

基于比特币区块链的公共无线局域网接入控制隐私保护研究

牛玉坤¹, 魏凌波¹, 张弛¹, 张霞², Gustavo Vejarano³

(1. 中国科学技术大学信息科学技术学院, 安徽 合肥 230026;

2. 武汉理工大学计算机科学与技术学院, 湖北 武汉 430047;

3. Department of Electrical Engineering and Computer Science, Loyola Marymount University, Los Angeles, CA 90045)

摘要: 在公共无线局域网的访问控制中, 用户隐私保护和用户可问责性是一对相互冲突的目标。针对该问题, 提出了一种基于比特币区块链和 Intel SGX 的匿名且可问责用户管理与访问控制方案。在不修改已有的比特币协议的前提下, 实现了对公共无线局域网访问凭证的安全管理, 而无须依赖可信第三方; 采用基于 Intel SGX 的混合技术, 通过较小的开销提供了用户可控的访问凭证匿名性保护; 设计的区块链验证路径规则在保持用户隐私的同时实现了对恶意用户的问责。理论分析和实验结果验证了该方案的安全性和可行性。

关键词: WLAN 访问控制; 比特币区块链; Intel SGX; 匿名性; 可问责性; 认证

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020022

Privacy-preserving access control for public wireless LAN utilizing the bitcoin blockchain

NIU Yukun¹, WEI Lingbo¹, ZHANG Chi¹, ZHANG Xia², Gustavo Vejarano³

1. School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China

2. School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430047, China

3. Department of Electrical Engineering and Computer Science, Loyola Marymount University, Los Angeles 90045, USA

Abstract: In designing an access control scheme for public wireless LAN (WLAN), user privacy protection and user accountability are two conflict goals. A novel user management and access control scheme was proposed to solve this problem by utilizing the bitcoin blockchain and Intel SGX. It utilized unmodified bitcoin blockchain to manage the ownership of access credentials for users without relying on any trusted third party. It adopted Intel SGX-based mixing technology to enhance anonymity of users' access credentials. It designed verification path rule to resolve the

收稿日期: 2020-01-15; 修回日期: 2020-02-22

通信作者: 魏凌波, lingbowei@ustc.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61702474); 国家重点研发计划基金资助项目 (No.2018YFB0804201)

Foundation Items: The Natural Science Foundation of China (No. 61702474), The National Key R&D Program of China (No.2018YFB0804201)

论文引用格式: 牛玉坤, 魏凌波, 张弛, 等. 基于比特币区块链的公共无线局域网接入控制隐私保护研究[J]. 网络与信息安全学报, 2020, 6(2): 56-66.

NIU Y K, WEI L B, ZHANG C, et al. Privacy-preserving access control for public wireless LAN utilizing the bitcoin blockchain [J]. Chinese Journal of Network and Information Security, 2020, 6(2): 56-66.

conflicts between the privacy-preserving and accountability objectives. The effectiveness and feasibility of the proposed scheme are also demonstrated by security analysis and performance evaluation.

Key words: WLAN access control, bitcoin blockchain, Intel SGX, anonymity, accountability, authentication

1 引言

公共无线局域网被广泛部署在机场、火车站、公园等公共场所, 为用户提供无处不在的网络连接, 这允许用户将大部分智能手机的流量卸载到公共无线局域网中, 以缓解移动网络的流量拥堵问题。由于无线连接是开放且分布式的, 网络服务提供者通常通过用户认证方案来实现公共无线局域网的访问控制, 从而防止未授权用户和恶意攻击者访问公共无线局域网。在当前的认证方案中(如 WPA2), 不诚实的网络服务提供者可以通过追踪一个用户在何时何地连接哪一个公共无线局域网中的 Wi-Fi 热点来推测用户的移动模式以及其他敏感信息^[1], 从而威胁用户的隐私。

在这样的场景下, 匿名认证可以提供安全、隐私保护的认证和访问控制。匿名认证方案可以隐藏用户的真实身份, 使认证服务器无法将相同用户的多次访问关联在一起。然而, 绝对的匿名性会带来新的问题。因为所有匿名用户看起来都一样, 网络服务提供者无法让执行恶意行为的匿名用户得到惩罚。为了约束用户行为并保护公共无线局域网不被滥用和攻击, 一个匿名认证方案应当具备可问责性。也就是说, 匿名认证方案应当允许网络服务提供者阻止恶意行为用户继续访问公共无线局域网。

针对公共无线局域网的访问控制, 已有的匿名认证研究要么未考虑用户可问责性, 要么采用可信第三方来解决用户匿名性和用户可问责性之间的冲突。Pisa 等^[1]设计使用基于属性加密来执行访问控制, Wi-Fi 热点将当前 WPA2 密码加密并嵌入信标中周期性地广播, 其中, 只有拥有所需属性的用户才能解开密文获取 WPA2 密码。Cassola 等^[2]提出使用私有信息检索(PIR, private information retrieval)技术获取 Wi-Fi 热点访问密钥, 从而隐藏用户的真实身份。然而, 这些文献只实现了用户匿名性, 而未实现用户可问责性。Lou 等^[3]使用群签名在无线接入网络中同时实现匿名性和可问责性。该方案基于“分权思想”, 组

管理员和网络服务提供者分别只能获取用户的部分信息, 从而实现用户匿名性。当发现用户存在恶意行为时, 执法部门可以分别从二者处收集用户的部分信息, 从而获取完整的用户信息。然而, 它需要一个可信第三方执行密钥分发。此外, 用户无法察觉组管理员和网络服务提供者的共谋攻击。这意味着用户的匿名性无法得到保证。

在公共无线局域网访问控制中, 网络服务提供者不希望引入可信第三方来实现认证。一方面, 可信第三方面临单点失败问题。一旦可信第三方无法工作, 整个认证系统将无法运行。另一方面, 一旦攻击者攻破可信第三方, 其带来的隐私泄露风险更加严重。

基于黑名单的匿名凭证^[4](BLAC, black listable anonymous credential)系统可以用来保护公共无线局域网中用户的匿名性且实现可问责认证, 同时不需要依赖可信第三方。在 BLAC 中, 用户使用零知识证明来证明其拥有一个有效凭证同时该凭证不在黑名单中。然而, 零知识证明是一个高计算开销的操作, 而且 BLAC 的计算开销随着黑名单的大小而线性增加。Tsang 等^[5]使用撤销窗口概念来优化 BLAC 的性能, 使零知识证明的开销不再随着黑名单大小而变化, 而是与撤销窗口的大小线性相关。通常, 撤销窗口是一个常数。尽管如此, 用户执行一次认证操作大约需要 0.7 s^[5]。更重要的是, 所有基于零知识证明的匿名凭证系统无法检测多个用户共享账号这一恶意行为。

比特币区块链是一个维护全局交易的分布式账本, 它允许参与者在完全互不信任的环境下完成资产所有权的转移并达成一致。自 2009 年比特币系统上线以来, 十多年的运行结果证明它是目前运行时间最长、安全性最高的区块链系统。其次, 比特币区块链天然地提供了一定的匿名性, 而混币技术的使用更进一步加强了用户使用比特币系统时的匿名性。因此, 比特币区块链可以用于管理用户访问公共无线局域网时的凭证, 而不需要引入可信第三方。

Niu 等^[6]提出使用比特币区块链来管理用户访问凭证, 基于染色币的思想将访问凭证与用户的比特币地址绑定, 然后利用比特币区块链中的混币技术 CoinShuffle^[7]实现凭证的匿名更换。当发现用户执行恶意行为时, 网络服务提供者只需将用户使用的凭证加入黑名单。根据验证路径规则, 其他用户将自发地拒绝加入黑名单的凭证执行匿名更换。其所有凭证相关操作都通过比特币交易来实现, 只有交易写入比特币区块链, 操作才算完成。然而, 比特币区块链具备有限的交易吞吐量, 其平均每 10 min 才生产一个区块, 每个区块只能存放大约 2 MB 的交易数据。因此, 访问凭证匿名更换产生的比特币交易至少需要 10 min 才能写入比特币区块链。而且为了尽快写入比特币区块链, 用户需要支付更多的交易费用给比特币“矿工”。

针对上述问题, 本文提出了一种基于比特币区块链和 Intel SGX 的匿名且可问责的用户管理与访问控制方案, 本文的主要贡献如下。

1) 提出一种适用于公共无线局域网的匿名可问责访问控制方案, 同时无须依赖任何可信第三方。使用完全未修改的比特币区块链进行管理访问凭证的所有权, 并利用基于 Intel SGX 的混合服务器实现访问凭证的匿名更换。利用验证路径规则, 可以在访问凭证匿名更换的同时兼顾可问责性。

2) 提出一种链下混合机制。实现访问凭证匿名更换的比特币交易不需要写入区块链, 避免低的比特币区块链吞吐量对访问凭证匿名更换带来的高延时、高金融成本的问题。

3) 安全分析与实验结果表明, 提出的方案具备用户匿名性以及用户可问责性, 同时认证过程具备良好的执行效率。

2 模型假设与设计目标

2.1 系统模型

一个经典的公共无线局域网接入场景通常包含用户、网络服务提供者, 以及一些 Wi-Fi 热点。网络服务提供者控制一些 Wi-Fi 热点并将其部署在公共区域, 如公园、机场、车站等。用户向网络服务提供者订阅网络访问服务。当一个用户连

接到任何网络服务提供者控制的 Wi-Fi 热点后, 用户与 Wi-Fi 热点执行双向认证。本文在此模型基础上, 引入比特币区块链和基于 Intel SGX 的混合服务器来实现访问凭证的管理和匿名更换。用户从网络服务提供者处获取访问凭证的授权信息, 然后使用比特币交易中的 OP_RETURN 交易输出将授权信息嵌入比特币区块链, 同时将访问凭证与用户拥有的比特币地址进行绑定。这样, 用户可以通过比特币区块链进行访问凭证的创建以及所有权的管理。为了增加访问凭证的匿名性, 一些用户通过基于 Intel SGX 的混合服务器来实现访问凭证的匿名更换。运行在 Intel SGX 混合服务器中的安全飞地 (secure enclave) 收集用户的凭证混合请求, 然后创建访问凭证混合交易将访问权限转移到新的访问凭证中。Intel SGX 技术保证安全飞地内访问凭证混合日志的机密性, 从而确保访问凭证更换时的匿名性。

2.2 攻击模型和假设

本文关注两类攻击目标: 滥用和隐私。一方面, 一些用户企图使用有效证书进行恶意行为; 另一方面, 给定一个匿名访问凭证, 网络服务提供者或者基于 Intel SGX 的混合服务器试图将该访问凭证与用户真实身份或者相同用户拥有的其他匿名访问凭证关联起来。

针对上述攻击模型, 本文假设用户在通信过程中不会泄露其身份信息, 如 MAC 地址和 IP 地址。实际中, 用户连接到公共无线局域网后可以使用随机 MAC 地址技术^[8]来隐匿其 MAC 地址, 当与安全飞地通信时可以使用 Tor^[9]来隐匿其 IP 地址。

本文假设网络服务提供者是诚实且好奇的。也就是说, 网络服务提供者会诚实运行协议, 但会根据比特币区块链以及其本地存储的凭证混合交易尝试链接匿名访问凭证到用户的身份或者相同用户拥有的其他匿名访问凭证。

基于 Intel SGX 的混合服务器, 在为用户提供访问凭证混合的同时, 试图解匿名混合后的用户凭证。混合服务器控制着操作系统和管理程序, 它可以丢弃或延迟安全飞地进出的通信数据。注意到安全飞地会受到侧信道攻击的威胁, 如时间攻击、缓存碰撞攻击、访问模式攻击、电力分析

2.3 设计目标

1) 安全性。用户和公共无线局域网中的 Wi-Fi 热点之间能执行双向认证。一方面, Wi-Fi 热点认证用户可以防止未授权用户通过 Wi-Fi 热点访问互联网;另一方面, 用户认证 Wi-Fi 热点可以禁止非法热点执行钓鱼攻击。

3) 可问责性。网络服务提供者要能撤销恶意行为用户持有的有效访问凭证, 阻止恶意行为用户继续访问公共无线局域网。

4) 不需要可信第三方。方案中对所有实体的信任都应当受限,以确保用户的匿名性得到保证。即使多方共谋也不能完全解匿名用户的所有访问凭证。

5) 高效性。对于用户和网络服务提供者来说, 认证过程应当具备低的通信、计算开销。

3 方案设计

3.1 方案概览

本文方案利用比特币区块链和基于 Intel SGX 的混合协议实现公共无线局域网中匿名且可问责的用户管理与访问控制方案。系统模型及方案概览如图 1 所示。

由于网络服务提供者通过一系列 Wi-Fi 热点为用户提供网络访问服务，所以它在系统建立之初为每个 Wi-Fi 热点颁发一个凭证，该凭证将在双向认证协议中证明 Wi-Fi 热点的身份。本文不需要保护 Wi-Fi 热点的匿名性。

为了访问 Wi-Fi 热点，用户首先在系统中完成注册以获得一个访问凭证。初始的访问凭证不是匿名的。为了获得匿名凭证，一些用户协同基于 Intel SGX 的混合服务器执行一个访问凭证混合协议，获得一个新的匿名访问凭证。

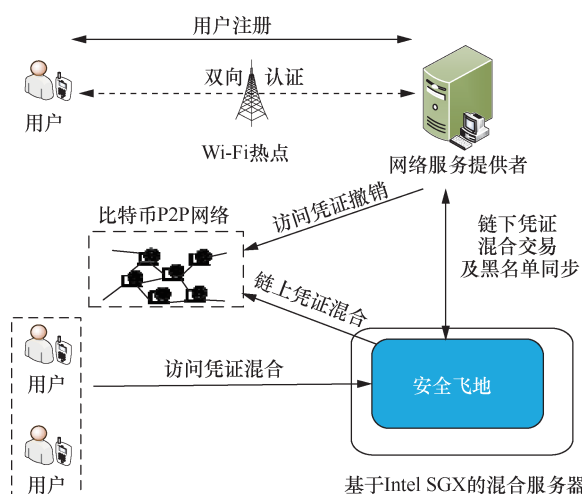


Figure 1 System model and overview of the scheme

当用户访问一个 Wi-Fi 热点，用户和 Wi-Fi 热点之间运行一个双向认证协议，各自分别验证对方的凭证。一旦双向认证成功，Wi-Fi 热点向用户提供网络访问服务。之后，用户参与访问凭证混合协议获得新的匿名凭证，用于下一次认证。

所有访问凭证的操作都通过创建或读取比特币交易来实现。考虑到比特币区块链低的交易吞吐量，访问凭证混合协议生成的凭证混合交易不写入比特币区块链。为了抵御网络服务提供商者、基于 Intel SGX 的混合服务器，以及一些用户的共谋攻击，用户执行一定次数的访问凭证混合后，安全飞地将生成一个链上凭证混合交易，该交易将写入比特币区块链。这样，链上凭证混合交易之前的所有链下凭证混合交易都不必存储。

在本文方案中，访问凭证是一个 ECDSA 公钥的哈希。凭证的拥有者可以使用对应私钥进行数字签名以证明其所有权。通常，凭证包含在 P2PKH (pay-to-public-key-hash) 交易输出的上锁脚本中。

本文方案中所有创建的交易都包含一个 OP_RETURN 交易输出，它也被称作标记输出。标记输出可将本文方案产生的交易与比特币区块链中其他交易区分开来，同时能用于标记交易类型。而且，本文可以通过在标记输出中嵌入数据来实现用户注册、黑名单更新等。标记

输出的格式为 $OP_RETURN<数据>$ ，自 Bitcoin Core 0.12.0 版本之后，用户可以在一个 OP_RETURN 交易输出中嵌入最多 83 B 的任意数据，故“数据”域至多 83 B。本方案中<数据>结构定义如下：<系统标识符><版本号><交易类型><载荷>。在不同的交易中，“载荷”域有所不同。

3.2 系统建立

本文假设每个用户和每个 Wi-Fi 热点都知晓网络服务提供者的公钥 pk_{sp} 。在系统建立阶段，网络服务提供者对每个 Wi-Fi 热点颁发凭证。Wi-Fi 热点各自生成它们的 ECDSA 公钥以及对应的私钥。然后，网络服务提供者收集所有 Wi-Fi 热点的公钥并创建一些热点列表交易，热点列表交易都使用 P2PKH 交易输出，每个 P2PKH 交易输出嵌入一个 Wi-Fi 热点公钥的哈希，该哈希结果即 Wi-Fi 热点的凭证。热点列表交易只有写入比特币区块链才生效。

类似地，网络服务提供者需要创建一些安全飞地列表交易，只有经过授权的安全飞地才能帮助用户执行访问凭证混合。为此，网络服务提供者与安全飞地之间执行 Intel SGX 提供的远程认证协议，以确保安全飞地被正确地初始化。在远程认证结束之后，网络服务提供者与安全飞地之间建立了一条安全信道。随后安全飞地通过该安全信道发送自己的凭证给网络服务提供者，只有该凭证对应私钥签名的凭证混合交易才被网络服务提供者认可。需要注意的是，安全飞地的代码将被公开以确保其不包含任何威胁用户隐私的后门程序。

3.3 用户注册

如图 2 所示，用户注册分为如下 4 个步骤。

1) 用户请求注册。用户 U 向网络服务提供者提交访问凭证注册请求。请求包含用户的真实身份信息 $Info_{id}$ ，以及其所拥有的一个输出指针 OP_U 。

2) 网络服务提供者处理请求。网络服务提供者检查 $Info_{id}$ 是否已经被用来注册。如果没有，网络服务提供者生成授权信息 $Sig_{sk_{sp}}(H(OP_U))$ 并发送给用户；否则，告诉用户该身份信息已经被用来注册。

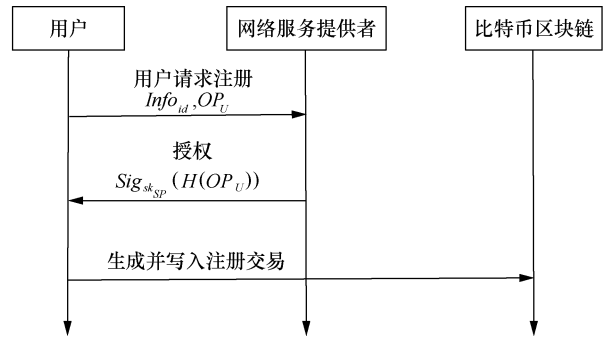


图2 用户注册流程
Figure 2 User registration

3) 用户创建注册交易。用户创建一个注册交易，该交易的输入花费输出指针 OP_U 中的未花费交易输出 (UTXO, unspent transaction output)。注册交易包含两个交易输出：一个交易输出为 P2PKH 交易输出，其上锁脚本中的 PKH 为用户的访问凭证 C_U ；另一个交易输出为标记输出，在载荷中填入授权信息 $Sig_{sk_{sp}}(H(OP_U))$ 。

4) 广播注册交易至比特币区块链网络。一旦注册交易被写入比特币区块链，用户的访问凭证 C_U 生效。

网络服务提供者通过对用户拥有的某个输出指针进行数字签名以完成授权操作，该交易输出也被称作授权交易输出。由于比特币区块链的不可“双花”特性，一个授权交易输出只能创建一个有效的注册交易。

3.4 访问凭证混合

用户可以通过执行访问凭证混合协议获得一个新的匿名访问凭证。访问凭证混合协议基于 Intel SGX 来实现，具体过程如下。

1) 用户认证安全飞地。用户和安全飞地执行 Intel SGX 提供的远程认证协议，以确保安全飞地被正确地初始化。之后，用户与安全飞地之间建立一条安全信道。此外，用户还需要验证安全飞地所拥有的凭证 C_{SE} 是否有效，凭证验证操作将在第 3.5 节详细介绍。

2) 链下混合开启。用户创建链下混合开启交易，交易的输入是用户凭证所在的未花费交易输出，输出则是一个 P2SH (pay-to-script-hash) 交易输出。该交易输出包含一个链下混合关闭脚本的哈希。链下混合关闭脚本如图 3 所示。它表示在 time-lock 定义的时间之前，只有安全飞地可以

花费该 P2SH 交易输出，而在 time-lock 定义的时间之后，用户可以花费该 P2SH 交易输出。这是为了在安全飞地永远失去的情况下，用户仍能取回自己的访问凭证。链下混合开启交易写入区块链后才能开启链下混合。

```
OP_IF
<pubkey_enclave> OP_CHECKSIG
OP_ELSE
<time-lock> OP_CHECKLOCKTIMEVERIFY OP_DROP
<pubkey_user> OP_CHECKSIG
OP_ENDIF
```

图3 链下混合关闭脚本

Figure 3 Close script of the off-chain mixing

3) 访问凭证混合请求。用户 U 发送访问凭证混合请求给安全飞地，安全飞地生成挑战 r 。随后用户发送信息 $\{C_u, \text{Sig}_{sk_U}(H(r)), C_{U_new}\}$ 给安全飞地，其中 C_{U_new} 为用户混合后所用的新凭证。

4) 访问凭证混合。安全飞地执行访问凭证混合算法，如算法1所示。安全飞地验证每个用户的访问凭证，一旦收集到 k 个有效的访问凭证混合请求后，安全飞地开始混合，并生成一个链下凭证混合交易，然后将链下凭证混合交易发送给对应的用户以及网络服务提供者。

算法1 访问凭证混合算法

输入 用户访问凭证混合请求、 k 、时间戳 $Time$

输出 链下凭证混合交易

$i=0; j=0;$

while(1){

wait(request);

$r_i = \text{random}();$ //生成挑战

send(r_i);

if(verify($r_i, C_u, \text{Sig}_{sk_U}(H(r_i))$))=1) //验证

用户访问凭证有效性，以及用户对凭证的所有权

$j=j+1;$

$C_{old} \leftarrow C_u;$

$C_{new} \leftarrow C_{U_new};$

end if

if($j \geq k$) break; // k 个有效请求后开始

混合

}

$C_{new} \leftarrow \text{Shuffle}(C_{new});$ //混淆新访问凭证集

合中的顺序

$TX \leftarrow \text{tx_generate}(C_{old}, C_{new}, \text{Time})$ //生成链下混合交易

安全飞地在验证用户凭证的有效性时，会判断该用户链下混合执行次数是否超过 L 。如果超过，则通知该用户需要执行链上凭证混合。这是为了应对可能存在的网络服务提供者、基于 Intel SGX 的混合服务器，以及一些用户的共谋攻击。由于每次链上凭证混合都耗费一定的交易费，共谋攻击需要花费一定的金融成本才能执行。此外，如果一个安全飞地所服务的某些用户链上混合频率过高，诚实用户可以发现该类共谋攻击。安全飞地具有完整的混合日志，所以给定一个有效凭证，安全飞地知晓其对应哪个用户。

安全飞地在创建链下凭证混合交易时需要嵌入一个时间戳。本文方案采用安全飞地本地最新的区块头哈希以及序列号作为时间戳，其中，序列号表明该链下凭证混合交易是第几个链下凭证混合交易，当本地最新的区块头哈希发生变化时，序列号从0重新计数。

3.5 凭证验证

当用户连接到 Wi-Fi 热点或者通过安全飞地执行访问凭证混合协议，需要证明其拥有一个有效的访问凭证。证明者可以使用数字签名来证明其拥有某个访问凭证，为了证明该访问凭证是有效的，需要构建一个基于授权交易输出的证明。

验证路径规则就是用于构建这样的证明。在比特币区块链中，交易输入包含一个指向之前交易输出的索引。因此，一个交易输入可以被链接到之前交易的某个交易输出。在定义相同交易中，交易输入和交易输出之间的映射关系后，访问凭证所在的交易输出与某个授权信息之间构成一条路径。为实现这种思想，本文方案定义某个交易内第 i 个交易输入链接到第 i 个交易输出，验证路径如图4所示。

给定一个访问凭证和一个授权交易输出，一个验证者可以检查它们之间是否存在一条验证路径。

网络服务提供者和安全飞地都可以通过同步比特币区块链、链下凭证混合交易以及黑名单来

维护一个当前有效访问凭证集合。该有效访问凭证集合至少包含授权交易输出、根据验证路径对应的最新凭证、最新凭证所在交易的 txid, 以及最新凭证是否有有效的标识位。

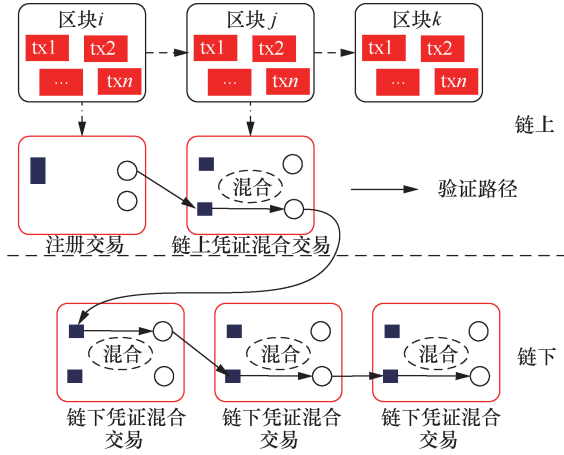


图4 验证路径
Figure 4 Verification path

安全飞地以及网络服务提供者通过访问凭证验证算法来验证一个访问凭证是否有效, 具体如算法2所示。

算法2 访问凭证有效性验证算法

输入 用户凭证 C_U , 验证路径 $\{tx1, tx2, \dots, txn\}$, 有效访问凭证集合 VAC

输出 是否有效

if($C_U \in VAC$) //检查用户凭证是否在有效访问凭证集合中

return true;

else

tx.time $\leftarrow$ find(tx1, VAC) //找到有效访问凭证集合中该验证路径起点对应的有效访问凭证, 找到其所在交易的时间戳

if(tx.time $\geq$ txn.time) //如果用户访问凭证所在的交易时间戳小于 VAC 中记录的时间戳, 访问凭证无效

return false;

else

TX $\leftarrow$ find($\{tx1, tx2, \dots, txn\}$); //说明链下混合交易未同步, 找到所有未同步的交易

end if

if(tx_verify(TX)=1)

update(VAC); //如果所有未同步交易都

有效, 根据这些交易更新有效访问凭证集合

return true;

else return false;

end if

通常用户只需提供访问凭证进行访问凭证的有效性验证。只有当用户提供的访问凭证不在有效访问凭证集合中时, 才需要提供完整的验证路径用于执行后续验证操作。

当用户连接到 Wi-Fi 热点时, Wi-Fi 热点需要向用户证明其拥有一个有效凭证。不同于用户访问凭证的证明, Wi-Fi 热点只需将凭证所在热点列表交易的 txid 发送给用户。用户可以根据热点凭证所在交易输出是否是 UTXO, 热点列表交易是否是网络服务提供者所创建, 来判断热点凭证是否有效。所以, Wi-Fi 热点只需向用户提供其凭证、凭证所在的热点列表交易, 以及凭证对应私钥的数字签名即可。

3.6 双向认证协议

当用户连接到 Wi-Fi 热点, 需要执行一个双向认证协议。由于用户和 Wi-Fi 热点都具有凭证以及对应的公私钥对, 本文方案使用挑战-应答握手技术构建双向认证协议。双向认证协议如下。

1) Wi-Fi 热点将消息 $M_1 = \{txid_{HP}, C_{HP}, pk_{HP}, Sig_{sk_{sp}}(H(CP_{HP} || C_{HP} || pk_{HP}))\}$ 插入信标, 然后周期性地广播信标, 其中, $txid_{HP}$ 为凭证所在的热点列表交易的哈希, C_{HP} 为热点的凭证, pk_{HP} 为热点凭证对应的公钥 $H(\cdot)$, 为哈希函数。

2) 用户捕获信标并从中提取出 M_1 , 然后用户如第3.5节所述验证热点凭证的有效性。

3) 如果凭证有效, 用户发送 $M_2 = \{C_U, pk_U, Enc_k(r_1), Sig_{sk_U}(H(C_U || pk_U || Enc_k(r_1 || k)))\}$ 给热点, 其中 C_U 为用户的访问凭证, pk_U 为用户访问凭证对应的公钥, k 为会话密钥, 它使用热点公钥、用户访问凭证对应私钥作为输入, 通过 ECIES 算法中的会话密钥计算方法计算而得, r_1 为随机数, $Enc(\cdot)$ 为加密算法。

4) Wi-Fi 热点将用户凭证 C_U 发送给网络服务提供者, 由网络服务提供者验证该凭证是否属于有效访问凭证集合。如果不是, 则 Wi-Fi 热点请求用户提供完整的凭证有效性证明, 如第3.5节

所述。如果用户的完整凭证的有效性证明仍未通过验证，则认证失败，结束认证；否则执行下一步。

5) Wi-Fi 热点使用用户公钥、热点凭证对应私钥作为输入，利用 ECIES 中会话密钥计算方法完成会话密钥的计算，随后 Wi-Fi 热点解密 $Enc_k(r_1 \| k)$ 获得解密结果，记为 r_2 以及 k' 。如果 k' 等于 k ，则说明用户拥有其发送的访问凭证。

6) Wi-Fi 热点发送密文 $Enc_k(r_2 \| k \| r_3)$ 给用户。随机数 r_3 是为了防止 Wi-Fi 热点直接将用户发送过来的密文返回给用户，从而规避用户对 Wi-Fi 热点的认证。

7) 用户解密 $Enc_k(r_2 \| k \| r_3)$ ，然后验证 $r_2 = r_1$ 是否成立。如果成立，则用户可以使用会话密钥 k 与 Wi-Fi 热点进行通信；否则，认证失败，Wi-Fi 热点为非法热点。

3.7 凭证撤销

当网络服务提供者发现用户执行恶意行为，它将用户所使用的访问凭证加入黑名单，然后生成黑名单更新交易。黑名单将采用 Merkle 树的形式组织，每个 Merkle 树的叶子节点为一个加入黑名单的凭证以及其所在混合交易的 txid，其对应的 Merkle 根将被嵌入黑名单更新交易中，如图 5 所示。黑名单更新交易需要写入比特币区块链才能生效。

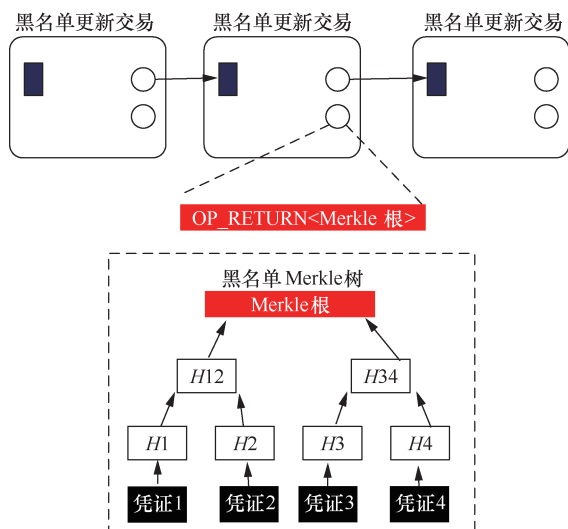


图5 黑名单更新交易

Figure 5 Blacklist update transaction

当安全飞地发现新的黑名单更新交易，它将与网络服务提供者执行同步黑名单操作，然后计算新的 Merkle 根，验证计算获得的 Merkle 根与黑名单交易中的 Merkle 根是否相同。如果相同，则黑名单未被篡改。

安全飞地同步黑名单之后，会根据新增加的黑名单更新有效访问凭证集合。如果黑名单的凭证在当前有效访问凭证集合，则将该凭证标识为无效。如果不在，则说明持有该凭证的用户参与了新的访问凭证混合协议。安全飞地可以根据黑名单中该访问凭证所在的 txid 查找交易链，由于安全飞地具有所有链下混合日志，所以它知晓具体哪个用户执行了恶意行为，然后查找有效访问凭证集合，将该用户的当前有效访问凭证标识为无效。随后，安全飞地将黑名单执行结果同步给网络服务提供者。

3.8 检查点更新

当用户的访问凭证不在有效访问凭证集合时，用户需要出示完整的验证路径证明其访问凭证的有效性。用户的通信开销将随着验证路径长度呈线性增长，为防止用户的通信开销无限增加，本文方案限制验证路径长度最大为 L ，即第 3.4 节用户能执行链下凭证混合的最大次数。

链下混合开启交易的 P2SH 交易输出将作为检查点，用户只需出示到达检查点这部分的验证路径。检查点更新操作可通过第 3.4 节的链下凭证混合重启操作来实现。这意味着有效的检查点必须为一个 UTXO。

4 安全性分析

本节对所提方案的特性进行分析，验证其是否满足第 2.3 节定义的安全需求，具体分析如下。

1) 安全性。用户和 Wi-Fi 热点之间可以执行双向认证协议。本文方案中，用户首先认证 Wi-Fi 热点凭证的有效性，但还无法确认该凭证是否由该 Wi-Fi 热点所拥有。随后用户采用 ECIES 的会话密钥协商算法使用该凭证的公钥计算会话密钥，并用该会话密钥加密一个随机数以及该会话密钥。用户再把自己的访问凭证发送给 Wi-Fi 热点。Wi-Fi 热点通过网络服务提供者验证用户凭证的有效性。然后根据 ECIES 的会话密钥协商算

法计算出会话密钥,再解密用户发送过来的密文。注意到,密文中同样包含用户计算的会话密钥,Wi-Fi 热点可以根据两个会话密钥是否一致判断用户是否拥有其发送过来的访问凭证。之后,Wi-Fi 热点需要将自己解密的结果发送给用户以证明其拥有对应的热点凭证。只有当用户和 Wi-Fi 热点都有其声称的凭证时,双向认证协议才能成功执行。

2) 匿名性与不可链接性。访问凭证交换都在安全飞地内执行,只有安全飞地知晓用户的新旧访问凭证对应关系。只要参与访问凭证交换的用户中至少存在两个诚实用户,攻击者就无法链接诚实用户的新旧凭证。

3) 可问责性。首先,根据验证路径规则,在访问凭证混合过程中,混合前后有效访问凭证数目相同。当发现用户执行恶意行为时,其当前所用访问凭证将被加入黑名单。而加入黑名单的访问凭证无法再参与访问凭证混合。即使该访问凭证被加入黑名单之前已经执行访问凭证混合,安全飞地可以根据完整的访问凭证混合日志将该用户所拥有的当前有效凭证撤销。而黑名单执行结果将同步给网络服务提供者,所以执行恶意行为的用户将不再能够通过 Wi-Fi 热点的认证。

4) 不需要可信第三方。本文方案对所有实体的信任都是有限的。针对可能存在的共谋攻击,3.4 节已经给出详细的抵抗方式。所以,即使网络服务提供者、基于 Intel SGX 的混合服务器以及一些用户共谋,也不能够完全解匿名用户而不被用户发现。

5 性能评估

本文使用 Crypto++^[23]提供的密码函数库进行实现,从而验证本方案中双向认证期间用户和网络服务提供者的通信和计算开销。实验采用的密码学算法以及相应的参数如表 1 所示。实验运行在 Dell OptiPlex 7050 上,使用 Intel i7-7700 CPU, CPU 频率为 3.60 GHz, 8 GB 内存。相同的参数下,本文执行 1 000 次双向认证协议,取其平均值。

当网络服务提供者与安全飞地完全同步链下凭证混合交易时,网络服务提供者只需查询有效访问凭证集合即可完成凭证有效性验证。当二者

未达成同步时,用户需要提供完整的验证路径以证明其访问凭证的有效性。此时,未同步交易的数量以及链下凭证混合交易的参与者数目 k 都会影响双向认证完成时间。本文方案首先验证未同步交易数目对双向认证完成时间的影响。实验结果如图 6 所示。

表 1 执行参数
Table 1 Implementation parameters

参数	值
签名算法	ECDSA
加密算法	ECIES + AES-256 CBC 模式
椭圆曲线	secp256k1
哈希算法	SHA-256
无线通信带宽	10 Mbit/s

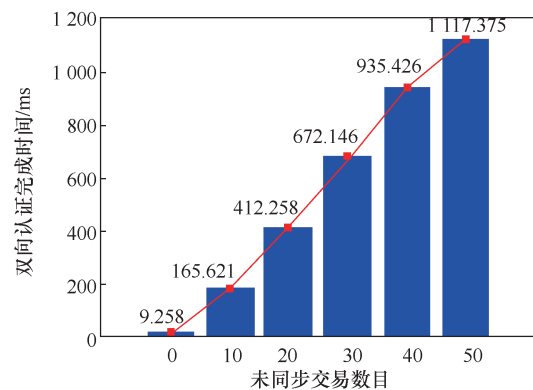


图 6 未同步交易数目对双向认证效率的影响
Figure 6 Impact of the number of the unsynchronized off-chain mixing transaction on mutual authentication efficiency

其中,固定参数 $k=10$,即安全飞地收集到 10 个有效访问凭证混合请求时才执行链下凭证混合。横轴代表未同步交易数目,纵轴代表用户和 Wi-Fi 热点完成双向认证协议所需时间。未同步交易数目为 0 时,表示网络服务提供者与安全飞地完成同步,直接查询有效访问凭证集合即可判断用户凭证的有效性。此时大约需要 9.258 ms 完成双向认证。与预期结果相同,总的双向认证完成时间与未同步交易数目呈线性增长。可以看到,未同步交易数目达到 30 时,完成双向认证所需时间大约需要 672 ms,仍低于 PEREA^[5]中的最好结果 0.7 s。

接着,本文假设平均未同步交易数目为 5,验证双向认证完成所需时间与执行链下凭证混合

所需的有效用户数目 k 之间的关系。实验结果如图 7 所示。

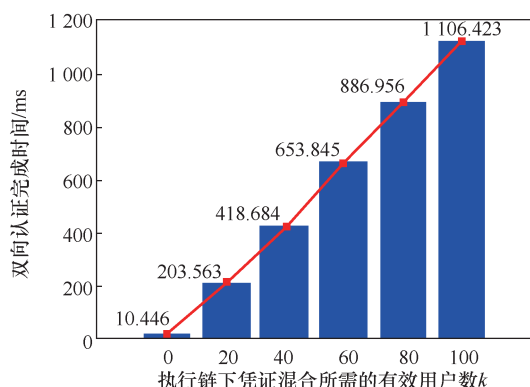


图7 执行链下凭证混合所需的有效用户数 k 对双向认证效率的影响
Figure 7 Impact of the number of users per off-chain mixing transaction on mutual authentication efficiency

横轴代表执行链下凭证混合所需的有效用户数 k , 纵轴代表用户和 Wi-Fi 热点完成双向认证协议所需时间。与预期结果相同, 总的双向认证完成时间与参数 k 呈线性增长。可以看到, 当平均未同步交易数目为 5 时, 安全飞地可以等到 60 个有效的访问凭证混合请求再执行链下凭证混合, 此时双向认证所需的平均时间大约为 653 ms, 仍低于 PEREA^[5]中的最好结果 0.7 s。

6 结束语

本文提出了一种基于比特币区块链和 Intel SGX 的匿名且可问责的用户管理与访问控制方案。该方案在不修改已有比特币区块链协议的前提下, 实现了对公共无线局域网访问凭证的安全管理, 而无需依赖可信第三方。比特币区块链只能对访问凭证提供弱的匿名性, 为此该方案采用基于 Intel SGX 的混合技术, 既增强了用户访问凭证的匿名性, 又降低了用户与网络服务提供者的通信和计算开销。该方案设计的区块链验证路径规则在保护用户隐私的同时实现了对恶意用户的问责。安全分析和实验结果验证了该方案的安全性和可行性。

参考文献:

[1] PISA C, CAPONI A, DARGAHI T, et al. WI-FAB: attribute-based WLAN access control, without pre-shared keys and backend infra-structures[C]//Proceedings of the 8th ACM International Work-

shop on Hot Topics in Planet-Scale Mobile Computing and Online Social Networking. 2016: 31-36.

- [2] CASSOLA A, BLASS E O, NOUBIR G. Authenticating privately over public Wi-Fi hotspots[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 1346-1357.
- [3] LOU W, REN K. Security, privacy, and accountability in wireless access networks [J]. IEEE Wireless Communications, 2009, 16(4): 80-87.
- [4] TSANG P P, AU M H, KAPADIA A, et al. Blacklistable anonymous credentials: blocking misbehaving users without TTPS[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. 2007: 72-81.
- [5] TSANG P P, AU M H, KAPADIA A, et al. PEREA: Towards practical TTP-free revocation in anonymous authentication[C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. 2008: 333-344.
- [6] NIU Y, WEI L, ZHANG C, et al. An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the bitcoin blockchain[C]//2017 IEEE/CIC International Conference on Communications in China (ICCC). 2017: 1-6.
- [7] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for bitcoin[C]//European Symposium on Research in Computer Security. 2014: 345-364.
- [8] MARTIN J, MAYBERRY T, DONAHUE C, et al. A study of MAC address randomization in mobile devices and when it fails[J]. Proceedings on Privacy Enhancing Technologies, 2017, 2017(4): 365-383.
- [9] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[R]. Naval Research Lab Washington DC, 2004.
- [10] BRASSER F, MÜLLER U, DMITRIENKO A, et al. Software grand exposure:SGX cache attacks are practical[C]//11th USENIX Workshop on Offensive Technologies (WOOT 17). 2017.
- [11] HÄHNEL M, CUI W, PEINADO M. High-resolution side channels for untrusted operating systems[C]//2017 USENIX Annual Technical Conference (USENIX ATC 17). 2017: 299-312.
- [12] GÖTZFRIED J, ECKERT M, SCHINZEL S, et al. Cache attacks on Intel SGX[C]//Proceedings of the 10th European Workshop on Systems Security. 2017: 2.
- [13] MOGHIMI A, IRAZOQUI G, EISENBARTH T. Cachezoom: how SGX amplifies the power of cache attacks[C]//International Conference on Cryptographic Hardware and Embedded Systems. 2017: 69-90.
- [14] SCHWARZ M, WEISER S, GRUSS D, et al. Malware guard extension: using SGX to conceal cache attacks[C]//International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2017: 3-24.
- [15] WANG W, CHEN G, PAN X, et al. Leaky cauldron on the dark land: understanding memory side-channel hazards in SGX[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Commu-

nications Security. 2017: 2421-2434.

- [16] STRACKX R, PIESSENS F. Ariadne: a minimal approach to state continuity[C]//25th USENIX Security Symposium (USENIX Security 16). 2016: 875-892.
- [17] CHEN S, ZHANG X, REITER M K, et al. Detecting privileged side-channel attacks in shielded execution with Déjà Vu[C]// Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017: 7-18.
- [18] COSTAN V, LEBEDEV I, DEVADAS S. Sanctum: minimal hardware extensions for strong software isolation[C]//25th USENIX Security Symposium (USENIX Security 16). 2016: 857-874.
- [19] GRUSS D, LETTNER J, SCHUSTER F, et al. Strong and efficient cache side-channel protection using hardware transactional memory[C]//26th USENIX Security Symposium (USENIX Security 17). 2017: 217-233.
- [20] SHIH M W, LEE S, KIM T, et al. T-SGX: eradicating controlled-channel attacks against enclave programs[C]//NDSS. 2017.
- [21] SHINDE S, CHUA Z L, NARAYANAN V, et al. Preventing page faults from telling your secrets[C]//Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. 2016: 317-328.
- [22] MISHRA P, PODDAR R, CHEN J, et al. Oblix: an efficient oblivious search index[C]//2018 IEEE Symposium on Security and Privacy (S&P). IEEE, 2018: 279-296.
- [23] Crypto++ [EB].

[作者简介]



牛玉坤 (1989-), 男, 河南周口人, 中国科学技术大学博士生, 主要研究方向为应用密码学和区块链技术。



魏凌波 (1979-), 女, 陕西周至人, 博士, 中国科学技术大学副研究员, 主要研究方向为应用密码学和区块链技术。



张驰 (1977-), 男, 广西百色人, 博士, 中国科学技术大学副教授, 主要研究方向为无线网络、网络安全和区块链技术。



张霞 (1979-), 女, 湖北武汉人, 博士, 武汉理工大学讲师, 主要研究方向为无线网络和区块链技术。



Gustavo Vejarano (1982-), 男, 哥伦比亚人, 博士, 洛约拉马利蒙特大学副教授, 主要研究方向为无线网络和安全技术。