云计算中基于 TPM 的多银行电子现金系统*

朱 变[1], 朱 海[1,2]

(1. 周口师范学院 计算机科学与技术学院, 河南 周口 466001; 2. 西安交通大学 过程控制与效率工程教育部重点实验室, 西安 710049)

摘 要: 针对云计算的虚拟化技术可以解决传统网络中电子现金系统存在的隐私泄露、交易不规范和高成本投入问题,在已有的工作中,考虑商家和用户使用同一银行在一定程度上限制了电子现金广泛使用的情况,提出了一种基于 TPM(trusted platform module)的可信云平台多银行电子现金方案。该方案从电子现金支付的效率和安全性方面考虑,利用群签名和椭圆曲线算法 ECC 提高协议的执行效率,运用可信平台模块提供的隐私保护和远程证明功能加强支付协议的安全性。最后,对方案的安全性和效率进行分析。

关键词: 云计算; 可信计算; 电子现金; 群签名; ECC

中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2014)02-0551-04

doi:10.3969/j.issn.1001-3695.2014.02.055

Electronic cash system with multiple banks based on TPM for cloud computing

ZHU Bian[1], ZHU Hai[1,2]

(1. *School of Computer Science & Technology, Zhoukou Normal University, Zhoukou Henan* 466001, *China*; 2. *Key Laboratory of Ministry of Education for Process Control & Efficiency Engineering, Xi'an Jiaotong University, Xi'an* 710049, *China*)

Abstract: According to the virtualization technology of cloud computing, it can solve the problems that the electronic cash systems exist leakage of privacy, non-standard transactions and high cost in the traditional network. In the existing work, considering merchants and customers used the same bank to restrict the widespread use of electronic cash in a certain degree, the paper presented an multi-bank electronic cash payment scheme for trusted cloud platform based on TPM. Considering the efficiency and security from the electronic cash payment of the scheme, the scheme used the group signature and elliptic curve algorithm ECC to improve the execution efficiency of the protocol, and used the privacy protection and remote attestation function of TPM to achieve security. Finally, the paper analyzed the safety and efficiency of the scheme.

Key words: cloud computing; trust computing; electronic cash; group signature; ECC

0 引言

云计算[1,2]作为信息产业的一大创新,受到产业界、学术界等各界研究学者的关注。特别是虚拟化技术以其独特的优点得到了广泛的应用。它能充分利用现有的资源,快速地调配以适应业务需求。作为一种新兴的计算模式,它将多个大型的计算中心整合起来,形成容量大、速度快的云服务中心。用户可以按其业务负载快速申请或释放资源,并以按需支付的方式对所使用的资源进行付费。可以肯定,云计算在不久的将来将改变人类的生活方式,人类将进入新的计算技术时代。

云计算的出现,给电子商务企业带来全新的机会。电子商务以低成本、超时空、多媒体手段与个性化服务等优点,一直成为研究的热点。电子商务中最核心和最关键的环节就是电子现金支付,如果没有支付系统,整个商务活动就不能实现。电子现金[3]就是一种非常重要的电子支付方式[4],传统网络中的电子支付存在用户隐私泄露、交易不规范和成本投入高等问题。云环境中的电子商务用户不需要购买复杂的硬件和软件,只需支付相应的费用给云计算服务提供商,通过网络就可以方便地获取所需要的计算、存储等资源,从而很好地解决企业成本投入高的问题。云计算的虚拟化技术同时也给电子商务企业带来更多的挑战和新问题。如云平台中的安全性问题将赋予新的内涵,按照云计算的理念,用户在本地几乎不保存任何数据,所有数据都存放在云端的数据中心,一旦云端发生故障,云电子商务企业将束手无策。并且在云安全领域,软件系统的安全问题仍然是一个挑战性难题。由于云计算里的数据中心、虚拟化技术等都依赖于各类计算机系统,云计算更需要计算机系统终端的安全可信。只有确保云计算机系统的安全可信,才能确保云计算上层应用的安全可信[5,6]。可信计算将计算的安全问题从新的角度解决,不同以往的安全概念,可信计算能够保证用户数据的安全性,也确保计算机系统的可信性。因此,将可信计算技术融入云计算[7]环境中,以可信赖方式提供云服务已成为云安全研究领域的一大热点。

云平台中的电子现金方案存在的安全问题,用传统的电子现金方案已不能解决。这里举出代表性的研究文献如下:文献[8,9]提出一种单银行电子现金方案,利用可信平台模块芯片来保证交互安全性,利用群签名[10,11]和盲签名技术来提高交

收稿日期: 2013-05-07; **修回日期**: 2013-07-04 **基金项目**: 国家自然科学基金资助项目(61103143);中国博士后科学基金资助项目(2012M512008);河南省高校科技创新人才支持计划项目(2012HASTIT032);周口师范学院青年科研基金资助项目(zksyqn201323A)

作者简介:朱变(1982-),女,河南周口人,助教,硕士,主要研究方向为云计算、可信计算、电子商务(zknulunwen@163.com);朱海(1978-),男,河南南阳人,博士(后),主要研究方向为云计算、信息安全与智能算法.

付效率。但是在现实生活中由多个电子银行系统[12]发行的电子现金要比单个银行发行的电子现金更适合于现代支付系统。因此,对多银行电子现金系统的研究更加符合实际需求。文献[13]提出一种椭圆曲线群签名方案,并把这种方案应用于多银行电子现金系统中,该方案可以很好地解决电子现金支付安全性,但实施的前提是交付的终端系统绝对安全可靠,很多情况下,用户的终端系统是不安全的。

目前,有很多学者对云平台中的电子商务安全问题做了大量的研究工作并取得较好的研究成果,然而在系统终端安全性方面仍然考虑不足。因此,本文提出了一种基于 TPM 的可信云平台多银行电子现金方案,方案运用可信计算技术中的远程证明功能加强云服务提供商和客户系统终端的安全性,利用群签名和椭圆曲线算法来提高电子现金支付的效率问题。

1 预备知识

1.1 可信计算技术

可信计算的概念由可信计算组织(Trusted Computing Group,TCG)提出。“可信”的概念被定义为:“一个实体在实现给定的目标时,若其行为总是如同预期,则该实体是可信的。”其核心思想是:在计算机系统中引入一个带有信任根并且具有一定防窜改能力的安全芯片 TPM,在保证信任根信任的前提下,建立一条信任链,一级测量一级,一级信任一级,从而将信任关系扩大到整个计算机系统中,保证计算机系统的可信。

可信计算平台[14](trusted computing platform,TCP)是在原有系统安全机制的基础上,基于可信计算模块,以密码技术、安全操作系统为核心,用于增强系统安全和网络安全功能的基本安全框架。可信计算模块[15](TPM)是可信计算平台的核心部件,完成对数据的加密、解密和认证等安全功能。

远程证明技术是用于解决可信计算平台之间与可信网络节点间信任的重要安全机制。该技术通过分析远程系统的完整性来确定其可信性。直接匿名认证(DAA)技术是一种基于身份的远程证明技术,该技术使用了群签名机制,使得通信双方不会暴露彼此的身份信息。此外,这种群签名机制还依赖零知识证明技术。

1.2 群签名技术

在群签名方案中,该技术允许群里任何成员以匿名的方式代表群签署文件,别的群体或者成员可以通过这个群签名验证这个数据的群体归属,而不需要知道具体是哪个群成员对其进行签名的。此外,群的管理者负责管理群成员的加入、退出,并且在发生争议的时候,可以验证签名者的身份。

群签名方案过程如下:

a)创建。用多项式时间概率算法来产生一个群公钥和私钥。

b)加入。用户通过群管理员定义的一种交互式安全协议来成为群成员。在这个过程将产生新的群成员私钥和证书,并使得群管理员得到该群成员的成员管理密钥。

c)签名。这是一个概率算法,把需群签名的数据经过一个群成员的私钥签名,得到签名结果。

d)验证。通过群公钥验证一个群签名是否为该群的签名。

e)打开。群管理员通过一个群私钥和用群私钥签名的数据,来验证群成员的身份是否合法。

2 模型设计

该模型的参与主体主要有银行、商家、用户和云服务提供商,并且假定所有主体的系统终端都嵌入了 TPM 模块。多家云电子银行构成一个群体,受云服务提供商管理,任意一个银行可以发行电子现金。用户和商家可以不在同一银行进行电子现金的提取和存款操作。模型示意图如图 1 所示。

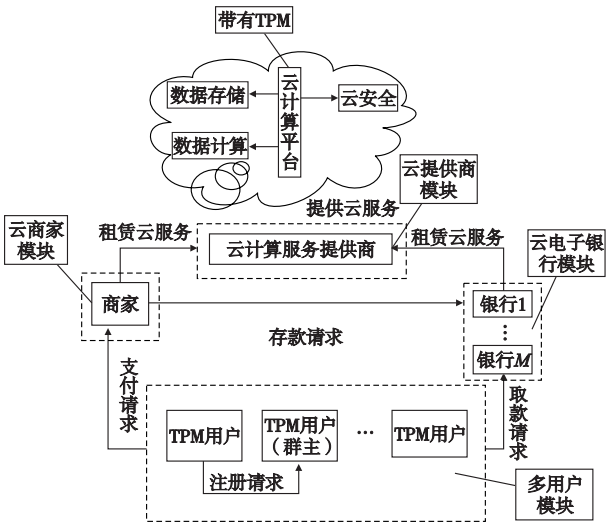

图1 云环境中支持隐私保护的多银行电子现金模型

云环境中基于 TPM 的多银行电子现金模型分为四个模块,分别如下:

a)云电子银行模块。多家电子银行组建的群体,群管理者 G_B,群成员 B_i,其群公私钥对为(PK_{B_i},SK_{B_i})。该模块具有存款和取款功能。

b)用户模块。由多个用户组建的群体,群管理者 G_U。用户 U_i(自己的银行 B_i),平台的身份证明密钥 AIK(公钥 PK_{AIK},私钥 SK_{AIK}),用户的身份 ID 用 I_U 表示,并且每个用户的系统终端嵌有 TPM 模块用来保护终端安全性。

c)商家模块。商家 S(自己的银行 B_j),其公私钥对为(PK_S,SK_S)。商家为降低成本投入,租用云服务。

d)云服务提供商模块。云服务提供商为商家和银行提供各种云服务。

方案中主体交互采用的加密算法用 E 表示。

该模型具有下面的性质:

a)云电子银行不能跟踪任何一笔电子现金,用户可以匿名地花费自己的电子现金。

b)商家只须利用用户模块群公钥执行一个简单的验证,就可以验证接收的电子现金是否合法,这样商家的验证工作就很简单。

c)云电子银行模块和用户模块的公钥分别只有一个,公钥不会随着成员个数的增加而增加。

d)用户从银行取走电子现金,除群管理者知道外,任何人都不知道是哪个银行发行,这样实现银行的匿名性。

3 协议流程

模型主体的交互过程如下:

a)注册。银行 B_i 要想成为云电子银行模块的群成员,先要与模块的群管理者进行交互,以确认自己身份的真实性;通

过后,银行 B_i 会获得模块的公私钥。

b)取款。用户 U 从银行 B_i 提取一笔电子现金。

c)支付。用户 U 将电子现金支付给商家 S。

d)存款。商家 S 将电子现金存入银行 B_j 中。

3.1　多用户模块系统初始化

这个阶段产生系统运行时所需要的参数。

设有一双线性对 $e:G_1 \times G_1 \rightarrow G_2$,其中 G_1 为具有相同序 q 的椭圆曲线加法循环群,G_2 为具有相同序 P 的乘法循环群,其中 G_1、G_2 的离散对数是 NP 难问题。用户群主 G_U 选择 $S_T \in Z_q^*$ 为私密参数,群公钥:$PK_{G_U} = S_T \cdot P$,TPM 设置一个具有强无碰撞散列函数为 H,群主 G_U 公开参数$\{G_1, G_2, P, q, H, S_T, PK_{G_U}\}$。商家选择 SK_S 为私密参数,则公钥为 $PK_S = SK_S \cdot P$。

用户加入多用户模块的交互协议过程如下:

U　　G_U

$R_i \in Z_q^*$

$I_i = I_U \parallel PK_{\mathrm{AIK}} \parallel R_i$

$\xrightarrow{E_{PK_{G_U}}(I_i)}$

利用 SK_{G_U} 验证 I_U,

若合法,则

$k, g, x, d \in Z_q^*$

$PK_U = g^{I_U - 1} \bmod (n)$

$SK_U = I_U x d + k_i \bmod (n)$

$\xleftarrow{(PK_U, SK_U)}$

在这里,用户群管理员把新加入的用户信息保存到一个专门的数据库以便查找。假定 G_U 是可信的,不需要可信第三方的参与,从而减少了交互过程,提高了系统的运行效率。

3.2　云电子银行模块系统初始化

图 1 中,云计算平台假定带有 TPM 芯片,用以保护整个云服务基础设施和上层服务的安全性。由于许多银行租用云服务,假定每个电子银行的系统终端也是安全的。假定云服务提供商是云电子银行模块的管理员。

银行模块管理员 G_B 选择 SK_S 为私密参数,则公钥为 $PK_{G_B} = SK_B \cdot P$。银行加入模块的过程类似用户成为群成员,在这里略去认证步骤。银行模块管理员 G_B 公布参数$\{G_1', G_2', P', q', H', SK_{G_B}, PK_{G_B}\}$,银行拥有$(PK_{G_B}, SK_{G_B})$。系统初始化完成后,假设商家、银行、用户都已获得了相应的公私钥对。

3.3　取款协议

当 U 想在 B_i 取款时,U 需要向 B_i 证明自己是该账户的所有者,通过验证后才能进行取款操作。交互协议如下:

U　　B_i

$\xrightarrow{E_{SK_{G_U}}(PK_{\mathrm{AIK}}, I_U)}$

$w \in_R Z_n^*$

$a \leftarrow wG$

$b \leftarrow w(I + G_2)$

并利用 SK_{G_U} 验证

$\xleftarrow{a, b}$

$\mathrm{data} = (\mathrm{cash} + \mathrm{value} + \mathrm{sign}_{SK_{\mathrm{AIK}}}(H(\mathrm{PCR} + \mathrm{time})) + \mathrm{binding} + I_U)$

其中:cash 为 U 取款金额;value 为电子现金的有效期;time 为时间标记并且唯一;binding 为逻辑值,表示电子现金是否与 TPM 绑定;data 表示用户取款的消息。

$t_1 \in Z_q^*$

$\mathrm{data}' = t_1 H(\mathrm{data})$

$\xrightarrow{\mathrm{data}', H(\mathrm{PCR} + \mathrm{time}), \mathrm{cash}}$

$k \in Z_q^*, R_1 = K \cdot P$

$S_1 = k^{-1}\mathrm{data}' \cdot P$

$S_2 = k^{-1} \cdot SK_{B_i}$

$\mathrm{data}'' = E_{SK_{G_B}}(R_1, S_1, S_2)$

$\xleftarrow{\mathrm{data}''}$

用户从银行 B_i 获得加密的电子现金 data″。

3.4　支付协议

当 U 在 S 购买商品后,需要和商家交互进行电子现金支付,支付协议如下:

U　　S

$\xleftarrow{\text{付款信息 } e}$

$E' = \mathrm{el} + E \ \mathrm{mon}\ (n)$

$Z' = S_{SK_S} \bmod (n)$

$\xrightarrow{E', Z'}$

$\xrightarrow{H(\mathrm{PCR} + \mathrm{time}), PK_{\mathrm{AIK}}, \mathrm{data}, \mathrm{data}''}$

S 利用 PK_{G_S} 验证现金的合法性,若通过,再验证电子现金的 time、binging、PCR 值。

若全部信息都正确,S 就接受 U 的电子现金。

商家 S 保存用户支付的电子现金。

3.5　存款协议

所有银行都有一个在线数据库,该数据库中保存着一个已花费现金的清单,它是由电子银行群管理员来公布,这样可以检测出电子现金的重复花费现象。商家向银行存款,交互协议如下:

S　　B_j

$\xrightarrow{\mathrm{data}'', \mathrm{sign}_{\mathrm{data}''} H(\mathrm{PCR} + \mathrm{time}), PK_{\mathrm{AIK}}, (e, E', Z')}$

检查电子现金是否有效,若有效,在已花费的电子现金数据库中进行查找。如果没有对应记录存在,就将电子现金存入商家账户中;否则,银行认为用户重复消费,拒绝接受。

银行群管理员维护已花费的电子现金数据库,定期查找有效期过期的电子现金,并将该电子现金删除。这样做可以不再维护庞大的电子现金数据库。

4　效率及安全性分析

4.1　效率分析

该方案采用的群签名是基于 ECC 加密算法基础上。与 RSA 算法相比较,文献[16~18]已经通过实验证明,在相同的密钥长度下,ECC 抗攻击性比 RSA 要强很多倍,ECC 能以更小的密钥长度提供更好的加密强度、更快的执行效率,而且计算量小,处理速度快。ECC 与 RSA 执行效率比较如表 1 所示。

表 1　ECC 与 RSA 执行效率比较

密钥长度	加密		解密		密钥对生成	
	RSA	ECC	RSA	ECC	RSA	ECC
1024/160	0	16	16	15	243	219
3072/256	31	31	625	32	4125	234
15360/512	78	63	74047	171	858906	375

理论上,160 位的 ECC 与 1024 位 RSA、DSA 具有相同的安全性。并且实验证明,在相同的计算环境下,使用 160 位的 ECC 技术加、解密要比用 1024 位 RSA 快 5~8 倍。

4.2　安全性分析

云平台中的电子现金支付安全性主要体现为用户敏感数据的安全、电子现金的安全、支付网关的安全(它们两两之间传输的数据不会被监听、窜改)。具体体现如下:

a)不可伪造性。发币虚拟银行受云电子中央银行的控制。电子现金必须经过银行的数字签名后才具有支付能力,除了银行外,其他的主体都无法伪造有效的电子现金签名。如果攻击者试图采用不同的消息 m_1 伪造签名,但由于 $e_1 = H(m_1) \neq e$,攻击者不知道 x 和 k 的值,所以无法伪造签名。如果攻击者通过 $y = g^x \bmod p$ 成功求得私钥 x,但由于签名过程中,选取随机数 k 来计算 $kP_{iss} = (x_1, y_1)$,而产生签名 $s_1 = ex + r_1 \bmod n$, $s_2 = ex + \bmod n$ 的计算需要 k 值参与运算,而 k 又是保密的,所以攻击者是不可能成功伪造签名的。

b)用户匿名性。该方案是基于 TPM 和群签名设计。TPM 具有匿名控制和远程证明的功能,而群签名也是基于零知识证明实现匿名功能及其离散对数问题和零知识证明问题。在签密算法中,接收者公钥由单向哈希函数进行运算,哈希运算的结果又由发送方的私钥 (x_A, S_A) 进行群上的乘法运算,从密文中获得接收方 ID_B 的身份信息是一个困难问题。所以三者在交易过程中,商家不能得知用户的身份,银行也不能把商家的存款记录和用户的取款记录联系起来,这样银行和商家就是共谋也不能确定用户的真实身份,从而实现了用户的匿名性。

c)平台绑定性。本方案与其他多银行电子现金方案最大的不同就是加入了 TPM 和使用云平台,TPM 把电子现金与平台身份、用户身份三者有机绑定在一起,即使非法主体盗用用户的电子现金,如果没有合法的 TPM 提供 PCR 值,盗用者也不能使用电子现金。对于没有加入可信平台的群签名方案,如果用户重复消费电子现金,那么他可以狡辩自己没有使用,本方案中针对这个情况,群管理员可以使用 TPM 来追踪用户的平台身份使之不能抵赖。

5 结束语

本文设计了基于 TPM 的可信云平台多银行电子现金方案。该方案通过运用 TPM 的远程证明功能和群签名技术来保证电子现金支付的安全性、匿名性和高效性。

参考文献:

[1] 叶可江,吴朝晖,姜晓红,等. 虚拟化云计算平台的能耗管理[J]. 计算机学报,2012,35(6):1262-1264.

[2] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing[C]//Proc of Conference on Hot Topics in Cloud Computing. Berkeley: USENIX Association, 2009.

[3] 彭建新,王常吉. 离线匿名电子现金系统的设计与实现[J]. 计算机科学,2007,34(3):129-131.

[4] 付雄,程文青,郎为民,等. 安全电子支付系统研究[J]. 计算机科学,2005,32(1):108-109.

[5] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011 ,22(1):71-83.

[6] 吴吉义,沈千里,章剑林,等. 云计算:从云安全到可信云[J]. 计算机研究与发展,2011,48(z1):229-233.

[7] LUCKY R W. Cloud computing[J]. IEEE Spectrum, 2009, 46(5): 27.

[8] 陈利,朱变. 一种改进的电子现金方案[J]. 计算机应用研究,2011,27(12):4659-4661.

[9] 沈丽红,徐震. 基于可信计算平台的电子现金技术[J]. 中国科学院研究生院学报,2009,26(5):715-717.

[10] WANG Shao-hui. Modification and improvement on group signature scheme without random oracles[C]//Proc of International Conference on Electronic Commerce and Security. 2008:462-466.

[11] ZHOU Xuan-wu, YANG Xiao-yuan, WEI Ping, *et al*. Dyanmic group signature with forward security and its application[C]//Proc of the 6th International Conference on Grid and Cooperative Computing. Piscataway, NJ: IEEE Press, 2007:473-480.

[12] 张方国,张福泰,王育民. 多银行电子现金系统[J]. 计算机学报,2001,24(5):455-462.

[13] 韩晓花,李乔良,袁遇晴. 基于椭圆曲线群签名方案的多银行电子现金系统[J]. 计算机研究与发展,2009,46(9):306-310.

[14] 刘宏伟. 朱广志. 可信计算平台认证机制研究[J]. 计算机工程,2006,32(24):148-149.

[15] CG. Trusted platform module (TPM) specifications [EB/OL]. (2009). https://www. trus ted computinggroup. Org/ specs/TPM/.

[16] GUPTA K, SILAKARI S, GUPTA R, *et al*. An ethical way for image encryption using ECC[C]//Proc of the 1st International Conference on Computational Intelligence, Communication Systems and Networks. 2009:342-345.

[17] HABIB M, MEHMOOD T, ULLAH F, *et al*. Performance of WiMAX security algorithm[C]//Proc of International Conference on Computer Technology and Development. 2009:108-112.

[18] YUAN Yang-tao, Liu Quan, LI Fen. A design of certificate authority based on elliptic curve cryptography[C]//Proc of the 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. 2010: 454-457.

(上接第 550 页)

[4] GU Guo-fei, PERDISCI R, ZHANG Jun-jie, *et al*. BotMiner: clustering analysis of network traffic for protocol- and structure-independent botnet detection[C]//Proc of the 17th Conference on Security Symposium. Berkeley, CA: USENIX Association, 2008:139-154.

[5] CHOI H, LEE H, LEE H, *et al*. Botnet detection by monitoring group activities in DNS traffic[C]//Proc of the 7th IEEE International Conference on Computer and Information Technology. 2007:715-720.

[6] GU Guo-fei, PORRAS P, YEGNESWARAN V, *et al*. BotHunter: detecting malware infection through IDS-driven dialog correlation [C]//Proc of the 16th USENIX Security Symposium. Berkeley, CA: USENIX Association, 2007:1-16.

[7] GIROIRE F, CHANDRASHEKAR J, TAFT N, *et al*. Exploiting temporal persistence to detect covert botnet channels[C]// Proc of the 12th International Symposium on Recent Advances in Intrusion Detection. 2009: 326-345.

[8] DIETRICH C J, ROSSOW C, POHLMANN N. CoCoSpot: clustering and recognizing botnet command and control channels using traffic analysis[J]. Computer Networks, 2013, 57(2):475-486.

[9] TEGELER F, FU X, VIGNA G, *et al*. Botfinder: finding bots in network traffic without deep packet inspection[C]//Proc of the 8th International Conference on Emerging Networking Experiments and Technologies. New York: ACM Press, 2012:349-360.

[10] HOLZ T, GORECKI C, RIECK K, *et al*. Measuring and detecting fast-flux service networks[C]//Proc of the 15th Network and Distributed System Security Symposium. 2008.

[11] BLOOM B. Space/time tradeoffs in hash coding with allowable errors [J]. Communications of the ACM, 1970, 13(7):422-426.