网络首发时间：2023-03-09 09:31:34
网络首发地址：https://kns.cnki.net/kcms/detail/50.1075.TP.20230308.1209.014.html

计算机科学 COMPUTER SCIENCE http://www.jsjkx.com
DOI:

基于秘密共享的多因素区块链私钥保护方案

肖 健　杨 敏

武汉大学国家网络安全学院空天信息安全与可信计算教育部重点实验室　武汉 430072
武汉大学国家网络安全学院 武汉 430072
（smithrb@163.com）

摘 要 针对区块链因缺少恢复机制导致用户私钥一旦丢失就难以找回的问题，提出了一种基于口令、秘密问题和指纹的多因素区块链私钥保护方案。该方案无需用户存储额外信息且可以完全在线上实施，并采用了抗遗忘的因素访问策略。在注册阶段，用户需要提供所有因素信息(包括口令、秘密问题和指纹)以及区块链私钥，并使用秘密共享方案为一组服务器分配秘密份额。在恢复阶段，用户仅需要提供部分因素并向多个服务器发送恢复申请，即可获得其秘密份额的信息并以此重构出区块链私钥。实验结果和启发式安全分析表明，该方案中客户端和服务端的计算开销都在毫秒级，可以抵抗已知攻击且通过支持多因素提供了更好的安全性。

关键词： 多因素区块链私钥保护；秘密共享；口令保护秘密共享；模糊提取

中图法分类号 TP309.7　　DOI：10.11896/jsjkx.220600069

Multi-factor Blockchain Private Key Protection Scheme Based on Secret Sharing

XIAO Jian and YANG Min

Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Abstract Aiming at the problem that the user's private key is difficult to retrieve once lost due to the lack of a recovery mechanism in the blockchain, a multi-factor blockchain private key protection scheme based on passwords, secret questions and fingerprints is proposed. The scheme does not require users to store additional information and can be implemented completely online, and adopts an anti-forgetting factor access strategy. During the registration phase, users need to provide all factor information (including password, secret question and fingerprint) and blockchain private key, and use a secret sharing scheme to assign a secret share to a group of servers. In the recovery phase, users only need to provide some factors and send recovery applications to multiple servers to obtain the information of their secret shares and reconstruct the private key of the blockchain. Experimental results and heuristic security analysis show that the computing cost of both client and server in this scheme is in milliseconds, and it can resist known attacks and provide better security by supporting multiple factors.

Keywords Multi-factor blockchain private key protection，Secret sharing，Password protected secret sharing，Fuzzy extraction

1 引言

区块链本质上是一个去中心化的分布式存储系统，它不需要中心化机构授信，而是通过共识算法和密码协议将数据传输到所有节点，从而构

到稿日期：2022-06-07　　返修日期：2022-11-09
基金项目：国家自然科学基金(62172308)；国家重点研发计划(2021YFB2700200)
This work was supported by the National Natural Science Foundation of China(62172308) and National Key R&D Program of China(2021YFB2700200).
通信作者：杨敏(yangm@whu.edu.cn)

建具有去中心化、公开透明、不可篡改等特性的存储系统。所有用户在使用区块链系统进行数据存储时，都必须使用区块链私钥作为访问区块链的唯一身份凭证。但是，区块链私钥可记忆性差，只能通过如硬件钱包、加密钱包、纸质钱包、脑钱包等将其保存。而且，正是由于区块链具有去中心化特征，使得区块链缺少类似于可信中心化机构的恢复机制，这导致区块链私钥一旦被遗忘或随着钱包丢失就难以找回[1]，即区块链无法使用中心化机构中的通过对用户的其他身份信息进行认证（如身份证、护照等）从而进行重构或恢复操作。据文献[2]所述，在比特币系统中，所有被遗忘私钥的区块链账户价值总额估计高达数十亿美元，达到了现有比特币总量的20%。因此，提出一种安全可行的区块链私钥恢复方案是亟待解决的问题。

目前，针对区块链的私钥保护问题，工业界和学术界主要围绕用户持有的社交关系、可记忆信息以及生物特征信息这几个方面进行研究。

社交恢复[3-4]是一种利用用户的社交关系来恢复账户的方案。该方案中，用户需要预先注册一个备用区块链账户，并登记社交伙伴的区块链账户。当用户的私钥丢失时，系统会通知其社交伙伴，请求其对该用户的私钥恢复请求进行签名。如果大多数社交伙伴发送的签名有效，系统会将原账户资金转移到备用账户。但是该方案在实际应用中存在着诸多问题。首先，用户的大部分社交伙伴都必须是拥有区块链账户且可信任的；其次，用户备用账户的私钥仍然可能丢失；最后，该方法仅仅实现了原始账户资金的转移，无法恢复原始账户的私钥。

托管服务[5-6]，是一种通过用户记忆口令来实现对私钥操作的方案，包括托管钱包、多签名钱包[7]等。当用户私钥丢失时，用户可以直接通过口令来进行资金转移或私钥恢复。但是这种中心化方案仍然存在着单点失效、后门攻击等问题，且一旦托管服务器被攻破，大量密钥失窃将会造成严重的损失[7]。

口令保护秘密共享[8-11]是一种通过用户记忆口令来进行私钥恢复的方案。该方案本质上是一种 t-of-n 的在线秘密共享方案。该方案中，用户需要将一个秘密随机数预先分割为多个份额，并发送到多个服务器（第三方平台服务器、用户智能设备等）中。当用户私钥丢失时，用户需要通过口令主动向这些服务器发送恢复申请，请求获得其秘密份额。当用户收集到大多数秘密份额后，就能从这些服务器中恢复出该秘密，进而通过该秘密恢复出原始私钥。并且在这一过程中，除了用户外，其他人无法获得用户口令和私钥的任何信息。这种方案为结合口令和秘密共享以保护和恢复区块链私钥提供了极好的思路，但是它无法避免参与秘密共享的服务器合谋所带来的口令猜测攻击。

上述基于口令的私钥保护方案，还面临着如下问题：1）口令作为低熵信息是一种较弱的认证方式，经常面临着数据库外部泄露、离线字典攻击和在线口令猜测的风险[12]，将区块链私钥的保护完全归结于口令存在着安全风险；2）口令同样有遗忘的风险[13]，一旦口令遗忘，用户将无法找回原始区块链账户的私钥。

生物特征密码[14-16]是一种利用指纹、人脸等生物特征信息来进行私钥恢复的方案。该方案中，用户需要预先采集一次生物特征信息，用于生成一个随机字串和公开辅助信息。当用户的私钥丢失时，用户只需再采集一次生物特征信息，只要两次输入的生物特征信息非常接近，即可利用公开辅助信息恢复上述随机字串，进而恢复私钥。但是，该技术事实上非常依赖于生物特征采样和

生物特征提取技术，使用不当的采样设备和提取算法会减少生物特征包含的信息量，难以保证生物特征的唯一性。同时，由于这种方案是纯离线实施的，因此还会面临着离线猜测攻击，这在特征信息没有足够的熵或生物特征部分信息意外泄露时是非常致命的。

综上所述，目前基于社交关系、可记忆信息以及生物特征信息的区块链私钥保护方案在实际应用、安全性等方面都存在着诸多问题。为了解决上述问题，本文提出了一种基于口令、秘密问题和指纹的多因素区块链私钥保护方案。相较于口令，秘密问题是一种具有更好记忆性的信息[17]，指纹则是一种安全性更好而且不易丢失的高熵信息[18]。本文方案在口令保护秘密共享方案的基础上进行优化，其本质是使用了一种 2-of-3 因素认证策略。即该方案与原有方案的不同之处在于，用户私钥丢失时，用户不但需要提供口令或秘密问题的答案作为因素之一，还需要提供指纹作为另一个因素，并通过这两个因素向服务器发送恢复申请，才能获得其秘密份额。该方案在保留了口令保护秘密共享方案和生物特征密码的优势的同时，还解决了其面临的问题。本文方案的特点如下：

(1) 方案的实施完全在线上完成。用户无需去某个机构办理注册或恢复事务，无需与某些伙伴预先或事后进行线下沟通。

(2) 可恢复原始区块链私钥。用户在私钥恢复阶段可以得到原始区块链私钥，相较于仅支持资金转移的方案更具备通用性，而且无需注册备用区块链账户以及保管其私钥。

(3) 降低了口令遗忘和泄露带来的风险。由于私钥恢复时口令是可选因素，因此即便用户遗忘了口令，也能通过秘密问题这一因素来找回私钥。由于私钥恢复时必须提供指纹因素，因此即便用户的口令泄露，恶意攻击者也不能仅凭口令得到用户的私钥。

(4) 增加了生物特征密码方案的安全性。由于方案是在线上实施，这阻止了生物特征信息不足或部分泄露时，攻击者直接通过离线猜测进行攻击的可能。

(5) 增加了秘密共享方案的安全性。由于方案中使用了指纹这一高熵的信息，这使得即便多个服务器进行合谋，也难以仅通过口令猜测攻击获得用户因素和私钥的信息。

2 预备知识

本文使用的相关符号如表 1 所列。

表 1 常用符号

Table 1 Common notations

Notation	Explanation
U	User
S	Server
sk	Blockchain private key
pw	Password
P_Q/a	Secret questions/answers
w	Biometric Information Template
P_w/R_w	Public helper string/secret random string extracted from w
$\mathbb{G}$	Finite cyclic groups with prime order p
$\mathbb{Z}_p$	{0, 1, …, p-1}
$\{0,1\}^*$	A collection of strings with arbitrary length
$\{0,1\}^l$	A collection of strings with l-bit length
$H_1:\{0,1\}^* \rightarrow \{0,1\}^l$	A hash function which can map strings of arbitrary length to l-bit strings
$H_2:\{0,1\}^* \rightarrow \mathbb{G}$	A hash function which can map strings of arbitrary length to group elements in $\mathbb{G}$
Gen( )/Rep( )	Fuzzy extraction generation algorithm/regeneration algorithm
ShamirGen( ) /ShamirRec( )	Shamir secret sharing generation algorithm/regeneration algorithm
||	Splice operation

2.1 Shamir 的(t,n)秘密共享方案

Shamir的(t,n)秘密共享方案[19]是一种基于拉格朗日插值算法的技术。在该方案中，秘密分发者需要将共享秘密s分为n份并分发给n个参与者，每个参与者拥有一个份额s_i。由其中任意的至少t个份额可以重构该秘密。Shamir的(t,n)秘密共享方案由以下两个阶段组成：

(1) 秘密分发阶段，执行秘密分割算法$\text{ShamirGen}(s) \to s_1, s_2, \dots, s_n$。

秘密分发者首先构造一个$t-1$次多项式$F(x)$，$F(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + s$，其中$a_1, \dots, a_{t-1} \in Z$，且$a_{t-1} \neq 0$。计算秘密份额$s_i = F(i)$，最后将$s_i$分发给各个参与者$P_i, i = 1,2, \dots, n$。

(2) 秘密重构阶段，不少于t个参与者可以利用拉格朗日插值法重构出秘密s。例如成员$P = \{P_1, P_2, \dots, P_t\}$执行秘密重构算法$\text{ShamirRec}(s_1, s_2, \dots, s_t) \to s$。

首先可以通过下述公式重构多项式，然后计算$s = F(0)$获得原始秘密，其中λ_i被称为拉格朗日系数：$F(x) = \sum_{i=1}^{t} s_i \lambda_i$，$\lambda_i = \prod_{1 \le j \le t, i \neq j} (x-j)/(i-j)$

也可以不重构多项式，直接通过方式$F(0) = \sum_{i=1}^{t} s_i \lambda_{i,0}$，$\lambda_{i,0} = \prod_{1 \le j \le t, i \neq j} -j/(i-j)$一步获得原始秘密$s$。

Shamir的(t,n)秘密共享方案保证了任何不少于t个正确的份额都可以重构出秘密，而任何少于t个正确的份额都无法重构出秘密。

2.2 口令保护秘密共享方案

口令保护秘密共享方案是一种基于茫然伪随机数生成器和Shamir秘密共享方案的技术。在该方案中，用户需要将一个秘密共享给多个服务器，随后用户可以凭口令从这一组服务器中恢复出秘密。在这一过程中，其他任何人无法获得用户口令和秘密的任何信息，也无法得到服务器秘密份额的任何信息。这种功能使得它非常适用于区块链的私钥保护场景。

(t,n)口令保护秘密共享方案由以下两个阶段组成：

(1)密钥生成阶段

1) 用户指定n个服务器$P = \{P_1, P_2, \dots, P_n\}$作为秘密共享的参与方。如第三方平台服务器、用户智能设备等。

2) 用户选择一个随机秘密k，通过Shamir秘密共享方案将其分割为n份，然后通过安全信道发送给各个服务器。每个服务器均持有秘密k的一个份额k_i。

3) 用户通过口令pw和秘密k，计算$s = H_1(pw||H_2(pw)^k)$作为密钥。其中H_1, H_2为哈希函数，且满足$H_1: \{0,1\}^* \to \{0,1\}^l, H_2: \{0,1\}^* \to \mathbb{G}$。

(2)密钥恢复阶段

1)用户通过口令pw向任意的至少t个服务器发送恢复申请$A = H_2(pw)^r$，其中r为随机数。

2) 每个服务器收到申请后利用份额k_i计算$B_i = A^{k_i \lambda_{i,0}}$作为回应，其中$\lambda_{i,0}$为拉格朗日系数。

3)用户收集到不少于t个服务器的回应后，即可恢复出密钥s。例如，当用户收到服务器$P' = \{P_1, P_2, \dots, P_t\}$的回应后，可以通过如下计算恢复密钥：$s = H_1\left(pw||(\prod_{i=1}^{t} B_i)^{1/r}\right) = H_1(pw||(A^{\sum_{i=1}^{t} k_i \lambda_{i,0}})^{1/r}) = H_1\left(pw||A^{k/r}\right) = H_1(pw||H_2(pw)^k)$。

在该方案中任意不超过t个服务器合谋不能得到任何关于密钥或口令的任何信息，也无法通过在线攻击猜出用户口令。

值得注意的是，文献[8-11]中指出，密钥生成阶段一般有两种方案。上述方案是在安全信道中执行，这是为了保证用户进行份额分发时的安全性，例如采用 TLS 流量传输。同时，也可以选

择使用分布式密钥生成算法(Distributed Key Generation,DKG)直接为每个服务器生成秘密份额k_i，然后额外执行一次密钥恢复算法作为密钥生成阶段的一部分。前者执行效率更高且更符合密钥找回策略的实际应用场景，后者则无需设置安全信道。

2.3 模糊提取方案

模糊提取方案是生物特征密码技术的一种，下面我们仅介绍其中基于数字锁技术来实现的方案[16]。该方案具有从有噪声的随机源中产生均匀随机且可再生的字串的功能，因此经常被用于从具有模糊性的生物特征信息（如指纹、人脸等特征）中提取出可再生随机字串的场景。如图 1 所示，该模糊提取方案由初始化阶段和恢复阶段组成。

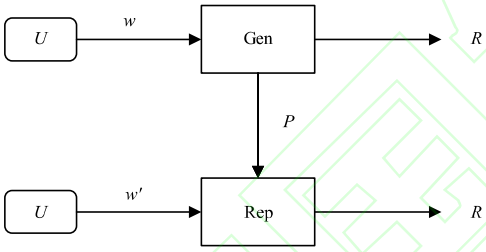

图 1 模糊提取

Fig.1 Fuzzy extraction

(1) 初始化阶段，用户执行生成算法$\mathrm{Gen}(w)\to R,P$。它以用户的有噪随机源（如人脸、指纹等生物信息）的一次采样为w输入，输出一个公开辅助字串P和可再生随机字串R。

1）用户对有噪随机源进行一次采样和特征提取，获得比特长度为n的特征串$w=w_1,w_2,\dots,w_n$。

2）用户选择一个比特长度为$l(l<n)$的随机串r作为密钥。

3）用户从$1,\dots,n$中随机选择l个不重复的数，记为$p=\{p_1,p_2,\dots,p_l\}$，计算$v=w_{p_1}||w_{p_2}||\dots||w_{p_l}$。

4）用户选择随机数$nonce$，计算$c=H(v||nonce)\oplus r$，其中H为哈希函数，且满足$H:\{0,1\}^*\to\{0,1\}^l$。

5）用户得到密钥$R=r$和公开辅助字串$P=(c,p,nonce)$。

(2) 恢复阶段，用户执行再生算法$\mathrm{Rep}(w',P)\to R$。它以用户的有噪随机源的一次采样w'和公开辅助字串P为输入，即可恢复出随机字串R。

1)用户对有噪随机源进行一次采样获得结果$w'=w'_1,w'_2,\dots,w'_n$。

2)用户利用公开辅助信息p计算得到$v'=w'_{p_1}||w'_{p_2}||\dots||w'_{p_l}$。

3)用户利用公开辅助信息$c,nonce$恢复$R=H(v'||nonce)\oplus c$。

该模糊提取方案来自于这样一个事实，即同一个人两次采样获得的生物特征中绝大部分比特位是相同的。该方案的容错能力由它所使用的参数l所决定。只要对于随机源的两次采样间的差距不超过容错阈值，恢复算法大概率能再生出随机字串R。用户可以通过对同一个密钥R多次执行初始化算法，以增加正确恢复出密钥的可能性，文献中给出了具体参数设置的建议，本文不再过多讨论。值得注意的是，上述描述的方案中，当用户恢复出私钥后，需要通过上层协议（例如用该密钥尝试打开对应的公钥账户）来确定是否正确恢复。

3 基于秘密共享的多因素区块链私钥保护方案

本研究方案是一种基于口令、秘密问题和指纹的多因素区块链私钥保护方案。该方案的实质是一种使用了 2-of-3 因素认证策略的秘密共享方案。该方案包含两个阶段，分别为注册阶段和恢复阶段。在注册阶段，用户需要提供所有因素

信息(包括口令、秘密问题和指纹)以及原始区块链私钥，并基于一个随机密钥为一组服务器分配一些秘密份额。在恢复阶段，用户需要提供口令或秘密问题的答案作为因素之一以及指纹作为另一个因素，并通过这两个因素向服务器发送恢复申请，才能获得其秘密份额的信息，从而重构出随机密钥，进而恢复原始区块链私钥。

3.1 注册流程

在注册阶段，用户首先需要将一个随机秘密共享给一组服务器，然后将该秘密以及所有因素信息生成一个随机密钥，最后将该随机密钥与原始区块链私钥进行绑定。其算法如图 2 所示。

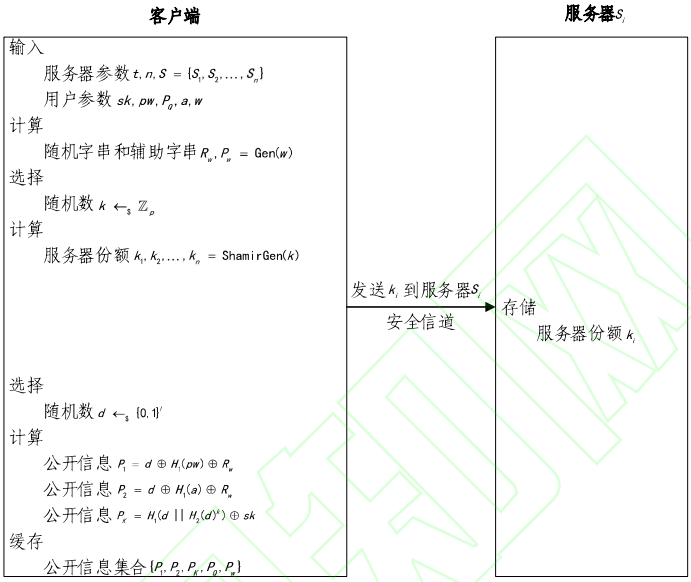

图 2 注册算法

Fig.2 Registration algorithm

(1) 客户端选取服务器设备参数，读取用户输入。

1) 用户U通过设备客户端指定任意n个服务器$S = \{S_1, S_2, \ldots, S_n\}$作为参与方，并选取参数$t$作为恢复阈值。服务器可以从第三方平台服务器、用户智能设备等中任意选取。

2)用户U在设备客户端输入长度为l的区块链私钥sk以及所有的3个因素：用户口令pw、用户自选的一组秘密问题及其答案集合P_Q/a，以及通过指纹特征采集装置获得的指纹特征信息模板w。

3) 客户端使用模糊提取生成算法Gen( )，生成指纹特征信息模板w所对应的随机字串和公开辅助字串$R_w, P_w = \mathrm{Gen}(w)$。

(2) 客户端向服务器发送秘密份额。

1) 首先生成秘密随机数$k \in \mathbb{Z}_p$，使用 Shamir的(t, n)秘密共享方案将其分为n个份额$k_1, k_2, \ldots, k_n$。

2)然后将上述份额安全传输给用户指定的n个服务器，即每个服务器都需要秘密保管一个份额k_i。

(3) 服务端存储秘密份额。

每个服务器S_i秘密保管一个份额k_i。

(4) 客户端生成公开信息，完成用户注册。

1) 首先生成秘密随机数$d \in \{0,1\}^l$，并以其构造出 2-of-3 的因素访问策略。

2) 构造使用口令因素以及指纹因素的访问策略。计算$P_1 = d \oplus H_1(pw) \oplus R_w$作为公开辅助字串。

3) 构造使用秘密问题因素以及指纹因素访问

策略。计算$P_2 = d \oplus H_1(a) \oplus R_w$作为公开辅助字串。

4)生成区块链私钥绑定信息。计算$s = H_1(d||H_2(d)^k)$作为随机密钥，计算$P_K = s \oplus sk$作为区块链私钥的绑定信息。

5) 缓存公开信息。将公开信息集合$\{P_1, P_2, P_K, P_Q, P_w\}$在客户端、服务器或者任意第三方数据库平台（如区块链）上缓存，以供查询。

至此用户完成了注册流程，之后用户无需保管除因素以外的任何信息，服务器仅需要秘密保管一个份额k_i，而公开信息集合$\{P_1, P_2, P_K, P_Q, P_w\}$可由任意方保管。

3.2 恢复流程

在恢复阶段，用户需要提供部分因素信息并向服务器发送恢复申请，然后通过服务器的回应消息重构出随机密钥，进而恢复出原始区块链私钥。其具体算法如图 3 所示。

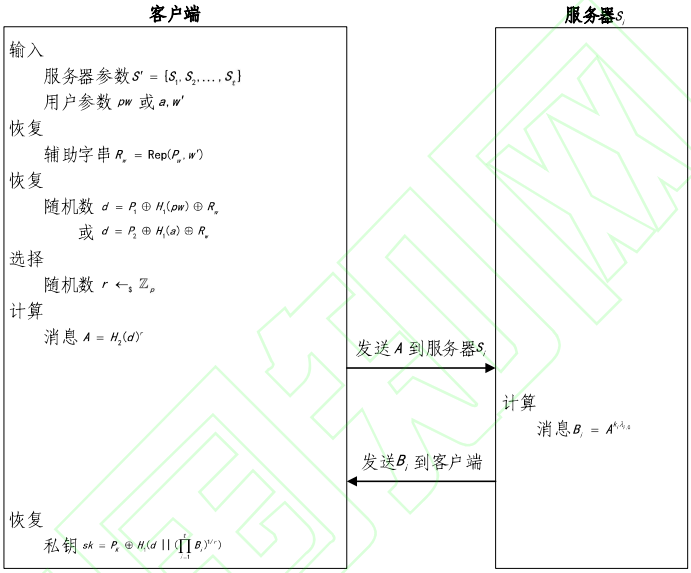

图 3 恢复算法

Fig.3 Recovery algorithm

(1) 客户端读取和处理用户输入。

1)用户U指定任意t个及以上服务器作为参与方，例如指定服务器组$S' = \{S_1, S_2, \ldots, S_t\}$作为参与方。在设备客户端输入任意满足访问策略的两个因素：用户口令pw或用户自选的一组秘密问题的答案a，以及通过指纹特征采集装置获得的指纹特征信息模板w'。

2)客户端使用模糊提取再生算法Rep( )，获得随机字串$R_w = \mathrm{Rep}(w', P_w)$。

(2) 客户端按照因素访问策略恢复秘密d。

1)若用户使用口令因素以及指纹因素的访问策略，则可以恢复秘密$d = P_1 \oplus H_1(pw) \oplus R_w$。

2)若用户使用秘密问题因素以及指纹因素的访问策略，则可以恢复秘密$d = P_2 \oplus H_1(a) \oplus R_w$。

3)客户端首先选取随机数$r \in \mathbb{Z}_p$，然后向各个服务器发送恢复申请$A = H_2(d)^r$。

(3) 客户端重构用户区块链私钥sk。

每个服务器收到恢复申请后，计算$B_i = A^{k_i \lambda_{i,0}}$作为回应。其中$\lambda_{i,0}$为拉格朗日系数。

(4) 客户端恢复用户区块链私钥sk。

1)客户端收到t个回应后即可恢复出随机密钥s，例如当收到服务器$S' = \{S_1, S_2, \ldots, S_t\}$的回应后，计算$s = H_1\left(d||(\prod_{i=1}^{t} B_i)^{1/r}\right) = H_1(d||(A^{\sum_{i=1}^{t} k_i \lambda_{i,0}})^{1/r}) = H_1(d||H_2(d)^k)$。

2)客户端恢复区块链私钥$sk = P_K \oplus s =$

$s \oplus sk \oplus s$。

至此用户完成了恢复流程，在这一过程中，只有当用户提供满足访问策略的因素时才能恢复出正确的区块链私钥。

4 方案分析

4.1 安全性分析

下面对因素访问策略的门限特性和一些重要的安全目标做启发式安全分析。

(1) (t,n)门限特性

对于(t,n)秘密共享方案来说，(t,n)门限特性是指将秘密分割并分发给n个参与方，满足至少t个正确份额即可恢复出原始秘密，少于t个正确份额不可以恢复出原始秘密，即攻击者使用$t-1$个秘密份额时，只能构造出$t-1$个含t个未知数的方程式组。本方案的因素认证事实上满足$(3,3)$门限特性。例如，通过口令和指纹来隐藏秘密d时，实际上是通过布尔秘密共享将d分割为如下 3 个份额：

$$d_1 = P_1 = d \oplus H_1(pw) \oplus R_w$$

$$d_2 = H_1(pw)$$

$$d_3 = R_w$$

只有已知d_1, d_2, d_3中的 3 个份额，才能求解d这个秘密，少于 3 个则不能。同理，通过秘密问题和指纹来分割秘密d时，也具有$(3,3)$门限特性。

(2) 2-of-3 因素认证策略

本方案的 2-of-3 因素认证不但满足$(3,3)$门限特性，而且满足访问策略，即只有提供用户口令pw和秘密问题的答案a作为份额之一，以及提供指纹因素w对应的份额才能从该秘密共享方案中恢复出秘密d。已知因素与份额之间存在如下关系：

$$P_1 = d \oplus H_1(pw) \oplus R_w$$

$$P_2 = d \oplus H_1(a) \oplus R_w$$

其中P_1, P_2均已知，实际只存在d, pw, a, w这 4 个未知数。当提供满足访问策略的因素时，用户可以从P_1或者P_2中解出d。然而当用户提供不满足访问策略的因素时，例如口令pw和秘密问题的答案a时，P_1和P_2将退化为同一个方程，此时无法解出d。

(3) 重要安全目标

1) 抵抗口令遗忘/泄露

本文 2-of-3 因素认证策略中使用了秘密问题因素，相较于口令，它是具有更好记忆性的信息。由于私钥恢复时用户口令是可选因素，因此即便用户遗忘口令，用户也能通过秘密问题这一因素来找回私钥。同时，指纹是一种安全性更好而且不易丢失的高熵信息。由于私钥恢复时必须提供指纹因素，因此即便用户的口令泄露，攻击者也不能仅凭口令得到用户的私钥。

2) 抵抗离线猜测攻击

虽然用户口令一般是低熵的，秘密问题也通常与用户身份相关，但在本文方案中它们仅出现在公开信息$P_1 = d \oplus H_1(pw) \oplus R_w$，$P_2 = d \oplus H_1(a) \oplus R_w$中，而$P_1, P_2$是高熵的，因为其中的$R_w$和$d$通常都是$l = 256$比特随机数，猜测得到$R_w$或$d$的可能性等价于直接猜测私钥。而离线猜测攻击成功的根本原因在于攻击者可以验证猜测的正确性，即尝试用恢复出来的区块链私钥对用户的区块链账户进行解密。而在本文方案中任何人都必须向服务器发送恢复申请才能恢复出区块链私钥，因此对于攻击者来说，由于无法获得秘密份额d使得其无法离线验证猜测是否成功，也就无法获得用户的区块链私钥。

3)抵抗冒充攻击

若攻击者选择对用户进行冒充，尝试在线猜测用户的口令(或秘密问题答案)以及指纹，并以此向服务器发送恢复申请，其首先会受到服务器的访问限制，即服务器不会允许对于同一个账户

无限次的恢复申请。

4) 抵抗窃听/重放攻击

在恢复阶段，对于用户发送的恢复申请$A = H_2(d)^r$，服务器发送消息$B_i = A^{k_i\lambda_{i,0}}$。由于对于用户发来的申请$A$，服务器发送的消息总是一致的，因此重放消息$A$并不比窃听攻击得到的信息更多。

由于除了用户没有其他人知道r，因此从消息A中猜测256比特的d是不可行的。根据离散对数难题的安全性，依靠服务器的消息获得秘密份额k_i的相关信息也是非常困难的。

5)抵抗合谋攻击

当多个服务器合谋时，它们可以利用各自的秘密份额重构获得秘密随机数k，并尝试从$P_K = H_1(d||H_2(d)^k) \oplus sk$获得用户的区块链私钥。如果合谋的服务器尝试直接猜测d，那么其难度相当于直接猜测私钥。而如果尝试从$P_1 = d \oplus H_1(pw) \oplus R_w$，$P_2 = d \oplus H_1(a) \oplus R_w$中先猜测$pw$或$a$以及$R_w$从而恢复$d$，并利用$P_K$验证猜测的正确性，即会归结于对于口令(或秘密问题答案)和指纹的猜测。只要用户保管指纹得当并且在注册时使用合适的指纹采集和提取算法，指纹作为高熵信息将难以被猜测出来。同时，服务器需要进行口令(或秘密问题答案)和指纹两个因素的猜测，其猜测难度仍相当大。

本文方案与各典型方案的比较如表2所列。

表2 本研究方案与现有典型方案的比较

Table 2 Comparison between ours work and typical studies

Target	Zhu 等[4]	Jarecki 等[9]	Canetti 等[16]	Ours
Offline process required	Y	N	N	N
Keep additional information	Y	N	N	N
Recover original private key	N	Y	Y	Y
Resist offline guessing attacks	Y	Y	Conditional	Y
Resist password forgetting	—	N	—	Y
Resist password leakage	—	N	—	Y
Resist impersonation attacks	Y	Y	—	Y
Resist eavesdropping Attacks	Y	Y	—	Y
Resist replay attacks	Y	Y	—	Y
Resist colluding attacks	N	N	—	Conditional

4.2 性能分析

基于秘密共享的多因素区块链私钥保护方案的测试客户端以及服务端使用Python 3实现，测试客户端安装在PC端，配置为：AMD R5-3550H CPU @ 2.1 GHz处理器；16GB DDR4-RAM内存；Windows 10操作系统。

测试服务端安装在云服务器，配置为：AMD R7-3700X CPU @ 3.59 GHz处理器；16GB DDR4-RAM内存；Windows 10操作系统。

私钥长度参数$l = 256$比特，群$\mathbb{G}$的阶为1024比特素数，服务器参数$t = 8, n = 10$。本文方案与其他典型方案的性能比较如表3所列。本文方案的客户端和服务端在注册阶段及验证阶段的计算开销在毫秒级，性能明显优于需要进行区块链广播交易的社交恢复方案[4]。但是，本文方案由于使用了多个因素，因此相较于仅使用口令的方案[9]或生物特征的方案[16]时间开销有所增加。

表3 本研究方案与现有典型方案的性能比较

Table 3 Performance comparison between ours work and typical studies

Stage		Zhu 等[4]	Jarecki 等[9]	Canetti 等[16]	Ours
Time cost of Registration /s	client	>5	0.153	0.118	0.300
	server	>5	0	—	0
Time cost of	client	>5	0.341	0.120	0.473

Recovery /s	server	>5	0.161	—	0.160
Total /s	client	>10	0.494	0.238	0.773
	server	>10	0.161	—	0.160

结束语 针对区块链缺少恢复机制导致用户私钥一旦被遗忘或因钱包丢失就难以找回的问题，本文提出了一种基于口令、秘密问题和指纹的多因素区块链私钥保护方案。该方案无需用户存储额外信息且可以完全在线上实施，而且多个因素的访问策略使得即使用户的部分因素丢失或遗忘，其私钥的可恢复性和安全性仍然能够得到保证。在下一步研究中，将对本方案所使用的秘密共享算法进行研究，使用基于属性的密码改进因素访问策略，进一步支持更灵活、更复杂、可撤销的访问策略，使用可公开验证秘密共享增加服务器作恶的检测和惩罚功能。

参考文献

[1] HAN X，YUAN Y，WANG F Y. Security Problems on Blockchain：The State of the Art and Future Trends[J]. Acta Automatica Sinica，2019，45(1)：206−225.

韩璇，袁勇，王飞跃. 区块链安全问题：研究现状与展望[J]. 自动化学报，2019，45(1)：206-225.

[2] JIANG Y. Vernacular Blockchain [M]. Beijing: China Machine Press, 2017: 363-365.

蒋勇.白话区块链[M]. 北京：机械工业出版社, 2017：363-365.

[3] LEE W, JIN J H, LEE M J. A Robust Identity Recovery Scheme for the Ethereum Blockchain Platform[J]. International Information Institute (Tokyo). Information, 2017, 20(11): 8133-8141.

[4] ZHU Y, XIA L, SENEVIRATNE O. A Proposal for Account Recovery in Decentralized Applications[C]//2019 IEEE International Conference on Blockchain (Blockchain). Halifax: IEEE, 2019: 148-155.

[5] LUSETTI M, SALSI L, DALLATANA A. A Blockchain Based Solution for the Custody of Digital Files in Forensic Medicine[J]. Forensic Science International: Digital Investigation, 2020, 35: 1-11.

[6] RAMOS S, PIANESE F, LEACH T, et al. A Great Disturbance in the Crypto: Understanding Cryptocurrency Returns Under Attacks[J]. Blockchain: Research and Applications, 2021, 2(3): 100021.

[7] ALFANDI O, KHANJI S, AHMAD L, et al. A Survey on Boosting IoT Security and Privacy through Blockchain[J]. Cluster Computing, 2021, 24(1): 37-55.

[8] JARECKI S, KIAYIAS A, KRAWCZYK H, et al. Highly-Efficient and Composable Password-Protected Secret Sharing (or: How to Protect Your Bitcoin Wallet Online)[C]// IEEE European Symposium on Security & Privacy. Saarbruecken: IEEE, 2016: 276-291.

[9] JARECKI S, KIAYIAS A, KRAWCZYK H, et al. TOPPSS: Cost-Minimal Password-Protected Secret Sharing Based on Threshold OPRF[C]// International Conference on Applied Cryptography and Network Security. Cham: Springer, 2017: 39-58.

[10] ERWIG A, HESSE J, ORLT M, et al. Fuzzy Asymmetric Password-Authenticated Key Exchange[C]//Advances in Cryptology – ASIACRYPT 2020. Cham: Springer, 2020: 761-784.

[11] JIANG J, WANG D, ZHANG G, et al. Quantum-Resistant Password-Based Threshold Single-Sign-On Authentication with Updatable Server Private Key[C]//European Symposium on Research in Computer Security. Cham: Springer, 2022: 295-316.

[12] HITAJ B, GASTI P, ATENIESE G, et al. Passgan: A Deep Learning Approach for Password Guessing[C]//International Conference on Applied Cryptography and Network Security. Cham: Springer, 2019: 217-237.

[13] LEE K, SJÖBERG S, NARAYANAN A. Password Policies of Most Top Websites Fail to Follow Best Practices[C]//Eighteenth Symposium on Usable Privacy and Security. 2022: 561-580.

[14] LAI Y L, LI M, LIANG S N, et al. Lossless Fuzzy Extractor Enabled Secure Authentication Using Low Entropy Noisy Sources[J]. Journal of Information Security and Applications, 2021, 58: 43-49.

[15] WEN Y, LIU S, HAN S. Reusable Fuzzy Extractor from The Decisional Diffie-Hellman Assumption[J]. Designs, Codes and Cryptography, 2018, 86(11): 2495-2512.

[16] CANETTI R, FULLER B, PANETH O, et al. Reusable Fuzzy Extractors for Low-Entropy Distributions[J]. Journal of Cryptology, 2021, 34(1): 1-33.

[17] MICALLEF N, ARACHCHILAGE N A G. Understanding Users' Perceptions to Improve Fallback Authentication[J]. Personal and Ubiquitous Computing, 2021, 25(5): 893-910.

[18] YANG W, WANG S, HU J, et al. Security and Accuracy of Fingerprint-Based Biometrics: A review[J]. Symmetry, 2019, 11(2): 141.
[19] LI Q, ZHOU Y. Research and Application Based on A Shamir’s (t, n) Threshold Secret Sharing Scheme[C]//7th International Conference on Computer Science and Education. Melbourne: IEEE, 2012: 671-674.

肖健，出生于 1999 年，硕士，CCF 会员，主要研究方向为区块链和密码学。
杨敏，出生于 1975 年，博士，副教授，硕士生导师，CCF 会员，主要研究方向为信息安全和应用密码学。

XIAO Jian， born in 1999, postgraduate, is a member of China Computer Federation. His main research interests include blockchain and applied cryptography.

YANG Min， born in 1975, Ph.D, associate professor , master supervisor, is a member of China Computer Federation. Her main research interests include information security and applied cryptography.

（责任编辑：何杨）