计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(8):1378~1382, 2007

加权门限秘密共享

黄东平 刘 铎 戴一奇
(清华大学计算机科学与技术系 北京 100084)
(hdping99@tsinghua.org.cn)

Weighted Threshold Secret Sharing

Huang Dongping, Liu Duo, and Dai Yiqi
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract A weighted threshold secret sharing scheme based on modular computation is proposed in this paper. Weights are used to give differential influence to participants. When the sum of weights of the participants is as big as or bigger than the threshold value, they can recover the secret, otherwise they can not. The participants of the previous weighted secret sharing schemes based on decomposition structure have to hold several sub-secrets which have different application circumstances and are very difficult to manage. But the proposed scheme only requires each participant to hold one single sub-secret, which simplifies the management and usage of the sub-secrets, and enables this scheme applicable for the cases where the management convenience is more important. In some cases, the weights and the threshold value could be adjusted to reduce the size of the scheme but still with the same effect compared with the original one. For this purpose, the concept of the equivalence of access structures is suggested, and an algorithm for parameter adjustment based on integer programming is proposed to minimize the threshold.

Key words threshold; weighted threshold; secret sharing; key management; Chinese remainder theorem

摘 要 提出了一种基于模运算的加权的门限秘密共享方案,当参与者的权重之和大于等于门限值时可以恢复秘密,而小于门限值时则不能.目前仅有的关于加权秘密共享方案都是基于分解结构的,其缺点是参与者需要掌握多个子秘密,并且各个子秘密使用场合不相同,管理和使用不太方便.方案中每个参与者只需要保存一个子秘密,简化了密钥管理与使用.该方案适用于强调管理方便性的环境.在某些情况下,还可以调整权重和门限参数来减小问题的规模,但达到的效果跟原来的系统一致,为此,提出了控制结构的等价性的概念,并提出了一种基于整数规划的参数调整算法.

关键词 门限;加权门限;秘密共享;密钥管理;中国剩余定理

中图法分类号 TN918;TP309.2

秘密共享研究如何给共享参与者集合中的每个成员子秘密,使得每个授权子集里的参与者合作通过运算可以恢复秘密,而非授权子集的成员则不可能得到秘密信息. 1979 年 Shamir[1] 和 Blakley[2] 分别基于 Lagrange 插值多项式和射影几何理论提出门限秘密共享方案,又称做阈值秘密共享方案. 其中文献[1]因为实现简单计算代价小而被学者们广泛研究. 文献[3]提出在线秘密共享机制,引入公告牌(NB)发布一些辅助信息. 在之后的方案中,公告牌被大量使用发布信息以支持一些新功能,如用于验证分发者和参与者发布信息的真实性,用于和参与者提供的子密钥合用以恢复秘密. 文献[4-5]等研

收稿日期:2006-11-02;修回日期:2007-02-13
基金项目:国家自然科学基金项目(90304014)

究了将模运算用于秘密共享,提出了基于中国剩余定理的秘密共享方案. 文献[6]讨论了多项式的运算与数的运算,以及 Lagrange 插值多项式与中国剩余定理的相似性. 近年来,研究人员主要针对多秘密共享、防欺骗等方面展开研究[7-8].

以往的研究较少讨论权重问题,但它确有其实际意义. 参与者在机构里可能担任不同角色,相应的他们所具有的发言权也彼此不同,因此需要赋予他们不同的权重,当参与者的权重之和达到门限值时即可恢复秘密. 用 Shamir 的方案[1]可以实现加权秘密共享,但其解决办法是给参与者多个子密钥,这势必给管理和使用带来诸多不便. 文献[9-10]等提出了基于分解结构的加权秘密共享解决方案. 文献[9]只适用于每个最小授权子集基数均为 2 的情形,这显然影响了它的适用范围. 基于分解结构的方案用在门限秘密共享中不方便,它们都需要给参与者一个或多个子秘密,并且在恢复秘密的时候,需要参与者根据授权子集的不同而选择不同的子密钥,管理使用上比文献[1]更不方便.

本文基于中国剩余定理提出一种加权门限秘密共享方案,可以分配给每个参与者不同的权重. 与已有的几个方案不同的是,本方案中,每个参与者只需要保存一个单一的子秘密,从而减轻了密钥管理的代价.

1 预备知识

在(k,n)门限秘密共享方案中,一个秘密被分成 n 份,分别给 n 个参与者,n 个参与者中的任意 k 个合作就可以得到秘密信息,而少于 k 个人却得不到.

定义 1. 加权门限秘密共享方案(k,n,w)表示加权门限秘密共享方案. 其中,k 是门限值,n 是参与者集合 U 的基数,$w:U\to R$ 是一个给每个参与者赋权的函数,本文用 $w_1,w_2,\cdots,w_n$ 表示每个参与者的权重. 对 U 的任意子集 U',如果 $\sum_{u\in U'}w(u)<k$,他们无法恢复秘密,而当 $\sum_{u\in U'}w(u)\geqslant k$ 时,他们能恢复.

定义 2. 加权门限秘密共享方案的等价,对于一个给定的加权门限秘密共享方案(k,n,w),如果存在另一个(k',n,w'),使得对 U 的任意子集 U',$\sum_{u\in U'}w'(u)<k'$ 当且仅当 $\sum_{u\in U'}w(u)<k$,$\sum_{u\in U'}w'(u)\geqslant k'$ 当且仅当 $\sum_{u\in U'}w(u)\geqslant k$,则称$(k',n,w')$是$(k,n,w)$的等价的加权门限秘密共享方案.

定理 1. 中国剩余定理[11]. 设 $p_1,p_2,\cdots,p_k$ 是两两互质的 k 个正整数,$k\geqslant 2$,令 $P=p_1p_2,\cdots,p_k$,$P_i=P/p_i$,$i=1,2,\cdots,k$,则同余方程组

$$\begin{cases} c\equiv r_1 \bmod p_1,\\ c\equiv r_2 \bmod p_2,\\ \quad\square\\ c\equiv r_k \bmod p_k. \end{cases}$$

存在整数解,且解 c 是所有满足下式的整数:

$$c\equiv r_1P_1'P_1+r_2P_2'P_2+\cdots+r_kP_k'P_k \bmod P,$$

其中,$P_i'P_i\equiv 1 \bmod p_i$,$i=1,2,\cdots,k$. 显然该同余方程用欧几里德算法容易求解.

2 方案描述

方案分为参数调整、准备阶段、秘密共享阶段和秘密恢复阶段.

2.1 参数调整

实际问题中的加权模型可能权重并不是整数,比如,一个公司的各个股东占有的股份不一定都是整数,假设他们在共享一个公司秘密时的权重与占有的股份成正比,那么,他们的权重完全可能不是整数.

文献[9]证明了一切非整数权的秘密共享控制结构都可以转化成整数权的结构,但它没有讨论针对一般情形如何优化系统参数以减小问题规模. 如果仅按文献[9]的构造性证明的方法可能会造成一些不必要的计算量. 例如某公司 3 个股东 P_1,P_2 和 P_3 分别占有公司 40%,32.5%和 27.5%的股份. 他们共享一个公司的秘密,要求参与者的股份之和不小于 50% 时可以恢复秘密. 用文献[9]的方法得到的调整后的整数权重都较大,结果不理想. 实际上,可以找到一个权小得多的等价的方案,如一个(2,3)门限方案就能与原来的系统达到一样的效果. 原问题要求任何两个股东的股份之和都不小于 50%,都可以恢复秘密;而(2,3)门限方案刚好可以到达这个效果,问题规模大大减小.

对于不出现在任何最小授权子集里的参与者 U_i,直接赋值其新的权为 0. 对于权大于门限 k 的参与者 U_i,先将其从集合 U 里删除,在后续步骤完成后直接赋值其新的权重为新的门限 k'. 下面讨论除了这两种特殊情况之外的参与者.

设 n 个参与者的权重共有 m 种不同取值 w_1',$w_2',\cdots,w_m'$. 由于秘密共享的控制结构的单调性,

用所有最小授权子集和最大禁止子集就可以描述所有授权情况. 每个最小授权子集 U_l 可以用下式描述:

$$\sum_{i=1}^{m}\lambda_{il}w_i' \geqslant k,$$

其中,λ_{il}表示 U_l 里权重为 w_i' 的参与者数目. 同样,每个最大禁止子集 U_j 也可以用下式描述:

$$\sum_{i=1}^{m}\lambda_{ij}w_i' < k.$$

那么,求解等价方案的过程就成了一个如下的整数规划问题:

$$\begin{aligned}&\min\ z = k'\\ &\text{s.t.}\quad w''_i > 0,\\ &\sum_{i=1}^{m}\lambda_{il}w''_i \geqslant k',\\ &\sum_{i=1}^{m}\lambda_{ij}w''_i < k'.\end{aligned}$$

由文献[9]任意权重的门限秘密方案都能转化成整数权的门限秘密共享方案,该整数规划问题一定有解. 整数规划问题是 NPC 的,不过对于秘密共享这样较小的规模,问题不难求解. 这样处理后的明显优势是每个参与者的权重变小,使得需要保存的信息减少,进而节省计算量.

2.2 准备阶段

秘密分发者选取 $n+1$ 个质数 $p_0,p_1,\cdots,p_n$,且满足 $p_1>2(p_0+1)$,$p_1<p_2<\cdots<p_n<tp_1$,这里 $t=2^{1/(k-1)}$,如此选取 t 的原因将在后面讨论. 这个过程没有必要保密,甚至可以通过查公开的质数表选取. 将 $p_0,p_1,p_2,\cdots,p_n$ 公布在公告牌里.

2.3 秘密的共享

设将要共享的秘密为 s,满足 $0\leqslant s<p_0$. 秘密分发者随机选取整数 s',满足:

1) $p_n^{k-1}<s'<p_1^k$;

2) $s'\equiv s \bmod p_0$.

事实上,由于 $p_n^{k-1}<(tp_1)^{k-1}=2p_1^{k-1}<p_1^k$,且 $p_1^k-p_n^{k-1}>p_1^k-2p_1^{k-1}=(p_1-2)p_1^{k-1}$,满足这两个条件的 s' 总能取到. 分发者计算 $r_i=s' \bmod p_i^{w_i}$,其中 $i=1,2,\cdots,n$,r_i 即为参与者 u_i 的子秘密. 分发者通过安全信道将 r_i 传送给 u_i.

2.4 秘密的恢复

不妨设 $u_1,u_2,\cdots,u_j$ 参与恢复秘密,其权满足 $w_1+w_2+\cdots+w_j\geqslant k$. 他们公布各自的子密钥:$r_1,r_2,\cdots,r_j$.

秘密恢复者利用中国剩余定理求解如下问题:

$$\begin{cases}c\equiv r_1 \bmod p_1^{w_1},\\ c\equiv r_2 \bmod p_2^{w_2},\\ \quad\square\\ c\equiv r_j \bmod p_j^{w_j}.\end{cases}$$

由于 $p_1,p_2,\cdots,p_j$ 都是素数,上述方程组有解,设 s' 为上述方程组在(p_n^{k-1},p_1^k)内的解(事实上,后面定理 2 指明在参与恢复的参与者的权之和不小于门限 k 时,上述方程组在(p_n^{k-1},p_1^k)内的解是惟一存在的). 计算 $s=s' \bmod p_0$,即共享的秘密.

3 方案分析

本节首先通过一个定理讨论方案的正确性和安全性,接下来说明在实际情况下有足够多的质数供选择,最后讨论在参与者的权和大于门限 k 时的处理办法.

定理 2. 选取 $t=2^{1/(k-1)}$ 可以保证本方案的正确性,即使得参与者的权之和小于 k 时无法恢复秘密,而当权之和不小于 k 时能正确恢复.

证明. 1) 当权的和小于 k 时,设由中国剩余定理得到的该同余方程组的解为:

$s''\equiv a \bmod (p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j})$,$0\leqslant a<p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j}$,

因此:

$$s''=a+x(p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j}),$$

其中 x 是整数. 下面通过分析区间长度讨论 x 可能的取值数目不小于

$$(p_1^k-p_n^{k-1})/(p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j}),$$

由于

$$p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j}\leqslant p_n^{k-1}<(tp_1)^{k-1}=2p_1^{k-1},$$

故 x 可能的取值个数不小于

$$(p_1^k-p_n^{k-1})/(p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j})>(p_1-2)p_1^{k-1}/(2p_1^{k-1})=(p_1-2)/2\geqslant p_0,$$

也就是说 x 可以取值某 p_0 个连续的整数值,使得相应 s'' 都是上述同余方程组的解,因而 x 可以是模 p_0 的一个完全剩余系里的任何一个值,由于 $gcd(p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j},p_0)=1$,$s=s'' \bmod p_0$ 的取值相应地构成模 p_0 的另一个完全剩余系[11],即 s 可以取 Z_{p_0} 中的任意整数. 无法恢复秘密.

2) 当权和不小于 k 时,不妨设权和为 m. 根据中国剩余定理,符合该方程组的所有解必然能被表示成 $s''=a+x(p_1^{w_1}p_2^{w_2}\cdots p_j^{w_j})$ 的形式. 由于 $p_1^k\leqslant$

$p_1^m \leqslant p_1^{w_1} p_2^{w_2} \cdots p_j^{w_j}$,在合法区间里 $s'' = a + x(p_1^{w_1} p_2^{w_2} \cdots p_j^{w_j})$最多只能取得惟一正整数,另一方面,$s'$必然是原方程组的一个解,它正好在合法区间里.可见,s'就是该问题惟一的解,也即可以惟一确定 s,可以恢复秘密. 证毕.

由于本方案中需要用到大量素数,下面简单地说明 $t = 2^{1/(k-1)}$的情况下有足够多的质数满足本方案的选择要求.根据素数定理(the prime number heorem)[11],$\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x/\ln x} = 1$,那么 p_1 与 $2^{1/(k-1)} p_1$ 之间的质数个数约为

$$\frac{2^{1/(k-1)} p_1}{\ln(2^{1/(k-1)} p_1)} - \frac{p_1}{\ln p_1} \approx \frac{(2^{1/(k-1)} - 1) p_1}{\ln p_1}.$$

粗略地举例来说明,以 $k = 100$,$p_1 \approx 2^{20}$为例,上式约为 531.实际使用的 p_1 可能大得多,也将有更多的质数可供选择.

下面讨论参与者的权和大于门限 k 时的处理办法.如定理 2 所述,当权之和大于 k 时可以直接用中国剩余定理求解,但如果按如下算法做一些预处理,能避免一些不必要的运算,提高秘密恢复过程的效率.

算法 1. 参与者权和大于门限 k 时的恢复算法.

① 将 j 个参与者按权由大到小排序,设为 u_1,u_2,…,u_j,$w \leftarrow w_1 + w_2 + \cdots + w_j$.

② 如果 $w = k$,跳转到⑤.

③ 如果 $w - w_j \geqslant k$,$w \leftarrow w - w_j$,$j \leftarrow j - 1$,跳转到②.

④ $l \leftarrow w - k$,$w_j \leftarrow w_j - l$,$r_j' \leftarrow r_j \bmod p_j^{w_j - l}$.

⑤ 按参与者权和等于门限的方法恢复秘密.

4 结 论

本文基于中国剩余定理提出一种加权门限秘密共享方案.该方案可以处理任意正整数权的情形,由于任意正实数权重的门限秘密共享问题可以转化成一个正整数权的问题,本文所提方案广泛适用于各种情况.

该方案的信息率不如文献[9-10]的方案高,约为 $\dfrac{1}{\max\ w_i}$.但文献[9-10]的方案分配给每个参与者一个或多个子秘密,并且每个秘密的使用方法不对称,因此用户在实施方案时必须记下子秘密与不同授权子集的对应关系信息,从而使子秘密管理和秘密恢复不方便.在使用便利性比信息率更重要的环境中,本方案将有明显优势.

参 考 文 献

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

[2] G R Blakley. Safeguarding cryptographic keys [C]. In: Proc of National Computer Conference. Montvale, NJ: AFIPS Press, 1979. 313-317

[3] M Stadler. Publicly verifiable secret sharing [C]. In: Proc of Advances in Cryptology—Eurocrypt '96. Berlin: Springer-Verlag, 1996. 190-199

[4] C Asmuth, J Bloom. A modular approach to key safeguarding [J]. IEEE Trans on Information Theory, 1983, 29(2): 208-210

[5] R J Hwang, C C Chang. An improved threshold scheme based on modular arithmetic [J]. Journal of Information Science and Engineering, 1999, 15(5): 691-699

[6] A Aho, J Hopcroft, J Ullman. The Design and Analysis of Computer Algorithms [M]. Reading, MA: Addison-Wesley, 1974

[7] C W Chan, C C Chang. A scheme for threshold multi-secret sharing [J]. Applied Mathematics and Computation, 2005, 166(1): 1-14

[8] T Y Chang, M S Hwang, *et al*. An improvement on the Lin-Wu (t, n) threshold verifiable multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2005, 163(1): 169-178

[9] P Morillo, C Padró, *et al*. Weighted threshold secret sharing schemes [J]. Information Processing Letters, 1999, 70(5): 211-216

[10] H M Sun, B L Chen. Weighted decomposition construction for perfect secret sharing schemes [J]. Computers and Mathematics with Applications, 2002, 43(6/7): 877-887

[11] K H Rosen. Elementary Number Theory and Its Applications, Fourth Edition [M]. Reading, MA: Addison-Wesley, 2000

Huang Dongping, born in 1977. Ph. D. His main research interests include network security and algorithm design and analysis.

黄东平,1977 年生,博士,主要研究方向为信息安全、算法设计与分析.

Liu Duo, born in 1978. Ph. D. His current research interests include elliptic curve cryptology, combinational algorithm, *etc*.

刘 铎,1978 年生,博士,主要研究方向为密码学、组合算法的设计与分析.

Dai Yiqi, born in 1947. Professor and Ph. D. supervisor in the Department of Computer Science and Technology, Tsinghua University. His main research interests include cryptology, combinational algorithm and network security.

戴一奇,1946 年生,教授,博士生导师,主要研究方向为信息安全、密码学、组合算法和网络安全.

Research Background

Over the recent years, secret sharing technologies, as an important utility for key management, have been receiving a great deal of research effort. Weighted threshold secret sharing is a special case of secret sharing. If and only if the sum of weights of the participants isn't less than the threshold value, they can recover the secret.

We propose a solution to reduce the scale of the weighted secret sharing by establishing integer programming problem exploiting the equivalence relation of access structure, and a new weighted threshold secret sharing scheme based on modular computation is proposed in this paper. The new scheme only requires each participant to hold one single sub-secret, which simplifies the management and using of the sub-secrets, and enables this scheme applicable for the cases where the management convenience is more important.

附录 A

在此给一个例子以说明本方案:设 $n=3, k=3$,参与者的权重分别为:$w_1=2, w_2=1, w_3=2, w_4=1$. 此时可选取系统参数为:$p_0=19, p_1=41, p_2=43, p_3=47, p_4=53$(满足 $p_4/p_1>2^{1/(3-1)}=\sqrt{2}$). 设需要共享的秘密为 $s=17$.

在 $p_n^{k-1}=p_4^2=2809$ 和 $p_1^k=p_1^3=68921$ 之间任意选取满足 $s'\equiv s \bmod p_0$,我们选取 $s'=65548$,那么 $r_1=1670, r_2=16, r_3=1487, r_4=40$. 下面分析恢复秘密时的几种可能情形.

1) 参与者的权和正好等于 k:以 u_1 和 u_2 合作为例. 利用欧几里得算法,求得 $P_1'=1251, P_2'=11$,由中国剩余定理解方程组得 $s'=65548$,进而可恢复 $s=17$.

2) 参与者的权和小于 k:以 u_1 单独恢复秘密为例. 他只能知道 s'为区间(2809, 68921)里能表示成 $s'=1681x+1670$ 的整数皆有可能,其中 x 为整数,无法确定 s'的具体取值. 实际上这种情况下 s' 可以取 3351, 5032, 6713, 8394, 10075, 11756, 13437, 15118, 16799, 18480, 20161, 21842, 23523, 25204, 26885, 28566, 30247, 31928, 33609, 35290, 36971, 38652, 40333, 42014, 43695, 45376, 47057, 48738, 50419, 52100, 53781, 55462, 57143, 58824, 60505, 62186, 63867, 65548, 67229, 68910. 相应的, s 的可能取值序列为:7, 16, 6, 15, 5, 14, 4, 13, 3, 12, 2, 11, 1, 10, 0, 9, 18, 8, 17, 7, 16, 6, 15, 5, 14, 4, 13, 3, 12, 2, 11, 1, 10, 0, 9, 18, 8, 17, 7, 16. 可见为[0, 18]之间的整数均有可能,U_1 无法得到 s.

3) 参与者的权和大于 k:以 u_1 和 u_3 恢复秘密为例. 将 $w_1'=1$ 和 $r_1'=30$ 用于计算,$P_1'=8, P_3'=1778$. 同样得到 $s'=65548, s=17$.