对Schnorr签名方案几种攻击的分析

胡国政[1,2] 洪 帆[1]

(华中科技大学计算机科学与技术学院 武汉 430074)[1] (武汉理工大学理学院数学系 武汉 430073)[2]

摘 要 Schnorr签名方案是一个基于离散对数的数字签名方案。最近,一些文献提出了新的攻击该签名方案的方法,并声称这些新的攻击成功率很高。分析了这些攻击方法,认为这些新的攻击本质上是平凡的穷搜索攻击。在系统给定的安全参数下,这些攻击成功的概率是可以忽略的。还指出了这些攻击成功率分析中的错误。

关键词 Schnorr签名,密码分析,穷搜索攻击

中图法分类号 TP309.7 **文献标识码** A

Analysis of Some Attacks against the Schnorr Signature Scheme

HU Guo-zheng[1,2] HONG Fan[1]

(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]

(School of Science, Wuhan University of Technology, Wuhan 430073, China)[2]

Abstract The Schnorr signature scheme is a digital signature scheme based on discrete logarithms. Recently some attacks against the Schnorr signature scheme were presented in the literature and they claimed that these new attacks had the greater success probability. However, these attacks were analyzed and the conclusion is that all these new attacks are essentially trivial exhaust search ones. Given certain system security parameters, the success probability of theses attacks is negligible. Moreover, some mistakes in the probability analysis of these attacks were pointed out.

Keywords Schnorr signature, Cryptanalysis, Exhaust search attack

1 引言

自1976年Diffie和Hellman[1]首先提出公钥密码后,数字签名成为了最有用和最基本的密码原型之一。Rivest, Shamir和Adleman[2]给出了第一个实用的数字签名方案,但它却不安全。早期对签名方案安全的研究是启发性的:如果没有找到攻击方法,就说该方案安全。实际上,早期许多签名方案是不安全的,即在适应性选择消息攻击下存在性可以伪造。于是,可证安全成为设计数字签名方案的基本要求。数字签名方案的形式化安全模型首先是由Goldwasser, Micali和Rivest[3]于1988年提出的,他们同时还提出了一个满足该安全模型却不实用的签名方案。

为了设计出既安全又实用的密码方案,Bellare和Rogaway[4]提出了利用理想的散列函数作为桥梁来设计高效密码方案的新方法,即所谓的随机预言模型。在该模型中,假设散列函数的输出像一个真正的随机数生成器。此后,有大量的签名方案被提出,且在随机预言模型中证明是安全的[5-8]。

Schnorr签名方案[9,10]是Schnorr于1989年提出的一个基于离散对数的高效的签名方案,但是直到1996年,Pointcheval[11]等人才给出它的形式化安全证明。在计算离散对数问题是困难的假设下,证明了该签名方案在随机预言模型中的存在性不可伪造。

最近,刘景美和王新梅[12]给出了对Schnorr签名方案的两种攻击方法:一种是选择消息下的攻击方法,攻击者可以假冒签名者进行签名;另一种是给出了一种攻击签名者私钥的选择消息攻击方法,其攻击性不依赖于离散对数的求解问题。文献[13]也对Schnorr签名方案提出了本质上一样的两种攻击方法。

2 Schnorr签名方案

下面描述Schnorr于1989年提出的基于离散对数的数字签名方案。

(1)系统参数

p,q:大素数,$q|p-1$,q是大于等于160bit的整数,p是大于1024bit的整数;

g:Z_p^*中元素,且$g^q=1 \bmod p$;

$H(\cdot):\{0,1\}^* \rightarrow Z_p$:密码散列函数;

x:用户私钥,$x \in Z_q^*$;

y:用户公钥,$y=g^x \bmod p$。

则全局系统参数为(p,q,g,H),签名者的公钥为y,私钥为x。

(2)签名过程

1)签名者选择秘密随机数$k \in Z_q$;

2)依次计算$r=g^k \bmod p$,$e=H(r||M)$和$s=k+xe \bmod$

到稿日期:2008-11-04 返修日期:2009-01-21 本文受国家自然科学基金项目(60703048),湖北省自然科学基金项目(2007ABA313)资助。

胡国政(1967-),男,博士研究生,主要研究方向为密码学和信息安全,E-mail:huguozheng@whut.edu.cn;洪 帆(1942-),女,博士生导师,主要研究方向为访问控制、密码学和信息安全。

q,其中||是字符串的级联符号;

3)将(e,s)作为消息M的签名送给验证者。

(3)验证过程

验证者收到消息M及签名(e,s)后,计算$r'=g^s y^{-e} \bmod p, e'=H(r'||M)$,验证$e'=e \bmod p$。若等式成立,则称$(e,s)$是消息$M$在公钥$y$下的有效签名。在这个签名方案中,对同一消息$M$,由于随机数$k$不同而有不同的签名$(e,s)$。

说明:文献[12]描述的Schnorr签名方案出现多处错误:(1)实际上Schnorr签名方案的签名是(e,s)而不是(r,s)。当然,这样写并没有改变Schnorr签名方案的安全性,只是增长了签名长度。(2)系统参数中没有介绍重要的参数——散列函数。(3)错误地把Z_q^*看作是由g生成的Z_p^*的子群。

3 文献[12]对Schnorr签名方案的攻击

下面给出文献[12]对Schnorr签名方案的两种攻击方法。除了少数笔误外,为了便于下一节的分析,基本未改变文献[12]的叙述。

方法一 伪造(r,s)的攻击

攻击者收集签名者的正确签名集$M_1,(r_1||s_1)$和$M_2,(r_2||s_2)$,若需要签名的消息为M',则进行如下计算:

(1)计算$r'=r_1 r_2 (\bmod p)$

(2)计算$e'=H(r'||M') \bmod p$

(3)计算$e_1=H(r_1||M_1) \bmod p$

(4)计算$e_2=H(r_2||M_2) \bmod p$

若集合中有签名使得$e'=e_1+e_2 \bmod p$,则攻击者可以选择这个签名集$M_1,(r_1||s_1)$和$M_2,(r_2||s_2)$,来实施攻击行为,然后进行后续的计算$s'=s_1+s_2 \bmod p$,则$M',(r'||s')$就是攻击者假冒签名者进行的正确签名,因此假冒者伪造签名成功。也就是说,只要攻击者选取一个满足要求的合法签名,则攻击者可以伪造任何合法的签名,因此说Schnorr签名方案是极其不安全的。鉴于一般签名的特殊性质,即任何人都可以验证签名的有效性,签名者可以对多份文件进行签署,只要攻击者选取了任何一个需求的签名,就可以伪装签名者进行非法的签名。已发现的对Schnorr签名方案的伪造签名大多存在离散对数的求解问题,实际中能否进行有效的攻击还难以确定。该攻击方案的提出无疑给签名的安全性提出了新的挑战。

方法二 对私钥x的攻击

另外,攻击者可以不用上述过程来进行伪造签名,而是直接攻击签名者的私钥。攻击过程也是选取签名集合,验证签名是否满足如下的关系:

$y^e \equiv 1 \bmod p \Rightarrow g^{xe} \equiv 1 \bmod p$。

若对某一签名满足上式,就选择这个签名进行攻击,因为g是Z_p^*中子群Z_q^*的一个生成元,即$g^q \equiv 1 \bmod p$,所以$g^{xe}=g^{tq}$,即$xe=tq$,于是$x=tqe^{-1} \bmod p$。其中t的计算过程为:

$t=0$;

while$(y^e=1)\{y^e=y^e/g^{p-1};t++;\}$。从而求出了签名者的私钥,攻击者可以利用签名者的私钥对任意的消息进行签名。下面来看一下这种攻击的概率分析。

攻击的重点是$y^e=g^{xe} \equiv 1 \bmod p$,因为$g^q \equiv 1 \bmod p$,所以$q|xe$,也就是说$\gcd(x,q)\neq 0$或$\gcd(e,q)\neq 0$。因为$x$是一个未知量,所以从已知量$e$出发来分析。设$\{\beta\}=\{\gamma:\gamma|q\}$,不同的$\gamma$对应不同的$e$值,则$e$出现的概率为$p(r)=1/[q-1-\Phi(q)]$,其中$\Phi(q)$表示$q$的欧拉函数值,也就是$Z_q$中与$q$互素的元素的个数,只要指定不同的$e_i$,就可以求出具体的私钥$x_i$的个数$\|\beta_i\|, i=1,2,\cdots,\|\beta\|$。因此,满足式子$q|xe$的$xe$出现的概率为$p(xe)=\sum_{i=1}^{\beta}\|\beta_i\|/[q-1-\Phi(q)]$。若$\varphi(q)$很大,则$q|xe$将以很大的概率出现,也就是说攻击者选择不多的正确签名就可以进行成功的攻击。

4 分析文献[12]中的攻击

4.1 分析伪造(r,s)的攻击

在这种攻击方法中,攻击者的出发点是在收集到的签名集合中寻找满足$e'=e_1+e_2 \bmod p$的签名$M_1,(r_1||s_1)$和$M_2,(r_2||s_2)$。这个方法本质上是穷搜索攻击。在Schnorr方案所给定的系统安全参数和现有最好的计算离散对数算法条件下,从正确生成的签名集合中搜索到满足这个条件的一对签名$M_1,(r_1||s_1)$和$M_2,(r_2||s_2)$的成功率可以忽略不计。另外,文献[12]认为g是Z_p^*中子群Z_q^*的一个生成元,这是不对的。首先,Z_q^*不是Z_p^*的子群。其次,由g生成的群不是Z_q^*。在Schnorr签名方案中,g是群Z_p^*中阶为q的元素,由它生成的群并不是Z_q^*。若记生成元g生成的群为$\langle g\rangle$,则$\langle g\rangle=\{h|h=g^k \bmod p, k=1,\cdots,q\}$。

4.2 分析对私钥x的攻击

在这种攻击方法中,攻击者的出发点是在收集到的签名集合中寻找满足方程$y^e \equiv 1 \bmod p$即$g^{xe} \equiv 1 \bmod p$的签名$M,(r||s)$,从而达到获得签名者的私钥这个目的。这个攻击方法本质上也是穷搜索攻击。在Schnorr方案所给定的系统安全参数和现有最好的计算离散对数算法条件下,从正确生成的签名集合中搜索到满足这个条件的一个签名$M,(r||s)$的成功率可以忽略不计。

另外,在文献[12]对攻击的概率分析中,还存在其他错误。

(1)由$q|xe$得到了$\gcd(x,q)\neq 0$或$\gcd(e,q)\neq 0$。实际上,对于任意非零整数,它们之间的最大公约数总是正整数。由于q是比x和e都大的大素数,因此总有$\gcd(x,q)=1$和$\gcd(e,q)=1$。

(2)令$\{\beta\}=\{\gamma:\gamma|q\}$。由于$q$是大素数,因此$\gamma=1$或者$\gamma=q$,从而$\|\beta\|=2$。由于$q$是大素数,因此欧拉函数$\varphi(q)=q-1$,从而$q-1-\Phi(q)=0$,即$q|xe$的$xe$出现的概率表达式$p(xe)=\sum_{i=1}^{\beta}\|\beta_i\|/[q-1-\Phi(q)]$中的分母为零,表达式无意义。实际上,$q$不可能整除$xe$,这是因为$q$是比$x$和$e$都大的大素数。

由上述分析可知,文献[12]对该攻击成功率的概率分析是错误的。

结束语 本文分析了最近两个文献对Schnorr签名方案的攻击方法,指出这些攻击方法都是平凡的穷搜索攻击。在给定的系统安全参数下,这些攻击成功的概率是可以忽略不计的。同时,还指出了这些攻击分析中的一些错误。正如文献[11]所证明的那样,Schnorr签名方案在计算离散对数困难的假设下,在随机预言模型中的存在性不可伪造。就我们所知,目前还没有证明这个签名方案在标准模型中的存在性不

可伪造。因此，在标准模型中证明 Schnorr 签名方案是一个公开问题。

参 考 文 献

[1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[2] Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126

[3] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen message attacks[J]. SIAM Journal on Computing, 1988, 17(2): 281-308

[4] Bellare B, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[A]// 1st ACM Conference on Computer and Communications Security[C]. ACM Press, 1993: 62-73

[5] Bellare B, Rogaway P. The exact security of digital signatures: How to sign with RSA and Rabin [A]// Advances in Cryptology-EUROCRYPT'96[C]. LNCS 1070. Berlin: Springer-Verlag, 1996: 399-416

[6] Zhu H. New digital signature scheme attaining immunity against adaptive chosen message attack[J]. Chinese Journal of Electronics, 2001, 10(4): 484-486

[7] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols[A] // Security in Communication Networks (SCN 2002) [C]. LNCS 2676. Berlin: Springer-Verlag, 2002: 268-289

[8] Fischlin M. The Cramer - Shoup strong - RSA signature scheme revisited[A]// Desmedt Y G, ed. Public Key Cryptography-PKC 2003[C]. LNCS2567. Berlin: Springer-Verlag, 2003: 116-129

[9] Schnorr C P. Efficient identification and signatures for smart cards[A]// Advances in Cryptology-CRYPT0 '89[C]. LNCS 435. Berlin: Springer-Verlag, 1990: 239-252

[10] Schnorr C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4: 161-174

[11] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13: 361-396

[12] 刘景美，王新梅. Schnorr 签名方案的一种攻击[J]. 计算机科学，2006，33(7)：141-142

[13] 邓从政. Schnorr 签名方案的两种伪签名算法及其安全性分析[J]. 中原工学院学报，2007，18(5)：45-47

(上接第 88 页)

其中，C_{i+1}是一个流中两个分组 p_i 与 p_{i+1}之间的时间间隔，T_{hl}是节点接收分组负载所用的时间，其它变量如图 3 所示。因此，在交换节点上，为了弥补尽力而为交换方式的不足，该竞争时间的上界应成为交换结构分组交换调度的一个重要决策依据。从式(7)中可以看出，C_i 是由分组流中分组间的时间间隔和交换节点的处理能力决定的，其中交换节点中决定分组竞争时间的有关性能参量值可在交换节点本地获取。因此，我们认为，在具有提供时间敏感类应用的分组交换网络中，时间敏感类应用的分组应携带分组流时间关系的表示信息，即分组时间间隔信息，用作网络节点分组转发的完成时间约束。

通过以上分析，根据时间关系对节点竞争时间和转发带宽的约束，若满足时间关系敏感类应用的要求，分组传输路径上的各节点要有依据分组流时间关系的约束进行调度转发的能力。因此，一体化网络的设计原则需进一步扩充，这个扩充原则这里称为节点按时调度原则。

节点按时调度原则要求：对时间敏感的应用而言，各个交换节点应该尽可能地按分组时间关系的约束进行交换转发，而不只是尽力而为。

结束语 虽然互联网得到了快速的发展和广泛的应用，能够满足多种应用的要求，但是还无法对交互式实时业务提供保证服务质量的支持。通过深入分析发现，现有互联网络在体系结构上存在缺陷，这种体系结构上的不足通过附加新的服务体系是无法弥补的。为构建更为理想的网络，应在体系结构上对互联网络进行完善和必要的扩充，融入新的设计原则。依据新的网络体系结构来进行的网络实现将具有结构上的一致性。虽然相对于现有互联网络的各种实现会增加一定的复杂性，但这是为满足当前及未来网络个性化、多样化网络应用的需求必须做出的改进。本文从体系结构角度，深入分析了做出这种改进的必要性，并提出了扩展体系结构的具体网络设计原则。

作为理论探索，一体化网络研究应充分总结现有互联网络的缺陷，从网络体系结构这一根本上来探讨互联网无法保证交互式实时应用服务质量的原因，构建更为理想化的网络体系结构。根据本文的论证，一体化网络应在互联网体系结构的基础上融入分组同步同路和分组限时调度两个新的设计原则，以便能在体系结构上继续保持互联网的现有各种优点，同时能根据应用的需要对建立分组传递路径和限定分组节点转发时延提供结构性支撑。据此，依据一体化网络体系结构设计实现的分组网络将能在满足现有网络应用的同时，还能从根本上解决交互式实时应用的服务质量保证问题。

参 考 文 献

[1] Braden R, Clark D, Shenker S. Integrated Services in the Internet Architecture: an Overview[OL]. http://www.ietf.org/rfc/rfc1633.txt, June 1994

[2] NICT. New Generation Network Architecture[OL]. http://akari-project.nict.go.jp/eng/, October 2007

[3] 张宏科，苏伟. 新网络体系基础研究——一体化网络与普适服务[J]. 电子学报，2007，35(4)：593-598

[4] 杨冬，周华春，张宏科. 基于一体化网络的普适服务研究[J]. 电子学报，2007，35(4)：599-606

[5] Clark D. The design philosophy of the DARPA Internet protocols[J]. Computer Communication Review, 1988, 18(4): 106-114

[6] Clark D, et al. NewArch Project: Future-Generation Internet Architecture[OL]. http://www.isi.edu/newarch/, December 2003

[7] Blake S, Black D, et al. An Architecture for Differentiated Services[OL]. http://www.ietf.org/rfc/rfc2475.txt, December 1998

[8] Firoiu V, Le Boudec J Y, Towsley D, et al. Theories and Models for Internet Quality of Service[J]. Proceedings of the IEEE, 2002, 90(9): 1565-1591

[9] Joung Jinoo, Song Jongtae, Lee Soonseok. Flow-based QoS Management Architectures for the Next Generation Network[J]. ETRI Journal, 2008, 30(2): 238-248