

## Fabric 中的匿名身份认证技术研究

叶岳洋, 张兴兰

北京工业大学信息学部, 北京 100124

**摘要:** 解决联盟链上用户的隐私问题成为加速区块链实际应用落地的关键。基于联盟链的典型代表 Hyperledger Fabric 平台设计了一套基于公钥基础设施的匿名身份认证方案。通过将私钥  $d$  分解为两部分, 由不同的角色使用各自私钥对匿名证书生成联合签名的方式实现证书生成过程中的权限分离, 并解决匿名证书追踪过程中的单点攻击问题。分析表明, 改进后的方案能够以更低的计算和存储开销, 实现比原有方案更高的安全性。

**关键词:** 联盟链; 超级账本; 公钥基础设施; 匿名身份认证; 非对称加密

**中图分类号:** TP309

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2021036

## Research on anonymous identity authentication technology in Fabric

YE Yueyang, ZHANG Xinglan

Faculty of Information Technology, Beijing University of Technology, Beijing 100124

**Abstract:** Solving the privacy problem of users in the consortium blockchain becomes the key to accelerate the implementation of the practical application of blockchain. A set of anonymous identity authentication scheme based on PKI is designed based on Hyperledger Fabric platform, a typical representative of the consortium blockchain. By splitting the private key  $d$  into two parts, different roles use each private key to generate the joint signature of the anonymous certificate to achieve the separation of permissions in the process of certificate generation and solve the single point attack problem in the process of anonymous certificate tracking. The analysis shows that the improved scheme can achieve higher security than the original scheme with lower computing and storage overhead.

**Keywords:** consortium blockchain, Hyperledger Fabric, PKI, anonymous identity authentication, asymmetric encryption

收稿日期: 2020-11-26; 修回日期: 2021-01-07

通信作者: 叶岳洋, 739541460@qq.com

基金项目: 国家自然科学基金 (61801008)

**Foundation Item:** The National Natural Science Foundation of China(61801008)

论文引用格式: 叶岳洋, 张兴兰. Fabric 中的匿名身份认证技术研究[J]. 网络与信息安全学报, 2021, 7(3): 134-140.

YE Y Y, ZHANG X L. Research on anonymous identity authentication technology in Fabric[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 134-140.

## 1 引言

区块链作为一种新兴存储技术,以其去中心化和不可篡改等特性而受到很多行业的广泛应用<sup>[1]</sup>。但作为一种公共账本,其存储在链上的数据能够直接被任何在该系统网络下的其他节点所查看,因此带来了严重的隐私泄露问题。例如,攻击者可以对区块链上的公开数据进行分析,由于链上数据保存了大量的交易样本,通过对输入输出地址建立映射关系并结合交易内容不难推断出交易账户背后对应的实体身份;还可以追踪交易数据在 P2P 组网的传播路径,分析交易账户对应的 IP 地址,从而确定账户对应的实体身份<sup>[2-4]</sup>。

相较于公有链,联盟链的特点在于它是由多个机构共同参与管理的区块链,网络节点的加入需要经过组织机构的准许,每个组织机构管理一个或多个节点,链上的数据只允许系统内部节点进行读写和发送。这种轻量级、可管理的区块链能够更好地落实在实际商业应用场景中,由于其链上往往会保存非公开的商业机密数据,数据隐私保护对于联盟链更为重要。因此,分析并解决区块链尤其是联盟链的安全隐私问题是推动区块链技术广泛应用于实际业务场景的关键。

目前,大部分联盟链通过公钥基础设施(PKI)体系完成系统内部成员身份的互相认证。用户将自己的真实身份与 PKI 系统内的 CA (certificate Authority) 颁发的自签名证书相互绑定,由于系统内的所有用户对 CA 是信任的,因此数字证书上用户的身份信息也是可信的<sup>[5-6]</sup>。这种认证体系的优点在于完成验证只需要验证证书上保存的 CA 自签名的有效性,证书的监管也由第三方 CA 来承担,无须给系统带来额外负担,但这样做的缺点也很明显,用户在网络上的行为都是实名制的,无法匿名化。

为解决这一问题,当前应用范围最广、落地项目最多的联盟链 Fabric 构建了身份证书和交易证书这样的二级证书体系。对于一般可公开的交易,用户可以直接使用基于传统 PKI 的身份认证体系,而当需要执行匿名交易时,用户可以使用由身份证书派生出的匿名证书实现认证节点的匿名化<sup>[7]</sup>。并且,在必要时,交易证书颁发机构和区块链的监管节点可以对交易去匿名化,降低

用户滥用匿名证书的风险,从而实现前台可匿名、后台可监管的功能<sup>[8-9]</sup>。但通过分析发现, Fabric 这种二级证书体系存在一些缺陷。首先,在交易证书的生成方案中使用了大量的 HMAC 运算,计算量比较大。其次,交易证书结构复杂,其扩展域中保存了大量用于生成交易证书的私钥的密文,但这在匿名认证的过程中是用不到的。最后,在监管方面, TCA 和监管节点都可以利用自己保存的密钥揭露交易证书持有者的真实身份,在功能上重叠,没有实现权限分离,因此其中一方不诚实或遭受单点攻击,匿名证书就失去了安全性<sup>[10]</sup>。针对上述问题,本文在 Fabric 已构建好的二级证书体系的基础上,通过改进交易证书生成算法,降低了证书生成过程中的计算量,优化了证书结构,实现了权限分离和解决了单点攻击问题并增强证书的匿名性,为 Fabric 提供了更为灵活、高效的匿名身份认证方案。

## 2 Fabric 中的匿名认证方案

Fabric 中的 PKI 匿名认证基于两级证书体系,用于匿名交易的匿名证书 Tcert 由身份认证证书 Ecert 生成<sup>[11]</sup>,并且 Tcert 公私钥的生成依赖于椭圆曲线公私钥的叠加特性,即多个对应的公私钥相加后得到的新的公私钥仍然具有对应关系。匿名证书 Tcert 的结构如表 1 所示。

表 1 Fabric 中的 Tcert 证书结构  
Table 1 Structure of Tcert certificate in Fabric

| 名称              | 描述          |
|-----------------|-------------|
| TcertID         | 匿名证书 ID     |
| encEcrtID       | 身份证书 ID 的密文 |
| encIndex        | Index 的密文   |
| Tcert_pk        | 匿名证书公钥      |
| Extension       | 证书扩展域       |
| Validity_Period | 证书有效期       |

### 2.1 匿名证书生成阶段

当用户需要申请匿名证书时,首先要向 TCA 提交申请, TCA 接收到用户提交的申请后,为了生成匿名证书, TCA 执行生成公钥、扩展域和私钥 3 个步骤,分别如图 1~图 3 所示。

(1) TCA 生成匿名证书公钥。

① TCA 选取随机数种子  $r_1$  计算后续用于派

生的密钥。

$$DF\_Key = H(r_1, Ec_{cert\_pk}) \quad (1)$$

② 计算扩展密钥。

$$Exp\_Key = H(DF\_key, "2") \quad (2)$$

③ TCA 选取随机数作为计数器 Index 的初始值，根据用户申请的证书数量 TcertIndex 逐次增加 1，并计算扩展值。

$$Exp\_Value = H(Exp\_Key, Index) \quad (3)$$

④ TCA 利用申请用户注册证书 Ec\_{cert} 中的公钥和扩展值生成 Tcert 证书公钥。

$$Tcert\_pk = Ec_{cert\_pk} + Exp\_Value \cdot G \quad (4)$$

⑤ TCA 将匿名证书 Tcert 以及派生密钥 DF\_Key 使用安全信道发送给用户。

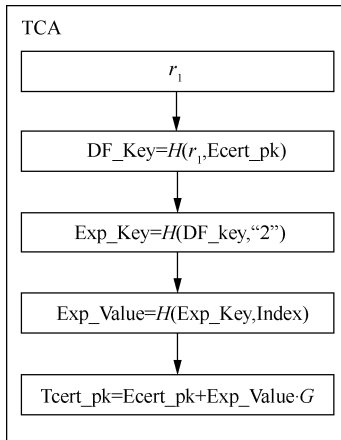


图 1 匿名证书公钥生成步骤

Figure 1 Anonymous certificate public key generation step

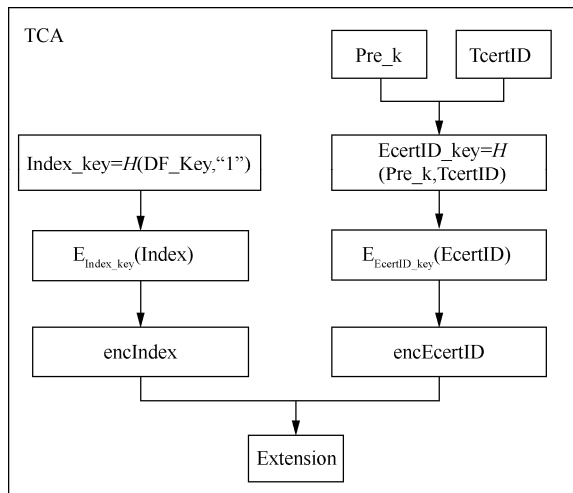


图 2 匿名证书扩展域生成步骤

Figure 2 Anonymous certificates extend the domain generation step

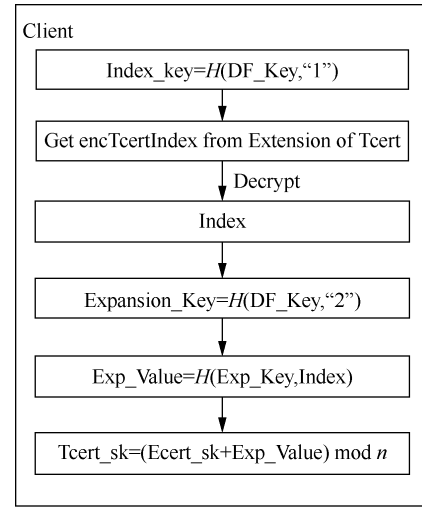


图 3 匿名证书私钥生成步骤

Figure 3 Anonymous certificate private key generation step

(2) TCA 生成匿名证书扩展域。

① TCA 计算用于加密索引值 Index 的密钥 Index\_key。

$$Index\_key = H(DF\_Key, "1") \quad (5)$$

② 加密 Index。

$$encIndex = E_{Index\_key}(Index) \quad (6)$$

③ TCA 利用 TcertID 以及只对 TCA 和监管者可见的 Pre\_k 计算用于加密 Ec\_{certID} 的密钥 Ec\_{certID}\_key。

$$Ec_{certID\_key} = H(Pre\_k, TcertID) \quad (7)$$

④ 加密 Ec\_{certID}。

$$encEcrtID = E_{Ec_{certID\_key}}(Ec_{certID}) \quad (8)$$

并由 encIndex 和 encEcrtID 共同组成匿名证书的 Extension 扩展域。

(3) 用户生成匿名证书私钥。

① 用户计算用于解密 encIndex 的密钥。

$$Index\_key = H(DF\_Key, "1") \quad (9)$$

② 用户从匿名证书的扩展域部分读取密文 encIndex，并对其解密。

$$Index = D_{Index\_key}(encIndex) \quad (10)$$

③ 用户计算扩展密钥。

$$Exp\_Key = H(DF\_Key, "2") \quad (11)$$

④ 用户计算扩展值。

$$Exp\_Value = H(Exp\_Key, TcertIndex) \quad (12)$$

⑤ 用户利用扩展值  $\text{Exp\_Value}$  和注册证书  $\text{Ecrt}$  对应的私钥  $\text{Ecrt\_sk}$  计算。

$$\text{Tcert\_sk} = (\text{Ecrt\_sk} + \text{Exp\_Value}) \bmod n \quad (13)$$

## 2.2 身份追踪阶段

在匿名证书使用过程中, 为了防止用户滥用匿名证书以及发生交易纠纷时能够确定责任方身份, 需要系统具备对匿名证书背后用户的真实身份追踪的功能。原方案中, TCA 或监管者可以利用自己掌握的  $\text{Pre\_k}$  完成对匿名证书真实身份的追踪, 其步骤如下。

① TCA 或监管者使用加密密钥  $\text{Pre\_k}$  和  $\text{TcertID}$  计算。

$$\text{EcrtID\_key} = H(\text{Pre\_k}, \text{TcertID}) \quad (14)$$

② TCA 或监管者解密得到  $\text{EcrtID}$ 。

$$\text{EcrtID} = D_{\text{EcrtID\_key}}(\text{encEcrtID}) \quad (15)$$

## 2.3 存在的问题

通过分析上述流程可以发现原始方案满足了匿名证书应具备的匿名性、无关联性以及可追踪性, 但仍然存在以下几个问题。

① 计算复杂: 在匿名证书以及公私钥的生成阶段需要进行大量的 HMAC 运算, 生成证书所需的计算代价比较大。

② 存储结构复杂: 匿名证书中存储了身份证书记录的密文以及匿名证书索引的密文, 因此证书的数据结构比较复杂。

③ TCA 和监管者在功能上重复且易遭受单点攻击: TCA 和监管者都掌握用于生成扩展域以及匿名身份追踪的  $\text{Pre\_k}$ , 但在证书生成阶段仅由 TCA 单方面完成, 且在追踪阶段只需任意一方即可单独完成, 倘若有一方不诚实或遭受攻击, 匿名证书就失去其安全性。

## 3 方案设计

为了在实现现有方案功能的基础上, 解决 2.3 节中提出的问题, 本文设计了一个可以实现权限分离的匿名证书解决方案。

新方案在证书的生成和追踪阶段都需要 TCA 和监管者联合才能完成。按照协议, 任一方想要单独完成匿名证书的生成或追踪理论上是不可行的。用于匿名追踪的关键信息分别由

TCA 和监管者加密存储在各自的数据库中, 因此仅对一方实施攻击无法追踪到匿名证书对应的真实身份, 具有抗单点攻击的特性。此外, 改进后的方案在证书生成阶段无须进行大量的 HMAC 运算, 提高了证书生成效率并且生成后的证书结构中无须保存多余密文数据, 降低了匿名证书的存储开销。

### 3.1 匿名证书发布

图 4 为改进方案匿名证书生成步骤, 该方案模型中主要角色为监管者、TCA、CA 以及用户。其中 TCA 和监管者均由 CA 的授权机构担任, CA 负责为监管者和 TCA 分别颁发身份证证书, 且监管者、TCA 以及 CA 各自具有独立数据库以便对匿名证书进行追踪和存储时所使用加密数据。

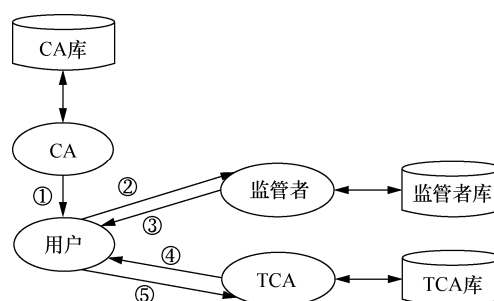


图4 改进方案匿名证书生成步骤

Figure 4 Anonymous certificate generation steps in improved scheme

本文方案使用 ECC(椭圆曲线)加密和 ECDSA 签名算法, TCA 和监管者共享公钥参数  $(g, Q)$ , 选择椭圆曲线上循环群  $G$  中的一个生成元用  $g$  表示, 其阶为  $n$ 。  $Q$  为群中一点, 满足  $Q = g^d$ , 其中  $d$  为随机选取的大整数。对于 TCA 和监管者的私钥  $d_1$ 、 $d_2$ , 为了实现权限分离, 令  $d = d_1 \cdot d_2$ 。本文方案假设 TCA 和监管者不能串通, 方案中使用的符号说明如表 2 所示。

匿名证书生成步骤如下。

① CA—>U: 用户将自己的个人信息以及实名证书请求提交给 CA, CA 核实用户的真实信息后, 为用户颁发实名证书  $\text{Ecrt}$ , 并将其保存在 CA 数据库中。

② U—>Admin: 在本地用户 U 设置个人的匿名证书  $\text{AID}$ , 同时建立对应证书的公私钥对  $(\text{APK}, \text{ASK})$ 。用户随机选择数字  $p$ , 同时计算得出序列号为

表2 符号说明  
Table 2 Symbol description

| 符号    | 符号说明     | 符号    | 符号说明     |
|-------|----------|-------|----------|
| CA    | 实名证书颁发机构 | TCA   | 匿名证书颁发机构 |
| U     | 用户       | Admin | 监管者      |
| PK    | 用户实名公钥   | SK    | 用户实名私钥   |
| $M$   | 匿名证书内容   | APK   | 匿名证书公钥   |
| ASK   | 匿名证书私钥   | Ecrt  | 实名证书     |
| Tcert | 匿名证书     | ID    | 实名身份     |
| AID   | 匿名身份     | SN    | 匿名证书序列号  |
| USig  | 联合签名     | SP    | 服务提供者    |

$$SN = H(APK, p) \quad (16)$$

匿名证书的头部  $b$  为  $(AID, SN, APK)$ 。这个匿名证书的内容  $M$  为  $(b, h(Ecrt))$ 。最后用户选取随机数  $r_1$  并计算  $u = g^{r_1}$ ，用户将  $u$  和实名公钥签名  $Sig_{PK}(u)$  发送给监管者 Admin。

③ Admin  $\rightarrow$  U: Admin 先对用户发送的签名消息进行验证以确认用户身份，如果验证通过，计算  $w = u^{d_1}$ ，将  $\langle E_{d_1}(u): ID \rangle$  以键值对的形式保存在监管者数据库中。最后将  $w$  发送给用户 U。

④ U  $\rightarrow$  TCA: 用户 U 接收到 Admin 发送的  $w$  后，用匿名私钥 ASK 对  $M$  进行签名  $Sig_{ASK}(M)$ ，并将签名、随机数  $r_1$  和  $w$  发送给 TCA。

⑤ TCA  $\rightarrow$  U: TCA 接收到消息后，首先验证 U 的匿名私钥签名。若验证通过，TCA 计算  $z = w^{d_2}$ ，再验证  $z^{r_1^{-1}}$  与公共公钥  $Q$  是否相等。若相等，TCA 将  $\langle SN: E_{d_2}(z) \rangle$  以键值对的形式保存在 TCA 数据库中。最后选取随机数  $r_2$ ，计算联合签名

$$USig_d = (g^{r_2}, (h^{-1}(M) + g^{r_2 d_1 d_2}) r_2^{-1}) \quad (17)$$

并发送给用户 U，则用户 U 得到匿名证书  $(M, USig_d)$ 。

这个模型实现了 TCA 在不知道用户真实身份的基础上验证匿名证书的内容，而监管者是在不知道匿名证书内容的基础上来验证用户的真实身份。在经过权限分离的验证后，最终由 TCA 和监管者共同为用户的匿名证书生成联合签名 USig。

### 3.2 匿名证书追踪

当发现匿名证书被滥用或私钥泄露时，服务

提供者 (SP) 可以向 TCA 提交匿名身份追踪请求，具体追踪步骤如下。

① SP  $\rightarrow$  TCA: SP 向 TCA 提交追踪申请和匿名证书序列号 SN。

② TCA  $\rightarrow$  Admin: TCA 根据服务提供者发送的匿名证书序列号 SN 检索 TCA 数据库得到对应的  $E_{d_2}(z)$ ，并使用  $d_2$  解密得到  $z$  的值。最后由 TCA 把  $z$  的值发送给监管者 Admin。

③ Admin: 监管者 Admin 接收到  $z$  后，根据公共公钥计算  $u = zQ^{-1}$ ，然后计算  $E_{d_1}(u)$ ，最后根据  $E_{d_1}(u)$  检索监管者数据库得到用户的真实身份 ID。

### 3.3 匿名证书撤销

由于匿名证书是由用户的实名证书构造得出，因此如果发现存在匿名证书私钥泄露、被他人私自使用以及时间过期的情况，则需要撤销该证书，撤销的具体步骤如下。

① 用户需要向 TCA 发出撤销匿名证书的请求，并且附带个人相关信息。

② 利用追踪功能，提交需要撤销证书的序列号确定到个人 ID。

③ TCA 会将用户的个人 ID 以及撤销证书的申请一起发送给 CA。

④ CA 会在库中通过提交的用户 ID，查找出实名证书，并验证用户提交的信息，待验证无误后准许证书撤销请求，同时将实名证书加入 CRL 撤销数据中，并向 TCA 回复应答信息。

⑤ 撤销匿名证书，TCA 会将匿名证书计入 CRL 撤销数据中，同时将撤销的结果回传给用户。

## 4 方案分析

### 4.1 匿名性分析

本文方案中发布的匿名证书虽然是由用户的实名证书派生，但用户的匿名证书标识是通过组合用户实名公钥以及随机生成的机密数并利用哈希运算方法得到的，同时在生成的匿名证书中不会存在用户的相关信息数据，所以匿名证书可以有效保护用户的个人信息，实现匿名性。

### 4.2 真实身份证明

在生成证书过程的步骤③中，用户通过个人实名私钥进行  $u$  的签名，同时将其提交给监管者，

监管者用接收到的实名公钥来验证用户提交的数据。如果验证通过,则用户的身份被证明,监管者获取了用户的真实身份。

### 4.3 联合签名生成分析

在生成证书阶段的步骤④中,用户向 TCA 发送了  $(\text{Sig}_{\text{ASK}}(M), r_1, w)$ 。TCA 首先使用用户的匿名公钥 APK 验证签名的有效性,然后计算  $z = w^{d_2}$ ,为了验证  $w$  是由监管者的私钥生成,TCA 使用公共公钥  $Q$  验证  $z^{r_1^{-1}}$  与  $Q$  是否相等,原因是

$$z^{r_1^{-1}} = w^{d_2 r_1^{-1}} = u^{d_1 d_2 r_1^{-1}} = g^{d r_1^{-1}} = Q \quad (18)$$

这里  $d = d_1 d_2$ ,所以上述等式成立,TCA 可以验证  $w$  是由监管者的私钥生成。最后 TCA 生成用于联合签名的随机数  $r_2$  并计算联合签名。

$$\text{USig} = (g^{r_2}, r_2^{-1} (h^{-1}(m) + g^{r_2 d_1 d_2})) \quad (19)$$

TCA 将  $z$  和联合签名 USig 发送给用户 U。

用户 U 在接收到  $z$  后,同样使用上述等式对  $z$  的有效性进行验证。如果验证通过,则用户 U 得到匿名证书  $(M, \text{USig})$ 。

### 4.4 可追踪性分析

当区块链系统中的服务提供者发现用户匿名证书被滥用时,可以向 TCA 提交身份追踪请求,在请求中包含匿名证书的 SN 序列号。TCA 在接收到 SN 序列号后,检索自己的数据库并得到对应的  $E_{d_2}(z)$ ,TCA 使用该加密算法中的对称密钥  $d_2$  解密得到  $z$  并发送给监管者 Admin。Admin 接收到  $z$  后,首先计算

$$u = zQ^{-1} \quad (20)$$

然后计算  $E_{d_1}(u)$  的值,并检索出数据库中对应的用户真实身份 ID,其证明如下。

$$zQ^{-1} = g^{r_1 d_1 d_2} Q^{-1} = g^{r_1} = u \quad (21)$$

此外,由于监管者和 TCA 各自的数据库中保存的是经各自私钥加密后的数据  $E_{d_1}(u)$ 、 $E_{d_2}(z)$ ,基于大数分解难题,攻击者至少需要掌握公共私钥  $d$ 、监管者私钥  $d_1$ 、TCA 私钥  $d_2$  中的两个或以上才能威胁到匿名证书的安全。

## 5 方案对比

对改进方案分析可知,新方案在证书生成效

率阶段无须进行大量 HMAC 运算,证书数据存储结构简单,符合 X.509 标准,并且在满足匿名证书所需的一般安全属性同时,实现了 TCA 与监管者的分权管理,解决了 TCA 或监管者单方不诚实和易遭受单点攻击等安全性问题。

### 5.1 证书生成效率对比

改进后的方案优化了原本生成匿名证书所需的计算量,表 3 是对匿名证书生成过程的两种方案计算复杂度的对比,其中,  $N_h$  表示计算哈希次数,  $N_s$  表示签名计算次数,  $N_e$  表示加密次数,  $N_d$  表示解密次数,  $N_p$  表示点乘次数。

表 3 两种方案计算复杂度的对比  
Table 3 Comparison of computational complexity between the two schemes

| 方案   | $N_h$ | $N_s$ | $N_e$ | $N_d$ | $N_p$ |
|------|-------|-------|-------|-------|-------|
| 原有方案 | 7     | 3     | 2     | 2     | 3     |
| 改进方案 | 1     | 3     | 2     | 0     | 3     |

通过改进前后的对比,能够清晰地看到改进后的方案比原有方案哈希运算次数减少 6 次,解密运算次数减少 2 次。

### 5.2 证书结构对比

在原有方案中,匿名证书结构包括了身份证书 ID 以及匿名证书索引的密文等数据项,因此证书结构比较复杂,占用系统的存储开支较大。改进后的方案无须保存除用户基本信息和 CA 签名外的任何多余信息,数据项符合 X.509 协议标准,从结构上来说,与一般的身份证书无异,方便证书授权机构与用户存储和管理证书。具体结构如图 5 所示。

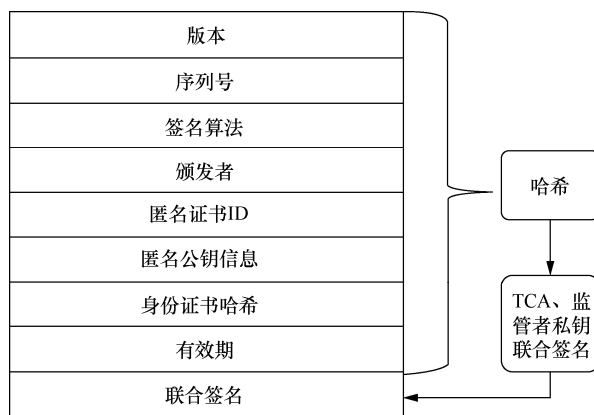


图 5 改进方案匿名证书结构  
Figure 5 Anonymous certificate structure in improved scheme

### 5.3 安全性对比

与原有方案相比,改进后的方案在匿名证书的生成过程中实现了TCA对证书内容可见,用户身份不可见。监管者对用户身份可见、对证书内容不可见的特性,增强了用户的匿名性。而且在用户真实身份追踪的过程中,需要TCA和监管者分别提供各自掌握的关键信息,解决了TCA和监管者单方不诚实以及单点攻击对匿名证书安全性造成的威胁。

## 6 结束语

本文提出了一种基于Hyperledger Fabric平台的权限分离的匿名认证体系。与原有方案相比,在安全性上,改进后的方案不仅实现了前台可匿名、后台可追踪的功能,还对监管者和TCA进行了权限分离,解决了TCA与监管者单方不诚信以及单点攻击等问题。在存储效率方面,改进后的方案在证书结构上无须保存在匿名证书生成阶段使用的密文,节省了系统对于匿名证书的存储开销。在证书生成效率方面,改进后的方案大幅减少了哈希以及解密的运算次数,节省了系统的计算开销。

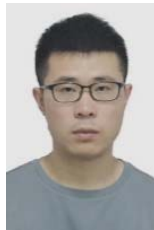
### 参考文献:

- [1] 工业和信息化部. 中国区块链技术和应用发展白皮书[R]. 2016. The Ministry of Information Industry. White paper on blockchain technology and application development in China[R]. 2016.
- [2] 张奥, 白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报, 2020, 31(5): 1406-1434. ZHANG A, BAI X Y. Review of blockchain privacy protection research and practice[J]. Journal of Software, 2020, 31(5): 1406-1434.
- [3] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20. SHEN X, PEI Q Q, LIU X F. An overview of blockchain technology[J]. Journal of Network and Information Security, 2016, 2(11): 11-20.
- [4] 刘九良, 付章杰, 孙星明. 区块链安全综述[J]. 南京信息工程大学学报(自然科学版), 2019, 11(5): 513-522. LIU J L, FU Z J, SUN X M. Blockchain security review [J]. Journal of Nanjing University of Information Science & Technology (Nat-

ural Science Edition), 2019, 11(5): 513-522.

- [5] 侍伟敏. PKI、IBE 关键技术的研究及应用[D]. 北京: 北京邮电大学, 2006. SHI W M. Research and application of PKI and IBE key technologies[D]. Beijing: Beijing University of Posts and Telecommunications, 2006.
- [6] 赵伟, 张问银, 王九如, 等. 基于区块链的企业管理系统框架设计与分析[J]. 网络与信息安全学报, 2019, 5(2): 13-22. ZHAO W, ZHANG W Y, WANG J R, et. Design and analysis of enterprise management system framework based on blockchain. Journal of Network and Information Security, 2019, 5(2): 13-22.
- [7] WANG R, HE J, LIU C, et al. A privacy-aware PKI system based on permissioned blockchains[C]//2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS). 2018: 928-931.
- [8] Membership service providers (MSP) [EB].
- [9] 张青禾. 区块链中的身份识别和访问控制技术研究[D]. 北京: 北京交通大学, 2018. ZHANG Q H. Research on identity recognition and access control technology in blockchain[D]. Beijing: Beijing Jiaotong University, 2018.
- [10] 郭青霄. Fabric 中的身份隐私和数据隐私保护技术研究[D]. 北京: 北京交通大学, 2019. GUO Q X. Research on identity privacy and data privacy protection technology in Fabric [D]. Beijing: Beijing Jiaotong University, 2019.
- [11] Hyperledger fabric documentation, getting started and developer guides[EB].

### [作者简介]



叶岳洋(1992-), 男, 北京人, 北京工业大学硕士生, 主要研究方向为区块链和信息安全。



张兴兰(1970-), 女, 山西吕梁人, 博士, 北京工业大学教授, 主要研究方向为区块链和经典密码学。