文章编号: 1007- 2985(2003)03- 0090- 02

基于 Meta- El Gamal 方案的多重签名体制的改进

鲁荣波[1,2], 朱西平[1,2]
(1. 吉首大学数学与计算机科学系, 湖南 吉首 416000; 2. 西南交通大学
计算机与通信工程学院, 四川 成都 610031)

摘 要: 对 Meta- El Gamal 方案的多重签名体制进行分析, 发现该体制存在一个安全漏洞, 即多个签名者如果在生成自己的密钥时相互合作就能达到日后否认消息签名的攻击手段. 通过改进 Meta- El Gamal 多重签名体制的密钥生成部分, 避免了上述攻击, 体制的安全性得到提高.

关键词: Meta- El Gamal; 多重签名体制; 密钥生成
中图分类号: TN915.08 文献标识码: A

数字签字在信息安全, 包括身份验证、数据完整、不可否认性以及匿名性等方面有广泛应用, 特别是在大型网络安全通信中的密钥分配、认证, 以及电子商务系统中具有重要作用. 数字签字在许多情况下往往不仅需要单人签名, 而且需要多人合作对同一份消息共同进行签名, 即所谓的多重签名问题. 最简单的解决办法是每个签名者独立地对同一份消息签名, 他们的签名合起来作为多重签名. 但这种方式不能称为合作, 而且无法令人满意的是, 随着签名者的个数增加签名长度成倍增加, 资源浪费严重. 于是专家提出了各种基于离散对数的多重签名体制, 如基于 Meta- El Gamal 方案的多重签名体制[1,2], 该体制在合作签名者和验证者都遵守签名协议的假设下安全等价于离散对数问题[3]. 但这只是一种理想状态. 经研究发现, 该体制存在一个安全漏洞, 即如果多个签名者在生成自己的密钥时相互合作, 就能达到日后否认消息签名的目的.

1 Meta- El Gamal 多重签名体制及安全性分析

一可信中心选择 1 个大素数 p, 生成元 $a \quad Z_p^*$ 作为系统参数公开. 签名者 $P_i(i = 1, 2, \quad , n)$ 选择 1 个随机数 $x_i \quad Z_{p-1}^*$, 计算 $y_i = a^{x_i} \bmod p$. P_i 公开 y_i, 密藏 x_i. 这些值对所有被签名的消息是不变的.

在多重签名中, y_i, x_i 分别为 P_i 的公开密钥和秘密密钥. P_i 选择 1 个随机数 $k_i \quad Z_{p-1}^*$, 并且计算 $r_i = a^{k_i} \bmod p$, 然后广播给所有其他的签名者, 这样每个签名者可计算 $r = \prod_{i=1}^{n} r_i \bmod p$. 现在每个签名者通过下面的公式可计算他的签名参数 S_i, $S_i = (x_i(m + r) - k_i) \bmod (p - 1)$, 并传送给另外一个还知道 m 和 r 的职员, 该职员的任务是通过同余式 $y_i^{m+r} = r_i \quad a^{S_i} \bmod p$ 检查每个单个的签名. 最后计算消息 m 的多重签名 $S = \sum_{i=1}^{n} S_i \bmod (p - 1)$. 三维数组 (m, r, S) 是消息 m 的多重签名, 可通过检查同余式 $y^{m+r} = r \quad a^S \bmod p$ 得到验证, 这里 $y = \prod_{i=1}^{n} y_i \bmod p$.

假设攻击者团体是 $\{p_1, p_2, \quad , p_t\}$, 他们与 $\{p_{t+1}, p_{t+2}, \quad , p_n\}$ 合作对消息 m 进行签名, 目的是伪造签名, 这里只考虑:

( ) 攻击者团体根据基本的多重签名体制产生自己的密钥 $x_1, x_2, \quad , x_t, z$ 满足

$$\sum_{i=1}^{t} x_i = 0 \bmod (p - 1); \tag{1}$$

( ) 攻击者团体不遵守协议随机产生 $k_i \quad Z_{p-1}^*(i = 1, 2, \quad , t)$, 而是协作生成 k_i, 满足

$$\sum_{i=1}^{t} k_i = 0 \bmod (p - 1).$$

收稿日期: 2003- 05- 13
作者简介: 鲁荣波(1970-), 男, 湖南省慈利县人, 西南交通大学通信与信息系统专业硕士研究生, 吉首大学数学与计算机科学系讲师, 主要从事码分多址与个人通信、信息安全理论的研究.

攻击者团体与$\{p_{t+1}, p_{t+2}, \ldots, p_n\}$一起对消息 m 多重签名, 签名为(m, r, s). 显然签名满足验证等式. (m, r, s) 即可认为是$\{p_1, p_2, \ldots, p_t\}$ 对 m 的签名, 也可认为是$\{p_{t+1}, p_{t+2}, \ldots, p_n\}$ 对 m 的签名.

在$\{p_1, p_2, \ldots, p_t\}$ 相互之间无条件信任的假设下, 他们只需在一起商定各自的 x_i, k_i 即可. 在$\{p_1, p_2, \ldots, p_t\}$ 相互之间没有无条件信任的假设下, 祈明等[4] 描述了一种可以使 p_i 保密k_i 的计算方法, 这也适合于 x_i 的计算. 如果基本的 Meta- El Gamal 多重签名体制不做任何技术上的改进, 那么$\{p_1, p_2, \ldots, p_t\}$ 能获得$\{p_{t+1}, p_{t+2}, \ldots, p_n\}$ 对 m 的签名(m, r, s).[5]

2　改进的多重签名体制及其安全性分析

基本的 Meta- El Gamal 签名体制存在安全漏洞, 是由于该体制具有由各签名者独自生成密钥的弱点而造成的. 经研究发现, 如果密钥的生成方式是由中心和签名者协作完成, 并且保证密钥仍然是随机的话, 那么就能避免上面的否认攻击. 下面笔者对 Meta- El Gamal 签名体制进行了改进.

一可信中心选择 1 个大素数 p, 生成元 $a \in Z_p^*$ 作为系统参数公开.

(1) 在中心完全可信的假设下, 在协议生成的密钥生成部分签名者 P_i 选择 1 个随机数 $x_{p_i} \in Z_{p-1}^*$, 计算 $y_{p_i} = a^{x_{p_i}} \bmod p$, 发送给中心. 中心再选择 1 个随机数 $L_i \in Z_{p-1}^*$, 计算 $y_i = y_{p_i} a^{L_i} \bmod p$, 计算 L_i, y_i 发送给p_i, 签名者 p_i 计算其密钥$x_i = x_{p_i} + L_i \bmod p$ 并公开密钥y_i. 最后中心广播 y_i, 以便其他签名者验证和查找, 而协议的其它部分不变. 这样, 攻击者团体$\{p_1, p_2, \ldots, p_t\}$ 无法计算满足(1) 式的 x_i, 从而避免了的安全上的攻击, 且协议的安全性仍等价于离散对数性.

(2) 在签名者没有无条件信任中心的假设下, 中心广播一单向 Hash 函数$f: Z_p \times Z \to \{0, 1, \ldots, 2^R - 1\}$(此处 R 为安全参数). 在协议的密钥生成部分签名者 $x_i (i = 1, 2, \ldots, n)$ 选择 1 个随机数 $x_{p_i} \in Z_{p-1}^*$, 计算 $y_{p_i} = a^{x_{p_i}} \bmod p$, 发送给中心. 中心再选择 1 个随机数 $L_i \in Z_{p-1}^*$, 计算 $y_i = y_{p_i} a^{f(y_{p_i}, L_i)} \bmod p$, 并将 L_i, y_{p_i}, y_i 发送给 p_i, 签名者 p_i 计算其密钥 $x_i = x_{p_i} + f(y_{p_i}, L_i) \bmod p$ 并公开密钥 y_i. 最后中心广播 L_i, y_{p_i}, y_i, 以便其他签名者验证(包括验证密钥生成) 和查找, 而协议的其它内容不变.

显然, 改进(1) 中密钥是随机的, 而改进(2) 中由于$f(y_{p_i}, L_i)$ 与 x_{p_i} 相关, 不能保证密钥的随机性(或在密钥空间均匀分布), 且即使中心与攻击者团体$\{p_1, p_2, \ldots, p_t\}$ 合作也难以产生满足(1) 式的 x_i, 所以f 的选择很重要.

(3) 对于上面所述方案中 k_i 的生成, 可再选择一单向函数 $: Z_{p-1}^* \to Z_{p-1}^*$, p_i 随机选择 $_i \in Z_{p-1}^*$, 计算 $k_i = (_i)$. 函数的要求是概率$P_r\{$组合$\{_1, _2, \ldots, _n\}: \sum_{i=1}^{n} k_i = 0, k_i = (_i), n \in \mathbf{N}\}$ 几乎接近于 0.

3　结语

密钥生成的改进对于其它基于离散对数问题的签名体制或多重签名体制也是有效的. 目前, 多重签名体制绝大多数是从单签名体制扩展而来, 由于有限域的相关性质, 其密钥生成会发生很大变化. 笔者的研究对多重签名及基于离散对数问题的签名体制有一定的借鉴价值.

参考文献:

[1] 王育民, 刘建伟. 通信网的安全理论与技术 [M]. 西安: 西安电子科技大学出版社, 1999.

[2] 曹珍富. 公钥密码学 [M]. 哈尔滨: 黑龙江教育出版社, 1993.

[3] JI J, ZHAO R J. Digital Multisignature Schemes Based on the Schnorr Scheme [A]. Advance in Cryptography- CHINACRYPT 96 [C]. 1996. 170- 176.

[4] 祈　明, HARNL. 基于离散对数的若干新型代理签名方案 [J]. 电子学报, 2000, 28(11): 114- 115.

[5] BYOUNGCHEON L, HEESUN K, KWANGJO K. Strong Proxy Signature and Its Applications [A]. Symposium on Cryptography and Information Security [C]. 2001. 104- 110.

Modification of Multisignature Schemes Based on Meta- El Gamal

LU Rong-bo[1,2], ZHU Xi-ping[1,2]

(1. Dept. of Mathematic and Computer Science, Jishou University, Jishou 416000, Hunan China; 2. College of Computer and Communication Engineering, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: This paper shows the security flaw which extends from the multisignature scheme based on Meta- El Gamal, i. e., the attackers can deny having taken part in the process of signing some message with others. A modification is made for these schemes　key generations, which can efficiently avoid this attack.

Key words: Meta- El Gamal; multisignature; schemes　key generation