一种基于双线性映射累积签名的递进清算认证协议*)

陈 舜 姚 前 谢 立
(南京大学计算机科学与技术系 南京 210008)

摘 要 本文基于双线性映射群,提出了一种全程累进签名方案,可有效解决网上证券交易和清算的多方认证问题,简化了认证过程,实现了全程认证,不需要可信第三方,避免了复杂的PKI体系,大大提高了计算效率。

关键词 双线性映射,累积签名,清算协议

An Incremental Clearing Authentication Protocol Based on Bilinear Map Aggregate Signature

CHEN Shun YAO Qian XIE Li
(Department of Computer Science and Technology, Nanjin Uniersity, Nanjin 210008)

Abstract This paper proposes a clearing authentication scheme based on the bilinear map group. The scheme is a kind of incremental aggregate signature protocol, provides a solution to the identify problem of online securities trading and clearing, realizes straight through processing without complex PKI and trusted third party, simplifies the identify procedure and enhances the computational efficiency.

Keywords Bilinear map, Aggregate signature, Clearing protocol

网上证券交易以其成本低、效率高的优势快速发展,已成为各国金融市场的主要交易手段。与一般电子商务不同的是,网上证券交易实时进行,涉及金额巨大,参与人数众多,安全问题尤其突出,并集中于清算环节[1]。

1 引言

在一般模式下,网上证券交易涉及多个主体,可简化为如图1所示。投资人通过券商下达买卖指令,通过银行划转资金,交易所负责买单和卖单的撮合,结算机构负责钱券的易手,托管机构负责资产保管。在传统的技术条件下,图1是一个封闭系统,安全问题并不突出。但现在,除了交易所、结算所和清算银行之间仍然主要由专线相连外,其他通讯过程大都开始走向公网,如图中虚线所示。

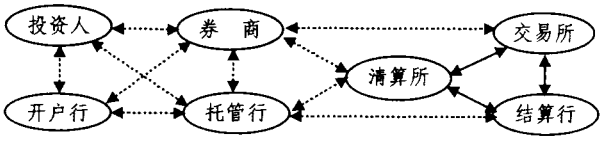

图1 网上证券交易的参与主体

通过网上完成一次证券交易,至少要经过以下主要步骤:通过相互认证后,投资人向券商提交买卖申请;券商经确认后,将买卖申请转发交易所;交易所将成交结果返回券商,同时传至结算所和清算行;券商将成交结果返回投资人,并通知托管行;投资人确认买卖无误后通知开户行;托管行确认钱券的对应关系无误后通知开户行划款;结算行根据清算结果通知托管行划付资金;清算所根据交易和确认结果进行清算。就一次交易而言,清算是处于后台的核心环节,每一步产生的错误,都会在此体现出来;就全天的交易而言,清算是集中进行的,只要一笔出错,就可能导致所有交易不能顺利清算。当受到恶意攻击时,不论发生在哪个环节,都会体现到清算上来,轻则导致券商或清算行的损失,重则引发系统性危机。因此,清算环节的安全,成为整个证券电子商务的瓶颈所在。

在现在的技术条件下,网上交易的安全性、完整性、可用性及身份识别等方面都存在相当的隐患,但从清算环节来看,最为重要的是交易认证或身份识别。每一笔交易及其结果,只要经过投资人、券商和银行三方的确认后,投资人就要负最终的交收责任,券商要负交收的连带责任,银行要负收付款的直接责任,这笔交易就是安全的。相反,如果任何一笔交易未经三方同时确认,就不应进入清算环节,否则就有风险。确认的效率对网上证券交易的安全和效率起着决定性的作用。

目前的确认方法存在两大缺陷。一是只能是两两确认,如投资人与券商确认,券商与银行确认,清算行与券商确认,等等。这样,针对每一笔交易,每一个主体必须完成多次确认,清算行要与各主体一一确认,确认环节过多和多次重复确认,严重影响了效率[2]。二是两两确认的方法,主要是基于IP层的VPN[3],以及传输层的SSL[4],绝大多数都需要PKI的支持,这不仅不能保证认证的安全性,让清算行对成千上万的交易进行同时认证也是不可能的。因此,如何找到一个高效的交易确认协议,成为解决清算安全的当务之急。双线性累积签名为此提供了一种可能。

2 双线性配对累积签名原理

采用RSA等经典签名方案,也可完成身份的确认,但由于效率太低,严重影响可用性,在实践中无法普及。这是因为,在每一笔交易中,都要验证若干主体,对于像证券交易这

*)Supported by the National 10.5 Plan Grand Science and Technloy Program(国家十五重大科技攻关项目;金融示范工程(200102A04))。陈 舜 博士生,主要研究领域为分布式系统,信息安全;姚 前 博士生,主要研究领域为信息安全;谢 立 教授,博士生导师,主要研究领域为分布式系统,并行计算,信息安全。

样的大规模复杂系统而言，PKI的布置十分困难，集中验证的计算时间也难以接受。

Dan Boneh 等人提出了一种累积签名方案[6]。在这种方案下，不同用户的签名可以累积在一起，形成一个总的签名，长度与单个签名相同，验证者只需计算一次，就可以验证所有签名的有效性。其基本原理如下。

定义 设 G 是一个双线性配对群，其素阶为 p，生成元为 g，则 G 上存在双线性配对 $e:G\times G\to G_T$，G_T 是也是素阶为 p 的循环群。对于 $u,v\in G$，e 具有以下性质：一是对于计算 $e(u,v)$，存在一个有效的计算方法；二是具有双线性，对于 $a,b\in Z_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$；三是不退化，$e(g,g)\neq 1$。G 是一个双线性群，也就同时拥有了 GDH(Gap Deffie-Hellman)群的特性，使得 CDH(computational Diffie-Hellman)问题同离散对数一样困难，而 DDH(Decision Diffie-Hellman)问题则较为容易[7]。

累积签名：设有 n 个用户，第 i 个的私钥为 $x_i\in z_p$，公钥为 $v_i=g^{x_i}$，对信息 $M_i\in\{0,1\}$ 进行确认后，先进行一次散列运算，$h_i\leftarrow H(M_i)$，$h_i\in G$ 再用私钥完成签名 σ_i，任一合成者(可以是一个签名方，也可以是系统外的第三方)计算 $\sigma\leftarrow\prod_{i=1}^{n}\sigma_i$，$\sigma\in G$ 就是累积签名。

签名验证：验证者拥有累积签名计 σ，每个用户的公钥 V_i，原始信息 $M_i\in\{0,1\}^*$，对 $1\leqslant i\leqslant n$，计算 $h_i\leftarrow H(v_i,M_i)$，如果 $e(\sigma,g)=\prod_{i=1}^{n}e(h_i,v_i)$，则所有签名的有效性同时得以验证，否则拒绝。

有效性证明：由于双线性特征的存在，可以很容易证明验证公式成立，因为：

$$e(\sigma,g)=e(\prod_i h_i^{x_i},g)=e(\prod_i h_i,g)^{x_i}=e(\prod_i h_i,g^{x_i})$$
$$=e(\prod_i h_i,v_i)$$

安全性证明：由于 G 为 GDH 群，虽然 DDH 问题相对容易，并且在验证过程中得以使用，但 CDH 问题仍然困难，以上计算过程并没有降低 CDH 的难度。在 D. Boneh 等人发表的文章中，已对基于以上原理的累积签名安全性进行了证明[8]。其基本结论是，当不同的用户对不同的信息进行签名时，使用以上原理设计的签名安全性同基于离散对数的协议一样安全。

3 一种全程递进认证方案

基于双线性累积签名的原理，我们提出一种签名方案，可用于网上证券交易清算的身份认证。从清算所的角度来看，在进行交收之前，只要得到三个主体的确认，就不会导致系统性风险。一是投资人确认买卖指令，二是开户行确认付款指令，三是券商确认交易指令。虽然这三者之间在确认之前还要通过各种方式予以认证，与其他主体之间也还存在多种形式的相互认证，但只要清算所得到以上三种确认，就可以基本排除恶意攻击者下达的买卖报单，就可以确信每一笔交收都能找到最终的责任人。为简化表述，假定投资者下达买卖指令为第一步，开户行承诺付款为第二步，券商完成交易为第三步，分别用下标 1、2、3 表示。

投资者签名：投资者任意选择 $x1\leftarrow Z_p$ 为私钥，计算出 $v1\leftarrow g^{x1}$ 为公钥，对买卖指令 $M1\in\{0,1\}^*$，计算 $h\leftarrow H(M1)$，$h\in G$，对散列结果进行签名 $\sigma1\leftarrow h^{x1}$，得到 $\sigma1\in G$。

开户行验证和签名：开户行首先验证投资者签名，计算 $h\leftarrow H(v1,M1)$，如果 $e(\sigma1,g)=e(h,v1)$，则投资者买卖指令得以确认。在对投资者的买卖指令予以确认后，开户行就应承诺付款，用自己的私钥对付款指令进行签名。开户行任意选择 $x2\leftarrow Z_p$ 为私钥，计算出 $v2\leftarrow g^{x2}$ 为公钥，先对付款指令 $M2\in\{0,1\}^*$，计算 $h\leftarrow H(M2)$，$h\in G$，再对散列结果进行签名 $\sigma2\leftarrow h^{x2}$，得到签名 $\sigma2\in G$。第三步是生成累积签名。计算 $\sigma12\leftarrow\sigma1\sigma2$，得到累积签名 $\sigma12\in G$。

券商验证和签名：首先验证投资者买卖指令和开户行付款指令，对 v_i 和 M_i，计算 $h_i\leftarrow H(v_i,M_i)$，其中 $i=1,2$，如果 $e(\sigma12,g)=\prod_{i=1}^{2}e(h_i,v_i)$，则投资人的买卖指令和开户行的付款指令得以同时确认，将买卖指令传往交易所进行交易撮合。按我国现行法律，一旦成交就不可撤消，这一步的验证非常重要。当交易所返回成交情况后，券商必须及时返回投资人和开户行，同时对成交结果予以确认，以作为清算的基础。任意选择 $x3\leftarrow Z_p$ 为私钥，计算出 $v3\leftarrow g^{x3}$ 为公钥，对成交结果 $M3\in\{0,1\}^*$，计算 $h\leftarrow H(M3)$，$h\in G$，再对散列结果进行签名 $\sigma3\leftarrow h^{x3}$，得到 $\sigma3\in G$。最后才是累积签名，计算 $\sigma123\leftarrow\sigma1\sigma2\sigma3$，得到 $\sigma123\in G$。

清算行验证：清算行收到签名后，对 v_i 和 M_i，计算 $h_i\leftarrow H(v_i,M_i)$，$i=1,2,3$，如果 $e(\sigma123,g)=\prod_{i=1}^{3}e(h_i,v_i)$，则对三个主体的指令得以同时确认，此单可进入清算过程。

在以上方案中，各主体只对自己确认和承诺的信息进行签名，确保了签名信息之间的差异性，符合 D. Boneh 等人提出的要求，也就保证了其安全性。

在以上方案中，如何选择具有双线特征的 G 成为应用的关键，A. Joux 和 K. Nguyen 已成功解决了这一问题。

4 全程递进认证方案的优越性

在金融证券交易中，如何利用非对称加密技术，是一个普遍困难的问题。由于交易金额大，现已提出的各类支付协议，如电子钱包、电子支票、电子货币等方案均难以应用[10]。即便专门为信用卡支付而开发的 SET 协议，也因为过于复杂，成本太大，未曾普及，而且也难以用于金融交易领域。全程递进认证方案在一定程度上克服了上述缺陷。

第一，避免了复杂的 PKI 体系。在金融和证券交易中，为了应用基于非对称密钥的加密和签名技术，业界一直致力于构建专用的 CA 中心或 PKI 体系。但由于用户数量太大，单我国境内的投资人就超过 7000 万，加上不同主体需求不同，安全要求不同，要设计出一个具有普遍用途的 PKI 系统看来非常困难。这里提出的方案并不要求统一的 PKI 体系，只要清算会员按统一标准提供公钥即可，而各级签名方案可自主形成。

第二，简化了签名确认过程。在网上交易中，身份认证是一个必要的前提。如投资人与券商之间，投资人与开户行之间，开户行与券商之间，等等。在现阶段的应用中，已有的方案都只提供两两认证，还没有找到全程认证的方法。这里提出的累积方案，同时也是一个层级认证过程。随着交易的进行，认证层次增加，安全性逐步提高。由于后一主体必须产生累积签名以作为下一阶段的认证条件，每一阶段的认证都对前面的主体进行了认证，最后的清算环节对所有主体进行一次认证，避免了重复繁杂的两两独立认证。

第三，提供了全程认证，且不需要可信第三方。与一般电子商务不同，证券交易涉及金额大，主体身份认证的主要目的，不仅是保证数据机密性和完整性的需要，更是为提供有效的法律证据，为事后的追查和审计提供基础，从而保证传统的

(下转第 118 页)

与度量集合相关联，保证了用户分析时对度量数据进行的各种汇总操作。同时本文参考多维数据库模型定义了支持复杂维结构的两个 OLAP 扩展操作：度量到维转化操作和维到度量转化操作，进而丰富了 OLAP 分析功能。

可以说，本文提出了一套较为完整的 OLAP 多维数据模型和立方体代数操作集合，具有很强的实用价值。

下一步工作是在此基础上对物化视图策略进行深入研究和分析，开发动态物化视图管理系统，并在此基础上制定一套基于物化视图集合的查询重定向机制，从而能够提高 OLAP 分析的响应效率。

参 考 文 献

1 Inmon W H. Building the Data Warehouse. 2nd edition. New-York: John Wiley and Sons, 2000

2 Codd E F, Codd S B, Salley C T. Providing OLAP to User-Analysts: An IT Mandate. White Paper. Arbor Software Corporation, 1993

3 Harinarayan V, Rajaraman A, Ullman J D. Implementing data cubes efficiently. In: Proc. of the 1996 ACM SIGMOD Intl. Conf. on Management of Data, Montreal, Canada, 1996

4 OLAP Council. The OLAP glossary. The OLAP Council, 1997. http://www.olapcouncil.org/research/glossary.htm

5 Pourabbas E, Rafanelli M. Characterization of Hierach- ies and Some Operators in OLAP Environment. In: Proc. of ACM Second Intl. Workshop on Data Warehousing and OLAP, Kansas City, 1999

6 Abelló A, Samos J, Saltor F. Understanding Analysis Dimensions in a Multidimensional Object-Oriented Model. In: Proc. of the 3rd Intl. Workshop on Design and Management of Data Warehouses, Interlaken Switzerlan, 2001

7 Gray J, Bosworth A, Layman A, Pirahesh H. Data cube: A relational aggregation operator generalizing group-by, cross-tabs and subtotals. In: Proc. f the 12th Intl. Conf. on Data Engineering, New Orleans, Louisiana, 1996

8 李建中，高宏. 一种数据仓库的多维数据模型. 软件学报，2000，11(7)：908～917

9 裴健，柴玮，赵畅，等. 联机分析处理数据立方体代数. 软件学报，1999，10 (6)：561～569

10 Nguyen T B, Tjoa A M, Wagner R. An Object Oriented Multidimensional Data Model for OLAP. In: Proc. of the 1st Intl. Conf. on Web-Age Information Management. Heidelberg, Berlin, 2000

11 Baralis E, Paraboschi S, Teniente E. Materialized View Selection in a Multidimensional Database. In: Proc. of the 23rd Intl. Conf. on Very Large Data Bases, San Fransisco, CA, 1997

12 Gupta H, Mumick I S. Selection of Views to Materialize Under a Maintenance Cost Constraint. In: Proc. of the 7th Intl. Conf. on Database Theory. Heidelberg, Berlin, 1998

13 Han Jia-wei, Micheline K. 数据挖掘概念与技术(影印版). 北京：高等教育出版社，2001. 182～194

14 Pedersen T B, Jensen C S, Dyreson C E. A foundation for capturing and querying complex multidimension-al data. Information System, 2001, 26(5): 383～423

15 Jensen C S, Kligys A, et al. Multidimensional data modeling for location-based services. In: Proc. of the 10th ACM Intl. symposium on Advances in GIS. New York: USA, 2002

(上接第 71 页)

法律监管有效，为各种欺诈和恶意侵害提供最终的制裁和追讨手段。在目前两两认证的条件下，最大的困难在于如何设置可信第三方，以保证签名和认证的过程留下可信的证据，也就是形成所谓的公平签名。在我们的方案中，签名是层次递进的，开户行签名的前提是收到并认可投资人的指令，券商签名的前提是收到并且确认前二者的指令，当通过清算验证后，前三者的签名都可作为有效证据。由于清算所是最后一个环节，它自己不可能形成交易单据，它也不能从制造虚假交易中获取不当利益，将所有证据保存在这一环节是可信的。这样，非否认性这一网上证券交易中最重要的问题，在本文提出的方案中得以有效解决。

第四，提高了计算效率。目前的非对称加密和认证方案中，几乎全都依赖于 CA 证书，在 SSL 层实现认证和安全传输，这就只能对整个交易报文全部进行加密计算，从而不可避免地增加了成本，影响了可用性，也是不能由两两认证过渡到全程认证的主要障碍。在本文提出的方案中，各主体只对自己承诺的部分进行签名，不仅分清了责任，也简化了计算。在 XML 日益成为报文标准的环境中，这就更为容易实现。由于签名是基于椭圆曲线的，在相同的安全水平下，签名长度要小得多，大大节约了计算资源，使得利用移动设备完成在线交易成为可能。当清算所进行验证的时候，其计算时间与主体数呈线性关系，并没有因此增加复杂性。可以进一步证明，当清算所为密钥管理中心时，验证时间会进一步下降。

参 考 文 献

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

2 天威诚信电子商务. 网上证券交易安全需求分析. 中国证券信息技术，2002(12)：29～31

3 Winbom H, Jones R P. Member Access via VPN, OM White Paper, March, 2003

4 邹彬琦. 利用 SSL 技术实现证券公司网上交易. 中国证券信息技术，2002(12)：32～34

5 Ellison C, Schneier B. Ten risks of PKI: What you are not being told about Public Key Infrastructure. Computer Security Journal, 2000, XVII(1)

6 Boneh D, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: E. Biham, ed. Proc. of Eurocrypt 2003, volume 2656 of LNCS, Springer-Verlag, 2003. 416～432

7 Boldyreva A. Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature. In: Y. Desmedt, ed. Proc. of PKC 2003, volume 2567 of LNCS, Springer-Verlag, 2003. 31～46

8 Boneh D, Gentry C, Lynn B, Shacham H. A survey of Two Signature Aggregation Techinques. RSA Laboratories, 2003, 6(2)

9 Joux A, Nguyen K. Separating decision Diffie-Hellman from Diffie-Hellman in Cryptographic groups. Cryptology ePring Archive: [Report 2001/003]. 2001. http://eprint.iacr.org/.

10 Jakobsson M, Mraihi D, Tsiounis Y, Yung M. Electronic Payments: Where Do We Go From Here? In: R. Baumgart, ed. LNCS 1740. Springer-Verlag, 1999. 43～63