一种基于椭圆曲线的高效移动支付系统*

彭 冰[a], 付 才[a], 付 雄[b]
(华中科技大学 a. 计算机科学与技术学院; b. 电子与信息工程系, 武汉 430074)

摘 要: 针对移动手持设备处理能力和存储空间较弱的限制,提出了一种基于椭圆曲线密码体制的移动电子支付系统。与传统的基于 RSA 及离散对数问题的电子支付系统相比,提出的系统所需安全参数字节较短且易于扩展,因而存储、计算和通信效率大大提高,能够很好地满足移动支付系统的所有安全要求,并能有效防止重复花费、欺诈行为和高手段犯罪。

关键词: 移动支付系统; 全球移动通信; 椭圆曲线密码体制; 公平性
中图分类号: TP309.2 **文献标志码**: A **文章编号**: 1001-3695(2008)09-2819-03

Efficient mobile payment system based on ECC

PENG Bing[a], FU Cai[a], FU Xiong[b]
(a. College of Computer Science & Technology, b. Dept. of Electronics & Information Engineering, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract: Since the computing power and storage space of mobile handle terminal were very poor, this paper introduced a mobile payment system based on elliptic curve cryptosystems. Compared with previous e-cash systems based on RSA or discrete logarithm, the new system required much shorter security parameter size and it was convenient to be expanded. Moreover, the storage, the computation and communicating efficiency were improved in the new system, at the same time, all the security features for mobile payment were kept as usual. Furthermore, the system can prevent from double spending, fraud and perfect crime effectively.

Key words: mobile payment systems; GSM; elliptic curve cryptosystems; fairs

0 引言

随着移动通信设备的迅猛发展和广泛应用,具有身份识别功能的移动电话能够代替各种银行卡成为个人的随身电子钱包,使支付形式彻底摆脱空间上的束缚[1]。移动支付作为一种全新的支付手段[2~4],实现了钱包的电子化和移动化,不仅快捷,而且实现方便,从而为客户创造了更灵活、更亲切的消费环境。

在 GSM 网络中,用户端的身份认证与密钥分配功能是由移动用户个人身份模块 SIM 卡来实现的[5,6]。目前的 SIM 卡相当于一个内嵌有 8 位微处理器的智能卡,其工作时钟通常在 8MHz 左右,内部数据存储器约 300 B,程序存储器 5 ~6 KB。公钥密码算法为了维持足够的安全性,目前都采用了更长的模,不仅增加了公钥密码算法实现的复杂度,也增加了密码协议中数据的传输量,这些不仅对计算能力低且计算资源有限的 SIM 卡构成挑战,也对通信带宽有限的移动通信网络构成挑战[7]。

随着移动通信网络的不断发展,网络的频率带宽也在不断增加,从而提高了数据传输速率,如第三代蜂窝系统可实现 2 Mbps 数据传输速率。而且,随着大规模集成电路技术的发展,微处理器的计算能力在成倍增强,存储器容量也在成倍增加,特别是内嵌 32 位微处理器的智能卡的出现,将极大地增强移动端的计算能力和计算资源。基于这种情况,一些新的短参数公钥密码系统也被不断提出[8,9],特别是基于椭圆曲线上离散对数难题的椭圆曲线密码体制(ECC),由于缺少亚指数性的攻击方法,从而可以使用较少位的椭圆曲线密码算法在安全性方面相当于多位的 RSA 算法[10,11]。由于椭圆曲线密码算法可以采用较短的参数,不仅占用更少的系统资源,极大地降低了椭圆曲线密码算法的实现复杂度,加快了计算速度使成本和能耗更低,而且减少了密码协议中的数据传输量。本文所提出的基于 ECC 的安全移动支付系统就是建立在椭圆曲线离散对数难解及散列函数单向性的基础上的。

1 系统基本模型

本文所提出的移动支付方案涉及到交易的四方,即移动用户 U、增值服务提供商 VASP、网络服务提供商 SP 和银行 B,如图 1 所示。其中,移动用户是使用数字货币和移动电话购买信息商品或服务的主体;增值服务提供商是为移动用户提供商品或服务并接受其支付的网上商店;网络服务提供商在方案中相当于经纪人的角色,其作用在于搭建移动支付服务平台,为移动用户和 VASP 开立并维护账户、认证交易双方的身份、进行货币销售和交易结算;银行是一个具有电子认证功能的参与者,并协调解决可能引起的争端。

2 基于 ECC 的移动支付系统

本文中所用符号的意义如下: $x \in_R N$ 表示 x 在集合 N 中

收稿日期: 2007-11-23; 修回日期: 2008-03-03 基金项目: 国家自然科学基金资助项目(60703048)

作者简介: 彭冰(1972-),男,湖北荆州人,博士,主要研究方向为电子商务安全、无线网络攻击与防御(pbdhl@sina.com);付才(1976-),男,讲师,博士,主要研究方向为无线网络路由协议安全、软件脆弱性分析与利用;付雄(1968-),男,博士研究生,主要研究方向为移动电子支付、信息安全、应用密码学.

随机地选取; $H(\cdot)$ 表示碰撞自由的单向散列函数; ‖ 表示字符串连接操作符; $R_x(A)$, $R_y(A)$ 表示取 A 点的 x、y 坐标; p、q 表示大素数, q 是 $p-1$ 的一个大的素因子(即 $q \mid (p-1)$); Z_p^* 表示小于 p 的正整数集合; G_p 表示乘法群 Z_p^* 的一个 q 阶子群, 并且假定在 G_p 上求解椭圆曲线离散对数是困难的; Z_q 表示小于 q 的非负整数集合; E 是方程为 $y^2 = x^3 + ax + b$ 的椭圆曲线, 且 $4a^3 + 27b^2 \neq 0$; B 为 E 上一个阶为 n 的基点(生成元)。

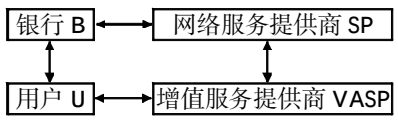

图 1 移动支付系统模型

基于 ECC 的移动支付系统中银行是一个具有电子认证功能的参与者, 它无须知道任何与用户有关的隐私信息, 只是起到一个可信第三方的作用, 在移动支付过程中证明电子现金使用的有效性。

2.1 开户协议

网络服务商 SP 选择大素数 p, q 且 $q \mid (p-1)$, 以及一个碰撞自由的单向散列函数 $H(\cdot)$, 由此可以构造乘法群 Z_p^* 的一个 q 阶子群 G_q, 并且假定 G_q 在上求解椭圆曲线离散对数是困难的。记 B 为 E 上一个阶为 n 的基点(生成元), 选取 $x_B \in_R Z_q^*$ 作为 SP 的私钥, 其对应的公钥为 $P_B = x_B B$。SP 公布 p、q、B、H 和 P_B。

移动用户选取 $x_U \in_R Z_q^*$, 计算 $ID_U = x_U B = (ID_{Ux}, ID_{Uy})$, 然后将 ID_U 和用户电话号码 N_U 一起发送给 SP, 作为用户的账号, 同时向 SP 出示其身份证或护照等来惟一标志其身份。SP 验证其证明, 为其开立并维护一个账户, 然后在移动用户账户数据库中存储该移动用户的身份识别信息及 ID_U、N_U, 账号 ID_U 与用户的身份信息必须一一对应。这样, 在用户实施重复花费后, SP 能通过计算得到该用户账号, 进而确定其身份。

移动用户 U 与 SP 共享一个秘密密钥 K_{US}, 并从 SP 处得到移动用户和 VASP 共享的会话密钥 K_{UV}。

增值服务提供商 VASP 也必须在 SP 开户。VASP 选取 $x_V \in_R Z_q^*$, 计算 $ID_V = x_V B = (ID_{Vx}, ID_{Vy})$ 并将 ID_V 作为其身份标志发送给 SP, 同时向 SP 出示其营业执照和网址 A_V 等来惟一标志其身份, 作为 VASP 的 SP 账号。SP 验证后存储 VASP 账号, 为其开立和维护一个账户, 并在 VASP 账户数据库中存储该 VASP 的身份识别信息 ID_V 和网址 A_V, 从而将 A_V 与 VASP 的身份识别信息 ID_V 绑定在一起。同样, VASP 也与 SP 共享一个秘密密钥 K_{VS}, 且可从 SP 处得到移动用户和 VASP 共享的会话密钥 K_{UV}。

用户及增值服务提供商的开户过程如图 2 所示。

2.2 取款协议

用户随机选取 $l \in_R Z_q^*$, 计算 $a = lB = (a_x, a_y)$, $M = lP_B + d ID_U = (M_x, M_y)$ (d 是由 SP 和用户共同计算的电子现金的私钥), $e' = H(M_x \oplus M_y, a_x \oplus a_y)$ 和 $\sigma = l - x_U e'$。这样一个电子现金 c 就可以用一个二元组 (a, M) 来表示, e', σ 是签名, 将 M、e'、σ 连同 ID_U 的值发送给 SP。

SP 计算 $a' = \sigma B + e' I_U = (a'_x, a'_y)$, 并进行如下验证: $e' \stackrel{?}{=} H(M_x \oplus M_y, a'_x \oplus a'_y)$。若通过, 则在调整用户账面余额后, 发送 $Cert_c$ 给用户。

用户保存 $\{l, d, Cert_c\}$ 的值, 然后发送 c 和 $Cert_c$ 给银行 B; 银行在保存了 c 的电子现金序列表中检测这些电子现金是否出现过(即银行是否已经处理过)。若没出现, 则检查电子现金 c 和证书 $Cert_c$ 的合法性。对于每个电子现金, 给定一个附加的数字 x_i $(1 \leq i \leq n)$, n 为用户一次从银行所取电子现金的个数, 记 $H(x_1) = y_1$, $H(x_2) = y_2$, …, $H(x_n) = y_n$, 并对 y_1, y_2, y_n 和 n 进行签名得到:

$$S_T = \mathrm{sign}_T\{y_1, y_2, \cdots, y_n, n\}$$

然后发 $\{S_T, y_1, y_2, \cdots, y_n, n\}$ 给用户。至此, 移动用户在其账户上存储了一定数额的电子现金。

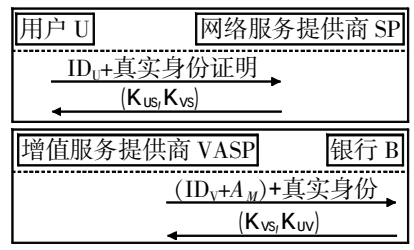

图 2 开户协议

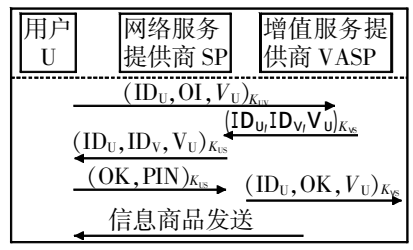

图 3 支付协议

2.3 支付协议

支付协议如图 3 所示。

具体执行步骤如下:

a) 用户 U 使用移动电话浏览 VASP 的站点选择需要购买的商品或服务, 并记录 VASP 的网址 A_V 及商品或服务的价格, 生成订单信息 OI, 它包含购买商品或服务的种类、数量和总金额等信息。

移动用户发送 m 和 x_k 给 VASP。其中: m 是包含电子现金 c、数字证书 $Cert_c$ 和时戳等信息的数据段; x_k 为用户支付给 VASP 的电子现金所对应的附加数字, 即发送给 VASP 的一个购买请求。用户购买请求的格式为

$$(ID_U, OI, V_U)_{K_{UV}}$$

其中: V_U 为本次交易总额。

b) VASP 为保证支付的安全可靠, 需要访问 SP 服务器, 验证电子现金和证书的合法性, 并计算 $H(x_k)$, 检查其是否在黑名单中(黑名单是丢失或失效电子现金散列值的列表)。同时, 将包含移动用户订单信息的支付授权请求发送给 SP 服务器:

$$(ID_U, ID_V, V_U)_{K_{VS}}$$

c) SP 服务器根据移动用户和 VASP 的标志通过遍历数据库来检查其对应账户的合法性, 以保证其处于良好的状态且没有任何使用限制, 选择 $\varepsilon \in_R Z_q^*$, 计算:

$$r = H(\mathrm{date} \parallel \mathrm{time} \parallel \varepsilon \parallel I_{sx} \parallel I_{sy})$$

其中: date、time 分别为交易的日期和时间。并发送 r 给用户; 然后根据 ID_U 确定移动用户的移动电话号码, 并向其发送如下的扣账请求:

$$(ID_U, ID_V, V_U)_{K_{US}}$$

d) 移动用户收到 SP 服务器发送来的扣账请求后, 首先检验其合法性并对支付信息进行确认, 即计算 $s = rP_B + dB = (s_x, s_y)$, $e = H(m, s_x \oplus s_y)$, $u = r - le$, $v = d - x_U e$, $t_1 = (d-1) x_U e B = (t_{1x}, t_{1y})$, (e, u, v, t_1) 即签名 S, 发送 (e, u, v, t_1) 及 m 给 VASP。然后将包含个人识别码 PIN(通常为四位数)的扣账响应发送给 SP 服务器:

$$(OK, PIN)_{K_{US}}$$

e) SP 服务器收到移动用户的个人识别码后, 确认是移动用户本身参与了此次交易, 然后向 VASP 发送如下的支付授权响应:

$$(ID_U, OK, V_U)_{K_{VS}}$$

如果在给定时间(2 min)内, SP 服务器没有收到移动用户发送来的扣账响应信息, 则该交易将被自动取消。

f) VASP 计算 $t' = uP_B + vB + eM = (t'_x, t'_y)$, 并检查:

$$t' \stackrel{?}{=} s + t_1,\ e \stackrel{?}{=} H(m, R_x(t' - t_1) \oplus R_y(t' - t_1))$$

确认无误后, VASP 将信息商品或服务发送给移动用户。

2.4　转账协议

VASP 发送支付协议的副本给 SP, 包括(e, u, v, t)及证书 $Cert_c$, 电子现金 c、挑战 r 和时戳。

当移动用户 U 收到 VASP 提供的商品或服务后, 他将使用其移动电话发送一个支付认可消息给 SP; SP 验证其合法性, 根据移动电话号码使用 GSM 中的 SIM 卡来鉴别并获得移动用户的身份 ID_U, 并检查电子现金的 $H(x_k)$ 是否在黑名单中, 然后从移动用户账户上扣除与交易额相当的电子现金转移到 VASP 账户上。

3　系统安全性与效率分析

3.1　安全性分析

由于每次支付执行时, 交易信息都使用公钥进行了加密, 攻击者无法获取相关的敏感信息, 从而保护了移动用户隐私和支付信息的安全。本系统的安全性是建立在椭圆曲线离散对数难解和散列函数单向性基础上的。它具有不可重用性, 即在用户实施重复花费后, 银行可通过计算得到该用户账号, 进而确定其身份。其过程如下:

在本系统中, 如果用户实施了重复花费, 则同一电子现金在支付过程中将有两个签名:

$$S_1 = (e_1, u_1, v_1, t_{11}),\ S_2 = (e_2, u_2, v_2, t_{12})$$

且有 $u_1 = r_1 - le_1$, $v_1 = d - x_U e_1$, $u_2 = r_2 - le_2$, $v_2 = d - x_U e_2$。

根据上述信息可得到$(v_2 - v_1) / (e_1 - e_2) = x_U$, 即用户 ID_U 的私钥。因此, 在本系统中用户的电子现金是不可重用的。

在本方案中, 移动用户企图使用账户上不足的余额与 VASP 进行交易(移动用户企图进行超支花费)是不可能的, 非良好状态的账户将直接导致支付的中止。另一方面, 若 VASP 发送与订单信息不同或便宜的商品, 则移动用户在对商品或服务进行检查后, 拒绝发送支付认可消息, 因而 VASP 无法得到相应的交易资金。

3.2　匿名性

本系统具有受限的不可追踪性。当用户构造一个电子现金时, 要用到私钥 x_U, 该参数在支付过程中对任何其他人是不可知的。因此没有人能够根据电子现金的支付信息来追踪用户。而且, 由于 I_U 的椭圆曲线离散对数 x_U 是难解的, 对用户进行非法攻击从而伪造签名是不可能的。

3.3　公平性

在本方案中, 电子现金的使用要得到银行的检验, 确保了电子现金使用的有效性。移动用户在获得商品或服务之前, VASP 无法得到相应的交易资金, 因为 SP 只有在得到移动用户的支付认可消息后才实施转账。同时, 若移动用户宣称其收到的商品或服务与订单信息中规定的不符合, 或否认已收到的 VASP 提供的商品或服务, 则 SP 服务器会要求 VASP 对信息商品或服务进行重发, 直到移动用户认可为止。在这种情况下, 移动用户的欺诈行为并不能使其得到相应收益, 因而方案使得消费者和商家的利益都得到了保障, 从而具有一定的公平性。

3.4　效率分析

与基于 RSA 和离散对数问题的电子支付系统(如 Okamoto[12] 和 Chan[4] 等人提出的电子现金支付系统)相比, 本文所提出的基于 ECC 的移动支付系统采用了椭圆曲线密码体制, 所需的安全参数字节数较短且易于扩展, 在占有较小系统空间的情况下仍能达到与使用模指数运算其他系统相同的安全水平, 因而存储、计算和通信效率大大提高。例如 RSA 加密体制进行模指数运算时需要 1 024 bit 的密钥, 在 ECC 中若要达到相同要求则只需 160 bit 即可。因此 ECC 中密钥的长度较短, 内存空间和计算能力都可以降低, 尤其适用于存储容量有限的基于智能卡的电子钱包。

4　结束语

本文设计了一个基于 ECC 的移动支付系统。与传统的基于效率不高的模指数运算的电子支付系统相比, ECC 具有密钥长度较短和安全性更高的特点, 从而使得本系统的存储、计算和通信效率大大地提高, 减少了移动终端计算和通信的负荷, 适用于移动支付系统。此外, 本系统还能有效地防止重复花费、窃听、窜改、非法攻击和犯罪。

参考文献:

[1] ZONG R, JAN M, JAHANNES S, *et al*. Comparing usage of mobile commerce in Taiwan[J]. International Journal of Services, Technology and Management, 2006, 7(3): 284-296.

[2] VEIJALAINENA J, TERZIYANB V, TIRRIC H. Transaction management for m-commerce at a mobile terminal[J]. Electronic Commerce Research and Applications, 2006, 5(3): 229-245.

[3] BRANDS S. Offline cash transfer by smart cards[C]//Proc of the 1st Smart Card Research and Advanced Application Conference. France: Chapman & Hall Press, 1994: 101-117.

[4] CHAN A, FRANKEL Y. Easy come-easy go divisible cash[C]// Proc of Advances in Cryptology EUROCRYPT '98. Helsinki, Finland: Springer-Verlag, 1998: 561-575.

[5] JAUME B, MIQUEL O, JORGE I. Adapting a captive portal to enable SMS-based micropayment for wireless Internet access[C]//Performability Has Its Price ICQT 2006. Heidelberg, Berlin: Springer-Verlag, 2006: 78-79.

[6] ISAAC J, CAMARA J, MANZANARES A, *et al*. Payment in a Kiosk centric model with mobile and low computational power devices[C]// Proc of Computational Science and Its Applications-ICCSA 2006. Berlin: Springer, 2006: 798-807.

[7] TSAUR W J, HO C H. A secure electronic payment system based on efficient public key infrastructure[C]//Proc of International Workshop for Asian Public Key Infrastructures-IWAP 2002. Taipei: [s. n.], 2002.

[8] LIU Jun, LIAO Jian-xin. A new universal model for mobile payment system and its protocol[J]. High Technology Letters, 2006, 16(6): 560-565.

[9] JIN K, SOOHYUN O, DONGHO W. Efficient key distribution protocol for electronic commerce in mobile communications[C]//Proc of the 7th International Conference on PARA 2004. Berlin: Springer-Verlag, 2006: 1009-1016.

[10] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名和盲签名[J]. 通信学报, 2001, 22(8): 22-27.

[11] 隋爱芬, 杨义先, 钮心忻, 等. 基于椭圆曲线密码的可认证密钥协商协议的研究[J]. 北京邮电大学学报, 2004, 27(3): 28-32.

[12] OKAMOTO T. An efficient divisible electronic cash scheme[C]// Proc of CRYPTO '95. Santa Barbara, California: Springer-Verlag, 1995: 438-451.