第 19 卷 第 3 期 电子科学学刊 Vol.19 No.3
1997 年 5 月 JOURNAL OF ELECTRONICS May 1997

两类 ElGamal 型数字签名方案的安全性和性能分析 [1]

祁 明 肖国镇 *

(华南理工大学网络中心 广州 510641)
*(西安电子科技大学信息保密研究所 西安 710071)

摘 要 本文对两类 ElGamal 型签名方案的安全性和基于两类签名方案的通行字认证方案进行了分析和讨论. 通过对这些问题的研究, 可以对两类 ElGamal 型签名方案的安全性、性能和相互关系有新的认识.

关键词 ElGamal 签名, 多重签名, 通行字认证

中图号 TN918.1

1 引 言

最近, Nyberg 和 Rueppel 对 p 型方案和 MR(p) 型方案及其变型方案之间的等效性 (即各签名之间的可转换性) 进行了研究 [1]. 由于目前还未能证明 p 型方案和 MR(p) 型方案等效, 从而使得关于这两类签名方案之间相互关系的研究显得十分必要. 本文首先讨论了两类签名方案的安全性及其分类, 提出了关于 p 型方案的一个改进型方案, 随后, 我们在 MR(p) 型方案上建立了两个多重签名方案, 并对基于 ElGamal 签名方案的 Chang-Liao 通行字认证方案 [2] 进行了改进和推广.

2 安全性及其分类

本节中, 我们首先对两类签名方案面临的各种攻击进行了分析, 提出了按照攻击的有效性进行分类的思想, 并对加强 p 型方案的安全性提出了一个改进型方案.

2.1 代换攻击和方案分类

对广义 p 型方案而言, 当前面临的主要攻击是代换攻击, 即对某些 p 型方案而言, 伪造者可以从关于报文 m 的有效签名 (r,s) 伪造出关于报文 m' 的有效签名 (r',s')[3]. 这里我们将指出, 除了已经受到攻击的一些 p 型方案外, 我们可采用与攻击 Yen-Laih 方案相类似的方法 [4] 对其它一些 p 型方案进行代换攻击. 例如, 当 $(a,b,c)=(1,-rs,m)$ 时所对应的签名方程为 $r=g^k \bmod p$ 和 $m=rsk+x \bmod q$, 相应的验证方程为 $g^m=r^{rs}y \bmod p$. 如果关于报文 m 的签名为 (r,s), 可令 $m'=m+trs \bmod q$, $r'=rg^t \bmod p$, $s'=r(rg^t \bmod p)^{-1}s \bmod q$, 则 (m',r',s') 仍满足验证方程.

为了便于对两类方案的安全性进行分析, 我们可将广义 p 型方案所包括的所有 ElGamal 型签名方案按代换攻击的有效性暂时分成以下三类: (1) 安全方案: 各种代换攻击无效. (2) 比

[1] 1995-03-20 收到, 1996-06-05 定稿

较安全方案：代换攻击有效，但伪造的报文 m' 难以自由控制. (3) 不安全方案：代换攻击有效，而且伪造的报文 m' 容易自由控制.

对广义 MR(p) 型方案而言，虽然也存在类似的代换攻击 [5]，但由于参数 (a,b,c) 中已不含 m，则利用 m 对某些 p 型方案有效的一些攻击方法对 MR(p) 型方案不一定就有效. 这里我们指出，当 $b=s$ 或 $c=s$ 时，伪造者可以利用报文还原方程 $m=y^{a^{-1}b}g^{a^{-1}c}r \bmod p$ 对 MR(p) 型方案进行另一种新的代换攻击. 例如，当 $c=s$ 时，若令 $\overline{m}=mg^u \bmod p$, $u\in z_q$, $\overline{r}=r$, $\overline{s}=s+au$，则 $(\overline{m},\overline{r},\overline{s})$ 满足报文还原方程：$y^{a^{-1}b}g^{a^{-1}\overline{s}}\overline{r} \bmod p = y^{-a^{-1}b}g^{a^{-1}s}rg^u \bmod p = mg^u \bmod p = \overline{m}$. 要使 $\overline{m}$ 有意义，则须确定 u 的值，这等于求离散对数. 因此，受到这种攻击的 MR(p) 型方案可被认为是比较安全的. 从这里我们已经看出，由于两类 ElGamal 型签名方案受到的攻击方式不全相同，所以当按攻击的有效性对两类 ElGamal 型签名方案进行分类时，两类方案的各分类之间并无必然的联系，也就是说，不能从某个 p 型方案具有某种安全性推出相应的 MR(p) 型方案也具有某种安全性.

2.2　安全性改进

这里我们提出了一个关于 p 型方案的改进型方案，该方案是 Chang-Liao 通行字认证方案的变型和推广 [2]. 改进型方案的特点是将原签名方案中的 s 隐蔽，既可使伪造者无法利用 s 进行通常的代换攻击，又可增加签名方程中的未知数 $(x,k,s$ 对伪造者均不知)，从而防止由于 k 的重复使用而暴露密钥 x. 我们在广义 p 型方案上建立了改进型方案，其详细情况由表 1 给出.

表 1　广义 p 型方案的改进

签名方案	分类		
	I (a 含 s)	II (b 含 s)	III (c 含 x)
签名方程	$r=g^k \bmod p$ $ax=bk+c \bmod q$ $A=y^t \bmod p$ $B=t+a \bmod q$	$r=g^k \bmod p$ $ax=bk+c \bmod q$ $A=r^t \bmod p$ $B=t+b \bmod q$	$r=g^k \bmod p$ $ax=bk+c \bmod q$ $A=g^t \bmod p$ $B=t+c \bmod q$
签名	(r,A,B)	(r,A,B)	(r,A,B)
签名验证	$A'=y^B(r^bg^c)^{-1} \bmod p$	$A'=r^B(g^{-c}y^a)^{-1} \bmod p$	$A'=g^B(r^{-b}y^a)^{-1} \bmod p$
	如果 $A'=A$ 成立，则签名被接受		

3　多重签名

由于多重签名的实用性，关于它的研究日益受到重视. 已有的多重签名方案都是基于 p 型方案之上的，而本文中我们在 MR(p) 型方案上建立了多重签名方案.

3.1　广义 MR(p) 型方案上的多重签名

与广义 p 型方案上的多重签名类似，可将广义 MR(p) 型方案中的签名方程改为：$r=mg^{-k} \bmod p, r'=r \bmod q$, $ak=bx+cs \bmod q$. 每个 U_i 从 x_i 和 k_i 得到 y_i 和 r_i' 后，可计算 $r'=\prod_{i=1}^n r_i' \bmod q$ 并从 $ak_i=bx_i+cs_i \bmod q$ 中求得 s_i，此时参数 (a,b,c) 是来自 $(r',m,1)$ 的 3 个参数，与每个 U_i 对应的报文还原方程为 $m=y_i^{a^{-1}b}g^{a^{-1}cs_i}r_i \bmod p$. 与许多已有的构造多重签名的方法类似，我们可由多重签名 (r,s) 和报文还原方程得到

$$m^n=(\prod_{i=1}^n y_i)^{a^{-1}b}g^{a^{-1}c\sum_{i=1}^n s_i}(\prod_{i=1}^n r_i) \bmod p = y^{a^{-1}b}g^{a^{-1}cs}r \bmod p = c \bmod p.$$

为了还原报文 m, 可假设 $gcd(n,p-1)=1$, 从而多项式 $p(x)=x^n-c \bmod p$ 在 Z_p 中有唯一的根且有等式 $x-m=gcd(x^n-c,x^p-x)$ 成立, 使用欧几里得算法, 签名收方可计算 $x-m \bmod p$, 从而可还原报文 m . 除此之外, 我们还可将每个 U_i 对 m 进行的签名改成对 $\overline{m}=m^{1/n}(\overline{m}\in Z_p)$ 进行签名. 按上述方法可得与每个 U_i 对应的报文还原方程为: $\overline{m}=y_i^{a^{-1}b}g^{a^{-1}cs_i}r_i \bmod p$. 签名收方在收到多重签名 $(r,s)=(\prod_{i=1}^{n}r_i,\sum_{i=1}^{n}s_i)$ 后可得: $m=\overline{m}^n=y^{a^{-1}b}g^{a^{-1}cs}r \bmod p$.

4 通行字认证

4.1 CL 通行字认证方案

最近, Chang 和 Liao 基于 ElGamal 签名方案建立了一个通行字认证方案 (简称 CL 方案)[2], 该方案具有系统不需存贮用户任何数据的特点, 而且任何人不可能用截获的认证数据对系统进行非法访问. CL 方案有两个弱点, 一是口令生成中心 (Password Gemeration Center, PGC) 对随机数 k 不可重复使用 (与 ElGamal 签名方案相同), 否则两个用户 U_i 和 U_j 合作便可求得系统密钥 x, 为此, PGC 不得不对选用的随机数 k 进行登记和存贮. 另外, 由于系统不存贮用户任何数据, 从而无法对通行字的使用进行调控. 为了克服这些弱点, 我们在下面对加强型 ElGamal 签名 [6] 稍做改进的基础上提出了一个与 CL 方案类似的通行字认证方案, 并将 CL 方案推广到广义 p 型方案和广义 MR(p) 型方案上. 由于加强型方案和原 ElGamal 签名方案十分类似, 这里不再单独介绍, 有关改动将在下面给出说明.

4.2 CL 方案的改进和推广

参数选取 p 是大素数, $p-1$ 有两个大素数因子 p_1 和 q_1,$n=p_1\cdot q_1$, $g\in$GF(p) 为本原元素, $x(1<x<n)$ 和 $y=g^x \bmod p$,$z=y^x=g^{x^2} \bmod p$ 是系统的密钥和相应的两个公钥.

通行字产生 用户 U_i 将 ID_i 送 PGC,PGC 选随机数 $t_i(0<t_i<n)$ 且 $(t_i,p-1)=1$, 由 t_i 可得 $k_i=t_i^2 \bmod p-1$, 并由签名方程 $r_i=g^{k_i} \bmod p$, $\mathrm{ID}_i=xr_i+t_iv_i \bmod p-1$ 求得 (r_i,v_i), 再计算 $s_i=v_i^2 \bmod p-1$, 则用户 U_i 的通行字 $\mathrm{PW}_i=(r_i,s_i)$. PGC 将 PW_i 和 r_i 分别秘密地送用户 U_i 和 S . 易验证通行字 (r_i,s_i) 满足 $g^{\mathrm{ID}_i^2}z^{r_i^2}=y^{2r_i\mathrm{ID}_i}r_i^{s_i} \bmod p$

用户访问 用户 U_i 选随机数 $w\in(1,p-1)$, 计算 $A'=r_i^w \bmod p$, $B=w+s_if(A,T) \bmod p-1$, 然后将认证数据 $C=(\mathrm{ID}_i,A,B,T)$ 送系统 S .

系统验证 先检查时间差 ΔT, 并利用存贮的 r_i 和 C 计算 $A'=r_i^B[(y^{-2r_i\mathrm{ID}_i}g^{\mathrm{ID}_i^2}z^{r_i^2})^{-1}]^{f(A,T)} \bmod p$, 如果 $A'=A$, 则系统接受用户访问.

关于新方案的安全性以及新方案与 CL 方案的比较有以下几点说明:

(1) 在加强型 ElGamal 签名方案中, 签名实际上是 (r_i,v_i), 如果直接利用该方案构造通行字认证方案, 当随机数 t_i 被重复使用时, 仍不可防止两人合作所进行的攻击. 而使用 (r_i,s_i) 作为通行字后, 即使 t_i 被重复使用 (此时 $r_i=r_j$), 两个伪造者仍难以从 $\mathrm{ID}_i=xr_i+t_iv_i \bmod p-1$ 和 $\mathrm{ID}_j=xr_i+t_iv_j \bmod p-1$ 求得 x, 因为要求 x, 必须知道 v_i 和 v_j, 若不知道 n 的分解, 则难以从 s_i 和 s_j 通过求平方根获得 v_i 和 v_j .

(2) 新方案的认证数据 C 中不含 r_i, 而是由系统对 r_i 进行存贮和调用. 这样做既可以使系统利用 r_i 对 PW_i 的使用进行控制 (如过期通行字) , 又可防止他人对废止的 PW_i 利用代换攻击进行通行字伪造. 当然, 系统存贮 r_i 比由用户传送 r_i 更安全, 即使系统泄露 r_i, 如同 C 被截获一样, 任何人也无法利用 r_i 求得 s_i, 并对系统进行非法访问, 更无法从 r_i 求得系统密钥 x .

5 结束语

通过对上述问题的研究，我们对这两类 ElGamal 型签名方案的安全性、性能和相互关系有了新的认识．由于种种原因，我们还未能对 MR(p) 型方案的安全性做必要的改进，基于 MR(p) 型方案上的多重签名由于受到某些限制还不十分有效，在这些方面还有待做进一步的工作．

参 考 文 献

[1] Nyberg K, Rueppel R A. Message recovery for signature schemes based on the discrete logarithm problem, Proc. of Eurocryrd'94, London: 1994, 175–189.

[2] Chang C C, Lao W Y. A remote password authentication based on ElGamal's signature scheme, Computer and Security, 1994, 13(2): 137–144.

[3] ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithm, IEEE Trans. on IT, 1985, IT-31(4): 469–472.

[4] Yen S M, Laih C S. New digital signature scheme based on discrete logarithm, Electron. Lett., 1993, 29(12): 1120–1121.

[5] Nyberg K. Comment: New digital signature scheme based on discrete logarithm, Electron. Lett., 1994, 30(6): 481.

[6] He J, Kiesler T. Enhancing the security of ElGamal's signature scheme. IEE Proc.-E, 1994. 141(4): 249–252.

SECURITY AND PERFORMANCE ANALYSIS OF TWO KINDS OF ELGAMAL SIGNATURE SCHEMES

Qi Ming　　Xiao Guozhen*

(*Network Center of SCUT, Guangzhou* 510641)

*(*Institute of Information Security, Xidian University, Xi'an* 710071)

Abstract　The security relationship between p-schemes and MR(p)-schemes is analysed and their security classes are given. In addition, some multisignature schemes based on MR(p)-schemes and some password authentication schemes based on improved ElGamal signature schemes are proposed. The results may be helpful for new understanding of the security, performance and relationship of two kinds of ElGamal type signature schemes.

Key words　ElGamal signature, Multisgnature, Password authentication

祁　明：　男，1957 年生，博士后，主要从事认证理论和计算机安全的研究．
肖国镇：　男，1934 年生，教授，博士生导师，主要研究领域为编码和流密码．