

Schnorr 数字签名的零知识证明

汤鹏志, 李 彪

(华东交通大学 基础科学学院, 江西 南昌 330013)

摘 要: 为防止数字签名的任意传播, 提出一种 Schnorr 数字签名的零知识证明协议. 签名者提供给接收方的不是消息的签名信息, 而是提供零知识证明协议的交互信息. 接收方通过交互信息不能获知任何与签名相关信息, 但可确信签名者拥有签名信息. 通过方案分析可知, 该协议已经具备安全性和可行性.

关键词: 零知识证明; 数字签名; 协议; Schnorr; 安全分析

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)06-0177-03

Zero-knowledge Proof Scheme of Schnorr Digital Signature

TANG Peng-zhi, LI Biao

(School of Basic Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: In order to prevent any spread of digital signatures, this paper propose a zero-knowledge proof scheme of Schnorr digital signature. Signer do not provide the signature information to Receiver, but provide the interactive information of zero-knowledge proof scheme. Receiver can not use interactive information to learn sign information, but Receiver Confident that Signer own signature information. this scheme has not only lower Data traffic, but also higher security.

Key words: zero-knowledge proof; digital signature; scheme; schnorr; safety analysis

1 引言

在普通数字签名协议中, 签名者对消息签名后的信息都是可以公开验证的. 验证者只需拥有签名信息和签名者的公钥, 就可以按照协议规定的验证算法验证签名信息的合法性. 1989 年 Chaum 和 Antwerpen 提出的不可否认的数字签名^[1], 可以控制验证者只有在签名者的配合下, 才能验证签名信息的有效性. 但这种签名体制存在缺点: 签名者主观上不愿意合作或者客观上无法进行合作时, 所产生的数字签名就得不到合法的验证. 舒麟等^[2]在前人的基础之上, 提出一种防止 DSA 数字签名任意传播的方法. 签名者提供给验证者的不是消息的 DSA 数字签名^[3], 而是该消息数字签名的一个零知识证明^[4]. 该方案比不可否认签名方案验证更简单, 且不

需要签名者的参与就能控制数字签名的任意传播. Schnorr 数字签名算法^[5], 是一种高效的签名算法, 且广泛应用于电子商务领域中. 为防止 Schnorr 数字签名的任意传播, 本文提出一种 Schnorr 数字签名的零知识证明. 该方案信息交互次数少, 降低数据传输的开销和中间人攻击的可能性, 使得方案具有更强的安全性.

2 基础理论

2.1 零知识证明

零知识证明 (Zero-knowledge Proof), 是 1985 年 Goldwasser 等人提出的交互式证明方案. 它是指证实者 (Prover) 在不向验证者 (Verifier) 提供任何有用信息的情况下, 使验证者相信自己拥有某种知识. 在信息安全的研究领域中, 零知识证明的存在是

收稿日期: 2011-10-30; 修回日期: 2011-12-26

基金项目: 国家自然科学基金项目 (11061014); 江西省教育厅青年科学基金项目 (GJJ10129); 江西省教育厅科研项目 (GJJ10708)

非常有价值的。

2.2 Schnorr 数字签名算法

1989 年 C. Schnorr 在 ElGamal 签名^[6]体制基础上,提出一种全新的基于离散对数数字签名方案 Schnorr. 它拥有计算量少,速度快的特性,得到广泛的应用. Schnorr 的签名算法:

设系统的公开参数是 (p, q, g, H) . 其中 p 是大于 1024 bit 的整数, q 是大于等于 160 bit 的整数, $q | p-1$, g 是乘法群 Z_p^* 中阶为 q 的元素, $H: \{0, 1\}^* \rightarrow Z_p$ 为安全抗碰撞的哈希函数^[7]. 系统随机地选择 $x \in Z_q^*$, 作为证实者的密钥; 计算 $y = g^x \bmod p$, 作为证实者的公钥; 私钥通过秘密信道传送给证实者, 公布 y 为证实者的公钥. 证实者随机选取 $k \in Z_q^*$, 然后计算 $r = g^k \bmod p$, $e = H(r || M)$ 和 $s = k + xemodq$, 其中 $||$ 是字符串的级联符号. 则消息 M 的 Schnorr 数字签名为 (r, s) .

验证者收到消息 M 及签名 (r, s) 后, 验证 $g^s \equiv ry^{H(r || M)} \bmod p$. 若等式成立, 则称 (r, s) 是消息 M 在公钥 y 下的有效签名. 在 Schnorr 签名方案中, 因为证实者选择了随机数 k , 所以同一证实者对消息 M 可以产生不同的签名 (r, s) .

3 Schnorr 数字签名的零知识证明方案

设 p 是大于 1024 bit 的整数, q 是大于等于 160 bit 的整数, $q | p-1$, g 是乘法群 Z_p^* 中阶为 q 的元素, $H: \{0, 1\}^* \rightarrow Z_p$ 为安全抗碰撞的哈希函数. 系统公开参数 (p, q, g, H) .

3.1 用户的密钥生成

系统随机地选择 $x \in Z_q^*$, 作为证实者 P 的密钥; 计算 $y = g^x \bmod p$, 作为证实者 P 的公钥; 私钥通过秘密信道传送给证实者 P , 公布 y 为证实者 P 的公钥.

3.2 签名信息生成

现有消息 $M \in \{0, 1\}^*$ 需要证实者 P 进行签名. 证实者 P 随机选取 $k \in Z_q^*$, 然后计算 $r = g^k \bmod p$, $e = H(r || M)$ 和 $s = k + xemodq$, 其中 $||$ 是字符串的级联符号. 则 $\delta = (r, s)$ 为消息 M 的正常 Schnorr 数字签名.

3.3 签名的零知识验证协议

证实者 P 在不提供消息 M 的数字签名 δ 的情况下, 必须使得验证者 V 确信自己拥有消息 M 的签名 δ . 证实者 P 和验证者 V 需要通过执行以下零知识证明协议, 向验证者 V 证明证实者 P 确实拥有签名信息 δ :

$$\begin{aligned} ZPK \{ \alpha, \beta \mid c_1 = (g^\beta \bmod p)^{k_1} \bmod q \wedge c_1 = \\ (\alpha y^{H(\alpha || M)} \bmod p)^{k_1} \bmod q \} (m, \text{Timestamp}) \in \\ Z_p \times Z_p \times Z_q \times \{0, 1\}^l \end{aligned} \quad (1)$$

在零知识证明协议中, 通过 α 和 β 来表示证实者 P 拥有的签名信息 δ , 其中 $\alpha = r, \beta = s$; 验证协议中的时戳: Timestamp. 协议的具体步骤如下所述:

(1) 证实者 P 任意选择随机数 $k_1, k_2 \in Z_q^*$, 首先计算:

$$c_1 = (g^\beta \bmod p)^{k_1} \bmod q \quad (2)$$

然后计算:

$$c = H(M || p || q || g || y || \text{Timestamp} || c_1) \quad (3)$$

(2) 证实者 P 使用签名信息 δ , 计算:

$$s_1 = ((\alpha y^{H(\alpha || M)} \bmod p)^{k_1} y^{(k_2 c - k_1 \bmod q)}) \bmod q \quad (4)$$

$$s_2 = k_1 - k_2 c \bmod q \quad (5)$$

并发送 $\{c, s_1, s_2, \text{Timestamp}\}$ 给验证者 V .

(3) 验证者 V 收到消息 $\{c, s_1, s_2, \text{Timestamp}\}$ 后, 验证等式是否成立:

$$\begin{aligned} c = H(M || p || q || g || y || \text{Timestamp} || \\ (s_1 y^{s_2} \bmod p)) \end{aligned} \quad (6)$$

若等式成立, 验证者 V 信任证实者确守拥有消息 M 的签名信息 (r, s) ; 否则, 拒绝相信证实者拥有签名信息.

4 方案分析

4.1 正确性分析

在零知识验证协议中, 根据式(1)和式(3)可知, 等式:

$$(g^\beta \bmod p)^{k_1} = (s_1 y^{s_2} \bmod p) \bmod q \quad (7)$$

的成立等同于等式(6)的成立.

将式(4)和式(5)代入式(7)右边, 进行运算:

$$\begin{aligned} s_1 y^{s_2} \bmod p \bmod q \\ = (\alpha y^{H(\alpha || M)} \bmod p)^{k_1} y^{(k_2 c - k_1 \bmod q)} \\ \times y^{k_1 - k_2 c \bmod q} \bmod p \bmod q \\ = (\alpha y^{H(\alpha || M)} \bmod p)^{k_1} \bmod q \end{aligned}$$

由式(1)可知, 式(6)的左边等于右边, 则上述零知识证明协议方案是正确的.

4.2 安全性分析

零知识验证协议方案的目的是: 让验证者 V 信任证实者 P 拥有消息 M 的签名信息 δ . 协议的运行过程中, 可能存在以下三种攻击形式:

(1) 证实者 P 的不诚实行为. 证实者 P 没有使用消息 M 的数字签名 δ , 而是用伪造的签名信息 $\delta^* = (r^*, s^*)$ 执行上述协议, 试图得到验证者 V 的信任. 但证实者 P 无法构造式(6)的成立, 原因在于式

(6) 中存在着 Schnorr 签名验证等式的变形结构和安全的抗碰撞哈希函数 H .

(2) 攻击者 A 冒充证实者 P 的行为. 攻击者 A 企图冒充证实者 P 与验证者 V 交互, 从而获取验证者 V 的信任. 第一, 攻击者 A 无法获取证实者 P 对消息 M 的数字签名 δ , 无法取得直接交互的信任. 第二, 如若伪造签名信息 δ^* , 攻击者 A 同样不能满足式(6)的成立, 无法取得间接交互的信任.

(3) 攻击者 A 的重放攻击. 攻击者 A 通过网络监听, 获得协议的交互信息 $\{c, s_1, s_2, \text{Timestamp}\}$, 妄想通过重放该信息取得验证者 V 的信任. 但等式(6)的验证过程中, 使用了证实者 P 的公钥 y , 然而公钥信息是通过公钥证书进行共享的. 攻击者 A 和证实者 P 的身份不一致, 验证者 V 无法信任攻击者 A 具有消息 M 的签名信息 δ .

上述协议方案中, c 的计算是在抗碰撞的哈希函数下进行的, 无法从 c 中获得任何有意义的信息; s_1 的计算是在 Z_q^* 的离散对数问题困难之下, 它的公布也不能从中获取任何有用的信息; s_2 是由证实者 P 任意选择的随机数 k_1, k_2 和 c 计算而来, 无法获知任何有价值的信息. 验证者 V 无法从协议的交互信息 $\{c, s_1, s_2, \text{Timestamp}\}$ 中, 获取任何与消息 M 的签名信息 δ 相关信息, 故上述方案是一个安全的零知识证明验证协议.

5 结束语

Schnorr 数字签名的零知识证明验证协议中, 证实者和验证者之间只存在一次信息交互, 减少数据传输的开销和中间人攻击的可能性, 安全性得到了有力的提升. 又由于协议仅在证实者和验证者之间进行, 从而可以应用于软件产品的版权保护中, 避

免签名信息的肆意传播.

参考文献:

- [1] Chaum D, Van Antwerpen H. Undeniable signatures [C] // Proceedings of the Advances in Cryptology (CRYPTO'89). Berlin: Springer-Verlag, 1990: 212-216.
- [2] 舒麟, 廖闻剑, 彭艳兵. 拥有 DSA 数字签名的零知识证明[J]. 计算机工程与应用, 2011, 47(16): 120-121.
- [3] National Institute of Standards and Technology. NIST FIPS PUB186 Digital signature standard[S]. Department of Commerce, NIST, 1994.
- [4] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems [C] // Proceedings of the 17th Annual ACM Symposium on Theory of Computing. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 1985: 291-304.
- [5] Schnorr C P. Efficient signature generation for smart cards[J]. Advances in cryptology-crypto'89 proceedings, Springer-Verlag, 1991: 239-252.
- [6] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans on Info Theory, 1985, 31(4): 469-472.
- [7] Wang Xiao-yun, Yu Hong-bo. How to break MD5 and other hash functions [C] // Cramer R. LNCS 3494: Advances in Cryptology-EUROCRYPT, 2005. [S. 1]: Springer, 2005: 19-35.

作者简介:

汤鹏志 男, (1964—), 硕士, 教授, 硕士生导师. 研究方向为信息系统及其安全.

李彪 男, (1988—), 硕士研究生. 研究方向为信息安全.

(上接第 176 页)

- [6] Yun Chiu. High-performance pipeline A/D converter design in deep-submicron CMOS [M]. University of California, Berkeley, 2004.
- [7] 刘蒲霞, 陆铁军, 王宗民. 16 位流水线 ADC 系统级建模及仿真[J]. 微电子学与计算机, 2009, 26(12): 120-124.
- [8] 彭隽, 马洪, 胡啸. 一种流水线 ADC 级间增益非线性误差的数字域补偿方法[J]. 微电子学与计算机, 2011, 28(2): 120-123.

作者简介:



丁洋 女, (1987—), 硕士研究生. 研究方向为高速高精度流水线 ADC 的设计.