门限多重秘密共享方案*)

石润华[1] 仲 红[1] 黄刘生[2]
(安徽大学计算机科学与技术学院 合肥 230039)[1]
(中国科学技术大学计算机科学与技术系 合肥 230027)[2]

摘 要 定义了门限多重秘密共享方案。该方案是一种完全动态的门限方案的自然扩展,能够共享多个秘密,每个秘密拥有独立的门限存取结构,每个参与者仅仅保留一份共享,能够分阶段重构所有的秘密。分析了共享和公开信息的下界(on size),并提出了一种最优的门限多重秘密共享方案。该方案是一种多阶段使用的秘密共享方案,其中参与者的共享与单个秘密同样大小,而且公开的信息量达到最优下界。

关键词 门限,多重秘密,多阶段使用,完备,理想

Threshold Multi-secret Sharing Scheme

SHI Run-hua[1] ZHONG Hong[1] HUANG Liu-sheng[2]
(School of Computer Science and Technology, Anhui University, Hefei 230039, China)[1]
(Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China)[2]

Abstract Defined the threshold multi-secret sharing scheme, which was naturaly extended from the full dynamic threshold secret sharing scheme. In such a scheme, many secrets are shared in such a way that each secret can be reconstructed according to independent (t_i, n)-threshold access structure without refreshing the shares. Then it analyzed the lower bounds of the shares and the public information (on size) for the threshold multi-secret sharing scheme, and proposed an optimal threshold multi-secret sharing scheme. This scheme is a multi-stage-use secret sharing scheme, in which the size of the participant's share is the same as that of each secret and the size of the public information achieves the optimal lower bound.

Keywords Threshold, Multi-secret, Multi-stage-use, Perfect, Ideal

1 引言

秘密共享在现代密码学中有着非常重要的应用,诸如在密钥分发、存取控制、安全多方计算、电子商务等领域,甚至是控制导弹的发射。最早的秘密共享方案是门限方案,分别由Blakley[1]和Shamir[2]于1979年提出。在(t,n)门限方案中,任意t个或多于t个用户联合起来可以恢复秘密,而任意少于t个用户却不能。随后,Ito等[3]和Benaloh等[4]提出了更一般存取结构(access structure)上的秘密共享方案。令参与者集合$\mathcal{P}=\{\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n\}$。$\Gamma\subset 2^{\mathcal{P}}$是由$\mathcal{P}$的子集所组成的集合,且$\Gamma$中任意子集都能够恢复秘密,则称$\Gamma$为存取结构,$\Gamma$中的元素称为授权子集(authorized subset)。

显然,单个秘密共享方案存在效率较低的缺点,而多重秘密共享方案[5-8]能很好地解决这一问题,它是单个秘密共享方案的自然扩展。在多重秘密共享方案中,各参与者只需保护一个秘密份额,就可以实现多个秘密的共享。例如,需要共享的秘密有m个:$K_1,K_2,\cdots,K_m$,而每个参与者仅仅保存一个共享份额S_i。另外,每个秘密K_i拥有各自独立的存取结构Γ_i。若$A\in\Gamma_i$,则A中所有参与者合作能够恢复秘密K_i,而任何其它子集$B\notin\Gamma_i$都不能恢复秘密K_i。门限多重秘密共享方案是一般存取结构上的多重秘密共享方案的特殊情形,其中$\Gamma_i=\{A\subseteq\mathcal{P}\}:|A|\geqslant t_i\}$,$i=1,\cdots,m$。

由文献[9]可知,不存在满足$|S_j|\leqslant|K_i|$的无条件安全的多阶段使用的秘密共享方案。在已有的多重秘密共享方案中,为了使得$|S_j|=|K_i|$,秘密持有者必须公开额外信息。而公开信息量的多少也成为衡量方案好坏的一个标准。虽然有多数文献[10,11]已提出了共享的下界(on size),但公开信息的下界还没有已知结果。本文中,我们对此进行了初步的探讨。首先借鉴动态的门限方案思想,重新定义了多重秘密共享方案。并分析了共享和公开信息的下界(on size)。然后提出了一种最优的门限多重秘密共享方案。

2 门限多重秘密共享方案

2.1 门限方案

设K(空间$\mathcal{K}$上的随机变量)为共享的秘密,S_j(空间S上的随机变量)是参与者j所拥有的共享,$j\in\{1,\cdots,n\}$。$H(\cdot)$:香农熵(Shannon entropy),$I(\cdot)$:互信息(mutual Information)。

定义1((t,n)门限秘密共享方案) 在n个参与者中共享秘密K并且满足:

1)任意t个或多于t个共享能够恢复秘密K。即,$H(K|S_{i_1},\cdots,S_{i_k})=0$ if $k\geqslant t$;

2)少于t个共享不能恢复秘密K。即,$H(K|S_{i_1},\cdots,S_{i_k})>0$ if $k<t$;

*)国家自然科学基金资助项目(60773114),安徽省自然科学基金资助项目(070412051),安徽高校省级重点自然科学研究项目(KJ2007A043)。
石润华 讲师,博士生,研究方向为信息安全;仲 红 博士,副教授;黄刘生 教授,博导。

其中$\{i_1,\cdots,i_k\}\subseteq\{1,\cdots,n\}$。若以上性质2)改为以下性质3)则称为完备的(perfect)门限秘密共享方案。

3)少于t个共享不仅不能恢复秘密K,而且不能够得到有关K的任何信息。即,$H(K|S_{i_1},\cdots,S_{i_k})=H(K)$ if $k<t$;

文献[12]给出了完备门限秘密共享方案的一个必要条件:

$$H(S_i)\geqslant H(K)\ \text{for}\ i=1,\cdots,n \tag{1}$$

通常把满足$H(S_i)=H(K)$ for $i=1,\cdots,n$的方案称为理想的方案。

2.2 门限多重秘密共享方案

在动态的秘密共享方案中,为了动态更新共享的秘密,秘密持有者需要公开部分信息。显然,动态的秘密共享方案可以扩展为多重秘密共享方案:一次共享过程可以分享多个秘密,只需要秘密持有者按照某种顺序公开多个信息。秘密重构时,授权子集中所有参与者根据公开信息可以恢复出相应的秘密,但所有秘密共用一个固定的门限值,因而这样扩展的方案不是多阶段使用的多重秘密共享方案。究其原因,已有的文献研究动态的秘密共享方案[13-15],多是停留在秘密、共享的更新,以及新个体的加入或参与者的删除,并没有涉及门限值t的改变。而多阶段使用的多重秘密共享方案中,每个秘密对应一个独立的门限值。所以当重构门限值不同的多重秘密时,以上扩展方案需要秘密持有者的参与。但是,我们可以借鉴动态秘密共享方案的思想,在多重秘密共享方案中,为了使得参与者保存的共享尽量地小,秘密持有者需要公开部分信息。于是,我们重新定义了多重秘密共享方案。

在下面定义的多重秘密共享方案中:参与者的共享独立随机生成,与单个秘密无关;所有的秘密也是独立随机生成,针对每个共享的秘密,秘密持有者事先发布各自独立的公开信息,并且每个秘密所对应的门限值由其公开信息确定。实质上,这是一种扩展的完全动态的门限多重秘密共享方案。

定义2(门限多重秘密共享方案) 在n个参与者中共享m个秘密$K_1,K_2,\cdots,K_m$,每个秘密K_i拥有各自的门限存取结构(t_i,n),并且满足:

1)根据公开信息P_i,任意t_i个或多于t_i用户能够恢复秘密K_i。即$H(K_i|S_{i_1},S_{i_2},\cdots,S_{i_k},P_i)=0$ if $k\geqslant t_i$ for $i=1,\cdots,m$;

2)如果没有公开信息P_i,即使所有的用户参与都不能恢复秘密K_i。即$H(K_i|S_1,S_2,\cdots,S_n)>0$ for $i=1,\cdots,m$;

3)少于t_i个用户不能恢复秘密K_i。即$H(K_i|S_{i_1},\cdots,S_{i_k},P_i)>0$ if $k<t_i$ for $i=1,\cdots,m$;

其中$\{i_1,\cdots,i_k\}\subseteq\{1,\cdots,n\}$。若以上性质2)、3)分别改为以下性质4)、5)则称为完备的门限多重秘密共享方案。

4)如果没有公开信息P_i,即使所有的用户参与不仅不能重构秘密K_i,而且不能得到有关K_i的任何信息。即$H(K_i|S_1,S_2,\cdots,S_n)=H(K_i)$ for $i=1,\cdots,m$;

5)少于t_i个共享不仅不能恢复秘密K_i,而且不能得到有关K_i的任何信息。即$H(K_i|S_{i_1},\cdots,S_{i_k},P_i)=H(K_i)$ if $k<t_i$ for $i=1,\cdots,m$。

3 共享及公开信息的下界

在这节,我们探讨门限多重秘密共享方案的共享及公开信息的下界,将以定理的形式引出。

定理1 假定$H(K_1)=H(K_2)=\cdots=H(K_m)=H(K)$,则对于完备的门限多重秘密共享方案,有$H(S_j)\geqslant H(K)$,$j=1,\cdots,n$。

证明:因为对于任意的随机变量X,Y,Z,有$I(X;Y|Z)=H(X|Z)-H(X|Y,Z)=H(Y|Z)-H(Y|X,Z)$,则$I(K_i;S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=H(K_i|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)-H(K_i|S_j,S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=H(K_i)-0=H(K)$,其中$S_j\notin\{S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}}\}$(根据定义2,$H(K_i|S_j,S_{i_1},S_{i_2},\cdots,S_{i_{t-1}},P_i)=0$),其中$i=1,\cdots,m$。

又因为$H(S_j)\geqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)$,故$H(S_j)\geqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)-H(S_j|K_i,S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=I(K_i;S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=H(K)$,即$H(S_j)\geqslant H(K)$。

同样对于$H(S_j)=H(K)$ for $j=1,\cdots,n$的多重秘密共享方案称为理想的多重秘密共享方案。

定理2 假设各参与者保存的共享相互间随机独立,则对于理想、完备的门限多重秘密共享方案,有$H(P_i)\geqslant(n-t_i+1)H(K_i)$ for $i=1,\cdots,m$。

证明:首先计算$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_k},P_i)$,$S_j\notin\{S_{j_1},S_{j_2},\cdots,S_{j_k}\}$,$1\leqslant k\leqslant n$。分以下4种情形考虑:

①$k=t_i-1$:$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)\geqslant I(S_j;K_i|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=H(K_i|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)-H(K_i|S_j,S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=H(K)-0=H(K)$

另一方面$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)\leqslant H(S_j)=H(K)$(理想、完备);

②$k<t_i-1$:$H(S_j)\geqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_k},P_i)\geqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i)=H(K)$;

③$k=t_i$:$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i,K_i)=H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i)+H(K_i|S_j,S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i)=H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i)+0=H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i)$

$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i,K_i)\leqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i,K_i)=0$

参考文献[16] lemma6:Let X,Y and Z be random variable. Given $H(X|Y,Z)=0$, and $H(X|Z)=H(Y|Z)$, then $H(Y|X,Z)=0$这里,若$X=K_i,Y=S_j,Z=S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i$,则$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i-1}},P_i,K_i)=0$,也即$H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i)=0$;

④$k>t_i$:$0\leqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_k},P_i)\leqslant H(S_j|S_{j_1},S_{j_2},\cdots,S_{j_{t_i}},P_i)=0$

综上,所以,$H(P_i)\geqslant I(P_i;S_1,S_2,\cdots,S_n,K_i)=I(P_i;S_1,S_2,\cdots,S_n)+I(P_i;K_i|S_1,S_2,\cdots,S_n)=\sum_{j=1}^{n}(H(S_j|S_1,\cdots,S_{j-1})-H(S_j|S_1,\cdots,S_{j-1},P_i))+H(K_i)=nH(K_i)-t_iH(K_i)+H(K_i)=(n-t_i+1)H(K_i)$

定理3 假设各参与者保存的共享相互间随机独立,则对于理想、完备的门限多重秘密共享方案,有$H(P)\geqslant(mn-\sum_{i=1}^{m}t_i+m)H(K)$,其中$P$表示秘密持有者公开的所有信息。

证明:由定理2知$\sum_{i=1}^{m}H(P_i)\geqslant\sum_{i=1}^{m}(n-t_i+1)H(K_i)$,则$H(P)\geqslant(mn-\sum_{i=1}^{m}t_i+m)H(K)$。

在理想、完备的门限多重秘密共享方案中,若$H(P)=$

$(mn-\sum_{i=1}^{m}t_i+m)H(K)$，则称该方案为最优的门限多重秘密共享方案。

4 一种最优的门限多重秘密共享方案

在这部分，我们提出了一种最优的门限多重秘密共享方案。该方案基于 Shamir 秘密共享，包含两个阶段：共享分发阶段和秘密重构阶段。前者由秘密持有者执行，后者由参与者实施。具体描述如下：

共享分发阶段：①随机选取共享 $S_j\in Z_p^*$，$j=1,\cdots,n$（p 是一个大素数），并把 S_j 秘密发送给参与者 j；②独立随机生成秘密 $K_1,K_2,\cdots,K_m\in Z_p^*$，对于每个秘密 K_i，由 $n+1$ 个点 $(0,K_i),(1,S_1),(2,S_2),\cdots,(n,S_n)$ 在域 Z_p 上构造 n 次多项式 $f_i(x)$，计算并公开 $f_i(n+1),f_i(n+2),\cdots,f_i(n-t_i+1)$ for $i=1,\cdots,m$。

秘密重构阶段：任意 t_i 个共享 $S_{j_1},S_{j_2},\cdots,S_{j_{t_i}}$，加上公开信息 $f_i(n+1),f_i(n+2),\cdots,f_i(n-t_i+1)$，得到 $n+1$ 个点 $(j_1,S_{j_1}),\cdots,(j_{t_i},S_{j_{t_i}}),(n+1,f_i(n+1)),\cdots,(n-t_i+1,f_i(n-t_i+1))$，从而可以构造一个 n 次多项式 $h(x)$。若用 $(X_i,Y_i)(i=1,2,\cdots,n+1)$ 依次表示这 $n+1$ 个点，则构造的多项式：

$$h(x)=\sum_{i=1}^{n+1}Y_i\prod_{j=1,j\neq i}^{n+1}\frac{x-X_j}{X_i-X_j}\bmod p$$

计算得到秘密 $K_i=h(0)$。

显然，这是一种多阶段使用的多重秘密共享方案，一次共享过程，可以分享多个秘密，每一阶段根据各自独立的公开信息可以重构一个秘密。以上方案基于 Shamir 秘密共享，因而是一种完备的门限方案；又因为 $|S_j|=|K|$，$j=1,\cdots,n$，所以该方案是理想的；其中公开的信息量为 $(mn-\sum_{i=1}^{m}t_i+m)|K|$，因而该方案是一种最优的门限多重秘密共享方案。

结束语 借鉴完全动态的门限秘密共享方案思想，重新定义了门限多重秘密共享方案，该方案是一种多阶段使用的多重秘密共享方案，一次共享过程可以分享多个秘密，每个秘密对应一个独立的公开信息，每一个重构阶段授权子集中的所有参与者合作，根据相应的公开信息可以恢复一个秘密；接着分析了共享和公开信息的下界，为寻找其它高效的门限多重秘密共享方案提供了理论基础；最后提出了一种最优的门限多重秘密共享方案，该方案基于 Shamir 秘密共享，是一种理想、完备的门限方案，能多阶段地共享多个秘密。其中共享与单个秘密同样大小，公开信息达到最优下界 $(mn-\sum_{i=1}^{m}t_i+m)H(K)$。因而非常有效，有着很好的应用前景。

参 考 文 献

[1] Shamir A. How to share a secret. Communications of the ACM 22,1979:612-613

[2] Blakley G. Safeguarding cryptographic keys // Proc. of the 1979 AFIPS National Computer Conference. AFIPS Press,1979,48:313-317

[3] Ito M,Saito A,Nishizcki T. Secret sharing scheme realizing general access structure// Proc. of IEEE Global Telecommunication Conf. Globecom 87. 1987:99-102

[4] Benaloh J C, Leichter J. Generalized secret sharing and monotone functions // Advances in Cryptology-CRYPTO'88, LNCS 403. 1990:27-35

[5] He J, Dawson E. Multistage secret sharing based on one-way function. Electronics Letters,1994,30 (19):1591-1592

[6] Harn L. Comment: Multistage secret sharing based on one-way function. Electronics Letters,1995,31 (4):262

[7] Harn L. Efficient sharing (broadcasting) of multiple secrets // IEEE Proceedings- Computers and Digital Techniques. 1995,142 (3):237-240

[8] He J,Dawson E. Multisecret-sharing scheme based on one-way function. Electronics Letters,1995,31 (2):93-95

[9] Karnin E D, Greene J W, Hellman M E. On secret sharing system. IEEE Trans. ,1983,IT-29 (1):35-41

[10] Jackson W A,Martin K M,O'keefe C M. Multisecret Threshold Schemes// Advances in Cryptology-CRYPTO'93, LNCS 773. 1994:126-135

[11] Blundo A,Santis A D,Crescenzo G D,et al. Multi-Secret Sharing Schemes // Advances in Cryptology-CRYPTO'94, LNCS 839. 1994:150-163

[12] Karnin E, Greene J, Hellman M. On secret sharing systems. IEEE Transactions on Information Theory,1983,IT-29(1):35-41

[13] Blundo C,Cresti A,Santis A D,et al. Fully dynamic secret sharing schemes // Advances in Cryptology, CRYPTO'93, LNCS 773. 1994:110-125

[14] Harn L, Hwang T, Laih C, et al. Dynamic threshold scheme based on the definition of cross-product in a n-dimensional linear space// Advances in Cryptology, Eurocrypt'89. 1990:286-298

[15] Sun H U, Shieh S P. On dynamic threshold schemes. Information Processing Letters,1994,52(4):201-206

[16] Li Ming-yan, Poovendran R. Disenrollment with Perfect Forward Secrecy in Threshold Schemes. IEEE Transactions on Information Theory,2006,52(4):1676-1682

(上接第 48 页)

[5] Milgram S. The small world problem [J]. Psychol Today, 1967, 2:60-67

[6] Kleinberg J. Navigation in a small-world[J]. Nature,2000: 406

[7] Mahajan R, Castro M, Rowstron A. Controlling the cost of reliability in peer-to-peer overlays[A] // Proceedings of IPTPS 2003[C]. vol. 2735 of Lecture Notes in Computer Science. Springer-Verlag, 2003:21-32

[8] Alima L, El-Ansary S, Brand P, et al. DKS(N,k,f): a family of low communication, scalable and fault-tolerant infrastructures for P2P applications[A]// Proceedings of 3rd IEEE/ACM Int'l Symposium on Cluster Computing and the Grid[C]. 2003: 344-350

[9] Leong B, Liskov B, Demaine E. EpiChord: parallelizing the Chord lookup algorithm with reactive routing state management [A] // Proceedings of the 12th IEEE ICON 2004[C]. Singapore, 2004:270-276

[10] Saroiu S, Gummadi P K, Gribble S D. A measurement study of peer-to-peer file sharing systems[A] // Proceedings of the 2002 Multimedia Computing and Networking (MMCN 2002)[C]. The International Society of Optical Engineering, 2002

[11] 杨峰，李凤霞，余宏亮，等. 一种基于分布式哈希表的混合对等发现算法[J]. 软件学报，2007，18(3)：714-721

[12] 李伟荣，吴国新，李建飞. Small-World 在对等网络中的应用研究[J]. 计算机工程与应用，2006，6：158-161