具有前向安全性质的秘密共享方案

王彩芬 刘军龙 贾爱库 于成尊
(西北师范大学数学与信息科学学院 兰州 730070)

摘 要 由于已有的秘密共享方案都不具有前向安全的性质，该文基于有限域上离散对数难解问题和强 RSA 假设，应用前向安全理论和已有的秘密共享方案特别是 Boyd 提出的乘法门限方案的思想，提出了一种具有前向安全特性的秘密共享方案。该方案具有子密的可验证性，能够检测伪子密，防止欺诈者；具有子密更新简便及更新后的子密的可验证性；具有秘密恢复快捷且能直接恢复时间周期 j 的秘密信息及检测恢复得到的秘密信息是否正确等功效。该文同时还对方案的安全性进行了分析。

关键词 秘密共享，前向安全，离散对数，强 RSA 假设
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)09-1714-03

A Forward Secure Secret Sharing

Wang Cai-fen Liu Jun-long Jia Ai-ku Yu Cheng-zun
(*College of Mathematics and Information Science, Northwest Normal University, Lanzhou* 730070, *China*)

Abstract As prior secret sharing can not provide forward-secure. So in this paper a forward secure secret sharing scheme is proposed to achieve security against cheating participants by using multiplicative threshold scheme of Boyd, based on discrete logarithms and the strong –RSA assumption. In the scheme participants can update and verify the shares. Security of the scheme is provided under the strong –RSA assumption and discrete logarithms.

Key words Secret sharing, Forward secure, Discrete logarithms, Strong –RSA assumption

1 引言

秘密共享是密钥管理的一个重大研究课题，也是密码技术中一个重要的研究方向。尤其是随着计算机网络技术的迅速发展，现在使用电子的方式存储重要档案和通信已经越来越普遍了，随之对各种密钥的管理也就成了一个必须解决的迫切问题。因此无论在理论上还是实践中，秘密共享对计算机及网络的安全保密均具有重要的意义。秘密共享是指将一个秘密信息在一组参与者的集合中进行分配，由他们共同分享，使该集合中的每个合格的子集都能恢复秘密的一种方式。自从 1979 年Blakley[1]和Shamir[2]分别提出了秘密共享体制以来，有关秘密共享问题的研究受到了广泛的关注。

在密钥管理过程中，密钥存在被动的和主动的泄漏问题，密钥的被动泄漏，意味着攻击者通过各种手段非法窃取密钥；而密钥的主动泄漏，则意味着密钥持有者自己把密钥暴露给其他人。若密钥是被动泄漏的，攻击者可以伪造签名、加密的密文等；若密钥是主动泄漏的，密钥持有者可以以此逃避承担必要的责任，如抵赖曾经发生的行为等。如何减少由于密钥泄漏所带来的对系统安全的影响，一直是人们十分关注的问题。1997 年，Anderson 首次提出了前向安全的理论[3]，它可以有效地减少由于密钥泄漏所带来的对系统安全的影响。1999 年Bellare 提出了前向安全的数字签名方案[4]，它是一种特殊的数字签名，它的公开钥是固定的，而秘密钥则随着时段的进化而更新，这样即使当前时段的密钥泄漏，攻击者也不能伪造与过去时段有关的数字签名，从而可以减少因签名密钥泄漏带来的损失。随后前向安全的理论便被广泛应用[5, 6]。

由于已有的秘密共享方案都不具有前向安全的性质，本文提出了基于离散对数的具有前向安全性质的秘密共享方案，该方案是可以防止欺诈的和可验证的，并且具有子密更新简便、秘密恢复快捷等特点。本文的组织结构如下：第 2 节概述前向安全的理论；第 3 节阐述秘密共享体制；第 4 节提出前向安全的秘密共享体制；第 5 节证明方案的正确性和安全性；第 6 节为结束语，概括全文。

2 前向安全的理论

前向安全的一个重要步骤是密钥的更新。系统建立的初期，用户首先得到公钥PK，并保密相应的密钥SK_0。将公钥的有效期划分为T个时间段，记为 1, 2,…,T 。在有效期内公钥保持不变，但是秘密钥随着时段逐步被更新，以SK_i表示i时间段的秘密钥，进入i时间段时，首先计算$SK_i=f(SK_{i-1})$，其中f是单向函数，秘密钥的更新过程如图 1 所示：

求出SK_i后，立即删除SK_{i-1}，这样当攻击者在i时间段内获得SK_i但是不能获得SK_0，SK_1,…, SK_{i-1}。

2005-02-28 收到, 2005-09-12 改回
甘肃省自然科学基金项目(3ZS051-A25-042)和西北师范大学网络安全重点学科基金项目资助课题

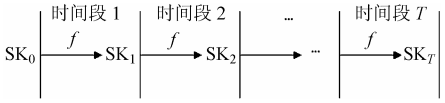

图 1　密钥更新过程

Fig.1 Secret key update

3　秘密共享方案

自从 1979 年Blakley[1]和Shamir[2]分别提出了秘密共享体制以来，已有各种各样的秘密共享方案被提出和设计，如(*t*,*n*)门限的[2]、动态的[7]、具有层次的门限的[8]、在线的[8]等适用不同应用背景下的方案。一般来说，秘密共享方案将一个秘密在一组参与者中进行分配，因此在进行分配之前首先要确定接入结构，之后要确定秘密的分配方法。在已有的秘密共享方案中，有的需要使用可信的分配者，有的不需要可信分配者参与。为了保证每个参与者得到的子密是正确的，在文献[10]中提出了VSS方案，在文献[11]中进一步提出了可公开验证的秘密共享方案PVSS。在恢复阶段为了能恢复出正确的秘密，必须保证每个参与者提供的子密是正确的，防止参与者的欺骗。

随着前向安全理论被广泛应用，如何将随着时间周期变化而改变的密钥进行共享成为迫切需要解决的问题。基于离散对数问题、前向安全理论和已有的秘密共享方案特别是Boyd提出的乘法门限方案的思想[12]。本文提出具有前向安全性质的秘密共享方案，该方案具有子密的可验证性，更新后的子密的可验证性，并且可以检测试图欺骗的参与者，也可以直接恢复时间周期j 的秘密信息。

4　前向安全的秘密共享方案

4.1 定义

前向安全的秘密共享方案是具有前向安全性质的、由如下 3 个算法组成的三元组(secret-share， subsecret-update, secert-recovery)，其中 secret-share 算法是对输入的参数(包括时间周期、秘密信息等)产生初始的 t 个子密；subsecret-update 是密钥更新算法，它的输入包括当前的周期 j 和当前的子密，每个参与者产生 j+1 时间周期的子密，之后将周期 j 的子密销毁；secert -recovery 是指在必要的时候(某个周期)t 个参与者一起合作出示各自的子密共同恢复出秘密信息。秘密共享方案具有前向安全性质是指在秘密共享过程中存在一个单向子密更新算法，使得参与者可以在第 i 时间段内将子密更新，并在不同的时期内使用不同的子密，在某个指定的周期可以恢复相应的秘密信息。

4.2　前向安全的秘密共享方案

4.2.1 *系统中的记号及参数*　P 为参与者的集合，$P_i \in P$，$1 \le i \le t$；D 为秘密分配者，$D \notin P$；Γ 为接入结构($\Gamma \in 2^{|P|}$)；α为要分享的秘密；　T 为时间周期。

系统参数　设 n 是一个大素数，p_1, p_2 是 $n-1$ 的两个大的素因子且满足 $p_1 \equiv 3 \bmod 4$，$p_2 \equiv 3 \bmod 4$，　g 是一个阶为 $q = p_1 p_2$ 的元素($g^q \equiv 1 \bmod n$)。

4.2.2 Secret-Share(*秘密分配*)　可信的秘密分配者 D 随机选择　$S_i \in_R Z_{n-1}^*$, i=1,2 ,⋯, t − 1 计算 $S_t = \alpha (S_1 S_2 \cdots S_{t-1})^{-1} \cdot \bmod (n-1)$，和 $S = g^{\alpha^{2^{T+1}}} \bmod n$，然后 D 公布 S 和 $\mathrm{SP}_i = S_i^{2^{T+1}} \bmod (n-1)$，并通过安全渠道将 S_i 发送给 P_i。

4.2.3 *子密的验证*　P_i 对收到的 S_i 以及D公布的S和 SP_i，验证 $\mathrm{SP}_i = S_i^{2^{T+1}} \bmod (n-1)$，以及 $S = g^{(\mathrm{SP}_1 \mathrm{SP}_2 \cdots \mathrm{SP}_t)} \bmod n$，$1 \le i \le t$ 是否成立，若成立则接受(S_i，SP_i)为有效的子密。

4.2.4 Subsecret-Update (*子密更新*)　在周期 j，子密持有者通过非交互的方式更新 $S_{ij} = S_{i(j-1)}^2 \bmod (n-1)$，$1 \le i \le t$，然后，将 $S_{i(j-1)}$ 删除。

4.2.5 Secert -Recovery(*秘密恢复*)　当需要使用共享的秘密信息时，t个参与者可以一起合作恢复秘密信息。假设在周期j，$P_1, P_2, \cdots, P_t$合作，利用它们所保管的t个子密通过下式可以一起恢复该时间段的秘密，$s_j = \alpha^{2^j} = S_{1j} S_{2j} \cdots S_{tj}$，并通过 $g^{s_j^{2^{T+1-j}}} = S$ 是否成立检验恢复的第 j个周期的秘密s_j是否正确。

4.2.6 *欺诈者的检测*　当需要恢复共享的秘密时，t个参与者中可能存在欺诈者，其中欺诈者出示假的子密以阻止共享的秘密信息α的正确恢复。在上述方案中可以通过 $S_{ij}^{2^{T+1-j}} = \mathrm{SP}_i$ 检测试图欺骗的参与者，若该式不成立，则说明P_i试图提供错误的子密。

5　安全性分析

定理 1　上述前向安全的秘密共享方案是有效的。

证明　子密的分配以及利用子密恢复秘密信息的算法是正确的。对欺诈者的检测算法，如果在周期j，P_i是出示真正子密的合法的参与者，则必定满足 $S_{ij}^{2^{T+1-j}} = \mathrm{SP}_i$。因此我们的方案是正确的。

定理 2　上述前向安全的秘密共享方案具有前向安全的性质。

上述前向安全的秘密共享方案基于强RSA 假设[13]，即已知n ,$\alpha \in Z_n^*$，n是两个大素数的乘积，则找出一个 $\lambda \in Z_n^*$，满足 $\lambda^\gamma \equiv \alpha \bmod n$　(γ>1)是一个非常困难的问题。

证明　上述前向安全的性质应该体现在两个方面：一是秘密共享体制的参与者所持有子密的前向安全性；另一个是秘密信息的前向安全性。

当攻击者得到秘密共享方案中某个参与者在j周期的子密 S_{ij}，试图通过 $S_{ij} = S_{ij-1}^2 \bmod (n-1)$ 计算S_{ik}，$k = 1, 2, \cdots, j-1$，因为提出的方案是基于强RSA 假设的，所以攻击者无法通过S_{ij}得到 $k < j$ 时间段的子密。同理，如果攻击者得到秘密共享方案中在j周期的秘密 $\mathrm{SE}_j = \alpha^{2^j} \bmod (n-1)$，试图通过 $\mathrm{SE}_j = \mathrm{SE}_{j-1}^2 \bmod (n-1)$ 计算SE_k，$k = 1, 2, \cdots, j-1$ 也是不可行的。

定理 3　上述秘密共享方案，是可以防止欺诈者的。

证明　由方案中提出的防止欺诈的算法可知，如果欺诈

者P_i改S_i为 S_i',则它必须计算 $\mathrm{SP}_i = S_i'^{2^{T+1}} \bmod(n-1)$，因为提出的方案是基于强RSA 假设的，故对$S_i$的伪造是不可行的。

定理 4 上述秘密共享方案，攻击者试图直接得到秘密α等价于解离散对数问题。

证明 由方案中提出的算法可知，如果攻击者试图从 S 直接计算α，则它必须计算 $S = g^{\alpha^{2^{T+1}}} \bmod n$，这等价于求解离散对数问题。

6 结束语

秘密共享方案无论在理论上还是实践中都具有重要的价值。目前的秘密共享方案都不具备前向安全的性质，这样当密钥泄漏(主动的和被动的泄漏)以后，若密钥在被动泄漏的情况下，则不能有效地保护密钥持有者的利益；若密钥持有者为了避免承担必要的责任，对发生的行为进行抵赖，它可以主动泄漏密钥，这样其他一方的利益就无法被保护。为此基于强 RSA 和离散对数的假设，构造了具有前向安全特性的秘密共享方案，该方案中的参与者可以简便地更新拥有的子密，特别是能检测伪子密，防止欺诈者，并且也可以检测恢复得到的秘密信息是否正确。同时对方案的安全性进行了分析。研究具有前向安全性质的门陷的秘密共享是我们进一步研究的方向。

参 考 文 献

[1] Blakley G R. Safeguarding cryptographic keys. Proceedings of AFIPS National Computer Conference. New York, USA, AFIPS Press,1979,Vol.48: 313−317.

[2] Shamir A. How to share a secret. *Communications of the ACM*, 1979, 24(11): 612−613.

[3] Anderson R. Invited Lecture. Proceedings of The 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, 1997: 1−7.

[4] Bellare M, Miner S K. A forward-secure digital signature scheme. Proceedings of 19th Annual International Cryptology Conference, Santa Barbara, California, USA, Springer, 1999, LNCS 1666: 431−448.

[5] Kozlov A, Reyzin L. Forward-secure digital signature scheme with fast key update. In Proceedings of Security in Communication Networks. Amalf, Italy, Springer, 2002, LNCS 2576: 241−256.

[6] Itkis G, Reyzin L. Forward-secure signature scheme with optimal signing and verifying. Proceedings of 21st Annual International Cryptology Conference, Santa Barbara, California, USA, Springer, 2001, LNCS2139: 332−354.

[7] Blundo C, Gressti A, Santis A D, *et al*.. Fully dynamic secret sharing schemes. Proceedings of 13th Annual International Cryptology Conference, Santa Barbara, California, USA, Springer,1993, LNCS773: 110−125.

[8] Tassa T. Hierarchical threshold secret sharing. Proceedings of Theory of Cryptography Conference 2004, Cambridge, MA, USA, Springer, 2004, LNCS 2951: 473−490.

[9] Cachin C. On-line secret sharing. Proceeding of the 5th IMA Conference on Cryptography and Coding, Cirencester, UK, Springer, 1995, LNCS 1025: 190−198.

[10] Chor B, Goldwasser S, Micali S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults. Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science, New York,1985: 383−395.

[11] Stadler M. Publicly verifiable secret sharing. Proceeding of International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, Springer, 1996, L NCS 1070: 190−199.

[12] Boyd C. Digital Multisignatures. In Cryptography and Coding, UK: Oxford University Press, 1989: 241−246.

[13] Fujisaki E, Okamoto T. Statistical zero knowledge protocols to prove modular polynomial relations. Proceedings of 17th Annual International Cryptology Conference, Santa Barbara, California, USA, Springer, 1997, LNCS 1294: 16−30.

王彩芬： 女，1963 年生，博士，教授. 目前主要研究方向为信息安全、协议的设计及协议的形式化分析等。在《计算机学报》《电子学报》《通信学报》等国内外刊物发表论文 30 余篇.

刘军龙： 男，1981 年生，硕士生，研究方向为信息安全、网络安全.

贾爱库： 男，1970 年生，硕士生，研究方向为信息安全、网络安全.

于成尊： 男，1982 年生，硕士生，研究方向为信息安全、网络安全.