对基于单向函数的 He-Dawson 多步骤秘密共享方案的改进

闫德勤 赵洪波 靳 虹
(辽宁师范大学计算机与信息技术学院 大连 116029)

摘 要 在(t,n)门限秘密共享方案中,有n个参与者,至少t个参与者拿出自己的子秘密就能够同时重构m个秘密。He-Dawson 提出了一个基于单向函数的多步骤秘密共享方案。但是他们的方案是一次方案而且不能抵抗合谋攻击。每个参与者的子秘密由参与者自己选取,所以不存在秘密分发者的欺骗。并且每个参与者能够验证其他合作者的欺骗。每个参与者选取的子秘密可以复用。并且组秘密可以以任意顺序重构。此方案还能够抵抗合谋攻击。本方案的安全是基于 Shamir 门限方案和 RSA 密钥体制。

关键词 密码学,秘密共享,多秘密共享,门限方案

Improvement on the He-Dawson Multi-stage Secret Sharing Based on One-way Function

YAN De-qin ZHAO Hong-bo JIN Hong
(Department of Computer Science, Liaoning Normal University, Dalian 116029, China)

Abstract In the (t,n) threshold multi-secret sharing scheme, there are n participants in the system. At least t or more participants can easily pool their secrets shadows and reconstruct m secrets at the same time. He-Dawson proposed a multistage secret sharing based on one-way function. But their scheme is one-time-use and suffers from the conspire attack. In this paper, each participant's secret shadow was selected by the participant himself, so the UD cheating is not exist. And every participant can detect the cheating by any other participant. Each participant can share many secrets with other participants by holding only one reusable shadow. And the group secret can be reconstructed in free order. Furthermore, the new scheme can withstand the conspiracy attack. The security of this scheme is that of the RSA cryptosystem and Shamir's (t,n) threshold secret sharing scheme.

Keywords Cryptosystem, Secret sharing, Multi-secret sharing, Threshold scheme

1 引言

为了保证秘密更安全,1979年,Shamir[19]和 Blakley[1]首先分别基于拉格朗日多项式和射影几何定理提出了(t,n)门限共享方案。在他们的方案中,秘密分发者首先将秘密分成n个不同的部分,每个部分都叫做子秘密,然后将子秘密通过安全信道分发给n个参与者,其中至少t个参与者合作就能重构秘密,而任意$t-1$或更少个成员不能够获得任何秘密信息。然而,在秘密共享方案中[1,19]有如下的不足:

(1) 在一次秘密共享过程只能共享一个秘密[10]。

(2) 一旦秘密被重构,需要通过安全信道重新发布新的子秘密给每个成员[15]。

(3) 一个恶意的秘密分发者可能会提供假的子秘密,这样成员就不能重构真正的秘密[7]。

(4)一个恶意的参与者可能会提供假的子秘密给其他成员,使得这个恶意参与者成为能够唯一重构秘密的人[22]。

为了解决第一个问题,提出了一些(t,n)门限多秘密共享方案[6,9,10]。为了解决第二个问题,Jakson 等人[15]更进一步把多秘密共享方案定义成两种类型:一次方案和多次方案。两者的不同在于多次方案中的子秘密可以复用,而一次方案的子秘密不能复用。我们知道,重新发布子秘密既耗费时间又耗费资源。

为了解决第3个问题,Chor 等人[7]提出了一个可验证的秘密共享方案来检测秘密分发者的欺骗。在 Chor 等人的方案中,每个参与者能够验证分发者分给他/她的子秘密,这就要求参与者必须诚实。可见,在 Chor 等人的方案中第4个问题仍然存在。很多年后,Stadler [20]提出了一个方案,同时解决了问题3和问题4。Stadler 的方案既防止分发者[8]的欺骗又可验证任何成员[2,3,16,21,22]的欺骗。但是,这些可验证的秘密共享方案都只能在一次秘密共享过程共享一个秘密。

1994年,He and Dawson [23]提出了一个基于单向函数的多步骤秘密共享方案。他们使用公开移动技术来获得秘密并且通过连续的单向函数来分步以特定顺序获得秘密。不久,Harn [24]在1995年提出了可验证的多秘密共享方案。但是在他们的方案中,为了验证密钥是否有效,每个参与者需要检测计算$n!/((n-t)!\,t!)$等式。在1997年,Chen 等人[5]提

到稿日期:2008-07-07 返修日期:2008-09-17 本文受国家自然科学基金(60372071),辽宁省教育厅高等学校科学研究基金(2004C031),大连市科技局科技计划项目(2007A10GX117),中国科学院自动化研究所复杂系统与智能科学重点实验室开放课题(20070101)资助。

闫德勤(1962—),男,博士,教授,主要研究方向为信息安全、密码学、数据挖掘,E-mail: yandeqin@163.com;赵洪波(1983—),女,硕士研究生,主要研究方向为信息安全与密码学;靳 虹(1983—),女,硕士研究生,主要研究方向为数字签名。

出了另外的可验证多秘密共享方案来改进 Harn 的方案，但是这个方案的计算量仍然很大。

2 He-Dawson 的方案介绍

He and Dawson 方案希望分发者能够控制秘密并且以特定顺序分步重构秘密，并且希望他们的方案是一个多次方案。

2.1 初始化

Let $f:Zp\sim Zp$ 是一个定义 k 次连续对 m 作用的单向函数 $h^k(m)$。举例为：$h^0(m)=m, h^k(m)=h(h^{k-1}(m))$。假定分发者想要分享 k 个秘密 (for $i=1,2,\cdots,k$)并且最少 t 个人能够重构秘密。

2.2 构造阶段

分发者随机选择 n 个不同的整数 x_i(for $i=1,2,\cdots,n$)作为每个参与者的公开信息并执行下面的操作：

1)随机选择 $y_1,y_2,\cdots,y_n$。

2)对 $i=1,2,\cdots,k$ 执行以下操作：

(a) 构造一个 $t-1$ 次多项式 $P_i(x)$且 $P_i(0)=s_i$。

(b) 计算 $Z_{ij}=p_i(x_j), j=1,2,\cdots,n$。

(c) 计算 $d_{ij}=Z_{ij}-h^{i-1}(y_j)$和 $h^{i-1}(y_j)$，$h^{i-1}(y_j)$为秘密份额。for $j=1,2,\cdots,n$。

3) 秘密送 y_i 给每个参与者，并且公开所有的 $d_{ij}, i=1,2,\cdots,k$ and $j=1,2,\cdots,n$。

2.3 秘密重构

最少 t 个参与者以特定顺序提供自己的秘密份额：$h^{k-1}(y_j),h^{k-2}(y_j),\cdots,h^0(y_j)$(for $j=1,2,\cdots,t$)，来重构多项式 $P_i(x)$ for $i=k,k-1,\cdots,1$。然后每个秘密可通过下式重构(for $i=k,k-1,\cdots,1$)：

$$s_i=P_i(0)=\sum_{a=1}^{t}(h^{i-1}(y_a)+d_{ia})\prod_{b=1,b\neq a}^{t}\frac{0-x_b}{x_a-x_b} \tag{1}$$

秘密重构也以特定顺序 $s_k,s_{k-1},\cdots,s_1$ 进行。

3 He-Dawson 的方案分析和对我们方案的介绍

在本节中，我们对于 He-Dawson 的方案作了简明的描述，证明了他们的方案不是多次方案并且某种情况下分发者不能控制特定顺序重构秘密。

为了重构秘密 s_1，最少 t 个参与者必须发布他们的秘密份额 $h^0(y_i)$for $i=1,2,\cdots,t$。根据定义 $h^0(y_i)=y_i$。所以，在重构所有秘密以后，分发者必须通过安全信道重新发布 y_i。这样，他们的方案就属于一次方案。

当最少 t 个参与者不是以特定顺序提供 $h^{k-1}(y_j),h^{k-2}(y_j),\cdots,h^0(y_j)$for $j=1,2,\cdots,t$ 时，秘密也不能以特定顺序重构。例如：当某个参与者率先发布他/她的秘密份额 $h^1(y_1)$，其他参与者很容易计算出他/她的秘密份额 $h^2(y_1),h^3(y_1),\cdots,h^k(y_1)$。这样，只要 $t-1$ 个参与者就能重构秘密 $s_2,s_3,\cdots,s_{k-1},s_k$。因此，分发者不能控制重构顺序而由这 t 个参与者决定。换句话说，他们的方案不能抵抗合谋攻击，也不能满足某些应用需求。

为了解决上述问题，我们基于 He-Dawson 方案提出了一个可验证的多秘密共享方案，本文方案有如下性质：

(1)每个参与者的子秘密由参与者自己选取，所以不存在秘密分发者的欺骗。

(2)每个参与者能够通过验证其他合作者的子秘密影子来检测其他成员的欺骗。

(3)每个参与者能够通过保存一个可以复用的子秘密来分享很多秘密。

(4)不同的秘密重构根据不同的门限值，这就使得此方案更加灵活，从而满足实际应用需求。因为不同的组秘密在初始化时产生不同的秘密多项式。所以组秘密 $s_i(i=1,2,\cdots n)$ 能够以自由顺序重构。

(5)如果某个组成员想要通过合谋攻击来获得组秘密是不可行的，因为攻击者不能获得其他参与者的正确的子秘密 $f(r,h^i(x_j))$。

(6)本文仍然具有 He-Dawson 方案的属性。

4 我们的方案

4.1 初始化阶段

在我们的方案中，$h^k(m)$和 He-Dawson 方案的定义相同，g 是 Z_P^* 的生成元。秘密分发者首先创建一个公示板(NB)来存放必要的公开信息，参与者也能够从公示板获得所需信息。公示板上的内容只能由秘密分发者来修改。假定秘密分发者要共享 k 个组秘密 $s_i, i=1,2,\cdots,k$。n 个参与者中的任意不同 t 个人就能够重构此组秘密。由秘密分发者定义的参数如下：N 是两个大素数 p 和 q 的乘积。其中 $p=2p'+1$ t and $q=2q'+1$，N'是两个大素数 p'和 q'的乘积。秘密分发者随机从$[2,N]$中选择一个整数 d，d 是不同于 $(p-1)$和 $(q-1)$ 的素数。分发者计算 e 使得 $d\times e=1 \bmod \Phi(N)$，其中 $\Phi(N)$ 是一个布尔函数。秘密分发者将$\{e,g\}$发布到 NB 并保密 d。$f(r,s)$是一个双变量单向函数，它在从前的文献[6,25]中有过定义，这里定义相同。

4.2 构造阶段

Step1 对于 $i=1,2,\cdots,k$ 执行以下步骤：每个参与者发送$(ID_i,f(r,h^i(x_j)))$(for $j=1,2,\cdots,n$)(其中 $f(r,h^i(x_i))$ 产生见步骤 2)给秘密分发者。秘密分发者就可以通过此 n 个点对来构造一个多项式：

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{n-1} \bmod N' \tag{2}$$

然后发布 $ID_i,f(1),f(2),\cdots,f(n-t),g^{f(r,h^i(x_j))}$。

Step2 每个参与者随机在$[2,N]$中选取整数 x_i，然后计算 $f(r,h^i(x_i))$作为他们的子秘密。然后秘密分发者随机选择 r_i,T_i，并计算 H_i。

$$C_i=r_ig^d \bmod N \tag{3}$$

$$H_i=(r_i^{a_0}T_i-s_i)C_i^{-a_0} \bmod N \tag{4}$$

Step3 分发者将$\{r_i,T_i,C_i,H_i\}$发布在 NB 上。

4.3 重构阶段

假定 $W=\{M_1,M_2,\cdots,M_n\}$，$M=\{M_1,M_2,\cdots,M_t\}$。M 中的成员将要恢复秘密 $s_1,s_2,\cdots,s_k$。

(1)他们利用他们的子秘密 $f(r,h^i(x_j))$来计算一个子秘密影子 A_{ij}。(for $j=1,2,\cdots,t$)

$$A_{ij}=r_i^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i} \bmod N \tag{5}$$

$$B_{ij}=C_i^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i} \bmod N, \text{publish } B_{ij} \tag{6}$$

其中 $\Delta_i=\prod_{k\in W,k\neq j}\frac{0-ID_k}{ID_j-ID_k} \bmod N$ (7)

(2)每个 M_i 都能够验证 A_{ij}：

$$A_{ij}{}^e g^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i}=B_{ij}{}^e \bmod N$$

(3)然后，计算

$$s_i = T_i \prod_{j \in W} A_{ij} - H_i \prod_{j \in W} B_{ij} \bmod N \quad (8)$$

5 性能分析

5.1 可行性分析

(1)每个人都可以验证由 M_i 提供的 A_{ij}，因为：

$$A_{ij}^{e} g^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i} = (r_i^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i})^e g^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i}$$

$$= r_i^{ef(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i} g^{f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i}$$

$$= (r_i g^d)^{ef(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i}$$

$$= B_{ij}^{e} \bmod N$$

(2)M 中的每个成员都能恢复秘密 s_j，因为：

$$T_i \prod A_{ij} - H_i \prod B_{ij} = T_i r_i^{\sum f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i} - (r_i^{a_0} T_i - P_i) C_i^{-a_0} C_i^{\sum f(r,h^i(x_j))f(1)f(2)\cdots f(n-t)\Delta_i} = T_i r_i^{a_0} - (r_i^{a_0} T_i - s_i) C_i^{-a_0} C_i^{a_0} = s_i \bmod N$$

5.2 安全性分析

(1) 如果恶意参与者 E 能够利用少于 t 个 (when $k \leqslant t$) 或者(when $k > t$)来重构多项式 $P(x) \bmod N'$，相当于 E 能够成功破坏 Shamir 的门限方案。He-Jawson 的方案和本方案都是基于 Shamir 的门限体制。

(2) 如果恶意参与者能够从公开信息 A_{ij} 和 B_{ij} 中获得参与者 M_i 的子秘密 $f(r,h^i(x_j))$，此难度相当于成功解决离散对数问题。然而，离散对数问题是一个 NP 问题。更进一步，任何人也不能获得 x_i，这是由双变量单向函数的性质决定的。所以此方案是一个多次方案。

5.3 方案对比

本文方案和原方案相比，具有明显的优越性，如表 1 所列。

表 1 本文与原方案实现功能对比

Capability	Our scheme	He-Jawson scheme
The verification	Yes	No
Withstand the conspiracy attack	Yes	No
Reconstruct several secrets parallelly	Yes	No
Reuse of the secret shadows	Yes	No

结束语 本文指出了 He-Dawson 方案是一次方案，并且它的门限值是确定的，从而提出了一个新的可验证的多秘密共享方案。本文是一个多次方案，并且每个参与者的子秘密由参与者自己选取，不存在管理者欺骗。每个参与者在共享多个秘密的时候只需要一个可以复用的子秘密，组秘密可以以任意顺序恢复，本文还可以抵抗合谋攻击。

参 考 文 献

[1] Blakley G. Safeguarding cryptographic keys[C]// Proc. AFIPS1979 Natl. Conf. NewYork, 1979: 313-317

[2] Carpentieri M. A perfect threshold secret sharing scheme to identify cheaters[J]. Designs, Codesand Cryptography, 1995, 5(3): 183-187

[3] Chang D C, Hwang R J, Cientcheateridenti E. cation method for threshold schemes[J]. IEE Proc. Comput. Digit. Tech., 1997, 144(1): 23-27

[4] Chang C-C, Hwang M-S. Parallel computation of the generating keys for RSA crypto systems[J]. IEE Electron. Lett., 1996, 32(15): 1365-1366

[5] Chen L, Gollmann D, Mitchell C J, et al. Secret sharing with reusable polynomials[C]// Proceedings of ACISP '97. 1997: 183-193

[6] Chien H-Y, Jan J-K, Tseng Y-M. Apractical (t, n) multi-secret-sharing scheme[J]. IEICE Trans. Fundamentals, 2000, E83-A(12): 2762-2765

[7] Chor B, Goldwasser S, Micali S, et al. Veri. able secret sharing and achieving simultaneity in the presence of faults[C]// Proc. 26th IEEE Symp. FOCS, 1985: 251-260

[8] Gennaro R, Micali S. Veritable secret sharing assecure computation [C] // AdvancesinCryptology, EUROCRYPT' 95, LectureNotesin Computer Science. 1995: 168-182

[9] Harn L E. Cient sharing (broadcasting) of multiple secret[J]. IEE Proc. Comput. Digit. Tech., 1995, 142(3): 237-240

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

[11] He W H, Wu T S. CommentonLin. Wu(t, n) thresholdveri. able multi secret sharing scheme [J]. IEE Proc. Comput. Digit. Tech., 2001, 148(3): 139

[12] Hwang M-S, Lee C-C, Lai Y-C. Traceability on RSA-based partially signature with low computation[J]. Appl. Math. Comput, 2002

[13] Hwang M-S, Lin I-C, Hwang K-F. Crypt an alysis of the batch verifying multiple RSA digital signatures[J]. Informatica, 2000, 11(1): 15-19

[14] Hwang M-S, Yang C-C, Tzeng S-F. Improved digital signature-scheme based on factoring and discrete logarithms[J]. Discrete-Math. Sci. Cryptography, in press

[15] Jackson W-A, Martin K M, O'Keefe C M. On sharing many secrets[C]// Asiacrypt'94. 1994: 42-54

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

[17] Lin T Y, Wu T C. (t, n) threshold veritable multi secret sharing scheme based on factorisation in tractability and discrete logarithm modulo a composite problems[J]. IEE Proc. Comput. Digit. Tech., 1999, 146 (5): 264 -268

[18] Rivest R L, Shamir A, Adleman L. A method for obtaining digitalsignatures and public key crypto systems [J]. Commun. ACM, February 1998, 21: 120-126

[19] Shamir A. How to share a secret, Commun[J]. ACM, 1979, 22: 612 -613

[20] Stadler M. Publiclyveri. ablesecret sharing [C] // Advances in Cryptology, EUROCRYPT' 96, Lecture Notesin Computer-Science. 1996: 190-199

[21] Tan K J, Zhu H W, Gu S J. Cheateridenti. cationin(t, n) threshold scheme[J]. Comput. Commun, 1999, 22 (8): 762-765

[22] Tompa M, Woll H. How to share a secret with cheaters[J]. Cryptol, 1988(1): 133-138

[23] He J, Dawson E. Multi stage secret sharing based on one-way function[J]. Electronics Letters, 1995, 31(4): 262

[24] Harn L. Comment: Multi stage secret sharing based on one-way function. Association for Computing Machinery[J]. New York, 2005, 39: 48-55

[25] YangChou-Chen, ChangTing-Ti, HwangMin-Shiang. A(t, n) multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490