隐私保护的传染病密切接触者身份追踪系统

陈梁景[1],王志伟[1,2,3]
(1. 南京邮电大学 计算机学院,江苏 南京 210003;
2. 江苏省大数据安全与智能处理重点实验室,江苏 南京 210023;
3. 江苏省计算机网络技术重点实验室,江苏 南京 210096)

摘 要:近年来,传染性疾病比如肺炎的大规模爆发给人们敲响警钟。关于传染病患者及其密切接触者的发现以及隔离对于控制疫情异常重要。传统的密切接触者身份追踪依靠被感染者的记忆来回忆他/她接触过的人的名单,并向医院工作人员报告。这种方法不准确、效率低,也不是一种快速抑制病毒传播的方法。针对传染病密切接触者的身份追踪及其隐私保护问题,该文设计了一个传染病密切接触者身份追踪系统,可以保证患者及密切接触者的隐私不被泄露。系统中的身份认证协议,利用零知识证明,证明相遇认证双方公钥的正确产生,节约了公钥证书验证的开销。系统中改进了带属性的群签名,认证患者确诊的事实的同时,隐藏患者的身份,保护了患者及密切接触者的隐私。系统能将患者的密切接触者信息及时锁定并秘密通知本人,来达到疫情控制的目的。从安全性分析和性能分析来看,该系统具有较好的灵活性、安全性、计算效率。

关键词:身份认证;群签名;匿名;隐私保护;零知识证明
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2022)09-0167-07
doi:10.3969/j.issn.1673-629X.2022.09.026

A Privacy-protected Identity Tracking System for Close Contacts of Infectious Diseases

CHEN Liang-jing[1], WANG Zhi-wei[1,2,3]
(1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing 210023, China;
3. Jiangsu Key Laboratory of Computer Networking Technology, Nanjing 210096, China)

Abstract: In recent years, large-scale outbreaks of infectious diseases such as pneumonia have sounded alarm bells. The detection and isolation of patients with infectious diseases and their close contacts is extremely important to control the outbreak. Traditional contact identity tracing relies on an infected person's memory to recall a list of people he/she has been in contact with and report it to hospital staff. This method is inaccurate, inefficient, and not a quick way to suppress the spread of the virus. Aiming at the identity tracking and privacy protection of close contacts of infectious diseases, we design an identity tracking system for close contacts of infectious diseases, which can ensure that the privacy of patients and close contacts is not leaked. The identity authentication protocol in the system uses zero-knowledge proof to prove the correct generation of the public keys of the two parties that meet and authenticate, saving the cost of public key certificate verification. The group signature with attributes has been improved in the system, which verifies the fact that the patient is diagnosed, and at the same time hides the patient's identity and protects the privacy of the patient and close contacts. The system can lock the patient's close contact information in a timely manner and secretly notify the patient to achieve the purpose of epidemic control. From the security analysis and performance analysis, the system has better flexibility, security and computational efficiency.

Key words: identity authentication; group signature; anonymous; privacy protection; zero-knowledge proof

0 引 言

近年来,传染性疾病比如肺炎的大规模爆发给人们敲响警钟。关于传染病患者以及其密切接触者的发现以及隔离对于控制疫情异常重要[1]。政府官员和业

收稿日期:2021-12-13 **修回日期**:2022-04-15
基金项目:江苏省六大人才高峰项目(RJFW-010)
作者简介:陈梁景(1996-),男,硕士研究生,通讯作者,研究方向为公钥密码学和密码学应用;王志伟,博士,教授,江苏省高校青蓝工程中青年学术带头人,江苏省六大人才高峰高层次人才,研究方向为公钥密码学、密码学应用等。

界人士所采取的一种通用方法是(全部或部分)实现人工追踪联系人的广泛任务的自动化。该文主要研究关于隐私保护的传染病密切接触者身份追踪系统。主要思路是:(1)密切接触者相互接触时取得彼此的公钥进行交互认证,认证成功交换彼此的身份密文信息;(2)患者被确诊后,通过执行带地域的群签名加入病人群,管理者为权威医疗机构。将患者保存的密切接触者的加密信息打包公布,并附上群签名;(3)用户读取公布的加密信息,若群签名验证成功且解密密文成功,则上报相关机构去隔离点隔离,从而达到追踪密切接触者身份的目的。必要的情况下,群管理者可以打开签名追踪到确认患者的人员信息。

1 相关工作

在隐私保护方面,Zhang 等人[2]提出了一种基于邻近性的移动社交网络的隐私保护配置文件匹配算法。该算法使用户能够匹配他们的个人资料,而不透露他们的个人资料的任何信息。另一个相关研究方向是移动社交网络中保护隐私的位置共享[3-5]。然而,该领域的大多数解决方案都假设社交网络平台知道每个用户的位置,并提供基于位置的隐私保护搜索功能。澳大利亚与以色列推出了新型冠状病毒安全应用[6]以及一款 HaMagen[7]的联系人追踪应用,然而用户需要对权威机构有高度的信任。另一个研究方向,Naren N[8]和 Alansari S A 等人[9]使用区块链来帮助推进隐私保护相关的接触追踪应用程序。Jan Camenisch[10]提出了一个紧凑群签名。允许授权机构向用户发出带有属性的成员资格凭证。该文将区域属性加入到群签名当中,区域记为相遇的区域编号。如果需要,权威医疗机构可以恢复患者的身份。

该文贡献列举如下:(1)提出了一个隐私保护的传染病密切接触者身份追踪系统方案;(2)方案第一部分提出了一个身份认证协议实现接触者双方的相遇认证,利用零知识验证公钥的正确性;(3)方案提出了一个基于 Jan Camenisch 等人群签名方案的带地域属性的群签名方案,实现了匿名确诊的匿名性、安全性、可追溯性。

2 预备知识

2.1 配 对

给定中性元 1_G 的群 G,G^* 为 $G\backslash\{1_G\}$。一个非对称配对组 (p,G_1,G_2,G_T,e),p 是一个质数,G_1,G_2,G_T 是 p 阶的群,以及 $e:G_1\times G_2\rightarrow G_T$ 是一个有效的可计算的非退化的双线性映射。类型 3 配对群是指已知 G_2 到 G_1 没有有效可计算同态的配对群。

2.2 Elgamal 公钥加密体制

Elgamal 加密算法[11]分为密钥生成算法、加密算法、解密算法,如下:

(1)密钥生成算法:随机选一个安全大素数 p,并生成有限域 Z_p 的一个生成元 $g\in Z_p^*$;选择随机数 $x(1<x<p-1)$,计算 $y\equiv g^x(\mathrm{mod}p)$,公钥为 (y,g,p),私钥为 x。

(2)加密算法:将明文比特串分组,每个分组对应的十进制数小于 p,对每个分组分别加密。用接收方的公钥 (y,g,p);把消息 m 分组为长度为 $L(L<\log_2 p)$ 的消息分组 $m=m_1m_2\cdots m_n$;对第 i 块消息 $(1\leqslant i\leqslant t)$ 随机选择整数 $r_i(1<r_i<p-1)$;计算 $c_i\equiv g^{r_i}(\mathrm{mod}p)$,$c_i'\equiv m_iy^{r_i}(\mathrm{mod}p)$;将密文 $C=(c_1,c_1')\cdots(c_t,c_t')$ 发送给接收方。

(3)解密算法:接收方收到密文,使用私钥 x 计算 $m_i\equiv(\frac{c_i'}{(c_i)^x})\mathrm{mod}p$。

2.3 q-MSDH-1 假设

Pointcheval 和 Sanders 引入了 Modified q-Strong Diffie - Hellman 假设,并证明它拥有一般双线性群模型[12]。暗示了 SDL 假设。

定义 1(q-MSDH-1 假设[12]):设 G 为 3 型配对群发生器。对 G 的 q-MSDH-1 假设,对所有 $\lambda\in\mathbb{N}$,$\Gamma=(p,G_1,G_2,G_T,e)\leftarrow G(1^\lambda)$,给定 $\Gamma,g\in_R G_1^*,\tilde{g}\in_R G_2^*$ 和两个元组 $(g^{x^i},\tilde{g}^{x^i})_{l=0}^q\in(G_1\times G_2)^{q+1}$ 和 $(g^a,\tilde{g}^a,\tilde{g}^{ax})\in G_1\times G_2^2$,对于 $x,a\in_R\mathbb{Z}_p^*$,没有高效的对手可以返回一个元组 $(w,P,h^{1/x+w},h^{a/P(x)})$,其中 $h\in G_1^*$,P 是在 $\mathbb{Z}_p[X]$ 上最多 q 阶的多项式以及 $w\in\mathbb{Z}_p$,这样多项式 $X+w$ 和 P 互素。

2.4 Pointcheval - Sanders 签名方案

Pointcheval 和 Sanders[13]引入一个签名方案,允许签署消息块 $(m_1\cdots m_k)$。G 为 3 型配对组生成器,安全参数 $\lambda\in N$,有配对组 $\Gamma=(p,G,\tilde{G},G_T,e)\leftarrow G(1^\lambda)$。

(1) PS.KG$(\Gamma,k)\rightarrow(\mathrm{pk},\mathrm{sk})$:生成 $\tilde{g}\in\tilde{G}*$,$x,y_1,\cdots,y_{k+1}\in_R\mathbb{Z}_p$,计算 $\tilde{X}\leftarrow\tilde{g}^x,\tilde{Y}_j\leftarrow\tilde{g}^{y_j}$,其中 $j\in[k+1]$。返回 $\mathrm{pk}\leftarrow(\tilde{g},\tilde{X},\tilde{Y}_1,\cdots,\tilde{Y}_{k+1})$ 以及 $\mathrm{sk}\leftarrow(x,y_1,\cdots,y_{k+1})$。

(2) PS.Sign$(\mathrm{sk},(m_1,\cdots,m_k))\rightarrow\sigma$:生成 $h\in_R\tilde{G}*,m'\in_R\mathbb{Z}_p$,并且返回 $\sigma\leftarrow(m',h,h^{x+\sum_{j=1}^k y_jm_j+y_{k+1}m'})$。

(3) PS.Vf$(\mathrm{pk},(m_1,\cdots,m_k),\sigma)\rightarrow b$:将 σ 解析为 (m',σ_1,σ_2),验证 $\sigma_1\neq 1_G$ 并且 $e(\sigma_1,\tilde{X}\prod_{j=1}^k\tilde{Y}_j^{m_j}$

$\tilde{Y}_{k+1}^{m'}) = e(\sigma_2, \tilde{g})$ 。若成立,则返回 1,否则返回 0。

Pointcheval 和 Sanders 证明了[13],该签名方案在 q-MDSH-1 假设下存在不可伪造(见 2.3 节定义 1)。

2.5　零知识证明

零知识证明是一种两方协议,允许一方说服另一方某件事是真的,而不透露其他任何东西。Yuen 等人[14]提出了一个未知阶数群上离散对数(DL)关系的紧凑零知识证明,该文首先考虑一个群元素 $g, w \in G$ 在未知阶群 G 中的简单 DL 关系 R 的 ZK 证明:$R = \{x \in \mathbb{Z} : w = g^x\}$ 。证明者 P 和验证者 V 之间的零知识证明由以下三部分组成。

(1)验证者发送一个随机 λ 位素数 l 。

(2)证明者发现 $q' \in \mathbb{Z}$ 以及 $r \in [0, l-1]$,有 $x = q'l + r$ 。证明者发送 $Q = g^{q'}$ 和 r 给验证者。

(3)验证者验证,如果 $r \in [0, l-1]$ 且 $Q^l g^r = w$,则接受。

3　系统模型和安全模型

3.1　系统模型

系统如图 1 所示,包含三个主体,权威医疗机构、用户和公告板。角色定义如下:

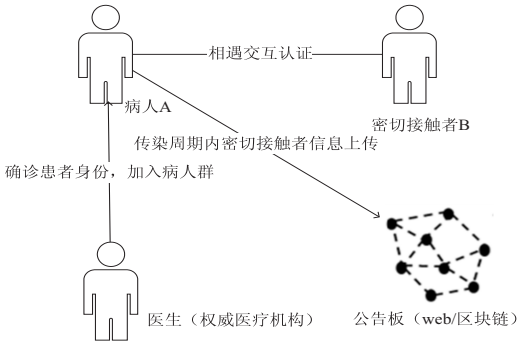

图 1　系统模型

-公告板:用于发布公共信息。它可以通过使用 web 或者区块链系统来实例化。

-用户(User):它可以被称为正常使用手机的人群。在其余部分,使用 Alice 和 Bob 来表示两个用户为密切接触者。

-权威医疗机构(D):只有医生才能将患者确诊,并颁发给患者确诊凭证患者,而医生也隶属于某家医院。

必须做出以下合理假设:

(1)用户不会公开他们的社交活动(例如在微博上发布与某人的合照)。

(2)系统和智能手机都连接到了互联网上。

(3)智能手机可以通过蓝牙连接。

(4)用户不会与他人共享私钥。

(5)医生或医疗机构是完全可信的。

3.2　威胁模型

在实际应用中,一个安全的隐私保护身份追踪系统应满足以下属性:

(1)正确性:用户相遇,彼此可以正确地进行相遇认证,并正确地将对方的身份信息用对方的公钥加密后,保存在自己手机上。若某用户被确诊后,可以正确入群,并取得医生颁发的确诊凭证。此外,若有需要,医生可以正确地恢复出患者的身份信息。

(2)匿名性:除医生外,任何人都不应知道确诊病人的身份详情。对手包括该患者的所有密切接触者(该密切接触者是确诊前的)和公众。任何人,都不应了解确诊患者密切接触者的身份信息,包括接触者的位置。这里的密码敌手试图找出确诊患者密切接触者的所有细节。

(3)可追溯性:当需要时,权威医疗机构可打开病人群签名,可追溯性对于任何有效的令牌,只要发行者是诚实的,它就保证了开放既不能失败,也不能暴露一个不正确的诚实身份。

4　关于隐私保护的密切接触者追踪协议

4.1　概　述

本协议有四个阶段。在注册阶段,用户选择自己的私公钥。医生将获得医院颁发的用户密钥,该密钥用于代表医院生成群签名。在相遇认证阶段,密切接触者之间相互接触取得彼此的公钥,进行公钥零知识证明。认证完毕后,交换彼此的身份信息密文。在匿名确诊阶段,用户确诊后,通过执行带区域属性的群签名加入病人群,管理者为权威医疗机构。在公示解密阶段,将该患者手机中传染周期内的密接者加密信息以及群签名张贴到公告牌上。若群签名验证成功且解密密文成功,则表示该密文信息指向他们自己。必要的情况下,群管理者(医生)可以打开签名追踪到确认患者的身份信息。

4.2　详细描述

4.2.1　注册阶段

(1)用户注册:

Step1:随机选择一个满足安全大素数 p ,并生成有限域 Z_p 的一个生成元 $g \in Z_p^*$;

Step2:用户 Alice 选择一个私钥 sk_A ,私钥为一个随机数 $a(1 < a < p-1)$,计算 $A \equiv g^a (\mathrm{mod} p)$,则公钥 pk_A 为 (A, g, p) ,私钥 sk_A 为 a 。

Step3:Alice 随机生成标识 $\mathrm{ID}_A \in \mathbb{Z}_p$ 。

(2)医生注册:

G 为 3 型配对组生成器, H 为哈希函数,PS 为改进 Pointcheval-Sanders 签名方案。用 k 来表示每个用户的属性个数,本方案仅仅采用一个区域属性, k 取值

为 1。

Step1：Setup(1^λ,k) → pp：生成 $\Gamma = (p, G_1, G_2, G_T, e) \leftarrow G(1^\lambda)$，返回 $(\Gamma, k+1)$。生成公共参数 pp，用于生成发行者(一般情况下为权威医疗机构)密钥。

Step2：KG. D(pp) → (GPK,(GSK,st))：生成 $\tilde{g} \in_R G_2^*$，$(x, y_{ID}, y_1, y_2) \in_R Z_p^{k+3}$，生成 $\tilde{X} \leftarrow \tilde{g}^x$，$\tilde{Y}_{ID} \leftarrow \tilde{g}^{y_{ID}}$，以及 $\tilde{Y}_j \leftarrow \tilde{g}^{y_j}$ $(j = 1,2)$。返回 GPK ← $(\tilde{g}, \tilde{X}, \tilde{Y}_{ID}, \tilde{Y}_1, \tilde{Y}_2)$，GSK ← (GPK, x, y_{ID}, y_1, y_2)，以及一个初始空状态 st ← ∅。

4.2.2 相遇认证阶段

(1)公钥零知识证明。

Alice 和 Bob 相遇，Alice 向 Bob 发送自己的公钥 pk_A。Alice 要向 Bob 证明，Bob 收到的 pk_A：$A = g^a \bmod p$ 是正确产生的，Bob 已收到有效的 Alice 公钥，如下：

①验证者(Bob)发送一个随机 λ 位素数 l 给证明者(Alice)。

②证明者(Alice)的私钥 sk_A 为 $a \in \mathbb{Z}$ 以及 $r \in [0, l-1]$，有 $a = ql + r$，计算 $g^q = Q$。证明者(Alice)发送 r 给验证者(Bob)。

③验证者(Bob)验证，如果 $r \in [0, l-1]$ 且 $Q^l g^r = A$，则确认收到的 pk_A 是正确的。

在另一方面，Bob 也这样做，向 Alice 发送自己的公钥 pk_B，让 Alice 验证他收到的自己的公钥是否是正确产生的。

(2)相遇认证。

相遇认证阶段协议模型如图 2 所示。

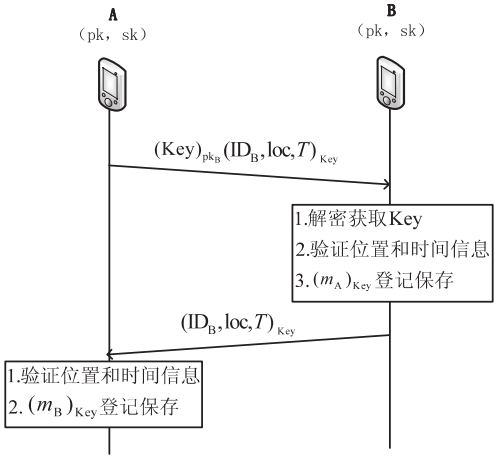

图 2 相遇认证协议模型

认证请求：将 Key 用 Bob 的公钥进行 Elgamal 加密 $C_B = (Key)_{pk_B}$，Key 为一次性会话密钥，用于此会话中接触者双方之间的信息加密通信如下：

Step1：对消息 Key 随机选择整数 r $(1 < r < p-1)$；

Step2：计算 $c \equiv g^r \pmod p$，$c' \equiv y^r \text{Key} \pmod p$；

Step3：生成密文 $C_B = (c, c')$。

将 $m_A = (ID_A, loc, T)$ 用 Key 加密 $C_{Key} = (ID_A, loc, T)_{Key}$ 并将 C_{Key} 和 C_B 一起发送给 Bob。

请求验证：Bob 在接收到消息后，用自己的私钥 sk_B 解密获得对称密钥 Key，如下：

Step1：Bob 收到密文 $C_B = (c, c')$；

Step2：用私钥 a 计算 $\text{Key} \equiv (\frac{c'}{c^a}) \bmod p$；

Step3：得到明文 m = Key。

接触者 Bob 可以解密 $(m_A)_{Key}$，从而获取 Alice 的相关信息(身份标识，相遇地点编号，时间戳)。用 pk_A 对 m_A 进行 Elgamal 加密。将加密完的信息登记在 B 的手机上。

请求响应：相对的，Bob 也这样做，将 m_B 用 Key 加密 $C_{Key} = (m_B)_{Key}$。Bob 向 Alice 发送响应消息 $(m_B)_{Key}$。其中 m_B 为 Bob 的相关信息，而 $m_B = (ID_B, loc, T)$，其中 ID_B 为 Bob 的身份标识，loc 为接触者双方相遇的地点，T 为接触者双方相遇的时间。

响应确认：在接收到消息后，Alice 使用对称密钥可以解密 C_{Key}，从而获取 Bob 的相关信息(身份标识，相遇地点编号，时间戳)。验证相遇地点编号以及时间戳，不同则验证失败。用 pk_B 对 m_B 进行 Elgamal 加密。将加密信息登记在 Alice 的手机上。

4.2.3 匿名确诊阶段

在本小节中，将介绍关于一个重要构建块，即带区域属性的动态群签名，基于动态群签名[15]改进而来。本阶段通过权威医疗机构和用户之间发行签名，来实现用户信息的隐私保护以及匿名。

(1)生成确诊凭证。

Issue：为了在用户 u 和权威医疗机构 D 之间发行签名，假设用户和发行者之间通信的信道是安全信道。如果一方中止协议，则返回 $\perp$。进一步假设身份空间 ID 是 Z_p 的多项式大小的子集。

Step1：Issue. D(sk,st,ID,regionid)。

–如果 st 中存在记录 (ID,regionid,*)，则中止；

– $\sigma = (a', \sigma_1, \sigma_2) \leftarrow$ PS. Sign(sk,(ID,T))；

–将 σ 发送给 u，并返回 st′

← st ∪ (ID,regionid,a')，将状态更新为 st′。

ID 是患者用户的身份标识，regionid 为患者用户所在区域的编号值。PS 为改进的 Pointcheval-Sanders 签名方案。

Step2：Issue. U(ID,regionid,pk)，一旦从 D 接收到 σ：

–验证 PS. Vf(GPK,(ID,regionid),σ) = 1，如果不是则中止；

– 返回 $\text{cred} \leftarrow (\text{ID}, \text{regionid}, \sigma, e(\sigma_1, \tilde{Y}_{\text{ID}}), e(\sigma_1, \tilde{Y}_2))$。

cred 为病人加入病人群的入群凭证。确诊的病人加入病人群。

(2)匿名签名。

对确诊患者的密切接触者的加密信息,用带地域属性的群签名签名。表明该信息确实是来自确诊病人,且是该确诊病人的密切接触者相关信息。

$\text{Auth}(\text{GPK}, \text{cred}, m) \rightarrow \text{tok}$:分析 $\text{cred} = (\text{ID}, \text{regionid}, \sigma, e(\sigma_1, \tilde{Y}_{\text{ID}}), e(\sigma_1, \tilde{Y}_2))$,生成 $r \in_R \mathbb{Z}_p^*$,计算 $(\sigma_1', \sigma_2') \leftarrow (\sigma_1^r, \sigma_2^r)$ 以及一个 (ID, a') 的知识的非交互式证明 π,如下:$e(\sigma_1', \tilde{X}\, \tilde{Y}_{\text{ID}}^{\text{ID}}\, \tilde{Y}_1^{a_1}\, \tilde{Y}_2^{a'}) = e(\sigma_2', \tilde{g})$。也就是说,计算 $u \leftarrow e(\sigma_1^{rs}\text{ID}, \tilde{Y}_{\text{ID}}) e(\sigma_1^{rs} a', \tilde{Y}_2)$,其中 $s_{\text{ID}}, s_{a'} \in_R \mathbb{Z}_p$,计算一个挑战 $c \leftarrow H(u, A, m, \sigma_1', \sigma_2', \text{pk}) \in \mathbb{Z}_p$ 以及一个响应 $v \leftarrow (s_{\text{ID}} - c\text{ID}, s_{a'} - ca') \in \mathbb{Z}_p$。设 $\pi \leftarrow (c, v)$,并且返回 $\text{tok} \leftarrow (\sigma_1', \sigma_2', \pi)$。

m 即为确诊病人最近传染周期内的密切接触者 Bob 的加密信息 $(m_{\text{B}})_{\text{pk}_{\text{B}}}$。tok 为确诊患者对其最近传染周期内的密切接触者(例如 Bob)的加密信息的签名。

4.2.4　公示解密阶段

(1)签名公示。

Step1:权威医疗机构对确诊患者最近传染周期内的若干个(n 个)密切接触者的加密信息进行签名。$\sigma* = (m', \sigma_1^*, \sigma_2^*) \leftarrow \text{PS.Sign}(\text{GSK}, (m_1, \cdots, m_n))$。$\sigma*$ 是权威医疗机构对确诊患者最近传染周期内的 n 个密切接触者的加密信息的签名。m_i 是确诊患者最近传染周期内的密切接触者(例如 Bob)的加密信息 $(m_{\text{B}})_{\text{pk}_{\text{B}}}$, $i \in [m_{\text{B}}]$。GSK 是权威医疗机构的私钥。

Step2:将确诊患者最近传染周期内的密切接触者(例如 Bob)的加密信息 $(m_{\text{B}})_{\text{pk}_{\text{B}}}$ 和 tok 以及 $\sigma*$ 公布在公告板上。公布信息时,按照患者所在区域划分进行公布。

(2)解密查询。

Step1:外界用户验证信息真实性以及是否被篡改。

①先验证该信息是否被权威医疗机构授权。验证 $\text{PS.Vf}(\text{GPK}, (m_1, \cdots, m_n), \sigma*) = 1$,若不是,则该信息无效。

②验证公布在公告板上的 tok 带属性的群签名,若验证成功,则该信息确实是来自确诊患者。$\text{Vf}(\text{GPK}, m, \text{regionid}, \text{tok}) \rightarrow b$:用 $\pi = (c, v_{\text{ID}}, v_a)$, $\text{regionid} = a_1$ 来分析 $\text{tok} = (\sigma_1, \sigma_2, \pi)$。如果 $\sigma_1 \neq 1_G$ 且 $c = H_0(u, \text{regionid}, m, \sigma_1, \sigma_2, \text{GPK})$,则返回 1。这是因为 $u \leftarrow e(\sigma_1^{v_{\text{ID}}}, \tilde{Y}_{\text{ID}}) e(\sigma_1^{v_{a'}}, \tilde{Y}_2) e(\sigma_2^c, \tilde{g})\, e(\sigma_1^c, \tilde{X}^{-1}\, \tilde{Y}_1^{-a_1})$。

Step2:验证成功之后,用户读取加密信息。如果可以用自己的私钥解密某个加密信息,若能解密其中某个信息,则说明该用户就是确诊患者的密切接触者之一。

4.2.5　身份追踪

医疗机构可打开群签名,找到确诊患者的身份信息。$\text{Open}(\text{GSK}, \text{st}, m, \text{regionid}, \text{tok}) \rightarrow \text{ID}/\perp$:为消息 m 属性 regionid 生成身份验证令牌 $\text{tok} = (\sigma_1, \sigma_2, \pi)$ 的用户恢复身份 ID。它首先验证 tok 对 m 和 regionid 是否有效。验证成功,遍历 st 中的元组 $(\text{ID}, \text{regionid}, a')$,直到找到一个使得 (a', σ_1, σ_2) 在 $(\text{ID}, \text{regionid})$ 上是一个有效的 PS 签名,然后返回 ID。如果没有找到这样的元组,则返回 $\perp$。

5　方案的安全性及性能分析

5.1　安全性分析

本方案的安全性主要是基于带属性的动态群签名方案[10]以及 ElGamal 加密体制的安全性。

定理 1:在随机 oracle 模型中,如果第一组 DDH 和 SDL 假设都对组生成器 G 有效,则带地域属性的动态群签名方案满足匿名性。

证明:类似于 Jan Camenisch 等人方案的证明,利用混合参数证明了 DGSR 的匿名性。由 C_b 挑战者,使用凭据 ID_b^* 和 regionid^*,其中 $b \in \{0,1\}$。让 Δ 算法,除挑战阶段外,过程和 C_0 完全一样。在挑战阶段,Δ 发送两个随机 G_1 的元素作为 PS 签名的再次随机化的群元素 $(\text{ID}_0^*, \text{regionid}^*)$,并相应地编写随机预言程序。准确地说,在匿名实验中考虑一个高效的对手 Λ。Δ 与 Λ 互相作用,当 Λ 发出挑战查询,Δ 先检查是否已生成一个凭证 cred_b,其中 $b \in \{0,1\}$。若不是,则中止,否则生成 $\sigma_1, \sigma_2 \in_R G_2$,以及 $s_{\text{ID}}, s_{a'} \in_R \mathbb{Z}_p$,计算 $u \leftarrow e(\sigma_1^{v_{\text{ID}}}, \tilde{Y}_{\text{ID}}) e(\sigma_1^{v_{a'}}, \tilde{Y}_2) e(\sigma_2^c, \tilde{g})\, e(\sigma_1^c, \tilde{X}^{-1}\, \tilde{Y}_1^{-a_1})$,以及 $c \leftarrow H_0(u, \text{regionid}^*, m^*, \sigma_1, \sigma_2, \text{GPK})$。$\Delta$ 设置 $\pi \leftarrow (c, s_{\text{ID}}, s_{a'})$,以及返回 $(\sigma_1, \sigma_2, \pi)$ 给 Λ。

Δ 对查询挑战的回答由于 C 计算的 σ_1 和 σ_2 的分布,在计算上与 C_0 的回答没有区别,且 Δ 在 G_1 中的 DDH 假设下是不可区分的。C_0 和 Δ 的不可区分性论证类似于 Jan Camenisch 等人方案[10]的证明。

为了回答 $(\text{ID}_0^*, \text{regionid}, m)$ 上的 Auth 查询,还原算法编写随机预言程序生成知识证明。

为了回答 Open 查询 $(m, \text{regionid}, \text{tok})$,还原算法首先验证其有效性,利用分叉引理[16],其过程类似于 Jan Camenisch 等人方案[10]的证明过程。在挑战阶段,

如果 $(ID_0^*, regionid_0^*) = (ID^*, regionid^*)$，查询和应答阶段类似于 Jan Camenisch 等人方案[10]的证明过程。证明可得在 SDL 假设下，tok 不可能是伪造的对于一个身份标识 ID，因为 (ID，regionid) 是诚实的。还原算法(对于 DDH 游戏)运行 Open 算法并返回其输出。

还原算法回答安全游戏中指定的其他查询。在挑战阶段，若猜测错误，还原算法会中止，否则计算 $(g_2, g_2^{x+y_1a_1+y_2a'} g_3^{ry_{i0}ID_0^*})$，通过编程随机预言模仿涉及到哈希中的 m^* 的知识证明，并将配对和证明作为挑战标记进行回复。如果 (g_0, g_1, g_2, g_3) 是 DDH 元组，它作为 C_0 或者 Δ 的响应分发。

还原(reduction)算法像挑战之前一样回答其他查询。因此，对 Issue，Issue. D，Auth， Corrupt，Open 查询和挑战的查询的联合分布的答案还原算法都相同地分布到 C_0 或 Δ，这取决于 (g_0, g_1, g_2, g_3) 是否为 DDH 元组。因此 DDH 假设下，C_0 和 Δ 在计算上不可区分(任何对手的明显优势最多是先验还原算法 $|ID|^2$ 倍 DDH 优势)。同样，Δ 和 C_1 在计算上无法区分。C_0 和 C_1 在计算上不可区分，DGSR 在 DDH 假设下满足匿名性。接着，列举一些典型的攻击进行分析：

5.1.1 敌手的窃听攻击

窃听是一种捕获未经授权的机密信息的攻击。加密提供了强大的防御窃听。在该框架中，所有通信都是加密的，以防止窃听。从理论上讲，如果攻击者无法获得密钥，他们就无法解密消息以获得消息内部的内容。

5.1.2 中间人攻击

中间人(man-in-middle，MITM)攻击是指攻击者在通信过程中伪装成正确的人，利用从一方接收到的信息欺骗另一方。受害者双方都觉得他们在直接交换信息。然而，本协议采用了零知识证明，能够验证彼此公钥是否是正确产生的，无法冒充其他人，并把自己的公钥顶替他人的公钥。不能将无效公钥引入认证。它保证了对 MITM 攻击的强大防御，因为 MITM 攻击者不可能在没有正确的私钥的情况下实现公钥的零知识证明。

5.1.3 重放攻击

在重放攻击中，攻击者获取两个受害者之间的信息并拦截该信息并欺骗性地重放它。这种攻击可以通过在相遇认证中使用一次性共享密钥来禁用。此外，这两个认证都使用时间戳和带随机数的 ElGamal 加密体制来防止应答攻击。如果攻击者想要实现他的目标，他必须猜测一次性共享密钥，但正如上面分析的，这几乎是不可能的。

5.2 性能分析

对协议进行性能评估，测试环境如下：处理器：Intel(R) Core(TM) i7-8550U CPU @ 1.80 GHz 2.00 GHz，RAM 16.00 GB。

语言：Java+JPBC 库+Bouncycastle 第三方库。

5.2.1 相遇身份认证性能分析

为方便后续的性能评估，定义以下符号：T_h ：运行 1 次 Hash 函数所需的时间($T_h \approx 0.32$ ms)；T_s ：运行 1 次对称加密所需的时间($T_s \approx 0.8$ ms)；T_e ：运行一次 Elgamal 加密或解密所需要的平均时间($T_e \approx 2.6$ ms)；T_{zk} ：运行 1 次公钥零知识证明所需的时间($T_{zk} \approx 13$ ms)。异或运算的计算量很小，忽略不计。上述这些操作运行所花费的时间为 10 次实验的平均值。

表 1 身份认证性能比较

协议	运算次数	总执行时间/ms
Zhao[17]	$6T_s + 14T_e + 3T_h$	56.16
文中协议	$2T_{zk} + 3T_s + 4T_e$	38.8

表 1 列出了文中相遇阶段身份认证协议与 Zhao[17]身份认证协议计算开销的对比。且文中对相遇双方执行了高效的零知识证明[14]。无需第三方 CA 机构，仅通过双方进行彼此公钥的零知识证明，即可确认彼此公钥的正确性。Zhao[17]协议是非对称密钥双向认证协议，需要彼此注册身份，且登录和双向认证阶段的信息构造运算较为复杂。文中相遇阶段身份认证协议相比 Zhao[17]的身份认证协议在保证安全性的同时也更加高效。且应用 Yuen[14]的紧致零知识证明仅仅需要一次实现验证，十分高效。

5.2.2 匿名确诊阶段性能分析

病人身份验证令牌包含两个 G_1 元素和三个 $\mathbb{Z}_p$ 元素，共计 232 个字节。群签名知识证明中的哈希值实际上可以缩短，进一步将群签名缩短为 216 字节。在本方案中，由于令牌大小为 216 字节，基于配对的实例化足够紧凑，可以与本协议的病人确诊方案结合使用。

本次测试分别测试文中方案匿名确诊阶段群签名的令牌生成过程、签名过程所消耗的时间，同时在相同环境下与 Jan Camenisch[10]方案进行了测量比较，结果如表 2 所示。

表 2 匿名确诊性能比较 ms

方案	入群令牌生成时间	群签名生成时间
Jan Camenisch[10]	281	156.16
文中方案	269	138.8

如表 2 所示，文中方案在效率上略优于 Jan Camenisch[10]方案。文中方案采用带地域属性的动态群签名方案，仅采用一个属性，相较于 Jan Camenisch 提出的多属性动态群签名方案更为简便，在性能上更

加优秀。

5.2.3　公示解密阶段性能分析

图 3 表示在公示解密阶段,512 bit 和 1 024 bit 密钥长度时,匹配解密一定数量的密文的性能情况。公布的密文越多,解密匹配的次数越多,运行时间也越多。密钥长度也会影响运行的时间。为了保证实验的随机性和真实性,分别随机选取 50 条,100 条,150 条,200 条密文进行解密匹配,计算时间消耗。计算 200 次时,1 024 bit 密钥长度的时间消耗都在 1 000 ms 以下,512 bit 密钥长度的时间消耗仅有 100 ms 左右。

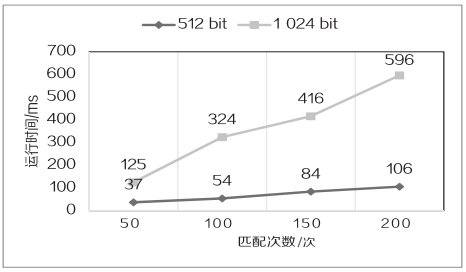

图 3　解密匹配执行时间

考虑到实际的计算能力远远高于文中的实验条件,解密匹配的时间消耗会更短,因此文中协议具有较好的性能。且 Elgamal 虽然是公钥密码体制,但身份信息较短,约 256 比特,解密代价较小,能够为资源受限的用户设备所容忍。

6　结束语

用 ElGamal 加密体制以及 Yuen 的零知识证明方法,来验证相遇双方身份。采用对称加密实现加密传输彼此身份信息,用对方公钥将对方身份信息加密保存在自己手机上。在病人匿名确诊认证阶段,基于带属性的群签名,对患者确诊进行匿名认证。在必要情况下,可以通过打开群签名的方式来达到追踪患者身份的目的。该方案的隐私保护特性在于:(1)匿名性:患者身份不能泄露;(2)可追踪性:在公示阶段,用户可通过尝试解密公布的加密信息来验证自己是否为患者的密切接触者。

参考文献:

[1] ALTUWAIYAN T,HADIAN M,LIANG X. EPIC:efficient privacy-preserving contact tracing for infection detection [C]//2018 IEEE international conference on communications (ICC). Kansas City:IEEE,2018:1-6.

[2] ZHANG R,ZHANG J,ZHANG Y,et al. Privacy-preserving profile matching for proximity-based mobile social networking[J]. IEEE Journal on Selected Areas in Communications,2013,31(9):656-668.

[3] PIETRZAK K. Delayed authentication:preventing replay and relay attacks in private contact tracing[C]//International conference on cryptology in india. [s.l.]:Springer,2020:3-15.

[4] WEI W,XU F,LI Q. MobiShare:flexible privacy-preserving location sharing in mobile online social networks[C]//IEEE infocom. Orlando:IEEE,2012:2616-2620.

[5] LI X Y,JUNG T. Search me if you can: privacy-preserving location query service[C]//2013 Proceedings IEEE infocom. Turin:IEEE,2013:2760-2768.

[6] Australian Government Department of Health. COVIDSafe app[EB/OL]. 2020-05-01. https://www.health.gov.au/resources/apps-and-tools/covidsafe-app.

[7] Israel Government Health Ministry. HaMagen[EB/OL]. 2020-05-01. https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/.

[8] TAHILIANI A,HASSIJA V,CHAMOLA V,et al. Privacy-preserving and incentivized contact tracing for covid-19 using blockchain[J]. IEEE Internet of Things Magazine,2021,4(3):72-79.

[9] ALANSARI S A,BADR M M,MAHMOUD M,et al. Efficient and privacy-preserving contact tracing system for Covid-19 using blockchain[C]//2021 IEEE international conference on communications workshops (ICC Workshops). Montreal:IEEE,2021:1-6.

[10] CAMENISCH J,DRIJVERS M,LEHMANN A,et al. Zone encryption with anonymous authentication for V2V communication[C]// 2020 IEEE European symposium on security and privacy (EuroS&P). San Francisco:IEEE,2020:405-424.

[11] GAMAL T E. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory,1985,31(4):469-472.

[12] POINTCHEVAL D,SANDERS O. Short randomizable signatures[C]//Cryptographers' track at the RSA conference. San Francisco:Springer,2016:111-126.

[13] POINTCHEVAL D,SANDERS O. Reassessing security of randomizable signatures[C]//Cryptographers track at the RSA conference. San Francisco:Springer,2018:319-338.

[14] YUEN T H,CUI H,XIE X. Compact zero-knowledge proofs for threshold ECDSA with trustless setup[C]//IACR international conference on public-key cryptography. [s.l.]:Springer,2021:481-511.

[15] BELLARE M,SHI H,ZHANG C. Foundations of group signatures:the case of dynamic groups[C]//Cryptographers' track at the RSA conference. San Francisco:Springer,2005:136-153.

[16] BELLARE M,NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[C]//Proceedings of the 13th ACM conference on computer and communications security. New York:ACM,2006:390-399.

[17] 赵玉超. 一种基于非对称加密算法的安全高效身份认证协议[J]. 工业技术创新,2020,07(6):103-107.