第 22 卷 第 5 期 电 子 科 学 学 刊 Vol.22 No.5
2000 年 9 月 JOURNAL OF ELECTRONICS Sept. 2000

关于“两类 ElGamal 型数字签名方案的安全性和性能分析”的讨论 [1]

邵祖华

(中国工商银行，杭州金融管理干部学院 杭州 310012)

摘 要 为了加强 ElGamal 型数字签名方案的安全性，最近祁明等人对两类 ElGamal 型数字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，并且提出了两类改进型的方案．本文首先指出了他们提出的第一个 p 型方案是不安全的，攻击者可以伪造任意消息的数字签名．本文证明了广义 ElGamal 型数字签名方案都不能抵御代换攻击．本文最后还证明了他们提出的两类改进型方案也不能抵御同态攻击，因而并不具有所说的安全性．

关键词 密码分析，数字签名方案，同态攻击，代换攻击，通行字认证

中图号 TN918.1

1 引 言

最近，祁明等人在电子科学学刊 1997 年第 3 期上发表了一篇题为“两类 ElGamal 型数字签名方案的安全性和性能分析”的文章 [1](以下简称文献 [1])．该文对两类 ElGamal 型数字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，并且提出了两类改进型的方案．该文认为，“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”。

本文首先指出文献 [1] 中讨论的第一个 p 型方案是不安全的，攻击者可以伪造任意消息的数字签名。本文又指出，文献 [1] 对广义 p 型 ElGamal 型数字签名方案的安全分类是错误的。如果不使用单向函数，就不存在可以抵御代换攻击的安全 ElGamal 型数字签名方案。本文还分析了文献 [1] 提出的 p 型方案的改进型方案，推导出它的真正的签名方程。它不但不能抵御同态攻击，而且许多改进型方案不能抵御代换攻击。本文最后分析了文献 [1] 对于 Chang-Liao 通行字认证方案 [2] 的改进和推广，指明了改进型方案的安全性没有加强，仍然不能抵御同态攻击。如果会话密钥被重复使用，攻击者可以求出系统密钥。

本文认为，由于文献 [1] 未能完成自己提出任务，仍有必要对两类 ElGamal 型签名方案的安全性、性能和相互关系等问题，作进一步的分析和讨论。

2 一个不安全的 ElGamal 型签名方案

文献 [1] 在研究 ElGamal 型签名方案的安全性时，列举了一个例子。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 $g^m=r^{rs}y \bmod p$．文献 [1] 正确地给出了代换攻击的方法．然而这个方案本身是不安全的。 Harn[3] 在研究广义 ElGamal 型签名方案时，已经指出 rs 不能组合在一起，否则攻击者可以伪造任意消息 m 的数字签名。

首先计算 $R=g^m/y \bmod p$.

任选一个整数 a，求 a 的逆 b，即 $ab=1 \bmod q$.

[1] 1998-01-13 收到，1999-09-30 定稿

计算 $r = R^b \bmod p$，即 $r^a = R \bmod p$.

再求 $s = a/r \bmod q$.

于是 $g^m = r^{rs} y \bmod p$.

这样，消息 m 的签名就是 (r, s)。

3 代换攻击和安全分类

文献 [1] 认为，对于广义 p 型方案，当前面临的主要攻击是代换攻击 [4,5]。所谓代换攻击，是指攻击者从一个已知的消息 m 的真实签名 (r, s) 推导出另一个消息 m' 的有效签名 (r', s')。文献 [1] 提出，“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。”

文献 [1] 只提出分类的概念，并没有给出具体的分类。

Harn[3] 在研究广义 ElGamal 型签名方案时，已经指出了，如果使用单向函数，总共有 18 个安全的方案。如果存在第 (3) 类方案，攻击者可以自由控制伪造的报文 m'，那么他们也可以自由控制伪造的报文 $H(m')$。然而，据我们所知，并没有可以自由控制伪造的报文 $H(m')$ 的方法，因此第 (3) 类是空集。

其次，我们可以给出 18 个广义 ElGamal 型签名方案的代换攻击方法如下：

(1) $y^m = r^r g^s \bmod p$, $y^{m+r} = (yr)^r g^s \bmod p$, $y^{(m+r)/r} = (yr) g^{s/r} \bmod p$, $y^{r'(m+r)/r} = (yr)^{r'} g^{r's/r} \bmod p$, $r' = yr \bmod p$, $m' = r'(m+r)/r \bmod p - 1$, $s' = r's/r \bmod p - 1$。

(2) 类似于 (1)。

(3) $y^r = r^m g^s \bmod p$, $y^r = (gr)^m g^{s-m} \bmod p$, $y = (gr)^{m/r} g^{(s-m)/r} \bmod p$, $y^{r'} = (gr)^{r'm/r} \times g^{r'(s-m)/r} \bmod p$, $r' = gr \bmod p$, $m' = r'm/r \bmod p - 1$, $s' = r'(s-m)/r \bmod p - 1$。

(4),(5),(6) 类似于 (3)。

(7) $y^{rm} = rg^s \bmod p$, $y^{rm} = (rg) g^{s-1} \bmod p$, $y^{r'(rm/r')} = (rg) g^{s-1} \bmod p$, $r' = gr \bmod p$, $m' = rm/r' \bmod p - 1$, $s' = s - 1 \bmod p - 1$。

(8) $y = r^{rm} g^s \bmod p$, $y = (rg)^{rm} g^{s-mr} \bmod p$, $y = (rg)^{r'(rm/r')} g^{s-mr} \bmod p$, $r' = gr \bmod p$, $m' = rm/r' \bmod p - 1$, $s' = s - mr \bmod p - 1$。

(9) 类似于 (7)。

(10) 类似于 (8)。

(11) $y^{rm} = r^s g \bmod p$, $y^{rm+s} = (ry)^s g \bmod p$, $y^{r'(rm+s)/r'} = (yr)^s g \bmod p$, $r' = yr \bmod p$, $m' = (rm+s)/r' \bmod p - 1$, $s' = s$。

(12) 类似于 (11)。

(13) ~ (18) 类似于 (7) ~ (12)。

由于 m' 是 m, r, s, g, y 的算术组合，不能代换成 $H(m'')$。因此只要使用单向函数 $H(\cdot)$。广义 ElGamal 型签名方案都是安全的。

由此可见，第 (1) 类也是空集。

对于广义 MP 型方案 $m = y^{b/a}g^{c/a}r \bmod p$， (a,b,c) 中已不含 m。作为两种最简单的情况，我们可以给出代换攻击方法如下：

$m = y^r g^s r \bmod p$, $(gm) = y^r g^{s+1} r \bmod p$, $m' = gm \bmod p$, $r' = r$, $s' = s+1 \bmod q$;

$m = y^s g^r r, \bmod p$, $(ym) = y^{s+1} g^r r \bmod p$, $m' = ym \bmod p$, $r' = r$, $s' = s+1 \bmod q$。

4 p 型方案的改进型方案的分析

文献 [1] "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，又可增加签名方案中的未知数 (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 "。

我们试举一个方案分析：

签名方案 I (a 含 s)

签名方程 $r = g^k \bmod p$, $ax = bk + c \bmod q$. (1)

$A = y^t \bmod p$, $B = t + a \bmod q$. (2)

签名 (r, A, B)

签名验证 $A = y^B (r^b g^c)^{-1} \bmod p$. (3)

这个方案与祁明等人早先的一篇文章 [6] "加强广义 ElGamal 型签名方案的安全性" 中提出的隐式 ElGamal 型签名方案相比，除了改变两个字母外，还少了一项单向函数 $f(A,T)$。

4.1 方案的简化

我们可以简化这个方案的签名计算，合并签名方程 (1) 和 (2) 式。从 (1) 式得

$$a = x^{-1}(bk + c) \bmod q.$$

代入 (2) 式，得

$$B = t + x^{-1}(bk + c) \bmod q.$$

整理，移项

$$xt = xB - (bk + c) \bmod q. \tag{4}$$

如果对 (4) 式两边以 q 为底作指数运算，得

$$g^{xt} = g^{xB}(g^{kb}g^c)^{-1} \bmod p$$

即

$$A = y^B (r^b g^c)^{-1} \bmod p$$

反之，如果对验证方程 (3) 式两边以 q 为底作对数运算，就得到 (4) 式。

在乘法循环群和加法循环群之间存在一个同构映射。每个乘法等式一一对应于一个加法等式。因此每个验证方程一一对应于一个签名方程。根据这个道理，例子中的签名方案中，真正的签名方程应该是 (4) 式。改进型方案只不过是引进一个中间变量，把一个签名方程人为地拆成两个等式。如果我们用 (4) 式来计算签名，还可以减少计算量，简化方案。因此，我们可以得到结论：

改进型方案本质上是一种使用一对会话密钥的广义 ElGamal 型方案.

在例子中，代替 ElGamal 方案中的部分签名 s 的是部分签名 B .

因此，文献 [1] 原先的想法是隐蔽部分签名 s ，防止攻击者利用. 这个初衷现在就无法实现，方案的基础就不复存在了. 攻击者就可以利用新的部分签名来攻击改进型签名方案.

4.2 伪造任意消息的签名

文献 [1] 中没有说明参数 (b,c) 的选取方法. 在广义 ElGamal 型方案中，参数 (a,b,c) 是 (r,s,m) 的算术组合. 现在 a 含 s ，因此 (b,c) 是 (r,m) 的算术组合. 在上面提到的文章中，也是这样选取参数的.

对于任意消息 m ，攻击者随意选择两个整数作为 r,B ，然后组合 b,c ，利用签名验证方程 (3) 式： $A=y^B(r^bg^c)^{-1} \bmod p$ 直接计算 A . 显然，签名 (r,A,B) 一定被接受.

造成攻击者能够如此容易伪造任意消息的签名的原因是，作者从 (b,c) 简化去部分签名 A .

4.3 同态攻击

在例子中，公钥 $y=g^x \bmod p$ ，会话密钥 r, t 使得

$$r=g^k \bmod p, \quad A=y^t=g^{xt} \bmod p,$$

签名方程　　$xt=xB-(bk+c) \bmod q.$

由于 x 是固定不变的，我们令 $z=xt$, 那么第 i 次签名的签名方程是

$$B_ix-z_i-b_ik_i=c_i \bmod q \qquad i=1,2,\cdots.$$

它是关于未知量 x,z_i,k_i 的一次同余方程. 如果攻击者还可以得到其它关于这些未知量的等式，他们就可以求出密钥 x .

作为最特殊的情况，如果攻击者发现 $r=y^n(\bmod p)$, $A=y^m(\bmod p)$ ，他们就可以得到等式：

$$k=nx \bmod q \text{ 和 } \quad z=mx \bmod q.$$

把它们与签名方程：

$$Bx-z-bk=c \bmod q$$

联立，解方程组，得到

$$x=c(B-m-bn)^{-1} \bmod q.$$

由于 q 是素数，对于任意会话密钥 k, z ，都存在这样的整数 n, m ，使得

$$k=nx \bmod q \text{ 和 } \quad z=mx \bmod q.$$

问题在于攻击者能否发现它们. 如果整数 n, m 都比较小，攻击者发现它们的机会就会增大.

下面假设 k_i,t_i 重复使用，不妨设 $k_1=k_2=k_3$, $t_1=t_2=t_3$ ，此时， $z_1=z_2=z_3$. 攻击者可以从等式 $r_1=r_2=r_3$ ， $A_1=A_2=A_3$ 判断上述等式的存在. 因此攻击者又得到

$$B_1x - z_1 - b_1k_1 = c_1 \mathrm{mod} q;$$
$$B_2x - z_1 - b_2k_1 = c_2 \mathrm{mod} q;$$
$$B_3x - z_1 - b_3k_1 = c_3 \mathrm{mod} q.$$

这是关于未知量 x, z_1, k_1 的线性同余方程组。只要它的系数阵模 q 可逆，攻击者就可以求出密钥 x 。

下面假设 $k_3 = k_1 + k_2 \mathrm{mod} q$, $t_3 = t_1 + t_2 \mathrm{mod} q$ ，此时， $z_3 = z_1 + z_2 \mathrm{mod} q$ 。攻击者可以从等式 $r_3 = r_1 \cdot r_2 \mathrm{mod} p$ ， $A_3 = A_1 \cdot A_2 \mathrm{mod} p$ 判断上述等式的存在。因此攻击者又得到

$$B_1x - z_1 - b_1k_1 = c_1 \mathrm{mod} q;$$
$$B_2x - z_2 - b_2k_2 = c_2 \mathrm{mod} q;$$
$$B_3x - (z_1 + z_2) - b_3(k_1 + k_2) = c_3 \mathrm{mod} q.$$

三个方程中有五个未知量 x,k_1,k_2,z_1,z_2 ，攻击者还不能求出密钥 x 。如果他们还能够得到两个关于这些未知量的一次等式，攻击者就可以求出密钥 x 。

如果签名方程中包含 A ，由于 A 是已知的，攻击者同样可以求出密钥 x 。

因此在改进型方案中，为了抵御同态攻击，会话密钥不仅不可以重复使用，而且还要防止它们之间产生较小系数的一次等式。

4.4 代换攻击

我们在 4.2 节已经说明了，如果参数 (b, c) 不含 A ，攻击者可以伪造任意消息的签名。下面我们假设参数 (b, c) 含 A 。把验证方程简化为 $y^B = r^b g^c A \mod p$ 。

假设 $b = r$ ， $c = mA$:

$y^B = r^r g^{mA} A \mod p$, $y^{B+1} = r^r g^{mA}(Ay) \mod p$, $y^{B+1} = r^r g^{(mA/A')A'}(Ay) \mod p$,

$A' = Ay \mod p$, $m' = mA/A' \mod q$, $r' = r$, $B' = B + 1 \mod q$ 。

假设 $b = mA$ ， $c = r$:

$y^B = r^{mA} g^r A \mod p$, $y^{B+1} = r^{mA} g^{rA}(Ay) \mod p$, $y^{B+1} = r^{(mA/A')A'} g^r(A/y) \mod p$,

$A' = Ay \mod p$, $m' = mA/A' \mod q$, $r' = r$, $B' = B + 1 \mod q$ 。

假设 $b = A$ ， $c = m + r$:

$y^B = r^A g^{m+r} A \mod p$, $y^B = (rg)^A g^{m+r-A} A \mod p$, $y^B = (rg)^A g^{(m+r-A-r')+r'} A \mod p$,

$r' = rg \mod p$, $m' = m + r - A - r' \mod q$, $A' = A$, $B' = B$ 。

假设 $b = m + A$ ， $c = r$:

$y^B = r^{m+A} g^r A \mod p$, $y^{B+1} = r^{m+A} g^r(Ay) \mod p$, $y^{B+1} = r^{(m+A-A')+A'} g^r(Ay) \mod p$,

$A' = Ay \mod p$, $m' = m + A - A' \mod q$, $r' = r$, $B' = B + 1 \mod q$ 。

总之，许多改进型方案都不能抵御代换攻击。

5 通行字认证方案改进型的分析

文献 [1] 的最后一段是对 Chang-Liao 通行字认证方案的改进和推广。文献 [1] 认为，改进方案克服了原方案的“两个弱点，一是口令生成中心 (PGC) 对随机数 k 不可重复使用。… 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。”

原先的 Chang-Liao 通行字认证方案是建立在 ElGamal 签名方案 [6] 上．文献 [1] 把改进型建立在加强的 ElGamal 签名方案 [7] 上．文献 [1] 以增加一个公钥和一个大数模的指数运算为代价，希望加强改进型方案的安全性．不幸的是，Harn[8] 指出了加强的 ElGamal 签名方案并没有像它的作者们希望的那样安全．因此以此为基础的通行字认证方案的改进型也没有像它的作者们希望的那样安全．

5.1 通行字认证方案改进型的简介

p, p_1, q_1 都是大素数，$p_1q_1|p-1$，$g \in \mathrm{GF}(p)$ 是本原元．x 和 $y = g^x \bmod p$, $z = y^x \bmod p$ 是系统的密钥和两个公钥．

用户 U_i 的通行字 $Pw_i = (r_i, s_i)$ 的计算如下：

PGC 选随机数 t_i, $(t_i, p-1) = 1$，计算 $k_i = t_i^2 \bmod p-1$, $r_i = g^{k_i} \bmod p$.

求 v_i, 使得 $\mathrm{ID}_i = xr_i + t_iv_i \bmod p-1$, 计算 $s_i = v_i^2 \bmod p-1$．

PGC 将 PW_i 和 r_i 分别秘密地送用户 U_i 和系统 s．这里 ID_i 是用户 U_i 的标识符．然后用户 U_i 利用通行字 $Pw_i = (r_i, s_i)$，计算认证数据，获准后，访问系统．

5.2 同态攻击

文献 [1] 说，在改进型方案中，“如果随机数 t_i 重复使用，攻击者难以求得 x”．假设 PGC 为用户 U_1,U_2,U_3 计算通行字时，使用相同的随机数 $t_1 = t_2 = t_3 = t$．攻击者可以从发现 $r_1 = r_2 = r_3 = r$ 中判断这个事实．因此

$$\begin{aligned}
&\mathrm{ID}_1 - xr = tv_1 \bmod p-1;\\
&\mathrm{ID}_2 - xr = tv_2 \bmod p-1;\\
&\mathrm{ID}_3 - xr = tv_3 \bmod p-1.
\end{aligned}$$

分别两边平方，得

$$\begin{aligned}
&\mathrm{ID}_1^2 - 2xr\mathrm{ID}_1 + (xr)^2 = (tv_1)^2 = ks_1 \bmod p-1;\\
&\mathrm{ID}_2^2 - 2xr\mathrm{ID}_2 + (xr)^2 = (tv_2)^2 = ks_2 \bmod p-1;\\
&\mathrm{ID}_3^2 - 2xr\mathrm{ID}_3 + (xr)^2 = (tv_3)^2 = ks_3 \bmod p-1.
\end{aligned}$$

我们把它们看作关于未知数 x, x^2, k 的线性方程组，只要系数阵不是零，就可以求出 x．因此随机数不可重复使用．

实际上，如果 $t_3^2 = t_1^2 + t_2^2 \bmod p-1$，就有 $k_3 = k_1 + k_2 \bmod p-1$, $r_3 = r_1r_2 \bmod p$，反之亦然．攻击者就可以利用这些关系．

5.3 系统存贮每个用户的部分通行字

原先 Chang-Liao 方案的一个特点是，系统不需要存贮用户的任何数据．如果按照文献 [1] 的意见，系统存贮每个用户的部分通行字的话，那还不如系统存贮每个用户的公开信息．每个用户可将自己的标识符 ID_i 和公钥 $y = g^{xi} \bmod p$ 存贮在系统里．当系统需要验证用户的身份时，用户只要提供他对 (ID_i, T) 的数字签名即可．

这种处理方法比文献 [1] 的改进型方案至少有两个优点：(1) 不需要通行字生成中心及其承担的任务，(2) 每次验证只需要两个大数模的指数运算，比文献 [1] 的改进型方案少两个．

6 结 束 语

以上我们分析了文献 [1] 中的许多错误，但是文献 [1] 也还是做了一些工作的．文献 [1] 在第 3 节介绍了基于广义 MR(p) 型方案的多重签名方案．尽管文献 [1] 认为“这类多重签名由于受到某些限制还不十分有效，…还有待做进一步的工作”．然而这毕竟是新的工作．

参 考 文 献

[1] 祁明，肖国镇．两类 ElGamal 型数字签名方案的安全性和性能分析，电子科学学刊，1997, 19(3): 346–349.

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

[3] Harn L, Xu Y. Design of generalized ElGamal type digital signature schemes based on the discrete logarithm, Electron. Lett., 1994, 31(24): 2025–2026.

[4] Boyb C. New digital signature scheme based on discrete logarithm(comment), Electron. Lett., 1994, 30(6): 480–481.

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

[6] 祁明，肖国镇．加强广义 ElGamal 型签名方案的安全性，电子学报，1996, 24(11): 68–72.

[7] He J, Keisler T. Enhancing the security of ElGamal's signature scheme, IEE Proc. Comput. Digit. Tech., 1994, 141(4): 249–252.

[8] Harn L. Enhancing the security of ElGamal's signature scheme (comment), IEE Proc. Comput. Digit. Tech, 1995, 142(5): 376.

DISCUSSION ON “SECURITY AND PERFORMANCE ANALYSIS OF TWO KINDS OF ELGAMAL SIGNATURE SCHEMES”

Shao Zuhua

(*Hangzhou Institute of Financial Managers, Hangzhou* 310012)

Abstract Qi Ming and others recently analyzed and discussed the security of two kinds of the ElGamal signature schemes and the password authentication scheme based on two kinds of the signature schemes, and proposed two kinds of improved schemes. This paper first points out that the first p type signature scheme proposed by Qi is not secure, since attackers can forge signature for any message. Then this paper shows that the generalized ElGamal signature schemes can not resist the substitution attack. Finally this paper shows that two kinds of the improved schemes proposed by Qi can not resist the homomorphism attack, and does not have the security as Qi said.

Key words Cryptanalysis, Digital signature scheme, Hormomorphism attack, Substitution attack, Password authentication

邵祖华： 男，1948 年生，副教授，主要从事认证理论和金融电子安全的研究．