第 20 卷 第 1 期 徐州师范大学学报(自然科学版) Vol. 20, No. 1
2002 年 3 月 J. of Xuzhou Normal Uni. (Natural Sciences) Mar., 2002

一个基于交互式零知识证明的身份鉴别协议

徐 明[1], 韩 维[2]

(1. 徐州师范大学 计算机科学系, 江苏 徐州 221009; 2. 徐州师范大学 数学系, 江苏 徐州 221116)

摘要: 提出了一个基于零知识证明的身份鉴别协议. 该协议的安全性依赖于大数的因子分解和离散对数两个 NP 完全问题. 该协议可以被方便地应用到智能卡系统中去. 协议中证明者(Prover)和验证者(Verifier)具有同样的计算能力, 而且该协议要求最小限度的计算量和通信流量.

关键词: 零知识证明; 身份鉴别

中图分类号: TP309; TN918 文献标识码: A 文章编号: 1007-6573(2002)01-0037-02

在 Internet 时代, 网络通讯中的实体迫切需要用一种可靠的身份鉴别方法来向对方证明自己的身份. 作为网络上最基本最必须的功能, 身份鉴别问题得到广泛和深入的研究, 特别是出现了许多基于零知识证明的方案. Feige-Fiat-Shamir 算法是第一个基于零知识证明的算法[1,2], 但由于与外部信息交换很耗时, 对于诸如智能卡的应用, 该算法不甚理想. 此后 Louis Guillouh 和 Jean-Jacques Quisqure 研究出的零知识证明身份鉴别的算法更适合于这些应用[3]. 后来 Claus Schnorr 提出了一个安全性基于离散对数的零知识证明身份鉴别方案[4,5]. 最近, DaeHun Nyang 和 JooSeok Song 提出了一个基于零知识证明身份鉴别方案[6], 该方案需要较小的的通讯量和计算量, 可以应用于智能卡系统.

在本文中, 我们给出一个新的交互式的基于零知识证明的身份鉴别和数字签名方案, 其安全性是基于对大数的因子分解的难题和对 RSA 破解的难题. 此方案对智能卡应用与 Nyang-Song 方案一样只需较少的通讯量和计算量, 至多只需要 K 轮就可达到零知识证明, 所需要的轮数 K 比 Nyang-Song 方案要少, 而且, 在轮数相同的情况下方案可提供比 Nyang-Song 方案更高的安全性能.

1 背景

交互式知识证明协议可定义为证明者(Prover, 简称 P)和验证者 (Verifier, 简称 V) 两个图灵机交互作用的过程. 两个图灵机有一些用于进行操作运算和相互通讯的纸带. L 是一正则语言, 对于相同的输入 x, P 欲使 V 确信其明确掌握的断言 $x\in L$. 为此, P 和 V 进行一系列的通讯过程(一般一个通讯过程是 commitment-challenge-response 的形式). 在完成交互作用过程后, 如果 $x\in L$, 那么 V 在高概率条件下相信这是事实, 这一条称为完备性(completeness). 但如果 $x\notin L$, 那么在高概率条件下 P 不可能欺骗 V (相信), 这一条称为公正性(soundness).

非正式地, 所谓的交互式零知识证明协议是指交互式证明协议结束后, P 只告诉 V 关于 $x\in L$ 断言成立的信息, 而 V 不能从交互式证明协议中获得其他任何信息. 即使在协议中使用诡计欺骗手段, V 也不可能揭露其他更多的信息. 我们的交互式协议是企图证明关于一个大数的因子分解的知识.

2 身份鉴别方案

我们的协议分成预处理和交互证明两个阶段. 第一阶段是由一个信任中心来完成预处理, 而第二阶段完成交互证明.

2.1 信任中心的预处理阶段

1) 信任中心为用户生成一个身份字符串 I.

收稿日期: 2001-12-21

作者简介: 徐明(1970—), 男, 江苏吴江人, 讲师, 浙江大学博士生, 主要从事网络安全和数据加密的研究.

万方数据

2) 随机选择两个大素数 p 和 q 并保持秘密. 假设 $n=pq$ 是一个 768 位或 1 024 位的公开数,要求 n 不易被分解. $\varphi(n)=(p-1)(q-1)$,随机选择素数 e 使 $(e,\varphi(n))=1$ 并求出 $d=e^{-1} \bmod \varphi(n)$(这里也要求 $(d,n)=1$). e 和 n 作为公开密钥,d 是私人密钥. 两素数 p 和 q 不再需要,销毁,但绝不可泄露.

3) 信任中心生成数字签名 $S=\text{signature}(I,e,n)$ 和公钥证书 $C(\text{user})=(I,e,n,S)$.

2.2 交互证明阶段

假定 P 和 V 进行交互证明.

1) P 将公钥证书 $C(\text{P})$ 发送给 V.

2) V 检查 P 的公钥证书 $C(\text{P})=(I,e,n,S)$.

3) P 选择一随机数 $r\in\{2,\cdots,n-1\}$,并将 $x=r^e \bmod n$ 作为 Commitment 发送给 V.

4) V 发送一随机数 $p\in\{1,\cdots,2^t\}$ 给 P 作为一个 Challenge.

5) P 将 $y=rp^d \bmod n$ 作为 Response 发送给 V.

6) V 检查 $x=y^e p^{-1} \bmod n$ 是否成立. 若等式成立,则 V 将接受这次有效证明. 否则将拒绝接受.

上面的交互证明能够提供 2^{-t} 的安全程度. 若要减少通讯量,P 可以在第 3 步中用一哈希函数将 $h(x)$ 的前 t 位发送给 V;而 V 在第 6 步中将 y 与 $h(x)$ 的前 t 位比较就可以. 协议中要求计算 $x=r^e \bmod n$ 和 $p^{-1} \bmod n$ 都可以在脱机时计算处理.

3 完备性和公正性

下面证明上面的交互式证明协议满足完备性和公正性,以确保协议的有效性和安全性.

定理 1(完备性) 如果 P 和 V 按协议完成了全部步骤,那么 V 总是能接受 P 的身份证明.

证 由定义知

$$y^e p^{-1}=(rp^d)^e p^{-1} \bmod n=r^e(p^{de})p^{-1} \bmod n=r^e(pp^{-1}) \bmod n=r^e \bmod n=x.$$

定理 2(公正性) 假设 P 不知道 d,并不能在多项式时间内解决 RSA 加密系统的破解问题和有效地通过 e 和 n 来计算得到 d,那么当 P 和 V 按协议完成了全部步骤,V 接受 P 的证明的概率是 2^{-t}.

证 假设 P 能在较高概率情况下欺骗 V. 由于 P 不知道 d,且不能在多项式时间内有效地通过 e 和 n 来计算得到 d,所以他无法在第 5 步中利用 d 来计算出 y. 为了能欺骗成功,对一个 r_2,他必须从方程 $y^e=xr_2 \bmod n$ 中解出 y 来(若能解出此方程,则 $y^e r_2^{-1} \bmod n=xr_2r_2^{-1} \bmod n=x$). 我们可以把这个问题看成 RSA 的破解问题,即将 $xr_2 \bmod n$ 看成用公钥 (n,e) 对 y 进行 RSA 加密后得到的密文,问题变成在不知道秘钥 d 的情况下,由已知密文求 RSA 加密系统对应的明文(与假设矛盾).

若 P 对询问 r_2 可预测,则他可以通过先任选择一数 y,并将 $x=y^e r_2^{-1} \bmod n$ 作为 commitment 发送给 V,则 V 将接受 P 的证明,但预测 r_2 的概率为 2^{-t}.

参数 t 的大小影响协议的速度和安全两个方面. 当 t 足够大时,安全性提高了但速度会降低;反之当 t 变小时,安全性会降低但速度会提高. 故在实际的系统中 t 的选择应该在安全和速度之间权衡.

协议中 $y=rp^d \bmod n$,故 V 在证明中不能揭示 P 的密钥 d 的任何信息. 然而与 Nyang-Song 协议[6] 一样,在一轮循环的证明情况下,该协议不是零知识证明的,但只要将协议循环 $k\left(k=\left[\frac{1}{t}\log_2 n\right]\right)$ 次就可以达到零知识证明,因为此时有 $2^{-kt}<\frac{1}{n}$. 在实际的应用中要选择合适的参数 t 和 k 以确保安全性和效率,而不一定要达到理论上的零知识证明.

本文中我们提出了一个新的高效安全的基于交互式零知识证明的身份鉴别协议. 方案中证明方和验证方的计算量是均衡而有效的,还可以通过预计算来进一步提高效率. 此身份鉴别方案也适合于智能卡的应用,且只要求最少的计算量和通信量.

参考文献:

[1] Feige U, Fiat A, Shamir A. Zero-knowledge proofs of identity[A]. Proceedings of the 19th Annual ACM Symposium on the Theory of Computing[C]. IEEE, 1987. 210－217.

万方数据

(下转第 64 页)

A Study on Static Adsorption Behaviors and Thermodynamic Properties of Adsorption Resins to 4-Methylaniline

SHI Wei-zhong, *FEI Zheng-hao*
(Department of Chemistry, Yancheng Teachers College, Yancheng 224002, China)

Abstract: A comparison study is made between Amberlite XAD-4 and the new type adsorption resins NK and new H on the static adsorption behaviors, including the static equilibrium adsorption isotherms and the adsorption thermodynamic properties. The adsorption capacities of new H and NK to 4-methylaniline are obviously much higher than that of Amberlite XAD-4, which is attributed to micropore mechanism and partial polarity. The negative values of the adsorption enthalpy ΔH are indicative of an exothermic process, thus lower temperature is better for adsorption. The studies both on the enthalpy and on the free energy of adsorption manifest a physisorption process. The negative values of the adsorption entropy ΔS indicate that the adsorption is well consistent with the restricted mobilities and the configurations of the adsorbed 4-methylaniline molecules on the surface of adsorption resins and with the superficial heterogeneity of the adsorption resins.

Key words: adsorption resin; 4-methylaniline; static adsorption behavior; thermodynamic parameter; adsorption enthalpy; adsorption entropy; adsorption free energy

---

(**上接第 38 页**)

[2] Feige U, Fiat A, Shamir A. Zero-knowledge proofs of identity[J]. Journal of Cryptology, 1988, 1(2): 77.
[3] Guillou L C, Quisquater J-j. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory[A]. Advance in Cryptology-EUROCRYPT'88 Proceedings[C]. Springer-Verlag, 1988. 123－128.
[4] Schnorr C P. Efficient signature generation for smart card[A]. Advances Cryptology-CRYPTO'89 Proceedings[C]. Springer-Verlag, 1990. 239－252.
[5] Schnorr C P. Efficient signature generation for smart card[J]. Journal of Cryptology, 1991, 4(3): 161.
[6] Nyang D, Song J. Knowledge-proof based versatile smart card verification protocol[J]. Computer Communication Review, 2000, 30(3): 39.

An Interactive Proof Protocol of Identity Based on Zero-knowledge

XU Ming[1], *HAN Wei*[2]
(1. Department of Computer Science, Xuzhou Normal University, Xuzhou 221009, China;
2. Department of Mathematics, Xuzhou Normal University, Xuzhou 221116, China)

Abstract: We propose an interactive proof protocol of identity based on zero-knowledge. The security of protocol is based on factorization of large number and RSA problems. This protocol can be applied to smart cards. Our scheme has symmetricity in the sense that the same computational complexity and the same hardware for both Prover and Verfier are required. Also, it requires minimal amount of computation and communications for secret information.

Key words: zero-knowledge proof; identification

万方数据