基于花费链最优匿名的等长可传递电子现金系统

张江霄[1],李舟军[2],高延武[1],冯春辉[1],郭 华[2]
(1.邢台学院数学与信息技术学院,河北邢台 054001;2.北京航空航天大学软件开发环境国家重点实验室,北京 100191)

摘 要: 针对现有的可传递电子现金系统在传递协议中电子现金长度和传递次数成正比的问题,利用Groth-Sahai证明系统和累加器原理,首次提出花费链构建法,并在标准模型下构建一个具有最优匿名性的传递协议中电子现金长度不变的可传递电子现金系统.基于花费链构建法,用户无需存储任何花费凭证;与现有系统相比,在传递协议中,用户传递电子现金的长度是常量;在安全性上,新系统具有最优匿名性,即全匿名性、完美匿名性1和完美匿名性2.最后,在标准模型下给出系统的安全证明,该系统具有不可伪造性、最优匿名性、不可重复花费性和不可诬陷性.

关键词: 可传递电子现金系统; 花费链; 有限累加器; Groth-Sahai证明; 交互签名
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2015)09-1805-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.09.019

Transferable E-cash System of Equal Length with Optimal Anonymity Based on Spending Chain

ZHANG Jiang-xiao[1], LI Zhou-jun[2], GAO Yan-wu[1], FENG Chun-hui[1], GUO Hua[2]
(1. *Mathematics and Information Technology Institute, Xingtai University, Xingtai, Hebei* 054001, *China*;
2. *State Key Laboratory of Software Development Environment, Beihang University, Beijing* 100191, *China*)

Abstract: There exist some problems such that the length of the E-cash is proportional to the number of the transfer protocol in the transferable E-cash system. Using the Groth-Sahai (GS) proof system and accumulator, we first propose spending chain algorithm and design a transferable E-cash system of equal length with optimal anonymity in the standard model. Based on the spending chain, the users do not need to keep in memory the data associated to all past transactions. Compared with the existing systems, the length of the E-cash is constant in the spending protocol. Meanwhile, the new system achieves the optimal anonymity, such as full anonymity, perfect anonymity 1 and perfect anonymity 2. At last, the security proof of the systemis given in the standard model, i.e. unforgeability, anonymity, identification of double spender and exculpability.

Key words: transferable E-cash system; spending chain; bounded accumulator; Groth-Sahai proof; commuting signature

1 引言

可传递电子现金系统允许用户在收到电子现金后,无需存入银行,就可以直接花费电子现金,从而避免用户把电子现金存入银行,再从银行取出电子现金,然后进行花费.因此可传递电子现金系统能减少用户和银行之间的通讯次数,增加电子现金的实用性.

由于可传递电子现金的实用性,近来很多学者对其进行研究[1~15].Okamoto和Ohta[1,2]首次引入电子现金的可传递性,并给出两个简单的可传递电子现金系统.但是攻击者能够链接相同花费者的不同花费,因此这两个电子现金系统只能达到弱匿名性.Chaum[3]在1992年,构建一个具有强匿名性的可传递电子现金系统,但是该系统电子现金长度和传递次数成正比.Canard和Gouget[8]在2008年提出一个高效可传递电子现金系统,然而该电子现金系统不具有强匿名性.随后Canard和Gouget[9]分析可传递电子现金系统的匿名性,把匿名性分为弱匿名性、全匿名性和完美匿名性,但是没有给出具有最优匿名性的可传递电子现金系统.Blanton[10]在2008年构建一个条件可传递电子现金系统,但是电子现金长度和传递次数成正比,同时该系统没有达到最优匿名性.2009年Fuchsbauer等人[12]给出一个长度不变的可传递电子现金系统,然后存在以下缺点,用户为了证明自己没有发生重复花费,在每一笔花费完成后,必须

收稿日期:2014-04-01;修回日期:2014-07-28;责任编辑:梅志强
基金项目:国家自然科学基金(No.60973105,No.61170189,No.61300172,No.61370126);博士点基金(No.20111102130003,No.20121102120017);软件开发环境国家重点实验室自主课题(No.SKLSDE-2013ZX-19.No.SKLSDE-2012ZX-11);中央高校基本科研业务专项资金(No.YWF-13-A02-13);河北省高等学校青年拔尖人才计划项目(No.BJ201414)

存储花费凭证,另外如果有用户发生重复花费,则诚实用户的身份也将被恢复.在 2011 年,Blazy 等人[13]构建一个能达到最优匿名性的可传递电子现金系统,但是该系统中电子现金长度和传递协议次数成正比,从而降低可传递电子现金系统的实用性.在 2012 年 Zhang 等人[14]构建一个最优匿名的条件可传递电子现金系统,但是电子现金长度仍然和传递次数成正比.

通过以上分析,我们知道,具有最优匿名性的可传递电子现金系统,电子现金长度和传递次数成正比;电子现金长度是等长的可传递电子现金系统,用户需要存储花费凭证,而且没有达到最优匿名性.为了解决这个问题,本文构建一个同时具有最优匿名性的、电子现金长度是常量的可传递电子现金系统.具体说来,Blazy[13]和 Zhang[14]等人的电子现金长度和传递的次数成正比,即电子现金的长度为 kn,在此我们假设 n 为传递次数,k 为系统的安全参数,而新系统中电子现金长度是常量,即电子现金长度为 k 因此提高可传递电子现金的实用性.基于 Groth-Sahai 证明系统和累加器原理,利用承诺和对应的证明表示电子现金,从而达到最优匿名性,即全匿名性,完美匿名性 1 和完美匿名性 2.

2 基本定义

定义 1(双线性对) 双线性对是一个满足下面条件的映射,定义 $e: G_1 \times G_2 \to G_3$,其中群 G_1, G_2 和 G_3 是 p 阶乘法循环群,p 为素数;g, h 分别是 G_1, G_2 的生成元.

(1)(双线性) $\forall x \in G_1$, $y \in G_2$ 且 a, $b \in Z_P^*$,则 $e(x^a, y^b) = e(x, y)^{ab}$;

(2)(非退化性) $e(g, h) \neq 1$;

(3)(可计算性) e 是多项式时间可计算的.

定义 2(SXDH 问题)[16] 设 $(p, G_1, G_2, G_3, e, g, h)$ 是一个素数阶群,其中 p 为素数,g, h 分别是 G_1, G_2 的生成元,$e: G_1 \times G_2 \to G_3$. SXDH(Symmetric external Diffe-Hellman)问题指在群 G_1 和 G_2 上 DDH 问题是困难的.

定义 3(GS 证明) GS 证明[16]在标准模型下给出有关双线性群中等式的非交互式零知识证明,它适合多种双线性群中群元素关系的等式,具体包括:双线性乘积等式、多标量乘法等式和二次等式,本文只使用基于 SXDH 假设下的双线性乘积等式.

定义 4(有限累加器) 有限累加器[17,18]最多可以累加有限个元素,同时存在一个证据,可以证明该元素被累加到累加值中,任何人无法证明一个没有累加的元素被累加到累加值中.

定义 5(交互签名) 交互签名[19]允许用户对消息、验证秘钥、对应的签名做承诺,并证明被承诺的签名是被承诺消息的签名.交互签名提供了很多算法,我们只需要算法 SigCom.

3 花费链构建法

花费链构建法允许用户向知道某个群元素离散对数的用户花费电子现金.在存款协议中,银行利用最后用户的序列号,就可以计算依次花费过该电子现金的用户的序列号.使得每次传递中,用户只需保存第一个序列号和自己的序列号,因此电子现金的长度是常量.具体的构建方法如下.

可信第三方 T 构建花费链,我们假设花费链的长度是 n(n 为自然数),T 随机选择 $k_0 \in Z_p^*$,计算 $k_1 = g_0^{k_0 (\mathrm{mod} q)} (\mathrm{mod} p)$,依次计算,直到 $k_n = g_0^{k_{n-1} (\mathrm{mod} q)} (\mathrm{mod} p)$,$g_0$ 是 G_q 的一个生成元.具体的花费链如图 1. T 从右往左构建花费链,用户从左往右进行花费,在构建后,利用累加器把花费链中每个节点的序列号 k_i 累加到累加值 Acc 中,并对每个节点给出一个被累加到累加值 Acc 的证据 w_i,然后银行对每个节点 k_i 以及对应的证据 w_i 进行签名,最后 T 利用安全的秘密认证信道把 k_i 和 w_i 分配给用户 U_i.

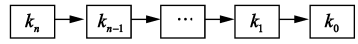

图1 花费链

4 可传递电子现金的构造

新的可传递电子现金系统由用户($U_1, \cdots, U_n$)、商家 M(特定的用户)、取款银行 WB、存款银行 DB 和可信第三方 T 组成.

4.1 基本参数

下面首先给出构造可传递电子现金系统所需的基本参数,λ 是安全参数,G_1, G_2 和 G_3 是阶为 p 的素数阶群.为构造花费链,可信第三方选择素数 q, p, P,在此 q 整除 $p-1$,并且 $P = 2p + 1$.同时定义 G_q 和 G_p 分别是 Z_p^* 和 Z_P^* 的子群,且 G_q 和 G_p 的阶分别是 q 和 p,g_0 是 G_q 的一个生成元.用户和银行计算交互签名所需的公私钥(pk_U, sk_U)、($\mathrm{pk}_{\mathrm{WB}}$, $\mathrm{sk}_{\mathrm{WB}}$)和($\mathrm{pk}_{\mathrm{DB}}$, $\mathrm{sk}_{\mathrm{DB}}$),另外存款银行还需生成一个承诺提取密钥对($\mathrm{ck}_{\mathrm{DB}}$, $\mathrm{ek}_{\mathrm{DB}}$).我们假定参加可传递协议的用户个数为 n.

4.2 最优匿名性

可传递的电子现金系统达到最优匿名性,是指可传递的电子现金系统同时满足全匿名性、完美匿名性 1 和完美匿名性 2[9].具体的定义如下:

全匿名性:指攻击者假扮银行,也不能链接已经收到的电子现金和以前观察过的电子现金;

完美匿名性 1:指攻击者假扮银行,也不能链接已观察过的电子现金和已经拥有过的电子现金;

完美匿名性 2:银行是诚实的,攻击者不能链接他已经接受过的两个电子现金.

4.3 安全属性

本文借助 GS 证明系统,在标准模型下,证明可传递电子现金系统的安全性,为了描述攻击者的能力,我们需要以下 5 个预言机:交互签名预言机(Sign())、用户建立预言机(Setup())、取款预言机(Withdraw())、传递预言机(Transfer())和存款预言机(Deposit()).

为了描述安全属性,首先引入以下 9 个算法:CashSetUp(λ)、WBSetUp(params)、DBSetUp(params)、USetUp(params)、Start(params, pk_{U_i}, sk_{U_i}, $\mathrm{pk}_{\mathrm{DB}}$)、Withdraw(U(params, pk_U, sk_U, $\mathrm{pk}_{\mathrm{WB}}$)$\leftrightarrow$WB(params, $\mathrm{pk}_{\mathrm{WB}}$, $\mathrm{sk}_{\mathrm{WB}}$, pk_U))、Transfer(U(params, pk_U, sk_U, pk_M)$\leftrightarrow M$(pk_U, pk_M, sk_M)、Deposit(M(params, pk_{U_i}, sk_{U_i}, $\mathrm{pk}_{\mathrm{DB}}$, coin)$\leftrightarrow$DB(params, $\mathrm{pk}_{\mathrm{DB}}$, $\mathrm{sk}_{\mathrm{DB}}$)、Identify(params, coin, db)

下面利用实验的方式描述各个安全属性.在实验中利用攻击者 A 与挑战者 B 之间进行实验.具体的描述如下.

(1)不可伪造性

定义 A 成功伪造一个电子现金的优势为:

$$\mathrm{Adv}_{c,A}^{\mathrm{unforge}}(\lambda)=\Pr[\mathrm{Exp}_{c,A}^{\mathrm{unforge}}(\lambda)=1]$$

定义 6(不可伪造性) 如果在多项式时间下,攻击者 A 成功的优势 $\mathrm{Adv}_{c,A}^{\mathrm{unforge}}(\lambda)$可忽略,则此协议具有不可伪造性.

(2)匿名性

匿名性包括全匿名性、完美匿名性 1 和完美匿名性 2.下面分别描述.

全匿名性 定义攻击者 A 攻破协议全匿名性的优势为:

$$\mathrm{Adv}_{c,A}^{\mathrm{fanon}}(\lambda)=\Pr[\mathrm{Exp}_{c,A}^{\mathrm{fanon}-0}(\lambda)=1-\mathrm{Exp}_{c,A}^{\mathrm{fanon}-1}(\lambda)=1]$$

完美匿名性 1 定义攻击者 A 攻破协议完美匿名性 1 的优势为:

$$\mathrm{Adv}_{c,A}^{\mathrm{panon1}}(\lambda)=\Pr[\mathrm{Exp}_{c,A}^{\mathrm{panon1}-0}(\lambda)=1-\mathrm{Exp}_{c,A}^{\mathrm{panon1}-1}(\lambda)=1]$$

完美匿名性 2 定义攻击者 A 攻破协议完美匿名性 2 的优势为:

$$\mathrm{Adv}_{c,A}^{\mathrm{panon2}}(\lambda)=\Pr[\mathrm{Exp}_{c,A}^{\mathrm{panon2}-0}(\lambda)=1-\mathrm{Exp}_{c,A}^{\mathrm{panon2}-1}(\lambda)=1]$$

定义 7(匿名性) 如果在多项式时间下,攻击者 A 成功的优势 $\mathrm{Adv}_{c,A}^{\mathrm{fanon}}(\lambda)$,$\mathrm{Adv}_{c,A}^{\mathrm{panon1}}(\lambda)$和 $\mathrm{Adv}_{c,A}^{\mathrm{panon2}}(\lambda)$可忽略,则此协议具有匿名性.

(3)不可重复花费性

定义攻击者 A 攻破协议不可重复花费性的优势为:

$$\mathrm{Adv}_{c,A}^{\mathrm{idds}}(\lambda)=\Pr[\mathrm{Exp}_{c,A}^{\mathrm{idds}}(\lambda)=1]$$

定义 8(不可重复花费性) 如果在多项式时间下,攻击者 A 成功的优势 $\mathrm{Adv}_{c,A}^{\mathrm{idds}}(\lambda)$可忽略,则此协议具有不可重复花费性.

(4)不可诬陷性

定义攻击者 A 攻破不可诬陷性的优势为:

$$\mathrm{Adv}_{c,A}^{\mathrm{exculp}}(\lambda)=\Pr[\mathrm{Exp}_{c,A}^{\mathrm{exculp}}(\lambda)=1]$$

定义 9(不可诬陷性) 如果在多项式时间下,攻击者 A 成功的优势 $\mathrm{Adv}_{c,A}^{\mathrm{exculp}}(\lambda)$可忽略,则此协议具有不可诬陷性.

4.4 开户协议

开户协议允许用户 $U_i(1\leqslant i\leqslant n)$从可信第三方 T 得到花费链的序列号 k_i 以及对应的证据 w_i,然后 U_i 才能花费该电子现金.具体协议如下:

(1) $T\rightarrow$DB:可信第三方 T 利用花费链构建法生成花费链,并计算累加值 Acc 的承诺 C_{Acc}以及对应的证明 $\pi_{C_{\mathrm{Acc}}}$.最后 T 发给存款银行 C_{Acc}和 $\pi_{C_{\mathrm{Acc}}}$.

(2)DB$\rightarrow T$:存款银行验证证明 $\pi_{C_{\mathrm{Acc}}}$的正确性,如果不正确,协议终止,否则利用算法 SigCom 对承诺 C_{Acc}生成承诺签名 $C_{\sigma_{\mathrm{Acc}}}$,以及对应的证明 π_{Acc},π_{Acc}证明承诺签名中的 σ_{Acc}是累加值 Acc 的银行签名.最后,存款银行发送 $C_{\sigma_{\mathrm{Acc}}}$ π_{Acc}给 T.

(3) $U_i\rightarrow T$: U_i 向 T 提供自己的公钥 pk_U.

(4) $T\rightarrow U_i$:可信第三方 T 核实用户 U_i 的公钥是否真实,如果不真实,协议终止,否则给用户 U_i 发送序列号和对应的证据,同时把用户的公钥和序列号对应起来,以便在用户发生重复花费后,通过序列号能恢复重复花费用户的身份.同时 T 也给出 k_i 被累加到累加器中的证明 π_{w_i}.最后,T 通过安全的秘密认证信道发送给用户 U_i 下面的值:k_i, w_i, $C_{\sigma_{\mathrm{Acc}}}$, π_{Acc}和 π_{w_i}.

4.5 取款协议

取款协议允许用户 U_1 从取款银行提取电子现金 coin_1.具体的协议如下:

(1) $U_1\rightarrow$WB: U_1 利用存款银行的承诺密钥 $\mathrm{ck}_{\mathrm{DB}}$对序列号 k_1 生成承若 C_{k_1},以及对应的证明 π_{k_1},最后 U_1 发送给取款银行 C_{k_1}和 π_{k_1}.

(2)WB$\rightarrow U_1$:WB 验证证明 π_{k_1}的正确性后,WB 利用算法 SigCom 对承诺 C_{k_1}生成承诺签名 $C_{\sigma_{\mathrm{bk1}}}$,以及对应的证明 π_{bk1}.最后 WB 发送给 U_1 下面的值:$C_{\sigma_{\mathrm{bk1}}}$和 π_{bk1}.

(3) U_1: U_1 验证证明 π_{bk1}的正确性后,为保证电子现金的不可诬陷性,U_1 也利用算法 SigCom 对承诺 C_{k_1}生成承诺签名 $C_{\sigma_{\mathrm{uk1}}}$,以及对应的证明 π_{uk1}.最终 U_1 得到 $\mathrm{coin}_1=\{C_{k_1},\pi_{k_1},C_{\sigma_{\mathrm{bk1}}},\pi_{\mathrm{bk1}},C_{\sigma_{\mathrm{uk1}}},\pi_{\mathrm{uk1}},C_{\sigma_{\mathrm{Acc}}},\pi_{\mathrm{Acc}},\pi_{w_i}\}$.

4.6 传递协议

传递协议允许 U_1 把电子现金 coin_1 花费给 U_2(商家 M 可以是任何用户 U_i),U_2 可以选择继续花费该电

子现金给 U_3,或者把电子现金存入银行,如果要存入银行,就执行下面的存款协议,否则就执行传递协议,在此我们给出 U_i 把电子现金花费给 U_{i+1}的传递协议,具体的传递协议如下:

(1) $U_{i+1}\rightarrow U_i$: U_{i+1}向 U_i 发送序列号 k_{i+1}.

(2) $U_i\rightarrow U_{i+1}$: U_i 利用花费链构建法,检查 k_{i+1}的正确性,即 $k_{i+1}=g_0^{k_i(\mathrm{mod}q)}(\mathrm{mod}p)$是否成立,如果不成立,协议终止,否则为避免电子现金可链接性,防止攻击者链接 U_i 提取的电子现金和花费的电子现金, U_i 先利用 Groth-Sahai 承诺和证明的可更新性,把 coin_{i-1}中不变的部分更新为 $\mathrm{coin}'_{i-1}=\{C_{k_1}^{i-1},\pi_{k_1}^{i-1},C_{\sigma_{\mathrm{bk1}}}^{i-1},\pi_{\mathrm{bk1}}^{i-1},C_{\sigma_{\mathrm{Acc}}}^{i-1},\pi_{\mathrm{Acc}}^{i-1},\pi_{w_i}^{i-1}\}$.然后 U_i 利用存款银行的承诺密钥 $\mathrm{ck}_{\mathrm{DB}}$对序列号 k_i 生成承诺 C_{k_i},以及对应的证明 π_{k_i}, U_i 也利用算法 Sig-Com 对承诺 $C_{k_1}^{i-1}$和 C_{k_i}生成承诺签名 $C_{\sigma_{\mathrm{uk}i}}$,以及对应的证明 $\pi_{\mathrm{uk}i}$.最后 U_i 发送给 U_{i+1}电子现金 $\mathrm{coin}_i=\{C_{k_1}^{i-1},\pi_{k_1}^{i-1},C_{\sigma_{\mathrm{bk1}}}^{i-1},\pi_{\mathrm{bk1}}^{i-1},C_{k_i},\pi_{k_i},C_{\sigma_{\mathrm{uk}i}},\pi_{\mathrm{uk}i},C_{\sigma_{\mathrm{Acc}}}^{i-1},\pi_{\mathrm{Acc}}^{i-1},\pi_{w_i}^{i-1}\}$.

(3) U_{i+1}: U_{i+1}验证 coin_i 中证明$\pi_{k_1}^{i-1},\pi_{\mathrm{bk1}}^{i-1},\pi_{k_i},\pi_{\mathrm{uk}i},\pi_{\mathrm{Acc}}^{i-1},\pi_{w_i}^{i-1}$的正确性,如果不正确,协议终止,否则 U_{i+1}给 U_i 提供商品或者服务.

4.7 存款协议

当用户 U_j 不想继续花费电子现金时,就把电子现金 coin_j 存入银行,在存入存款银行以前,为保持电子现金的不可链接性, U_j 利用 Groth-Sahai 承诺和证明的可更新性,把 coin_j 更新为 coin'_j.

在存款银行收到电子现金 coin'_j 后,验证 coin'_j 中证明$\pi_{k_1}^j,\pi_{\mathrm{bk1}}^j,\pi'_{k_j},\pi'_{\mathrm{uk}j},\pi_{\mathrm{Acc}}^j,\pi_{w_j}^j$的正确性,如果不正确,协议终止,否则 DB 利用提取密钥 $\mathrm{ek}_{\mathrm{DB}}$从 $C_{k_j}^j$中提取序列号 k_j,并从数据库 db 中,查找 $\mathrm{ek}_{\mathrm{DB}}$是否存在相同的序列号,如果没有,说明此电子现金没有发生重复花费,给 U_j 的账户存入等值的电子现金,否则说明此电子现金被重复花费,此时存款银行从 C'_{k_j}中提取出 U_j 的序列号 k_j,利用花费链构建法,存款银行可以计算出一个花费链 $k_1,k_2,\cdots,k_j$,同时存款银行也能从数据库 db 中找到另一个 k_1 开始的花费链 $k_1,k_2,\cdots,k_i$,且 $i\neq j$.存款银行就能从 k_1 开始,从这两个花费链中找到相同序列号的最后一个序列号 k_t,然后把 k_t 以及相应的两个电子现金 coin'_t 和 coin'_j 发送给可信第三方,可信第三方在验证电子现金 coin'_t 和 coin'_j 的正确性后,根据序列号 k_t 恢复出用户的公钥 pk_{U_t}.

5 效率分析与比较

本节分析并对比文献[13]、文献[14]和新协议的效率,我们用 C 表示所需做的承诺次数,GS 表示所需做的零知识证明次数, V 表示要验证的零知识证明次数, L_C 表示一个承诺的长度, L_{GS}表示一个零知识证明的长度.具体的分析见表 1.

表 1 协议计算效率和传递电子现金大小的比较

	取款协议(U)	传递协议($U_i\rightarrow U_{i+1}$)		存款协议(B)	传递电子现金大小
文献[13]	$5C+3\mathrm{GS}$	U_i	$(9+6i)C+1V+(7+4i)\mathrm{GS}$	$(5+4i)V+(n+1)E$	$(8+4i)L_C+(5+4i)L_{\mathrm{GS}}$
		U_{i+1}	$5C+3\mathrm{GS}$		
文献[14]	$5C+5\mathrm{GS}$	U_i	$(9+6i)C+1V+(11+8i)\mathrm{GS}$	$(5+8i)V+(n+1)E$	$(16+8i)L_C+(11+6i)L_{\mathrm{GS}}$
		U_{i+1}	$5C+4\mathrm{GS}$		
新协议	$2C+1V+2\mathrm{GS}$	U_i	$5C+1V+6\mathrm{GS}$	$6V$	$5L_C+6L_{\mathrm{GS}}$
		U_{i+1}	$6V$		

由表 1,可以知道,新协议在取款协议、传递协议和存款协议中,用户和银行的计算量都优于文献[13]和文献[14].而且新协议在传递中电子现金的大小是常量,但是文献[13]和文献[14]在传递中电子现金的大小和传递的次数成正比.因此新协议比文献[13]和文献[14]更实用.

6 安全证明

我们利用攻击者 A 和挑战者 c 之间的一系列实验序列,在标准模型下证明新协议的安全性.具体的安全证明如下:

定理 1 如果交互签名是不可伪造的,并且有限累加器的累加具有有限性,则新协议是不可伪造的;如果 Groth-Sahai 证明具有零知识性,且 SXDH 假设成立,则新协议具有匿名性(全匿名性、完美匿名性 1 和完美匿名性 2);如果交互签名是不可伪造的,则新协议具有不可重复花费性;如果 Groth-Sahai 证明具有零知识性,并且交互签名是不可伪造的,则新协议具有不可诬陷性.

7 结束语

本文首次提出花费链构建法,同时利用 Groth-Sahai 证明系统和累加器原理,在标准模型下,构建了一个最优匿名的等长可传递电子现金系统.基于花费链,用户无需存储任何花费凭证,银行就可以直接计算出已经

传递过该电子现金的用户;与现有的系统相比,新系统传递的电子现金长度是常量;在安全性上,新系统具有最优匿名性,即同时满足全匿名性、完美匿名性 1 和完美匿名性 2.同时我们在标准模型下给出系统的安全性证明.

参考文献

[1] T Okamoto, K Ohta. Disposable zero-knowledge authentications and their applications to untraceable electronic cash[A]. CRYPTO'89[C]. Santa Barbara, California, USA: Springer New York, 1990.481 – 496, .

[2] T Okamoto, K Ohta. Universal electronic cash[A]. CRYPTO'91[C]. Santa Barbara, California, USA: Springer Berlin Heidelberg, 1992.324 – 337.

[3] D Chaum, T P Pedersen. Transferred cash grows in size[A]. EUROCRYPT'92[C]. Balatonfüred, Hungary: Springer Berlin Heidelberg, 1993.390 – 407.

[4] R S Aand, C E V Madhavan. An online, transferable E-cash payment system[A]. Indocrypt'00[C]. Calcutta, India: Springer Berlin Heidelberg, 2000.93 – 103.

[5] I R Jeong, D H Lee, J I Lim. Efficient transferable cash with group signatures[A]. ISC'01[C]. Malaga, Spain: Springer Berlin Heidelberg, 2001.462 – 474.

[6] J K Lin, S H Wong, D S Wong. Transferable E-cash revisit[A]. IFIP'05[C]. Chiba, Japan: Springer US, 2005.171 – 188.

[7] 李梦东,杨义先.无可信第三方的离线电子现金的匿名性控制[J].电子学报,2005,3(33):456 – 458.
Li Meng-dong, Yang Yi-xian. Revocable anonymous off-line E-cash scheme without TTP[J]. Acta Electronica Sinica, 2005, 3(33):456 – 458.(in Chinese)

[8] S Canard, A Gouget, J Traore. Improvement of efficiency in (unconditional) anonymous transferable E-cash[A]. FC'08[C]. Cozumel, Mexico: Springer Berlin Heidelberg, 2008.202 – 214.

[9] S Canard, A Gouget. Anonymity in transferable E-cash[A]. ACNS'08[C]. New York, NY, USA: Springer Berlin Heidelberg, 2008.207 – 223.

[10] M Blanton. Improved conditional E-payments[A]. ACNS'08[C]. New York, NY, USA: Springer Berlin Heidelberg, 2008.188 – 206.

[11] 刘文远,张江霄,胡庆华,谷秀芝.可直接计算高效可分电子现金系统[J].电子学报.2009,2(37):368 – 371.
Liu Wen-yuan, Zhang Jiang-xiao, Hu Qing-hua, Gu Xiu-zhi. Divisible E-cash system with direct computation and efficiency[J]. Acta Electronica Sinica, 2009, 2(37):368 – 371.(in Chinese)

[12] G Fuchsbauer, D Pointcheval, D Vergnaud. Transferable constant size fair E-cash[A]. CANS'09[C]. Kanazawa, Japan: Springer Berlin Heidelberg, 2009.226 – 247.

[13] OBlazy, S Canard, G Fuchsbauer, A Gouget, H Sibert, J Traore. Achieving optimal anonymity in transferalbe E-cash with a judge[A]. AFRICACRYPT'11[C]. Dakar, Senegal: Springer Berlin Heidelberg, 2011.206 – 223.

[14] J X Zhang, Z J Li, H Guo. Anonymous transferable conditional E-cash[A]. Secure Comm'12[C]. Padua, Italy: Springer Berlin Heidelberg, 2013.45 – 60.

[15] 张江霄,郭华,李舟军.基于逆序二叉树的高效可分电子现金系统[J].电子与信息学报,2014,1(36):22 – 26.
Zhang Jiang-xiao, Guo Hua, Li Zhou-jun. Efficient divisible E-cash system basedon reverse binary tree[J]. Journal of Electronics and Information Technology, 2014, 1(36):22 – 26.(in Chinese)

[16] J Groth, A Sahai. Efficient non-interactive proof systems for bilinear groups[A]. EUROCRYPT'08[C]. Istanbul, Turkey: Springer Berlin Heidelberg, 2008.415 – 432.

[17] M H Au, Q Wu, W Susilo, Y Mu. Compact E-cash from bounded accumulator[A]. CT-RSA'07[C]. San Francisco, CA, USA: Springer Berlin Heidelberg, 2007.178 – 195.

[18] J Camenisch, M Kohlweiss, C Soriente. An accumulator based on bilinear maps and efficient revocation for anonymouscredential[A]. PKC'09[C]. Irvine, CA, USA: Springer Berlin Heidelberg, 2009.481 – 500.

[19] G Fuchsbauer. Commuting signatures and verifiable encryption[A]. CRYPTO'11[C]. California, USA: Springer Berlin Heidelberg, 2011.224 – 245.

作者简介

张江霄　男,1983 年 2 月生,河北邢台人.2014 年获得北京航空航天大学计算机网络与信息安全博士学位.现为邢台学院数学与信息科学技术学院讲师.主要研究兴趣为电子现金、网络与信息安全.

E-mail: orange_0092008@163.com

李舟军　男,1963 年 9 月生,湖南湘乡人.1999 年获国防科技大学计算机博士学位.现为北京航空航天大学计算机学院信息安全系主任、教授、博士生导师.主要研究兴趣为网络与信息安全、数据挖掘与社交网络分析.

E-mail: lizj@buaa.edu.cn