基于安全电子交易协议(SET)的网上银行身份认证

Certification Authority In Online Banking Based On Secure Electronic Transaction

曹海平 (南通大学 电气工程学院 江苏 南通 226007)

摘要:论文针对电子商务的发展对电子支付环境提出的要求,分别论述了安全电子交易协议、椭圆曲线密码的功能,比较了安全电子交易协议与 SSL 协议之间的差异以及椭圆曲线密码相对于 RSA 的优势,并由此讨论了基于椭圆曲线密码体制实现安全电子交易协议的身份认证。

关键词:网上银行 安全电子交易协议 椭圆曲线密码 认证中心

1 引言

随着网上银行的发展,其核心问题交易的安全性问题也凸现出来,因此如何构筑安全的交易模式也是各方最担心的问题[1]。解决这一问题的关键是使用安全的电子支付模式,安全电子交易协议(SET)是目前最常用的模式之一,已获得 IETF 标准的认可,是未来网上银行的发展方向。

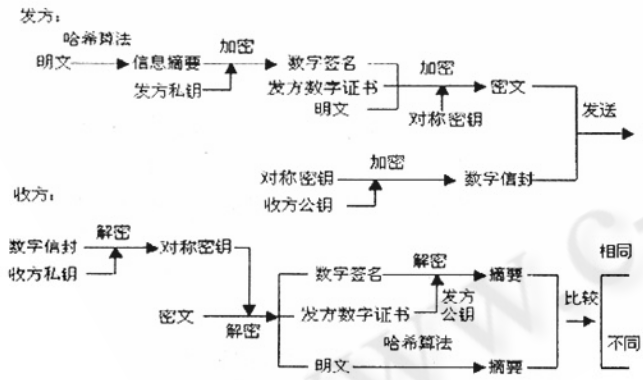

图 1 SET 协议采用的数据加密模型

2 网上银行交易的身份认证

网上银行的建立,CA 的建立是关键,只有建立一个较好的 CA 体系,才能较好地发展网上银行。在用户身份认证方面,SET 引入了证书和证书管理机构机制。证书就是一份文档,它记录了用户的公共密钥和其他身份信息。在 SET 中,最主要的证书是持卡人证书和商家证书,还有支付网关证书、银行证书、发卡机构证书。通过 SET 的认证机制,用户不再需要验证并信任每一个想要交换信息的用户的公共密钥,而只需要验证并信任颁发证书 CA 的公共密钥就可以了。

3 安全电子交易协议概述

安全电子交易协议(SET)[2]使用了公开密钥体系对通信双方进行认证,利用对称加密方法进行信息的加密传输,并利用 Hash 算法鉴别消息的真伪。SET 中的核心技术主要有公开密匙加密、电子数字签名、电子信封、电子安全证书等。交易参与者的身份鉴别采用数字证书的方式来完成;用报文摘要算法来保证数据的完整性;由于非对称加密算法的运算速度慢,所以要和对称加密算法联合使用,用对称加密算法来加密数据,用数字信封来交换对称密钥。

SSL 协议和 SET 协议是目前在电子商务中使用最为广泛的两种安全模式,两相比较 SET 协议具有如下优点:

(1) 认证要求。SSL 不能实现多方认证,而且只有商家服务器的认证是必须的。SET 协议的认证要求较高,所有参与 SET 交易的成员都必须申请数字证书,并且解决了多方认证问题。

(2) 安全性。SET 协议采用了公钥加密、信息摘要

和数字签名可以确保信息的保密性、可鉴别性、完整性和不可否认性，且 SET 协议采用了双重签名来保证各参与方信息的相互隔离。SSL 协议缺乏一套完整的认证体系，不能提供完备的防抵赖功能。

(3) 协议层次和功能。SSL 属于传输层的安全技术规范，不具备电子商务的商务性、协调性和集成性功能。而 SET 协议位于应用层，它不仅规范了整个商务活动的流程，而且制定了严格的加密和认证标准，具备商务性、协调性和集成性功能。

但是 SET 协议有一个致命的问题：非常复杂、庞大，处理速度慢。一个典型的 SET 交易过程需验证电子证书 9 次、验证数字签名 6 次、传递证书 7 次、进行 5 次签名、4 次对称加密和 4 次非对称加密，整个交易过程可能需花费 1.5 至 2 分钟。

随着椭圆曲线密码在密钥长度、加密强度和速度上的种种优越性越来越明显，椭圆曲线密码受到了更多的关注[3]。椭圆曲线密码算法相对于 RSA 系统而言，只需要 160 位的密钥就可以达到 1024 位 RSA 算法提供的安全等级。因此，在 SET 协议中使用椭圆曲线密码算法代替 RSA 算法，将使网络交易的性能和速度获得显著的提高。

4 椭圆曲线密码体制概述

射影平面 Pk2 上的齐次表达式 E：$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ 称为 Weirstrass 等式。其中 $a_1, a_2, a_3, a_4, a_6 \in Fq$，Fq 为有限域。如果椭圆曲线特征值不等于 2 和 3，则椭圆曲线的一般形式可以简化为 $Y^2 = X^3 + aX + b$，$\Delta = 4a^3 + 27b^2 \neq 0$，其中 $a、b \in Fq$。

椭圆曲线密码体制的加密原理基于有限域上椭圆曲线离散对数问题(ECDLP)的困难性[4]：给定素数 p 和椭圆曲线 E，对 Q = kP，在已知 P，Q 的情况下难以求出小于 p 的正整数 k。

在 SECI 及 IEEE P1363ECC[5] 工作草案中，将有限域上椭圆曲线域参数 T 定义为一个六元组：T = (p，a，b，C，n，h)。G(xCG，yG) 是椭圆曲线上的一个基点，$G \neq O$；使 nG = O 的最小正整数 n 称为点 C 的阶；整数 h 是余因子，是椭圆曲线上所有点的个数 m 与 n 相除的整数部分。由以上参数可以惟一地确定一个椭圆曲线。在[1，n −1]之间随机地确定一个整数 k，计算 Q = kP，由此就确定了密钥对(k，Q)，其中：k 是私钥，需要保密，Q 是公钥，需要公开。而 T 也要完全公开。

5 基于的安全电子交易的网上银行 CA 系统

CA(认证中心)选取有限域 GF(p) 上的一条椭圆曲线 E，在 E(a，b)(GF(p)) 上选取一点 G，确定参数 T(p，a，b，G，n，h)，选取安全的 Hash 函数 H，T、H 公开。

假定用户 S 的个人身份资料为 ID，公钥为 Ksp，S 将 ID 和 Ksp 发往 CA 申请数字证书：

① CA 选取随机数 k(1 < k < n)，计算 kG = (x，y)，r = x mod n；如果 r = 0，则重做本步；

② 计算 e = H(ID + Ksp)，得到信息的摘要；

③ 计算 $s = k^{-1}(e + rd) \pmod n$，如果 s = 0，则返回到②；

CA 生成的签名为(r，s)，CA 向 S 颁发的数字证书为(ID，Ksp，(r，s))。

当用户 S 和商家 A 进行交易时，S 要把自己的证书 CAs 发给 A，而 A 可以通过 CA 对证书 CAs 进行验证，过程如下：

① 验证 r，s 是否为[1，n −1]间的整数；

② 计算 e = H(ID + Ksp)，$w = s^{-1} \pmod n$；

③ 计算 $U_1 = ew \pmod n$，$U_2 = rw \pmod n$；

④ 计算 $X = U_1G + U_2Q = (X_1, Y_1)$，令 $V = X_1 \bmod n$，只有当 V = r 时才能证明签名是有效的；

设用户 S 的签名证书为 (SS_{PU}, SS_{PV})，商家 A 的交换证书为 (AE_{PU}, AE_{PV})，当用户 S 和商家 A 进行交易时必须对信息作数字签名并将使用的对称密钥加密生成数字信封，过程如下：

① S 从证书中提取 AE_{PU}；

② 对定单信息 OI、信用卡信息 PI 生成双摘要 e = H(H(OI) + H(PI))；

③ S 生成随机密钥对(k，X)，其中 X = (x，y)，然后计算 r = xe(mod n)，$s = k^{-1}(e + r\,SS_{PV}) \pmod n$，S = (r，s) 就是持卡人的数字签名；

④ 把 OI、H(PI)、S 和 CAs 连接到一起，用随机的对称密钥 K 加密，得到加密信息 D；

⑤ S 生成随机密钥对(k′，y′)，计算 $i = k'AE_{PU}$，X′ = (x′，y′) = k′G，j = x′K，则 E = (i，j) 就是数字信封；

数字签名校验和数字信封解密过程如下：

① A 首先用 AE_{PV} 解密信封，根据 $GAE_{PV} = AE_{PU}$，求

出(x′,y′);

② 由 I=x′K,可导出 K=jx′-1,得到对称密钥 K;

③ 用 K 解密信息 D,得到 OI、H(PI)、S 和 CAs;

④ A 通过 CA 中心对 S 的证书 CAs 进行验证,提取 S 的签名公钥 SS_{PU};

⑤ 验证数字签名 S=(r,s),判断 r、s 是否为[1,n-1]间的整数;

⑥ 生成双摘要,e=H(H(OI)+H(PI)),$w=s^{-1}(\mathrm{mod}\ n)$;

⑦ 计算 $U_1=ew(\mathrm{mod}\ n)$,$U_2=rw(\mathrm{mod}\ n)$;

⑧ 计算 $X=U_1G+U_2Q=(X_1,Y_1)$,令 $V=X_1 \mathrm{mod}\ n$,只有当 V=r 时才能证明签名是有效的。

系统包括:基本模块,诸如长整数的左右移位、加法、减法、模乘与反元素等。第二层则建立椭圆曲线的加法、乘法等模块,在此二模块基础上构筑椭圆曲线[6],搭配 DES 等模块建立椭圆曲线密码体制,公钥产生后,私钥将以 DES 加密存放。最上层为基于椭圆曲线密码体制实现 SET 协议中公开密匙的加密解密、数字签名的生成认证、电子信封的加密解密和数字证书的生成认证等核心功能模块。

表 1　ECC 与 RSA 速度比较

功能	160 位 ECC(ms)	1024 位 RSA(ms)
密钥对生成	3.8	4708.3
签名	2.1	228.4
认证	9.9	12.7
密钥交换	7.3	1654.0

6　结束语

论文提出一套基于椭圆曲线密码算法 ECC 的 SET 协议的身份认证系统,藉以提升安全电子交易协议的效率,使即时性的安全电子交易成为可行的方案,并在此基础上实现网上银行交易的 CA 系统。

参考文献

1 张一卓,电子商务支付系统[M],成都 四川大学出版社,2002。

2 梁普等,电子商务核心技术—安全电子交易协议的理论与设计[M],西安大学出版社,2003。

3 V. S. Miller. Use of elliptic curves in cryptography [J]. Advances in Cryptology – Crypto'85,1986,LNCS 218 Springer – Verlag:417 – 426.

4 Christof Paar," Implementation Options for Finite Field Arithmetic for EllipticCurve Cryptosystems," 3rd workshop on Elliptic Curve Cryptography 99,Nov1999.