基于椭圆曲线的公平交换协议

陈 俊
(泰山职业技术学院 建筑工程系,山东 泰安 271000)

摘 要:基于椭圆曲线密码体制,提出了一个数字签名方案,并据此建立了一个适用于电子商务的公平交换协议,该协议通过在交易双方之间建立一个安全承诺作为凭证交换数字签名,以达到摆脱可信第三方参与的目的。此公平交换协议具有一般椭圆曲线密码体制密钥较短、安全性能良好的特点,能够摆脱第三方参与,提高运行效率,并同时保证交换双方的模糊性。分析证明,该协议具有可验证性、不可否认性、不可滥用性以及公平性等特点。

关键词:椭圆曲线;协议;公平交换;模糊性;离散对数

中图分类号:TP309.7 **文献标志码**:A **文章编号**:1672-3767(2014)06-0103-04

A Fair Exchange Protocol Based on Elliptic Curve

Chen Jun
(Department of Building Engineering, Taishan Vocational & Technical College, Taian, Shandong 271000, China)

Abstract: A digital signature scheme was proposed based on the elliptic curve crypto-system, then a suitable protocol for fair exchange in electronic commerce was established accordingly. This protocol can keep out the trusted third party and can guarantee the ambiguity of the exchange as well as the general advantages of short key, high level of security and effective operation brought by elliptic curve crypto-system. This protocol analysis proves its verifiability, non-repudiation, abuse-freeness and fairness.

Key words: elliptic curve; protocol; fair exchange; ambiguity; discrete logarithm

随着计算机网络的迅猛发展,电子商务在人们的日常生活中扮演着极其重要的角色。在网络环境中进行商品交换,互不信任的交换双方除了要满足各自的保密性、完整性和不可否认性等传统需求,还需要引入一种快速公平的方式来交换数据信息。所谓公平性包括信息交换时的公平性和信息接收时的公平性。

相互交换信息的两个人 Alice 和 Bob,当发生下列两种情况之一时,Alice 的优势会大于 Bob:①Alice 一旦得到 Bob 的信息后就终止交易;②Alice 通过伪造虚假信息与 Bob 进行数据交换。所以,在电子商务中参与数据信息交换的双方或者多方都需要通过保护自身的信息来达到信息交换的公平性。另外,Alice 和 Bob 一般通过安全信道来完成数据传输,信息数据收发的时间延迟并不会阻止信息送达对方。当 Alice 接收到 Bob 所发送的数据以后,她会验证这些数据的正确性,如果信息正确便回执对方,以显示她接收到了所需信息,这些信息一旦通过验证便不能被交换双方否认,这就是信息接收的公平性。

在电子商务中,买卖双方进行网络交易时,一方面,双方都会担心各自的隐私信息被滥用于购买其他商品或者签署其他协议上;另一方面,买家又会担心付款后不诚信的卖家不发货,或者在送货途中货物出现问题,卖家也会担心对方账户信息存在错误或者欺骗行为。公平交换协议就是为了解决这种在电子商务过程中交易双方互不见面、互不相信的情况而产生并发展起来的。所谓公平交换,就是确保交易的双方都享有利益安全,也就是说,在交易完成后,交易双方都获得各自想要的东西或者都不获得对方有价值的信息或物品。

收稿日期:2014-09-26

作者简介:陈 俊(1976—),女,山东泰安人,讲师,主要从事应用数学研究. E-mail: tacj7694@sina.com

公平交换协议的基本要求包括合法性、保密性、事实存在性、平等性、及时性以及第三方可确认性等[1]。2007年,马昌社等[2]提出改进的基于 RSA 签名的公平交换协议,其协议改进了文献[3]方案中交换数据不具有可恢复性的缺点,使协议更安全、高效。2010 年,罗铭等[4]利用双线性对提出基于签密的公平交换协议,其方案在适应性选择攻击下能抵抗存在性伪造。同年,李向东等[5]提出离线公平交换协议的自协议分析,研究了自协议之间的关系对协议安全性的影响。随着计算机技术的发展,如何保证信息的安全高效交换已成为人们越来越关注的问题。

相对于其他密码体制而言,椭圆曲线能够使用更短的密钥得到更强的安全性。椭圆曲线密码体制的概念由 Victor Milier 和 Neal Koblitz 在 1985 年首次提出[6],随后被广泛运用到电子商务、在线投票和电子邮件等方案中。2010 年,俞慧芳等[7]提出基于椭圆曲线的自认证签密方案,其方案不需要使用任何公钥证书,私钥由用户自己生成,传输过程中可以保证认证性和保密性。2013 年,王笑海等[8]提出了以椭圆曲线加密体制和零知识身份证明为基础的一种标签与读写器双向身份认证的协议,其安全性建立在椭圆曲线离散对数问题难解性的基础之上。2014 年,周克元等[9]给出一个基于椭圆曲线和因子分解双难题的数字签名方案,其安全性基于椭圆曲线离散对数问题难解性和因子分解问题难解性。

本研究运用椭圆曲线数字签名的思想建立一个新的公平交换协议。在用户运行椭圆曲线数字签名算法之后,将椭圆曲线上点的坐标与关键数 keystone 用 hash 函数加密在一起,生成新的关键数,然后运用这一新的关键数,进行一系列运算输出用户的模糊签名。在签名过程中保证签名的模糊性,即任何外部人员在关键数释放以前都不能确定到底是哪个人签了哪个签名,以此使方案具有更好的公平性,满足双方公平交换的要求。

1 椭圆曲线数字签名算法

椭圆曲线上的离散对数是指:给定有限域 F 上的一条椭圆曲线,若已知这条曲线上的两点 G 和 Q,要求得正整数 k(假设 k 存在),使之满足 $Q=kG$,kG 表示曲线上点的倍乘,即 $kG=G+G+\cdots+G$,k 为倍数。由椭圆曲线上离散对数问题的难解性原理,已知 k 和点 G 求点 Q 比较容易,反之已知点 Q 和点 G 求 k 却十分困难。

Step 1 参数建立(Set-up)

设 $GF(q)$ 是有 q 个元素的有限域,$a,b\in GF(q)$,$GF(q)$ 上的椭圆曲线为 $E:by^2=x^3+ax^2+x$,椭圆曲线域参数 $D=(F,a,b,G,n)$,F 表示有限域 $GF(q)$,G 为椭圆曲线上的一个基点,n 为点 G 的阶,keystone 空间 $K=\{0,1\}^*$,$H_1:\{0,1\}^*\times\{0,1\}^*\rightarrow Z_q$,$H_2:\{0,1\}^*\rightarrow\{0,1\}^*$,$H_3:\{0,1\}^*\times Z_q\rightarrow Z_q$ 为 hash 函数。

Step 2 密钥生成(Key Generation)

用户 i 随机选择一个数 $d_i\in Z_n$,计算 $Q_i=d_iG$,得到密钥对(d_i,Q_i),其中 d_i 为私钥,Q_i 为公钥。

Step 3 模糊签名算法(Asign)

在模糊签名算法中用户需做如下工作:

1)输入系统参数 $D=(F,a,b,G,n)$,用户 i 选择随机数 $\alpha_{ij}\in Z_n^*$,$j=1,2,3$,计算椭圆曲线 E 上点的坐标 $(x,y)=\alpha_{i1}G+\alpha_{i2}G+\alpha_{i3}(Q_i+Q_j)$,得 $\beta=x\bmod n$;

2)利用用户 i 自身的公私钥,计算 $\beta'=\beta d_iQ_j=(x_i,y_i)$,$x_i'=x_i\bmod q$;

3)选择随机数 $k\in K$ 作为自己的关键数 keystone,计算 $k_i=H_3(k\parallel x'_i)$,其中,$\parallel$ 表示前后串数的连接,得到新的用于加密的 keystone。将信息 m 与 k_i 进行 hash 计算后得 $\gamma_i=H_1(m\parallel k_i)$,然后计算 $t_i=H_3(m\parallel\beta_i\gamma_i\bmod n)$,$t_i'=(t_i-\alpha_{i3})\bmod n$,$\mu_i'=(\alpha_{i1}-t_i'd_i)\bmod n$,$\mu_i=(\mu_i'+\alpha_{i2})\bmod n$,则得到关于信息 m 的模糊签名为 $\sigma_i=(\alpha_{i3},t_i,\mu_i,\gamma_i)$。

Step 4 模糊验证算法(Averify)

对于给定的消息 m 和签名 σ 计算 $\beta_i=R_x((t_iQ_i+\mu_iG+\alpha_{i3}Q_j)\bmod n)$,$R_x$ 表示取横坐标。如果 $H_3(m\parallel\beta_i\gamma_i\bmod n)=t$ 成立,则接受。

Step 5 Keystone 验证算法(Kverify)

当双方的 keystone k_i,k_j 都被释放后,其他验证者就可以验证 keystone 的正确性,即验证是否满足

$H_1(m \| k)=\gamma_i$。

Step 6 验证算法(Verify)

外部验证者输入(k_i,k_j,γ),运行 Kverify 算法,如果 $H_1(m \| k_i)=\gamma$,则 i 为初始签名者,若 $H_i(m \| k_j)=\gamma$,则为 j。如果都不相等,则 k 无效,输出“拒绝”。若 k 有效,接着运行 Averify 算法,如果输出“接受”,则最终算法有效,否则无效。

2 公平交换协议

假设 A 与 B 分别是用户和商家,则基于椭圆曲线的公平交换协议如下。

M1 $A\rightarrow B$:(σ_A,m):设商家将商品进行加密后的信息为 m'_B,用户的订单及相应的支票信息为 m_A。当 A 得到 B 的 m'_B后,计算 $m_B=H_2(m'_B)$和 $m=m_A \| m_B$。选择一个随机数 $k_A\in K$,计算 $\beta_A=\beta d_A Q_B=R_x(x_A,y_A)$,$x'_A=x_A \bmod q$,$k'_A=H_3(k_A \| x'_A)$,$\gamma_A=H_1(m \| k'_A)$。然后,运行 Asign 算法,得到$\sigma_A=(\alpha_{A3},t_A,\mu_A,\gamma_A)$。发送$(\sigma_A,m)$给 B。

M2 $B\rightarrow A$:(σ_B,m,k'_B):B 收到 A 的 m_A 后,验证是否正确、合法,如果不正确,退出;如果正确,运行 Averify 算法。若 Averify 算法输出接受,则选择一个随机数 $k_B\in K$,计算 $\beta'=\beta d_B Q_A=R_x(x_B,y_B)$,$x'_B=x_B \bmod q$,$k'_B=H_3(k_B \| x'_B)$,$\gamma_B=\gamma_A+H_1(m \| k'_B)$,然后,运行 Asign 算法输出 $\sigma_B=(\alpha_{B3},t_B,\mu_B,\gamma_B)$。最后,发送$(\sigma_B,m,k'_B)$给 A。

M3 $A\rightarrow B$:(k_A,k_B):B 发送给 $A(\sigma_B,m,k'_B)$后,A 计算$\beta'=\beta d_A Q_B=R_x(x,y)$,运行 Kverify 算法,验证等式 $\gamma_B=\gamma_A+H_1(m \| k'_B)$是否成立,若等式成立,则输入 $D=(F,a,b,G_B,n)$运行 Averify 算法;若不成立,则退出。若 Averify 算法通过,把(k_A,k_B)发送给 B。

M4 $B\rightarrow A$:k:B 首先验证(k_A,k_B),如果正确则把解密商品的密钥 k 发送给 A。因此,双方都达到了交易目的,同时签名也与各自的签名方绑定在一起。想再次购买商品的用户或对商品感兴趣、对这次交易有疑虑的人,都可以通过验证得知签名具体是由谁签署的。其他用户只需计算 $\gamma_A=H_1(m_A \| k_A)$,$\gamma_B=\gamma_A+H_1(m_B \| k_B)$,且运行 Averify 算法后,是否都输出“接受”,若上述条件都成立则签名合法。

3 协议分析

3.1 可验证性

对于给定的 m 及σ 计算$\bar{x}=R_x((tQ_i+\mu G+\alpha_{i3}Q_j) \bmod n)$,若 $H_1(m \| \bar{x}\zeta \bmod n)=c$ 成立,则输出“接受”,若不相等则输出“拒绝”。

证明:因为

$$tQ_i+\mu G+\alpha_{i3}Q_j=tQ_i+(\mu'+\alpha_{i2})G+\alpha_{i3}Q_j=$$
$$tQ_i+(\alpha_{i1}-t_i d_i)G+\alpha_{i2}G+\alpha_{i3}Q_j=tQ_i+(\alpha_{i1}-(t_i-\alpha_{i3})d_i)G+\alpha_{i2}G+\alpha_{i3}Q_j=$$
$$tQ_i+\alpha_{i1}G-t_iQ_i+\alpha_{i3}Q_i+\alpha_{i2}G+\alpha_{i3}Q_j=\alpha_{i1}G\alpha_{i3}Q_i+\alpha_{i2}G+\alpha_{i3}Q_j,$$

所以

$$\alpha_{i1}G+\alpha_{i2}Q_i+\alpha_{i3}Q_i=tQ_i+\mu G+\alpha_{i3}Q_j=(x,y);$$
$$x=R_x((tQ_i+\mu G+\alpha_{13}Q_j) \bmod n);$$
$$H_1(m \| \bar{x}\gamma_i \bmod n)=t。$$

3.2 不可否认性

在签名运行过程中,keystone 始终与签名者的私钥及相应的信息绑定在一起,因此当 keystone 被释放以后,任何人都可以仲裁签名的有效性。

3.3 不可滥用性

如果用户主动向商家递交订单,一般情况下不会退单;另一方面,商家通过出售商品获取利润和信誉,如果没有特殊情况不会无故欺骗消费者。由文献[10]可知,为了使消费者和商家都保证足够的诚信,参与交易的双方均不能向任何第三方证明其有能力使交易内容生效或无效。本方案中,关键数 keystone 已经与签名

者的私钥和个人信息绑定，一旦释放 keystone，任意第三方就可以通过验证得知哪笔消费具体购买了哪个商品，因此满足不可滥用性。

3.4 公平性

假设 A 不诚实，B 诚实，则由文献[4]可知，A 有两次机会欺骗 B。第一次机会出现在签名阶段，此阶段 A 有两种方式进行诈骗，如果 A 不发送签名消息给 B，显然这样的交易不会进行，如果 A 发送错误的签名，B 验证后发现错误，随之终止交易以避免损失。因此，在签名阶段双方是公平的。第二次机会出现在模糊验证后，如果 A 发送错误的 keystone 给 B，B 无法通过验证也不会把解密商品的密钥发给 A，A 无法在交易中取得任何优势。如果 B 不诚实，A 诚实，B 同样有两次机会欺骗 A。最后，双方或者都得到了自己想要的，或者都没得到。因此，本协议是公平的。

4 结束语

通过提出一个基于椭圆曲线密码体制的数字签名方案，建立了一个适用于电子商务的公平交换协议。该协议有椭圆曲线密码体制秘钥短、对硬件要求低且具有良好安全性的特点，除此之外，由于两个参与者通过一个安全承诺——keystone 来交换各自的数字签名，因而整个协议不涉及任何可信第三方，在保证交换双方模糊性的条件下提升了协议运行效率。

参考文献：

[1]樊妹妹，冯蕾，彭长根. 一种无证书的公平交换协议[J]. 贵州大学学报：自然科学学报，2011，28(3)：75-77.
Fan Meimei，Feng Lei，Peng Changgen. A certificateless fair exchange protocol[J]. Journal of Guizhou University：Natural Sciences，2011，28(3)：75-77.

[2]马昌社. 改进的基于 RSA 签名的公平交换协议[J]. 计算机系统应用，2007(2)：28-31.
Ma Changshe. Improvement of fair exchange protocol based on RSA signature[J]. Computer Systems Applications，2007(2)：28-31.

[3]闫乐林，蔡平胜. 一种基于 RSA 签名的公平交换协议的算法设计[J]. 计算机系统应用，2006(5)：40-42.
Yan Lelin. Cai Pingsheng. A fair data exchange protocol based on RSA signature[J]. Computer Systems Applications，2006(5)：40-42.

[4]罗铭，邹春华，胡军. 基于签密的公平交易协议[J]. 通信学报，2010，31(8A)：87-93.
Luo Ming，Zou Chunhua，Hu Jun. Signcryption-based fair exchange protocol[J]. Journal on Communications，2010，31(8A)：87-93.

[5]李向东，陈莉，王清贤. 离线公平交换协议的子协议分析[J]. 计算机工程，2010，36(3)：7-12.
Li Xiangdong，Chen Li，Wang Qingxian. Analysis of sub-protocol in offline fair exchange protocol[J]. Computer Engineering，2010，36(3)：7-12.

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

[7]俞惠芳，王彩芬，王之仓. 基于椭圆曲线的自认证签密方案[J]. 微计算机信息，2010，26(1-3)：94-95.
Yu Huifang，Wang Caifen，Wang Zhicang. Self-certified signcryption scheme based on elliptic curve[J]. Microcomputer Information，2010，26(1-3)：94-95.

[8]王笑梅，张秋剑. 基于椭圆曲线零知识的 RFID 双向身份认证[J]. 计算机工程与应用，2013，49(15)：97-100.
Wang Xiaomei，Zhang Qiujian. Mutual authentication for RFID based on elliptic curve and zero knowledge[J]. Computer Engineering and Applications，2013，49(15)：97-100.

[9]周克元. 基于椭圆曲线和因子分解双难题的数字签名方案[J]. 计算机科学，2014，41(6A)：366-368.
Zhou Keyuan. Digital signature scheme based on elliptic curve and factoring[J]. Computer Science，2014，41(6A)：366-368.

[10]孙艳宾，谷利泽，孙燕，等. 基于并发签名的公平交易协议的分析与改进[J]. 通信学报，2010，31(9)：146-150.
Sun Yanbin，Gu Lize，Sun Yan，et al. Analysis and improvement of the CS-based fair exchange protocol[J]. Journal on Communications，2010，31(9)：146-150.

（责任编辑：吕文红）