文章编号:1005－0523(2005)01－0127－02

几种新的 ElGamal 型签名方案及其加强型

王庆菊,亢保元,韩金广

(中南大学 数学科学与计算技术学院,湖南 长沙 410083)

摘要:对 ElGamal 型签名规则做出适当修改,并列出了几种新的签名方案.同时给出了新方案的加强型,使其安全性基于大整数分解和离散对数两大数学难题,从而具有较高的安全性.

关 键 词:数字签名;ElGamal 型;离散对数;大整数分解

中图分类号:TP311　　**文献标识码**:A

0 引 言

数字签名是密码学研究领域的热门问题之一,它是传统手写签名的电子模板,能够实现用户对消息的认证.在数字化浪潮冲击着传统生活方式的今天,数字签名作为一种重要的信息安全技术,在人们的生活与工作中扮演着不可或缺的角色.1985 年,ElGamal[1]基于离散对数问题提出了数字签名方案.此后,对 ElGamal 方案的变形相继被提出[2－4].对于 ElGamal 数字签名方案的变形统称为 ElGamal 型数字签名方案.1994 年 Harn .L.和 xu .Y.[5]提出了设计 ElGamal 型数字签名的规则,并列出了 18 种安全的 ElGamal 型数字签名方案.本文对[5]中的一些规则作出适当修改,并在遵循这些规则的前提下,给出了另外几种签名方案.之后又给出了新方案的加强型,使它的安全性建立在整数分解和离散对数两大数学难题之上,从而具有较高的安全性.

1 一般的 ElGamal 型数字签名方案

设 p 是一个大素数,α 是 $GF(p)$的本原元,每个用户选择私钥 $x\in[1,p-1]$,并计算 $y=\alpha^{x}\bmod p$ 作为其公钥.$h()$是一公开的单向 HashHash 函数,所有的 ElGamal 型数字签名方案并不是直接对消息 m 签名,而是对 $h(m)$进行签名.为了简便,我们仍记 $h(m)$为 m.

对任意消息 m,用户随机选择保密的整数 $k\in[1,p-1]$,使 $GCD(k,p-1)=1$.计算 $\gamma=\alpha^{k}\bmod p$,并利用私钥 x 及 k 对消息 m 签名 $m=ks+\gamma s\bmod(p-1)$,求解出 $s=(m-\gamma s)k^{-1}\bmod(p-1)$.则$(\gamma,s)$就是对 m 的一个签名.将(γ,s)发送到验证者.

验证者验证 $\alpha^{m}=\gamma^{s}y^{\gamma}\bmod p$,如果成立,则$(\gamma,s)$就是正确的签名.

2 ElGamal 型签名规则和一些新方案

不失一般性,我们用 $ax=bk+c\bmod\Phi(p)$代表所有的 ElGamal 型签名方程,其中(a,b,c)是(m,γ,s)中参数的置换或数学组合.例如,参数 a 可以是 γ 或 γm,等等.相应的验证方程为 $y^{\alpha}=\gamma^{b}\alpha^{c}\bmod p$

对[5]中的一些签名规则我们将作出适当的修改,如下:

1) x 和 k 不能在同一项中.因为 x 和 k 都是保密的,如果出现在同一项中,验证方程中将会出现 y^{k} 或 γ^{x},验证者无法对签名进行验证.

收稿日期:2004－12－12

作者简介:王庆菊(1981－),女,山东临沂人,中南大学在读研究生.

2) 对消息 m 签名，m 应包含在签名方程中，且应可以包含在(a,b,c)中任意一个参数中.

3) 出于安全性考虑，s 和 m，s 和 γ 不能在同一项中. 如 $x=\gamma k+sm \bmod \Phi(p)$，，已知消息 m 的签名为(γ,s). 攻击者只需选取 $m'=\beta m \bmod \Phi(p)$，$s'=\beta^{-1} \bmod (p)$，则(γ,s')就是消息 m'的签名. 又如 $mx=k+\gamma s \bmod \Phi(p)$，相应的验证方程为 $y^m=\gamma\alpha^{\gamma s} \bmod (p)$. 攻击者首先选择整数 R，计算 γ'使得 $y^m=\gamma'\alpha^R \bmod (p)$，再由 $\gamma's'=R \bmod (p)$解出 s'，则(γ',s')就是消息 m 的一个签名. 但 γ 和 m 能在同一项中，这是由于 $\gamma=\alpha^k \bmod (p)$，而 k 保密，仅改变 γ 的值无法伪造签名.

4) 签名方程中必须包含 3 个独立项，否则易攻击. 如$(m+\gamma)x=sk \bmod \Phi(p)$，已知消息 m 的签名为(γ,s). 则可以伪造 m'的签名(γ,s')，其中，$m'=m-\beta \bmod \Phi(p)$，$s'=(1-\beta(m+\gamma)^{-1})s \bmod \Phi(p)$

5) 签名方程可包含 5 个或 4 个参数，(x,k,m,γ,s)或(x,k,m,s)，其中(m,γ,s)公开，x 是用户的私钥，k 是与消息对应的随机保密参数. 由于保密参数总比攻击者可以得到的签名方程数目多 1 个，所以攻击者无法从签名方程中得到 x 和k.

遵循以上签名规则，使签名方程包含 4 个参数(x,k,m,s)，我们提出几种新的 *ElGamal* 型数字签名方案.

选择大素数 p，使得 $p-1$ 有两个大素因子和 p'和 q'. α,k,γ,h 同原 ElGamal 型签名方案. 忽略 $+d$ 和 $-d$，d 和 d^{-1}之间的不同，$d\in(x,k,m,s)$. (a,b,c)是$(1,m,s)$的置换或数学组合. 仍用 $ax=bx+c \bmod \Phi(p)$代表 ElGamal 型签名方程.

参数(a,b,c)不含 γ，如果 k 作为单独的一项，可以伪造签名. 如：签名方程为 $sx=k+m \bmod \Phi(p)$，验证方程为 $y^s=\gamma\alpha^m \bmod p$. 攻击者只要随机选择 s'，计算 γ'容易做到. 可以验证(γ',s')就是 m 的一个伪造签名. 所以 k 不能作为单独的一项，也就是 $b\neq 1$，则 $b=m,s,m+s$ 或 ms. 但由上述签名规则(3)知，s 和 m 不能在同一项中，所以 $b=m$ 或 s，因此这类签名方程有 $C_2^1\cdot 2=4$ 个，列出如下：

	签名方程	验证方程
I(a 含 s)	$sx=mk+1 \bmod \Phi(p)$	$y^s=\gamma^m\alpha \bmod p$
II(b 含 s)	$x=sk+m \bmod \Phi(p)$	$y=\gamma^s\alpha^m \bmod p$
	$mx=sk+1 \bmod \Phi(p)$	$y^m=\gamma^s m\alpha^m \bmod p$
III(c 含 s)	$x=mk+s \bmod \Phi(p)$	$y=\gamma^m\alpha^s \bmod p$

3 安全性及性能分析

攻击者对消息伪造签名时，如果给定 γ'，求解 s'等同于求解离散对数问题；如果给定 s'，求解 γ'是整数分解问题，也是困难的. 如果同时给定 γ'和 s'，求解 m'也等同于求解离散对数问题，同时由于单向函数 h 作用于消息，要想求得消息 m，需要求单向函数的逆，这也是困难的. 故这些签名方案的安全性仍基于离散对数问题，同原 ElGamal 方案相比，安全性并没有降低.

在签名方程中只含 4 个参数，可以减少计算量，从而简化签名生成过程. 又在验证方程中仅出现 2 个模指数运算，原需要 3 个模指数运算，从而加速了签名验证过程.

第 III 类签名方程与原 ElGamal 型签名方程相比，除具有上述优点外，由签名方程求解 s 时，无需任何求逆运算，这又大大简化了签名生成过程. 基于上述种种优点，第 III 类方程在实际中具有良好应用.

4 加强型方案

ElGamal 型签名方案的安全性都是建立在离散对数问题基础上的，在此提出一个对新方案的加强型，使其安全性建立在整数分解和离散对数两大数学难题上.

4.1 参数选择

1) 大素数 $p=2p'q'+1$ $p'=2p''+1$ $q'=2q''+1$ 且 p',q',p'',q'' 也是大素数.

2) α 是 GF(p)的本原元

3) 随机数 $x\in[1,p-1]$，用户 A 计算 $y=\alpha^x \bmod p$，并求 d，使得 $3\cdot d\equiv 1 \bmod \Phi(\Phi(p))$. $(p,\alpha,y,3)$是 A 的公钥，(p',q',x,d)是 A 的私钥.

4.2 签名生成

对消息 m，A 随机选择 $k\in[1,p-1]$，计算 $\gamma=\alpha^k \bmod p$ 其中 $h()$是一个单向 hash 函数. 找到 s'，使得 $s'=x+kh(m) \bmod (p-1)$，其中 $h()$是一个单向 hash 函数. 并计算 $s=(s')^d \bmod (p-1)$. (γ,s)就是 A 对消息 m 的签名. 将(γ,s)发送到验证者.

4.3 签名验证

验证者接收到(γ,s)后，利用 A 的公钥$(p,\alpha,y,3)$进行验证. 首先计算 $s'=s^3 \bmod (p-1)$，然后验证 $\alpha^{s'}=y\gamma^{h(m)} \bmod p$ 的成立. (下转第 138 页)

Application of Empirical Mode Decomposition to Fault Diagnosis of Rolling Bearing

LI Yi, XIONG Guo-liang, ZHANG Long

(School of Mechanical Engineering, East China Jiaotong Univ., Nanchang 330013, China)

Abstract: In non-stationary processes, as machines are subjected to larger stress than that in stationary processes, monitoring of the non-stationary process is helpful to find early faults and prevent machines from severe broken. In this paper, the empirical mode decomposition (EMD) is introduced to analyze mechanical faults. Since EMD is self-adaptive, it is applicable to non-stationary processes. The application of EMD shows that it can highlight the fault characteristics of vibration signals in diagnosing rolling bearings and improve the accuracy of the fault diagnosis.

Key words: empirical mode decomposition; non-stationary signal; fault diagnosis; bearing

(上接第 128 页)

若成立,则接受签名,否则拒绝接受签名.

上述签名验证过程是正确的.这是因为 $\alpha^{s'} = \alpha^{x+kh(m)} = y\gamma^{h(m)} \bmod(p)$

5 结束语

本文对 ElGamal 型签名规则作出适当修改,并列出了几种新的签名方案.同时给出

新方案的加强型,使其安全性基于大整数分解和离散对数两大数学难题,具有较高的安全性.

参考文献:

[1] ElGamal .T. , A public cryptosystem and signature scheme based on discrete logatithms, IEEE Trans, 1985, IT-31: 469-472

[2] Agnew .G.B., et al , Improved digital signature scheme based on discrete logarithm, Electron Lett , 1990, 26(4): 1024-1025

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

[4] Harn .L., New digital signature scheme based on discrete logarithm, Electron Lett , 1994, 30(5): 396-398

[5] Harn .L. and Xu .Y. , Design of generalized ElGamal type digital signature schemes based on discrete logarithm, Electron Lettt , 1994, 30(24): 2025-2026

[6] Lee .Y. and Hwang .T. , Modified Harn signature schemes based on factorizing and discrete logarithms, IEE Proc.-comput . Digit. Tech, 1996, 1 43(3): 196-198

Several New ElGamal Type Digital Signature Schemes and Their Enhanced Schemes

WANG Qing-ju, KANG Bao-yuan, HAN Jin-guang

(School of Mathematical Sciences and Computing Technology, Central South University, Hunan Changsha 410083, China)

Abstract: In this paper , we modify the design criteria of ElGamal type digital signature schemes , and several new schemes are put on the list . Moreover , an enhanced scheme is provided , whose security property is based on the factorizing and discrete logarithm problems simultaneously , so it is much safer.

Key words: digital signature; ElGamal type; factorisation discrete logarithm