一种基于票据的新型微支付方案*)

程文青[1] 郎为民[1,2] 杨宗凯[1] 谭运猛[1]

(华中科技大学电子与信息工程系 武汉430074)[1] (中国国家信息安全测评中心 北京100091)[2]

摘 要 本文提出了一种基于票据的新型高效微支付方案,它采用票据许可生产的模式,由商家授权经纪人生成商家票据,并由商家在线验证票据的合法性。同时,该方案使用会话密钥对交易信息进行加密,大大地提升了安全性等级,票据标识的唯一性又能够有效防止消费者的重复花费。与其它微支付方案相比,由于本方案完全没有使用公开密钥算法,且协议执行中所需保存的信息比较简单,因而系统的计算开销和存储开销大大减少。此外,本方案支持数字货币的可分性和可转移性。

关键词 微支付,票据,Subscrip,可分性

A New Micropayment Scheme Based on Scrip

CHENG Wen-Qing[1] LANG Wei-Min[1,2] YANG Zong-Kai[1] TAN Yun-Meng[1]

(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)[1]

(China National Information Security Testing Evaluation and Certification Center, Beijing 100091)[2]

Abstract This paper proposes a new efficient micropayment scheme based on scrip, where a merchant can authorize the broker via licensed scrip production to produce vendor scrip the vendor validates and accepts on-line during payment. Moreover, all the information with regard to payment is encrypted using a shared symmetric key, which improves the security standard of our scheme and it can prevent the consumer from double spending because the identifier of the scrip is unique. Compared with other micropayment schemes in existence, no public-key operation is required and the information stored is very simple, which minimizes the computation and storage overhead dramatically. In addition, our scheme supports divisibility and transferability of digital coins in a simpler way.

Keywords Micropayment, Scrip, Subscrip, Divisibility

1 引言

微支付[2~5]作为数字货币的一种支付形式,是目前电子支付发展的一个新方向,它能够较好地满足信息商品或服务的需求。与大额支付相比,它的每一笔交易额非常低,在满足安全性的前提下要求系统简单高效。票据(Scrip)是微支付系统中最为常见的支付工具之一,它是一种面值很小的数字货币,一般由商家或经纪人产生,也可以由经纪人独立产生。在不需要第三方参与的情况下,可以由商家在线验证数字货币的合法性。采用票据作为支付工具的微支付系统一般不使用公钥加密技术,而使用对称密钥加密技术或散列算法。目前比较典型的基于票据的微支付系统主要是 SubScrip[1]等。但 SubScrip 在交易过程中,票据是以明文的形式进行传送的,消费者和商家的交互信息也没有采用加密和散列算法,所以攻击者可以窃取交易信息(如购买商品的种类和交易额等),商家数据库中消费者所持商家票据的余额也可以由商家返回的新票据得到,因而系统没有提供机密性保护。

本文提出了一种新的基于票据的微支付方案,它采用票据许可生产的模式,由商家授权经纪人生成商家票据,并由商家在线验证票据的合法性。它是一种预支付方案,支持数字货币的可转移性和可分性,且使用会话密钥对交易信息进行了加密,方案的安全性较高。与其它微支付方案相比,其显著特征就是本方案完全没有使用公开密钥算法,因而其效率比较高,适用于短期内消费者与同一商家的重复交易。

本文第2节描述我们所提出的基于票据的新型微支付方案;第3节详细分析了系统的有关性能;最后对全文进行总结。

2 基本模型和协议

本文所提出的微支付方案涉及到交易的三方:消费者 C(Customer)、商家 M(Merchant)和经纪人 B(Broker)。其中,消费者 C 是使用数字货币购买信息商品或服务的主体,商家 M 是为消费者提供商品或服务并接受消费者支付的网上商店,经纪人 B 在方案中相当于经纪人的角色,它作为消费者和商家之间的中介,能够为消费者和商家开立并维护账户、认证交易双方的身份、进行货币销售和交易结算,并协调解决可能引起的争端,其基本的支付模型如图1所示。

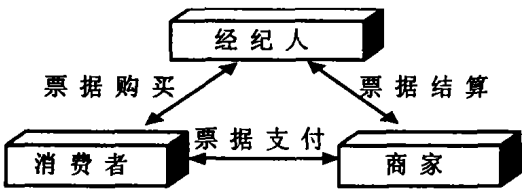

图1 基于票据的微支付模型

2.1 开户协议

消费者选择一个经纪人可以接受的宏支付系统,并与经

*)基金项目:国家自然科学基金项目(90104033)。程文青 副教授,研究方向为网络安全和下一代互联网。郎为民 博士研究生,讲师,研究方向为信息安全、应用密码学和电子商务。杨宗凯 教授,博士生导师,主要研究领域为现代信息网络理论及应用、远程教育、信息安全。谭运猛 博士,副教授,主要研究方向为电子支付、信息安全和应用密码学。

纪人进行能够满足大额支付要求的交易，在经纪人处开立一个账户，且存入一定数额的现金。同时，消费者与经纪人共享一个秘密密钥 K_{CB}。商家在经纪人处开立账户的过程与消费者类似，他与经纪人也共享一个秘密密钥 K_{MB}。

2.2 授权协议

在本方案中，商家可以授权经纪人来生成商家票据，且商家能够验证和接收经纪人生成的票据。

(1)商家发送一个授权指令给经纪人，该指令包括主票据密钥 K_S、主消费者密钥 K_C、票据标识 ID_S 和消费者标识 ID_C 等信息，授权指令的格式如下：

$(K_S, K_C, ID_S, ID_C)_{K_{MB}}$

(2)经纪人生成商家票据，将产生的全部票据标识值发送给商家，并通过销售从消费者处获益；

(3)商家记录其授权经纪人产生的全部票据标识值，并可以通过使用不同的序列和密钥将票据生成权授予不同的经纪人。

2.3 票据购买协议

在本方案中，为使消费者可以通过账户进行微支付交易，经纪人需返回一个商家票据给消费者，使其具备一定的支付能力。

(1)消费者生成一个票据购买请求并将其发送给经纪人，该请求包括商家标识 ID_M、消费者标识 ID_C 和票据面额 V_S 等信息，其格式如下：

$(ID_M, ID_C, V_S)_{K_{CB}}$

(2)经纪人将根据消费者标识产生一个主消费者密钥 K_C，对票据中消费者标识与某个主消费者密钥进行散列运算，即可得到消费者密钥 K_{CM}，其产生过程如图2所示。

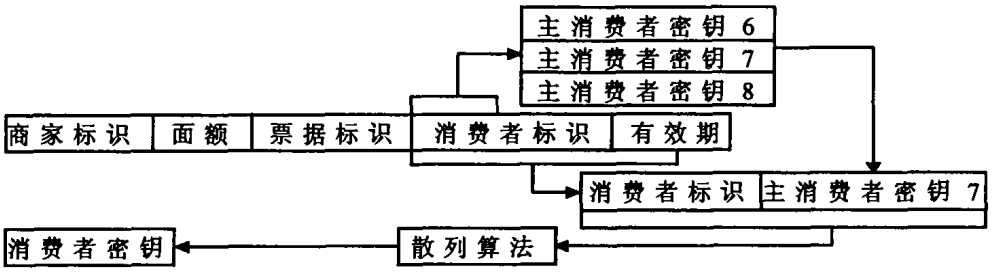

图2 消费者密钥产生过程示意图

(3)经纪人将带有消费者密钥 K_{CM} 的商家票据使用会话密钥 K_{CB} 加密后，返回给消费者，即票据购买响应格式为

$(S, K_{CM})_{K_{CB}}$

同时，从消费者账户上扣除与票据价值相当的资金。图3给出了票据中所包含的域，每个数据域代表的意义详述如下：

商家标识(ID_M)：标识出了票据使用有效的商家名称。

面额(V_S)：给出了票据的价值。

票据标识(ID_S)：它是唯一的，其作用有些类似于序列号，用于防止重复花费，它的一部分用来选择生成证书的主票据密钥。

消费者标识(ID_C)：一个用来产生消费者密钥 K_{CM} 的标识符，消费者密钥可用于防止票据的非法使用。消费者标识不需要与消费者的真实身份有任何联系，但它必须是唯一的，它的一部分用于选择产生主消费者密钥。

有效期(E_S)：标识了票据的过期时间，即票据能够使用的最后期限，到期票据将会失效。

证书(C_S)：它可以防止票据被以任何形式进行修改并证实它是合法的(没有进行重复花费)。从这个意义上说，它是票据的数字签名，尽管它不是通过公钥加密算法生成和认证的。证书可以通过使用密钥对票据的其他域进行散列运算得出。商家为产生票据，需要维护一个从1到 N 的主票据密钥列表。究竟使用哪个主票据密钥取决于票据标识的内容，如果票据标识的最后一位数字是4，则使用主票据密钥4产生证书。

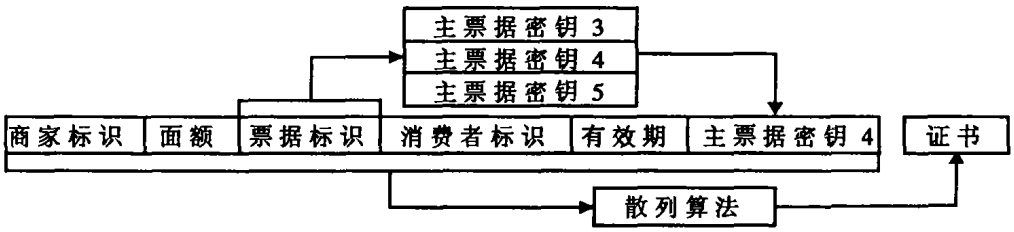

图3 票据结构示意图

2.4 支付协议

(1)消费者向商家发送支付指令，该指令包括商家标识 ID_M、订单信息 OI(包含购买商品或服务的种类、数量和总金额等信息)和票据 S 等信息，其格式如下：

$(ID_M, OI, S)_{K_{CM}}$

同时将消费者标识 ID_C 告知商家。

(2)商家根据消费者标识 ID_C 计算出消费者密钥 K_{CM}，用它来解密支付指令。

(3)商家验证票据合法性。

票据合法须具备两个条件：它是由商家产生的，且没有进行重复花费。商家对票据的验证可分为两步。首先，商家使用票据对证书进行重新计算，并同消费者发送过来的票据证书进行比较，如图4所示。如果票据被修改或破坏的话，两个证书将不会匹配；其次，商家通过遍历其数据库，检查票据标识 ID_S 是否已经被记录，以判断该票据是否进行了重复花费。

(3)若票据合法，则商家为消费者提供商品或服务，并返回一个支付响应，包括消费者标识 ID_C、商家的标识 ID_M、具有新面值的票据 S' 等信息，其格式如下：

$(ID_C, ID_M, S')_{K_{CM}}$

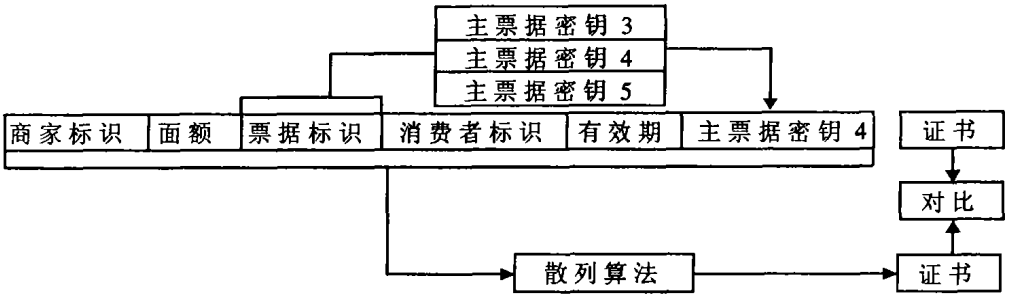

图4 票据合法性验证示意图

2.5 存款协议

当商家票据被消费者在有效期花费完毕后，则商家通过执行如下存款协议与经纪人进行资金转账：

(1)商家发送一个存款请求给经纪人，包括消费者标识 ID_C、商家的标识 ID_M、原始票据的标识 ID_S、面额 V_S 和票据有效期 E_S 等信息，其格式如下：

$(ID_C, ID_M, ID_S, V_S, E_S)_{K_{MB}}$

(2)经纪人通过遍历数据库来验证存款请求的合法性，若通过，则经纪人将与票据价值相当的资金转移到商家的账户上。

3 系统性能分析

3.1 可转移性

在本文提出的微支付方案中，票据是可以转移的。消费者可将商家票据转让给其他人，这可以通过商家更换票据中的消费者标识，并为其他消费者颁发一个新的等额合法票据来实现。

3.2 可分性

消费者在经纪人处购买的大额票据，可以与同一商家进行多次交易，并更新相应票据的面值。也就是说，商家在对票据扣除掉与商品或服务价格相当的数额后，为消费者提供一个具有新面值的票据和证书，从而实现了数字货币的可分性。

3.3 安全性

为了提高协议的安全性和机密性，防止票据被入侵者截获或交易信息被窃听者获取，本方案在交易双方之间建立了一个共享的对称密钥，并使用安全高效的密码算法来加密交易信息，为交易双方建立一个安全的通信通道，从而使得攻击者无法获取相关的敏感信息，也无法伪造合法的票据。同时，由于证书是单向散列函数运算的结果，它能够有效地防止对票据域进行任何形式的修改，票据域内容的任何变化将导致重新计算得到的证书与原证书不同。此外，只有知道主票据密钥的商家和可信的经纪人才能产生合法的票据，票据标识的唯一性又能防止消费者进行重复花费。

3.4 效率

在本方案中，由于商家票据可根据需要由经纪人实时产生，因而经纪人不需要保存大量的票据代码，存储开销大大减小；商家也不需要因生成票据而进行大量的计算，从而大大节省了计算开销；通过网络传输和验证生产许可证比传输大量的票据要经济得多，即减少了通信开销。同时，由于本方案完全没有采用公钥密码算法，因而协议的执行效率大大提高。

结论 本文设计了一个基于票据的新型高效微支付方案，它采用票据许可生产的模式，由商家授权经纪人生成商家票据，并由商家在线验证票据的合法性。该方案是一个离线的预付方案，它使用会话密钥对交易信息进行了加密，方案的安全性较高，且能够有效防止消费者的重复花费。同时，该方案支持数字货币的可分性和可转移性，适用于短期内消费者与同一商家的重复交易。与其它微支付方案相比，由于本方案完全没有使用公开密钥算法，且协议执行中所需保存的信息比较简单，因而系统的计算开销和存储开销大大减少。

参 考 文 献

1 Furche A, Wrightson G. SubScrip—An Efficient Protocol for Pay-Per-View Payment on the Internet. In: Proc. 5th Int. Comf. on Computer Communications and Networks (ICCCN'96), Rockville, MD, Oct. 1996. 16～19

2 Burstein J. An Implementation of MicroMint. M. Sc thesis. Massachusetts Institute of Technology, Cambridge, Massachusetts, May 1998

3 Buttyán L. Removing the Financial Incentive to Cheat in Micropayment Schemes. IEEE Electronics Letters, 2000, 36(2): 132～133

4 Adachi N, Aoki S, Komano Y, et al. The Security Problems of Rivest and Shamir's PayWord Scheme. In: Proc. of the IEEE Int. Conf. on E-Commerce (CEC'03), 2003. 126～129

5 Yen S, Lee C, Ho L. PayFair: a prepaid Internet micropayment scheme promising customer fairness. In: IEEE Proc of Comput. Digit. Tech. 2001, 148(6): 207～213

(上接第117页)

参 考 文 献

1 Fernandez M, Tan W-C, Suciu D. SilkRoute: trading between relations and XML. Computer Networks, 2000, 33: 723～745

2 孟小峰. Web 信息集成技术研究. 计算机应用与软件, 2003, 20(11): 32～36

3 Deutsch A, Fernandez M, Florescu D, Levy A, Suciu D. A query language for XML. Computer Networks, 1999, 31: 1155～1169

4 Siberschatz A, Korth H F, Sudarshan S. Database System Concepts (Fourth Edition). McGraw-Hill companies, 2002

5 XSL transformation (XSLT) specification. http://www.w3.org/TR/XSLT/

6 XSLerator, IBM. http://www.alphaworks.ibm.com/tech/xslerator/

7 XML Transform, TIBCO. http://www.tibco.com/