短 文

基于椭圆曲线的盲签名与离线电子现金协议

郭涛[1]，李之棠[1]，彭建芬[2]，吴世忠[3]

（1. 华中科技大学 计算机学院，湖北 武汉 430074；

2. 华中科技大学 数学系，湖北 武汉 430074；3. 中国信息安全产品测评认证中心，北京 100089）

摘 要：将基于乘法群的离散对数的数字签名映射到椭圆曲线上，提出了一个基于椭圆曲线的盲签名方案，并在其基础上利用 Brands 的受限盲签名技术构建了一个高效的离线电子现金协议。

关键词：电子支付；电子现金；盲签名；椭圆曲线

中图分类号：TN918 **文献标识码**：A **文章编号**：1000-436X(2003)09-0142-05

Blind signature and off-line e-cash system based on elliptic curve

GUO Tao[1], LI Zhi-tang[1], PENG Jian-fen[2], WU Shi-zhong[3]

(1. Department of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan 430074, China;

2. Department of Mathematics, Huazhong University of Science and Technology, Wuhan 430074, China;

3. China National Information Security Testing Evaluation & Certification Center, Beijing 100089,China)

Abstract: Elliptic curve digital signature is the elliptic curve analogue of the digital signature based on multiplicative group's discrete logarithm. In this paper, by using restrictive blind signature technique, we present an efficient off-line electronic cash system based on a kind of elliptic curve digital signature.

Key words: blind signature; electronic cash; electronic payment; elliptic curve

1 引言

随着计算机运算速度的加快和因特网分布式协同计算的发展，人们不得不采用增加密钥长度的方法来提高基于大数分解的传统公钥密码体制的安全性。但是，对于一些对密钥长度比较敏感的应用，尤其是采用智能卡的电子现金支付系统来说，密钥长度的无限延长不是解决问题的最终办法。

收稿日期：2003-03-13；修订日期：2003-06-02

基金项目：国家自然科学基金资助项目（90104033）

作者简介：郭涛（1974-），男，湖北宜昌人，华中科技大学博士生，主要研究方向为电子支付、信息安全；李之棠（1951-），男，湖北监利人，华中科技大学教授、博士生导师，主要研究方向为信息安全；彭建芬（1977-），女，湖北衡山人，华中科技大学研究生，主要研究方向为椭圆密码曲线；吴世忠（1962-），男，湖南永顺人，中国信息安全产品测评认证中心主任，研究员，主要研究方向为信息安全，密码学。

数学家们研究椭圆曲线已有一百多年历史，直到 20 世纪 90 年代，Koblitz 和 Miller[1,2] 才开始将其应用到密码领域中。椭圆曲线密码体制的数学基础就是利用椭圆曲线上的点构成的 Abelian 加法群构造的离散对数的计算复杂性。椭圆曲线密码体制与基于离散对数的传统公钥密码体制相比有两个优点：密钥长度较短和安全性更高。文献[3]提出了几种基于椭圆曲线的盲签名协议，我们将 Schnorr 盲签名方案扩展到椭圆曲线上，并利用 Brands 的受限盲签名技术提出了一个高效的离线电子现金方案。

2　有限域上的椭圆曲线

椭圆曲线，指的是由韦尔斯特拉方程：$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ 所确定的平面曲线，通常用 E 表示。如果 F 是一个域，$a_i \in F, i = 1,2,\cdots 6$，则满足上述韦尔斯特拉方程的二元组 (x, y) 称为 F 域上的椭圆曲线 E 上的点。F 域可以是有理数域、复数域或有限域 $\mathrm{GF}(p^r)$ 等。椭圆曲线除了曲线 E 上的所有点以外，还包括一个特殊的无穷远点 O。

通常我们在有限域（伽罗瓦域）上研究椭圆曲线 E。设 $P = (x_1, y_1)$，$Q = (x_2, y_2)$ 为椭圆曲线 E 上任意两点，定义运算 $\oplus$ 如下：设 L 是 PQ 的连线（若 P、Q 两点重合，即 $P = Q$，则 L 退化为 P 点的切线）。设 L 与曲线相交于另一点 R，L' 是 R 点和无穷远点 O 的连线（即 L' 是过 R 点与 y 轴的平行线），L' 和曲线相交于另一点，用 $P \oplus Q$ 表示。

容易证明，椭圆曲线上的点关于 $\oplus$ 运算构成一个 Abel 群[4]，其单位元为无穷远点 O。若 P 是椭圆曲线 E 上的一点，存在最小的正整数 n，使得 $\underbrace{P + P + \cdots + P}_{n\text{次}} = nP = O$，则称 n 是 P 点的阶。鉴于椭圆曲线上的运算 $\oplus$ 具有上述特性，我们可以实现椭圆曲线上的密码系统，实际上，这样的密码系统就是将一些传统的加密运算移植到椭圆曲线上。

3　基于椭圆曲线的盲签名方案

3.1　Schnorr 盲签名

运用 Okamoto 和 Ohta 提出的可转移的零知识证明，可以根据基于交互式零知识身份识别方案的签名方案来构造盲数字签名方案，其中较典型的是最早由 Okamoto 提出的 Schnorr 盲签名方案[5]。

Schnorr 盲签名方案的系统设置、密钥产生、签名验证和 Schnorr 签名相同。设 G 是阶为 q 的有限循环群，$g \in G$ 是 G 的生成元，在 G 中计算离散对数是困难的。签名者的私钥是 x，公钥是 $y = g^x$。散列函数：$H: \{0,1\} \to Z_q$。签名协议如图 1 所示，其中消息 $m \in \{0,1\}^*$，产生的签名为 $(c, s) \in Z_q \times Z_q$。签名的验证方程是 $c = H(m \| g^s y^c)$。

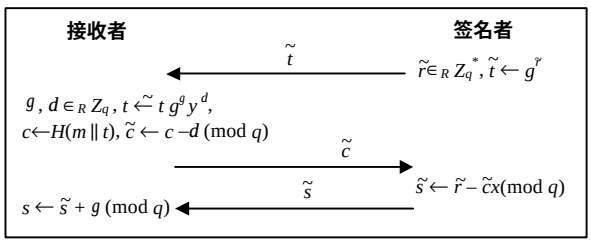

图 1　Schnorr 盲签名协议

该签名的不可伪造性由 Schnorr 签名方案的安全性保证。该签名还具有统计盲性：假设 $(m,(c,s))$ 是任意一次签名协议产生的消息/签名对，$(\tilde{r},\tilde{t},\tilde{c},\tilde{s})$ 是任意一次签名协议中签名者的协议信息，则签名者可以计算盲因子 $g=s-\tilde{s}(\bmod q)$ 和 $d=c-\tilde{c}(\bmod q)$，由于 $\tilde{s}=\tilde{r}-\tilde{c}x(\bmod q)$，所以有：$g^s y^c=g^{\tilde{s}+g}y^{\tilde{c}+d}=g^{\tilde{s}+\tilde{c}x}g^g y^d=\tilde{t}g^g y^d=t$，即 $(m,(c,s))$ 能够通过签名验证，这就说明对签名者来说任意一个通过验证的消息/签名对可能由任意一次签名会话产生。

3.2 椭圆曲线上的 Schnorr 盲签名方案

椭圆曲线的盲签名方案实际上可以看作是 Schnorr 盲签名方案在椭圆曲线上的模拟。在本协议中，定义 m 为接收者发送给签名者的消息，d 为签名者私钥，$Q=dG$ 为签名者公钥。将 $(q,FR,a,b,G,n,h,Q,H())$ 公开（符号的具体定义见 4.1 节）。盲签名协议具体的执行步骤如图 2 所示。最后接受者得到签名者对 m 的盲签名为 (c,r)，证明略。

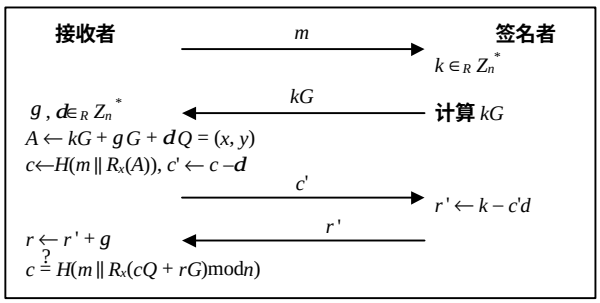

图 2 椭圆曲线盲签名方案

4 基于椭圆曲线盲签名的离线电子现金方案

4.1 系统参数

有限域 $\mathrm{GF}(q)$ 上椭圆曲线的有理点的个数 $\#E(\mathrm{GF}(q))$ 可以被一个大素数 n（$n>2^{160}$ 且 $n>4\sqrt{q}$）整除，有限域 $\mathrm{GF}(q)$ 的特征为 p，基点 $G,G_1,G_2\in E(\mathrm{GF}(q))$。将 d 保密，并将 $(q,FR,a,b,G,G_1,G_2,n,h,Q,H())$ 公开，其中

- q 是有限域 $\mathrm{GF}(q)$ 中元素的个数，这里 $q=p$ 或 $q=2^m$；
- FR 是有限域中元素的表示方法，例如多项式表示或者正规基表示等；
- $a,b\in\mathrm{GF}(q)$，$\mathrm{GF}(q)$ 上的椭圆曲线：$y^2=x^3+ax+b\quad p>3$，$y^2+xy=x^3+ax^2+b\quad p=2$；
- $h=\#E(\mathrm{GF}(q))/n$ 称为余因子，h 远小于 n，可以利用 h 来计算基点；
- $d\in_R Z_n^*$ 是银行签名私钥，$Q=dG$ 是银行签名公钥；
- $H()$ 为散列函数，记号 $\|$ 表示两个比特串的级联，$R_x(A)$ 表示取 A 点的 x 坐标。

4.2 开户协议

1) 用户选取 $u_1\in_R Z_n^*$，计算 $I_u=R_x(u_1\cdot G_1)$ 并将其发送给银行；银行在其用户数据库中存储用户的身份识别信息以及 I_u。

2) 商家选取 $u_2\in_R Z_n^*$，计算 $I_s=R_x(u_2\cdot G_1)$ 并将其发送给银行，银行存储商家帐号；

4.3　提取协议

当用户想要从银行处自己的帐户上提取电子现金时，就和银行一起执行提取协议，如图 3 所示。该提取协议实际上就是一个受限盲签名协议，其中的消息为 $m = I_u + R_x(G_2)$。

银行收到挑战 c 后，计算响应 $r = (k - cd) \bmod q$，将其发送给用户，并从用户的帐户中减去相应数目的金额。用户收到 r 后，验证是否满足：$a = rG + cQ$ 和 $b = rm + cz$。如果满足，则计算 $r' = (r + v) \bmod q$，并存储 $Sign(pk_1, pk_2) = (z', a', b', r')$。因此，六元组 $coin = (pk_1, pk_2, Sign(pk_1, pk_2))$ 就是一个合法的电子现金，只有用户知道该现金的一个表示。限于篇幅，对提取协议中若干等式的推导及对签名的合法性的证明均略。

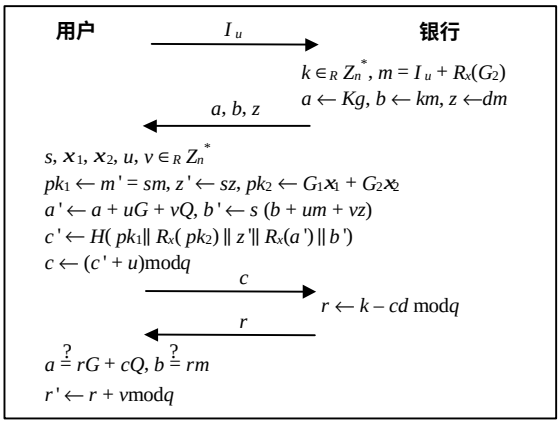

图 3　提取协议

4.4　支付协议

当用户在任何时间在商家处进行购物时，和商家一起执行支付协议。支付协议的具体流程见图 4 所示。记 $msg = I_s \| amount \| t_p$，其中 I_s 为商家在银行处的帐号，标识商家的身份，$amount$ 为交易金额，t_p 为交易时间。

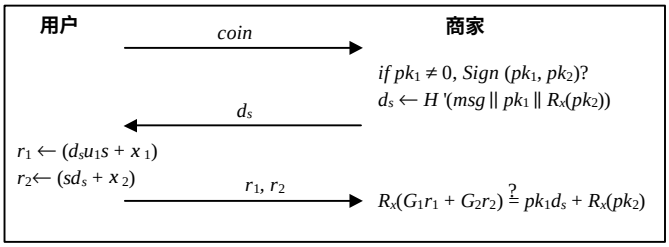

图 4　支付协议

用户计算并发送响应 r_1 和 r_2 给商家，商家首先要判断 $Sign(pk_1, pk_2)$ 为合法签名，并验证等式 $R_x(G_1r_1 + G_2r_2) = pk_1d_s + R_x(pk_2)$ 成立（推导略）。只有两个条件同时满足，商家才接受该电子现金，并给用户提供商品或者服务。

4.5　存储协议

存储协议比较简单：经过一段固定的交易周期后，商家将收到的电子现金到银行处批量进行存储。商家将在支付协议中得到的电子现金的一个副本 $\{coin, r_1, r_2, msg\}$ 传递给银行，银行验证电子现金 $coin$ 的有效性，如果验证不通过，则拒收该电子现金；否则，就继续在银行

的电子现金数据库中搜索该电子现金，如果搜索失败，则说明此电子现金有效，银行就在数据库中录入该电子现金和 (r_1, r_2, msg)，并在其帐目数据库中为商家入帐；如果搜索成功，则说明用户或者商家存在欺诈企图，银行拒绝接收此电子现金。

5 系统安全性和效率分析

在本协议中，不仅可以利用椭圆曲线上离散对数的计算困难性来保证用户的匿名性，而且可以防止双重花费。在存储阶段，当银行发现用户或商家可能存在欺诈行为时，银行可以将商家新传递过来的 t_p 与数据库中的原交易时间进行比较，如果相同则说明商家企图在银行多次存储同一电子现金；否则就是用户在商家双重花费同一电子现金，此时不论用户是否在同一商家处多次花费同一个电子现金，都会使得 msg 不同，因此两次存储的记录不同，设新旧记录分别为 (d_s, r_1, r_2) 和 (d_s', r_1', r_2')，根据等式 $r_2 = sd_s + x_2, r_2' = sd_s' + x_2$ 和 $R_x(G_1 r_1 + G_2 r_2) = pk_1 d_s + R_x(pk_2)$，可得双重花费用户的身份：$u_1 = (r_1 - r_1')/(r_2 - r_2')$。

在我们的电子现金方案中，由于采用椭圆曲线密码算法，因此密钥的长度选取比较短，尤其适用于存储容量有限的基于智能卡的电子钱包。而且在提取协议中，可以采用将 $pk_1 = sm, pk_2 = x_1 G_1 + x_2 G_2$ 和 $uG + vQ$ 的点加运算进行前置处理的方法来提高在线处理速度，以减轻银行处提取协议产生的计算和通信负担。

6 结论

本文将基于乘法群的离散对数的数字签名映射到椭圆曲线上，提出了一个基于椭圆曲线的盲签名方案，并在其基础上构建了一个离线电子现金协议。本协议可以实现用户的匿名性并可防止恶意用户进行双重花费；由于椭圆曲线的运算位数远小于传统离散对数的运算位数，而且在提取协议中可进行前置预处理运算，所以本协议是一个高效的离线电子现金协议。

参考文献：

[1] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48:203-209.

[2] MILLER V S. Use of elliptic curve in cryptography[A]. Advances in Cryptology-CRYPTO'85, Lecture Notes in Computer Science[C]. Springer-Verlag, 1986. 417-426.

[3] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报, 2001, 22 (8): 22-28.

[4] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全(第 2 版)[M]. 北京：清华大学出版社, 1998.

[5] CAMENISCH J L, PIVETEAU J M, STADLER M A. Blind signatures based on the discrete logarithm problem[A]. Advances in Cryptology —EuroCrypto' 94[C]. 1995.428-432.