在线金融交易确认框架协议研究*

陈 舜+, 姚 前, 谢 立

(计算机软件新技术国家重点实验室(南京大学),江苏 南京 210093)

A Study of Online Financial Trading Confirmation Scheme

CHEN Shun+, YAO Qian, XIE Li

(State Key Laboratory for Novel Software Technology (Nanjing University), Nanjing 210093, China)

+ Corresponding author: Phn: +86-10-88061289, E-mail: chenshun@csrc.gov.cn

Received 2004-06-24; Accepted 2004-11-04

Chen S, Yao Q, Xie L. A study of online financial trading confirmation scheme. *Journal of Software*, 2005,16(10):1811−1815. DOI: 10.1360/jos161811

Abstract: In order to find a way of fast confirmation for the real time clearance of online financial trading, this paper analyzes the typical online trading process and the security characteristics. Based on the principle of elliptic curves signing, a kind of clear confirmation scheme is proposed, which can confirm the trading result step by step, and finish it once a time at the final clear. This scheme can avoid the complicated PKI system and the one by one confirm process, realize the non-reputation efficiently, keep the proof of signing easily, and make straight through process and online clear and possible.

Key words: elliptic curves cryptography; multisignature; confirmation

摘 要: 为了解决网上金融交易实时清算的快速确认问题,分析了典型的交易过程及安全特性,并基于椭圆曲线签名原理,提出了一种基于双线性映射的清算确认框架协议,使得对交易结果的确认可以递进进行,并在最终清算时一次完成,有效地实现了不可否认性和证据留存,避免了复杂的 PKI 体系和两两确认的繁琐过程,使真正的直通式处理和在线清算成为可能.

关键词: 椭圆曲线加密;多方签名;确认

中图法分类号: TP301 文献标识码: A

全球金融市场是高度一体化的,无论是外汇市场、证券市场,还是衍生品市场,每天都进行着成千上万亿美元的交易.在传统的技术条件下,这些高度一体化的金融市场都是封闭系统,参与者必须拥有专用终端(如外汇交易的 SWIFT 系统),通过专用线路,使用专有协议(如金融交易中的 FIX 协议),才能接入交易中心,由主机进行买卖配对.随着互联网技术的普及,很多金融交易已经可以通过网络完成.相比于传统的专用系统,网上金融成本低,随时随地接入,不再受时空限制,效率得以极大地提高.

* Supported by the Key Science-Technology Project of the National 'Ten Five-Year-Plan' of China under Grant No.2001BA102A04 (国家"十五"重点科技攻关项目)

作者简介: 陈舜(1964－),男,云南昭通人,博士,主要研究领域为分布式并行计算;姚前(1970－),男,博士生,主要研究领域为信息安全;谢立(1942－),男,教授,博士生导师,CCF 高级会员,主要研究领域为分布式系统,信息安全.

但是,潜在的安全问题极大地阻碍了互联网在金融领域的应用.这是因为,与一般的电子商务相比,金融交易的安全特性大不相同[1].第一,普通电子商务的商品流和资金流是分开的,身份确认、交易确认和支付确认可以分开进行,只要采用适当的付款或结算方式,就可以将安全性提高到可接受的水平,而金融交易本身就是资金的交易,整个交易和结算过程都通过网络完成.第二,金融交易是集中清算的,无论是买方或是卖方,都不知道真正的交易对手方是谁,清算公司或清算银行作为中间人,对于每一笔确认的交易,都必须予以结算和支付,如果确认环节出了问题,清算行就要承担损失.第三,金融交易是大额的,任何一笔交易出现错误,都可能导致清算失败,引发系统性风险.截止到 20 世纪末,仍未找到一种安全、可靠的适用于网上金融交易的清算支付协议[2].

对于网上金融交易的安全,除一般电子商务所要求的机密性以外,最突出的要求一是非否认性,如果非否认性不能保证,无论是恶意攻击,还是故意否认,都会构成严重威胁;而只要非否认性得以保证,每一笔交易都有人负责,传统的法律就仍然适用,各种欺诈行为就能得以有效避免.二是可用性.金融交易是实时的,金融产品的价格瞬间之内就可能发生剧烈的变化,网络的可用性或效率直接影响着投资人的成交价格.成交后,如果清算能够很快完成,资金就可以另作他用,否则就要支付成本.这两条中,非否认性是根本,不满足就难以进行网上交易,但效率也很重要,否则,互联网的优势就体现不出来.例如,我国的 B 股交易,虽然可以通过互联网下单,但清算要第 3 天才能完成,滞后的根本原因之一就是缺乏高效的确认手段.

1 网上金融交易过程分析

网上金融交易不可否认性的实现与一般电子商务也有很大的不同.因为网上金融市场是松散的分布式结构,每一次交易的完成都涉及多个主体及多个环节.以一次买入为例,至少包括以下几步:第 1 步,投资人向经纪商下达买入指令;第 2 步,经纪商向银行查询投资人的支付能力;第 3 步,银行向经纪商确认投资人的支付能力;第 4 步,经纪商将投资人的买入指令传向交易所;第 5 步,交易所将来自不同投资人(或经纪商)的指令按“价格优先、时间优先”的原则撮合成交,将成交结果返回经纪商,同时传向清算所;第 6 步,经纪商请求投资人确认成交结果;第 7 步,投资人向经纪商确认成交结果;第 8 步,投资人向银行下达结算指令;第 9 步,清算所要求经纪商确认成交结果;第 10 步,经纪商向清算所确认成交结果;第 11 步,清算所要求银行确认支付;第 12 步,银行向清算所确认支付;第 13 步,清算所向银行返回清算结果;第 14 步,银行向投资人返回清算结果.整个过程简化成如图 1 所示.

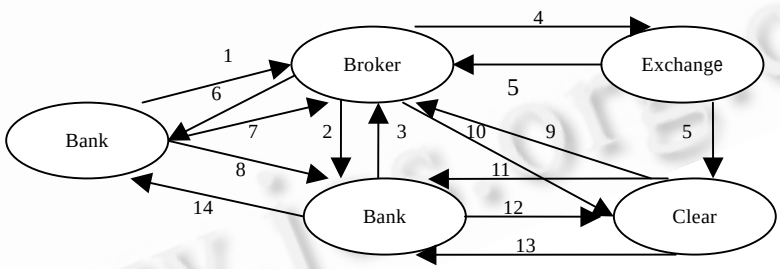

Fig.1 Online financial trading process

图 1 在线金融交易过程

在以上各步中,交易所与清算所之间由于数据量大,一般采用专用通道和协议,其他各步均可由网上实现.到目前为止,确认问题主要还是由相邻主体各自应对,如投资人和经纪商之间是一种解决方案,经纪商和银行之间可能是另一种方案.两个主体之间的确认,可以在 3 个层次实现.一是 IP 层的 IPsec,二是传输层的 SSL,三是应用层的 CA 认证.在我国的网上证券交易系统中,绝大多数是在 SSL 中应用非对称加密实现的[3],也有利用 CA 证书,在应用层实现身份认证的[4].

这种两两确认的过程,难以满足在线交易的效率要求.一是确认环节过多.每一笔交易的完成,从下达交易指令到清算结束,要在主体间进行多次确认,每一个主体要与其他关联主体就同一次交易进行多次重复确认,清算所要同多个主体就成交结果一一确认.二是 IP 层 VPN 及传输层的 SSL,不仅效率低,最主要的是不能跨主体实现,因为一旦实现透明传输,中间节点认证的功能就弱化了.

为了解决两两确认的低效率问题,过去几年业界较为一致的选择是建立行业 PKI,让参与金融交易过程的

每一主体有单一的 CA 证书,经过一次(登录)身份认证后就可以进行若干次交易.正是基于这种计划,银行、证券等行业都在建立 CA 中心.现在看来,这种解决方案存在很大的隐患.一是 CA 并不能提供足够的认证安全性[5];二是要在全球范围内建立高效的 PKI,CA 相互认证十分困难[6];三是在清算环节在线完成如此大规模的认证计算几乎是不可能的.

必须找到一个高效的超越两两确认过程的方法,才能真正解决网上金融交易的清算认证问题.清算确认的目标很简单,即确保成功交收.要保证成功交收,就得有人对该笔交易负责,并且不可否认.从清算所的角度看来,只要得到 3 个主体的确认,就可以有效避免交收风险:一是交易的发起者,二是交易的代理者,三是交易的支付者.也就是说,要实现非否认性,必须进行 3 类确认:一是投资人的身份认证,即对交易结果的认可,并据此承担最终的交收责任;二是经纪商的交易认证,确认该笔交易已经完成,并据此承担连带的交收责任;三是银行的支付认证,承诺按交易结果收付款,并据此承担直接的交收责任.

一是投资人确认买卖的数量,二是银行确认与买卖对应的支付指令,三是经纪人确认成交结果.经过这三者的确认后,清算所就取得了不可否认的证据,一旦违约,各主体将承担相应的交收责任.在本质上,各方确认的核心内容是一致的,都是对成交结果进行签名认证.因此,我们的目标可以简化描述为,找到一个签名方案,让多个主体对同一个信息进行签名,但能分清各自签名的责任,并且能被验证者快速确认.我们的分析框架可简化为如图 2 所示的结构.基于椭圆曲线的多方签名提供了一种很有前景的选择.

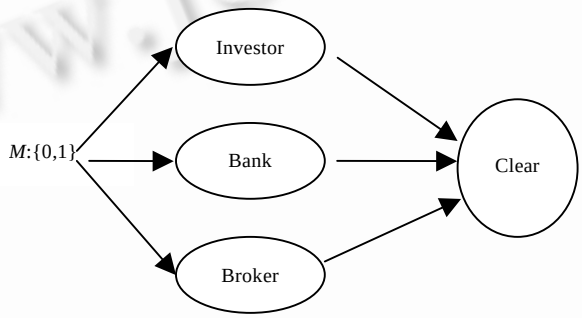

Fig.2 Tri-Parties confirmation of trading result

图 2 对成交结果的三方确认

2 椭圆曲线多方签名原理

在现有的签名方案中,基于椭圆曲线的算法具有明显的效率优势.由于椭圆曲线数据签名算法(ECDSA)已标准化,为叙述简便,我们以此为起点[7].在 ECDSA 中,整个签名过程可简述如下:

生成密钥:签名者 A 选择定义于 Z 上的椭圆曲线 E,$E(Z)$上的点数由大素数 n 可分;选择一个点 $p \in E(Z_p)$,选择一个整数 $d \in [1, n-1]$,计算 $Q = dp$,于是得到 A 的公钥为(E,P,n,Q),私钥为 d.

生成签名:A 拟签名的信息为 m;选择 $k \in [1, n-1]$;计算 $kp = (x, y)$ 和 $r = x \bmod n$,如果 r=0,则重选 k 计算;计算 $k^{-1} \bmod n$;选择 Hash 函数 h,计算 $s = k^{-1}\{h(m) + dr\} \bmod n$;如果 s=0,则重选 k 计算;(r,s)为 A 对消息 m 的签名.

验证签名:计算 $w = s^{-1} \bmod n$,计算 $h(m)$;计算 $u_1 = h(m)w \bmod n$,计算 $u_2 = rw \bmod n$;计算 $u_1P + u_2Q = (x_0, y_0)$,计算 $v = x_0 \bmod n$;如果 $v = r$,则接受签名.

在以上算法中,如果多个主体选择相同的 E,P 和 n,就拥有共同的公钥 Q.只要多个主体拥有相同的公钥,根据椭圆曲线上加法的特性,就可以汇总出某种形式的多方签名,使简化验证成为可能.Popescu 进行了尝试,提出了基于椭园曲线的多方签名方案[8].在此,我们以 Popescu 的方案为基础,描述一种更为简洁的形式.

生成密钥:设有 t 个主体,它们的 P 和 n 相同,第 I 个主体选择 $d_i \in [1, n-1]$,计算 $Q_i = d_i p$,则得到其公钥为 Q_i;根据椭圆曲线上点的加法,计算 $Q = Q_1 + Q_2 + ... + Q_t = dp = (x_Q, y_Q)$,其中 $d = d_1 + d_2 + ... + d_t (\bmod n)$,得到群体的公钥为 Q.

生成多方签名:第 i 个签名者随机选择一个数 $k_i \in [1, n-1]$,计算 $k_i p = (x_i, y_i), 1 \le i \le t$,计算 $r_i = x_i \bmod n$, 如果

$r_i=0$,则重选 k_i 计算,并将 r_i 传给群体中其他签名者,每个签名者独立计算 $r=r_1+r_2+...+r_t(\mathrm{mod}\,n)$;签名者用自己的私钥 (k_i,d_i) 对消息进行签名,$s_i=k_i^{-1}\{h(m)+d_ir\}\,\mathrm{mod}\,n$,每个签名者将 r_i, s_i,传给多方签名的代理,代理者计算 $s=s_1+s_2+...+s_t(\mathrm{mod}\,n)$,$r$ 和 s 为 t 个用户的多方签名.

验证多方签名:计算 $(r^{-1}h(m)\,\mathrm{mod}\,n)Q+(r^{-1}s\,\mathrm{mod}\,n)p=(x_0,y_0)$,如果 $r=x_0(\mathrm{mod}\,n)$,则多方签名有效.

证明:每一个体的签名满足下式:

$$(r^{-1}h(m)\,\mathrm{mod}\,n)Q_i+(r^{-1}s_i\,\mathrm{mod}\,n)p=(x_i,y_i)$$,其中 $1\le i\le t$.

对上式两边从 1~t 相加,有:

$$(r^{-1}h(m)\,\mathrm{mod}\,n)\sum Q_i+(r^{-1}\sum s_i\,\mathrm{mod}\,n)P=(x_0,y_0).$$

根据定义,$Q=\sum Q_i=dp$, $s=s_1+s_2+...+s_t(\mathrm{mod}\,n)$,代入上式,即可得到验证方程.

这里,由于每一个体的签名都是 ECDSA 签名,其安全性与 ECDSA 一样强.但由于多个主体有共同的公钥,对群体签名的验证可以一次完成.

3 金融交易清算确认框架

根据图 2,我们的问题是,要求投资人、经纪商和银行对同一个信息(成交结果)进行签名,并能让清算行快速确认.按照第 2 节描述的原理,设 P 为全局变量,即为公钥的一部分,整个方案如下:

密钥生成:投资人随机选择 $k_1\in[1,n-1]$, $d_1\in[1,n-1]$,计算 $Q_1=k_1p=(x_1,y_1)$,计算 $r_1=x_1\,\mathrm{mod}\,n$,如果 $r_1=0$,则重选 k_1 计算;银行随机选择 $k_2\in[1,n-1]$, $d_2\in[1,n-1]$,计算 $Q_2=k_2p=(x_2,y_2)$,计算 $r_2=x_2\,\mathrm{mod}\,n$,如果 $r_2=0$,则重选 k_2 计算;经纪商随机选择 $k_3\in[1,n-1]$, $d_3\in[1,n-1]$,计算 $Q_3=k_3p=(x_3,y_3)$,计算 $r_3=x_3\,\mathrm{mod}\,n$,如果 $r_3=0$,则重选 k_3 计算;各自将已方计算的 r 值传给另两方.根据前面的定义,(k_1,d_1), (k_2,d_2), (k_3,d_3) 分别为投资人、银行为经纪商的私钥.

生成个体签名.各方独立计算 $r_{123}=r_1+r_2+r_3(\mathrm{mod}\,n)$,投资人用 (k_1,d_1) 对成交结果 (m) 进行签名,得到 $s_1=k_1^{-1}\{h(m)+d_1r_{123}\}\,\mathrm{mod}\,n$,将 s_1 传给银行和经纪商.银行验证投资人的签名,验证方法与 ECDSA 相同;验证通过后,用 (k_2,d_2) 对成交结果进行签名,得 $s_2=k_2^{-1}\{h(m)+d_2r_{123}\}\,\mathrm{mod}\,n$,将 s_2 传给经纪商;经纪商验证投资人和银行签名,验证方法与 ECDSA 相同;验证通过后,用 (k_3,d_3) 对成交结果进行签名,得到 $s_3=k_3^{-1}\{h(m)+d_3r_{123}\}\,\mathrm{mod}\,n$.

生成多方签名.经纪商计算 $s_{123}=s_1+s_2+s_3(\mathrm{mod}\,n)$ 得出多方签名,计算 $Q=Q_1+Q_2+Q_3=dp$,为群体的公钥,其中 $d=d_1+d_2+d_3(\mathrm{mod}\,n)$.将 (r_{123},s_{123}) 和 Q 传给清算所.

清算所确认.清算所有了 r_{123}, s_{123}, Q,全局变量 P 以及从交易所收到的 m,计算 $(r_{123}^{-1}h(m)\,\mathrm{mod}\,n)Q+(r_{123}^{-1}s_{123}\,\mathrm{mod}\,n)p=(x_0,y_0)$,如果 $r_{123}=x_0(\mathrm{mod}\,n)$,则多方签名有效,予以清算,否则,拒绝清算.整个确认框架协议如图 3 所示.

以上方案较好地解决了前面提出的要求.第 1,在不可否认方面,基于椭圆曲线离散对数困难问题,利用 ECDSA 协议框架,实现了不可否认的签名.第 2,在效率方面,一是避免了两两认证,对一次交易,每一主体只认证一次,计算过程大大简化;二是相对于 RSA 体系,椭圆曲线签名长度本来就小,计算速度快得多;三是多方签名的长度与单一签名一样长,对每笔交易清算行也只计算一次,而且很多变量,如 Q,P 等可以预置,极大地提高了计算速度.第 3,每一个体都是自主选择私钥,避免了复杂的 PKI 体系结构,也避免了复杂的密钥管理和分配问题.第 4,经过投资人到银行、银行到经纪商、经纪商到清算行的层层认证,不仅完成了确认,也留下了有效证据,为事后的追查奠定了基础,保证了传统法律的有效性.

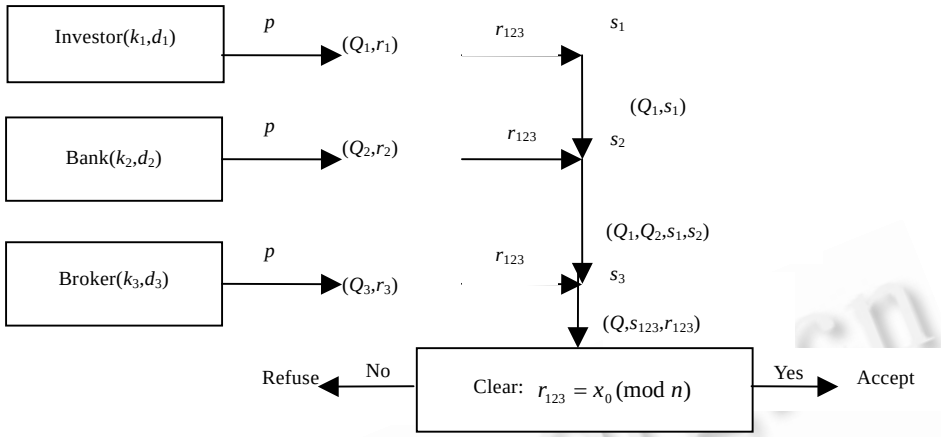

Fig.3 Online clear confirmation scheme

图 3 在线清算确认框架协议

4 结束语

本文的分析表明,网上金融交易的安全特性,集中体现于清算环节的不可否认性及可用性.针对这种安全需求,我们提出了一种基于椭圆曲线多方签名的清算确认协议框架,用递进认证代替两两认证,用自主选择私钥代替密钥分配,极大地提高了确认效率,避免了复杂的 PKI 体系,使业界一直向往的网上金融交易的实时清算成为可能.

References:

[1] Chen S. The security characteristics of securities online business. Financial Computer of China, 2003,(12):61−63 (in Chinese with English abstract).

[2] Jakobsson M, Mraihi D, Tsiounis Y, Yung M. Electronic payments: Where do we go from here? In: Baumgart R, ed. LNCS 1740. Berlin: Springer-Verlag, 1999. 43−63.

[3] Zou BQ. Use SSL technology realizing broker online trading. China Securities Information Technology, 2002,(6):32−34 (in Chinese with English abstract).

[4] Jiang T, Wu P, Xu ZW. Online trading security system based on PMI technology. China Securities Information Technology, 2002,(4):48−51 (in Chinese with English abstract).

[5] Ellison C, Schneier B. Ten risks of PKI: What you are not being told about public key infrastructure. Computer Security Journal, 2000,XVI(11):1−8.

[6] Nash A, Duane W, Joseph C, Brink D, Wirte; Zhang YQ, Chen JQ, Yang B, Xue W, *et al*., Trans. PKI implementing and managing E-Security. Beijing: Tsinghua University Press, 2001. 250−252 (in Chinese).

[7] American National Standard. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA). ANS X9.62-1998, Washington: American Bankers Association, 1998. 14−18.

[8] Popescu C. A digital multisignature scheme with distinguished signing responsibilities. Studies in Informatics and Control, 2003,12(3):227−231.

附中文参考文献:

[1] 陈舜.证券电子商务的安全特性.中国金融电脑,2003,(12):61−63.

[3] 邹彬琦.应用 SSL 技术实现证券公司网上交易.中国证券信息技术,2002,(6):32−34.

[4] 蒋韬,伍评,徐正文.基于 PMI 技术建立网上交易安全系统.中国证券信息技术,2002,(4):48−51.

[6] Nash A,Duane W, Joseph C, Brink D,著;张玉清,陈建奇,杨波,薛伟,等,译.公钥基础设施(PKI):实现和管理电子安全.北京:清华大学出版社,2001.250−252.