基于智能卡的无证书离线电子现金方案

唐 洋, 常友渠, 徐 倩
(重庆电力高等专科学校, 重庆 400053)

摘 要: 无证书密码体制避免了基于 PKI 密码体制的证书管理负担和基于身份密码体制的密钥托管问题。提出一种无证书的部分盲签名机制,并以此为基础,使用部分盲签名产生电子货币,利用智能卡防窜改技术防止电子货币的重复消费行为,设计了一种无证书的离线电子现金方案。新的部分盲签名机制是可证明安全的,仅需要三次对运算,计算性能较优。电子现金方案无须电子银行在线支持,在实现预付电子现金的同时能有效防止重复消费,并且计算开销和通信开销都低于其他无证书电子现金方案,可适用于移动电子支付场景。

关键词: 部分盲签名; 无证书; 电子现金; 离线支付; 智能卡
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)03-1095-05
doi:10.3969/j.issn.1001-3695.2012.03.081

Certificateless offline e-cash scheme based on smart card

TANG Yang, CHANG You-qu, XU Qian
(*Chongqing Electric Power College*, *Chongqing* 400053, *China*)

Abstract: The certificateless cryptography avoids the certificate management burden that exists in the PKI-based cryptography and the key escrow issue of identity-based cryptography. This paper proposed a certificateless partially blind signature scheme, and was used to generate the electronic money. It also proposed a certificateless offline electronic cash scheme, and adopted the tamper-proof smart card to prevent the double-spending of the electronic money. The new partially blind signature was provably secure, and it had better computing performance-only three times pairing calculation. The new e-cash scheme, without the online e-banking, realized the prepaid electronic cash, and could effectively prevent the double-spending of the electronic money. The computational costs and the communication overheads of the e-cash scheme are lower than the other certificateless ones. So, the new scheme can be used for the payment in the mobile scenarios.

Key words: partially blind signature; certificateless; electronic cash; offline payment; smart card

0 引言

无证书的公钥密码体制是由 Al-Riyami 等人[1]首次提出,被用于解决基于身份公钥密码体制中的密钥托管问题,同时又继承了基于身份公钥密码体制的优点,不使用公钥证书,解决了基于证书公钥系统的证书管理问题。随后几年中,无证书的公钥密码体制得到了国内外研究者的广泛关注。

盲签名概念由 Chaum[2]提出,与一般数字签名不同,签名者并不知道他所签发文件的具体内容,且不能将签名过程与最终所得的签名对应起来,这种特性称为盲性。盲签名被广泛应用于具有匿名性要求的领域(如电子支付或匿名的电子选举等)。然而在完全盲签名中,签名者不知道最终签名的任何信息,这样的签名系统是不完善的,可能造成签名被非法使用等问题。部分盲签名[3]克服了完全盲签名的这一缺点,允许将客户与签名者协商好的公共信息嵌入到签名中,以便在签名者不知道所签署消息具体内容的情况下有效保护签名者的合法权益。

一些研究者提出了无证书的部分盲签名机制[4~6]。苏万力等人[4]的部分盲签名机制计算开销较高;李明祥等人[5]提出的方案存在公共协商信息替换攻击;余丹等人[6]提出的方案在签名验证阶段没有使用 KGC 的公钥,存在签名公钥替换攻击(无证书的签名方案不再依靠公钥证书验证用户公钥的有效性,必须依赖在签名算法中嵌入 KGC 的公钥参数来确保系统的安全性)。

最近,Zhang 等人[7]提出一种基于无证书部分盲签名的电子现金方案,但是,他们提出的部分盲签名机制共需要五次对运算(对运算的计算开销远高于其他运算),计算性能较低。并且,该电子现金方案采用银行在线验证方式检验电子货币的有效性及重复消费行为,通信开销较大。

针对上述不足,本文提出一种新的无证书部分盲签名机制,并以此为基础构建了一个离线电子现金系统。新签名机制不仅满足协商信息不可替换,且仅需要三次对运算,计算开销较优。采用智能卡防窜改技术在实现离线支付和预付电子现金的同时能有效防止电子货币的重复消费。

1 背景知识

1.1 双线性映射及困难数学问题

假设 G_1 和 G_2 分别是素阶为 q 的循环加法群和循环乘法群,定义 $e: G_1 \times G_1 \rightarrow G_2$ 为满足以下性质的双线性映射:

a) 双线性性: 对于 $\forall (P, Q) \in G_1$ 和 $\forall (a, b) \in Z_q^*$ 有

收稿日期: 2011-07-28; **修回日期**: 2011-09-07

作者简介: 唐洋(1981-),男,重庆人,讲师,硕士,主要研究方向为计算机网络技术、计算机应用(dztyang@163.com);常友渠(1979-),女,重庆人,讲师,硕士,主要研究方向为计算机应用;徐倩(1981-),女,重庆人,硕士,主要研究方向为计算机信息管理.

$e(aP,bQ)=e(P,Q)^{ab}$;

b)非退化性:存在$(P,Q)\in G_1$ 满足 $e(P,Q)\neq 1$;

c)可计算性:对于$\forall(P,Q)\in G_1$,能有效计算 $e(P,Q)$。

双线性映射理论存在以下困难数学问题:

a)k-CAA 问题(collusion attack algorithm with traitors)。对于整数 k 和任意的 $x\in Z_q^*$,已知 $P\in G_1$, xP, $h_1,h_2,\cdots,h_k\in Z_q^*$,$(x+h_1)^{-1}P$, $(x+h_2)^{-1}P,\cdots,(x+h_k)^{-1}P$,计算$(x+h)^{-1}P$, 其中 $h\notin\{h_1,h_2,\cdots,h_k\}$。

b)mICDH 问题(modified inverse computational Diffie-Hellman problem)。对于 $a,b\in Z_q^*$,已知 b、$P\in G_1$ 和 aP,计算$(a+b)^{-1}P$。

1.2 无证书部分盲签名及其安全模型

1.2.1 无证书的部分盲签名机制

无证书的部分盲签名方案主要包含七个算法:系统建立、部分私钥产生、设置秘密值、设置私钥、设置公钥、签名发布和签名验证。其中签名发布算法是签名者与请求者之间的交互协议,它包括签名(阶段 1)、盲化、签名(阶段 2)和去盲四个步骤。

系统建立:输入安全参数 k,输出系统参数 param。

部分私钥产生:输入(params,ID_i),输出 ID_i 的部分私钥 D_i。

设置秘密值:输入(params,ID_i),输出实体 ID_i 的长期私有秘密 x_i。

设置私钥:输入(params,ID_i, x_i, D_i),输出 ID_i 的签名私钥 S_i。

设置公钥:输入(params,ID_i, x_i),输出 ID_i 的公钥 P_i。

签名发布:假设签名者与请求者已协商好公共信息 c,则执行以下交互算法:

a)签名(阶段 1)。签名者选择随机值 r,输入公共信息 c,计算临时签名参数 U 并发送给请求者。

b)盲化。请求者选择随机值 α、β,输入待签名消息 m、协商信息 c 和签名参数 U,计算盲消息 U' 和 h,并发送 h 给签名者。

c)签名(阶段 2)。签名者输入(r,h,c),计算签名 W,并发送给请求者。

d)去盲。请求者输入(W,α,β),计算部分盲签名(U',W')。

签名验证。输入(param,ID,P_{ID},m,c,U',W'),如果验证签名有效则接受签名,否则拒绝。

1.2.2 无证书的部分盲签名的安全模型

无证书部分盲签名应满足三项主要安全要求:正确性、部分盲性和不可伪造性。正确性,即可验证性,是指由签名算法产生的有效签名一定能通过验证算法的验证。部分盲性,即无连接性,是指签名者不能通过公开信息将最终签名结果与具体的签名实例相对应。

不可伪造性是签名机制的基本安全属性,本文形式化地定义挑战者 C 和无证书体制[1]下的两类敌手 $\mathrm{A}\in\{A_I,A_{II}\}$ 之间的游戏来模拟部分盲签名机制不可伪造性(existential unforgeability of certificateless partially blind signature under adaptive chosen-message attack,EUF-CLPB-CMA2)。

第一类敌手 A_I 是一个外部的攻击者,他可以替换任何实体的部分公钥,获得部分实体的私钥,但不能获得 KGC 的主密钥和特定实体的部分私钥。

第二类敌手 A_{II} 模拟恶意但受限的 KGC,他拥有 KGC 的主密钥,可获得任何实体的部分私钥,但不能获得实体的私有秘密以及替换特定实体的公钥。

A_{II} 敌手用于分析无证书密码体制的无密钥托管特性。

EUF-CLPB-CMA2 Game:

Initialization:挑战者 C 输入安全参数 k,执行系统建立算法,输出系统公共参数 params。C 将 params 发送给 A。此外,对于 A_{II} 敌手,C 还将 KGC 的主密钥 s 发送给他。

Attack:敌手 A 可自适应地执行多项式时间有界的查询(每一次查询输出取决于前面的查询输出结果)。

a)Hash 查询:A 可以请求任意消息 x 的散列值 hash(x)。

b)部分私钥查询:A 提交一个身份 ID 给 C,C 计算用户部分私钥 D_{ID},并返回给 A;

c)私钥查询:A 提交一个身份 ID,挑战者 C 返回用户私钥 x_{ID} 给 A;

d)公钥查询:A 提交一个身份 ID,C 根据用户公钥生成算法生成用户 ID 的公钥 P_{ID},并发送给敌手 A;

e)公钥替换查询:对身份 ID,A 可以选择一个新的秘密值 x_{ID}^*,计算新公钥 P_{ID}^*,并用 P_{ID}^* 替换原有 P_{ID};

f)签名发布查询:A 选择身份 ID,公钥 P_{ID},明文 m 和协商的信息 c 提交给 C,C 返回签名结果 $\sigma=IS(m,c,\mathrm{ID},P_{\mathrm{ID}})$ 给 A;

g)签名验证查询:A 提交$(m,c,\mathrm{ID},P_{\mathrm{ID}},\sigma)$给 C,若验证签名 verify$(\sigma,m,c,\mathrm{ID},P_{\mathrm{ID}},P_0)=1$,C 返回 1,否则返回 0。

Forgery:最后,A 输出伪造签名 $(\sigma',m',c',\mathrm{ID}_I,P_I)$。这里,A 在 attack 阶段从未请求过对$(m',c',\mathrm{ID}_I,P_I)$的签名发布查询和签名验证查询;并且,对于 A_I 敌手,他从未请求针对 ID_I 的(部分)私钥查询,对于 A_{II} 敌手,他从未请求针对 ID_I 的私钥查询和公钥替换查询。如果 verify$(\sigma',m',c',\mathrm{ID}_I,P_I,P_0)=1$,那么敌手 A 赢得游戏。

敌手 A 赢得 EUF-CLPB-CMA2 游戏的优势定义为

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CLPB\text{-}CMA2}}(\mathrm{A})=Pr[\mathrm{A\ wins}]$$

定义 2 假设 k-CAA 和 mICDH 问题是多项式时间难解的,如果不存在敌手 $\mathrm{A}\in\{A_I,A_{II}\}$ 以不可忽略的优势赢得 EUF-CLPB-CMA2 游戏,那么无证书部分盲签名机制满足不可伪造性。

2 无证书部分盲签名

系统建立:系统参数 param$=\{G_1,G_2,e,P,g,q,P_0,H_1,H_2,H_3\}$。其中,$G_1$,$G_2$,$P$ 和 e 与前面方案类似;g 是 G_2 的生成元,且 $e(P,P)=g$;$P_0=sP$ 为 KGC 的公钥,对应的 $s\in Z_q^*$ 是 KGC 的主密钥;$H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:G_1\rightarrow Z_q^*$ 和 $H_3:\{0,1\}^*\times\{0,1\}^*\times G_2\times G_1\rightarrow Z_q^*$,$H_4:\{0,1\}^*\rightarrow G_1$ 是安全的散列函数。

部分私钥产生:输入(params,ID_i),KGC 计算 $q_A=H_1(\mathrm{ID}_i)$ 和 $D_i=(s+q_i)^{-1}P$ 并返回 D_i 作为 ID_i 的部分私钥。

设置秘密值:输入(params,ID_i),ID_i 随机选择 $x_i\in Z_q^*$ 作为其私有秘密。

设置私钥:输入(params,ID_i, x_i, D_i),ID_i 计算 $q_i=H_1(\mathrm{ID}_i)$, $Q_i=P_0+q_iP$, $R_i=x_iQ_i$, $y_i=H_2(R_i)$ 和 $w_i=(x_i+$

$y_i)^{-1}$,输出其私钥 $S_i=(w_i, D_i)$。

设置公钥:输入(params,ID_i,x_i),输出 ID_i 的公钥 $P_i=R_i=x_i(P_0+q_iP)$。

签名发布:用户 B 请求签名者 A 对消息 m 进行部分盲签名,c 是 A/B 双方共同协商的对消息 m 的说明信息,那么 A 和 B 执行以下交互协议。

a)签名(阶段 1)。签名者 A 选择随机数 $r\in Z_q^*$,计算 $U=g^r$ 并将 U 发送给用户。

b)盲化。用户随机选择 $\alpha,\beta\in Z_q^*$,计算 $Q=H_4(c)$,$g_1=e(Q,Q_A)$,$U'=U^{\alpha}g_1^{\alpha\beta}$,$v=H_3(m, c, U', ID_A)$ 和 $h=\alpha^{-1}v+\beta$,然后发送 h 给 A。

c)签名(阶段 2)。A 计算 $Q=H_4(c)$ 和 $W=rw_AD_A+hw_AQ$,将 W 返回给用户。

d)去盲。用户收到 W 后,计算 $W'=\alpha W$。得到对 (m, c) 的部分盲签名 (U', W')。

签名验证:验证者计算 $q_A=H_1(ID_A)$,$Q_A=P_0+q_AP$,$y_A=H_2(R_A)$,$Q=H_4(c)$ 和 $v=H_3(m, c, U', ID_A)$,验证等式 $e(W', R_A+y_AQ_A)=e(vQ, Q_A)U'$ 是否成立。若等式成立则接受签名,否则拒绝。

上述部分盲签名方案的正确性通过下式证明:

$$\begin{aligned}&e(W', R_A+y_AQ_A)=e(\alpha W,(x_A+y_A)Q_A)=\\&e(\alpha rw_AD_A+(v+\alpha\beta)w_AQ,(x_A+y_A)Q_A)=\\&e(w_AD_A,(x_A+y_A)Q_A)^{\alpha r}e(w_AQ,(x_A+y_A)Q_A)^{v+\alpha\beta}=\\&e(P,P)^{\alpha r}e(Q,Q_A)^{v+\alpha\beta}=g^{\alpha r}e(Q,Q_A)^{v+\alpha\beta}=\\&e(Q,Q_A)^{v}g^{\alpha r}e(Q,Q_A)^{\alpha\beta}=e(vQ,Q_A)U'\end{aligned}$$

3　无证书离线电子现金方案

新方案包含五类角色:KGC;电子银行经理 M,负责电子货币的签名和发布;客户 C,拥有一张智能卡;商家 V。无证书离线电子现金方案如下:

a)系统初始化。KGC 产生并发布系统参数;电子银行经理生成密钥对(S_M, P_M)(详见第 2 章)。

b)电子银行注册。假设客户在某银行拥有现金账户 I_C,向银行经理 M 进行注册。M 通过物理方式验证客户身份,并分配给客户一张智能卡(记为 S)作为用户的电子钱包。卡内存储$(ID_S, S_S, P_S, T, Cert_S)$。其中:$ID_S$ 是智能卡唯一标志,(S_S, P_S)是智能卡的公私密钥对;T 是智能卡有效期;$Cert_S=Sign_M(ID_S, P_S, T)$为电子银行经理 M 的签名(本文使用的无证书一般签名算法可参考文献[8],下同)。

c)电子钱币取款。假设客户与银行经理已协商公共信息 c,主要包括电子货币面额和使用日期等信息。客户使用电子钱包 S(智能卡)与银行经理 M 执行下列协议:

(a)M 选择随机数 $r\in Z_q^*$,计算 $U=g^r$ 并将 U 发送到 S;

(b)收到 U 后,S 随机选择 $\alpha,\beta\in Z_q^*$,计算 $Q=H_4(c)$,$g_1=e(Q, Q_M)$,$U'=U^{\alpha}g_1^{\alpha\beta}$,$v=H_3(m,c,U', ID_M)$(这里,$m$ 包含一个预定义格式的消息,用于检验电子货币的有效性)和 $h=\alpha^{-1}v+\beta$,然后发送 h 给 M;

(c)收到 h 后,M 计算 $Q=H_4(c)$ 和 $W=rw_MD_M+hw_MQ$,将 W 返回给 S,然后从客户账户中冻结相应款项(注意,冻结时间必须与电子货币使用期限保持一致)。

(d)S 收到 W 后,计算 $W'=\alpha W$,并存储 ecoin=$(U'\|W'\|c)$作为一个电子货币。

d)支付。当客户需要向供应商 V 支付电子货币,那么 S 与 V 执行下列协议:

(a)S 计算无证书签名 $\sigma=Sign_S(ecoin, ID_M, ID_V, P_{ID}, t)$,其中,$P_{ID}$ 是待购买的商品编号,t 是当前系统时间。然后将$(ecoin, ID_M, ID_V, P_{ID}, t, \sigma, ID_S, P_S, T, Cert_S)$发送给 V,并将对应的 ecoin 从电子钱包中删除(注意,为了确保电子货币不被重复消费,电子钱包必须是防窜改的)。

(b)收到消息后,V 验证 $Cert_S$、T 以及签名 σ。若验证不通过,则终止支付过程;否则计算 $q_M=H_1(ID_M)$,$Q_M=P_0+q_MP$,$y_M=H_2(R_M)$,$Q=H_4(c)$ 和 $v=H_3(m, c, U', ID_M)$,验证等式 $e(W', R_M+y_MQ_M)=e(vQ, Q_M)U'$ 是否成立。若等式不成立则终止支付过程,否则接受该电子货币并保存。

e)兑换:V 将电子货币 ecoin 和支付凭证 σ 发送给电子银行。银行经理首先查询该电子货币是否已兑换,然后验证所有证据有效,则从客户账户冻结款项中转出相应金额到供应商账户,并存储(ecoin,σ)。为了提高效率,供应商可一次兑换多个电子货币(注意,电子货币必须在有效期之前兑换)。

4　分析与比较

4.1　无证书部分盲签名安全性分析

4.1.1　部分盲性

部分盲性的定义可以参考文献[3],本文提出的部分盲签名方案满足部分盲特性。其证明思路如下:对于任意给定的一个有效的部分盲签名(m,c,U',W')以及在部分盲签名发布中产生的中间变量(U,g_1,v,h,W),总是存在一对唯一的随机盲因子(α,β),所以方案满足部分盲性。

定理 1　本文无证书部分盲签名方案满足部分盲性。

证明　对于给定的(U',W')和部分盲签名发布中产生的中间变量(U,g_1,v,h,W),考虑如下等式:

$$W'=\alpha W \tag{1}$$

$$h=\alpha^{-1}v+\beta \tag{2}$$

$$U'=U^{\alpha}g_1^{\alpha\beta} \tag{3}$$

根据以上等式可知,一定存在唯一的 $\alpha\in Z_q^*$ 使式(1)成立;进一步可以通过式(2)计算出唯一的 β,即 $\beta=h-\alpha^{-1}v$。因为(U', W')是有效的部分盲签名,所以下式成立:

$$e(W', R_A+y_AQ_A)=e(vQ, Q_A)U'$$

由此可推断出下式成立:

$$e(Q, Q_A)^{v}g^{\alpha r}e(Q, Q_A)^{\alpha\beta}=e(vQ, Q_A)U'$$

进而推断出式(3)也成立。因此,盲因子 α、β(在部分盲签名的生成中总是存在。由定义可知,本方案满足部分盲性。

4.1.2　不可伪造性

定理 2　若存在 A_I 敌手能够在概率多项式时间 t 内以 $\varepsilon\geqslant 10(q_{is}+q_1)(q_{is}+q_2)/2^k$ 的优势赢得 EUF-CLPB-CMA2 游戏。假设 A_I 最多进行 q_i次 H_i查询($i=1,2,3,4$)、q_s 次私钥查询、q_p 次公钥替换查询和 q_{is}次签名发布查询,则存在算法 C 能够在概率多项式时间内以 $\tau\geqslant\varepsilon/12q_1q_{is}$ 的优势解决 k-CAA 问题。

证明　定理 2 的证明可归结为 A_I敌手求解 k-CAA 问题。给出一个 k-CAA 问题实例(假设 A_I已知 $P_0=sP,q_1,q_2,\cdots,q_k$,$(s+q_1)^{-1}P,(s+q_2)^{-1}P,\cdots,(s+q_k)^{-1}P$(这里分别对应 k 个已被攻破的签名实体即 A_I 已获得这 k 个实体的部分私钥),

$q_A \notin \{q_1, q_2, \cdots, q_k\}$(即 ID_A 未被攻破)),演示 C 如何利用 A_I 解决 k-CAA 问题。首先,C 以 A_I 为子程序并充当 EUF- CLPB-CMA2 游戏中的挑战者。

Initialization:C 产生并发送 params 给 A_I,维持初始为空的列表 L_1, L_3, L_4, L_{PK}, L_{IS}分别用于跟踪 A_I 对预言机 H_1,H_3, H_4,公/私钥和签名发布查询。

Attack:A_I 自适应地执行多项式时间有界的查询。

a)H_1 查询。当收到 $H_1(ID_i)$查询时,C 首先查询 L_1(格式为(ID,q,d)),若(ID_i, q_i, d_i)已存在,则返回 q_i;否则,C 随机选择 $q_i \in Z_q^*$,如果 $ID_i = I$,设置 $d_i = \perp$,否则计算 $d_i = (s + q_i)^{-1}$,将(ID_i, q_i, d_i)插入 L_1,并返回 q_i。

b)H_2 查询。当收到 $H_2(R_i)$查询时,C 首先查询 L_{PK}(格式为(ID,R,x,y)),若(ID_i, R_i, x_i, y_i)已存在,则返回 y_i;否则,C 随机选择 $y_i \in Z_q^*$,返回 y_i。

c)H_3 查询。当收到 $H_3(m,c,U',ID_i)$查询时,C 首先查询 L_3(格式为(ID,m,c,U',v)),若(ID_i,m_i,c_i,U',v_i)已存在,则返回 v_i;否则,C 随机选择 $v_i \in Z_q^*$,将(ID_i,m_i,c_i,U',v_i)插入 L_3,并返回 v_i。

d)H_4 查询。当收到 $H_4(c_i)$查询时,C 首先查询 L_4(格式为(c,Q)),若(c_i,Q_i)已存在,则返回 Q_i;否则,C 随机选择 $Q_i \in G_1$,将(c_i,Q_i)插入 L_4,并返回 Q_i。

e)部分私钥查询。当收到对 ID_i 的部分私钥查询时,如果 $ID_i = I$,C 终止模拟(事件 1);否则 C 执行 $H_1(ID_i)$查询并检索 L_1,然后返回 d_i。

f)私钥查询。当收到对 ID_i 的私钥查询时,C 查询 L_{PK},若(ID_i, R_i, x_i, y_i)已存在则返回 $w_i = (x_i + y_i)^{-1}$;否则 C 执行对 ID_i 的公钥查询和 H_2 查询,并返回 $w_i = (x_i + y_i)^{-1}$。

g)公钥查询。当收到对 ID_i 的公钥查询时,C 首先查询 L_{PK},若(ID_i, R_i, x_i, y_i)在 L_{PK}中存在,则返回 R_i;否则 C 随机选择 $x_i \in Z_q^*$,并查询 L_1,计算 $Q_i = P_0 + q_iP$,$R_i = x_iQ_i$,然后执行 H_2 查询,取得 y_i,将(ID_i,R_i,x_i,y_i)插入 L_{PK},返回 R_i。

h)公钥替换查询。当收到对 ID_i 的公钥替换查询时,C 用 R_i^* 替换原有 R_i,然后用$(ID_i, R_i^*, \perp, \perp,)$更新 L_{PK}。注意,这里需要 A_I 提供 R_i^*。

i)签名发布查询。当收到 $IS(m_i,c_i,ID_i,P_i)$查询,如果 $ID_i = I$, $m_i = m'$, $c_i = c'$,则 C 终止模拟(事件 2);否则 C 查询 L_{IS}(格式为(m,c,ID,P,U',W')),如果$(m_i,c_i,ID_i,P_i,U_i',W_i')$已存在,则返回$(U_i',W_i')$,否则 C 按下列步骤执行:

(a)执行前述相应查询;

(b)如果 $ID_i = I$, 随机选择 $W_i' \in G_1$,计算 $U_i' = e(W_i', R_I + y_I(P_0 + q_IP))e(v_iQ_i, P_0 + q_IP)^{-1}$;

(c)否则,如果 $ID_i \neq I$, 随机选择 $r,\alpha,\beta \in Z_q^*$,计算 $U_i' = g^{r\alpha}e(Q_i, P_0 + q_iP)^{\alpha\beta}$和 $W_i' = r\alpha w_i d_i P + v_i\beta w_i Q_i$;

(d)将$(m_i,c_i,ID_i,P_i,U_i',W_i')$插入 L_{IS},用(ID_i,m_i,c_i,U',v_i)更新 L_2,返回(U_i', W_i')。

j)签名验证查询。当收到对(U_i',W_i',m_i,c_i,ID_i)的签名验证查询,C 查询 L_1、L_3 和 L_{PK},如果相应列表中不存在(q_i, v_i, Q_i, R_i)中任一项,则拒绝该签名验证;否则,若验证签名 verify $(U_i',W_i',m_i,c_i,ID_i,P_i,P_0) = 1$,C 返回 1,否则返回 0。

Forgery:经过概率多项式次数上述查询后,A_I 从 $W_i'(i \in [1, q_{is}])$中随机选择 $W', r,\alpha,\beta \in Z_q^*$,计算 $Q' = H_4(c')$,$U' = g^{r\alpha}e(Q', P_0 + q_IP)^{\alpha\beta}$, $v' = H_3(m',c',U',ID_I)$和 $h' = \alpha^{-1}v' + \beta$,输出对$(m',c')$的伪签名 $\sigma' = (U', W')$。若伪造签名成功,则 C 输出 $D_I = \alpha^{-1}r^{-1}(x_I + y_I)(W' - h'w_IQ') = (s + q_I)^{-1}P$ 作为解决 k-CAA 问题的回答。

若事件 1/事件 2 发生,则 A_I 失败,失败的概率$\geqslant 1/q_1q_{is}$。假设 A_I 最多进行 q_i次 H_i查询$(i = 1,2,3,4)$、q_s 次私钥查询、q_p 次公钥替换查询和 q_{is}次签名发布查询,根据二分引理[9],如果 A_I 以 $\varepsilon \geqslant 10(q_{is} + q_1)(q_{is} + q_2)/2^k$ 的优势赢得 EUF-CLPB-CMA2 游戏,那么 C 解决 k-CAA 问题的优势为 $\tau \geqslant \varepsilon/12q_1q_{is}$。证毕。

定理 3 若存在 A_{II}敌手,能够在概率多项式时间 t 内以 $\varepsilon \geqslant 10(q_{is} + q_1)(q_{is} + q_2)/2^k$ 的优势赢得 EUF-CLPB-CMA2 游戏。假设 A_{II}最多进行 q_i次 H_i查询$(i = 1,2,3,4)$、q_s 次私钥查询、q_p 次公钥替换查询和 q_{is}次签名发布查询,则存在算法 C 能够在概率多项式时间内以 $\tau \geqslant \varepsilon/12q_sq_pq_{is}$的优势解决 mICDH 问题。

证明 与定理 2 的证明类似。给出一个 mICDH 问题实例,$a,b \in Z_q^*$,已知 b、$P \in G_1$ 和 aP,计算$(a + b)^{-1}P$,演示 C 如何利用 A_{II}解决 mICDH 问题。C 以 A_{II}为子程序并充当 EUF-CLPB-CMA2 游戏中的挑战者。

Initialization:C 产生并发送 params 和主密钥 s 给 A_{II},维持初始为空的列表 L_1、L_3、L_4、L_{PK}、L_{IS}分别用于跟踪 A_I 对预言机 H_1,H_3, H_4, 公/私钥和签名发布查询。

Attack: A_{II}敌手自适应地执行多项式时间有界的查询,查询过程同定理 2。不同之处在于,A_{II}被允许执行任意身份的部分私钥查询,但不被允许执行 ID_I 的私钥查询(事件 1)和公钥替换查询(事件 3)(事件 2 同定理 2)。

Forgery:经过概率多项式次数上述查询后,A_{II}随机选择 $W' \in G_1$, $r,\alpha,\beta \in Z_q^*$,计算 $Q' = H_4(c')$, $U' = g^{r\alpha}e(Q', P_0 + q_IP)^{\alpha\beta}$, $v' = H_3(m',c',U',ID_I)$和 $h' = \alpha^{-1}v' + \beta$,输出对$(m', c')$的伪签名 $\sigma' = (U', W')$。若伪造签名成功,则 C 输出$(x_I + y_I)^{-1}P = (\alpha r d_I - h')^{-1}W'$作为解决 mICDH 问题的回答。

若事件 1/事件 2/事件 3 发生,则 C 失败,失败的概率$\geqslant 1/q_sq_pq_{is}$。根据二分引理[9],如果 A_{II}以 $\varepsilon \geqslant 10(q_{is} + q_1)(q_{is} + q_2)/2^k$ 的优势赢得 EUF-CLPB-CMA2 游戏,那么 C 解决 mICDH 问题的优势为 $\tau \geqslant \varepsilon/12q_sq_pq_{is}$。证毕。

定理 4 假设 k-CAA 和 mICDH 问题是多项式时间难解的,那么本文提出的无证书部分盲签名机制满足 EUF-CLPB-CMA2 安全性。

证明 定理 4 可由定理 2 和 3 直接推导得到。证毕。

4.1.3 协商信息不可替换

在实际应用中,协商信息被替换会导致盲签名被滥用。在李明祥等人方案中存在协商信息替换攻击,本文方案改进了这一缺陷。

假设协商信息 c 被替换为 c',验证者计算 $Q' = H_4(c')$,而签名者对原有信息 $Q = H_4(c)$进行签名得到 hSK_AQ,那么验证者计算:

$$e(W', R_A + y_AQ_A) = e(Q, Q_A)^v g^{\alpha r} e(Q, Q_A)^{\alpha\beta} = e(vQ, Q_A)U' \neq e(vQ', Q_A)U'$$

如果要使得下式成立:

$$e(\alpha hSK_AQ, R_A + y_AQ_A) = e(vQ', Q_A)e(Q', Q_A)^{\alpha\beta} \quad (4)$$

这里存在求解离散对数问题,即对于未知的 $a,b\in Z_q^*$ 给定 $aP,bP\in G_1$,求解 $x\in Z_q^*$ 使得 $axP=bP$。令 $Q=aP,Q'=bP$,根据双线性映射原理,不能由 Q 和 Q'求解 a 和 b。那么,签名请求者必须求解 $x\in Z_q^*$ 使得 $xQ=Q'$。计算 $h=x(\alpha^{-1}v+\beta)$ 使得 $\alpha hSK_AQ=x(v+\alpha\beta)SK_AQ=(v+\alpha\beta)SK_AQ'$。根据离散对数问题难解假设,本文部分盲签名方案满足协商信息不可替换。

4.2　电子现金安全性分析

电子现金方案应满足不可伪造性、用户匿名性和消费行为可追踪性,此外还应当具有防止电子现金重复消费行为的能力。

4.2.1　不可伪造性

电子现金方案的不可伪造性包括电子货币(ecoin)、电子钱包证书($Cert_S$)和支付凭证(σ)的不可伪造性。

电子现金不可伪造性由本文提出的无证书部分盲签名机制的不可伪造性确保。根据定理 4,在 k-CAA 和 mICDH 问题难解的假设下,本文提出的无证书部分盲签名机制满足不可伪造性,进而本文提出的无证书电子现金方案满足电子现金不可伪造性。

电子钱包证书和支付凭证不可伪造性由文献[8]提出的无证书签名机制的不可伪造性确保。文献[8]已证明该无证书签名机制满足不可伪造性,这里不再详述。

4.2.2　用户匿名性

在支付阶段,供应商仅仅与客户的电子钱包进行交互,所有证据由电子钱包的私钥签名,电子钱包与客户身份无直接联系。因此,供应商不能从支付凭证中获得客户的任何身份信息。此外,根据 4.1.1 节,本文提出的无证书部分盲签名机制满足部分盲性,且电子货币仅由电子银行经理签名,不包含客户的任何身份信息,故供应商不能从电子货币中取得客户身份信息。可见,本文电子现金方案满足支付阶段的用户匿名性。

4.2.3　防止电子货币重复消费

防止电子货币的重复消费行为是电子现金机制的一项重要属性,是指电子货币只能被使用一次。在现有许多电子现金方案中采用电子银行在线服务方式验证电子货币是否被重复使用,即:在支付阶段,供应商收到电子货币后,需要通过在线方式将电子货币发送给银行,由银行来验证电子货币是否已被使用,并返回验证结果。这种方式增加了系统的通信开销,同时需要银行在线支持,容易遭受 DoS 攻击,并且降低了系统的灵活性。本文采用智能卡来防止电子货币的重复消费行为,无须银行在线支持,因此实现了离线支付。基于电子钱包(智能卡)是防窜改的假设,电子钱包一旦签发,任何人不能随意窜改电子钱包的数据,不能修改电子钱包协议。在支付阶段,电子货币在第一次使用后即被删除,因此不可能被重复使用。

此外,本文的电子现金方案是完备的。如果支付不成功,而电子货币已被删除,那么被冻结的款项将在该电子货币使用期限结束之后立即返还到客户的现金账户。

4.3　性能分析与比较

表 1 比较了本文提出的无证书部分盲签名方案与其他三种类似方案[5~7]的计算性能。这里,T_p 表示对运算开销,T_s 表示 G_1 中标量乘的计算开销,T_e 表示 G_2 中模指数运算的计算开销,T_h 表示 map-to-point 哈希函数的计算开销。根据文献[10],可以得到如下关系:$1T_p\approx 1440t_m$, $1T_s\approx 29t_m$, $1T_e\approx 21t_m$, $1T_h\approx 23t_m$(t_m 是整数域上的乘法运算,表示一个基本计算单元)。

表 1　计算性能比较　　次数

方案	Issue 算法	Verify 算法	总开销
方案 1[5]	$1T_p+7T_e+3T_s$	$1T_p+2T_e+2T_s$	$\approx 3214t_m$
方案 2[6]	$2T_p+3T_e+2T_s$	$2T_p+2T_e$	$\approx 5923t_m$
方案 3[7]	$2T_p+1T_e+6T_s+1T_h$	$3T_p+1T_e+1T_h$	$\approx 7462t_m$
本文方案	$1T_p+3T_e+3T_s+2T_h$	$2T_p+3T_s+1T_h$	$\approx 4626t_m$

从表中对比看,本文方案的计算性能略低于方案 1,优于其他两种无证书的部分盲签名方案。但是方案 1 和 2 存在安全缺陷。

表 2 对几种电子现金方案的功能和性能进行了对比。

表 2　电子现金方案功能比较

方案	支付方式	不可伪造性	匿名性	防止重复消费	电子现金生成算法
方案 1[11]	在线	是	是	是	盲签名
方案 2[12]	离线	是	是	否	代理签名
方案 3[13]	离线	是	是	是	部分盲签名
方案 4[7]	在线	是	是	是	部分盲签名
本文方案	离线	是	是	是	部分盲签名

从表中可以看出,方案 2 虽然实现了离线支付方式,但是仅实现了电子货币重复消费行为的可追踪性,不能有效防止重复消费行为。上述电子现金方案中,仅方案 4 采用了无证书的部分盲签名生成电子货币。根据表 1,方案 4 提出的签名机制计算开销明显高于本文提出的签名机制,并且该方案需要银行在线验证电子货币,可知其计算开销和通信开销均高于本文方案。方案 1 采用基于 RSA 算法的盲签名机制,根据文献[14],如果实现相同安全级别,RSA 算法的计算开销更高于基于双线性映射的密码体制的计算开销。在方案 2 中,采用了大量对运算,其总的计算性能较低。方案 3 采用基于 PKI 的部分盲签名算法,由于需要进行公钥证书验证,增加了一定的计算开销,总的计算性能有所降低。总体来看,本文提出的电子现金方案计算性能较优。

5　结束语

文章指出了李明祥等人提出的无证书部分盲签名方案存在公共协商信息替换攻击,在此方案基础上提出一种新的无证书部分盲签名机制改进了这一缺陷,并以此为基础构建了一个无证书的离线电子现金系统。新提出的签名机制是可证明安全的,且计算开销较优。电子现金方案采用智能卡技术在实现离线支付和预付电子现金的同时能有效防止电子货币的重复消费行为,且计算开销和通信开销较优。

参考文献:

[1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]//Proc of ASIACRYPT 2003. Berlin: Springer-Verlag, 2003: 452-473.

[2] CHAUM D. Blind signatures for untraceable payments [C]// Advances in Crypto'82. 1982: 199-203.

(下转第 1110 页)

局部频繁项集的加/解密计算;而 PPARSCR 算法只涉及候选频繁项集支持数的加法运算,从而有效减少了计算量。

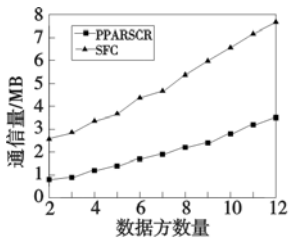

图2　算法通信量比较

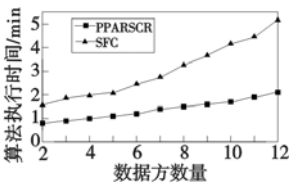

图3　算法执行时间比较

因此,对通信量和算法执行时间测试结果表明,PPARSCR 优于 SFC 算法。

3.3　参数 w 对性能的影响

为了检测算法的精度,利用挖掘出的频繁项集来衡量算法的精度。由于 SFC 算法挖掘出的频繁项集是精确的,所以以 SFC 挖掘出的频繁项集为标准来评价 PPARSCR 算法。

实验针对三方情况下,数据集为 20k,最小支持度为 0.01 条件下,参数 w 选择不同的值时对性能的影响。

从表 3 和图 4 可以看出,随着 w 值的增加,挖掘出来的频繁项集结果越来越准确,但是算法的执行时间逐渐增多。这是因为 w 越大剪枝掉的项集越少,于是更多的项集将有机会通过安全求和协议精确求出其支持度,从而得到的频繁项集的结果也越来越准确,但计算量也越来越大。

表 3　参数 w 的选择对精确度的影响

频繁项集长度	频繁项集数目	参数 w 值		
		0.001	0.002	0.003
1	47	44	45	47
2	896	887	890	892
3	4 835	4 689	4 738	4 811
4	6 483	6 256	6 321	6 468
5	2 077	2 062	2 072	2 077
6	45	45	45	45

4　结束语

本文通过数据变换以及安全计算协议解决了半诚实模型下水平分布数据的隐私数据保护问题,提出项集随机干扰矩阵对多个属性同时进行干扰,保持了属性之间的相关性,提高了挖掘精度,使用安全多方计算获得最终结果之前对候选频繁项集进行剪枝,减少了大量计算与通信开销,提高了挖掘效率。实验表明,本文所提算法与最新算法相比,当精确度为 90% 左右时,挖掘效率至少提高了 50%。

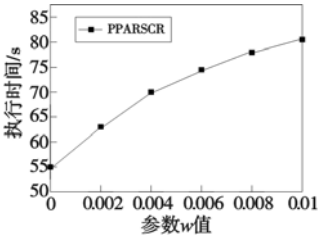

图4　w的选择对执行时间的影响

参考文献:

[1] AGRAWAL R, SRIKANT R. Privacy-preserving data mining[C]// Proc of ACM SIGMOD Conference on Management of Data. 2000:439-450.

[2] 周水庚,李丰,陶宇飞,等. 面向数据库应用的隐私保护研究综述[J]. 计算机学报,2009,32(5):847-861.

[3] KANTARCIOGLU M, CLIFTION C. Privacy-preserving distributed mining of association rules on horizontally partitioned data [J]. IEEE Trans on Knowledge and Data Engineering,2004,16(9):1026-1037.

[4] HUSSEIN M, EL-SISI A, ISMAIL N. Fast cryptographic privacy preserving association rules mining on distributed homogenous data base [C]//LNCS, vol 5178. 2008:607-616.

[5] KUNO S Y, DOI K, YAMAMOTO A. Frequent closed itemset mining with privacy for distributed databases[C]//Proc of IEEE International Conference on Data Mining Workshops. 2010:483-490.

[6] ZHANG Peng, TONG Yun-hai, TANG Shi-wei, *et al*. An effective method for privacy preserving association rule mining [J]. Journal of Software,2006,17(8):1764-1774.

[7] TENG Zhou-xuan, DU Wen-liang. A hybrid multi-group approach for privacy-preserving data mining [J]. Knowledge and Information Systems,2009,19(2):133-157.

[8] SHASKANKA M. A privacy preserving framework for Gaussian mixture models[C]//Proc of IEEE International Conference on Data Mining Workshops. Washington DC: IEEE Computer Society, 2010: 499-506.

[9] HAN Jia-wei, KAMBER M. 数据挖掘概念与技术[M]. 范明,孟小峰,译. 北京:机械工业出版社,2001.

(上接第 1099 页)

[3] ABE M, FUJISAKI E. How to date blind signatures [C]// Advances in Cryptology-AisaCrypt'96. Heidelberg: Springer-Verlag, 1996: 244-251.

[4] 苏万力,谭示崇,李艳平,等. 无证书部分盲签名[J]. 吉林大学学报:工学版,2009,39(4):1094-1098.

[5] 李明祥,杜光辉,罗新方. 高效的无证书部分盲签名方案[J]. 计算机工程与设计,2010,31(22):4817-4819, 4892.

[6] 余丹,杨晓元,黄大威. 新的无证书部分盲签名方案[J]. 计算机应用研究,2010,27(11):4319-4321.

[7] ZHANG Lei, ZHANG Fu-tai, QIN Bo, *et al*. Provably-secure electronic cash based on certificateless partially-blind signatures [J]. Electronic Commerce Research and Applications,2011,10(5): 545-552.

[8] CHOI K, PARK J, HWANG J, *et al*. Efficient certificateless signature schemes [C]// Proc of the 5th International Conference on Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2007:443-458.

[9] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures [J]. Journal of Cryptology , 2000, 13 (3):361-396.

[10] SHACHAM H. New paradigms in signature schemes [D]. Stanford: Stanford University, 2005.

[11] 刘晓亚,辛小龙. 改进的盲签名电子现金方案[J]. 计算机工程与应用,2011,47(4):114-116.

[12] 孟显勇. 基于双线性对的多银行电子现金方案[J]. 计算机工程,2010,36(19):154-155,158.

[13] JUANG W S. RO-cash:an efficient and practical recoverable pre-paid offline e-cash scheme using bilinear pairings [J]. Journal of Systems and Software,2010,83(4):638-645.

[14] LENSTRS A, TROMER E, SHAMIR A, *et al*. Factoring estimates for a 1024-bit RSA modulus [C]//Advances in Cryptology-AsiaCrypt'03. New York: Springer-Verlag,2003:55-74.