计算机科学2004Vol. 31№. 6

复合离散对数与安全认证研究*)

李 波 邱小平
(重庆工学院计算机学院 重庆400050)

摘 要 本文首先回顾了Girault的认证算法以及Poupard和Stern对这个算法安全性所作的分析,在此基础上研究了基于证据不可分辨性的Girault算法只进行一次迭代也能达到抵抗主动攻击的安全性要求。最后给出了一种盲签名算法,算法以安全的因式分解问题为基础。这个新算法的最大特点就是高效。

关键词 复合离散对数,零知识,盲签名

The Composite Discrete Logarithm and Secure Authentication

LI Bo QIU Xiao-Ping
(Department of Computer Science and Engineering, ChongQing Institute of Technology, Chongqing 400050)

Abstract In this paper, we review Girault's Authentication algorithm and Poupard's Secure analysis for the algorithm. Security condition that can resist initiative attack is given based on undistinguished evidence Girault's algorithm even if processing one overlap. Finally an new Blind Signature scheme is put forward which is based on security decompose factor. High efficiency is the most peculiarity of the blind signature algorithm.

Keywords Composite discrete logarithm, Zero knowledge, Blind signature

1 引言

很显然,安全已经成为研究密码学的重要目标。然而效率很少作为一个相关的重要属性被人们考虑,即使是在鉴定技术得到广泛应用的今天,也很少有算法能兼顾安全与效率,其主要原因就是零知识协议的大量应用。论文首先回顾了Girault的认证算法以及Poupard和Stern对这个算法安全性所作的结论。给出了基于证据不可分辨性的Girault算法即使只进行一次迭代也能达到抵抗主动攻击的安全性要求。给出了一种盲签名算法,算法以安全的因式分解问题为基础。这个新算法的最大特点就是高效。

Schnorr[1]认证算法作为一个非常有名的零知识算法,其使用的挑战是固定在一个有限的区域内的,并且需要进行相当数量的迭代操作。然而,许多应用把这种协议,包括基本的三次传递(three-pass)协议的安全性归结到大量挑战的使用。这种安全性理解基于一个尚未被证明的假设,那就是:这个算法是证据隐藏的。Brickell和McCurley[2]提出了一种达到证据隐藏的身份认证算法,它是一个Schnorr认证算法的改进算法。随后,Okamoto提出了一种效率很高的三次传递身份认证算法,因为这个算法是证据不可分辨的,因此即使是在抵抗主动攻击上也可证明是安全的。其中一个算法用到了"代表系问题(representation problem)",也就是基于作用域为质数阶子群的离散对数问题。第二个用到了RSA算法理论。然而,以上所提到的算法在效率上都比Schnorr算法要低。

Girault[3]用复合模数代替质数对Schnorr身份认证算法作了改进。从证明者的角度看它同样使效率得到了提高。Poupard[4]为这个算法的统计零知识属性给出了证明,并证明这个改进算法基于复合离散对数问题的安全性。然而,这个证明显示,基于零知识属性的认证算法同样需要大量的迭代以实现高安全性,更不幸的是算法用到了只适用于使用大参数的大量归并,而这是缺乏实用性的。最近,他们改进了归并算法,使得安全性只是同因式分解相联系,更进一步地解决了高效率实现签名的问题。

然而,这些算法都存在一个主要的弊端,那就是计算代价太大,即使是那些与标准模型中安全的算法相比较更可行的算法也是如此。直到现在,找到一种可证明安全的高效算法对盲签名来说依然是一个重要的挑战,尤其是从签名者的角度来看,因为它们往往在同一时间要进行上千个签名。

2 离散对数问题

正如Feige[5]所指出的那样,一个算法具有证据不可分辨性(也包括证据隐藏性)便足以达到抵抗主动攻击的安全性要求。Pointcheval[6]更进一步地证明这个属性使得盲签名算法足以抵抗并行攻击者进行一次以上的伪造。离散对数问题提供了一个协议,协议基于这样一个函数:$f_{N,g}(x)$,对于适当选取的N和g,$f_{N,g}(x)=g^x \bmod N$。

定义1(α-强素数) 一个整素数P,如果$P=2r+1$,并且r是一个大整数,它的每一个素因子都比α要大,我们就说P是一个α-强素数。

定义2(α-强RSA模数) 如果整数$N=pq$,并且p和q都是α-强素数,我们就称整数N为一个α-强RSA模数。

定义3(不对称基) 设$N=pq$是一个RSA模数,g是Z_N^*的一个基,如果g在Z_p^*和Z_q^*中的秩$Ord(g)$不相等,我们就称g是不对称的。

换一种说法,一个不对称基就是一个二次剩余,它要么是Z_p^*的二次剩余,要么是Z_q^*的二次剩余,但不同时为Z_p^*和Z_q^*的二次剩余。

定理1 假设$N=pq$是一个α-强RSA模数($\alpha>2$),g是Z_N^*中的一个秩大于α的不对称基,那么函数$f_{N,g}(x)=g^x \bmod N$的一个冲突对应于N的一个因式分解。

*)基金项目:教育部科技重点项目(03115),重庆市科委项目(2002C013)。李 波 博士,研究方向:计算机网络,信息安全技术。邱小平 助教,研究方向:信息安全技术,数据库技术。

证明：假定 g 在 Z_N^* 中的秩为$2m$(因为 g 在 Z_p^* 和 Z_q^* 中的秩至少其中之一是偶数，所以 g 在 Z_N^* 中的秩一定是偶数)，并且 m 是一个大于 a 的奇数(理由是：首先 $m>a/2>1$，而且$(p-1)/2$和$(q-1)/2$的素因子都是大于 a 的质数)。因此有：

$g^{2m}=1 \bmod p, g^{2m}=1 \bmod$ 并且 $g^m=-1 \bmod p, g^m=1 \bmod q$

假设存在冲突 $x<y$，使得 $f_{N,g}(x)=f_{N,g}(y)$，令 $L=y-x$，则$2m|L$，将 L 的表达式写作 $L=2^a b$，其中 b 为奇数，则 b 是 m 的倍数，于是有：

$g^{2b}=1 \bmod p, g^{2b}=1 \bmod$ 并且 $g^b=-1 \bmod p, g^b=1 \bmod q$

因此 g^b 是1在 Z_N^* 中的一个非平凡二次方根，于是有 $\gcd(g^b-1, n)\in\{p,q\}$

这样，就存在一个可用两种完全不同的方法对模数 N 因式分解的难题。

3 在密码协议中的应用

我们把离散对数问题应用到密码协议中，取得了比较好的效果。现在介绍一下 Girault[3]认证算法及对该算法的分析，以及由此衍变出的签名算法。然后，我们重点研究一种新的盲签名算法。

3.1 认证

3.1.1 表示 首先介绍一下 Girault[3]认证算法(图1)：

·两个安全参数 k 和 k'，其中 k 代表挑战的大小，k' 与消息泄露有关，S 代表秘钥的边界。然后，我们定义 $R=2^{k+k'}S$。我们使用一个 RSA 模 $N=pq$ 和一个高秩元素 $g\in Z_N^*$。证明者选择一个随机秘钥 $s\in\{0,\cdots,S-1\}$并且公布 $v=g^{-s} \bmod N$；

·证明者随机选择一个 $r\in\{0,\cdots,R-1\}$，并且发送"承诺"$x=g^r \bmod N$；验证者随机地选择一个"挑战"$e\in\{0,\cdots,2^k-1\}$，并把它发送给证明者；最后，证明者计算并发送 $y=r+es$；

·验证者检查 $x=g^y v^e \bmod N$ 成立与否。

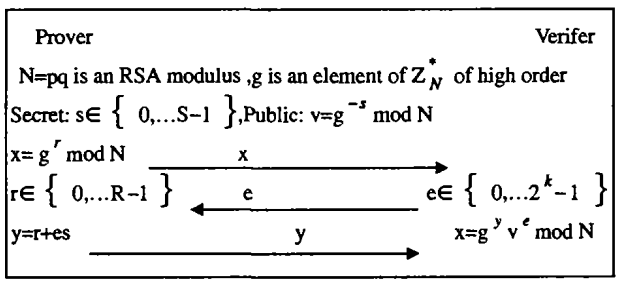

图1 Girault 认证算法

定理2 设 N 是一个2^k-强的 RSA 模，假如存在一个攻击者 A，它可以在时间 T 内，以概率为 ε 的可能性被接受，$\varepsilon>2\cdot 2^{-k}$，则基为 g，模数为 N 的离散对数问题可以在$4T/\varepsilon\times S/Ord(g)$的时间内被计算出。

定理3 这个协议是统计零知识的。

定理4 这个协议是统计证据不可分辨的。

定理5 设 N 是一个2^k-强的 RSA 模，g 是一个属于 Z_N^* 的秩数较高的基。假如，$S\geqslant 2\cdot Ord(g)$则这个协议的安全性可以抵抗对 N 进行因子分解的主动攻击。

3.1.2 计算负载 使用 Girault[7]的证明对原来的算法可以进行优化，从而产生一个非常有效且低代价的算法，如图2所示。

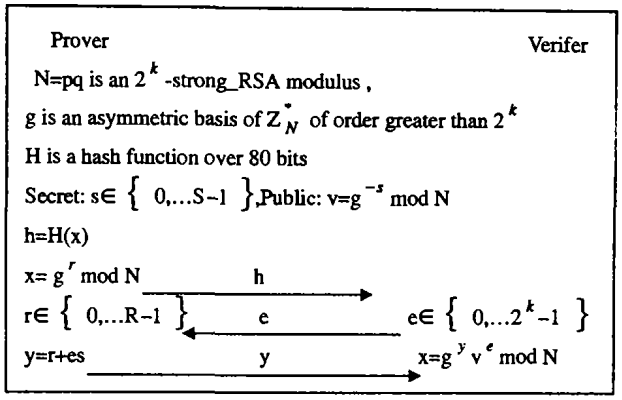

图2 优化后的 Girault 认证算法

3.2 签名

由上面讨论的认证的算法我们可以很容易得到一个签名算法，如图3所示。其中，我们使用一个哈希函数产生一个随机的挑战。

Initialisation
N = pq is a 2^k-strong-RSA modulus g is an asymmetric basis of Z_N^* of order greater than 2^k
Key Generation
Secret: $s\in\{0,...,S-1\}$; Public: $v=g^{-s} \bmod N$
Signature of m
choose $r\in\{0,...,R-1\}$ and compute $x=g^r \bmod N$ get e = H(m.x) and compute y = r+es $\sum(m)=(e,y)$
Verification of (m,e,y)
$e\overset{?}{=}H(m, g^y v^e \bmod N)$

图3 签名算法

定理6 当 $S\geqslant 2\cdot Ord(g)$时，在对这个协议的适应性消息选择攻击下，一个存在的伪装要比因子分解困难。

3.3 一种新的盲签名算法

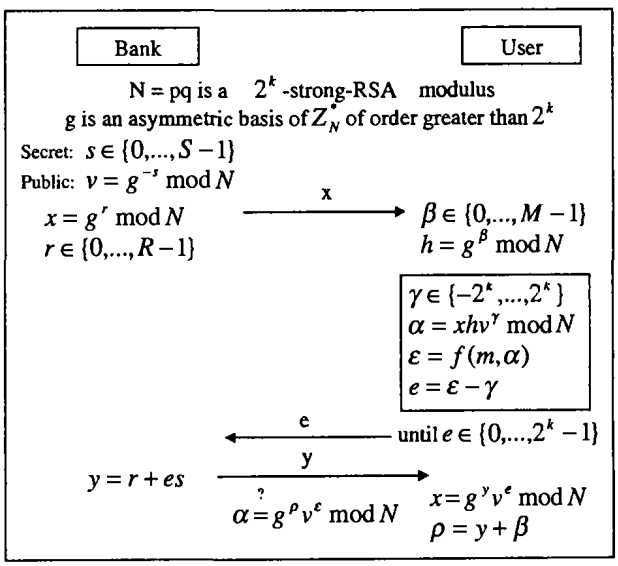

图4 盲签名算法

现在，我们看一个基于前面讨论的问题的签名算法。盲签

名的构造不是很简捷，因为协议的初始化要求仔细地选择安全参数。下面我们先介绍一下这个算法(图4)。其中，k 是安全参数，k' 是消息泄漏参数。我们定义 $R=2^{k+k'}S$ 和 $M=2^{k+2k'}S$，其中 $S\geqslant 2\cdot Ord(g)$ 用来限定秘钥的范围。

定理7 这个协议是统计盲签名协议。

定理8 在随机 oracle 模型中，对这个盲签名协议采用平行攻击时，构造一个一次以上的伪造(one-more forgery)比对 N 进行因子分解要困难。

4 安全和效率

从使用的角度来看，选择一个1024位长的模 N 和一个160位长的非对称基 g 是合适的。消息泄漏参数可以固定为64位，安全参数则根据情况从24位变化到128位。所以，它的安全性依赖于1024位模的因子分解。从证明者的观点来看，这些协议非常有效。确实，我们只需要做少量必要的实时计算，包括一次乘法和一次加法，而且所使用的数字都非常小。

由于一些数据可以预先计算，因此证明者在执行证明的过程中只要进行一次乘法和一次加法。对于盲签名，银行只要用一个168位的数去乘一个128位的数，并把结果加到一个360位的数上。这样，银行可以以很小的存储代价每秒盲签成百万条的消息。

下面，我们对算法的效率能进行一个直观分析(表1)。

结论 我们列出了许多基于复合离散对数问题的算法。从认证算法到盲签名算法，我们已经证明了有效的算法安全性至少和因子分解问题一样。而且，我们提出了一种新的盲签名算法，其计算负载非常小，所以该算法非常适合成千上万个用户的大范围应用。

表1 算法的效率分析

算法	认证	签名	盲签名
模	|N|=1024位；|p|=|q|=512位		
Ord(g)	160位		
安全参数	k=24	K=128	
消息泄漏参数	K'=64		
|S|(>|Ord(g)|)	168位		
|R|(=|S|+k+k')	256位	360位	
|M| (=|S|+k+2k')			424位
在线代价(证明者)	Mult(24,168) +Add(256,192)	Mult(128,168) +Add(360,296)	
通信	360位(45字节)		
签名大小		488位(61字节)	552位(69字节)

参考文献

1 Schnorr, Guillou. Quistquater Composite discrete logarithm and secure authentication. In: Third Intl. Workshop on Practice and Theory in Public Key Cryptosystems, PKC, 2000

2 Brickell E F, McCurley K S. An interactive identification scheme based on discrete logarithm and factoring …, Advances in Cryptology-Eurocrypt'90, LNCS 473, Springer-Verlag, pp. 481～486

3 Girault M. An identity-based identification scheme based on discrete logarithms modulo. a composite number Advances in Cryptology-Eurocrypt'90, LNCS 473, Springer-Verlag, pp. 581～586

4 Poupard. Practical multi-candidate election system. PODC, 2001. 274～283

5 Feige U, Shamir A. Zero knowledge proofs of identity. In: Proc. the Nineteenth Annual ACM Symposium on Theory of Computing, New York City, 1987. 210～217

6 Pointcheval. Provably Secure Blind Signature Schemes (1996) David. ASIACRYPT: Advances in Cryptology--International Conference on the Theory and Application of Cryptology

7 Girault M, Stern J. On the Length of Cryptographic Hash-Values used in Identification Schemes. Identification schemes. In: Proc. of Crypto 94, Lecture Notes in Computer Science 839, 202～215

(上接第145页)

3 梁锦华，蒋建春，戴飞雁，卿斯汉. 计算机取证技术研究. 计算机工程，2002，8：12～14

4 钱桂琼，杨泽明，许榕生. 计算机取证的研究与设计. 计算机工程，2002，6：56

5 David WJ, Stringer-Calvert. Digital evidence. Communications of the ACM, 2002, 45(4): 128

6 Carrier B. Open Source Digital Forensics Tools: The Legal Argument: [Research report]. http://www.atstake.com/.

7 Garber L. Computer forensics: high-tech law enforcement. IEEE Computer, 2001, 34(1): 22～27

8 Judd R. An Explanation of Computer Forensics. http://www.computerforensics.net/forensics.htm

9 MacCrimmon M T. Expert Systems in Case-Based Law: The Hearsay Rule Advisor. In: Proc. of the second intl. on conf. on Artificial intelligence and law. Vancouver, British Columbia, Canada, 1989. 68～73

10 King R, Stanley C. Ensuring court admissibility of computer-generated records. ACM Transactions on Information Systems (TOIS), 1985, 3(4): 398～412

11 Farmer D, Venema W. Forensic Discovery. FIRST. 2002 Hawaii, USA, 2002

12 Schaffer G P. The Role of Computer Forensics in the Investigation of Network Intrusion Activity. FIRST. 2002 Hawaii, USA, Jun 2002

13 Lunn D A. Computer Forensics: An Overview. http://www.sans.org/rr/incident/forensics.php.

14 Carrier B. Defining digital forensic examination and analysis tools Using Abstraction Layers. International Journal of Digital Evidence. 2003, Volume 1, Issue 4, http://www.ijde.org/.

15 Schneier B, Kelsey J. Secure audit logs to support computer forensics. ACM Transactions on Information and System Security (TISSEC), 1999, 2(2): 159～176

16 http://www.guidancesoftware.com/encase/frame_encase.html

17 http://www.forensics-intl.com/safeback.html

18 http://fish.com/tct/

19 蒋晓宁，叶澄清. 一种新的公平反拒认协议. 计算机工程与应用，2000，5：40～42

20 蒋晓宁，叶澄清. 电子证据与反拒认协议. 通信学报，2000，7：76～81

21 Giordano J, Maciag C. Cyber Forensics: A Military Operations Perspective. International Journal of Digital Evidence. 2002, Volume 1, Issue 2. http://www.ijde.org/.

22 Mukkamala S, Sung A H. Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques. International Journal of Digital Evidence. 2003, Volume 1, Issue 4. http://www.ijde.org/