文章编号:1005－0523(2007)04－0144－03

一个基于 Schnorr 算法的可公开验证的加密方案

吴晓波[1],辛 英[2],曲 慧[2],陆洪文[3]

(1.烟台职业学院 软件工程学院,山东 烟台 264003;2.山东工商学院 数学学院,山东 烟台 264005;
3.同济大学 应用数学系,上海 200092)

摘要:基于离散对数问题和 Schnorr 算法提出了一个新的有效的认证加密方案,新方案具有以下优点:该方案在不暴露消息明文的情况下,任何第三方都可验证签名的有效性,实现公开验证;降低了计算量和占用带宽;在签名中加入了时间戳,能够有效防止重发密文攻击.

关 键 词:Schorr 算法;认证加密;随机预言模型
中图分类号:O29 **文献标识码**:A

随着计算机与通信技术的发展,信息安全问题也越来越被人们关注,如何安全、有效、可认证地对消息进行传输/存储成为一个重要的研究内容.为了验证传送信息的真实性和证明当事者的身份,数字签名是必不可少的技术,可认证的加密方案就是由此而被提出的一个新的密码学概念.认证加密方案的优点在于可以同时实现消息的机密性与完整性,与直接分别使用对消息进行加密和签名方法相比,认证加密在实现消息的机密、完整与认证等功能时需要更小的通信代价与计算量.1993 年,Nyberg 和 Rueppel[1]提出了具有消息恢复的新型数字签名方案,该方案是数据加密与数字签名密码技术的结合.在此基础上一些具有低通信代价的认证加密方案被提出[2],然而它们不能有效解决签名者否认签名等问题.1999 年,Araki 等[3]首次提出了一种可转换的认证加密方案,在他们的方案中,如果签名者否认签名,接收者可将认证加密签名转换为一般的签名,使任何人都可以验证签名的有效性.然而 Wu 和 Hsu[4]指出 Araki 等的方案中,接收者要实现签名转换需签名者的合作,这样不仅占用带宽和增加计算量,更重要的是如果签名者不合作,接收者无法单独完成签名转换.本文提出了一个新的可公开验证的认证加密方案.新方案具有以下优点:首先在通信占用带宽以及计算量方面非常有效;其次该方案无需转换可允许任何第三方验证签名,实现公开验证;第三在签名中加入了时间戳,可以有效防止重发密文攻击.

1 新的认证加密方案

方案参与者:签名者 Alice、接受方 Bob 及密钥分发中心 CA.

1.1 方案的初始化

在方案中由 CA 中心按照以下过程产生系统用户的共享公钥(p,q,g).

(1) 由密钥中心 CA 产生两个大素数 p 和 q,$2^{511}<p<2^{512}$,$2^{139}<q<2^{140}$,q 是 $p-1$ 的素因子,按 Schnorr 身份鉴别与数字签名协议[5]中产生 p 和 q 的过程,先产生素数 q,然后再去找到相应的 p.再选择 $g\in Z_p=\{0,1,2,\cdots,p-1\}$ $(g\neq 1)$,满足 $g^q\equiv 1 \pmod p$ 而 $g^k \pmod p \neq 1$,$k=1,2,\cdots,q-2$.将 g、p、q 公开作为所有用户的公钥.选择安全散列函数 $H(\cdot)$,如 SHA－1 算法.

收稿日期:2007－03－18
基金项目:国家自然科学基金资助项目(10471104),上海市科委基金资助项目(03JC14027).
作者简介:吴晓波(1979－),女,山东蓬莱人,助教,研究方向:计算机网络与信息安全.

(2) 系统中的每个用户都要注册其身份. 签名者 Alice 向 CA 中心注册其身份 ID_A(可以是姓名、地址、电子邮件地址等等信息)，并选择随机数 x_a 发给 CA 中心，CA 计算 $y_a=g^{x_a}(\mathrm{mod}p)$；同样 Bob 也向 CA 中心注册其身份 ID_B，并选择随机数 x_b 发给 CA 中心，CA 计算 $y_a=g^{x_b}(\mathrm{mod}p)$. 随机数 x_a，x_b 分别为 Alice 和 Bob 的秘密私钥，y_a，y_b 是其公钥，由 CA 中心公布.

1.2　签名加密

Alice 可电话通知 Bob，有一则消息 $m\in Z_p^*=\{1,\cdots,p-1\}$要发给 Bob.

(1) Alice 随机选择 $1<k<q$，计算 $A=g^k(\mathrm{mod}p)$，$B=m\times y^k b(\mathrm{mod}p)$.

(2) 计算 $r=H(A\parallel B\parallel ID_A\parallel ID_B\parallel t_A^*)$，其中“‖”表示连接符号，$t_A^*$ 表示 Alice 的当前时间戳.

(3) 计算 $s=(k-r)x_a^{-1}(\mathrm{mod}p-1)$.

(4) 将(r,s,B,t_A^*)作为其对消息 m 的签名，密文发给 Bob.

1.3　验证签名

Bob 收(r,s,B,t_A^*)后，计算 $Vt=t_B-t_A^*$，t_B 是 Bob 收到密文的时间，如果 Vt 超过规定时间，则拒绝签名，否则执行以下步骤：

(1) 计算 $A'=g^r y_a^s(\mathrm{mod}p)$.

(2) 验证 $H(A'\parallel B\parallel ID_A\parallel ID_B\parallel t_A^*)=r$. 若等式成立，则认可签名正确，即确认 Alice 的真实身份；否则拒绝签名.

(3) 当验证签名正确时，Bob 可恢复出消息 $B(A')^{-x_b}(\mathrm{mod}p)=m$.

注意在这个阶段，经过(1)、(2)验证签名时，没有用到 Bob 的私钥，从而任何第三方都可以验证签名，确定签名者的真实身份，并且无需转换，达到可公开验证的目的；但第三方无法继续(3)，因为在计算离散对数困难假设下，第三方并不知道 Bob 的私钥 b，故只有合法接收方 Bob 才能恢复出消息 m，其他任何第三方无法恢复 m.

1.4　签名证明

首先：事实上，$A'=g^r y_a^s(\mathrm{mod}p)\equiv g^r\cdot(g^{x_a})^{(k-r)x_a^{-1}}\equiv g^k(\mathrm{mod}p)=A$，所以有 $H(A'\parallel B\parallel ID_A\parallel ID_B\parallel t_A^*)=r$，从而任何第三方都可以验证签名.

其次：$B(A')^{-x_b}(\mathrm{mod}p)\equiv(m\times y_b^k)\cdot(g^k)^{-x_b}\equiv m\times y_b^k\times y_b^{-k}(\mathrm{mod}p)=m$，故只有 Bob 可以恢复消息 m.

2　方案的安全性讨论

这部分将引入随机预言模型(Random Oracle Model)[6]，讨论该认证方案是否满足签名方案应该具有的不可伪造性和安全机密性. 假设有一个敌对攻击者 Eve.

定理 1　基于离散对数的困难性假设，如果没有获得签名者 Alice 的秘密数 k，x_a，敌对者 Eve 无法成功伪造有效签名.

证明　由于 Elgamal 签名方案、Schnorr 签名都可被看作随机预言模型[6]，同样该方案也可看作类似模型.

利用 Forking 引理[6]，假若在适应性选择密文攻击的条件下，敌对者 Eve 经过多次询问，以不可忽略的概率伪造了两个有效签名(r,s,B,t_A^*)、(r',s',B,t'_A)，其中 $r\neq r'$，$s\neq s'$，则可以得到两个同余式 $\begin{cases}k=r+x_a s(\mathrm{mod}p-1)\\k=r'+x_a s'(\mathrm{mod}p-1)\end{cases}$，那么就有可能以不可忽略的概率在多项式时间里求解出 x_a，k，这与解决有限域 F_p 上的离散对数问题的困难性相矛盾.

所以提出的新的认证加密方案满足不可伪造性.

定理 2　基于求解离散对数问题的困难性假设，该方案可有效抵抗重发密文攻击.

证明　签名时加入时间戳 t_A^* 能够方便的提供给 Bob 实体认证，时间差 $Vt=t_B-t_A^*$ 保证签名的新鲜性属性. 如果敌对者 Eve 获得一份以前的签名密文(r,s,B,t_A^*)，他可以将时间戳 t_A^* 换成当前时间 t_0，如同定理 1 一样，利用 Forking 引理，可以证明，在基于求解离散对数问题的困难性假设下，Eve 无法改掉签名中的 r 所含有的时间戳 t_A^*，因而可以有效抵抗重发密文攻击.

定理 3　签名方程 $s=(k-r)x_a^{-1}(\mathrm{mod}p-1)$的优点是其安全性基于两个困难问题的复杂度：计算 Z_p^* 上的 q 阶循环子群的对数和分解 $p-1$. 如果其中任意一个是困难的，那么计算 Z_p^* 上的离散对数也是困难的.

详细证明请见[6].

根据 ElGamal 加密方案已经在选择明文攻击的条件下证明是安全的，可以推出所提的方案满足机密性.

3 有效性分析

从计算量考虑,该方案产生签名所需的大部分计算都可在系统初始化阶段完成,并且与待签名的消息无关,这样可在空闲时间计算,不影响签名速度,Alice 和 Bob 仅需要一次散列、一次模逆和两次模幂运算;对于相同的安全级,该方案的签名长度比 Elgamal 短的多,仅需要传送 $|p|+|q|+|H(\cdot)|$ 比特,所以占用带宽低.

4 结束语

本文提出了一个新的可公开验证的认证加密方案,并且证明了该方案是安全的,该方案具有下列优点:签名中加入了时间戳,能够有效防止重发密文攻击;签名与消息解密两个步骤可以分离,无需转换可允许任何第三方验证签名,实现公开验证;在通信占用带宽以及计算量方面具有较高效率.可以被应用到电子货币、移动支付等电子商务领域.

参考文献:

[1] Nyberg K, Rueppel R. A new signature scheme based on the DSA giving message recovery[R]. Proceeding of the FirstACM Conf on computer and Communications Security, Fairfax, VA, 1993.

[2] Horster P, Michels M, Petersen H. Authenticated encryption schemes with low communication costs [J]. Electron Letters1994, 30(15): 1212—1213.

[3] Araki S, Uehara S, Imamura K. The limited verifier signature and its application[J]. ICICE Transactions on Fundamentals, 1999, E82—A(1): 63—68.

[4] Wu T S, Hsu C L. Convertible authenticated encryption scheme [J]. Journal of System and Software, 2002, 62(6): 205—209.

[5] 施奈尔(Schneider, B). 吴世忠, 祝世雄, 张文政等译. 应用密码学:协议、算法与C原程序[M]. 北京:机械工业出版社, 2000.

[6] Pointcheval D, Stern J. Security Proofs for Signature Schemes [C]. Proc. of Euro—crypt '96, LNCS 1070, Springer—Verlag, 1996: 387—398.

A New Authenticated Encryption Scheme with Public Verifiability Based on Schnorr Algorithm

WU Xiao-bo[1], XIN Ying[2], QU Hui[2], LU Hong-wen[3]

(1. School of Software Engineering, Yantai Vocational College, Yantai, Shandong 264003; 2. College of Mathematics, Shandong Institute of Business and Technology, Yantai, Shandong 264005; 3. Department of Applied Mathematics, Tongji University, Shanghai 200092, China)

Abstract: A new authenticated encryption scheme is proposed based on the discrete logarithm and Schnorr algoritnm. The scheme bears the following characteristics: anyone can identify its source which obtains public verifiability without disclosing any messages; it reduces the com—putting complexity and band—width; the timestamp has been adopted which can resist the attack which sends cryptograph continuously.

Key words: Schnorr algorithm; authenticated encryption; random oracle model