2008 世界通信大会中国论坛——网络和信息安全分论坛
（暨第三届中国电信行业信息安全论坛）

基于 ECC 的公平盲签名方案

高海英
（ 西安航空职业技术学院，西安，710094）

摘要：提出了一种新的基于椭圆曲线密码体制的公平盲签名方案。该方案结合了已有的公平盲签名和基于双线性配对函数的短签名方案。方案中裁判者可在特殊情况下揭示签名文件的原文，可有效阻止利用盲签名的匿名性进行犯罪的行为。最后对方案作了安全性分析。

关键词：*RSA*　盲签名　公平盲签名　ECC　双线性配对
中图分类号：TN918.1　　**文献标识码**：A

Fair blind signature scheme based on ECC

Gao Haiying
（Xi'an Aeronautical Polytechnic Institute, Xi'an, 710094）

Abstract: Based on ECC ,a new fair blind signature scheme is proposed. The scheme combines the existing notions of fair blind signatures and the short-signature scheme which is based on bilinear pairings. The scheme allows the judge to find out the contents of the messages and to identify the sender of the digital data, so that it can efficiently prevent the criminality of using the anonymous property of blind signatures. Finally, its security is analyzed.

Key words: *RSA*　blind signature　fair blind signature　ECC　bilinear pairings

1 引言

盲签名方案首先由Chaum于1983首次提出，方案的安全性是基于大整数分解困难性之上的。盲签名要遵循以下原则:发送者能够得到签名者对他所提供的消息的签名,但签名者事后并不知道他所签名的消息内容以及签名。盲签名技术作为一种特殊的签名方式，由于其良好的匿名性，使其在电子货币、股票交易、匿名投票等领域中得到广泛应用。盲签名在一定程度上保护了用户的利益，但是这种匿名性也能被犯罪分子所利用。VonSol和Naccache[1]指出完全匿名的电子支付由于无法跟踪,可能被利用于犯罪如洗黑钱等,于是M. Stadler等提出了公平盲签名[2],它可以在需要的时候让一个可信任的第三方发布信息,允许签名人把消息—签名对和他签名时的具体的内容联系起来,揭开签名,实现对发送消息的人的追踪。在电子支付系统中,就是在必要的时候对电子现金的使用者和电子现金流向进行跟踪,以便减少和挽回损失的。

目前的公平盲签名方案大多基于 *RSA* [3]。为了适应特定领域对数字签名的特殊需求，新的数字签名方案不断提出。近年来，以椭圆曲线上的有理点构成的阿贝尔群为基础建立的椭圆曲线密码体制因其更高的运行效率，更好的安全强度，较短的传输长度和简单、易于实现的优势成为目前的研究热点。基于椭圆曲线的盲签名方案已被提出[4]。文献[4]中采用了基于交互式零知识身份识别的Schnorr盲签名方案。该方案只包含用户和签名者两方，交互的过程比较复杂。本文提出了一种新的基于ECC的公平盲签名方案，大大简化了整个盲签名过程，同时可以追踪用户的身份

实现公平盲签名。该方案以双线性函数为工具，利用短签名方案实现公平盲签名的。方案包含三方参与者，包括用户、签名者以及可信第三方。具体过程为：用户注册，并将注册信息传送给可信第三方；可信第三方验证、保存用户注册信息并进行相关签名；用户验证可信第三方签名，申请签名者进行签名；签名者进行盲签名；用户对盲签名脱盲。

2 预备知识

Bilinear pairings[5]是代数曲线的Weil pairing 和Tate pairing，是构造基于身份的加密方案的重要工具。在文献[6]的加密和签名系统中使用了一个称为双线性映射的特殊函数，这个双线性映射可通过椭圆曲线上的Weil配对构造出来。下面简单介绍其定义及性质。

设G_1是一个由P产生的循环加法群，它的阶是q，G_2是一个阶为q的循环乘法群，则Bilinear pairings是映射e：$G_1\times G_1\to G_2$。更具体的说，G_1可以是某个有限域上的椭圆曲线上的点构成的点群的一个子群，G_2是该有限域上的乘法群的一个子群，e是由椭圆曲线上的Weil pairing 或Tate pairing 产生的。

Bilinear pairings有以下性质：

（1）双线性性：$e(aP,bQ)=e(P,Q)^{ab},\forall P,Q\in G_1,a,b\in Z_q^*$；

（2）非退化性：$e(P,Q)=1,\forall Q\in G_1$，则$P=O$；

（3）可计算性：存在有效算法计算$e(P,Q),\forall P,Q\in G_1$

设G是一个由P生成的阶为素数l的加法循环群（$G=<P>$），假定在G上乘法和逆是可计算的，且$a,b,c\in Z_q^*$，目前有如下4个结论：

（1）DLP（离散对数问题）：给定两个成员P,Q，很难找到一个存在的整数n 使得$Q=nP$。

（2）$CDHP$（计算上的Diffie-Hellman 问题）：给出(P,aP,bP)，计算abP是困难的，不存在多项式时间算法。

（3）$DDHP$（决定性的Differ-Hellman 问题）：给出(P,aP,bP,cP)，能够判断在Z_q^*上$c=ab$是否成立。

（4）$GDHP$：在素数阶循环群G上，$DDHP$在多项式时间内能被解决，但没有任何可能的算法可以解决$CDHP$。

本文所提出的方案正是建立在$GDHP$上的，在随机Oracle模型下，基于$GDHP$的方案已被证明对任意选择明文攻击是安全的。

3 基于ECC的公平盲签名方案

3.1 系统初始化

设椭圆曲线密码体制的系统参数$D=\{E,F_q,n,G,H\}$，其中E为有限域F_q上选取的安全曲线，G为椭圆曲线的基点，且G的阶为n，H为选定的$Hash$。另外，函数e是由选定的椭圆曲线上的Weil pairing 或Tate pairing 产生的双线性函数。

该方案中的参与者为用户U、签名者S以及可信第三方TTP，三者分别随机选取自己的私钥x_U，x_S，x_{TTP}，并分别计算$Y_U=x_UG$，$Y_S=x_SG$，$Y_{TTP}=x_{TTP}G$且公开，则用户、签名者、可信第三方的公私钥对为：（x_U,Y_U），（x_S,Y_S），（x_{TTP},Y_{TTP}）。

假设可信第三方与用户所采用的签名算法为基于双线性配对函数的短签名方案。

3.2 方案执行步骤

3.2.1 用户注册

1、 用户随机选取$r\in Z_q$（$1<r<n$），计算$T=rH(m)G$，（m为真实待签名的消息）。

2、 用户对T进行签名，即计算$s_U=(H(T)+x_U)^{-1}G$。

3、 将(m,ID_U,T,s_U)发送给TTP

3.2.2 可信第三方保存用户信息

1、 可信第三方收到(m,ID_U,T,s_U)后，验证用户的签名是否是他本人的正确签名。验证方程为：

$$e(H(T)G+Y_U,s_U)=e(G,G) \qquad (1)$$

2、 若验证通过，则保存用户的注册信息(m,ID_U,T,s_U)，且计算对T的签名，即计算

$s_{TTP}=(H(T)+x_{TTP})^{-1}G$。

3、 将s_{TTP}发送给用户。

3.2.3 用户验证签名

1、 接收到s_{TTP}后，用户验证s_{TTP}是否是可信第三方的正确签名。验证方程为：

$$e(H(T)G+Y_{TTP},s_{TTP})=e(G,G) \qquad (2)$$

2、 若验证通过，将(T,s_{TTP})发送给签名者。

3.2.4 签名者进行盲签名

1、 签名者接收到(T,s_{TTP})后验证其正确性，验证方程为：

$$e(H(T)G+Y_{TTP},s_{TTP})=e(G,G) \tag{3}$$

2、 计算$s^{'}=x_S^{-1}T$，并将其发送给用户。

3、 保存(T,s_{TTP})。

3.2.5 用户脱盲

计算$s=r^{-1}s^{'}$，则s为m的签名。验证签名算法为：

$$e(Y_S,s)=e(T,r^{-1}G)。 \tag{4}$$

盲签名的执行过程完毕。

我们可以用图 1 来表示该方案的整个过程。

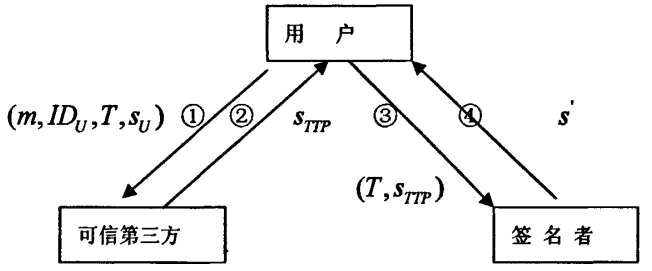

图 1 基于 ECC 的公平盲签名过程

3.3 方案分析

3.3.1 方案的正确性分析

该方案中的签名及验证过程是有效的。证明如下：

方程（1）证明：

$$\begin{aligned}&e(H(T)G+Y_U,s_U)\\&=e((H(T)+x_U)G,(H(T)+x_U)^{-1}G)\\&=e(G,G)^{(H(T)+x_U)\cdot(H(T)+x_U)^{-1}}\\&=e(G,G)\end{aligned}$$

方程（2）证明：

$$\begin{aligned}&e(H(T)G+Y_{TTP},s_{TTP})\\&=e((H(T)+x_{TTP})G,(H(T)+x_{TTP})^{-1}G)\\&=e(G,G)^{(H(T)+x_{TTP})\cdot(H(T)+x_{TTP})^{-1}}\\&=e(G,G)\end{aligned}$$

方程（3）证明同方程(1)(2)的证明。

方程（4）证明：

$$e(Y_S,s)=e(x_SG,r^{-1}s')=e(x_SG,r^{-1}x_SrH(m)G)=e(G,G)^{H(m)}$$

$$e(T,r^{-1}G)=e(rH(m)G,r^{-1}G)=e(G,G)^{H(m)}$$

因此，$e(Y_S,s)=e(T,r^{-1}G)$ 成立。

3.3.2 方案的安全性分析

1、用户发送给 TTP 的数据中，包含有用户对盲化后的消息 T 的签名，这样，别的用户就不能假冒 U 的 ID_U 去 TTP 处登记，否则不能通过 TTP 的验证。别的用户要冒充 U 的难度相当于攻破 U 的签名算法。

2、TTP 发送给用户的盲化后的消息 T 是计算后所得的结果，TTP 不能更改消息 m，否则，(T,s_{TTP}) 不能通过验证。

3、用户发送给签名者 S 的数据是 TTP 对盲化后的消息 T 的签名，用户就不能对已盲化后的消息作任何的修改。

4、当某种情况下要追踪用户时，可通过可信第三方得到用户的信息。

5、方案中的签名算法选取的是基于双线性函数的短签名方案。短签名方案具有计算量小，过程简洁等特点，而且已被证明对于选择明文攻击是安全的。

6、文献[3]中有多步签名过程，本方案中采用了验证过程替代签名对比过程。方案所用的运算主要包括 $GF(p)$ 中的点的数乘、Z_q 中的乘法、双线性对的运算等。与现有的各种基于RSA和离散对数的秘密分享方案相比，我们所用的双线性对方案计算的效率更高。

7、该方案的安全性是基于有限域上椭圆曲线离散对数问题（ECDLP）的困难性之上的。基于模运算的整数因式分解问题和离散对数问题都存在亚指数时间复杂度的通用算法。目前采用最快的算法来计算这两类问题所需要的时间复杂度 $O(\exp((c+o(1)))(\ln q)^{1/3}(\ln\ln q)^{2/3})$（$q$ 为模的大小）[7]；椭圆曲线上的离散对数问题在 $\#E(F_q)$ 有大的素因子时是一个难题，最有效的算法只有指数时间算法。指数时间算法比亚指数时间算法复杂，因此 ECDLP 较另两类问题更为难解，表明 ECC 能以更小的密钥长度产生与其他公钥体制相同等级的安全性。

4 结束语

本文提出了一种基于 ECC 的公平盲签名方案，以双线性函数为工具，利用短签名方案实现了公平盲签名。短签名方案的利用及可信第三方的引入使得方案的计算量降低且过程简洁。另外，同基于 RSA 的同类方案相比，安全性有很大提高，在实际应用中有了更广泛的应用。

参考文献

1. S. von Solms and D. Naccache , On blind signature and perfect crime[J] , Computer and Security , 1992 ,vol . 11:209-219

2. Stadler M,Piveteau J,Camenisch J.Fair blind signatures[A].Proc of Euro-Cryp'95,LNCS 921[C].Berlin;Spring-Verlag,1995:209-219

3.张金全，刘焕平.一个基于 RSA 的公平盲签名方案[J].绥化学院学报，2005，26（2）：166-167

4.王化群，张力军，赵君喜.基于椭圆曲线的Schnorr 盲签名[J]. 计算机工程和设计,2005,26(7):1819-1822

5. Bonch D, Franklin M. Identity based encryption from the weil pairing: Proc crypto 2001 [C]. LNCS: Springer-Verlag, 2001.;213-229.

6.蔡庆华，陈群.基于bilinear pairing的签名方案[J].计算机工程和设计，2005，26（12）：3257-3258

7.Darrel Hankerson,Alfred Menezes, 椭圆曲线密码学导论[M].张焕国等. 北京:电子工业出版社,2005.

作者简介：

高海英（1981—），女，山东德州人，西安航空职业技术学院教师，主要研究方向为椭圆曲线密码。