Computer Science and Application 计算机科学与应用, 2021, 11(7), 1845-1852
Published Online July 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.117189

Hans汉斯

边缘计算环境下基于区块链的双因子跨域认证

刘欢欢，许豪杰

长安大学理学院，陕西 西安
Email: 1968104743@qq.com, xuhaojiechn@163.com

收稿日期：2021年6月3日；录用日期：2021年7月1日；发布日期：2021年7月8日

摘　要

本文针对边缘计算环境下用户间跨域认证与密钥协商问题，基于区块链技术，利用口令的简便性及生物特征的唯一性设计跨域协议。该协议融入了模糊提取技术，提高了用户在认证密钥协商阶段的安全性和便捷性。协议中用户端选取性能高的边缘设备完成注册及认证过程，实现了用户在边缘认证服务器和区块链处的双重认证，在保障用户之间安全通信的同时减轻了云端的网络负担。此外，本文分析了协议满足的安全属性，且本文方案通信消耗较低。

关键词

边缘计算，区块链，跨域认证，模糊提取

Two-Factor Cross-Domain Authentication Based on Blockchain in Edge Computing Environment

Huanhuan Liu, Haojie Xu

School of Science, Chang'an University, Xi'an Shaanxi
Email: 1968104743@qq.com, xuhaojiechn@163.com

Received: Jun. 3rd, 2021; accepted: Jul. 1st, 2021; published: Jul. 8th, 2021

Abstract

Aiming at the problem of user-to-user authentication and key agreement of cross-domain in edge computing environment, a cross-domain is proposed under the blockchain technology with the simplicity of password and the unique identification of biometric features. The protocol enhances the security and convenience of user-to-user authentication and key agreement phase by using fuzzy

文章引用: 刘欢欢, 许豪杰. 边缘计算环境下基于区块链的双因子跨域认证[J]. 计算机科学与应用, 2021, 11(7): 1845-1852. DOI: 10.12677/csa.2021.117189

extraction technology. The edge devices with high performance are selected to complete the registration and authentication process. And the authentications of the user in the edge server and the blockchain are realized, which ensures the security communication of user-to-user and reduces the network burden of the cloud. In addition, the security of the protocol satisfies is analyzed and lower communication cost is required in the proposed scheme.

Keywords

Edge Computing, Blockchain, Cross-Domain Authentication, Fuzzy Extraction

1. 引言

物联网开启了万物互联时代，尤其是 5G 的普及和应用，将会构建一个智能化和数字化的世界，物联网的应用将逐渐延伸到我们的生活中。面对大量的智能设备，传统的终端－云端网络架构存在缺陷，当大量的数据传输到云端时增加了云中心的负担，而且云服务器与用户设备的距离较远，会引起能耗问题并且造成通信延迟[1]。为解决云计算问题，引入了边缘计算[2]，将部分计算和数据转移到终端附近，即在靠近终端处可以找到计算和存储节点的边缘设备。边缘计算环境下的网络结构为终端－边缘－云端，此时用户之间需要跨域通信，涉及到身份认证与密钥协商。

已有的云计算环境下物联网跨域认证问题，主要是基于 PKI 的，即用户的公私钥由数字证书发放，解决了用户密钥托管问题，避免了无证书密码体系的复杂搭建过程。文献[3]中移动设备的公私钥由基于证书的签名方法得到，不涉及复杂的证书管理，当设备访问外域网络时需进行全认证和重认证，提高了认证效率。文献[4]研究了边缘环境下的物联网认证架构，提出一种基于标识的密钥管理方法，并设计了基于身份标识的认证方案。而区块链的引入弥补了数字证书需要认证、管理、更新等不足，其核心优势是去中心化，数据安全透明。文献[5]利用区块链的优势对密钥托管问题进行优化，结合区块链证书机制和改进的 SM9 密钥生成算法进行身份认证，并保存认证信息，通过查询过程，设计快速的重认证协议。文献[6]提出一种基于区块链的分布式车载雾服务轻量级匿名认证，实现了跨数据中心身份认证。文献[7]基于区块链和边缘计算，提出了分布式可信身份验证系统，设计的非对称加密算法防止区块链节点和终端之间的连接被攻击，提高了认证效率。文献[8]基于联盟链，将终端设备的证书哈希值存于区块链上，避免了复杂的证书验证过程。

综上，边缘计算弥补了云计算的不足，就跨域认证问题，本文提出了基于口令和生物特征的用户间跨域认证与密钥协商协议，使得不同域中的用户可以完成注册和认证密钥协商。该协议通过区块链共识机制选取性能高的边缘服务器，参与终端注册和认证与密钥协商阶段。生物认证技术的利用提高了用户在认证密钥协商阶段的安全性和便捷性，从而实现了有效安全的跨域认证目标。

2. 预备知识

2.1. 椭圆曲线上离散对数困难问题[9]

假设 E 是一条椭圆曲线，g 为 p 阶循环群 G 的本原元，考虑方程 $y = g^x \bmod p$ (p 是一大素数)，给定 y，g，p，其中，$y, g \in Z_p^*$，计算 x 是不可行的。

2.2. 哈希函数

哈希函数可以将不同长度的字符串，转换成固定长度的散列值，如果输入的数据略有不同，那么输出完全不同。单向哈希函数 $h(\cdot)$ 是满足以下条件的函数：

1) 函数的输入 x 为任意长度，输出的 $h(x)$ 是固定长度。

2) 给定函数 h 和输入 y， $x=h^{-1}(y)$ 在计算上是不可行的。

3) 对任何给定的 x，寻找 $x'=x$ 使得 $h(x')=h(x)$ 在计算上是不可行的。

2.3. 模糊提取器

生物特征的模糊性是指对于生物特征，在每次提取时与生物模板比对会有细微的差别。若将生物信息直接用于哈希函数，则注册阶段与认证阶段存在容错性问题，为此提出了模糊提取器[10]。

模糊提取器主要包含两个算法，生成算法 *Gen* 和恢复算法 *Rep*：

1) $Gen(B)=(R,P)$，输入生物信息 B，*Gen* 输出提取的随机字符串 R 和辅助字符串 P。

2) $Rep(B',P)=R$，输入用户的生物信息 B'与辅助字符串 P，*Rep* 可以从 B'和 P 中恢复 R。

2.4. ElGamal 加密[11]

给定素数 p 及其本原根 g，用户 A 按如下方式生成密钥对：

1) 随机生成整数 a，使得 $0<a<p-1$。

2) 计算 $y_A=g^a \bmod p$。

3) A 的私钥为 a，公钥为 $\{p,g,y_A\}$。

用户 B 通过用户 A 的公钥按如下方式计算密钥：

1) 选择任意整数 b，使得 $1\le b\le p-1$。

2) 计算密钥 $y_B=(y_A)^b \bmod p$。

3. 系统结构与区块链技术

3.1. 系统结构

本文基于区块链的双因子跨域认证方案由多个域联接组成，每个域都独立存在，实现域内用户的注册。用户 U_i 与模糊提取器 *FE* 相连接，通过区块链共识机制选择域内计算能力较强的，配置较高的边缘设备(认证服务器) *ES*，物联网终端区块链中存储由证书中心 *CA* 颁发的数字证书的哈希值，方便之后和用户端存储的哈希值进行对比，从而完成用户身份验证，其中，*ES* 和 *CA* 都是选自区块链中的节点。

3.2. 区块链技术[12]

在区块链中，每个区块由区块高度和区块哈希组成的区块标识进行识别，包含区块头和区块体：前一区块包含后一区块的哈希值，当前时间和随机数；区块体中记录某一时间段的交易信息。因此，区块与区块之间形成链式结构，在其上可以进行数据的计算和存储。

本文采用基于联盟链的 *DPOS* (股权授权证明)共识机制，其原理是让所有股民(代表所有节点)进行投票，由此产生代表，即超级节点，这些代表轮流生成区块负责记账，除代表外的其余节点同步账本实现区块链内的共识。

4. 基于口令和生物特征的跨域认证密钥协商协议

本文设计的跨域协议主要包括用户注册(见图 1)、认证协商(见图 2)两个阶段，在边缘认证服务器上

完成注册，在边缘设备处比对用户的随机密钥，以及数字证书的哈希值，完成用户身份的双重验证，最后协商密钥。本文中主要符号的意义如表 1 所示。

Table 1. Description of symbols
表 1. 符号说明

符号	意义
D_i	第 i 个域
U_i	第 i 个域的用户
FE	模糊提取器
ES_i	第 i 个域的边缘设备
CA	证书颁发中心
ID_i	第 i 个域的用户身份
PW_i	口令
B_i	生物特征
R_i	用户的生物特征随机密钥
S_{U_i}, P_{U_i}	用户的公私钥
P_{ES}, S_{ES}	边缘设备的公私钥
$E_{P_{ES}}, D_{S_{ES}}$	公钥加解密
$Sig_{S_{ES}}, V_{P_{ES}}$	数字签名验证
$H(\ )$	哈希函数
r_i	随机数

4.1. 注册阶段

1) D_i 域中用户 U_i 在其端口输入 ID_i， PW_i，通过模糊提取器 FE 采集生物特征 B_i。

2) FE 利用生成算法 $Gen(B_i)$，获得一随机密钥 R_i 和辅助字符串 P_i，将口令 PW_i 作哈希运算，并删除 PW_i， B_i。通过安全信道向 ES_i 发送注册请求 $Reg_i = \left(ID_i, E_{P_{ES_i}}(R_i), W_i, P_i\right)$。

3) ES_i 端用私钥解密 $E_{P_{ES_i}}(R_i)$，判断 ID_i 是否已注册，若已注册，则终止；否则，保存 P_i， W_i， R_i。对 Reg_i 和 ID_{ES} 进行签名，向 CA 端发送 $RCert_i = \left(ID_i, R_i, Sig_{S_{ES_i}}(Reg_i, ID_{ES}), r_1\right)$ 申请证书。

4) CA 端用 ES_i 的公钥验证签名 $Sig_{S_{ES_i}}(Reg_i, ID_{ES})$，将生成的数字证书 $Cert_i = (ID_i, R_i, T)$ 发送至区块链，并保存其哈希值 H_i。

5) CA 端向 ES_i 端发送数字证书交易 $tx = (R_i, RCert_i, r_2)$。

6) CA 端将证书哈希值 H_i 发送给 U_i 并保存。

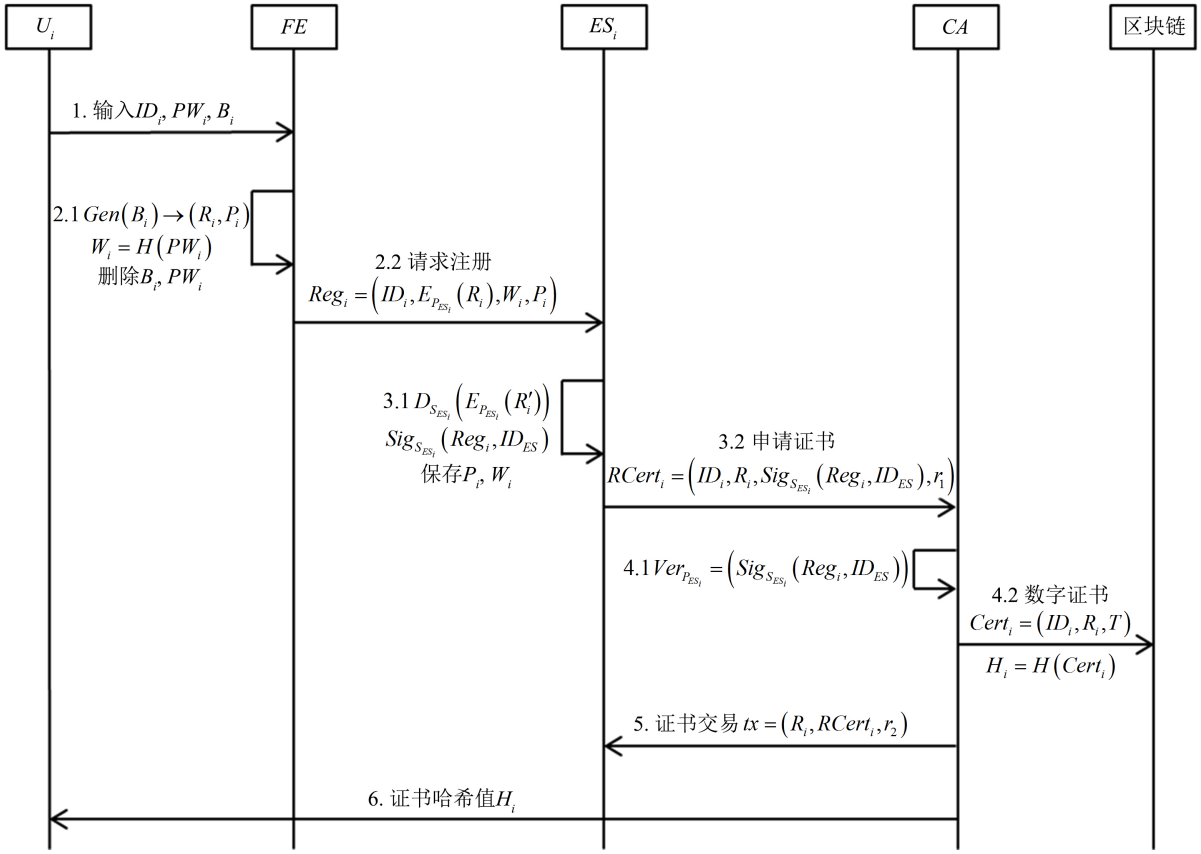

Figure 1. Registration phase
图 1. 注册阶段

4.2. 认证协商阶段

D_i 域中用户 U_i 与 D_j 域中用户 U_j 需要取得联系，首先在 ES_i 端验证 U_i 的身份， ES_j 端对 ES_i 端进行认证，通过后 U_i 和 U_j 可以保持通信。

1) U_i 端口输入 ID_i， PW_i'， H_i'， FE 采集生物特征 B_i'。

2) FE 端计算 PW_i' 的哈希值 W_i'，请求访问 ES_i 并发送 $Req_i = E_{P_{ES_i}}(ID_i, H_i', W_i', r_3)$。

3) ES_i 端用私钥解密 Req_i，并验证 W_i' 与 W_i 是否相等，若不相等，则终止认证；否则将 P_i 返回给 FE。

4) FE 端采用恢复算法 $Rev(B_i', P_i)$ 获得用户生物特征的随机密钥 R_i'，对其加密为 $E_{P_{ES_i}}(R_i')$ 发送给 ES_i。

5) ES_i 端用其私钥解密收到的信息，判断 $R_i' \stackrel{?}{=} R_i$ 是否成立，若成立，则向 ES_j 发送认证请求 $AReq_i = (ID_i, R_i, H_i', r_4)$。

6) ES_j 端首先验证随机数 r_4 的有效性，接着发送 $HReq_i = (ID_i, R_i, r_5)$，请求 U_i 注册时在区块链保存的证书的哈希值。

7) 区块链接收到请求信息后，将哈希值 H_i 返回给 ES_j。

8) ES_j 端判断 $H_i' \stackrel{?}{=} H_i$ 是否成立，若成立，则返回 U_i 表明认证成功；若不成立，则返回认证失败。

9) U_i 用私钥对 g^a 进行签名，其中， a 是随机数，发送至 U_j。

10) U_j 用 U_i 的公钥验证 $Sig_{S_{U_i}}(g^a)$，选随机数 b 作签名 $Sig_{S_{U_j}}(g^b)$，并计算会话密钥 $KS_j = (g^a)^b$。发送给 U_i， U_i 用 U_j 的公钥验证签名并计算 $(g^b)^a \stackrel{?}{=} KS_j$ 是否成立，若成立，则会话密钥为 $(g^b)^a$。

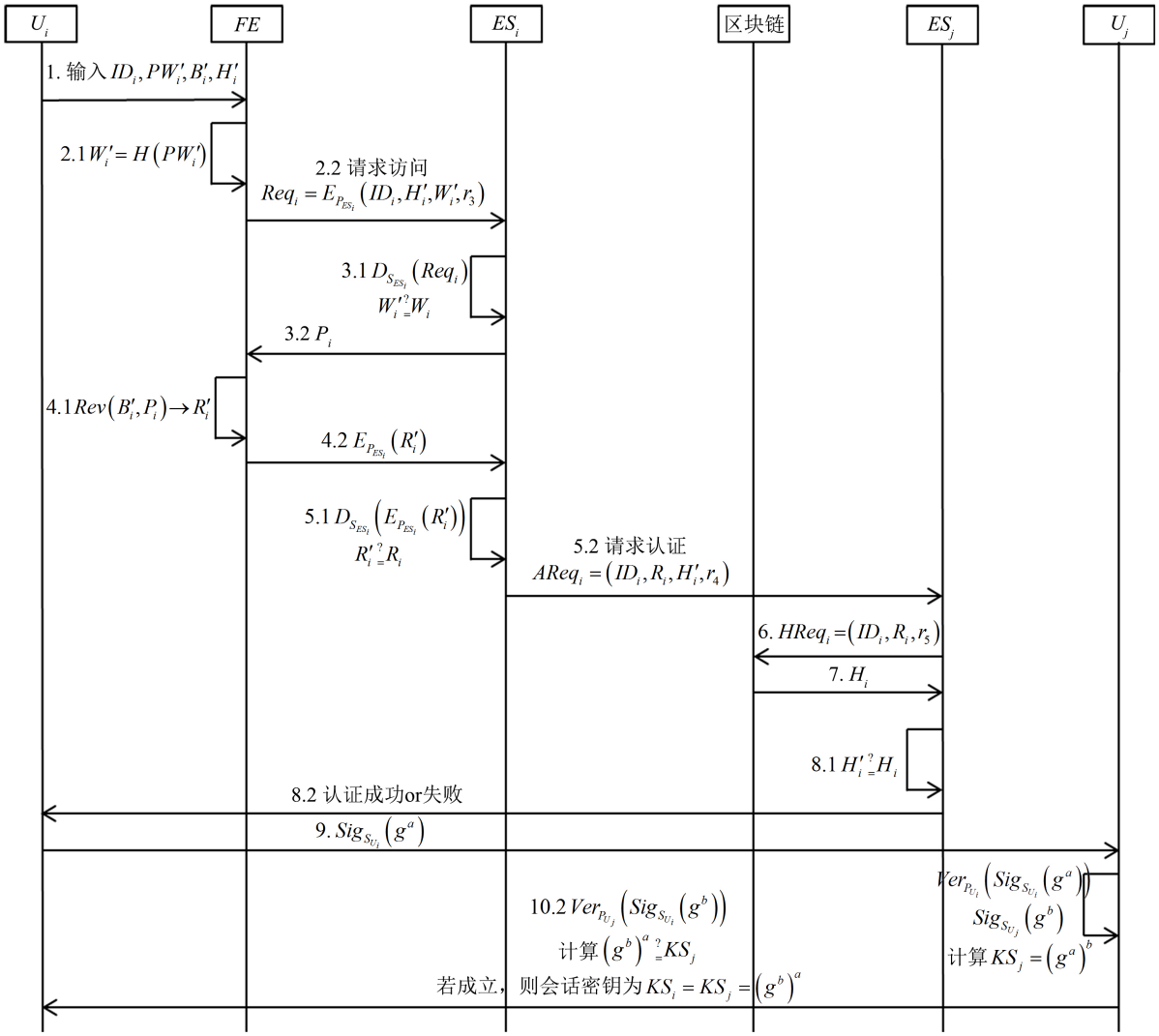

Figure 2. Certification negotiation stage
图 2. 认证协商阶段

5. 安全性分析

5.1. 认证安全性

注册阶段和认证协商阶段，模糊提取器采用生成和恢复算法，获得随机字符串作为生物特征因子参与生物识别。将数字证书的哈希值存储在区块链节点上，避免了丢失和被篡改。用户 U_i 需要在 ES_i 和 ES_j 端完成双重验证，消息由公钥加密后传输，私钥是未知的，因此该认证是安全的。

5.2. 会话密钥安全性

密钥协商是基于 DH 算法，采用 Canetti 和 Krawczyk 提出的签名认证器[13]，将原来的 g^a，g^b 进行签名，发送给对方，转换为对签名的验证，因此该密钥协商过程是安全的。

5.3. 抗重放攻击

认证协商阶段，用户请求访问边缘认证服务器时发送 $Req_i = E_{P_{ES_i}}(ID_i, H_i', W_i', r_3)$，其中 r_3 是随机数。

还有请求认证 $AReq_i=(ID_i,R_i,H_i',r_4)$ 时也会加入随机数，当区块链接收请求消息 $HReq_i=(ID_i,R_i,r_5)$ 时，其上的节点会验证随机数的有效性。因此即使攻击者截取了消息，在验证随机数时效性时也会失败。

5.4. 抗口令猜测攻击

用户端输入口令后，在模糊提取器端计算口令的哈希值，随即删除口令，使其无法被非法用户窃取。又哈希函数具有单向性，攻击者无法恢复真实的口令，之后在信道上传输也具有安全性。

5.5. 前向安全性

用户在协商密钥过程中，用 ElGamal 加密算法计算各自的公私钥，其中 a，b 是随机数，在每次加密时计算得 g^a 和 g^b 也是随机的。另外，该加密算法是基于离散对数困难问题的，攻击者很难得到会话密钥，即使攻击者破解了前一次会话密钥后，仍然无法知道下一次会话时用户双方产生的密钥。

6. 性能分析

本文选取已有的跨域认证方案进行比较，只讨论认证协商阶段的计算效率(见表 2)。由于 Hash 函数运算的单次计算时间很小，可以忽略其运算量。下面比较不同协议中数字签名与验证(Sig/Ver)、公钥加解密(E_p/D_s)、双线性对(E_e)与指数运算(E_{Dex})。

Table 2. Comparison of computational efficiency
表 2. 计算效率对比

协议	运算量	运行时间/ms
方案 1 [14]	$2(Sig/Ver)+1(E_p/D_s)+4E_e$	73.553
本文方案	$2(Sig/Ver)+2(E_p/D_s)+4E_{Dex}$	62.28

实验环境为：英特尔酷睿 i5-7300HQ，2.5 GHz 主频，8 GB 内存，Win10，64 位，Python3.9。其中，执行一次签名与验证的时间为 4.363 ms，执行一次加解密的时间为 5.851 ms，执行一次双线性对的时间为 14.744 ms，执行一次指数运算的时间为 10.463 ms。

通过对比可知，本文方案的运算量是 $2(Sig/Ver)+2(E_p/D_s)+4E_{Dex}$，与方案 1 相比，本文方案多一次公钥加解密，但无双线性对运算。本文是基于口令和生物特征设计的协议，用户不需要携带智能卡，避免了智能卡的丢失。

7. 结束语

本文基于区块链技术，在边缘计算环境下，设计了一种双因子的跨域认证密钥协商协议，通过边缘设备对用户进行认证，方便了用户且提高了认证效率，减轻了云端认证的压力。在保证安全性的基础上，利用口令、生物特征完成对用户的身份认证。分析表明，本文提出的跨域认证方案具有较好的计算性能和较高的安全性。

参考文献

[1] 周俊, 沈华杰, 林中允, 等. 边缘计算隐私保护研究进展[J]. 计算机研究与发展, 2020, 57(10): 2027-2051.

[2] Satyanarayanan, M. (2017) The Emergence of Edge Computing. *Computer*, **50**, 30-39. https://doi.org/10.1109/MC.2017.9

[3] 丁永善, 李立新, 李作辉. 基于证书的匿名跨域认证方案[J]. 网络与信息安全学报, 2018, 4(5): 32-38.

[4] 吴卫. 边缘计算环境下物联网身份认证与隐私保护技术研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2019.

[5] 马晓婷. 基于区块链技术的证书管理与跨域认证方案[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2019.

[6] Yao, Y., Chang, X., Misc, J., *et al*. (2019) BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services. *IEEE Internet of Things Journal*, **6**, 3775-3784. https://doi.org/10.1109/JIOT.2019.2892009

[7] Guo, S., Hu, X., Guo, S., *et al*. (2019) Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. *IEEE Transactions on Industrial Informatics*, **16**, 1972-1983.

[8] 张金花, 李晓伟, 曾新, 等. 边缘计算环境下基于区块链的跨域认证与密钥协商协议[J]. 信息安全学报, 2021, 6(1): 54-61.

[9] 帕尔, 佩尔茨尔. 深入浅出密码学－常用加密技术原理与应用[M]. 马小婷, 译. 北京: 清华大学出版社, 2012: 204-205.

[10] Dodis, Y., Reyzin, L., Smith, A., *et al*. (2004) Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *Theory and Application of Cryptographic Techniques*, **2004**, 523-540. https://doi.org/10.1007/978-3-540-24676-3_31

[11] 威廉·斯托林斯. 密码编码学与网络安全: 原理与实践[M]. 第八版. 陈晶, 等, 译. 北京: 北京工业出版社, 2021: 204-206.

[12] 邓上煜, 魏周思宇, 吴鹏程. 关于区块链技术的研究与分析[J]. 科技风, 2019, 382(14): 90.

[13] Canetti, R. and Krawczyk, H. (2001) Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Berlin, 453-474. https://doi.org/10.1007/3-540-44987-6_28

[14] 谭琛, 陈美娟, Amuah, 等. 基于区块链的分布式物联网设备身份认证机制研究[J]. 物联网学报, 2020, 4(2): 71-78.