。后一个问题的解决可以根据文献[7]提出的可验证秘密共享方案,在参与者和分发者之间加上一个验证算法,参与者通过验证算法可以确定分发者分发给他的共享的有效性。但是两个问题要同时解决,则需要建立无分发者的秘密共享体制来实现。

1990 年,Ingemarsson 等人[8] 首次提出了一个无可信第三方参与的(t,n)秘密共享方案,在该方案中每个参与者也是分发者。首先,每个分发者 P_i(也是参与者)随机地选择一个子秘密 S_i(其中 $i=1,2,\cdots,n$),主秘密 S 就由 $S=\sum_{i=1}^{n}S_i$ 确定;然后每个分发者 P_i 在其他的 $n-1$ 个参与者中利用 Shamir$(t,n-1)$秘密共享方案(记做 Shamir$(t,n-1)$SS)共享他选择的子秘密 S_i;最后,每个分发者 P_i 就会收到 $n-1$ 个来自其他分发者分发的共享。任何 t 个参与者子集把他们自己选择的子秘密放在一起并且利用 Shamir$(t,n-1)$SS 重构出剩余的 $n-t$ 个子秘密, 从而由 $S=\sum_{i=1}^{n}S_i$ 重构出主秘密。但是这个方案存在一个潜在的问题,即每个参与者持有的共享个数 n 是与参与者的个数 n 成比例的。随着参与者人数的增加,每个参与者收到的共享的个数就会相应增加。对每个参与者来说,共享的存储和管理就会成为一个非常复杂的问题。

Harn 等人[9] 根据 Pedersen[10] 在 1991 年提出的无可信中心的(t,n)密码体制定义了一个(n,t,n)秘密共享方案,记做(n,t,n)SS。在这个方案中,每个参与者也是分发者,主秘密由每个分发者选择的子秘密决定,即主秘密是所有子秘密的和。每个分发者利用 Shamir(t,n)SS 在所有的参与者中共享他选择的子秘密,最后每个参与者(也是分发者)都会收到 n 个子共享,对这些子共享求和就得到其主共享。根据 Shamir(t,n)

收稿日期: 2010-10-05; **修回日期**: 2010-12-28 **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资助项目(GK200902051)

作者简介: 张倩倩(1985-),女,河南焦作人,硕士研究生,主要研究方向为有限域、密码学(wszqq_507@163.com); 李志慧(1966-),女,教授,博士,主要研究方向为有限域、密码学; 雷娟(1986-),女,硕士研究生,主要研究方向为有限域、密码学.

SS 满足(+,+)同态性质[11],任何 t 个参与者把他们的主共享放在一起就可以恢复出主秘密。也就是说,每个参与者只需秘密地保管一个主共享就可以恢复出主秘密,避免了 Ingemarsson 和 Simmons 提出的(t,n)SS 中存在的每个参与者对收到的多个共享的存储和管理问题。但该方案只适用于门限访问结构。

本文将 Harn 等人提出的(n,t,n)SS 的思想应用到向量空间秘密共享方案[12],提出了一个基于向量空间上无分发者的秘密共享方案。该方案中每个参与者也是分发者,根据定义的向量空间秘密共享的(+,+)同态性质,每个参与者也只需保管其主共享。该方案适用于向量空间访问结构,与(n,t,n)SS 相比,更具一般性,应用范围更广。本文最后通过举例说明了该方案的一个实际应用。

1　向量空间秘密共享方案及其(+,+)同态性质

1.1　向量空间秘密共享方案

1)初始化阶段

设 $P=\{P_1,P_2,\cdots,P_n\}$是 n 个参与者组成的集合, 分发者 $D\notin P$。$K=GF(q)$是一个有限域,$E=K^t$ 是 K 上的 t 维向量空间。Γ 是 P 上的一个单调访问结构,且 t 不小于所有最小合格子集的最大基数。称 Γ 是一个向量空间访问结构,如果存在函数 $\varphi:P\cup\{D\}\to E$ 满足特性 $\varphi(D)=(1,0,\cdots,0)\in\langle\varphi(P_i):P_i\in B\rangle\Leftrightarrow B\in\Gamma$。

D 向全体参与者公布函数 φ。

2)共享分发阶段

对要分享的秘密 $S\in K$,D 随机地选取 $v_2,v_3,\cdots,v_t\in K$,并令 $V=(v_1,v_2,\cdots,v_t)$,其中 $v_1=S$。显然,$V\cdot\varphi(D)=S$。D 计算 $s_i=V\cdot\varphi(P_i)$,并把 s_i 的值作为 P_i 的共享秘密发给 P_i。

3)秘密恢复阶段

当 P 的一个授权子集 $B=\{P_1,P_2,\cdots,P_l\}$要恢复秘密时,根据初始化阶段中定义的 φ 函数的特性,则有 $\varphi(D)=(1,0,\cdots,0)\in\langle\varphi(P_i):P_i\in B\rangle$,$B$ 中参与者先求出 E 中的一个向量 $x=(c_1,c_2,\cdots,c_l)$,满足$\sum_{i=1}^{l}c_i\varphi(P_i)=(1,0,\cdots,0)$,则有 $S=V\cdot\varphi(D)=V\cdot\sum_{i=1}^{l}c_i\varphi(P_i)=\sum_{i=1}^{l}c_i(V\cdot\varphi(P_i))=\sum_{i=1}^{l}c_is_i$。从而对 B 中的参与者来说,秘密 S 由他们所拥有的共享的线性组合来恢复。

1.2　向量空间秘密共享方案的(+,+)同态性质

定义 1　在向量空间秘密共享方案中,设 K 是秘密集,S_i $(i=1,2,\cdots,n)$是 P_i 的共享集,Γ 是一个向量空间访问结构。$\forall B=\{P_1,P_2,\cdots,P_l\}\in\Gamma$,定义函数 $\psi_B:(s_1,s_2,\cdots,s_l)\to K$。令 $S,S'\in K$,其中,$S=\psi_B(s_1,s_2,\cdots,s_l)$,$S'=\psi_B(s'_1,s'_2,\cdots,s'_l)$,若有 $S+S'=\psi_B(s_1+s_1',s_2+s_2',\cdots,s_l+s_l')$,则称这种性质为向量空间秘密共享方案的(+,+)同态性质。

Benaloh[11]定义了(t,n)门限方案关于$(\oplus,\otimes)$的同态性质,并且指出 Shamir(t,n)SS 具有(+,+)同态性质以及同态性质没有泄露秘密的任何信息。在向量空间秘密共享方案中,由其安全性(即非授权子集不能得到秘密的任何信息)可以得到其(+,+)同态性质也不会泄露秘密的任何信息。

2　向量空间上无分发者的秘密共享方案

概括地讲,方案中每个参与者也是分发者,每个分发者(也是参与者)想要参与和共享一个主秘密。首先,每个分发者随机选取一个秘密,称该秘密为一个子秘密,主秘密就由所有的子秘密决定;然后每个参与者按 1.1 节中的向量空间秘密共享方案中的共享方式来和其他分发者共享该子秘密。根据向量空间秘密共享方案的秘密恢复算法和(+,+)同态性质,任何授权子集 $B\in\Gamma$ 中的参与者就可以通过他们主共享的线性组合恢复出主秘密。

定义 2　假定有 n 个分发者(也是参与者)$P=\{P_1,P_2,\cdots,P_n\}$,$K=GF(q)$是一个有限域,$E=K^t$ 是 K 上的 t 维向量空间。Γ 是 P 上的一个向量空间访问结构,且 t 不小于所有最小合格子集的最大基数,ϕ 为公开函数。基于向量空间上的无分发者的秘密共享方案由四个算法组成,如表 1 所示。

表 1　基于向量空间上的无分发者的秘密共享方案由四个算法组成

S	S_1	…	S_n	主共享
p_1	s_{11}	…	s_{n1}	$s_1=\sum_{j=1}^{n}s_{j1}$
p_2	s_{12}	…	s_{n2}	$s_2=\sum_{j=1}^{n}s_{j2}$
…	…		…	…
p_n	s_{1n}	…	s_{nn}	$s_n=\sum_{j=1}^{n}s_{jn}$

方案 1

a)主秘密生成算法。每个分发者 P_i(其中,$i=1,2,\cdots,n$)随机独立地选取子秘密 S_i,主秘密 S 就由 $S=\sum_{i=1}^{n}S_i$ 决定。

b)子共享生成算法。对每个子秘密 S_i,分发者 P_i 首先随机选取一个向量 $V_i\in E$,满足 $V_i\cdot(1,0,\cdots,0)=S_i$。$P_i$ 计算 $s_{ij}=V_i\cdot\phi(P_j)$(其中 $j=1,2,\cdots,n$),并把 s_{ij}作为 P_j($j=1,2,\cdots,n$ 且 $j\neq i$)的子共享秘密地发送给 P_j。最后每个分发者 P_i 都将持有 n 个子共享 $s_{1i},s_{2i},\cdots,s_{ni}$。

c)主共享生成算法。每个参与者 P_i(也是分发者)将收到的 n 个子共享 s_{ji}($j=1,2,\cdots,n$)求和来计算他的主共享 s_i,即 $s_i=\sum_{j=1}^{n}s_{ji}=\sum_{j=1}^{n}V_j\cdot\phi(P_i)$。

d)主秘密恢复算法。设 $B\in\Gamma$ 是一个授权子集,则 B 中的参与者利用他们的主共享的线性组合恢复主秘密 S,其中,$S=\sum_{i=1}^{n}S_i=\sum_{i=1}^{n}V_i\cdot(1,0,\cdots,0)$。

定理 1　在方案 1 中,设 $B=\{P_1,P_2,\cdots,P_l\}\in\Gamma$,其中,$1<l<n$。根据 1.1 节中向量空间秘密共享方案的秘密恢复算法,主秘密 S 可由 B 中参与者的主共享的线性组合恢复。

证明:根据方案 1 中的主秘密生成算法,B 中的参与者可先恢复出各子秘密,再通过 $S=\sum_{i=1}^{n}S_i$ 恢复主秘密 S。具体如下:

已知 $B\in\Gamma$,所以$(1,0,\cdots,0)\in\langle\phi(P_i):P_i\in B\rangle$。不妨设 $(1,0,\cdots,0)=\sum_{i=1}^{l}c_i\phi(P_i)$。由 1.1 节中向量空间秘密共享方案

的秘密恢复算法,B 中的参与者可以恢复出子秘密 $S_1, S_2, \cdots, S_n$。其中

$$S_1 = V_1 \cdot (1,0,\cdots,0) = V_1 \cdot \sum_{i=1}^{l} c_i \phi(P_i) = \sum_{i=1}^{l} c_i (V_1 \cdot \phi(P_i)) = \sum_{i=1}^{l} c_i s_{1i}$$

$$S_2 = V_2 \cdot (1,0,\cdots,0) = V_2 \cdot \sum_{i=1}^{l} c_i \phi(P_i) = \sum_{i=1}^{l} c_i (V_2 \cdot \phi(P_i)) = \sum_{i=1}^{l} c_i s_{2i}$$

$$\cdots$$

$$S_n = V_n \cdot (1,0,\cdots,0) = V_n \cdot \sum_{i=1}^{l} c_i \phi(p_i) = \sum_{i=1}^{l} c_i (V_n \cdot \phi(p_i)) = \sum_{i=1}^{l} c_i S_{ni}$$

然后,根据方案 1 中的主秘密生成算法中的等式 $S = \sum_{i=1}^{n} S_i$,将上边得到的 $S_1, S_2, \cdots, S_n$ 代入此式,得出

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

$$\sum_{i=1}^{l} c_i s_{1i} + \sum_{i=1}^{l} c_i s_{2i} + \cdots + \sum_{i=1}^{l} c_i s_{ni} = \tag{2}$$

$$c_1 \sum_{j=1}^{n} s_{j1} + c_2 \sum_{j=1}^{n} s_{j2} + \cdots + c_l \sum_{j=1}^{n} s_{jl} = \tag{3}$$

$$c_1 s_1 + c_2 s_2 + \cdots + c_l s_l \tag{4}$$

式(1)是按照主秘密生成算法得出的;式(2)是由向量空间秘密共享方案的秘密恢复算法恢复子秘密;式(3)由向量空间秘密共享方案的加法同态性质得到;式(4)表明 $B = \{P_1, P_2, \cdots, P_l\}$ 是一个授权子集,B 中参与者的主共享 $s_1, s_2, \cdots, s_l$ 的线性组合恢复主秘密。

另外,若 A 为方案 1 中的任一个非授权子集,根据向量空间秘密共享方案的安全性,$(1,0,\cdots,0)$ 不能由向量组 $\{\phi(P_i): P_i \in A\}$ 线性表示,故 A 中的参与者不能由其主共享恢复出主秘密;同时也不能由其子共享恢复出其他参与者选择的子秘密,进而对子秘密求和得到主秘密。

3 例子

一个银行有两个经理 P_1、P_2 和两个出纳 P_3、P_4。已知金库的大门需要这四个人按照 $\Gamma = \{\{P_1, P_2\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}\}$ 存取结构来管理,密钥集 $K = F_3$。构造函数 $\phi: P \to K^3$,其中,$\phi(P_1) = (1,2,2)$,$\phi(P_2) = (1,2,1)$,$\phi(P_3) = (0,1,0)$,$\phi(P_4) = (0,0,1)$。可验证 Γ 是一个向量空间访问结构。由于没有密钥管理中心,金库门的密钥,即电子锁号码必须由这四个人共同决定,于是 P_1、P_2、P_3、P_4 各自秘密地输入各自的子密钥,即 S_1、S_2、S_3、S_4,主密钥 $S = S_1 + S_2 + S_3 + S_4$ 就确定了。然后每个人选择 $V_i \in K^3 (i = 1,2,3,4)$ 使得 $V_i \cdot (1,0,0) = S_i$。P_i 计算 $S_{ij} = V_i \cdot \phi(p_j)$,并把 s_{ij} 作为 $P_j (j = 1,2,3,4$ 且 $j \neq i)$ 的子共享秘密地发送给 P_j,从而 $P_i (i = 1,2,3,4)$ 持有的子共享为 s_{1i}、s_{2i}、s_{3i}、s_{4i}。P_i 对他收到的子共享求和得到他的主共享 $s_i = s_{1i} + s_{2i} + s_{3i} + s_{4i}$。

假如 Γ 中的授权子集 $\{P_1, P_3, P_4\}$ 要恢复主密钥(即电子锁号码),根据方案 1 的 d) 主秘密恢复算法,可按照如下步骤操作:

a) P_1, P_3, P_4 先求出向量 $x = (c_1, c_3, c_4)$ 满足 $c_1\phi(P_1) + c_3\phi(P_3) + c_4\phi(P_4) = (1,0,0)$;

b) P_1, P_3, P_4 将掌握的主共享 s_1, s_3, s_4 与 $x = (c_1, c_3, c_4)$ 做内积得到主秘密,即 $S = c_1 s_1 + c_3 s_3 + c_4 s_4$。

假如 Γ 的一个极大非授权子集 $\{P_3, P_4\}$ 要恢复秘密,由于方程 $c_3\phi(P_3) + c_4\phi(P_4) = (1,0,0)$ 无解,他们除了最多知道自己选择的子秘密外并不能得到其他的子秘密和主秘密。

4 结束语

在实际应用中,考虑无可信第三方的秘密共享方案是很有必要的,而目前已提出的两个方案都是基于门限访问结构的。本文将 (n,t,n)SS 的思想应用到向量空间秘密共享上,提出了一个向量空间上的无分发者的秘密共享方案,并证明了它的可行性。新方案适用于向量空间访问结构,与 (n,t,n)SS 相比,更具一般性,应用范围更广。

参考文献:

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11):612-613.

[2] BLAKLEY G. Safeguarding cryptographic keys[C]//Proc of National Computer Conference. New York: AFIPS Press, 1979:313-317.

[3] LAIN C, HARN L, LEE J, *et al*. Dynamic threshold scheme based on the definition of cross-product on *N*- dimensional linear space [C]//Proc of Advances in Cryptology. 1989: 20-24.

[4] 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.

[5] PANG Liao-jun, WANG Yu-min. A new (t,n) multi- secret sharing scheme based on Shamir secret sharing[J]. Applied Mathematics and Computation, 2005, 167(2): 840-848.

[6] CHARNES C, MARTIN K, PIEPRZYK J, *et al*. Secret sharing in hierarchical groups[C]//Proc of the 1st International Conference on Information and Communication Security. London: Spriger-Verlag, 1997:81-85.

[7] CHOR B, GOLDWASSER S, MICALI S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Proc of the 26 th IEEE Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 1985:383-395.

[8] INGEMARSSON I, SIMMONS G J. A protocol to set up shared secret schemes without the assistance of a mutually trusted party[C]// Proc of Workshop on the Theory and Application of Cryptographic. Berlin: Springer-Verlag,1991:266-282.

[9] HARN L, LIN Chang-lu. Strong (n,t,n) verifiable secret sharing scheme[J]. Information Science, 2010, 180(16):3059-3064.

[10] PEDERSEN T P. A threshold cryptosystem without a trusted party [C]//Proc of the 10th International Conference on Theory and Application of Cryptographic. Berlin:Springer-Verlag,1991:522-526.

[11] BENALOH J C. Secret sharing homomorphisms: keeping shares of a secret[C]//Proc of Aavances in Cryptology. Berlin:Springer-Verlag, 1987:251-260.

[12] STINSON D R. 密码学原理与实践[M]. 冯登国,等译. 3 版. 北京: 电子工业出版社,2009.