一个安全高效的门限多重秘密共享方案*)

庞辽军　王育民

(西安电子科技大学综合业务网国家重点实验室　西安 710071)

摘　要　秘密共享在信息安全和数据保密中起着重要的作用。本文基于 Shamir 的门限方案提出一个新的(t, n)多重秘密共享方案，p 个秘密被 n 个参与者所共享，至少 t 个参与者联合可以一次性重构这 p 个秘密，而且参与者秘密份额长度与每个秘密长度相同。与现有方案比较，该方案具有秘密重构计算复杂度低，所需公共信息量小的优点。方案的安全性是基于 Shamir 的门限方案的安全性。分析表明本文的方案是一个安全、有效的方案。

关键词　信息安全，秘密共享，多重秘密共享，门限方案

A Secure and Efficient Threshold Multi-secret Sharing Scheme

PANG Liao-Jun　WANG Yu-Min

(National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　Secret sharing plays an important role in information security and data privacy. Based on Shamir's threshold scheme, a new (t, n) multi-secret sharing scheme is proposed in this paper. In this scheme, there are p secrets shared among n participants and at least t or more participants can easily reconstruct these p secrets at the same time. Each participant's secret shadow is as short as each secret. Compared with the existing schemes, the proposed scheme is characterized by the lower complexity of the secret reconstruction and less public information. The security of this scheme is the same as that of Shamir's threshold scheme. Analyses show that this scheme is a secure and efficient scheme.

Keywords　Information security, Secret sharing, Multi-secret sharing, Threshold scheme

秘密共享是信息安全和数据保密中的重要手段，它在重要信息和秘密数据的安全保存、传输及合法利用中起着非常关键的作用；它也是密码学和分布式计算领域中一个非常重要的研究内容。(t, n)门限秘密共享方案是由 Shamir[1] 和 Blakley[2] 在 1979 年分别基于 Lagrange 插值法和多维空间点的性质提出的。一个秘密被 n 个参与者所共享，至少 t 个参与者联合可以重构该秘密；而 $t-1$ 个或更少的参与者不能得到该秘密的任何信息。除了 Shamir 和 Blakey 的方案外，还有基于中国剩余定理的 Asmuth-Bloom 法[3] 以及使用矩阵乘法的 Karnin-Greene-Hellman 方法[4] 等。其共同缺点是一个秘密被重构后，秘密分发者必须重新分配各参与者的秘密份额。基于这个原因，(t, n)多重秘密共享方案文[5,6]被提出。在多重方案中，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。在秘密重构过程中，合作的参与者只需提交一个由秘密份额计算得到的伪份额而并非提交真正的秘密份额，一个秘密的重构不会披露各参与者所拥有的秘密份额，也不会影响其它未重构秘密的安全性。

Chien 等人[7] 在 2000 年基于系统分组码(Systematic block codes)提出了一种新的(t, n)门限多重秘密共享方案，与方案文[5, 6]等所不同的是，p 个秘密可以在一次秘密重构过程中同时得到，而且在一次共享过程中，秘密分发者仅需公布$(n+p-t+1)$个信息。这个方案有非常重要的应用价值，尤其是在共享大的秘密时比其它的方案更为方便[8]，但是在重构秘密时，需要进行解方程组的运算，因而效率不高。2004 年，Yang 等人[8] 基于 Shamir 的秘密共享方案给出了另一个实现，其秘密的重构计算要比 Chien 的方案简单，因为构造 Lagrange 插值多项式比解方程组容易[8]。在 Ynag 的方案中，当 $p>t$ 时，需要公布$(n+p-t+1)$个信息；当 $p\leqslant t$ 时需要公布$(n+1)$个公共信息。很明显，当 $p<t$ 时 Yang 的方案要比 Chien 的方案需要公布的公共信息多，尤其当 $p=1$ 和 $t=n$ 时，Chien 的方案只需要公布 2 个公共信息，而 Yang 的方案仍需要公布$(n+1)$个信息，这是 Yang 的方案的不足之处。因为公共信息量的大小是决定一个方案性能优劣的重要参数之一，影响着方案中的存储和通信的复杂度[9]。

本文基于 Shamir 的秘密共享方案，提出了一个新的(t, n)多重秘密共享方案，其秘密的重构计算比 Yang 的方案一要简单，而所需公布的公共信息量与 Chien 的方案相同。有关 Chien 的方案和 Yang 的方案的细节可以阅读文[7, 8]，限于篇幅，这里不再赘述。下面，首先给出本文所提出的方案，然后对其安全性和性能进行分析，最后对这三种方案进行比较分析并给出结论。

1　本文提出的新方案

1.1　相关技术

在描述本文方案之前，首先需要给出一个双变量单向函数 $f(r, s)$的定义，在 Chien 的方案、Yang 的方案以及本文的方案中都使用了这个函数。

定义 1[7]　双变量单向函数。$f(r, s)$表示一个有两个变

*)基金项目：973 国家重大项目资助(G19990358-04)。**庞辽军**　博士生，主要研究方向为电子商务中的安全理论与技术；**王育民**　博士生导师，主要研究方向为信息论，密码，编码。

量的单向函数，能够将任意长的 r 和 s 映射为固定长的函数值 $f(r, s)$。

该函数具有以下性质[8]：(1)已知 r 和 s，$f(r, s)$易于计算；(2)已知 s 和 $f(r, s)$，求 r 在计算上是不可行的；(3)在 s 未知的情况下，对于任意的 r，难以计算 $f(r, s)$；(4)已知 s 的情况下，找到不同的 r_1 和 r_2 满足 $f(r_1, s)=f(r_2, s)$是不可行的；(5)已知 r 和 $f(r, s)$，求 s 在计算上是不可行的；(6)已知任意多的$(r_i, f(r_i, s))$对，求 $f(r', s)$是不可行的，其中 $r' \neq r_i$。

1.2 方案构成

本文提出的方案跟 Yang 的方案一样，是基于 Lagrange 插值多项式的。下面从三个方面进行描述：

(1)系统参数：单向函数 $f(r, s)$，其定义与 Chien 的方案以及 Yang 的方案中的 $f(r, s)$定义相同；q 为一大素数；系统工作在有限域 $GF(q)$上，系统中所有的参数都是 $GF(q)$的元素；可信的秘密分发者随机选择 n 个整数 $s_1, s_2, \cdots, s_n$ 分别作为 n 个参与者的秘密份额，并从$[p, q-1]$中选取 n 个随机数 $u_1, u_2, \cdots, u_n$ 分别作为 n 个参与者的公开身份信息。

这里，我们用 $P_1, P_2, \cdots, P_p$ 表示 p 个秘密。

(2)秘密分发：可信的秘密分发者执行以下步骤完成秘密的分发。

a. 随机选取一个整数 r，对所有的 $s_i(i=1,2,\cdots,n)$计算 $f(r, s_i)$；

b. 根据$(n+p)$个数值对$(0, P_1), (1, P_2), \cdots, (p-1, P_p)$以及$(u_i, f(r, s_i))$，$i=1,2,\cdots,n$ 构造$(n+p-1)$次 Lagrange 插值多项式[1] $h(x)=a_0+a_1x+\cdots+a_{n+p-1}x^{n+p-1}$；

c. 从集合$[p, q-1]-\{u_i \mid i=1,2,\cdots,n\}$中取出最小的 $n+p-t$ 个整数 $d_1, d_2, \cdots, d_{n+p-t}$，并分别计算函数值 $h(d_i)$，$i=1,2,\cdots, n+p-t$；

d. 以认证的方式[10]公布 $(r, h(d_1), h(d_2), \cdots, h(d_{n+p-t}))$。

(3)秘密重构：为了重构这 p 个秘密，需要至少 t 个参与者成交其伪份额 $f(r, s_i)$，$i=1', 2', \cdots, t'$。有了这 t 个份额，可以构成 t 个数值对$(u_i, f(r, s_i))$，$i=1', 2', \cdots, t'$。这时，再以同样的方法从集合$[p, q-1]-\{u_i \mid i=1,2,\cdots,n\}$中取出最小的 $n+p-t$ 个整数 $d_1, d_2, \cdots, d_{n+p-t}$，并利用所公布的信息 $h(d_1), h(d_2), \cdots, h(d_{n+p-t})$，构成 $n+p-t$ 个数值对$(d_i, h(d_i))$，$i=1,2,\cdots, n+p-t$。如果用(X_i, Y_i) $i=1, 2, \cdots, n+p$ 分别表示所得到了这$(n+p)$个数值对，就可以将所重构的$(n+p-1)$次 Lagrange 插值多项式[1]$h(x)$表示如下：

$$h(x)=\sum_{i=1}^{n+t} Y_i \prod_{j=1, j\neq i}^{n+t} \frac{x-X_j}{X_i-X_j}=a_0+a_1x+\cdots+a_{n+p-1}x^{n+p-1}$$

这时，p 个秘密 $P_1, P_2, \cdots, P_p$ 就可以得到了，其中 $P_i=h(i-1)$，$i=1,2,\cdots,p$。

要说明的是，以上计算均在模 p 条件下进行。

1.3 骗子的揭发

在秘密共享方案中，如何发现存在欺骗以及指出骗子非常重要。许多研究人员对这一方面做了大量的研究，读者可以参考文[11]。因此本文不再重复给出相关的讨论。但是，为了使得在欺骗验证过程中能够保护参与者的秘密份额不被泄露，有一点需要指出：秘密分发者在构造用于进行欺骗验证的公共信息时，应当使用各参与者的伪份额 $f(r, s_i)$，而不应当直接使用其秘密份额 s_i；同样，验证者能够使用各参与者的伪份额 $f(r, s_i)$进行验证，而不需要知道其秘密份额 s_i。这样，即使每个参与者都给出自己的伪份额 $f(r, s_i)$进行欺骗验证，由单向函数 $f(r, s)$的性质可知，他的秘密份额 s_i 却不会被披露。

2 安全性和性能分析

2.1 安全性分析

方案的安全性可以从以下方面分析：

1)尽管公布了$(n+p-1)$次多项式 $h(x)$的 $n+p-t$ 个函数值$h(d_i)$，$i=1,2,\cdots,n+1-t$，但是攻击者不会得到 $h(x)$，因此就得不到秘密的任何信息。这是因为 $h(x)$的构造需要 $n+p$ 个不同的数值对。使用少于 $n+p$ 个数值对成功地构造 $h(x)$等价于攻破了 Shamir 的秘密共享方案。

2)如果少于 t 个参与者进行秘密的重构计算，他们仍旧不能构造出多项式 $h(x)$，原因同 1)。而当 t 个或 t 个以上的参与者合作，便能确定唯一的多项式 $h(x)$。因此，本文所提出的方案是一个(t, n)门限秘密共享方案。

3)秘密的重构过程不会披露各参与者的秘密份额。即使 n 个伪份额 $f(r, s_i)$被披露，由单向函数 $f(r,s)$的性质可知，任何参与者秘密份额 s_i 都不会被披露。而且每一次的秘密重构过程都不会影响下一次秘密共享所对应的伪份额的安全性。因此，在下一次共享过程中，秘密分发者不需要重新分配秘密份额 s_i，只需重新选取一个随机整数 r。

通过以上分析，可以看出本文所提出的方案也是一个(t, n)多重秘密共享方案，具有和 Chien 的方案以及 Yang 的方案相同的优点：(1)允许并行地恢复多个秘密，可以一次性重构 $p(p\geqslant 1)$各秘密；(2)秘密的分发者可以动态地决定本次所要共享的秘密的数量；(3)可以多次用来进行秘密共享而不必重新分配各参与者的秘密份额。

2.2 性能分析

本小节讨论方案的性能。很明显，该方案中最耗时的操作为多项式插值计算和模指数运算，方案性能的提高主要取决于如何有效地进行多项式插值运算和模指数运算。许多文献已经对这两个问题分别进行了研究，并取得了许多成果。例如：在文[12]中给出了多项式插值计算的有效方法，其算法复杂度为 $O(n\log^2 n)$；在文[13,14]中也给出了若干快速模指数运算的方法。这些方法的使用必将提高本文方案的性能，因此，可以说本文的方案是非常有效的，而且容易实现。

3 三种方案的比较

下面，我们分别从秘密重构的计算复杂度和需要公布的公共信息量来对 Chien 的方案、Yang 的方案以及本文所提出的方案加以比较。

首先，从秘密构建的计算复杂度来看，本文的方案比 Yang 的方案更为简单，因为在 Yang 的方案中，秘密的分发及其重构需要区分两种不同的情况，$p\leqslant t$ 和 $p>t$，并进行不同的处理，这也使得 Yang 的方案比本文的方案更复杂。而在 Chien 的方案中，秘密的重构是通过解 $n+p-t$ 元方程组来完成的，而解方程组要比构造 Lagrange 插值多项式复杂得多[8]。因此，本文的方案的秘密重构计算的复杂度比 Chien 的方案和 Yang 的小，是目前最为有效的方案。

公共信息量的大小是决定一个方案性能的重要参数，影响着方案中的存储和通信的复杂度。从需要公布的公共信息量来看，本文的方案和 Chien 的方案比 Yang 的方案更优越。为了共享 p 个秘密 $P_1, P_2, \cdots, P_p$，本文的方案和 Chien 的

方案需要公布($n+p-t+1$)个信息;而对于 Yang 的方案,当 $p>t$ 时,需要公布($n+p-t+1$)个信息,但是当 $p\leqslant t$ 时需要公布($n+1$)个公共信息。很明显,当 $p<t$ 时,本文的方案和 Chien 的方案需要公布的信息量小于 Yang 的方案需要公布的信息量。尤其当 $p=1$ 和 $t=n$ 时,本文的方案和 Chien 的方案只需要公布 2 个公共信息,而 Yang 的方案仍需要公布 $n+1$ 个信息,这也是本文方案最为吸引人的地方之一。

通过以上分析,可以发现:Chien 的方案的优点是需要公布的信息量小,而缺点是秘密重构的计算复杂度大;Yang 的方案的优点是秘密构建的计算复杂小,而缺点是需要公布的信息量大,而且需要区分两种不同的情况并给以不同的实现。本文的方案正好综合了这两个的方案的优点,而避免了它们的缺点,因而是一个很有效的门限多重秘密共享方案。

结论 本文基于 Shamir 的秘密共享方案,提出了一个 (t,n) 多重秘密共享方案,一组秘密被 n 个参与者所共享,t 个或 t 个以上的参与者联合可一次性重构这些秘密,而少于 t 个参与者合作得不到秘密的任何信息。在每次秘密分发过程中,秘密分发者只需重新选取一个随机整数 r,而不必重新分配各参与者的秘密份额。比起 Chien 的方案,其秘密重构计算简单;比起 Yang 的方案,需要公布的公共信息量少且实现单一。安全性和性能分析表明,本文的方案是一个安全、有效的方案。

参 考 文 献

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

2 Blakley G. Safeguarding cryptographic keys [A]. In: Proc. AFIPS 1979 Natl. Conf. [C], New York, 1979. 313~317

3 Asmuth C, Bloom J. A Modular approach to key safegrarding [J]. IEEE Transactions on Information Theory, 1983, 29:208~210

4 Karnin E D, Green J W, Hellman M E. On sharing secret system [J]. IEEE Transactions on Information Theory, 1983, 29:35~41

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

6 Harn L. Efficient sharing (broadcasting) of multiple secret [J]. IEE Proceedings-Computers and Digital Techniques, 1995, 142 (3):237~240

7 Chien H-Y, Jan J-K, Tseng Y-M. A practical (t, n) multi-secret sharing scheme [J]. IEICE Transactions on Fundamentals, 2000,E83-A (12):2762~2765

8 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

9 Crescenzo G D. Sharing one secret vs. sharing many secrets: Tight Bounds on the average improvement ratio [J]. Theoretical Computer Science,2003,295(1-3):123~140

10 ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions on Information Theory, 1985,IT-31:469~472

11 Tan K J, Zhu H-W, Gu S J. Cheater identification in (t, n) threshold scheme [J]. Computer Communications, 1999,22:762~765

12 Rosen K H. Elementary Number Theory and Its Applications [M]. Addison-Wesley, MA, 1993

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

14 Chang C C, Horug H J, Buehrer D J. A cascade exponentiation evaluation scheme based on the Lempel-Ziv-Welch compression algorithm [J]. Journal of Information Science and Engineering, 1995,11(3):417~431

(上接第 59 页)

须对文件是否进行过压缩进行判断,否则反而会增加数据传输的时间。

结论及未来工作 基于网格服务的数据传输具跨越防火墙进行数据传输的能力,是一种完整的跨异构平台进行数据传输的方式。采用数据压缩、并行数据传输和缓冲区调整机制可以提高这种传输方式的传输效率。本文提出的基于传输日志机制的故障恢复机制又提高了这种方式进行数据传输的可靠性。虽然在传输效率上这种方式与现有的 GridFTP 仍然有一定的差距,但是在需要跨防火墙进行数据传输的网格应用中,这种方式比 GridFTP 具有更强的适用范围。目前影响这种传输方式性能的关键因素在于二进制转化为字符过程中所增加的数据量。这是由于 SOAP 无法直接表示二进制所造成的。为了解决这一问题,国外已经展开了相应的研究工作。例如 SUN 的 Fast Infoset 项目[12],W3C 在 2005 年 1 月 25 日发布的 XOP(XML-binary Optimized Packaging)[13]、SOAP MTOM(SOAP Message Transmission Optimization Mechanism)[14]、RRSHB(Resource Representation SOAP Header Block)[15]规范。以及采用二进制方式传输 Web 服务消息的 Hessian 二进制 Web 服务协议(Hessian Binary Web Service Protocol)[16]。当前这些研究还处于起步阶段,未来的研究工作需要结合这些相关研究,将其应用到网格领域,彻底地解决基于网格服务进行数据传输所存在的效率问题。

参 考 文 献

1 Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations [J]. Supercomputer Applications, 2001

2 Allcock B, Bester B, Bresnahan J, et al. Secure, Efficient Data Transport and Replica Management for High-Performance Data-Intensive Computing [J]. IEEE Mass Storage Conference, 2001

3 Mandrichenko I. GridFTP Protocol Improvements [S]. GridFTP WG, 2003

4 Kesselman F C, Nick J, Tuecke S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration [J]. Ope Grid Service Infrastructure WG, Global Grid Forum, 2002

5 Czajkowski T K, Foster I, Frey J, et al. Open Grid Services Infrastructure (OGSI) Version 1. 0 [S]. Global Grid Forum Draft Recommendation, 2003

6 Simple Object Access Protocol [EB/OL]. http://www. w3. org/TR/soap/, 2005-03-05

7 Globus project [EB/OL]. http://www. globus. org/,2005-03-05

8 Web Service [EB/OL]. http://www. w3. org/2002/ws/, 2005-03-05

9 Extensible Markup Language [EB/OL]. http://www. w3. org/XML/,2005-03-05

10 Josefsson S. The Base16, Base32 and Base64 Data Encodings [S]. RFC 3548, 2003

11 Deutsch P. GZIP file format specification version 4. 3 [S]. RFC 1952, 1996

12 Fast Infoset [EB/OL]. http://java. sun. com/developer/technicalArticles/xml/fastinfoset/

13 Gudgin M, Mendelsohn N, Nottingham M, Ruellan H. XML-binary Optimized Packaging [S]. W3C Recommendation, 2005

14 Gudgin M, Mendelsohn N, Nottingham M, Ruellan H. SOAP Message Transmission Optimization Mechanism [S]. W3C Recommendation, 2005

15 Karmarkar A, Gudgin M, Lafon Y. Resource Representation SOAP Header Block [S]. W3C Recommendation, 2005

16 Hessian Binary Web Service Protocol [EB/OL]. http://www. caucho. com/hessian/