

基于 SM2 算法和区块链的移动端身份认证协议设计

吴邱涵, 胡卫

(海军工程大学信息安全系, 湖北 武汉 430033)

摘要: 针对目前二代居民身份证在进行身份认证过程中存在的隐私泄露问题, 采用 SM2 算法和区块链技术, 结合动态口令、面部识别、二维码等技术优势, 对传统的身份认证方式进行改进, 设计了一种适合移动终端设备的身份认证协议, 并进行了协议的效率和安全性分析。分析表明, 该协议在实现高效的用户身份认证的同时, 确保了用户的身份隐私安全。

关键词: SM2 算法; 区块链; 身份认证; 移动端

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018046

Design of identity authentication agreement in mobile terminal based on SM2 algorithm and blockchain

WU Qiuhuan, HU Wei

Department of Information Security, Naval University of Engineering, Wuhan 430033, China

Abstract: To solve the privacy leakage problem in the process of identification by second generation residents' ID card, the SM2 algorithm and the blockchain technology were adopted, and the dynamic password, facial recognition and two-dimension code to modify the traditional identification method were combined to design a kind of identification agreement on mobile terminal. The study analyzed the efficiency and security of the agreement, which reflected that the agreement could guarantee users' privacy when it provide high-efficient identification.

Key words: SM2 algorithm, blockchain, identity authentication, mobile terminal

1 引言

目前, SM2 算法的可证安全性已经达到了公钥密码算法的最高安全级别, 其实现效率相当于或略优于一些国际标准的同类椭圆曲线密码算法^[1]。因此, 许多国内学者基于 SM2 算法设计了身份认证协议。其中, 任子荣^[2]采用 SM2 算法设计实现了基于 PKI 技术的第三方身份认证服务系统, 谷国进^[3]提出了基于 SM2 数字证书的认证授权模型, 使用

SM2 证书来实现客户端的身份认证, 王杰^[4]基于 SM2 算法设计了证书状态查询系统。王佳强等^[5]采用 SM2 算法设计了一个适用于移动设备的双方身份认证与密钥共识协议 (AKA)。李子臣等^[6]提出基于 SM2 算法与零知识的射频识别双向认证协议。但是, 上述协议均采用中心化的认证方式, 存在潜在的单点失败和多 CA 信任难问题^[7]。

区块链是一种分布式数据库, 通过去中心化、去信任的方式, 集体维护一个可靠数据库。由于

收稿日期: 2018-04-10; 修回日期: 2018-05-25

通信作者: 胡卫, huwei-1212@126.com

基金项目: 海军工程大学自主立项基金资助项目 (No.20161607)

Foundation Item: Naval University of Engineering Independent Project (No.20161607)

其去中心化的特性，区块链技术得到了广泛的应用。其中，闵旭蓉等^[8]基于区块链技术设计了电子证照共享平台，黄永刚^[9]提出了基于区块链的电子健康档案，Wang 等^[10]将区块链技术引入建筑工程管理领域中。

当前，二代居民身份证读取设备容易被不法分子利用，基于中心的认证服务大量存储用户实名信息，具有隐私泄露的风险，因此有必要设计一款安全的电子身份证来保护公民隐私。截至2017年8月，我国网民已达7.51亿，其中，使用手机上网的网民占比达96.3%，智能手机已然成为现代生活密不可分的一部分^[11]。综合考虑上述技术的优势，本文基于SM2和区块链设计了一种适用于移动端的身份认证协议。

2 预备知识

2.1 SM2/SM3 算法

国家商用密码局在ECC算法的基础上，自主设计了SM2椭圆曲线公钥密码算法。SM2算法的安全性源于求解离散对数问题的困难强度，相比RSA算法，其密钥的长度更短一些^[12]，具有安全性高、存储空间小、签名速度快的优点。同时，相对于国际标准ECC算法，SM2算法在解密正确性判断、明文编码问题、对待加密数据长度的限制及加密计算效率上更好^[2]。因此在移动应用中，SM2算法能有效降低运算、存储和通信的损耗，比RSA、国际标准ECC算法更具有优势。

SM3算法是密码杂凑算法，其压缩函数的整体结构与SHA-256算法相似，但能够有效地避免高概率的局部碰撞，抵抗强碰撞性的差分分析、碰撞性

的线性分析和比特追踪法等密码分析^[13]。

本文采用SM2作为公钥密码算法产生公私钥来对用户身份信息进行加密保护，采用SM3算法作为生成区块地址及散列计算的散列算法。

2.2 区块链

区块链是依托P2P网络，由多个独立节点参与的分布式数据库系统，可理解为分布式账簿^[14]。区块链是比特币的底层技术，由Nakamoto于2008年提出，具有去中心、可追溯、难篡改、难伪造的特点^[12,15]。

如图1所示，区块链分为区块头和区块体。区块头包含版本号、上一区块的散列值、Merkle根节点散列值、时间戳、难度值、随机数和交易记录。任意交易记录被篡改，按照散列加密算法的特性，二叉树结构的Merkle树的根节点都会发生很大变动，因此其他节点在验证区块链的散列值时，就能够很明显地发现问题。

区块链可分为公有链、私有链和联盟链。区块链可选择不同的加密方法，如RSA加密算法、我国的国密算法、Ed25519算法等签名算法^[9]。本文在设计移动端身份认证协议时，将认证数据写入身份认证区块链，借助私有链形式的区块链实现对用户身份的验证。

3 身份认证协议

3.1 注册阶段

用户A在移动客户端上注册时，采取手机动态口令验证手机号码真实性。完成手机号码验证后，用户填写基本身份信息 ID_i （包含姓名、性别、民族、地址等），通过摄像头进行动态面部识

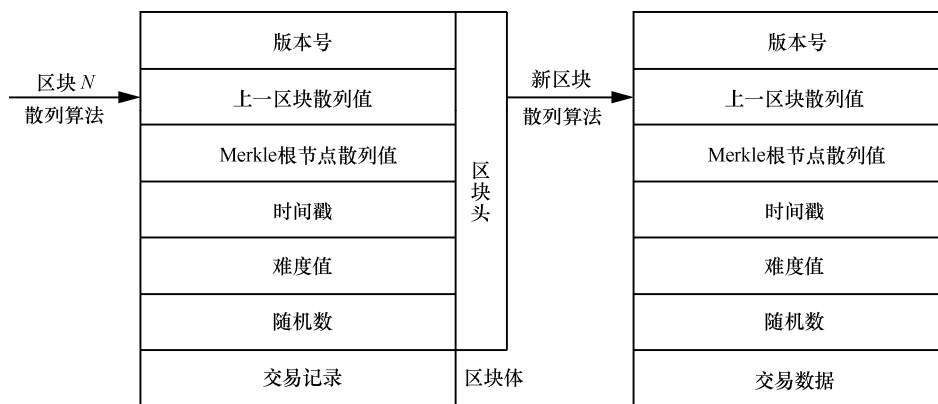


图1 区块链的数据结构

别, 获取面部特征值 ID_{f_0} , 并设置用户名 ID_a 和登录口令 P_a 。系统后台利用 SM3 算法对文本信息和图片信息进行散列运算后, 将 $H(ID_i \| ID_{f_0})$ 传输至公安认证服务系统, 然后, 公安认证服务系统在国家人口库中进行身份信息核对, 核对通过后, 用户完成系统注册。注册阶段如图 2 所示。

3.2 生成身份认证区块阶段

用户 A 注册成功后, 公安认证服务系统签发用户 eID 。移动客户端通过 SM2 算法产生私钥 d_A 和公钥 $P_A = [d_A]G = (x_A, y_A)$, 将 d_A 加密存储于本地。通过 SM3 算法对用户 eID 、身份信息、面部特征值等进行散列运算得到身份散列值 $H_{ID} = H(eID \| ID_i \| ID_{f_0})$ 。利用 SM2 签名算法对 H_{ID} 和注册时间戳 T_r 进行签名, 置 $M_0 = \{H_{ID}, T_r\}$, 之后得到注册身份签名值 $SIG_r = (r, s)$ 。将消息

$M = \{P_A, M_0, SIG_r\}$ 发送至公安认证服务系统。

公安认证服务系统计算用户的 H_{ID} , 通过 P_A 计算验证 SIG_r 。若验证通过, 则用 SM3、RIPEMD160、BASE5 等算法对 P_A 进行计算^[15], 获得区块地址 Add , 作为该用户的身份认证区块标识, 在该区块体中记录用户的 H_{ID} 、 T_r 和 SIG_r 。公安认证服务系统内部计算资源通过共识机制完成区块的生成。区块生成流程如图 3 所示。

3.3 登录阶段

用户通过系统用户名 ID_a 、登录口令 P_a 和摄像头面部识别上传面部特征值 ID_{f_n} 来登录系统, 以确认是用户本人登录系统。

3.4 生成电子身份证阶段和身份认证阶段

登录后, 移动客户端使用 d_A 对 H_{ID} 与时间戳 T_{C_n} 进行实时签名, 置 $M_n = \{H_{ID}, T_{C_n}\}$, 产生态

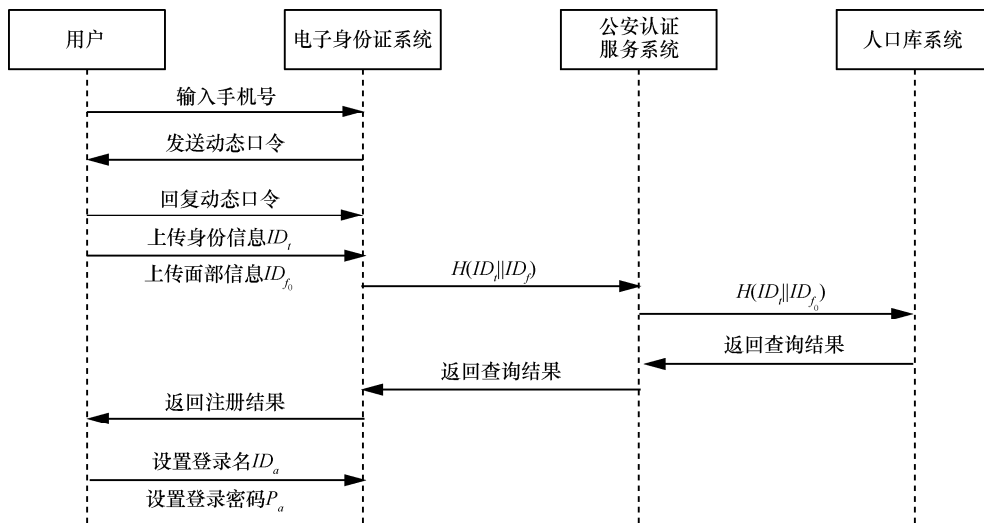


图2 注册阶段

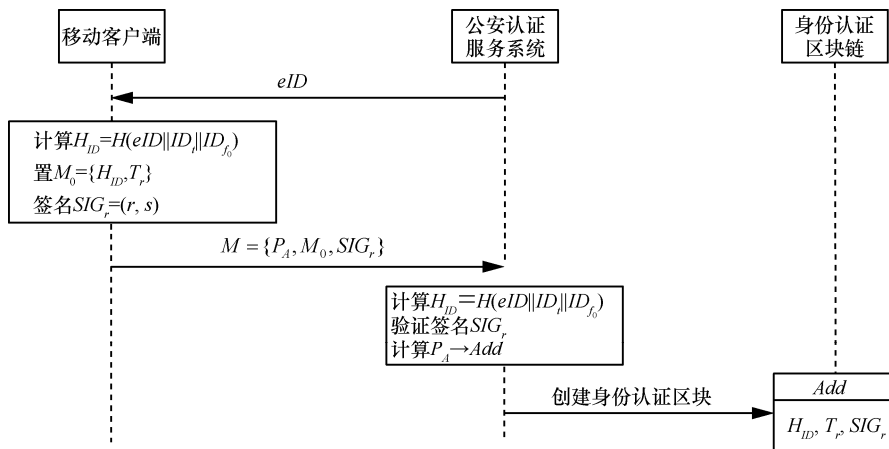


图3 生成身份认证区块阶段

身份签名值 $SIG_{d_n} = (r_n, s_n)$ 。系统根据 P_A 、 H_{ID} 、 T_{C_n} 和 SIG_{d_n} ，产生动态身份二维码 QR_n ，即电子身份证。该二维码的刷新时间设置为 1 min。过程如图 4(a)所示。

认证服务应用系统读取用户的动态身份二维码 QR_n ，获取消息 $M_n = \{P_A, H_{ID}, T_{C_n}, SIG_{d_n}\}$ 。首先，通过 T_{C_n} 判断 QR_n 的时效性，使用 P_A 计算验证动态身份签名值 SIG_{d_n} 。签名验证通过后，通过 P_A 计算区块地址 Add ，访问身份认证区块，对比二维码和身份认证区块中的 H_{ID} 是否一致，计算验证 SIG_r 。通过上述步骤可确定用户身份是否合法。过程如图 4(b)所示。

4 系统性能分析

4.1 效率分析

1) SM2/SM3 算法

本文采用 SM2 作为公钥密码算法产生公私钥来对用户身份信息进行加密保护，采用 SM3 算法作为生成区块地址及散列计算的散列算法。SM2 算法的安全强度高于 RSA-2048，大致与 RSA-3072 相当。但是如果在芯片中运行 RSA-3072，运算将相当耗时，相比之下，SM2

算法所需的运算负载更小，运算速度更快。SM3 算法在不显著增加硬件开销的情况下，采用 P 置换，加速了算法的雪崩效应，提高了运算效率，具有跨平台实现的高效性和广泛的适用性。

2) 面部识别

目前，基于卷积神经网络的人脸识别算法，识别率可达到 99% 以上，识别单张人脸的时间小于 0.05 s，并且对光照差异、面部表情变化、有无遮挡物等干扰具有顽健性。可采取卷积神经网络进行面部识别，提高注册登录效率。

3) 建立及访问身份认证区块链

本文采用私有链的形式构建用户的身份认证区块链，由公安系统负责维护和管理，既确保数据的权威与安全，也提高了建立区块的效率。

4.2 安全性分析

本节从以下 6 个方面对本协议的安全性进行分析。

1) 去中心化密态存储：传统认证系统为集权管理，而区块链上没有集权节点，所有节点都参与系统运行和维护，每个节点都包含同样的信息记录。采用区块链对用户身份信息进行去中心化的密态存储，可有效防止传统认证方式中存在的单点失败和多 CA 信任难的问题。

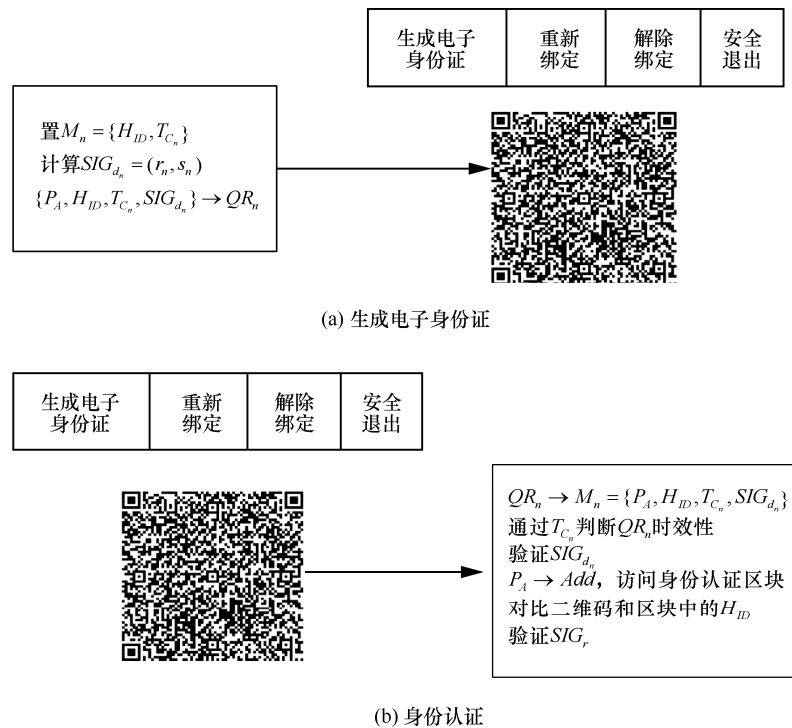


图4 电子身份证生成与身份认证阶段

2) 多因素认证: 本协议采取动态口令、面部识别和身份二维码的多因素认证方式, 引入了生物特征认证因素和动态口令机制, 相比传统的智能卡与口令的双因素认证方式更加安全。即使攻击者通过监听获得用户的相关信息, 也无法通过实时的面部识别验证, 因此无法冒充用户进行认证。

3) 防伪造: 假设攻击者掌握用户的身份散列值, 置消息 $M_n = \{H_{ID}, T_{C_n}\}$, 但其不具备用户私钥, 无法对消息进行签名, 因此无法伪造用户的动态身份签名值 $SIG_{d_n} = (r_n, s_n)$, 进而无法伪造该用户的身份二维码。

4) 抗重放攻击: 每个区块的区块头包含的时间戳和随机数可以有效防止创建区块过程中的重放攻击。在认证过程中, 每次传送的消息和二维码中都加入了时间戳, 且二维码每分钟刷新一次。如果攻击者将消息重放, 收方可通过时间戳判断该消息为重放消息, 拒绝其认证请求。

5) 防止攻击者离线破解身份信息: 用户私钥加密存储在本地客户端, 即使攻击者获得用户公钥, 推算出身份认证区块地址, 查询得到的身份信息仍是密文状态, 无法破解用户身份信息。

6) 有效保护用户隐私: 采用动态二维码和区块链的认证方式, 用户的身份信息不会在网上直接传送。密态的身份二维码不会泄露个人隐私, 相比实体身份证具有更强的隐私保护功能。根据最小信息暴露原则, 认证服务应用系统通过区块链验证成功后返回的是验证结果而非用户身份信息, 更有效地保护了用户隐私。

5 结束语

本文所设计协议广泛结合了动态口令、面部识别、二维码等技术的优势, 采用 SM2 算法和区块链技术设计了一款移动端的二维码电子身份证。经过分析, 本文提出的电子身份认证协议采取去中心化的密态存储方式和多因素的认证方式, 可有效抗重放攻击, 防止攻击者离线破解用户身份信息, 做到对用户隐私信息的有效保护。但目前区块链在我国的具体应用较少, 而一旦区块链应用得到推广, 节点数量将呈几何级数增加, 其频繁的关系数据查询请求及数据安全的保证将对现有的数据架构提出非常严峻的挑战^[16-17]。

参考文献:

- [1] 汪朝晖, 张振峰. SM2 椭圆曲线公钥密码算法综述[J]. 信息安全研究, 2016, 2(11): 972-982.
WANG Z H, ZHANG Z F. Overview of public key cryptography algorithm for SM2 elliptic curve[J]. Information Security Research, 2016, 2(11): 972-982.
- [2] 任子荣. 基于移动终端和 PKI 技术的第三方身份认证服务系统[D]. 上海: 上海交通大学, 2014.
REN Z R. Third party identity authentication service system based on mobile terminals and PKI technology[D]. Shanghai: Shanghai Jiaotong University, 2014.
- [3] 谷国进. 基于 SM2 算法的认证授权系统研究与实现[D]. 济南: 山东大学, 2013.
GU G J. Research and implementation of authentication authorization system based on SM2 algorithm[D]. Jinan: Shandong University, 2013.
- [4] 王杰. 基于商密 SM2 算法的证书状态查询机制设计与实现[D]. 西安: 西安电子科技大学, 2015.
WANG J. Design and implementation of certificate state query mechanism based on SM2 algorithm[D]. Xi'an University of Electronic Science and Technology, 2015.
- [5] 王佳强, 亢保元, 邵栋阳. 一个新的适用于移动设备的双方身份认证与密钥共识协议[J]. 软件, 2017, 38(10): 73-76.
WANG J Q, KANG B Y, SHAO D Y. A new protocol for mutual authentication and key agreement for mobile devices[J]. Software, 2017, 38(10): 73-76.
- [6] 李子臣, 刘博雅, 王培东, 等. 基于 SM2 与零知识的射频识别双向认证协议[J]. 计算机工程, 2017, 43(6): 97-100.
LI Z C, LIU B Y, WANG P D, et al. Two-way RFID certification protocol based on SM2 and zero knowledge[J]. Computer Engineering, 2017, 43(6): 97-100.
- [7] YAN J Z, PENG J, ZUO M, et al. PKI digital certificate system based on blockchain[J]. Telecommunications Engineering Technology and Standardization, 2017(11): 16-20.
- [8] 闵旭蓉, 杜葵, 戴逸聪. 基于区块链技术的电子证照共享平台设计[J]. 指挥信息系统与技术, 2017, 8(2): 47-51.
MIN X R, DU K, DAI Y C. Design of electronic license sharing platform based on block chain technology[J]. Command Information System and Technology, 2017, 8(2): 47-51.
- [9] 黄永刚. 基于区块链技术的电子健康档案安全建设[J]. 中华医学图书情报杂志, 2016, 25(10): 38-40.
HUANG Y G. Security construction of electronic health records based on block chain technology[J]. Chinese Medical Book Intelligence Journal, 2016, 25(10): 38-40.
- [10] WANG J, PENG W U, WANG X, et al. The outlook of blockchain technology for construction engineering management[J]. Frontiers of Engineering Management, 2017, 4(1).
- [11] China Internet Network Information Center. The 40th statistical report on the development of China's Internet network[R]. 2017.
- [12] 宁晓斐. 区块链技术及其应用[J]. 信息与电脑(理论版), 2018(17): 115-116.

- NING X F. Blockchain technology and application[J]. China Computer and Communication, 2018(17): 115-116.
- [13] 王小云, 于红波. SM3 密码杂凑算法[J]. 信息安全研究, 2016, 2(11): 983-994.
- WANG X Y, YU H B. SM3 cipher hash algorithm[J]. Research on Information Security, 2016, 2(11): 983-994.
- [14] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.
- CAI W D, YU L, WANG R, et al. Research on application system development methods based on block chain[J]. Software Journal, 2017, 28(6): 1474-1487.
- [15] 黄征, 李祥学, 来学嘉, 等. 区块链技术及其应用[J]. 信息安全研究, 2017, 3(3): 237-245.
- HUANG Z, LI X X, LAI X J, et al. Blockchain technology and application[J]. Research on Information Security, 2017, 3(3): 237-245.
- [16] 卿苏德, 姜莹, 王秋野. 区块链的技术原理和意义[J]. 电信网技术, 2016(12): 14-20.
- QING S D, JIANG Y, WANG Q Y. Technical principle and significance of block chain[J]. Telecommunication Network Technology, 2016(12): 14-20.
- [17] LUO X L. Application exploration of block chain technology in logistics field[J]. China Business Theory, 2017(24): 7-8.

[作者简介]



吴邱涵（1995-），女，湖北武汉人，海军工程大学硕士生，主要研究方向为密码学与信息安全、身份认证、区块链。



胡卫（1979-），男，湖北宜城人，博士，海军工程大学副教授，主要研究方向为密码学、隐私保护。