一种基于群签名的流行病密接者追踪方案

潘阿磊　岳笑含
沈阳工业大学　辽宁沈阳　110870

摘　要：流行病的传播严重威胁着全世界的生命和经济。2019 年冠状病毒 COVID-19 的爆发促使科学界设计并实施了“密接者追踪”机制，该机制通过移动设备记录密切接触者，以减缓此类流行病的进一步传播。然而，由于密接追踪涉及大量隐私数据，此类应用程序引起的安全和隐私问题引起了公众的关注。本文针对现有联系人跟踪方案的不足，利用非交互式零知识证明和群签名等密码学技术提出了一种隐私保护且可验证的联系人跟踪方案。此外，本方案保证了一定的安全性，可以抵抗大多数攻击。

关键词：密接者追踪；流行病；群签名；隐私保护

An epidemic contact tracing scheme based on group signature

Alei Pan,Xiaohan Yue
Shenyang University of Technology,Shenyang,Liaoning,110870

Abstract: The spread of epidemics poses a serious threat to life and the economy worldwide. The outbreak of the coronavirus COVID-19 in 2019 prompted the scientific community to design and implement "close contact tracing" mechanisms, which record close contacts through mobile devices to slow down the further spread of such epidemics. However, as close contact tracing involves a large amount of privacy data, security and privacy issues arising from such applications have raised public concerns. This paper proposes a privacy-preserving and verifiable contact tracing scheme using cryptographic techniques such as non-interactive zero-knowledge proofs and group signatures to address the shortcomings of existing contact tracing schemes. In addition, this scheme guarantees a certain degree of security and can resist most attacks.

Keywords: Contact tracing; Epidemics; Group signature; Privacy protection

引言

长期以来，流行病一直是人类社会最致命的威胁之一，例如Ebola、SARS等。而最近的例子就是2019冠状病毒(COVID-19)的爆发，世界卫生组织(WHO)在2020年1月30日正式宣布COVID-19为突发公共卫生事件[1-2]。新冠病毒爆发改变了世界各国每个人的生活方式，迫使各国政府采取一系列的防疫措施以控制疾病的再次传播[3]。其中密接者追踪[4]是遏制大流行的一个相当重要的概念，其目的是识别并随后隔离可能是病毒携带者的人。传统的密接者追踪基于一个过程，在该过程中，负责流调的工作人员根据阳性感染者所述到过的地方以及时间点来进行密接者追踪[5]。

一、本文的主要贡献

综上所述，根据现有密接者追踪应用需要解决的一些问题，本文利用群签名和零知识证明[5]等密码学技术和BLE通信技术，提出了一种基于群签名的流行病密接者追踪隐私保护方案，该方案满足密接者追踪所需要的有效性、隐私性和安全性等需求。贡献如下：

1）本文的方案通过非交互式零知识证明和群签名技术允许用户以保护隐私但经过身份验证的方式记录他们的密切接触者。不论是密切接触者还是阳性用户都不能通过匿名认证信息把彼此真实身份关联起来。

2）本文的方案通过撤销列表实现访问控制，通过将阳性用户撤销，限制阳性用户生成与未来时间段的有效令牌，使阳性用户不能以正常用户的方式继续进行交互，防止阳性患者与正常用户混淆而破坏追踪的有效性。

3）由于本文的方案是根据XDH，DDH，DL和q-SDH假设构建的，因此可以完全保证安全性，抵御一些敌手的攻击。

二、系统模型和安全需求

2.1系统模型

本文定义的系统模型如图1所示，其中包含四种参与的实体，即可信中心(TA)，应用管理员(GM)，用户(User)以及医疗机构(HA)。

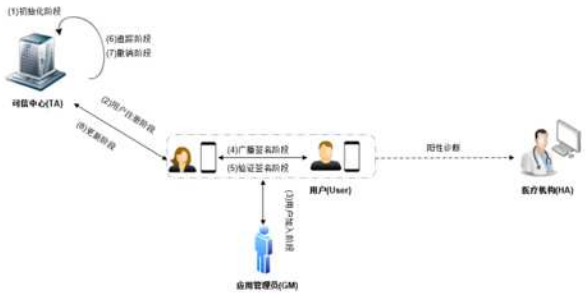

图 1 系统模型

1）可信中心(TA):可信中心作为一个可信的实体，负责维护整个系统。在我们的方案中，可信中心负责用户的注册和密接者的追踪以及阳性用户的撤销。生成并发布全局的公共参数，供实体生成各自的公私钥。

2）应用管理员(GM):应用管理员作为该手机应用的管理员，为每个申请加入应用的用户生成一个有效的成员资格证书，用户获得有效的成员资格证书后才能进行交互。

3）用户(User):用户在智能移动设备安装密接者追踪应用程序。每个用户通过成员资格证书和用户的签名私钥生成可供验证的签名，在与其他用户相遇时通过蓝牙通信协议交换签名，互相验证通过后，作为彼此密接的凭证保存。若用户被诊断为阳性后，将会把过去14天接收到的签名上传给可信中心。

4）医疗中心(HA):负责阳性用户的诊断。

2.2安全需求

有效的密接者追踪方案必须有效防止各种攻击，并保护所有参与者的隐私免受侵害。为了实现我们的目的，本文的方案需要满足以下的一些安全和隐私需求：

1）隐私性：所有交互的用户都不知道对方的身份，并且数据都具有可验证性，在验证时不必交互相关数据就能通过公开参数验证数据的正确性。

2）不可诬陷性：所有用户都不能够产生能让验证者通过的证据，这就避免了某些恶意用户生成伪造的凭证去诬陷他人。

3）后向安全性：能够有效及时的撤销阳性患者，使阳性患者不在参与过程的交互，从而避免了破坏追踪效率的可能。

三、预备知识

在本节，我们将列举本方案所用到的一些密码学原语。

3.1 双线性映射

设G_1,G_2,G_T是三个阶乘法循环群，P为λ位的大素数，其中g_1是G_1的生成元，g_2是G_2的生成元，则$e:G_1\times G_2\to G_T$是G_1和G_2的一个双线性配对或双线性映射，并且满足以下的性质：

1）双线性：对于任意的

$a,b\in\mathbb{Z}_p$，$g_1\in G_1$，$g_2\in G_2$，均有$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$成立。

2）非退化性：存在

$g_1\in G_1$，$g_2\in G_2$，满足$e(g_1,g_2)\neq 1_{G_T}$，1_{G_T}是G_T的单位元。

3）可计算性：存在有效的算法，对任意的

$g_1\in G_1$，$g_2\in G_2$，存在一个有效的算法计算$e(g_1,g_2)$。

3.2 零知识证明

零知识证明，是指证明者向验证者证明其拥有解决某困难问题的知识，证明完成后，验证者可以确信证明者有此能力，但验证者只能验证证明者的证明有效，并不能从证明的交互过程中获得任何解决该困难问题的知识。非交互式零知识证明具备以下性质：

1）完备性：对于任意x属于NP语言L的元素，其证据为w，有：

$$Pr[s\leftarrow_R\{0,1\}^{poly};\pi\leftarrow P(s,x,w):V(s,x,\pi)=1]=1$$

2）可靠性：如果x不属于NP语言L的元素，以下概率都是可忽略不计的：

$$Pr[s\leftarrow_R\{0,1\}^{poly};\pi\leftarrow P^*(s,x):V(s,x,\pi)=1]$$

3）零知识性：假设存在一个多项式时间的模拟器S，使得所有的X属于NP语言L的元素，其证据为w，以下两个分布在计算上是不可区分的：

$$\{s\leftarrow_R\{0,1\}^{poly};\pi\leftarrow P(s,x,w):(s,x,\pi)\},$$
$$\{(s,\pi)\leftarrow S(x):(s,x,\pi)\}$$

四、方案设计

在本节中，提出了一种基于群签名的流行病密接者追踪隐私保护方案，并给出了方案的设计。我们假设方案中实体的交互是通过安全信道完成的。

1）参数生成阶段：生成参与实体的密钥对。具体步骤如下：

1.1）初始化算法（$Setup(1^\lambda)\to(p)$）：此算法主要用于生成全局公共参数。可信中心输入一个安全参数λ，输出全局的公共参数P。

1.2）可信中心密钥生成算法

（$RKeyGen(pp)\to(tk_T,rk_T)$）：此算法将全局参数P作为输入，输出可信中心的密钥对（tk_T,rk_T）。分别作为注册中心的追踪令牌密钥和撤销令牌密钥，tk_T可在追踪阶段进行用户的追踪，rk_T根据撤销令牌的有效性可以确认用户是否处于撤销状态。

1.3）应用管理员密钥生成算法

（$GKeyGen(p)\to(sk_G,pk_G)$）：此算法将全局参数p作为输入，输出应用管理员密钥对（sk_G,pk_G）。其中sk_G管理员的签名私钥，用于新用户加入。sk_G为应用管理员的公钥。

1.4）用户密钥生成算法

（（$UKeyGen(p)\to(sk_u,pk_u)$）：此算法将全局参数P作为输入，输出用户密钥对（sk_u,pk_u）。其中sk_u用于生成签名。

2）用户注册阶段：用户向可信中心注册，生成关于自己公钥pk_u的公钥证书$TCert_u$，并且可信中心维

护一个撤销列表 RL_t，具体步骤如下：

2.1) 所有用户与可信中心TA交互，通过零知识证明技术向可信中心证明自己是私钥 sk_u 的持有者。

2.2）：可信中心利用私钥生成一个关于用户公钥 pk_u 的公钥证书 $TCert_u$，并且维护一个撤销列表 RL_t。最后可信中心将会 $\{i, TCert_{u,i}, pk_{u,i}\}$ 把保存在本地注册列表 reg 中，其中*是在成员加入阶段生成的成员资格证书。

3）成员加入阶段：用户需向应用管理员请求成员资格证书，由应用管理员来颁发成员资格证书 $GCert_u$ 成为一名合法的成员。具体步骤如下：

3.1）当用户申请加入应用时，向应用管理员发送请求获取应用管理员公钥 pk_G。

3.2）用户用应用管理员公钥 pk_G 执行加密算法加密 $(TCert_u, pk_u)$ 输出 C_u。将 C_u 发送给应用管理员。此步骤的目的是让用户向群管理员发送凭证用以验证身份的有效性。

3.3）应用管理员收到 C_u 并解密，然后检查 $TCert_u$ 是否存在于由可信中心维护的已撤销公钥证书列表 RC_t，其中 RC_t 中保存的是阳性用户的公钥证书。如果不存在且 $(TCert_u, pk_u)$ 有效则执行下一步。

3.4）应用管理员计算生成这个用户的成员资格证书 $GCert_u$，并返回给给用户和可信中心。用户验证 $GCert_u$ 的有效性，若有效则保存。可信中心将 $GCert_u$ 保存到 reg 中。

3.5）广播签名阶段：用户执行签名算法 $Sign\ (p, t, token_{i,t}, GCert_u, sk_u, M)$ 输入一个有效的纪元和此纪元的有效的未撤销令牌 $token_{i,t}$，一个有效的成员资格证书 $GCert_u$，签名私钥 sk_u 和M消息，利用非交互式零知识证明技术构建并输出一个签名 σ。最后将签名消息对 $C = (M, \sigma)$ 广播出去。

3.6）验证阶段：当两位用户在某个时间某个地点在某个距离之内相遇，会通过蓝牙交互通信技术互相交互自己的签名消息对 $m = (M, \sigma)$。两位用户彼此交换签名后，先执行验证算法 $Verify(p, t, m, pk_G)$ 验证签名的有效性和身份的有效性，若验证通过再保存在本地。验证算法输入一个有效的签名 σ 和M消息，一个撤销纪元t，群管理员公钥 pk_G，若验证通过，则相遇的两人保存彼此的签名消息对 $m = (M, \sigma)$。

3.7）追踪阶段：此阶段用于追踪阳性用户和密接者，一旦某个用户被医疗机构诊断为阳性，他将会向可信中心上传自己过去14天接收其他用户的签名密钥对 $m_i = (M, \sigma)$。可信中心将会执行追踪算法 $Trace(p, tk_T, RL_t, m)$ 最后从可信中心本地存储的注册列表 $\{i, TCert_{u,i}, pk_{u,i}, GCert_u\} \in reg$ 追溯到这些人的公钥证书，从而找到密接者并及时隔离。具体步骤如下：

7.1）可信中心运行此算法可以从追踪到用户，即 $GCert_u = \mu_1/\mu_3^{tk_T}$。然后在注册列表 reg 中可以确定用户的成员资格证书 $GCert_u$，从而找到密接者。

7.2）若用户为阳性，用步骤6.1）的方法追踪到阳性患者，并将阳性患者 $TCert_{u,i}$ 加入到阳性公钥证书列表 RC_t。

五、结束语

在本文中，我们针对流行病密接者追踪应用中的关键隐私性问题，提出了一种基于群签名的、保护隐私且可验证的密接者追踪方案。既满足了追踪的有效性，也保护了隐私和安全性。在注册阶段仅通过零知识证明向TA证明私钥的合法性。在广播签名阶段，仅将通过非交互式零知识证明生成的一个可验证知识的签名通过BLE广播出去，不暴露任何私有知识。除了可信中心之外任何人都不能通过这个可验证知识的签名识别出用户的身份信息，因此很好的保证了用户的隐私，并保证了身份有效性和数据完整性。当用户被确诊为阳性时，该用户的公钥证书会被TA添加到撤销列表中，以此来保障后向安全性。并且利用BBS+签名不可伪造性的特点，使任何阳性用户或敌手不能够伪造一个能够通过验证的成员资格证书和撤销令牌，有效防止了大部分的攻击。

参考文献：

[1] A. E. Gorbalenya et al., “The species severe acutacute respiratory syndromerelated coronavirus: Classifying 2019–nCoV and naming it SARS–CoV–2,” Nat. Microbiol., vol. 5, pp. 536 – 544, Mar. 2020.

[2]WHO.Who Declared the Corona Virus Disease 2019[DB /OL],2020.

[3]A. Hekmati, G. Ramachandran, and B.Krishnamachari, “Contain:Privacy–oriented contact tracing protocols for epidemics,” arXiv preprint arXiv:2004.05251, 2020.

[4]A. Hekmati, G. Ramachandran, and B.Krishnamachari, “Contain:Privacy–oriented contact tracing protocols for epidemics,” arXiv preprint arXiv:2004.05251, 2020.

[5]C. Watson, A. Cicero, J. Blumenstock, and M. Fraser, “A national plan to enable comprehensive COVID–19 case finding and contact tracing in the US,” 2020.

[6] 王 冬, 徐正全，“新冠肺炎疫情下接触者追踪的隐私风险及保护”. 吉林大学学报(信息科学版), 2021, 39(5): 562–568.

[7]H.Cho,D. Ippolito,Y. Yu.Contact Tracing Mobile Apps for Covid–19: Privacy Considerations and Related–Trade–offs [DB/OL],2020.

[8]Washington Post.Contact Tracing Apps Can Help Stop Corona Virus.But They Can Hurt Privacy [DB/OL],2020.

[9]K. Nabben，C.Berg. The Covid Safe App Was Just one Contact Tracing Option.These Alternatives Guarantee More Privacy［DB /OL］,2020.

[10]N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere,A. Seneviratne, W. Hu, H. Janicke,

and S. K. Jha, ‘A survey of COVID-19 contact tracing apps,’’ IEEE Access, vol. 8, pp. 134577 - 134601, 2020.

[11] Yue X, Chen B, Wang X, Duan Y, Gao M, He Y . An efficient and secure anonymous authentication scheme forvanets based on the framework of group signatures. IEEE Access6(1):62584-62600,2018