第 24 卷 第 2 期 华 侨 大 学 学 报 (自 然 科 学 版) Vol. 24 No. 2
2003 年 4 月 Journal of Huaqiao University (Natural Science) Apr. 2003

文章编号 1000-5013(2003)02-0222-03

ElGamal 密码系统的改进

蒋 吉 频

(广东外语外贸大学计算机科学与技术系, 广东 广州 510420)

摘要 改进后的 ElGamal 加密解密法、数字签名算法, 它是基于 $x(x=g^t(\mathrm{mod}p)$ 代替生成元 g, 并对传统的算法作些适当的变换而得到的. 公开 x, 保密 g, 使得攻击者在寻找私钥 t 时无从下手. 由此, 可以彻底消除了攻击者猜测私钥的空间, 使得 ElGamal 密码系统更安全.

关键词 ElGamal 密码系统, 生成元, 隐藏

中图分类号 TP 309.7 文献标识码 A

ElGamal 密码算法系统, 是基于有限域上离散对数的困难性而进行设计的. 对于方程 $y=g^t(\mathrm{mod}\ p)$ 来说(其中 p 是素数, g 是有限域 Z_p 上的生成元), 已知 t, 很容易求出 y; 但反过来很困难, 即已知 y, 很难易求出 t. ElGamal 加密解密算法和数字签名算法, 都是先按方程 $y=g^t(\mathrm{mod}\ p)$ 计算出 y, 然后公开 y, g, p, 保密私钥 t. 但因为公开了生成元 g, 所以攻击者还是可以按照上述的方程不断的猜测私钥 t, 即给了攻击者一个猜测的空间, 尤其当素数 p 和私钥 t 不够强壮时. 本文试图对 ElGamal 密码系统作些改进, 不公开生成元 g, 使攻击者无从猜测私钥.

1 ElGamal 加密和解密系统的改进

1.1 传统的 ElGamal 加密和解密算法

设通信双方为 A 和 B, B 向 A 发送加密信息. 其操作可有以下 3 个步骤. (a) A 产生公钥和私钥. A 选择一个大素数 p、生成元 g 和私钥 t, 其中

$$1<g<p-1,\qquad 1<t<p-1,$$

计算公钥 $y=g^t(\mathrm{mod}\ p)$. 然后公开 y, p, g, 保密私钥 t. (b) B 利用 A 的公钥向 A 发送加密信息 m. B 产生一个随机数 $k(1<k<p-1)$, 计算

$$C1=g^k(\mathrm{mod}\ p),\qquad C2=my^k(\mathrm{mod}\ p).$$

然后, 将 $C1, C2$ 发送给 A. (c) A 用自己的私钥解密 B 的信息. A 计算 $C2\ (C1^t)^{-1}$, 就可得到了 B 的加密信息 m. 因为

$$C2\ (C1^t)^{-1}=my^k(g^{kt})^{-1}=mg^{kt}(g^{kt})^{-1}(\mathrm{mod}\ p), \tag{1}$$

又因为 $1<g, k, t<p-1$, 根据有限域 Z_p 的性质, 可得

$$1<g^{kt}(\mathrm{mod}\ p)<=p-1,\qquad (g^{kt}, p)=1.$$

收稿日期: 2002-10-22 作者简介: 蒋吉频(1963-), 女, 副教授

所以, 存在唯一的$(g^{kt})^{-1}$, 且

$$g^{kt}(g^{kt})^{-1} \equiv 1(\mathrm{mod}\ p).$$

那么, 由式(1)可得

$$C2\ (C1^{t})^{-1} \equiv m(\mathrm{mod}\ p).$$

1.2　ElGamal 加密和解密算法的改进——隐藏生成元

可按以下 3 个步骤进行操作. (a) A 产生公钥和私钥. A 选择一个大素数 p、生成元 g 和两个私钥 t 和 d, 其中 $1< g< p-1, 1< t< p-1, 1< d< p-1$. 计算公钥

$$x = g^{t}(\mathrm{mod}\ p), \qquad y = g^{td}(\mathrm{mod}\ p).$$

然后, 公开 x, y, p, 保密 g, t, d. (b) B 利用 A 的公钥向 A 发送加密信息 m. B 产生一个随机数 $k(1< k< p-1)$, 计算

$$C1 = x^{k}(\mathrm{mod}\ p), \qquad C2 = my^{k}(\mathrm{mod}\ p).$$

然后将 $C1, C2$ 发送给 A. (c) A 用自己的私钥解密 B 的信息. A 计算 $C2\ (C1^{d})^{-1}$就可得到了 B 的加密信息 m. 因为

$$C2\ (C1^{d})^{-1} = my^{k}(x^{kd})^{-1} = mg^{ktd}(g^{ktd})^{-1}(\mathrm{mod}\ p), \tag{2}$$

又因为 $1< g, k, t, d< p-1$, 根据有限域 Z_p 的性质, 可得

$$1 < g^{ktd}(\mathrm{mod}\ p) \leq p-1, \qquad (g^{ktd}, p) = 1.$$

所以, 存在唯一的$(g^{ktd})^{-1}$, 且 $g^{ktd}(g^{ktd})^{-1} \equiv 1(\mathrm{mod}\ p)$, 则由(2)可得 $C2\ (C1^{d})^{-1} \equiv m\ (\mathrm{mod}\ p)$. 通过这个算法, 就可隐藏生成元 g, 使攻击者无从下手.

2　ElGamal 数字签名系统

2.1　传统的 ElGamal 数字签名算法

设通信双方为 A 和 B, A 向 B 发送带有数字签名的信息. 其操作可按以下 3 个步骤进行. (a) A 产生公钥和私钥. A 选择一个大素数 p、生成元 g 和私钥 t, 其中

$$1 < g < p-1, \qquad 1 < t < p-1.$$

计算公钥 $y = g^{t}(\mathrm{mod}\ p)$. 然后, 公开 y, p, g, 保密 t. (b) A 利用自己的私钥求出信息 m 签名文选择随机数 k, 且满足$(k, p-1) = 1$, 计算签名文. 即

$$r = g^{k}(\mathrm{mod}\ p),$$

$$s = k^{-1}(m - tr)\ (\mathrm{mod}\ (p-1)).$$

(c) B 验证 A 的签名, B 验证式子为

$$g^{m} \equiv y^{r} \cdot r^{s}(\mathrm{mod}\ p). \tag{3}$$

若式(3)存立, 则该数字签名确实是由 A 发出的; 否则, 该数字签名是伪造的. 因为

$$y^{r} \cdot r^{s} = g^{tr} \cdot g^{ks} = g^{tr} \cdot g^{kk^{-1}(m-tr)(\mathrm{mod}(p-1))} \equiv g^{m}(\mathrm{mod}\ p).$$

2.2　ElGamal 数字签名算法的改进——隐藏生成元

可按以下 3 个步骤进行操作. (a) A 产生公钥和私钥. A 选择一个大素数 p、生成元 g 和两个私钥 t, d, 其中 $1< g< p-1, 1< t< p-1, 1< d< p-1$. 计算公钥

$$y = g^{t}(\mathrm{mod}\ p), \qquad x = g^{d}(\mathrm{mod}\ p).$$

然后公开 x, y, p, 保密 g, t, d. (b) A 利用自己的私钥求出信息 m 签名文选择随机数 k, 且满足

$(d\ k, p-1)=1$, 计算签名文. 即

$$r = x^k \pmod p,$$

$$s = (d^k)^{-1}(m - t\ r) \pmod{(p-1)}.$$

(c) B 验证 A 的签名, B 验证式子为

$$x^m \equiv y^r \cdot r^s \pmod p. \tag{4}$$

若式(4)存立, 则该数字签名确实是由 A 发出的; 否则, 该数字签名是伪造的. 因为

$$y^r \cdot r^s = g^{tr} \cdot g^{dks} = g^{tr} \cdot g^{(dk)(dk)^{-1}(m-tr)\pmod{(p-1)}} \equiv g^m \pmod p.$$

3 结束语

改进后的ElGamal 加密解密算法和数字签名算法, 它是基于 x (这里 $x = g^t \pmod p$) 代替生成元 g, 并对传统的算法作些适当的变换而得到的. 公开 x, 保密 g, 使得攻击者在寻找私钥 t 时无从下手. 这样, 可以彻底消除攻击者猜测私钥的空间, 使得 ElGamal 密码系统更安全.

参 考 文 献

1 Carton R D 著. IPSec VPN 的安全实施[M]. 周永彬等译. 北京: 清华大学出版社, 2001. 82～84

2 赖溪松. 计算机密码学及其应用[M]. 北京: 国防工业出版社, 2001. 1～30

3 卢开澄. 计算机密码学 —— 计算机网络中的数据保密与安全[M]. 第 2 版. 北京: 清华大学出版社, 1998. 84～109

4 潘承洞, 潘承彪. 初等数论[M]. 北京: 北京大学出版社, 1992. 232～248

5 屈婉玲. 代数结构与组合数学 —— 离散数学: 第 3 分册[M]. 北京: 北京大学出版社, 1998. 50～128

6 黄友谦, 黄东斌. 网络安全与密码技术[M]. 香港: 博士苑出版社, 2002. 17～25

The Improvement of EIGamal Cryptosystem

Jiang Jiping

(Dept. of Computer Sci. & Tech., Guangdong Univ. of Foreign Studies, 510420, Guangzhou, China)

Abstract Based on the replacement of generator g by $x(x = g^t \pmod p)$ and proper conversion of traditional algorithm, the improved algorithm of encryption and decryption and the algorithm of digital signature can be obtained. By making x known to the public and keeping g secret, the attacker who wants to seek private key t will have no way to begin. The space for the attacker to guess private keys can thus be thoroughly eliminated, and the EIGamal cryplosyslem can thus be safer.

Keywords EIGamal cryptosystem, generator, concealment

本期英文审校 李 坚