第 36 卷 第 7 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.7 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)07—0126—03 文献标识码：A 中图分类号：TP309

3 个秘密共享方案的弱点分析与改进

张建中，屈 娟
(陕西师范大学数学与信息科学学院，西安 710062)

摘 要：通过对秘密共享的研究与分析，发现现有的秘密共享方案几乎都有其弱点，导致这些方案不能在实际中得到应用。分析 3 个秘密共享方案，指出它们各自存在的安全漏洞，并通过系统初始化、秘密份额生成和验证、秘密承诺生成和恢复等对刘锋等人的方案(计算机应用研究，2008 年第(1)期)进行改进。结果表明，改进后的方案克服了原有方案的缺点，是一个安全的可验证的秘密共享方案。

关键词：秘密共享；主动攻击；欺诈；可验证

Weaknesses Analysis and Improvement of Three Secret Sharing Schemes

ZHANG Jian-zhong, QU Juan
(College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062)

【Abstract】Through the research and analysis of secret sharing, it is found that all the existing secret sharing schemes have weaknesses, thus results in these schemes be not applied. Three secret sharing schemes are analyzed and the secure hole of them is pointed, through system initialization, secret part building and validating, secret acceptance building and recovery, Liufeng et al scheme(application research computers, 2008,(1)) is improved. Result shows that the improved scheme overcomes the security problem of the original scheme, and it is a safe verifiable secret sharing scheme.

【Key words】secret sharing; active attack; cheating; verifiable

1 概述

秘密共享是密钥管理的重要研究课题，无论在理论上还是在实践上都具有重要的意义。秘密共享即秘密分发者将秘密 K 分成多个子秘密，并分发给不同的参与者，参与者中的全部或一部分在提供正确的子秘密后可重构出秘密 K。在实际中，为了有效防止秘密分发者和参与者的欺诈，许多学者提出一些可验证的秘密共享方案[1-4]。在一次秘密共享方案中使得分享者重复使用其秘密份额，有学者提出多秘密共享方案[5-7]。考虑到成员集合的变动问题，还有一些学者提出非交互式的秘密共享方案[8]。为了避免门限方案中门限值的限制，又有学者提出一般访问结构上的秘密共享方案[9]。

本文主要分析文献[10-12]中的方案。通过分析文献[10]方案可知，一旦每个参与者知道 $\Phi(N)$，就会导致整个系统崩溃，整个系统毫无秘密而言，这个方案彻底失败。文献[11]指出该方案能防止参与者的欺诈，但是笔者指出这是不正确的， 能够伪造假的信息通过验证等式。文献[12]的方案不仅不能抵抗参与者的欺骗，而且也不能抵抗秘密分发者的欺诈，它不是一个可验证的秘密共享方案。

2 动态 (t,n) 门限多秘密分享方案及弱点

2.1 文献[10]方案门限秘密共享方案简介

门限秘密共享方案由系统初始化、秘密份额的生成与验证、秘密承诺生成阶段、秘密份额的验证和秘密回复 4 个阶段组成。

2.1.1 系统初始化

秘密分发者 D 首先创建一个公告栏，以便向系统成员提供必要的公开参数。每个成员均可以访问公告栏中的参数，但是只有 D 才能更改或刷新公告栏中的内容。然后，D 定义如下参数：N 是 2 个大素数 p,q 的乘积。其中，$p=2p'+1$，$q=2q'+1$，且 p',q' 也是参数；e,d 分别是 D 的公钥和私钥，这里 $e\times d\equiv 1 \bmod \Phi(N)$；$H$ 是 $Z^*_{\Phi(N)}$ 上的一个安全的单向函数。将数组 $\{N,e\}$ 公布在公告栏上。

2.1.2 秘密份额的生成和验证

假设 $G=\{U_1,U_2,\cdots,U_n\}$ 是 n 个参与者的集合，$S=\{S_1,S_2,\cdots,S_m\}$ 是 m 个待分享秘密的集合，ID_i 是 $U_i(i=1,2,\cdots,n)$ 的身份标志，则秘密份额和验证信息的生成算法如下：D 随机地选取一个多项式 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1} \bmod \Phi(N)$。其中，$a_k\in Z^*_{\Phi(N)}$ 为多项式的系数建立一个验证向量 $\boldsymbol{V}=\{V_0,V_1,\cdots,V_{t-1}\}$，使得 $V_k=ea_k \bmod \Phi(N)$ $(k=0,1,\cdots,t-1)$。将 $\boldsymbol{V}$ 公布在公告栏上。计算 U_i 的秘密份额：$x_i=f(ID_i\times d\times p_i^{-1} \bmod \Phi(N)$，其中，$p_i=\prod_{U_k\in G,U_k\neq U_i}(ID_i-ID_k) \bmod \Phi(N)$。将 $y_i=e\times x_i \bmod \Phi(N)$ 作为其公钥公布在公告栏上。当 $U_i\in G$ 收到秘密份额 x_i 后，就可以利用式(1)来验证其有效性：

$$\sum_{k=0}^{t-1}V_k\times ID_i^k=e\times p_i\times y_i \tag{1}$$

基金项目：国家自然科学基金资助项目(10571113)；陕西省自然科学基金资助项目(2004A14)；陕西省教育厅科学研究计划基金资助项目(07JK375)

作者简介：张建中(1960－)，男，教授、博士，主研方向：信息安全，密码学及认证理论；屈 娟，硕士研究生

收稿日期：2009-12-10 **E-mail：**qulujuan@163.com

如果式(1)不成立，则说明 D 对 U_i 有欺诈行为，这是 D 发出抱怨；否则，继续下列步骤。

2.1.3 秘密承诺生成阶段

D 按下述算法为每一个待分享的秘密 $S_1,S_2,\cdots,S_m\in S$ 计算一个承诺值 $h_1,h_2,\cdots,h_m$，随机选取 m 个不同的整数 $r_1,r_2,\cdots,r_m\in Z^*_{\Phi(N)}$，计算 $C_i=d\times r_i \bmod \Phi(N)$。其中，$H$ 是一个单向函数；$j=1,2,\cdots,m$。将三元组 $\{r_j,C_j,h_j\}$ 公布在公告上。

2.1.4 秘密份额的验证和秘密恢复

令 $\Gamma\{|\Gamma|=t\leqslant n\}$ 是 G 中参与者的一个访问结构，不妨设 t 个参与者的集合 $U_i\in\Gamma$ 合作重构秘密 $S_j\in S$。每个参与者 $U_i\in\Gamma$ 从公告栏上获取秘密 S_j 的承诺 $\{r_j,C_j,h_j\}$；利用其子秘密 x_i，计算并公布 $A_{ij}\equiv x_i\times C_j \bmod \Phi(N)$。这时，任何其他合作者均可利用公告栏上 U_i 的公钥 y_i 验证 A_{ij} 的有效性：

$$e^2\times A_{ij}=y_i\times r_j \bmod \Phi(N)$$

如果上式不成立，则表明参与者 U_i 有欺诈行为；反之，如果 t 个参与者的公开值均能通过验证，则访问结构 Γ 中的任何一个成员均能由式(2)恢复出秘密：

$$S_j=h_j\oplus H(e\times\sum_{i=1}^{t-1}(A_{ij}\times\Delta_i \bmod \Phi(N))) \tag{2}$$

其中，$\Delta=[\prod_{U_k\in G,U_k\neq U_i}(-ID_k)]\times[\prod_{U_k\in G,U_k\notin\Gamma}(ID_i-ID_k)]$。

重复执行这一阶段的算法就能恢复出所有的待分享秘密。

2.2 文献[10]门限秘密共享方案的弱点

文献[10]方案存在严重的安全漏洞，非常脆弱，经不起攻击，方案存在以下问题：

(1)从 2.1.4 节方案秘密份额的验证和恢复阶段中看出群 G 中每个参与者 U_i 知道 $\Phi(N)$，那么，由公开的验证向量 $\boldsymbol{V}$，U_i 可得到 $a_0(a_0=e^{-1}V_0 \bmod \Phi(N))$。另外，由 $ed\equiv 1 \bmod \Phi(N)$，且 e 是公开已知的，每个 U_i 可得到秘密分发者 D 的私钥 $d(d\equiv e^{-1} \bmod \Phi(N))$，且从公告栏中每个 U_i 可得到 r_j，那么 U_i 可计算出 $C_j=d\times r_j \bmod \Phi(N)$。因此，$U_i$ 可根据 $S_i=h_i\oplus H(a_0\times C_j \bmod \Phi(N)$ 独自计算出秘密 S_i。因而，文献[10]方案不再是 (t,n) 门限秘密共享方案。

(2) G 中的每个参与者都知道 $\Phi(N)$，从而导致整个系统崩溃。因为每个参与者由公开参数可以得到其他参与者的子秘密，进而能够得到所有的秘密 $S_i(i=1,2,\cdots,n)$，所以整个系统毫无秘密而言。

2.3 对文献[10]方案的改进和安全性分析

2.3.1 系统初始化

秘密分发者 D 创建一个公告栏 NB，D 定义以下参数：N 是 2 个大素数 p，q 的乘积，$\varphi(N)$ 是欧拉函数，H 是 $Z^*_{\varphi(N)}$ 上的一个安全单向函数。

2.3.2 秘密份额的生成和验证

设 $G=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参与者的集合，$S=\{S_1,S_2,\cdots,S_m\}$ 是 m 个待分享秘密的集合。ID_i 是 $P_i(i=1,2,\cdots,n)$ 的身份标志，则秘密份额和验证信息的生成算法如下：

(1)秘密分发者 D 随机地选取一个多项式：

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\in Z_{\varphi(N)}[x]$$

为该多项式的系数建立一个验证向量 $\boldsymbol{V}=\{V_0,V_1,\cdots,V_{t-1}\}$，使得 $V_k=g^{a_k} \bmod N$，将 $\boldsymbol{V}$ 公布在公告栏上。

(2)计算 P_i 的秘密份额：$x_i=f(ID_i)\times h_i^{-1} \bmod \varphi(N)$，其中，$h_i=\prod_{P_k\in G,P_k\neq P_i}(ID_i-ID_k) \bmod \varphi(N)$，并公开 $y_i=g^{x_i} \bmod N$。当 $P_i\in G$ 收到秘密份额 x_i 后，检查 $g^{x_i}\equiv y_i \bmod N$ 和 $(g^{x_i})^{h_i}=\prod_{k=0}^{t-1}(V_k)^{ID_i^k} \bmod N$。

2.3.3 秘密承诺生成阶段

D 随机选取 $C_1,C_2,\cdots,C_m,k\in Z^*_{\varphi(N)}$，其中，$C_i(i=1,2,\cdots,m)$ 和 k 是互不相同的。计算 $K=g^k \bmod N$，$W_j=S_j\oplus H(C_j^{a_0} \bmod N)$。并将 $\{C_j,W_j,k\}$ 公开。

2.3.4 秘密恢复

假定 $\Gamma(|\Gamma|\geqslant t)$ 中 t 个成员要恢复秘密 S_j。首先，每个 $P_i\in\Gamma$ 利用它的秘密份额 x_i 计算 $A_{ij}=C_j^{x_i} \bmod N$，$B_{ij}=A_{ij}\times y_j^{\,k} \bmod N$，并发送给 Γ 中的其他成员 P_j。那么，P_j 可利用子秘密 x_j 验证 A_{ij} 的有效性，$B_{ij}=A_{ij}\times K^{x_j} \bmod N$，如果等式不成立，$P_j$ 发出抱怨，否则，当 A_{ij} 的有效性通过验证后，Γ 中的每个成员就可恢复出秘密 S_j，$S_j=W_j\oplus H(\prod_{j\in\Gamma}A_{ij}^{\Delta_i} \bmod N)$。

2.3.5 方案分析

文献[10]方案分析如下：

(1)上述方案的安全性主要是基于离散对数的，因而是计算安全的。攻击者试图通过以下 2 种方法恢复秘密 S_j:1)攻击者从公告栏中获知 V_0，但是即使攻击者知道 V_0 $(V_0=g^{a_0} \bmod N)$，还是不能恢复出秘密，因为面临着解离散对数问题。2)攻击者通过计算 A_{ij} 来恢复秘密。这也是不可行的，因为计算 A_{ij} 需要参与者的秘密份额 x_i，显然参与者的秘密份额是不可知道的。

(2)方案是(t, n)门限方案，当 Γ 中的成员有了 t 个 A_{ij} 后，由 Lagrange 插值公式可知：

$$\prod_{j\in\Gamma}A_{ij}^{\Delta_i} \bmod N=\prod_{j\in\Gamma}C_j^{x_i\Delta_i} \bmod N=C_j^{\sum_{j\in\Gamma}x_i\Delta_i} \bmod N=C_j^{a_0} \bmod N$$

于是通过 $S_j=W_j\oplus H(\prod_{j\in\Gamma}A_{ij}^{\Delta_i} \bmod N)$ 就可恢复出秘密。

(3)秘密分发者对参与者的欺诈行为是可以检测出来的。因为向量 $\boldsymbol{V}$ 是公开的，如果发送假的秘密份额 x_i'，则不能通过式(2)的验证。

(4) Γ 中一个秘密分享者发送给其他秘密分享者的秘密影子是可以验证的。因此，本文方案能防止参与者的欺诈。

3 多秘密分享方案及其弱点

文献[11]的方案由系统初始化、秘密份额的生成、秘密子份额的生成与验证和子秘密的恢复 4 个阶段组成。下面主要说明方案的缺点：

在文献[11]方案中，笔者指出其中的攻击 2 是不成立的，即在子秘密 S_i 恢复期间，ω 中某一不诚实成员 P_j 企图交出一不正确的 $\{A_{ij},B_{ij},D_{ij},\Delta_j\}$ 给其他合作者。P_j 给出的伪 $\{A_{ij},B_{ij},D_{ij},\Delta_j\}$ 不能成功地通过等式 $B_{ij}^{\,e}\equiv D_{ij}y_j^{\,r_i\Delta_j}A_{ij}^{\,r_i} \bmod N$ 的验证，因为将面临求解 *RSA* 因式分解难题。本文指出这样的攻击是成立的，参与者 P_j 利用伪子秘密 x_j' 计算 $A_{ij}'=T_i^{x_j'\Delta_j} \bmod N$，$B_{ij}'=C_i^{x_j'\Delta_j} \bmod N$，$D_{ij}'=B_{ij}'^{\,e}y_j^{-r_i\Delta_j}A_{ij}'^{-r_i} \bmod N$。其中，$\{T_i,C_i,e,r_i,y_j\}$ 都是公开的。当 P_j 把 $\{A_{ij}',B_{ij}',D_{ij}',\Delta_j\}$ 送给 ω

中的其他合作者时，这样的 $\{A_{ij}^{'},B_{ij}^{'},D_{ij}^{'},\Delta_j\}$ 是能够成功地通过等式的验证，即 $B_{ij}^{'e}\equiv B_{ij}^{'e}y_j^{-r_i\Delta_j}A_{ij}^{'-r_i}y_j^{r_i\Delta_j}A_{ij}^{'r_i} \bmod N$ 。因此，在 ω 中的其他诚实合作者将获得假的秘密 $S_i^{'}$ 而只有 P_j 能获得真实的秘密 S_i 。

4 可验证的秘密共享方案及其弱点

4.1 文献[12]门限秘密共享方案简介

4.1.1 系统初始化

p,q 是 2 个大素数且满足 $q/p-1$， G_q 是 Z_q^* 阶为 q 的子群， g 是 G_q 的一个生成元，即若 $a\in G_q$ ，则有 $a^q=1$ 。

4.1.2 子秘密生成及分发

D 是秘密分发者，在这个 (k,n) 门限方案中有 n 个成员。不失一般性，假设 $S\in Z_q$ 是秘密， D 随机选择 $A=(a_1,a_2,\cdots,a_{t-1})$ ，其中， $a_i\in Z_q$ ，构造多项式 $f(x)=S+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$ 。 D 为每个 P_i 随机选择 $c_i\in Z_q^*$ ，并计算 $f(i)$ 。则有 $s_i=f(i)$ ， $\chi_i=g^{c_i}$, $\delta_i=\dfrac{S}{s_i+c_i}$ 。 D 为每个 P_i 分发 (s_i,χ_i,δ_i) ，并且公开 g^S 作为验证信息。

4.1.3 子秘密验证和秘密恢复阶段

参与者 P_i 验证 s_i 的有效性通过 $(g^{s_i}\chi_i)^{\delta_i}=g^S$ ，若该式成立，则子秘密是有效的，任何 t 个诚实的参与者 $P_{i_1},P_{i_2},\cdots,P_{i_t}$ 合作可计算出秘密 S ，即 $S=\sum_{j=1}^{t}(\prod_{l\neq j}\frac{0-i_j}{i_l-i_j})f(i_j)$ 。

4.2 文献[12]方案的弱点

本文指出该方案不能抵抗秘密分发者和参与者的欺诈，因而不满足可验证性，因为当一个不诚实的参与者 P_i 随机选择一个整数 $k\in(0,q)$ 和其他的成员合作恢复秘密 S 时，可计算出 $s_i^{'}=ks_i \bmod p$ ， $\chi_i^{'}=(\chi_i)^k \bmod p$ ， $\delta_i^{'}=k^{-1}\delta_i \bmod q$ 。当交出伪子秘密 $(s_i^{'},\chi_i^{'},\delta_i^{'})$ 时， P_i 给出的伪子秘密 $(s_i^{'},\chi_i^{'},\delta_i^{'})$ 能够通过等式 $(g^{s_i}\chi_i)^{\delta_i}=g^S$ 的验证，即 $(g^{ks_i}\chi_i^{\,k})^{k^{-1}\delta_i}=(g^{s_i}\chi_i)^{\delta_i} \bmod p$ 。因此，只有 P_i 能恢复秘密 S ，其他 $t-1$ 个成员不能获得秘密 S 。秘密分发者也可利用这样的方法对参与者进行欺诈。因此，这个方案不能抵抗秘密分发者和参与者的欺诈，不是一个可验证的秘密共享方案。

5 结束语

秘密共享是密钥管理的一个重大研究课题，但现有的秘密共享方案几乎都有弱点。本文分析 3 个秘密共享方案，指出它们各自存在的一些安全漏洞并对其中的一些方案进行了改进。在文献[10]的方案中，一旦参与者知道了大整数的分解，整个系统就被破坏，本文对其进行了改进，改进后的方案克服了原有方案的缺点，是一个安全的可验证的秘密共享方案；文献[11]的方案不能抵抗参与者的欺诈行为；文献[12]的方案，不能抵抗秘密分发者及参与者的欺诈。通过对这些方案弱点的分析，有利于进一步地改进方案。

参考文献

[1] Stadler M. Public Verifiable Secret Sharing[C]//Proc. of Advances in Cryptology-EUROCRYPT' 96. Berlin, Germany: Springer Verlag, 1996: 190-199.

[2] Zhao Jianjie, Zhang Jianzhong, Zhao Rong. A Pratical Verifiable Multi-secret Sharing Scheme[J]. Computer Standards and Interfaces, 2007, 29(1): 138-141.

[3] 张建中，肖国镇. 可防止欺诈的动态秘密分享方案[J]. 通信学报, 2000, 21(5): 81-83.

[4] 叶蓉丽，张建中. 基于 ECC 的无可信中心的组密钥生成协议[J]. 计算机工程, 2009, 35(6): 150-152.

[5] 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.

[6] 施荣华. 一种多密钥共享认证方案[J]. 计算机学报, 2003, 26(5): 552-556.

[7] 黄东平，刘　铎，王道顺，等. 一种安全的门限多秘密共享方案[J]. 电子学报, 2006, 34(11): 1937-1940.

[8] Feldman P. A Pratical Scheme for Non-interactive Verifiable Secret Sharing[C]//Proc. of the 28th IEEE Symposium on Foundations of Computer Science. [S. 1.]: IEEE Press, 1987.

[9] 李慧贤，程春田，庞辽军. 一般访问结构上的多秘密共享方案[J]. 华南理工大学学报: 自然科学版, 2006, 34(6): 95-98.

[10] 刘　锋，何业锋，程学翰. 动态的(*t*, *n*)门限多秘密共享方案[J]. 计算机应用研究, 2008, 25(1): 241-242.

[11] 甘元驹，谢仕义，沈玉利. 基于 RSA 与 DLP 可证实的多秘密分享方案[J]. 小型微型计算机系统, 2006, 27(3): 454-457.

[12] Ao Jun, Liao Guisheng, Ma Chunbo. A Novel Non-interactive Verifiable Secret Sharing Scheme[C]//Proc. of ICCT'06. [S. 1.]: IEEE Press, 2006: 1-4.

编辑　索书志

（上接第 125 页）

参考文献

[1] 洪　亮，洪　帆. 移动Ad hoc网络中一种信任评估模型[J]. 计算机科学, 2006, 33(7): 31-33.

[2] 王健新，张来男. 移动自组网中基于声誉机制的安全路由协议设计与分析[J]. 电子学报, 2005, 33(4): 596-601.

[3] Cordasco J, Wetzel S. Cryptographic vs. Trust-based Methods for MANET Routing Security[J]. IEEE Wireless Communications, 2007, 11(1): 62-67.

[4] 周尚波. 移动 Ad Hoc 网络中自私行为特性及应对策略[D]. 重庆: 重庆大学, 2007.

[5] 宋　健，王建华. 移动自组网信任模型研究[J]. 计算机安全, 2006, 26(2): 11-13.

[6] Zouridaki C. E-Hermes: A Robust Cooperative Trust Establishment Scheme for Mobile Ad Hoc Networks[J]. Ad Hoc Networks, 2009, 7(6): 1156-1168.

编辑　索书志