无可信中心的(t, n)门限签名方案

王 斌 李建华
(上海交通大学电子工程系 上海 200030)

摘 要 在基于离散对数的安全机制的前提下讨论了(t, n)门限群签名方案.目前流行的门限签名方案一般可分为需要可信中心和不需要可信中心两类.由于在许多特定的应用环境下,一个可被所有成员信任的可信中心并不存在,所以不需要可信中心的门限群签名方案就显得很有吸引力.但已有的方案中使用了秘密共享技术,超过门限值的小组成员利用他们所掌握的秘密份额就能够恢复某个成员的私钥.为了解决这个问题,在新的方案中,利用联合秘密共享技术(joint secret sharing)解决了传统的秘密共享技术造成的成员的私钥泄露问题.

关键词 门限签名;秘密共享;可信中心
中图法分类号 TP309

(t, n) Threshold Signature Scheme Without a Trusted Party

WANG Bin LI Jian-Hua
(*Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai* 200030)

Abstract This paper discusses the (t, n) threshold signature scheme based on the difficulty of solving the discrete logarithm problem. All up-to-date solutions for threshold signature can be classified into the two categories: (1) solutions with the assistance of a trusted party (2) solutions without the assistance of a trusted party. Generally speaking, as an authority which can be trusted by all members doesn't exist, a threshold signature scheme without a trusted party appears more attractive. However, Secret Sharing technique used in previous schemes may cause some colluding members of the group to obtain secret keys of others. In order to solve the problem, authors present a new scheme by use of Joint Secret Sharing technique to protect secret keys of group members.

Keywords threshold signature; secret sharing; trusted party

1 引 言

在一个门限签名方案中,只有参与签名的小组成员数目大于或等于规定的门限值时才能生成群签名,而任何群签名的接收者都可以用公开的群公钥来验证群签名的正确性.由于门限签名需要多方的参与,与普通的数字签名相比,门限签名的安全性和健壮性有了很大的提高.1991 年 Desmedt 和 Frankel 提出了基于 RSA 的(t, n)门限签名方案[1],文献[2]则给出了一种基于离散对数的门限群签名方案.和基于 RSA 的方案相比,它具有实现方便的优点.不过这些方案都需要有一个可信中心来决定群私钥和小组成员的私钥.

Harn 提出了一种基于 ElGamal 签名的、不需要可信中心的门限群签名方案[3].由于在许多特定的应用环境下,一个可被所有小组成员信任的可信中心并不存在,所以不需要可信中心的门限群签名方

收稿日期:2001-12-28;修改稿收到日期:2003-03-07.**王 斌**,男,1976 年生,博士研究生,主要研究方向为安全组播、电子商务安全.E-mail:jxbin76@sina.com.**李建华**,男,1965 年生,教授,博士生导师,主要研究方向为数据通信与计算机通信网、网络安全技术.

案就显得很有吸引力.

然而,在 Harn 的方案中,每个小组成员首先确定自己的私钥,然后利用秘密共享技术把自己的私钥分割给其余的小组成员,这就意味着,超过门限值的小组成员联合起来,利用他们所掌握的秘密份额就能够恢复某个成员的私钥,在这个意义上,Harn 的方案是不安全的.而本文则利用联合秘密共享技术[4](joint secret sharing),由所有的小组成员来共同决定群公钥和小组成员的私钥.这样每个小组成员只了解群公钥,没有掌握与其它小组成员的私钥有关的任何信息.

2 改进的 ElGamal 签名方案

方案中使用的数字签名方案是基于 Agnew 在 1990 年提出的一种改进的 ElGamal 签名方案[5].下面先简单地介绍一下这个 ElGamal 签名方案.

首先选择一个大素数 p 和素域 Z_p 上的生成元 g,用户 U_i 从 $[1, p-1]$ 中选一个数 x_i 作为私钥,把 $y_i = g^{x_i} \bmod p$ 作为公钥.

如果用户 U_i 要对消息 m 进行签名,U_i 从 $[1, p-1]$ 中选一个随机数 k_i,计算 $r_i = g^{k_i} \bmod p$.然后解下面的同余式求出 s_i:

$$s_i = x_i m' - k_i r_i \bmod p - 1 \qquad (1)$$

$s_i \in [1, p-2]$,$m' = h(m)$,$h()$ 是一个单向哈希函数,用于增加消息 m 的冗余性.(r_i, s_i) 就代表用户 U_i 对消息 m 的签名.

接收方可按下式验证 U_i 对消息 m 的签名:

$$(y_i)^{m'} \equiv r_i^{r_i} g^{s_i} \bmod p \qquad (2)$$

3 无可信中心的 (t, n) 门限签名方案

先由所有的组成员选定公共参数,即安全的大素数 p 和 q(q 是 $p-1$ 的素因子,例如 p 的位长为 512 位,q 的位长为 160 位)以及元素 g(g 在素域 Z_p 上的阶为 q).

3.1 密钥生成阶段

首先,每个成员 U_i 对外公开自己的唯一标识号 x_i.根据事先确定的门限值 t,每个组成员 U_i 选定一个 $t-1$ 次的多项式 $f_i(x) \bmod q$,U_i 为其余 $n-1$ 个成员计算 $\lambda_{i,j} = f_i(x_j) \bmod q$,并通过广播方式将 $\lambda_{i,j}$ 发送给 U_j,注意到 $\lambda_{i,i} = f_i(x_i) \bmod q$,$U_i$ 保留 $\lambda_{i,i}$.

在每个成员都完成上面的步骤后,组成员 U_i 可以计算 $\lambda_i = \sum_{j=1}^{n} \lambda_{j,i} \bmod q$,即 $\lambda_i = \sum_{j=1}^{n} f_j(x_i) \bmod q$.现在定义一个新函数 $F(x) = \sum_{i=1}^{n} f_i(x) \bmod q$,虽然 U_i 不知道 $F(x)$,但不难知 $\lambda_i = F(x_i)$.U_i 在 $[1, p-1]$ 上选一个随机数 k_i,把 $X_i = \lambda_i k_i \bmod q$ 作为组成员 U_i 的秘钥,而 $y_i = g^{X_i} \bmod p$ 作为 U_i 的公钥.令 $r_i = g^{k_i} \bmod p$,U_i 把 r_i 通过广播的方式发给其它成员.

每个成员可计算 $R = \prod_{i=1}^{n} r_i \bmod p$.由于门限值为 t,t 个成员利用多项式插值 $F(0) = \left(\sum_{i=1}^{t} F(x_i) \cdot \prod_{j=1, j \neq i}^{t} \frac{(-x_j)}{(x_i - x_j)} \right) \bmod q$ 可以恢复 $F(0)$,然后就把 $y = g^{F(0)} \times R \bmod p$ 作为组的公钥,相应的组秘钥 x 为 $F(0) + \sum_{i=1}^{n} k_i \bmod q$.

3.2 部分签名生成阶段

首先经协商确定哪些组成员将参与群签名,参与群签名的组成员形成集合 S,在集合 S 中按成员编号的递增顺序来排列组成员.然后 S 中的每个成员 U_i 在 $[1, q-1]$ 上选一个新随机数 t_i,接下来 U_i 计算下面的等式:

$T_i = g^{t_i} \bmod p$ 以及 $z_i = g^{t_i \times (k_i)^{-1}} \bmod p$,其中 k_i 为组成员 U_i 在密钥生成阶段选择的随机数,k_i^{-1} 为 k_i 在素域 Z_q 上的逆元.U_i 把 T_i 和 z_i 通过广播的方式发送给参与签名的其它成员.

在收到其它成员发送的 T_i 和 z_i 后,U_i 从 S 中选最前面的 t 个成员,形成集合 S_t,集合 S_t 中也按成员编号的递增顺序来排列组成员.U_i 计算 $r = \prod_{U_j \in S_t} z_j \cdot \bmod p$,然后根据下面的同余式求解 s_i:

$$k_i s_i = (k_i \lambda_i C_i) \times h(m) - r \times t_i \bmod q \qquad (3)$$

上式等价于

$$s_i = (\lambda_i C_i) \times h(m) - r \times t_i \times (k_i)^{-1} \bmod q \qquad (4)$$

式(4)的 $C_i = \prod_{j=1, j \neq i}^{t} \frac{(-x_j)}{(x_i - x_j)}$,为插值系数.

根据式(3)可以验证

$$r_i^{s_i} (T_i)^r \equiv (y_i)^{h(m) C_i} \bmod p \qquad (5)$$

U_i 把 $(m, r_i, s_i, y_i, r, T_i, i)$ 发送给指定的群签名的生成者 DC(Designated Combiner),i 为序号,用于确定 C_i.

3.3 群签名的生成阶段

群签名的生成者 DC 先根据收到的签名验证同

余式(5)是否成立,成立则根据集合 S_t计算:

$$s=\sum_{U_i\in S_t}s_i,$$

即

$$s=\sum_{U_i\in S_t}(\lambda_i C_i)h(m)-r\sum_{U_i\in S_t}(t_i\times k_i^{-1})\bmod q.$$

那么最终的群签名为(m, s, r, R).

任何群签名的接收者都可以验证下面的等式是否成立:

$$g^s r^r\equiv(y\times R^{-1})^{h(m)}\bmod p \tag{6}$$

上式中 R^{-1}为 R 在素域 Z_p上的逆元.由于

$$g^s\times g^{r\sum_{U_i\in S_t}(k_i)^{-1}}\equiv g^{h(m)\sum_{U_i\in S_t}\lambda_i C_i}\bmod p \tag{7}$$

且有$g^{\sum_{U_i\in S_t}\lambda_i C_i}\bmod p=g^{F(0)}\bmod p$,可知式(6)成立.

4　安全分析

接下来我们将通过以下几个定理分析本文方案的安全性.

定理 1.　根据组的公钥 y 和各个成员的公钥 y_i来分别推导出组的秘钥 x 和各个成员的密钥 X_i的困难性等价于求解离散对数问题.

证明.　组的公钥为 $y=g^{F(0)}\times R\bmod p$,各个成员的公钥 $y_i=g^{X_i}\bmod p$. $X_i=\lambda_i k_i\bmod q$,由于 k_i是成员 U_i随机选择的,确保了 X_i对组内部的其它成员来说是一个随机变量.由 $y_i=g^{X_i}\bmod p$,我们知道根据 y_i推导 X_i等价于求解离散对数问题.同理可知根据 y 要推导出 x 等价于求解离散对数问题.此外,组的秘钥 x 为 $F(0)+\sum_{i=1}^{n}k_i\bmod q$,知道 $F(0)$和所有的 k_i也可以推导出 x,而这就意味着求解所有的 k_i或所有的成员都泄露自己选择的 k_i.由于 $X_i=\lambda_i k_i\bmod q$,求解所有的 k_i同样等价于求解离散对数问题,而所有的成员都泄露自己选择的 k_i,则意味着方案已经失去了使用意义.　证毕.

定理 2.　即使一个攻击者获得了一个或多个部分签名 s_i,求解成员的密钥 X_i的难度至少等价于破解改进的 ElGamal 签名方案.

证明.　在获得了部分签名 s_i后,一个攻击者可以列出等式

$$s_i=(\lambda_i C_i)\times h(m)-r\times t_i\times(k_i)^{-1}\bmod q \tag{8}$$

和改进的 ElGamal 签名方案的等式

$$s_i=x_i m'-k_i r_i\bmod p-1$$

进行比较,可知求解($\lambda_i C_i$)或 $t_i\times(k_i)^{-1}$等价于破解改进的 ElGamal 签名方案.由于 $X_i=\lambda_i k_i\bmod q$,定理得证.即使攻击者和 t 个内部组成员合谋获得 $\lambda_i=F(x_i)$,从式(8)中解出 $t_i\times(k_i)^{-1}$,但 t_i的存在保证了$(k_i)^{-1}$是安全的.因此在这种情况下成员的密钥 X_i仍是安全的.　证毕.

定理 3.　即使一个攻击者获得了一个或多个群签名 s,求解组秘钥 x 的难度不低于破解改进的 ElGamal 签名方案.

证明.　获得群签名后,攻击者可以列出等式:

$$s=\sum_{i=1}^{t}(\lambda_i C_i)h(m)-r\sum_{i=1}^{t}(t_i\times k_i^{-1})\bmod q \tag{9}$$

在上式中,s, r, C_i和 $h(m)$是已知的.和改进的 ElGamal 签名方案的等式比较可知道它的安全性不低于破解改进的 ElGamal 签名方案.即使攻击者能够和 t 个内部组成员合谋获得 λ_i.此时上式仍然存在 t 个未知数,相应地组秘钥 x 仍是安全的.　证毕.

定理 4.　在部分签名的生成阶段,一个攻击者不能假冒合法用户提交一个正确的部分签名.

证明.设攻击者 A_i试图假冒用户 U_i, A_i随机选择了$\overline{t_i}$和$\overline{k_i}$,则$\overline{z_i}=g^{\overline{t_i}\times(\overline{k_i})^{-1}}\bmod p$. A_i把$\overline{z_i}$通过广播的方式发送给参与签名的其他成员.则有$\overline{r}=\left(\prod_{U_j\in S_t}^{j\neq i}z_j\right)\times\overline{z_i}\bmod p$.但只知道$\overline{r}$,不知道用户 U_i的密钥 X_i, A_i无法提交完整的部分签名信息,因为 A_i无法通过部分签名的生成等式(3)求出一个 s_i,使部分签名的验证等式(5)成立.定理得证.　证毕.

定理 5.　即使已获得一个合法群签名,一个攻击者也不能为自己选定的一条消息伪造一个合法群签名.

证明.　假设一个攻击者 A_i已获得一个合法群签名(m, s, r, R), A_i选定一条消息$\overline{m}$.注意到 R 是固定的,我们分析一下 A_i是否有可能伪造一个合法群签名($\overline{m}$, $\overline{s}$, $\overline{r}$, R).根据(m, s, r, R), A_i列出式(9).

A_i在式(9)的两端同乘以 $h^{-1}(m)\times h(\overline{m})$,可得下式:

$$\begin{aligned}&h^{-1}(m)\times h(\overline{m})\times s\\&=\sum_{i=1}^{t}(\lambda_i C_i)h(\overline{m})-h^{-1}(m)\times h(\overline{m})\times\\&\quad r\sum_{i=1}^{t}(t_i\times k_i^{-1})\bmod q\end{aligned} \tag{10}$$

令 $h^{-1}(m)\times h(\overline{m})\times s=\overline{s}$,要使验证等式(6)成立, A_i需根据下式:

$$\bar{r}^{\bar{r}} = g^{h^{-1}(m)\times h(\bar{m})\times r\sum_{i=1}^{t}(t_i\times k_i^{-1})} \bmod p$$

解出$\bar{r}$.然而,其中的$\sum_{i=1}^{t}(t_i\times k_i^{-1})$对$A_i$来说是未知的,$A_i$只能通过猜测的办法求出一个$\bar{r}$使得验证等式(6)成立.定理得证. 证毕.

5 小 结

在分析 Harn 提出的不需要可信中心的门限群签名方案存在的安全问题的基础上,利用联合秘密共享技术来对原方案进行了改进,使得安全性得到了提高.原方案容易使成员的私人密钥被 t 个成员利用多项式插值解出,新方案则由组成员共同生成群公钥和私人密钥,避免了泄露成员的私人密钥的问题.安全分析表明新方案是安全的.

参 考 文 献

1 Desmedt Y, Frankel Y. Shared generation of authenticators. In: Proceedings of Crypto '91, Santa Barbara, California, USA, 1991. 457～469

2 Wang C T, Lin C H, Chang C C. Threshold signature schemes with traceable signers in group communications. Computer Communications, 1998, 21(8): 771～776

3 Harn L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. IEE Proceedings of Computers and Digital and Technique, 1994, 141(5): 307～313

4 Rosario G, Stanislaw J, Hugo K. Robust threshold DSS signatures. Information and Computation, 2001, 164(1): 54～84

5 Agnew G B, Mulin R C, Vanstone S A. Improved digital signature scheme based on discrete exponentiation. Electronic Letters, 1990, 26(14): 1024～1025

WANG Bin, born in 1976, Ph. D. candidate. His research interests include multicast security and security problems related with electronic commerce.

LI Jian-Hua, born in 1965, professor, Ph. D. supervisor. His research interests include data communication, computer communication network, network security.