一个安全电子商务身份验证协议*

张龙军, 黄继武
(中山大学信息科学与技术学院, 广东 广州 510275)

摘 要: 针对电子商务活动中存在的冒名欺诈问题, 设计了一个安全的电子商务身份验证协议。协议的安全性是建立在目前尚未存在有效攻击方法的有限域上非超奇异椭圆曲线的椭圆曲线离散对数问题之上的。从理论上分析, 该协议是安全的并具有一定的实用价值。为了提高协议在实际应用当中的运算速度, 设计了实现该协议的椭圆曲线密码体制基本算法。这些算法具有形式简单、运行速度快的特点, 完全可以满足实际应用的需要。

关键词: 电子商务; 身份验证; 安全协议
中图分类号: TP309 文献标识码: A 文章编号: 0529-6579 (2003) 01-0020-03

随着 Internet 的发展, 电子商务已经逐渐成为人们进行商务活动的新模式。信息安全是电子商务发展的一个核心问题[1], 完整的电子商务系统应当满足以下安全性要求: ①信息的保密性; ②信息的完整性; ③身份的确定性; ④不可否认性。现代电子商务以 Internet 为基础, 它利用世界范围连通的、无中心管理机构的、交互式的、低成本的 Internet 发展业务。Internet 在建立之初, 主要是考虑到便于应用, 其 TCP/IP 协议及原代码的设计要求开放与共享。在这样的环境下进行安全要求很高的电子商务活动必然存在着很大的安全隐患。认证技术是信息安全理论与技术的一个重要方面, 在计算机网络中用于鉴别用户身份合法性的身份验证技术又是认证技术的重要组成部分。在计算机网络安全的许多重要问题中, 身份验证是关键问题之一。在电子商务活动中, 身份验证是进入系统的第一道程序。出于对执行速度的考虑, 现有的身份验证协议大都是基于私钥密码体制的[2-7], 也有基于 RSA 公钥密码体制的[8,9]。RSA 公钥密码体制是目前通用的加密体制, 基于 RSA 公钥密码体制的身份验证协议虽然可以克服基于私钥密码体制的身份验证协议存在的密钥管理困难的问题, 但是由于目前 RSA 公钥密码体制的安全受到了严重的威胁, 其安全性已经不能够得到足够保证。

为了解决 RSA 公钥密码体制所面临的安全问题, 本文设计了一种基于椭圆曲线公钥密码体制的身份验证协议及其实现算法。椭圆曲线密码体制是一种公开钥密码体制, 具有公开钥密码体制的所有优点。它的安全性高, 不易攻破, 已经被许多应用协议推选为下一代公钥密码算法, 其应用有着广阔的前景。

1 验证协议设计与分析

在 Internet 系统中, 非法攻击者常采用的攻击手段有: 非法窃取合法用户的口令, 进而非法访问未获授权的系统资源; 对合法通信者的通信信息进行窃取分析并进行破译; 截获合法用户信息, 然后再重传给接收者; 阻止系统资源的合法管理和使用。因此, 系统应当能提供如下防止非法攻击的相应认证功能: 能够确信信息来源于合法用户, 即信息的接收者能够确认所获得的信息不是来源于非法用户; 信息在传输过程中能够保证其完整性, 接收者能够确认所获得的信息在传输过程中没有被篡改; 信息发送方对其已经发出的信息不能抵赖, 同时信息接收方也不能对已经收到的信息进行否认; 非法用户不能访问系统资源, 合法用户也只能访问系统授权及指定的资源[10]。

1.1 协议描述

1.1.1 初始化

(1) 构造椭圆曲线 $E: y^2 2 = x^3 + ax + b$ ($a, b \in F_q$, q 是一个素数), 该曲线是非超奇异的;

(2) 选择一个公开的基点 $P \in E(F_q)$, 其阶为 $l = \mathrm{ord}(P)$;

(3) 用户 U 随机选取一个整数 d_U 作为秘密钥,

* 收稿日期: 2002-06-15
基金项目: 国家自然科学基金重点资助项目 (60133020); 国家自然科学基金资助项目 (60172067); 国家“863”计划资助项目 (2002AA144060); 广东省自然科学基金重点资助项目 (013164)
作者简介: 张龙军 (1964 年生), 男, 博士, 副教授; E-mail: zhangwithyan@bta.net.cn

计算 $e_U = d_U P$，将 e_U 作为其公开钥。用户 U 同时拥有椭圆曲线签名方法 S_U；

(4) 系统认证中心 AC 随机选择一个整数 $d_A \in \{0, 1\}$ 作为其秘密钥，计算 $e_A = d_A P$，将 e_A 作为其公开钥。同时 AC 也拥有椭圆曲线数字签名方法 S_A。

1.1.2　身份验证

(1) U 生成自己的标识符 V，并选择一个随机整数 r_1，计算 $C = e_A\ (r_1 V \bmod l)$；

(2) U 向 AC 发出请求准予访问系统信息 R，并用椭圆曲线签名方法进行签名，即计算 $U_R = S_U(R)$，然后将 (U_R, C) 发送给 AC；

(3) AC 用 U 的公开钥验证 U_R 是不是 U 的签名，即计算 $e_U(U_R)$，与 R 相比较，如果相等则说明 U 是合法用户；否则说明 U 是非法用户；

(4) AC 随机选择一个整数 $k \in \{1, \cdots, l-1\}$，计算 $Q = kP$ 并传送给 U；

(5) U 另选一个随机整数 $r_2 \in \{1, \cdots, l-1\}$，计算 $Q' = r_2 Q = (r_x, r_y)$，$r = r_1 r_x \bmod l$。将 r 传送给 AC。

(6) AC 由 C 解密得到 $r_1 V \bmod l$，为 U 生成一个惟一的身份识别符 ID，计算：

$$U_{ID} = S_A(ID)$$

$$y = \frac{r_1 V d_A + r}{l} \bmod l$$

$$A_{ID} = e_U(U_{ID} \| y)$$

AC 将 A_{ID} 传送给 U。

(7) U 得到 A_{ID} 以后，解密得到 U_{ID} 和 y，计算：

$$C' = (r_1^{-1} r_2^{-1} y) = \left(f_1^{-1} \frac{r_1 V d_A + r}{k} \right) \bmod l$$

(8) U 向系统发出访问信息 (V, C')，AC 验证其身份是否合法，即计算 $C'Q = Ve_A + r_x P$ 是否成立，如果正确则准予访问系统，否则回绝。

1.2　验证协议分析

密码学家普遍认为椭圆曲线离散对数问题是一个非常难以求解的问题，而椭圆曲线密码体制就是以椭圆曲线离散对数问题的难解性为其安全性基础的。对于椭圆曲线离散对数问题，如果是超奇异椭圆曲线则可以利用 MOV 归约法将 $E(F_q)$ 上的椭圆曲线离散对数问题归约为 Fq 的一个小的扩展域上的椭圆曲线离散对数问题，然后在上使用指数计算法求解。对于有限域上的非超奇异的椭圆曲线，目前还没有有效的求解其上的椭圆曲线离散对数问题的方法。而 MOV 归约法只是对有限域上的超奇异椭圆曲线才有较高的效率。虽然也可以使用对一般群都有效的 Baby-step Giant-step 算法，但是该方法为完全指数时间，仅当椭圆曲线上的点加群的阶不含大素因子时才是有效的。在当前，相对来说最好的求解椭圆曲线离散对数问题的算法是 Pollard ρ 方法和 Pohling-Hellman 方法，其时间复杂度都是指数级的。但是，当椭圆曲线上的阶含有较大素因子时这两种方法也是无效的[11]。本协议的安全性是以椭圆曲线密码体制的安全性为保证的，而椭圆曲线密码体制的安全性是基于椭圆曲线离散对数问题的难解性之上的。由于目前还没有对椭圆曲线离散对数问题的有效解法[12]，所以本协议是安全的。合法用户采用椭圆曲线加密方法和椭圆曲线数字签名方法处理请求信息和标识符之后，非法用户无法伪造合法用户的请求信息和标识，因为在不知道合法用户秘密钥的情况下是不能对椭圆曲线离散对数问题求解的。从而系统不会接受其访问请求。同样基于椭圆曲线离散对数的难解性，非法用户也不可能得知双方交换信息的内容，因此无法对截获的信息进行流量分析、重传以及修改或伪造。

实际应用时可以采用预处理的方法，给系统的每一个合法用户预先产生好身份标识符，当用户要访问系统时只要进行身份验证即可，这样可以减少计算时间。

2　协议实现算法的分析与设计

椭圆曲线密码体制是建立在有限域 F_q 上的，因而有限域上的大整数运算就构成它的基本算法，主要包括模加、模乘、模逆和模幂运算。为了保证密码体制的安全强度，要求 q 很大，本文工作中，要求 $q > 2^{140}$。如此大的整数运算是很费时的，尤其是模逆和模幂运算。因此，为了得到较快的加、解密速度，必须对这些基本算法进行优化。

2.1　快速取模算法

为了保证有限域 F_q 上运算的封闭性，所有基本运算的结果都要对 q 取模，所以设计高效的取模算法对提高所有基本运算的速度至关重要。快速取模算法的基本思想是采用预计算，将预计算的结果造表待用，以空间换取时间，因而不再需要在调用时临时计算。算法由建表、初步模和同阶模三个步骤完成。

对于 $A * B \equiv C \bmod P$，A 和 B 均为 n 位的二进制数，C 为 $2n$ 位的二进制数，采用本算法求模，只需做 $(2n - n) / 8 = n/8$ 次的二进制加法。相比之下，这种算法的效率是常用的模余数表法的 4 倍。在最坏情况下，模余数表法需要 n 次 n 位的二进制加法，而本文所述的这种快速模运算法只需

要 2（2n－n）/8＝n/4 次 n 位的二进制加法。所以，无论在什么情况下，快速模运算法的速度都是模余数表法的 4 倍。

2.2 模加算法

模加算法很简单。设 $A, B, C \in F_q$, $C = A + B \bmod q$, 则：

当 $A + B \leqslant q$ 时, $C = A + B$;

当 $A + B > q$ 时, $C = A + B - q$。

2.3 模乘算法

大数模乘法是其它各算法的公用支撑子程序，被其它各功能模块频繁调用。有限域上大数模乘法的效率极大地影响着系统的整体效率。模乘可以分为求积和取模两步求解。设 A, B, $C \in Fq$, $C \equiv A * B \pmod q$, 则先求出 A 与 B 的乘积，再利用快速求模算法对乘积取模即可得到模乘的结果。这里只给出大数乘法。

设模数 q 的位长为 n，用 $A * B \pmod q$ 表示模乘，其中 A, $B \in [0, q-1]$, 均为 n 位长的二进制数。首先计算 $A * B$，得到一个 $2n$ 位长的积。若处理器的寄存器字长为 b，则把 A, B 按字长各分为 K 块。

实际处理时，可先计算 A 的有效字块数 KA, B 的有效字块数 KB。则：

$$A = A_0 + A_1 \cdot 2^B + \cdots + A_{K_{A-1}} \cdot 2^{K_{A-1}b} = \sum_{i=0}^{K_{A-1}} A_i \cdot 2^{ib}$$

$$B = B_0 + B_1 \cdot B^B + \cdots + B_{K_{B-1}} \cdot 2^{K_{B-1}b} = \sum_{i=0}^{K_{B-1}} B_i \cdot 2^{ib}$$

$$C = A * B = A * B_0 + A * B_1 + \cdots + A * B_{K_{B-1}} \cdot 2^{K_{B-1}b}$$

在此式中，通过部分积结果移位求和得结果 C，可比一般方法提高速度 2～4 倍。然后再对大数相乘的积使用快速求模算法取模，就可以得到模乘的结果。

2.4 模逆算法

已知 $a \in F_q$, $\gcd(a, q) = 1$, 满足等式 $aX \equiv 1 \bmod q$ 的 $X \in F_q$ 称为有限域 F_q 中 a 的逆，可表示为 $a^{-1} \bmod q$。在椭圆曲线密码体制的实现过程中，模逆算法是必不可少的。求模逆的算法有许多种，其中以 Euclid 算法最为简便快捷，本文采用一种 Euclid 算法的变化形式来求模逆。

2.5 模幂算法

模幂即计算 $y \equiv x^m \bmod q$，算法依据是：

若 $m = m_n 2^n + m_{n-1} 2^{n-1} + \cdots + m_1 2^1 + m_0$, 其中 $m_i \in \{0, 1\}$, $m_n = 1$, 则：

$$x^m = x^{m_n 2^n + m_{n-1} 2^{n-2} + \cdots + m_1 2^1 + m_0} = (x^{m_n 2^{n-1} m_{n-1} 2^{n-2} + \cdots + m_1})^2 \cdot x^{m_0} = ((x^{m_n 2^{n-1} m_{n-1} 2^{n-2} + \cdots + m_1})^2 \cdot x^{m_1})^2 \cdot x^{m_0} = \cdots = ((\cdots((x^{m_n})^2 \cdot c^{m_{n-1}})^2 \cdots x_2^m)^2 \cdot x_1^m)^2 \cdot x_0^m$$

3 椭圆曲线快速点加算法分析与设计

在椭圆曲线密码体制中，椭圆曲线群上点的加法占了整个运算的很大比例，所以加法朱效率关系到整个全制的执行效率。所以还应当对提高点加算法速度的途径进行分析和研究，给出相应的算法，为提高椭圆曲线密码全制的运行速度提供有效的方法。对于形如 $y^2 = x^3 + ax + b$ 的椭圆曲线的一般形式，在仿射坐标和射影坐标下具有不同形式的点加公式。

仿射坐标的点加公式需要 2 次或 3 次模乘，1 次模逆。模逆的计算量比模乘的诸量要大得多，很费时间。而射影坐标的点加公式可以避免模逆，比用仿射坐标点加公式要快得多。为了适应点的数乘算法，应当采用射影坐标点加公式来计算点加，这样可以大提高椭圆曲线密码体制的执行速度。所谓点的数乘即给定整数 k 和椭圆曲线上的点 p 来求 k_p。设 $k = k_0 + k_1 2 + k_2 2^2 + \cdots k_{n-1} 2^{n-1}$，其中 $k_i \in \{0, 1\}$，$i = 0, 1, \cdots, n-1$。求解 k_p 可以分为两步：①利用点加公式迭代出所有的 $2^i p$，$i = 1, 2, \cdots, n-1$；②对于所有的 $k_i \neq 0$，利用点加公式累加对应的 $2^i p$。通过分析可知，kP 的平均计算量为（3/2）n 次点的加法运算。考虑到大部分时候 P 是固定的，为了减少 kP 的计算量，从而提高椭圆曲线密码体制的加、解密速度，可以采用预计算法预先计算出所有的 $2^i p$（$0 \leqslant i \leqslant n-1$ 来减少点加运算的次数。

4 结 语

本文针对电子商务活动中存在的安全问题，将下一代公钥密码体制——椭圆曲线密码体制引入到电子商务安全解决方案之中，提出了一个电子商务身份验证协议并设计了实现该协议的基本算法。本文提出的电子商务安全身份认证协议能够满足对于用户身份合法性检验的一切要求，其安全性是建立在目前尚没有有效解法的椭圆曲线离散对数问题上的，所以其安全性完全能够得到保证。本文针对椭圆曲线密码体制存在的计算复杂、运算速度慢的问题，首先在身份验证协议设计时力求简单，其次研

究设计了影响其运算速度的基本运算的快速算法和在椭圆曲线密码体制中占整个运算很大比例的椭圆曲线群上点的加法的快速算法。这些措施为提高椭圆曲线密码体制的运行速度提供了有效的方法。大大提高了椭圆曲线密码体制实际应用时的运行速度。因此，所提出的协议具有安全性高、密钥较短、计算简单和速度快的优点，完全可以满足电子商务应用中的要求。

参考文献：

[1] KAILAR R. Accountability in electronic commerce protocol [J]. Information and Communications. 1996, 22(5): 313—328.

[2] PARK J S, SANDHU R. RBAC on the Web by smart certificates // Proc of the ACM Workshop on Role-Based Access Control[M]. 1999: 1—9.

[3] YAMAZAKI Y, KOMATSU N. A secure communication system using biometric identify verification[J]. IEICE Trans on Information and Systems, 2001, E84-Dn(7): 879—884.

[4] LIN D T. Computer-access authentication with neural network based keystroke identity verification[J]. Proc of the IEEE Int Conf on Neural Networks, 1997, 1: 174—178.

[5] ROBINSON J A, LIANG V M, CHAMBERS J A M, et al. Computer user verification using login string keystroke dynamics[J]. IEEE Trans on Systems, Man, and Cybernetics, Part A: Systems and Humans, 1998, 28(2): 236—241.

[6] NYANG D, KIM E, SONG J. Interactive identification scheme based on quadratic residue problem[J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 1997, E80-An(7): 1330—1335.

[7] SABOURIN R, GENEST G, PRETEUX F J. Off-line signature verification by local granulometric size distributions[J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 1997, 19(9): 976—988.

[8] ZHANG N, SHI Q, MERABTI M. Anonymous public-key certificates for anonymous and fair document exchange[J]. IEE Proceedings: Communications, 2000, 147(6): 345—350.

[9] MAO W. Blind certification of public keys and off-line electronic cash[C]. HP Laboratories Technical Report, 1996: 1—16.

[10] KENT S. Evaluating certification authority security. Proc of the IEEE Aerospace Applications Conference, 1998, 4: 319—327.

[11] PANDIARAJAN V, MARTIN T L, JOINER L L. Recommendations on a new cellular encryption standard using elliptic curve cryptography //Proc of the IEEE Southeastcon[M]. 2001: 136—142.

[12] ERNST M, KLUPSCH S, HAUCK O, et al. Rapid prototyping for hardware accelerated elliptic curve public-key cryptosystems // Proc of the Int Workshop on Rapid System Prototyping[M]. 2001: 24—29.

An Identity Verification Protocol for E-Commerce

ZHANG Long-jun, *HUANG Ji-wu*

(School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: In allusion to cheat, this paper proposes a secure electronic commerce identity verification protocol. The safety of this protocol is based on the elliptic curve discrete logarithm of non-supersingular elliptic curve over finite field, on which there has been no efficient attack method up to now. The protocol is secure in theory and is suitable for some applications. For improving the speed of this protocol in practical application, this paper designs the base algorithm of elliptic curve cryptosystem. The algorithm is simple, has low computation complexity and can satisfy the practical application require.

Key words: E-commerce; identity verification; security protocol