文章编号:1007-5321(2021)05-0114-07 **DOI**:10.13190/j.jbupt.2021-004

强隐私保护的移动群智感知方案

史 瑞[1], 封化民[1,2], 杨 旸[3], 袁 峰[2], 刘 飚[2]
(1. 北京邮电大学 网络空间安全学院, 北京 100876; 2. 北京电子科技学院, 北京 100070;
3. 福州大学 数学与计算机科学学院, 福州 350108)

摘要: 为了实现移动群智感知系统中身份隐私、证书撤销和积分激励功能,同时解决恶意用户身份追踪与诚实用户隐私保护之间的矛盾,提出了强隐私保护的移动群智感知方案. 基于门限密码思想将身份追踪能力分散到多个实体上,使得多个追踪者合作才能追踪用户身份; 将 Pointcheval-Sanders 签名和基于 RSA 假设的 Camenisch-Lysyanskaya 累加器结合起来实现了证书的安全快速撤销; 利用 Pointcheval-Sanders 签名构造了保护隐私的积分激励机制. 对该方案进行了安全性分析和实验分析. 研究结果表明,该方案不仅满足安全要求,而且在实际应用中具有可行性.

关 键 词: 密码学; 移动群智感知; 知识签名; 门限追踪; 动态累加器
中图分类号: TP309.2 **文献标志码**: A

Mobile Crowdsensing Scheme with Strong Privacy-Preserving

SHI Rui[1], FENG Hua-min[1,2], YANG Yang[3], YUAN Feng[2], LIU Biao[2]
(1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Beijing Electronic Science and Technology Institute, Beijing 100070, China;
3. College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China)

Abstract: To realize the identity privacy, credential revocation, credit incentive features and mediate the contradiction between the identity tracking of malicious users and the privacy protection of honest users in a mobile crowdsensing system, a mobile crowdsensing scheme with strong privacy-preserving is proposed. Based on threshold cryptography, the new scheme distributes the identity tracking capability of anonymous users to multiple entities, which guarantees that multiple trackers can cooperatively reveal the real identity of users. Pointcheval-Sanders signature and Camenisch-Lysyanskaya accumulator based on Rivest-Shamir-Adleman assumption are combined to realize efficient and secure revocation of credentials. The privacy-preserving credit management mechanism is constructed by adopting the Pointcheval-Sanders signature. The security and experimental analysis of the scheme is carried out. The experimental results show that the scheme not only meets the security requirements, but also has feasibility in practical deployment.

Key words: cryptography; mobile crowdsensing; signature of knowledge; threshold cryptography; dynamic accumulator

收稿日期: 2021-01-13
基金项目: 国家重点研发计划资助项目(2018YFB0803600); 国家自然科学基金项目(61872091); 北京电子科技学院一流学科建设项目(3201024)
作者简介: 史 瑞(1988—), 男, 博士生.
通信作者: 封化民(1963—), 男, 教授, 博士生导师, E-mail: fenghm@besti.edu.cn.

移动群智感知是以用户为中心进行数据收集的分布式网络，具有感知范围广、成本低、扩展性强等优点. 移动群智感知在将数据收集变得轻松的同时，也面临用户身份信息泄露、恶意用户重复提交报告、缺乏安全的积分激励机制等问题.

为了解决移动群智感知中的安全和隐私保护问题，国内外学者做了大量研究. Qiu 等[1]提出了一种基于 k 匿名的隐私保护方案. Rahaman 等[2]基于群签名构造了一种可撤销的假名方案保护用户身份信息. Sucasas 等[3]利用基于假名的签名构造了一种不可链接但是有责任的身份认证方案. Ni 等[4]利用有高效协议的签名构造了一种强隐私保护方案. Zhao 等[5]提出了一种基于数据质量的隐私保护激励方案. Sun 等[6]提出了一种基于契约的个性化隐私保护激励机制. 可靠的群智感知方案要求其他用户、服务平台，甚至证书中心都不能窃取用户身份信息，而在现有方案[2-3]中，好奇的证书中心可以将任意用户的感知报告与身份链接. 对于多次提交不合格感知报告的恶意用户，证书中心有权撤销其证书，但是现有方案有的不支持证书撤销功能[1,4-6]，有的通过白名单[3]方式进行证书管理，有的证书撤销[2]的计算开销较大. 另外，安全的信誉积分激励机制，可以激励用户诚实地参与感知任务，目前大部分群智感知方案[1-3]不具备保护隐私的积分激励功能.

为了解决现有方案存在的缺陷，提出了一个既具有身份隐私保护、证书快速撤销和积分激励功能，又可以防止证书中心恶意追踪用户身份的强隐私保护群智感知方案.

1　预备知识

1.1　双线性对

设 $G,\widetilde{G},G_T$ 是阶为素数 p 的循环群，$G\neq\widetilde{G}$，G 与 $\widetilde{G}$ 之间不存在同态映射，双线性[7]映射 $e:G\times\widetilde{G}\rightarrow G_T$ 满足双线性，非退化性和可计算性.

1.2　知识签名

$\boldsymbol{\Pi}=\mathrm{SoK}\{(x):(x,y)\in R\}(m)$ 定义了多项式时间非确定性(NP, non-deterministic polynomial)关系 R 的知识签名[8]，其中验证方不知道秘密值 x，知识签名满足完备性和模拟可提取性. 所提方案使用 Camenisch 等[9]提出的技术构造知识签名.

1.3　DDH 假设

判定性狄菲-赫尔曼(DDH, decision Diffie-Hellman)假设是指给定四元组 $g,g^x,g^y,g^z\in G$，其中 $x,y,z\in Z_p^*$，$Z_p^*=Z_p\setminus\{0\}$，Z_p 为模 p 的有限群. 任意概率多项式时间(PPT, probabilistic polynomial time)敌手成功判断 $z=xy \bmod p$ 是否成立的概率是可忽略的.

1.4　PS 签名

PS(Pointcheval-Sanders)签名[10]包含初始化、密钥生成、签名和验签算法，PS 签名的安全性可归约到 PS 假设，使用知识签名可以证明 PS 签名是合法的但不泄露消息和签名的任何信息.

1.5　CL-RSA 累加器

CL-RSA (Camenisch-Lysyanskaya based on Rivest-Shamir-Adleman)累加器[11]包含密钥生成、成员添加、成员验证、成员删除和证据更新算法. Baldimtsi 等[12]定义了动态累加器的 2 种安全性：自适应完备和非自适应完备，并证明了 CL-RSA 累加器是非自适应完备的.

2　问题分析

2.1　系统模型

移动群智感知系统的参与方包括服务平台、用户、证书中心和追踪者. 如图 1 所示，系统模型可由以下步骤描述：① 证书中心将追踪者的公钥公布在追踪者公钥数据库；② 证书中心为用户签发证书并将注册信息公布在用户注册信息数据库；③ 服务平台发布感知任务；④ 用户申请感知任务，服务平台为用户分配任务；⑤ 用户收集数据并向服务平台提交感知报告；⑥ 服务平台验证感知报告的合法性并评估报告的质量；⑦ 服务平台向用户发放积分；⑧ 多个追踪者联合追踪恶意用户身份；

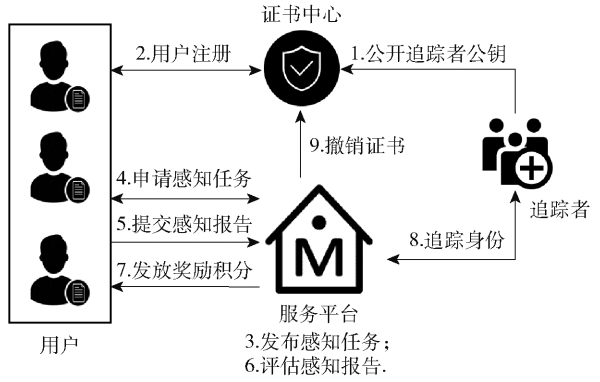

图 1　移动群智感知系统模型

⑨证书中心撤销恶意用户证书.

2.2 威胁模型

服务平台诚实地发布感知任务、评估感知报告并为用户发放积分,但是好奇的服务平台试图获取移动用户的敏感信息. 恶意用户会伪造、修改感知数据,或者传递模糊、有偏差的感知数据欺骗服务平台. 为了获得更多的积分,恶意用户可能会在同一个感知任务中匿名提交多份感知报告. 证书中心诚实履行用户注册、证书撤销以及公布用户注册信息和追踪者公钥信息的职责,但是好奇的证书中心试图将用户的感知报告与身份链接. 系统有多个具有追踪能力的追踪者,不排除存在恶意的追踪者,也不能保证所有追踪者时时在线履行追踪职责.

2.3 设计目标

为了实现方案并抵抗安全威胁,所提方案需满足以下要求. ① 感知报告的匿名性:用户、服务平台和证书中心无法将感知报告与用户身份链接. ② 恶意用户的身份可追踪:服务平台可以识别在单个任务中提交多份感知报告的用户,并恢复其身份信息,对于提交不合格感知报告的用户,可以使用门限追踪机制追踪用户身份. ③恶意用户证书可撤销:对于多次提交不合格感知报告的用户,证书中心可以撤销其证书,非注册用户或已被撤销证书的用户无法参与感知任务. ④ 保护隐私的积分激励:用户的精确积分值被隐藏起来,不被服务平台、其他用户和证书中心发现,用户若私自修改积分值将无法通过服务平台的认证.

3 方案构造

3.1 设计思想

为了防止证书中心恶意追踪用户身份,使用Camenisch门限群签名[13]技术,将追踪功能分散给多个追踪者. 身份追踪的目的是揭露参与本次感知任务的恶意用户身份,但不能泄露用户的历史信息,并且在用户证书未被撤销前仍可匿名地参与感知任务,因此在身份追踪时既要揭露用户身份又不能泄露私钥信息. 为了解决身份追踪与私钥保护的矛盾,注册时使用追踪者的公钥将私钥共享份额加密发送给追踪者,在身份追踪时多个追踪者可以恢复用户私钥的承诺值,而不泄露私钥信息.

利用PS签名和知识签名可以使用户随时参与感知任务而不会泄露身份信息,但是在基于签名的匿名方案中,证书快速撤销是个难题. 为了实现既能匿名认证又能快速撤销证书,利用PS签名将CL-RSA累加器的用户累加值与用户信息绑定,签发证书时执行PS签名和CL-RSA累加器的成员添加算法,撤销证书时执行CL-RSA累加器的成员删除和证据更新算法. 撤销的安全性满足自适应完备,证据更新只需2个群元素,更重要的是,用户仍然可以匿名的参与感知任务.

匿名性使用户可以安全地参与感知任务而无需担心身份泄露,但这也给积分管理带来了挑战. 服务平台需要在不知道用户身份的条件下分配积分. 为了解决用户积分管理困难问题,使用PS签名将累计积分和用户信息绑定,通过知识签名在不泄露积分信息的前提下证明累计积分的正确性. 服务平台可以在更新后的积分承诺上生成新的PS签名,如果移动用户提交的报告是可信的,服务平台可以增加积分,否则就会降低积分. 表1所示为本节使用的符号说明.

表1 符号定义

符号	说明
I	用户身份,$I\in Z_p^*$
(p_u,s_u)	用户公私钥对
v	用户累加值
s	用户累计积分
Δs	奖励积分
T_s	任务序号
(h_1,σ_1)	用户属性证书
(h_2,σ_2)	包含积分值的属性证书
(h_3,σ_3)	包含任务序号的属性证书
D_u	用户注册信息数据库
D_o	追踪者公钥数据库

3.2 系统初始化

给定安全参数 λ,证书中心选择双线性对参数 $(p,G,\widetilde{G},G_T,e)$,其中 $g,\widetilde{g}$ 分别为 $G,\widetilde{G}$ 的生成元;设置门限参数(t,n),其中 $n\geqslant t$;选择单向函数 H_1 和 H_2,其中 $H_1:\{0,1\}^*\rightarrow Z_p$,$H_2:\{0,1\}^*\rightarrow G$.

3.3 密钥生成

1) 服务平台选取 $a,b_1,\cdots,b_4\in Z_p^*$,计算$(A,B_1,\cdots,B_4)\leftarrow(g^a,g^{b_1},\cdots,g^{b_4})$,$(\widetilde{A},\widetilde{B}_1,\cdots,\widetilde{B}_4)\leftarrow(\widetilde{g}^{b_1},\cdots,\widetilde{g}^{b_4})$. 设置私钥为 A,公钥为$(B_1,\cdots,B_4,\widetilde{A},\widetilde{B}_1,\cdots,\widetilde{B}_4)$.

2) 追踪者选取私钥 $\alpha_i\in Z_p^*$,$i\in[1,\cdots,n]$,计算公钥 $\widetilde{\beta}_i=\widetilde{g}^{\alpha_i}$和$\boldsymbol{\Pi}_0^i=\mathrm{SoK}\{(\alpha_i):\widetilde{\beta}_i=\widetilde{g}^{\alpha_i}\}$,将$(i,\widetilde{\beta}_i,\boldsymbol{\Pi}_0^i)$发送至证书中心.

3) 证书中心设置 $D_u=\varnothing$; 验证$\boldsymbol{\Pi}_0^i$ 后将$(i,\widetilde{\beta}_i)$添加到 D_o; 选取 2 个安全素数 $\bar{p}$ 和 $\bar{q}$, 计算 $N=\bar{p}\,\bar{q}$, $N'=(\bar{p}-1)(\bar{q}-1)/4$; 选取 $\mu\in QR_N, x, y_1, \cdots, y_4\in Z_p^*$, 计算$(X,Y_1,\cdots,Y_4)\leftarrow(g^x,g^{y_1},\cdots,g^{y_4})$, $(\widetilde{X},\widetilde{Y}_1,\cdots,\widetilde{Y}_4)\leftarrow(\widetilde{g}^x,\widetilde{g}^{y_1},\cdots,\widetilde{g}^{y_4})$. 设置私钥为$(X,N')$, 公钥为$(Y_1,\cdots,Y_4,\widetilde{X},\widetilde{Y}_1,\cdots,\widetilde{Y}_4,N,\mu)$.

3.4　用户注册

1) 证书中心选取 $u_1,u_2\in Z_p^*$, 计算 $\boldsymbol{\Pi}_1=\mathrm{SoK}\{(u_1,u_2): h_1=g^{u_1}\wedge h_2=g^{u_2}\}$, 将$(h_1,h_2,\boldsymbol{\Pi}_1)$发送给用户.

2) 用户产生注册信息

① 验证$\boldsymbol{\Pi}_1$ 后, 选取 $s_u,k_1,k_2\in Z_p^*$, 计算 $C_1=g^{k_1}Y_1^{s_u}$, $C_2=g^{k_2}Y_1^{s_u}$, $p_u=h_1^{s_u}$ 和$\boldsymbol{\Pi}_2=\mathrm{SoK}\{(k_1,k_2,s_u): C_1=g^{k_1}Y_1^{s_u}\wedge C_2=g^{k_2}Y_1^{s_u}\wedge p_u=h_1^{s_u}\}$;

② 选取$f_1,f_2,\cdots,f_{t-1}\in Z_p^*$, 生成 $t-1$ 次私钥共享多项式 $F(x)=s_u+f_1x+\cdots+f_{t-1}x^{t-1}$, 计算$s_i=F(i), i\in[1,2,\cdots,n], p_j=h_1^{f_j}, j\in[1,2,\cdots,t-1]$;

③ 对每一个秘密份额 s_i, 选取 $r_i\in Z_p^*$, 计算$\widetilde{C}_i=(\widetilde{C}_i^1,\widetilde{C}_i^2)=(\widetilde{g}^{r_i},\widetilde{\beta}_i^{r_i}\widetilde{Y}_1^{s_i})$, $\boldsymbol{\Pi}_3^i=\mathrm{SoK}\left\{(r_i): \widetilde{C}_i^1=\widetilde{g}^{r_i}\wedge e(h_1,\widetilde{C}_i^2/\widetilde{\beta}_i^{r_i})=e\left(p_u\prod_{j=1}^{t-1}p_j^{i^j},\widetilde{Y}_1\right)\right\}$;

④ 将注册信息$\{I,h_1,p_u,C_1,C_2,\boldsymbol{\Pi}_2,p_1,\cdots,p_{t-1},(\widetilde{C}_1,\boldsymbol{\Pi}_3^1),\cdots,(\widetilde{C}_n,\boldsymbol{\Pi}_3^n)\}$发送至证书中心.

3) 证书中心签发证书

①验证$\boldsymbol{\Pi}_2,\boldsymbol{\Pi}_3^1,\cdots,\boldsymbol{\Pi}_3^n$ 后, 评估积分初始值 s; 选取奇素数 v, 计算累加器证据 $w=\mu^{v^{-1}\bmod N'}\bmod N$;

②将用户身份、累加值和积分信息绑定: $\delta_1'=(XC_1Y_2^IY_3^v)^{u_1}$, $\delta_2'=(XC_2Y_2^IY_3^vY_4^s)^{u_2}$;

③将用户注册信息$(I,v,h_1,p_u,C_1,C_2,\boldsymbol{\Pi}_2,p_1,\cdots,p_t,(\widetilde{C}_1,\boldsymbol{\Pi}_3^1),\cdots,(\widetilde{C}_n,\boldsymbol{\Pi}_3^n))$写入 D_u, 将证书$(s,w,v,h_1,\delta_1',h_2,\delta_2')$发送给用户.

4) 用户计算 $\delta_1=\delta_1'/h_1^{k_1}$, $\delta_2=\delta_2'/h_2^{k_2}$, 验证等式 $\mu=w^v$, $e(\delta_1,\widetilde{g})=e(h_1,\widetilde{X}\widetilde{Y}_1^{s_u}\widetilde{Y}_2^I\widetilde{Y}_3^v)$, $e(\delta_2,\widetilde{g})=e(h_2,\widetilde{X}\widetilde{Y}_1^{s_u}\widetilde{Y}_2^I\widetilde{Y}_3^v\widetilde{Y}_4^s)$后接受证书$(s_u,I,v,s,w,\mu,h_1,\delta_1,h_2,\delta_2)$.

3.5　申请感知任务

1) 服务平台发布感知任务 T_k 和时间 T_t.

2) 用户选取 $\varepsilon_1,\varphi_1\in Z_p^*$, 计算 $\hat{\delta}_1=(\delta_1h_1^{\varphi_1})^{\varepsilon_1}$, $\hat{h}_1=h_1^{\varepsilon_1}\tau=\widetilde{g}^{\varphi_1}$ 和 $\boldsymbol{\Pi}_4=\mathrm{SoK}\{(s_u,I,v,w,k,\varphi_1): e(\hat{\delta}_1,\widetilde{g})=e(\hat{h}_1,\widetilde{X}\widetilde{Y}_1^{s_u}\widetilde{Y}_2^I\widetilde{Y}_3^v\tau)\wedge\tau=\widetilde{g}^{\varphi_1}\wedge\mu=w^v\wedge C'=g^kB_1^{s_u}B_2^IB_3^v\}(T_k\parallel T_t)$将申请信息$(\hat{h}_1,\hat{\delta}_1,\tau,\boldsymbol{\Pi}_4)$发送至服务平台.

3) 服务平台验证$\boldsymbol{\Pi}_4$ 后, 为用户生成任务序号 T_s; 选取 $z_1\in Z_p^*$, 计算 $h_3=g^{z_1}$, $\delta_3'=(AC'B_4^{T_s})^{z_1}$, 将任务分配信息$(T_s,h_3,\delta_3')$发送给用户.

4) 用户计算 $\delta_3=\delta_3'/h_3^k$, 验证等式$e(\delta_3,\widetilde{g})=e(h_3,\widetilde{A}\widetilde{B}_1^{s_u}\widetilde{B}_2^I\widetilde{B}_3^v\widetilde{B}_4^{T_s})$后接受任务.

3.6　提交感知报告

1) 用户完成感知数据 m 的收集后, 首先计算 $d_1=H_1(T_k\parallel T_t\parallel m)$, $d_2=H_1(I\parallel T_s\parallel T_k\parallel T_t)$, $D=g^{d_2}$ 和 $E=h_1^{sk_u}H_2(T_k\parallel T_t)^{d_1d_2}$; 然后选取 $r',\varepsilon_2,\varepsilon_3,\varphi_2,\varphi_3\in Z_p^*$, 计算 $\hat{h}_2=h_2^{\varepsilon_2}$, $\hat{\delta}_2=(\delta_2h_2^{\varphi_2})^{\varepsilon_2}$, $\hat{h}_3=h_3^{\varepsilon_3}$, $\hat{\delta}_3=(\delta_3h_3^{\varphi_3})^{\varepsilon_3}$, $C''=g^{r'}B_1^{s_u}B_2^IB_3^vB_4^s$ 和$\boldsymbol{\Pi}_5=\mathrm{SoK}\{(s_u,I,v,s,d_2,r',\gamma,\varphi_2,\varphi_3): e(\hat{\delta}_2,\widetilde{g})=e(\hat{h}_2,\widetilde{X}\widetilde{Y}_1^{s_u}\widetilde{Y}_2^I\widetilde{Y}_3^v\widetilde{Y}_4^s\widetilde{g}^{\varphi_2})\wedge e(\hat{\delta}_3,\widetilde{g})=e(\hat{h}_3,\widetilde{A}\widetilde{B}_1^{s_u}\widetilde{B}_2^I\widetilde{B}_3^v\widetilde{B}_4^{T_s}\widetilde{g}^{\varphi_3})\wedge C''=g^{r'}B_1^{s_u}B_2^IB_3^vB_4^s\wedge D=g^{d_2}\wedge E=h_1^{s_u}H_2(T_k\parallel T_t)^{d_1d_2}\}(T_k\parallel T_t\parallel m)$. 最后, 将感知报告信息$(T_s,m,C'',D,E,\hat{h}_2,\hat{\delta}_2,\hat{h}_3,\hat{\delta}_3,\boldsymbol{\Pi}_5)$发送至服务平台.

2) 服务平台验证$\boldsymbol{\Pi}_5$ 后, 查询是否有另一份感知报告$(T_s,m^*,(C'')^*,D,E^*,\hat{h}_2^*,\hat{\delta}_2^*,\hat{h}_3^*,\hat{\delta}_3^*,\boldsymbol{\Pi}_5^*)$存在相同的 T_s 和 D, 但是 $E\neq E^*$. 若出现上述情况则计算 $p_u=[E^{d_1^*}/(E^*)^{d_1}]^{(d_1^*-d_1)^{-1}}$, 并根据 D_u 中的用户注册信息查询恶意用户身份 I.

3.7　获取激励积分

1) 服务平台根据感知报告的质量, 为用户分配积分 Δs. 服务平台选取 $z_2\in Z_p^*$, 计算 $h_2=g^{z_2}$和 $\delta_2'=(AC''B_4^{\Delta s})^{z_2}$, 将$(\Delta s,h_2,\delta_2')$发送给用户.

2) 用户计算 $\delta_2=\delta_2'/h_2^{r'}$, $s=s+\Delta s$, 验证等式$e(\delta_2,\widetilde{g})=e(h_2,\widetilde{A}\widetilde{B}_1^{s_u}\widetilde{B}_2^I\widetilde{B}_3^v\widetilde{B}_4^s)$后更新$(s,h_2,\delta_2)$.

3.8　追踪用户身份

服务平台根据恶意用户的任务序号 T_s 查询感知任务申请信息$(\hat{h}_1,\hat{\delta}_1,\tau,\boldsymbol{\Pi}_4)$, 并广播给 t 个追踪者. 追踪者遍历 D_u, 对每一个注册用户执行追踪操作. 对于注册用户 I, 第 i 个追踪者首先计算$T_i^I=e(\hat{h}_1,\widetilde{C}_i^2/(\widetilde{C}_i^1)^{\alpha_i})$, 并广播给其他追踪者; 然后计算 $\omega_i=\prod_{j=1,j\neq i}^{t}j/(j-i)$; 若等式$e(\hat{h}_1,\tau\,\widetilde{X}\,\widetilde{Y}_2^I\,\widetilde{Y}_3^v)\times$

$\prod_{i=1}^{t}(T_i^I)^{\omega_i}=e(\hat{\delta}_1,\tilde{g})$,则追踪到用户 I,否则继续对下一个用户执行追踪操作,直到追踪到用户身份或者完成 D_u 的遍历.

3.9 撤销用户证书

1)证书中心更新累加器值 $\mu=\mu^{-v_{I'}\bmod N'}\bmod N$,广播累加器更新信息 $(\mu,v_{I'})$,并删除用户注册信息.

2)合法用户 I 收到更新信息后,计算 (a,b),满足 $av_I+bv_{I'}=1$,并更新证据 $w_I=w_I^b\mu^a$.

4 安全性分析

4.1 匿名性

定理1 在随机预言机模型下,对于任意的2个注册用户 (I_0,I_1),如果存在PPT敌手 A 能够以不可忽略的概率区分出感知报告由哪个用户提交,那么存在挑战者 C 能够以相同的概率解决DDH问题.

证明 设 $T_1,T_2,T_3,T_4\in G$ 是DDH四元组,A 与 C 做如下交互:

1)初始化. C 设置 $g=T_1$,执行系统初始化、密钥生成操作并将参数发送给 A. C 任意选择2个身份 (I_0,I_1),执行用户注册,并将注册信息发送给 A.

2)敌手询问.

申请感知任务询问:A 选择 I_0 或 I_1 并发送给 C,C 诚实地执行申请感知任务操作.

提交感知报告询问:A 选择 I_0 或 I_1 以及 m 并发送给 C. 若为 I_0,C 诚实地执行提交感知报告操作,若为 I_1,C 选取 $d_1,d_2\in Z_p$,计算 $D=T_1^{d_2}$,$E=h_1^{sk_u}H_2(T_k\parallel T_t)^{d_1d_2}$ 和 $\boldsymbol{\Pi}_5$,将 $(D,E,\boldsymbol{\Pi}_5,\cdots)$ 发送给 A.

3)挑战应答. 多项式次询问后,A 随机选择 m 发送给 C,C 随机选择 $b\in\{0,1\}$. 若 $b=0$,C 诚实地执行提交感知报告操作. 若 $b=1$,C 设置 $D=T_2$,$H_2(T_k\parallel T_t)=T_3$,$E=h_1^{s_u}T_4^{d_1}$,$C$ 模拟知识签名 $\boldsymbol{\Pi}_5$,然后将 $(D,E,\boldsymbol{\Pi}_5,\cdots)$ 发送给 A. 如果 $z=xy\bmod p$,则知识签名的模拟是完美的. 最后,A 输出 $\hat{b}$,若 $\hat{b}=b$,C 以相同的概率确定存在 (x,y),满足 $T_2=T_1^x$,$T_3=T_1^y$,$T_4=T_1^{xy}$,因此 C 解决了DDH问题.

4.2 可追踪性

定理2 在随机预言机模型下,如果存在PPT敌手 A 能够以不可忽略的概率 ε 构造知识签名 $\boldsymbol{\Pi}_4$,该签名可以通过服务平台验证但身份追踪失败,那么存在挑战者 C 能够以 ε^2 的概率伪造PS签名.

证明 设PS签名的公共参数为 $(p,G,\tilde{G},G_T,e,g,\tilde{g})$,公钥为 $(Y_1,\cdots,Y_4,\tilde{X},\tilde{Y}_1,\cdots,\tilde{Y}_4)$,$C$ 可以不限制次数的访问预言机 $O_{ps}(\cdot)$. A 与 C 做如下交互:

1)初始化. C 设置公共参数 $(p,G,\tilde{G},G_T,e,g,\tilde{g})$,执行系统初始化产生其他公共参数,设置证书中心的公钥 $(Y_1,\cdots,Y_4,\tilde{X},\tilde{Y}_1,\cdots,\tilde{Y}_4)$,执行密钥生成操作产生其他密钥,将参数发送给 A.

2)敌手询问. A 产生注册信息,C 通过访问预言机 $O_{ps}(\cdot)$ 完成用户注册,并诚实地执行 A 的其他询问.

3)挑战应答. 多项式次询问后,对于感知任务 T_k^* 和任务时间 T_t^*,A 提交申请感知任务签名 $(\hat{h_1},\hat{\delta}_1,\tau,\boldsymbol{\Pi}_4)$. 若 A 以 ε 的概率赢得了游戏,C 执行用户身份追踪操作时将出现2种情况:或者追踪到没有申请该任务的其他诚实用户,或者追踪到没有注册的用户. 若是第1种情形,表明 A 伪造了一个合法用户的签名,这与知识签名的模拟可提取性矛盾. 若是第2种情形,根据分叉引理,C 能够以 ε 的概率得到另一个签名 $\boldsymbol{\Pi}_4'$,因此可以提取证据 $(s_u^*,I^*,v^*,\varphi^*)$,满足 $e(\hat{\delta}_1,\tilde{g})=e(\hat{h_1}^{\varphi^*},\tilde{X}\tilde{Y}_1^{s_u^*}\tilde{Y}_1^{I^*}\tilde{Y}_1^{v^*})$,因此 C 以 ε^2 的概率伪造了消息 (s_u^*,I^*,v^*) 的签名 $(\hat{h_1}^{\varphi^*},\hat{\delta}_1)$.

4.3 自适应完备性

定理3 若PS签名是不可伪造的,CL-RSA累加器非自适应完备的,那么方案满足自适应完备性.

证明 假设存在PPT敌手 A 能够为非法用户产生有效的知识签名,使得用户通过了服务平台的验证. 那么该用户或者从未注册,或者证书已被撤销.

对于未注册用户,若敌手产生了一个有效的签名,等价于敌手伪造了一个PS签名,因为PS签名方案在PS假设下是存在不可伪造的,因此第1种情况发生的概率是可忽略的.

对于已撤销用户,若敌手产生了一个有效的签名,等价于敌手产生了的一个证据 (w',v'),使得 $\eta=w'^{v'}$. 因为CL-RSA累加器在强RSA假设下满足非自适应完备,因此第2种情况发生的概率也是可忽略的. 因此方案满足自适应完备性.

4.4 积分平衡性

定理4 设PPT敌手 A 的积分初始值为 s_0,A 最多参加 l 次感知任务,每次获得的积分激励为

Δs_i，若 A 能够以不可忽略的概率获得积分 $s > s_0 + \sum_{i=1}^{l} \Delta s_i$，那么存在挑战者 C 能够以相同概率伪造 PS 签名.

证明　设 PS 签名的参数为 $(p, G, \widetilde{G}, G_T, e, g, \widetilde{g})$，公钥为 $(Y_1, \cdots, Y_4, \widetilde{X}, \widetilde{Y}_1, \cdots, \widetilde{Y}_4)$，$C$ 可以不限制次数的访问预言机 $O_{ps}(\cdot)$. 对于知识签名 $\boldsymbol{\Pi}_1, \cdots, \boldsymbol{\Pi}_5$，存在证据提取器 $E_{x_1}, \cdots, E_{x_5}$. A 与 C 做如下交互：

(1)初始化. C 设置参数 $(p, G, \widetilde{G}, G_T, e, g, \widetilde{g})$，执行系统初始化产生其他参数，设置证书中心的公钥为 $(Y_1, \cdots, Y_4, \widetilde{X}, \widetilde{Y}_1, \cdots, \widetilde{Y}_4)$，执行密钥生成操作产生其他密钥，将参数发送给 A.

(2)用户注册询问. A 发起注册请求，C 随机产生 $(h_1, h_2, \boldsymbol{\Pi}_1)$ 发送给 A；A 生成注册信息发送给 C；C 利用 E_{x_2}, E_{x_3} 获取证据 $(k_1, k_2, s_u, r_1, \cdots, r_n)$，选取 (s_0, v)，询问预言机 $O_{ps}(\cdot)$ 获得签名 $(h_1, \delta_1, h_2, \delta_2)$. C 计算 $\delta_1' = \delta_1 h_1^{k_1}, \delta_2' = \delta_2 h_2^{k_2}, w = \mu^{v^{-1}}$，将 $(s_0, w, v, h_1, \delta_1', h_2, \delta_2')$ 发送给用户.

(3)申请感知报告询问. 对于第 i 次感知任务，A 将感知报告 $(T_s^i, m_i, C_i'', D_i, E_i, \hat{h}_2^i, \hat{\delta}_2^i, \hat{h}_3^i, \hat{\delta}_3^i, \boldsymbol{\Pi}_5^i)$ 发送给 C；C 利用 E_{x_5} 获取证据 $(s_u, I, v, s, d_2, r', \varphi_2, \varphi_3)$. 如果 $s = s_0 + \sum_{j=1}^{i-1} \Delta s_j$，$C$ 随机产生 Δs_i，对消息 $\left(s_u, I, v, s_0 + \sum_{j=1}^{i} \Delta s_j\right)$，询问预言机 $O_{ps}(\cdot)$ 获得签名 (h_2, δ_2). C 计算 $\delta_2' = \delta_2 h_2^{r'}$，将 $(\Delta s_i, h_2, \delta_2')$ 发送给 A. 若 $s > s_0 + \sum_{j=1}^{i-1} \Delta s_j$，$C$ 计算 $h^* = \hat{h}_2^i, \delta^* = \hat{\delta}_2^i / (\hat{h}_2^i)^{\varphi_2}$，则 C 得到一个伪造的消息 (s_u, I, v, s) 的签名 (h^*, δ^*).

5　功能对比和效率评估

5.1　功能对比

表 2 所示为所提方案与其他方案[1-6]的功能对比，文献[1-6]的方案虽然支持用户身份隐私，但是都不支持恶意用户的门限追踪机制；文献[1,4-6]的方案不支持证书撤销；文献[1-3]的方案不具有安全的积分激励机制. 所提方案支持身份隐私、证书撤销、门限追踪和积分激励功能，实现了移动群智感知更全面的隐私保护.

表 2　所提方案与其他方案的功能对比

方案	身份隐私	证书撤销	门限追踪	积分激励
文献[1]	√	×	×	×
文献[2]	√	√	×	×
文献[3]	√	√	×	×
文献[4]	√	×	×	√
文献[5]	√	×	×	√
文献[6]	√	×	×	√
所提方案	√	√	√	√

5.2　理论评估结果

令 U 为系统用户数量，$E^G, E^{\widetilde{G}}, E^{G_T}, E^{Z_N}, E^e$ 分别表示 $G, \widetilde{G}, G_T, Z_N$ 中的幂运算和双线性对运算. 参与实体主要操作的计算开销如表 3 所示. 由表可知，用户注册和签发证书的计算开销与追踪者数量呈线性关系，追踪用户身份的计算开销与用户数量呈线性关系.

表 3　计算开销

操作	计算开销	时间/ms
用户注册	$(12+t)E^G + 4n \cdot E^{\widetilde{G}} + n \cdot E^{G_T} + n \cdot E^e$	216.9
签发证书	$12E^G + 2n \cdot E^{\widetilde{G}} + 2n \cdot E^{G_T} + 2n \cdot E^e + E^{Z_N}$	219.4
验证证书	$2E^G + 4E^{\widetilde{G}} + 4E^e + E^{Z_N}$	60.7
申请感知任务	$20E^G + 2E^{\widetilde{G}} + 4E^{G_T} + 4E^e + 14E^{Z_N}$	100.1
提交感知报告	$28E^G + 9E^{G_T} + 9E^e$	198.8
验证感知报告	$14E^G + 12E^{G_T} + 14E^e$	260.5
追踪用户身份	$U \cdot [(1+2/t)E^{\widetilde{G}} + E^{G_T} + (1+2/t)E^e]$	30 150.2

令 $|G|, |\widetilde{G}|, |G_T|, |Z_p|, |Z_N|$ 分别表示 $G, \widetilde{G}, G_T, Z_p, Z_N$ 中的元素大小. 表 4 所示为参与实体各个操作的通信开销. 由表可知，注册信息发送证书中心的通信开销与追踪者数量呈线性关系. 表 5 所示为各个参与实体的存储开销. 由表可知，证书中心的存储开销与用户数量、追踪者数量相关，追踪者和服务平台的存储开销均与用户数量呈线性关系.

表 4　通信开销

数据流说明	数据流大小
注册信息发送证书中心	$(4+t)\|G\| + 2n \cdot \|\widetilde{G}\| + (2n+5)\|Z_p\|$
签名证书发送用户	$4\|G\| + 2\|Z_p\| + \|Z_N\|$
任务申请发送服务平台	$4\|G\| + \|\widetilde{G}\| + 12\|Z_p\| + 8\|Z_N\|$
任务序号发送用户	$2\|G\| + \|Z_p\|$
感知报告发送服务平台	$9\|G\| + 10\|Z_p\|$
积分签名发送用户	$2\|G\|$
证书撤销	$\|Z_N\| + \|Z_p\|$

5.3　效率对比

所提方案在身份隐私、证书撤销、门限追踪和积

表5 存储开销

实体	存储大小
用户	$4\|G\|+4\|Z_p\|+2\|Z_N\|$
追踪者	$\|\widetilde{G}\|+U\cdot\|G_\tau\|$
服务平台	$(11\|G\|+\|\widetilde{G}\|+22\|Z_p\|+8\|Z_N\|)U$
证书中心	$[(5+t)U+5]\|G\|+(5+2nU+n)\|\widetilde{G}\|+(2n+6)U\cdot\|Z_p\|+\|Z_N\|$

分激励方面实现了强隐私保护的移动群智感知方案,已有的工作中[1-6]没有将前述4种功能全部实现的方案,因此无法与已有工作在效率方面进行全面对比. 本小节在证书撤销功能上与已有方案进行了对比,文献[3]的方案使用白名单方式实现证书撤销,其证书撤销具有线性复杂度 $O(U)$. 文献[2]的方案使用群签名技术实现了亚线性复杂度 $O(\mathrm{lb}U)$ 的证书撤销. 所提方案使用 CL-RSA 动态累加器实现了常数复杂度的证书撤销,撤销证书只需要2个 E^{Z_N} 运算,撤销证书的广播消息只有2个群元素.

5.4 实验分析

为了评估效率使用基于数论的密码库 MIRACL[14]在联想 ThinkPadT450 上实现了方案. 设置安全参数 $\lambda=128$,门限参数 $n=5$,$t=3$,用户最大数量 $U=1\,000$,单向函数 H_1,H_2 由安全散列算法[15]构造,选择 Barreto-Naehrig 曲线[16]:$E:y^2=x^3+2$ 和 R-ate对实现双线性对. 所提方案主要操作的时间消耗如表3所示. 由表可知,追踪用户身份消耗的时间最长,但是执行追踪用户身份操作的次数是很少的,通过积分激励机制也可以激励用户诚实地参加感知任务. 用户注册、申请感知任务和提交感知报告的计算开销较高,但是执行时间都小于300 ms.

6 结束语

提出了一种具有隐私保护、证书快速撤销和积分激励功能,同时支持门限追踪的移动群智感知方案. 方案解决了身份追踪完全依赖证书中心的问题,以较低的通信和计算开销实现了证书撤销,支持了保护隐私的积分激励功能. 理论分析表明方案满足安全目标,软件实验表明方案在实际应用中具有可行性.

参考文献:

[1] Qiu Fudong, Wu Fan, Chen Guihai. Privacy and quality preserving multimedia data aggregation for participatory sensing systems[J]. IEEE Transactions on Mobile Computing, 2014, 14(6): 1287-1300.

[2] Rahaman S, Cheng L, Yao D D, et al. Provably secure anonymous-yet-accountable crowdsensing with scalable sublinear revocation[J]. Privacy Enhancing Technologies, 2017(4): 384-403.

[3] Sucasas V, Mantas G, Bastos J, et al. A signature scheme with un-linkable-yet-accountable pseudonymity for privacy-preserving crowdsensing[J]. IEEE Transactions on Mobile Computing, 2019, 19(4): 752-768.

[4] Ni Jianbing, Zhang Kuan, Xia Qi, et al. Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing[J]. IEEE Transactions on Mobile Computing, 2019, 19(6): 1317-1331.

[5] Zhao Bowen, Tang Shaohua, Liu Ximeng, et al. PACE: privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing[J]. IEEE Transactions on Mobile Computing, 2020, 20(5): 1924-1939.

[6] Sun Peng, Wang Zhibo, Feng Yunhe, et al. Towards personalized privacy-preserving incentive for truth discovery in crowdsourced binary-choice question answering[C]// IEEE Conference on Computer Communications. Toronto: IEEE, 2020: 1133-1142.

[7] Galbraith S D, Paterson K G, Smart N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113-3121.

[8] Chase M, Lysyanskaya A. On signatures of knowledge[C]// Annual International Cryptology Conference. Berlin: Springer, 2006: 78-96.

[9] Camenisch J. Group signature schemes and payment systems based on the discrete logarithm problem[D]. Zurich: Swiss Federal Institute of Technology, 1998.

[10] Pointcheval D, Sanders O. Short randomizable signatures[C]// Cryptographers' Track at the RSA Conference. San Francisco: Springer, 2016: 111-126.

[11] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials[C]// Annual International Cryptology Conference. Berlin: Springer, 2002: 61-76.

[12] Baldimtsi F, Camenisch J, Dubovitskaya M, et al. Accumulators with applications to anonymity-preserving revocation[C]// IEEE European Symposium on Security and Privacy. Paris: IEEE, 2017: 301-315.

[13] Camenisch J, Drijvers M, Lehmann A, et al. Short threshold dynamic group signatures[C]// International Conference on Security and Cryptography for Networks. Amalfi: Springer, 2020: 401-423.

[14] MIRACL Company Limited. Multiprecision integer and rational arithmetic cryptographic library version 7.0[EB/OL]. (2019-08-21)[2020-10-20]. https://github.com/miracl/MIRACL.

[15] Dang Q H. Secure Hash standard: NIST FIPS 180-4—2015[S]. Gaithersburg: National Institute of Standards and Technology, 2015: 21-23.

[16] Fan J, Vercauteren F, Verbauwhede I. Faster F_p-arithmetic for cryptographic pairings on Barreto-Naehrig curves[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2009: 240-253.