第 27 卷第 12 期 合肥工业大学学报(自然科学版) Vol. 27 No. 12
2004 年 12 月 JOURNAL OF HEFEI UNIVERSITY OF TECHNOLOGY Dec. 2004

Harn 数字签名方案的改进

于宝证， 侯整风

(合肥工业大学 计算机与信息学院，安徽 合肥 230009)

摘 要：Harn 数字签名方案中，签名者不需计算任何逆，验证者只需计算 2 个模指数，因此相对于其它基于离散对数数字签名方案计算量大大减少。但该方案，不能抵抗同态攻击，并且随机密钥 k 不能重复使用。文章针对该方案的不足，提出一种改进方案，新方案不但保留了 Harn 数字签名计算速度快及容易实现密钥共享等优点，而且能够有效抵抗同态攻击，并且在随机密钥 k 重复使用时能够确保方案的安全性。

关键词：数字签名；离散对数；模逆运算；同态攻击

中图分类号：TP309.2 **文献标识码**：A **文章编号**：1003-5060(2004)12-1562-03

Improvement of Harn digital signature scheme

YU Bao-zheng， HOU Zheng-feng

(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: In the Harn digital signature scheme, the signatory need not compute any inverses and the person who verifies the key only need compute two modular exponents, so the computation work is less in comparison with other schemes based on discrete logarithm. But in using the Harn scheme, the homomorphism attack can not be resisted and the random key k can not be used reduplicatively. Aiming at this drawback, an improved scheme is introduced, in which not only the advantages of the Harn scheme are kept, but also the homomorphism attack is resisted effectively. In addition, the new scheme can ensure the scheme's security when the same random key k is used.

Key words: digital signature; discrete logarithm; modular inversion; homomorphism attack

设 p 为大素数，$g\in CF(p)$ 是 p 的本元元素，在 $CF(p)$ 上求解离散对数 $y=g^x \bmod p$ 是数学中的一个难题。大多数基于离散对数的数字签名方案都需要进行模逆运算，因此计算速度都较慢[1]。1994 年，Harn 提出了一个基于离散对数的数字签名方案[2]，签名者不需计算逆，验证者只需计算 2 个模指数，计算量大大减少，因此在认证方案设计、密钥交换协议及多重数字签名系统中广泛使用。但该方案不能抵抗同态攻击，并且签名随机密钥不能重复使用，否则系统不安全[3]。本文针对该方案的不足，提出一种改进方案，新方案在保留 Harn 数字签名系统优点的前提下能有效抵抗同态攻击，并且在随机密钥重复使用时方案仍然是安全的。此外，本文还利用新方案构造出一种实现密钥共享的方法。

收稿日期：2004-08-31

作者简介：于宝证(1971－)，男，山东高密人，硕士，合肥工业大学助理研究员.

1　Harn 数字签名方案

令 p 为大素数，g 是 $CF(p)$ 的本原元素。每个用户都有一个私钥 $x\in[1,p-1]$ 和公钥 $y=g^x \bmod p$，对于待签的信息 $m\in[1,p-1]$，用户首先秘密地选择 1 个随机整数 $k\in[1,p-1]$，满足 $\gcd(k,p-1)=1$，然后计算 $r=g^k \bmod p$ 和 $s=[x(H(m)+r)-k]\bmod(p-1)$。其中，$H(\cdot)$ 是单向散列函数[4]，于是消息 m 的签名为 $\mathrm{sig}(m)=(r,s)$。

接收方收到签名后，可以通过 $y^{H(m)+r}=rg^s \bmod p$ 验证消息的签名，但该签名方案存在着安全隐患[5]，签名过程中如果 3 个随机密钥 $k_i(i=1,2,3)$ 满足 $k_3=k_1+k_2$，由于 $r=g^k \bmod p$，于是 $r_i(i=1,2,3)$ 就满足 $r_3=r_1r_2$，攻击者可以利用签名方程 $s=[x(H(m)+r)-k]\bmod(p-1)$ 构成方程组，即

$$\begin{cases} s_1=[x(H(m_1)+r_1)-k_1]\bmod(p-1) \\ s_2=[x(H(m_2)+r_2)-k_2]\bmod(p-1) \\ s_3=[x(H(m_3)+r_3)-k_3]\bmod(p-1) \\ k_3=k_1+k_2 \end{cases} \tag{1}$$

(1)式有 4 个方程和 4 个未知数，攻击者可以利用上述关系求得密钥 x，这就是所谓的同态攻击[6]。

另外，随机密钥 k 若被重复使用，攻击者可从形式为

$$\begin{cases} s_1=[x(H(m_1)+r)-k]\bmod(p-1) \\ s_2=[x(H(m_2)+r)-k]\bmod(p-1) \end{cases} \tag{2}$$

构成的方程组中惟一确定 x，且 x 可被恢复出来。因此，为了安全，必须确保 k 不被重复使用[7]。

1.1　改进的 Harn 数字签名方案

受 Okamoto 数字签名方案[8]设计思想的启发，设计了改进的 Harn 数字签名方案。令模数 p 是一个大素数，g 是 $CF(p)$ 中的本原元素。每个用户都有 2 个私钥 x_1、$x_2\in[1,p-1]$ 和 2 个公钥 $y_1=g^{x_1} \bmod p$，$y_2=g^{x_2} \bmod p$，公开 y_1、y_2、p，保密 x_1、x_2、g。

对于待签的每个信息 $m\in[1,p-1]$，用户首先秘密地选择 1 个随机整数 $k\in[1,p-1]$，满足 $\gcd(k,p-1)=1$，然后计算 $r=y_2^k \bmod p$ 和 $s=[x_1x_2^{-1}(H(m)+r)-k]\bmod(p-1)$。

于是消息 m 的签名即为 $\mathrm{sig}(m)=(r,s)$，将 (m,r,s) 发送给接收方。一旦接收方收到 (m,r,s)，任何人都可以通过 $y_1^{H(m)+r}=ry_2^s \bmod p$ 验证消息的签名是否成立，若相等，则该签名有效，否则拒绝接受该签名。这个签名体制的正确性可由以下等式证明，即

$$\begin{aligned} y_1^{H(m)+r}=ry_2^s \bmod p=y_2^k y_2^s \bmod p=y_2^{k+s} \bmod p=y_2^{x_1x_2^{-1}(H(m)+r)} \bmod p= \\ g^{x_2x_1x_2^{-1}(H(m)+r)} \bmod p=g^{x_1(H(m)+r)} \bmod p=y_1^{H(m)+r} \bmod p \end{aligned} \tag{3}$$

在本方案中，x_2^{-1} 可以进行预运算，供签名时重复使用，在签名时不需进行模逆运算，从而确保新方案继承 Harn 方案中签名者不需要计算任何逆，验证者只需要计算模指数。

1.2　安全性分析

(1) 对于改进的 Harn 数字签名方案，也可以按照同态攻击构造方法，构造如下方程组，即

$$\begin{cases} s_1=[x_1x_2^{-1}(H(m_1)+r_1)-k_1]\bmod(p-1) \\ s_2=[x_1x_2^{-1}(H(m_2)+r_2)-k_2]\bmod(p-1) \\ s_3=[x_1x_2^{-1}(H(m_3)+r_3)-k_3]\bmod(p-1) \\ k_3=k_1+k_2 \end{cases} \tag{4}$$

(4)式由 4 个方程组成，里面有 5 个未知数 $\{x_1、x_2、k_1、k_2、k_3\}$，攻击者无法恢复秘密密钥 x_1、x_2，因此同态攻击对本方案不成立。

(2) 签名密钥 k 若重复使用时,对给出的$\{m_i:i=1,2\}$个信息及相应的消息签名$\{(r_i,s_i):i=1,2\}$,攻击者也可以利用签名方程构造如下方程组,即

$$\begin{cases} s_1 = [x_1 x_2^{-1}(H(m_1)+r)-k] \bmod (p-1) \\ s_2 = [x_1 x_2^{-1}(H(m_2)+r)-k] \bmod (p-1) \end{cases} \tag{5}$$

(5)式有 3 个未知数(x_1、x_2、k),但只有 2 个方程,无法惟一地确定 x_1、x_2,因此随机密钥 k 重复使用时对本方案是安全的,这在较大程度上简化了系统对 k 的要求。

2 利用新方案实现密钥共享

利用新方案可以较方便地实现密钥共享,假设进行密钥共享的用户为 A、B,其方案如下:

(1) A 的参数。秘密密钥 x_{1A}、x_{2A};公开密钥 $y_{1A}=g^{x_{1A}} \bmod p$,$y_{2A}=g^{x_{2A}} \bmod p$,随机签名密钥为 k_A。

(2) B 的参数。秘密密钥 x_{1B}、x_{2B};公开密钥 $y_{1B}=g^{x_{1B}} \bmod p$,$y_{2B}=g^{x_{2B}} \bmod p$,随机签名密钥为 k_B。

则 A 与 B 的共享密钥为

$$K = r_A^{k_B x_{2B}} \bmod p = r_B^{k_A x_{2A}} \bmod p \tag{6}$$

具体实现过程为:A 在获得 B 的签名信息(m_B,r_B,s_B)后,先验证该签名的真实性,若正确,则 A 通过计算 $K=r_B^{k_A x_{2A}} \bmod p$ 来实现密钥共享。

同理,B 在获得 A 的数字签名(m_A,r_A,s_A)后,通过计算 $K=r_A^{k_B x_{2B}} \bmod p$ 来实现密钥共享。

该密钥共享机制的正确性可由以下等式证明,即

$$K = r_A^{k_B x_{2B}} \bmod p = g^{x_{2A} k_A k_B x_{2B}} \bmod p = g^{x_{2B} k_B k_A x_{2A}} \bmod p = y_{2B}^{k_B k_A x_{2A}} \bmod p = r_B^{k_A x_{2A}} \bmod p \tag{7}$$

由于新的数字签名方案能够保证 x_1、x_2 及 k 的安全性,因此,攻击者不可能伪造出共享密钥。

3 结束语

本文在分析 Harn 数字签名安全性的基础上,对 Harn 数字签名方案进行改进。改进后的新方案不但保留了 Harn 数字签名计算速度快的优点,而且能够有效抵抗同态攻击,并且在随机密钥 k 重复使用时,能够确保方案是安全的。

[参 考 文 献]

[1] 杨义先. 现代密码新理论[M]. 北京:科学出版社,2002. 106－110.

[2] Harn L. New digital signature scheme based on discrete logarithm[J]. Electronics Letters,1994,22(1):396－398.

[3] Nyberg K, Rueppel R A. Message recovery for signature schemes based on the discrete logarithm[A]. Advances in Cryptology[C]. Berlin:Springer-Verlag,1994. 175－190.

[4] 祁 明,肖国镇. 加强广义 ElGamal 型签名方案的安全性[J]. 电子学报,1996,24(11):68－72.

[5] ElG T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans Info Theory,1985,31(4):469－472.

[6] 卢开澄. 计算机密码学[M]. 北京:清华大学出版社,2003. 332－340.

[7] Schneier B. 应用密码学[M]. 吴世忠译. 北京:机械工业出版社,2000. 371－374.

[8] Ohta K,Okamoto T. A digital multisignature scheme based on the Fiat-Shamir scheme[A]. Advances in Cryptology[C]. New York:Springer-Verlag,1991. 139－148.

(责任编辑 吕 杰)