文章编号:1671-6833(2006)03-0101-03

一种基于DSA变体的盲签名方案

耿永军[1,2], 闫洪亮[2]

(1.华中科技大学计算机学院,湖北 武汉,430074;2.平顶山工学院计算机系,河南平 顶山,467001)

摘 要:盲签名在数字现金、电子投票等领域都有较大应用价值,特别是目前的数字现金,大部分是采用盲签名的原理实现的.通过对DSA数字签名机制进行改进,提出了一种新的DSA变体签名算法,改进算法中签名过程不再有求逆运算.然后,在DSA变体签名机制基础之上,提出一种安全、高效的基于DSA变体的盲签名方案.

关键词:数字签名;盲签名;DSA变体

中图分类号:TP 301.6 **文献标识码**:A

0 引言

常见的数字签名算法都是基于大整数的因子分解问题、离散对数问题和椭圆曲线离散对数问题三个难题之上[1],其安全性也是由这些难题保证的.数字签名标准(DSS)由美国NIST于1991年8月提出,于1994年底正式成为美国联邦信息处理标准.DSS中采用的用于签名的算法称为"数字签名算法"-DSA[2],其安全性基于离散对数问题的.DSA算法是ElGamal和Schnorr数字签名算法的改进,与RSA数字签名算法不同,DSA数字签名算法在每一次签名的时候,使用了随机数,所以它是概率签名,即对同一个消息签名,每次签名结果是不同的.盲签名是由David Chaum[3]于1983年提出的,盲签名在数字现金、电子投票等领域都有较大应用价值,特别是目前的数字现金,大部分是采用盲签名的原理实现的.盲签名能完成这样的功能:用户可以验证签名者签过名的消息,但签名者对已签名的消息却不知道其真实的内容.有关盲签名的各种方案可参看文献[3~5].笔者简要介绍了DSA数字签名机制,并对其进行改进,使改进DSA在签名阶段不再有求逆运算,签名速度提高了,验证签名的过程简化了.最后,在改进DSA签名机制基础之上,提出一种新的、安全高效的盲签名方案.

1 DSA及其变体签名算法的描述

1.1 DSA数字签名算法描述[5]

签名算法由算法参数的选定、签名和验证签名3个阶段完成,过程如下:

1.1.1 *算法参数的构成*

(1) 选取全局参数:p、q 是大素数,且 $q \mid p-1$,$g \in Z_p^*$,其阶为 q;

(2) 私钥参数:x 是一个随机数,且 $x \in Z_q^*$;

(3) 公钥参数:$y = g^x \bmod q$; (1)

1.1.2 *签名过程*

按如下两个步骤对消息 m 签名.

(1) 选择随机数 k,$k \in Z_q^*$,

(2) 计算 $r = (g^k \bmod p) \bmod q$,$s = (k^{-1}(H(m) + xr)) \bmod q$

签名结果为(r,s)发送给对方.

1.1.3 *验证过程*

(1) 计算 $v = (g^{(H(m)s^{-1}) \bmod q} y^{(rs^{-1}) \bmod q} \bmod p) \bmod q$

(2) 比较等式 $r = v \bmod q$,等式成立表示签名有效,否则无效.

1.2 DSA变体签名算法的描述

下面对DSA算法进行改进,得到一种改进的DSA变体数字签名算法,该变体算法也由三个阶段完成,第一阶段参数的构成与DSA基本签名一样,第二、三阶段如下:

1.2.1 *签名过程*

(1) 选择随机数 k,$k \in Z_q^*$,

(2) 计算 $R = g^k \bmod p$ (2)

$r = R \bmod q$ (3)

收稿日期:2006-04-25;**修订日期**:2006-06-11

作者简介:耿永军(1971—),男,河南襄县人,平顶山工学院讲师,华中科技大学在读博士研究生,主要从事网络安全方面的研究.

$$s = rk + mx \bmod q \tag{4}$$

签名结果为(γ, s),发送给对方.

1.2.2 验证过程

(1)计算 $t = R^{-r} \bmod p$

$$T = g^{-s} y^{m} \bmod p$$

(2) 比较等式 $t = T \bmod q$ 等式成立表示签名有效,否则无效.

1.2.3 算法证明

该算法是否成立,可如下证明:

$$\begin{aligned} T &= g^{-s} y^{m} \bmod p \\ &= g^{-rk - mx \bmod q} g^{xm \bmod q} \bmod p \\ &= g^{-rk \bmod q} \bmod q \\ &= R^{-r} \bmod p \\ t &= T \bmod q \end{aligned}$$

进一步说明,DSA 变体算法和 DSA 算法在求 s 时都进行两次乘和一次加运算,但 DSA 变体算法没有求 k^{-1}运算,所以在效率上高于 DSA 算法.攻击者试图通过 r 求出随机数 k,将面临求解离散对数问题,由于 k 是未知随机数,x 是密钥,知道 r 和 m 攻击者通过式 $s = rk + mx \bmod q$ 伪造签名是困难的,所以 DSA 变体签名算法安全性与 DSA 签名算法相当.

2 基于 DSA 变体的盲签名算法

全局参数和公私钥的选取于前面相同.

2.1 签名者 B 的准备工作

(1) 随机选择 $k \in {}_{R}Z_q^*$;

(2) 计算 $R = g^k \bmod p$;

2.2 用户 A 进行消息的盲变换

选择一个随机数作 a 为盲因子,$a \in Z_q^*$,计算 m',并且将 m'传送给 B;

$$m' = am \bmod q \tag{5}$$

2.3 签名者 B 进行盲签名

计算 s',然后 s'将传送给 A;

$$s' = Rk + m'x \bmod q \tag{6}$$

签名结果为(R, s')发送给用户 A.

2.4 A 取得消息的签名

计算 r 和 s,(r, s)等价于前面介绍的 DSA 变体签名算法生成的签名.

$$r = R \bmod q$$

$$s = s' + xm - amx \bmod q \tag{7}$$

2.5 验证过程

(1) 计算 $t = R^{-r} \bmod p$,

$$T = g^{-s} y^{m} \bmod p$$

(2) 比较等式 $t = T \bmod q$,等式成立表示签名有效,否则无效.

这和前面的 DSA 变体签名算法认证过程完全一样.

3 算法证明及安全性分析

3.1 算法证明

对盲签名验证阶段的等式 $t = T \bmod q$,进行证明如下:

$$\begin{aligned} T &= g^{-s} y^{m} \bmod p \\ &= g^{-s' - xm + amx + mx} \bmod p \\ &= g^{-Rk - mx + xma} \bmod q \\ &= g^{-Rk} \bmod p \\ &= R^{-r} \bmod p = t \bmod q \quad \text{得证.} \end{aligned}$$

3.2 安全性分析

按照盲数字签名的特征,用户请求签名者对明文消息 m 进行签名,签名者看到的是变换后的密文 m',在本方案中明文 m 乘以随机数 a 得到密文 m',而签名者想要由 m'求 m 相当于求大整数因子分解问题,所以签名者不可能看到明文消息 m.要伪造签名也是不可能的,知道 y、m、g、T,求 s 相当于求解离散对数问题.本盲签名方案的安全性是以大整数分解和离散对数问题为保证的,由于目前还没有对这两个问题有效的解法,所以本方案是安全的.合法用户进行盲变换处理信息之后,签名者得不到明文.同样基于大整数分解和离散对数难题,攻击者也就不可能得知双方交换信息的内容,也就无法对截获的信息进行流量分析、重传以及修改和伪造.因此,本方案满足盲数字签名的要求.

4 结束语

我们首先介绍 DSA 签名算法,然后对其进行改进,并提出基于 DSA 变体盲签名方案.盲因子是完全随机数,显然签名者不能获得所签署文件的内容,即使他签署用户上万份文件.但这些文件确实是他签署的,并可以在以后得到验证.该算法与基于 DSA 的盲签名算法相比,具有一样的安全性,但签名效率提高了,当有大量文档需要签名服务器进行签名时,可采用该方案以减轻签名服务器的负担.

参考文献:

[1] 张先红.数字签名原理及技术[M].北京:机械工业出版社.2004.

[2] NIST FIPS PUB 186, Digital Signature Standard(DSA),

National Institute of Standards and Technology, U. S. Department of Commence, 1994.

[3] CHAUM D, CAMENISCH J L, PIVETEAU J M, et al. Blind signature based on discrete logarithm problem[A]. Advances in Cryptology-EUROCRYPT'92 Proceeding[C]. Springer-verlog, 1992, 428 ~ 432.

[4] CHAUM D. Blind signature for untraceable payment[A]. Advances in Cryptology-EUROCRYPT'82 Proceeding[C]. Plenum Press, 1983, 199 ~ 203.

[5] Chaum D, FIAT A. Untraceable Electronic Cash[A]. Advances in Cryptology, Crypto'88, LNCS 403[C]. Springer-Verlag, 1988, 319 ~ 327.

A New Blind Signature Scheme Based on Convertible DSA

GENG Yong-jun[1,2], YAN Hong-liang[2]

(1. College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074 China; 2. Department of Computer, Pingdingshan Institue of Technology, Pingdingshan 467001, China)

Abstract: Blind signature plays a more and more important role in digital cash and electronic voting. Currently digital cash mainly adopts the theory of blind signature. This paper converted the DSA signature scheme and proposed a new secure and efficient blind signature based on convertible DSA. The improved algorithm does not involve the inverse calculation any more in the stage of signature.

Key words: digital signature; blind signature; convertible DSA

(上接第 100 页)

参考文献:

[1] BEEK J J V, SANDELL M, BORJESSON P O. ML estimation of time and frequency offset in OFDM systems[J]. IEEE Transactions on Signal Processing, 1997, 45(7): 1800 ~ 1805.

[2] MOSTOFI Y, COX D C. Timing synchronization in high mobility OFDM systems[A]. 2004 IEEE International Conference on Communications[C]. New York. 2004. 4: 2402 ~ 2406.

[3] MINN, ZENG M, BHARGAVA V K. On Timing Offset Estimation for OFDM Systems[J]. IEEE Communications Letters, 2000, 4(8): 242 ~ 244.

[4] LIU S Y, CHONG J W. A Study of Joint Tracking Algorithms of Carrier Frequency Offset and Sampling Clock Offset for OFDM - Based WLANs[A]. 2002. IEEE International Conference on Communications[C]. New York. 2002. 109 ~ 113.

[5] IEEE Std 802.11a - 1999(R2003). Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High - speed Physical Layer in the 5GHz Band[S].

A Simple Timing Synchronization Algorithm for IEEE 802.11a WLANs

ZHAO Shu-guang, CHEN Rong, ZHAO Min

(The 28th Institute of China Electronics Technology Group Corporation, Nanjing 210007, China)

Abstract: Timing synchronization is a key technology in OFDM systems. Based on training sequences of IEEE 802.11a standard, we propose a simple correlation timing synchronization scheme. Improved auto - correlation function reduces stochastic fluctuation of function value significantly. Therefore, it is possible to choose optimal detection threshold. Moreover, increased detection width obviously extends application range of correlation algorithm. Simulation results illustrate that when frame detection probability is 90% and frequency offset is 200kHz, SNR of proposed algorithm improves 8dB compared with that of traditional algorithm.

Key words: orthogonal frequency division multiplexing; training sequence; timing synchronization