第42卷 第8期 西 安 交 通 大 学 学 报 Vol.42 №8
2008年8月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Aug. 2008

一个可验证秘密共享新个体加入协议的安全性分析

郝蓉[1,2]，宋智玲[1]，李绪亮[1]
（1.青岛大学信息工程学院，266071，山东青岛；2.山东大学网络信息安全研究所，250100，济南）

关键词：秘密共享；门限方案；安全性
中图分类号：TP 309.2 **文献标志码**：A **文章编号**：0253-987X(2008)08-1059-02

秘密共享的成员加入协议是一种特殊的秘密再分发协议[1-2]，完成的是在一个秘密共享方案中加入新的成员来共享秘密的操作，在协议的执行过程中，不需要安全的分发中心的参与，同时应该满足3个安全性需求：①不能泄漏关于秘密的任何信息；②除了新加入成员外，其他任何成员都不能获得为其产生的新份额；③旧成员的份额是安全的. 2006年2月，李慧娴等提出了一个可验证的秘密共享新个体加入协议[3]，本文对上述协议的安全性进行了分析，证明了此协议不满足秘密共享成员加入协议的任何一个安全性需求，是完全不安全的.

1 李慧娴等提出协议[3]的预览

系统由 n 个成员 $P_1,\cdots,P_n$ 构成，不失一般性，设成员 $P_1,\cdots,P_t$ 为加入成员 P_{n+1} 产生的新份额，t 为门限，s_i 表示 P_i 持有的份额，令插值系数 $\omega_i(n+1)=\prod_{j=1,j\neq i}^{t}\frac{n+1-j}{i-j}$，新份额产生过程如下.

(1)For $P_i=P_1$ to P_t

(1-1)随机选择整数 e_i 和 l_i，计算 $K_i^0=s_i\omega_i(n+1)e_i$，广播 K_i^0 和 g^{l_i} $(i=1,2,\cdots,t)$.

(2)For $j=1$ to t

For $P_i=P_1$ to P_t

(2-1)如果 $j\neq i$，计算 $K_i^j=K_i^{j-1}\cdot g^{(k+d_{n+1})l_j}$；

(2-2)否则，令 $K_i^j=K_i^{j-1}$；

(2-3)广播 K_i^j $(i=1,2,\cdots,t$ 且 $i\neq j)$.

(3)令 $M_i=K_i^t$.

(4)For $j=1$ to t

For $P_i=P_1$ to P_t

(4-1)如果 $j\neq i$，计算 $W_i^j=M_ig^{(k+d_{n+1})l_j}$；

(4-2)否则 $W_i^j=0$；

(4-3)广播 W_i^j $(i=1,2,\cdots,t$ 且 $i\neq j)$.

(5)For $P_i=P_1$ to P_t

(5-1) 计算 $W_i^e=\sum_{j=1}^{t}W_i^j$；

(5-2) $W_i=s_i\omega_i(n+1)g^{(k+d_{n+1})(\sum_{j=1}^{t}l_j-l_i)}\cdot\sum_{j=1,j\neq i}^{t}g^{(k+d_{n+1})l_j}$；

(5-3) $Q_i=s_i\omega_i(n+1)g^{(k+d_{n+1})(\sum_{j=1}^{t}l_j-l_i)}$；

(5-4)广播 W_i,Q_i；

(5-5)计算：$A=\sum_{i=1}^{t}Q_i$.

(6)For $P_i=P_1$ to P_t

(6-1)计算并广播 $A=g^{(k+d_{n+1})l_i}$；

(6-2)计算 $B=\sum_{i=1}^{t}Ag^{(k+d_{n+1})l_i}-\sum_{i=1}^{t}W_i$.

(7) $P_1,P_2,\cdots,P_t$ 联合解密 B，得到 $C=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{d_{n+1}\sum_{j=1}^{t}l_j}$.

(8) P_{n+1} 进行如下操作：

(8-1)计算 $(g^{\sum_{j=1}^{t}l_j})^{d_{n+1}}=g^{d_{n+1}\sum_{j=1}^{t}l_j}$ 和 $g^{-d_{n+1}\sum_{j=1}^{t}l_j}$；

(8-2)然后解密得到自己的份额

$$s_{n+1}=Cg^{-d_{n+1}\sum_{j=1}^{t}l_j}=\sum_{i=1}^{t}s_i\omega_i(n+1)$$

收稿日期：2008-01-06. 作者简介：郝蓉（1976－），女，讲师. 基金项目：国家高科技研究发展计划资助项目(2003AA141120,2004AA001260)；国家重点基础研究发展规划资助项目(G1999035802).

验证新份额：判断等式

$$g^{s_{n+1}} = g^{k}\prod_{l=1}^{t-1}(g^{a_l})^{(n+1)^l}$$

是否成立，若成立，则新份额是正确的；否则，是错误的. 其中，g^k 和 g^{a_l} 是秘密分发时，公开地对秘密和多项式系数的承诺.

2 安全性攻击

下面，我们构造一个敌手 A 执行以下步骤来获得共享秘密和所有成员 $P_j(j=1,2,\cdots,n+1)$ 的份额：

(1)通过广播通道得到第(2-3)步的所有 K_i^j ($i=1,2,\cdots,t$; $j=1,2,\cdots,t$, 且 $i\neq j$)；

(2)然后计算 $K_i^j/K_i^{j-1}=g^{(k+d_{n+1})l_j}$；

(3)For $P_t=P_1$ to P_t

计算$\left(\prod_{j=1}^{t} g^{(k+d_{n+1})l_j}\right)/g^{(k+d_{n+1})l_i} = g^{(k+d_{n+1})(\sum_{j=1}^{t} l_j-l_i)}$；

(4)通过广播通道得到第(5-3)步的 $Q_i = s_i\omega_i(n+1)g^{(k+d_{n+1})(\sum_{j=1}^{t} l_j-l_i)}$ $(i=1,2,\cdots,t)$；

(5)然后计算 $s_i\omega_i(n+1) = Q_i/g^{(k+d_{n+1})(\sum_{j=1}^{t} l_j-l_i)}$ $(i=1,2,\cdots,t)$；

(6)再计算 $s_i = s_i\omega_i(n+1)/\omega_i(n+1)$，这里 $\omega_i(n+1) = \prod_{1\leqslant j\leqslant t, j\neq i}\frac{n+1-j}{i-j}$；

(7)插值计算共享秘密 $k = \sum_{i=1}^{t} s_i\omega_i(0)$；

(8)插值计算成员 $P_j(j=1,2,\cdots,n+1)$ 的份额 $s_{j1} = \sum_{i=1}^{t} s_i\omega_i(j)$，这里 $\omega_i(j) = \prod_{1\leqslant k\leqslant t, l\neq i}\frac{j-l}{i-l}$.

上述方法可获得共享秘密和所有成员 $P_j(j=1,2,\cdots,n+1)$ 的份额.

3 结 论

通过对李慧娴等提出协议[3]的安全性分析，指出了此协议可以完全泄漏共享的秘密和包括新成员份额在内的所有成员的份额，是完全不安全的.

参考文献：

[1] 于佳，李大兴，范玉玲. 基于加法共享的可验证秘密再分发协议[J]. 计算机研究与发展，2006，43(1)：23-27.
YU Jia, LI Daxing, FAN Yuling. Verifiable secret redistribution protocol based on additive sharing [J]. Journal of Computer Research and Development, 2006, 43(1): 23-27.

[2] YU Jia, KONG Fanyu, LI Daxing. Verifiable secret redistribution for proactive secret Sharing Schemes [J]. Journal of Shanghai Jiaotong University (Science), 2006, 11(2): 236-241.

[3] 李慧娴，程春甜，庞辽军. 一个可验证的秘密共享新个体加入协议[J]. 西安交通大学学报，2006，40(2)：207-210.
LI Huixian, CHENG Chuntian, PANG Liaojun. Verifiable protocol for member expansion in secret sharing schemes [J]. Journal of Xi′an Jiaotong University, 2006, 40(2): 207-210.

(编辑 刘杨)