引用格式: 史爱武, 韩超, 付科巽, 等. 基于区块链和 IPFS 远程医疗的安全方法研究[J]. 微电子学与计算机, 2024, 41(6): 73-82.

SHI A W, HAN C, FU K X, et al. Research on security methods of blockchain and IPFS telemedicine[J]. Microelectronics & Computer, 2024, 41(6): 73-82.

DOI: 10.19304/J.ISSN1000-7180.2023.0326

基于区块链和 IPFS 远程医疗的安全方法研究

史爱武, 韩　超, 付科巽, 盛　鐘

(武汉纺织大学 计算机与人工智能学院, 湖北 武汉 430200)

摘　要: COVID-19 的大规模感染给人民生活造成了不便, 比如就医难、医疗学术交流共享不便、医疗资源不平衡, 从而衍生远程医疗。目前远程医疗数据仍然以集中式存储、互联网协议(Internet Protocol, IP)传输和签证机构(Certificate Authority, CA)颁发的证书为主, 导致数据安全性低、网络通讯延迟和 CA 维护成本高。本文提出一种 SMSSS-CA 签名机制、智能合约和私有区块链解决 CA 维护成本高、医疗数据隐私泄露和安全性低的问题。此外, 还提出命名数据网络(Named Data Network, NDN)集成星际文件系统(InterPlanetary File System, IPFS)、联盟区块链和智能合约, 用来提高远程会诊时 SMSSS-CA 签名或验签时获取患者病例和共享会诊信息的响应速度和降低区块链传播开销。实验分别从 NS3 和 NDNSIM 两种实验环境对比, 结果表明, 该方法比现有方案更安全和共享更及时。

关键词: 区块链; 签名; 命名数据网络; 智能合约; 远程医疗; 星际文件系统

中图分类号: TP309.7　　**文献标识码**: A　　**文章编号**: 1000-7180(2024)06-0073-10

Research on security methods of blockchain and IPFS telemedicine

SHI Aiwu, HAN Chao, FU Kexun, SHENG Bei

(School of Computer Science and Artificial Intelligence, Wuhan Textile University, Wuhan 430200, China)

Abstract: The massive infection of COVID-19 has caused inconvenience to people's lives, such as the difficulty of seeking medical treatment, the inconvenience of medical academic exchanges and sharing, and the imbalance of medical resources, which has resulted in telemedicine. At present, telemedicine data is still mainly stored in centralized mode, transmitted over Internet Protocol (IP) and issued by Certificate Authority (CA),which leads to low data security, delayed network communication and high maintenance cost of CA. This paper proposes a SMSSS-CA mechanism signature, smart contract and private blockchain to solve the problems of high maintenance cost of CA and low privacy disclosure and security of medical data. In addition, the Named Data Network (NDN) is proposed to integrate InterPlanetary File System (IPFS), alliance blockchain and smart contracts to improve the response speed of obtaining patient records and sharing consultation information when the SMSSS-CA mechanism signs or verifies signatures during remote consultations, and reduce the blockchain propagation cost. Experiments were conducted to compare NS3 and NDNSIM experimental environments, and the results show that this method is safer and more timely than the existing schemes.

Key words: blockchain; signature; named data network; smart contract: telemedicine; interplanetary file system

1　引言

由于新冠肺炎疫情的爆发, 疫情防控给医疗卫生行业带来了巨大的冲击。在实践中发现, 不同的远程医疗系统采用的加密方式参差不齐, 数据存储方式有些采用本地数据库集中式存储[1], 有些则采

收稿日期: 2023-04-21; **修回日期**: 2023-06-02

基金项目: 国家自然科学基金面上基金(61170093); 湖北省教育厅科学技术研究计划重点基金(D20141603)

用云服务存储[2]。一旦网络节点被攻击，就会导致数据隐私被暴露，威胁到医患的数据安全和隐私。此外，远程医疗通常使用互联网协议(Internet Protocol, IP)，现有的传输控制协议(Transmission Control Protocol, TCP)方式只能提供一个通信管道[3-4]，医疗数据传输时容易造成数据传输响应慢或无法上网，导致远程医疗视频服务中出现通讯中断或者访问视频时出现卡顿。

为了解决远程医疗系统在提供透明、不可篡改、加密、通讯、数据安全和可信的服务方面存在的问题，Hasan 等[5]提出了使用区块链和星际文件系统(InterPlanetary File System, IPFS)存储医疗数据的方案，能够提供更加安全可信的服务。关志涛等[6]提出了在半诚实云存储上的属性加密方案，能够提高访问控制的灵活度和效率，但随着访问量的增大，通信开销显著增加。Nzanywayingoma 等[7]提出了一个基于 CP-ABE 的数据访问控制方案，能够实现恒定的密文大小和计算成本，但是对授权机构的可信度要求较高。Chen 等[8]提出用区块链代替签证机构(Certificate Authority, CA)，虽然能够降低成本，但是对于密钥管理方式存在较大的风险和采用里维斯特-沙密尔-阿德曼(Rivest-Shamir-Adleman, RSA)算法在解密/加密时产生更大的性能损耗和时间延迟。张利华等[9]提出了使用 CA 对数据进行身份认证的方案，能够提高加密的灵活性和方便性，但是维护证书链的成本较高。Khalid 等[10]提出了使用点对点(Peer-to-Peer, P2P)网络解决 IP 网络单通道缺点的方案，能够实现网络的负载均衡，但是存在转发网络文件不能有效重用的问题。

本文提出 SMSSS-CA 签名机制和命数据名网络(Named Data Network, NDN)架构方法解决远程医疗现有问题。通过 SMSSS-CA 签名机制和区块链结合解决传统的 CA 的高昂维护成本和跨平台服务信息更新延迟的问题。同时 NDN 命名网络结合区块链、IPFS 技术和智能合约控制 NDN 命名网络检索无效信息的策略，解决 IP 网络和 P2P 网络对 SMSSS-CA 数字签名和解签后存在远程医疗数据响应慢、转发率低和大数据存储安全的问题。

2 相关工作

2.1 区块链和智能合约

区块链技术能够建立一个分散的、安全的、不可篡改的、公开可访问的数据存储库，其结构如图 1 所示。系统中所有完整的客户端节点都是对等的，并保存一份相同的账本。该账本包含区块链系统中所有经过确认的交易，这些交易通常以 Merkle 树[11]的形式存储，并打包到每个区块中。智能合约是可跟踪且不可逆的脚本，表示可以自动执行的真实世界合约，减少了去中心化环境对中介的需求。通过以太坊虚拟机(Ethereum Virtual Machine, EVM)处理智能合约的字节码，区块链节点在其 EVM 中的智能合约字节码上处理这些请求，并将结果存储在区块链中。智能合约提供了处理任何应用程序的灵活性，执行所需的业务逻辑或操作，提供生成数据的不可变性、透明性以及执行的流程或事务的可审核性。

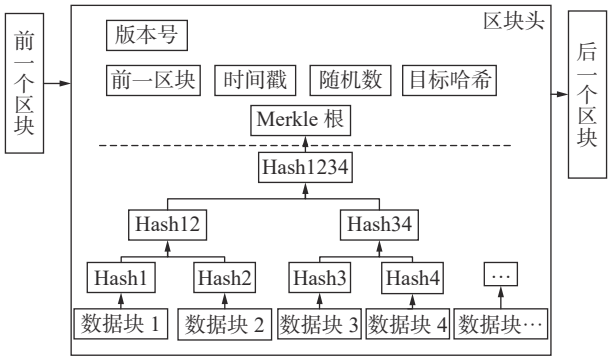

图 1 区块链结构

Fig. 1 Blockchain structure

2.2 命名数据网络(NDN)

NDN 命名数据网络的基本设计原理是构建在互联网基础之上，因此可以直接使用主要的 IP 服务，例如域名系统和区域间路由策略。NDN 允许路由器跟踪数据包的状态，并支持多路径转发[12]。它采用了以内容为中心的去中心化架构，数据传输过程中分为兴趣请求和数据包请求。在 NDN 中，每一个数据包都需要签密，因此，安全性被植入每一个数据包中[13]。如图 2 所示，当收到一个兴趣请求时，NDN 会在缓存表(Content Store, CS)中检查是否存在所请求的数据。如果数据存在，则直接返回数据；否则，它会检查待定兴趣表(Pending Interest Table, PIT)中是否存在相同的请求。如果存在，则返回最初的请求。如果在缓存表和待定兴趣表中都没有找到数据，则 NDN 会在转发表(Forwarding Information Base, FIB)中查找前缀。如果前缀存在，则将数据发送到与前缀匹配的路由器；否则，将返回数据不存在的错误信息。当数据到达时如图 3 所示，NDN 会按原路径将数据返回给请求者，以避免数据反复传输，从而提高了数据传输的效率。同时，由于数据包

和兴趣请求都需要进行签名验证，安全性得到提升。

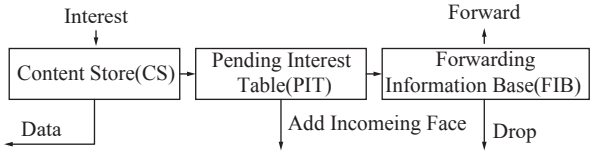

图 2　兴趣请求

Fig. 2 Interest request

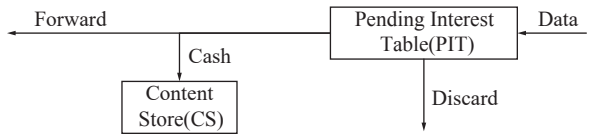

图 3　数据包请求

Fig. 3 Packet request

2.3　星际文件系统(IPFS)

IPFS 是一种全球性的点对点分布式文件系统，旨在优化当前的超文本传输协议并形成一个庞大的分布式系统。IPFS 通过将文件加密后进行碎片化处理，并将碎片分散存储在承担志愿的数据存储器，最终通过 IPFS 整合将文件拼凑成一个完整的文件。IPFS 的容错机制可以保证文件复制足够多的数据，同时在某一地区文件被完全摧毁时，也可以通过其他地方恢复数据。由于 IPFS 被加密且被分成若干个碎片，即使志愿存储器能够查看，也只能看到一小段加密后的密文。在安全性方面，IPFS 提供了更好的保护措施[14]。区块链上如果存储较大数据在广播过程中是非常慢的。IPFS 可以存储大容量数据，IPFS 存储完成后会返回唯一哈希值，区块链只需要存储哈希值即可，在传播过程中性能有很大的提升。

2.4　Shamir 门限算法

Shamir 门限算法将一个密钥通过多项式分散成 m 个影子秘密，并分发给多个参与方，其中只有不少于 t 个影子秘密时，才能恢复出原始密钥；否则，少于 t 个影子秘密时则无法恢复完整密钥[15]。

3　基于区块链和 IPFS 的远程医疗安全模型

3.1　系统业务模型

基于区块链与 IPFS 的远程医疗安全共享模型如图 4 所示，其中 a、b 和 c 代表 3 条操作路线，在图中表示输入时，“1a”代表注册认证，“2b”代表用户组上传操作，“3c”代表用户组访问操作。

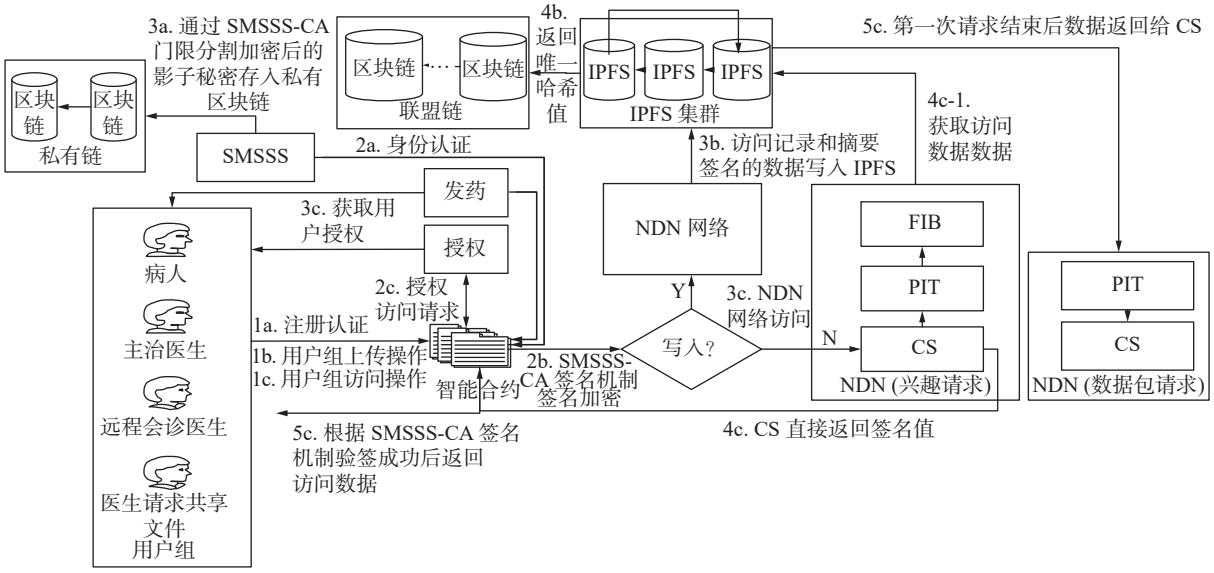

图 4　基于区块链与 IPFS 的远程医疗安全共享模型

Fig. 4 Telemedicine security sharing model based on blockchain and IPFS

该模型主要功能分为以下 5 个：

(1)SMSSS-CA：一组医生和患者通过 SMSSS-CA 生成影子秘密存入私有区块链，在上传时通过多于 t 个影子进行恢复完整私钥对摘要进行签名和下载时通过多于 t 个影子进行恢复完整公钥对密文进行验签获取摘要。

(2)智能合约：根据一套以数字形式的承诺，智能合约规定医患的权限，计算机自动执行注册，获取完整密钥，信息检索和访问控制等操作，防止恶意行为造成威胁。

(3)NDN 命名数据网络：在用户组之间进行视频和音频大文件数据传输时，数据会再次加密以提高安全性。此外，系统还支持路由器跟踪数据包状态和多路径转发等功能，这些特性可以缓存内容以

便未来的远程医疗会诊请求同一文件时能够快速响应。NDN 命名数据网络和 IPFS 集群节点相连，可以快速共享文件。

(4)IPFS：具有大容量存储和去除冗余数据，在远程医疗会诊存储的长达几小时视频大文件可以得到很好的保存。在本文设计模型中，构建了一个由 3 个节点组成的 IPFS 专用存储网络，以提高整个模型的传输效率。

(5)区块链：私有区块链主要是存储用户的密钥对，远程医疗数据会被存储至联盟链中，保证数据真实性，防止信息被篡改。

3.2 SMSSS-CA 签名机制

区块链是一个去中心化账本，用于以可验证和永久的方式记录所有的交易，每一笔交易中的数据都被防篡改。区块链类似于证书链如图 5 所示，但其主要区别在于区块链是一种分散的信任机制，而证书链则是由一系列受信任的第三方机构构成。本文区块链技术可以提供一种分散式的密钥管理方法。具体来说，区块链技术使用一种去中心化的方式来管理密钥。这意味着密钥不再存储在单个中心位置，而是分布在网络上的多个节点中。这些节点之间相互验证和同步，从而确保密钥的安全性和可靠性。

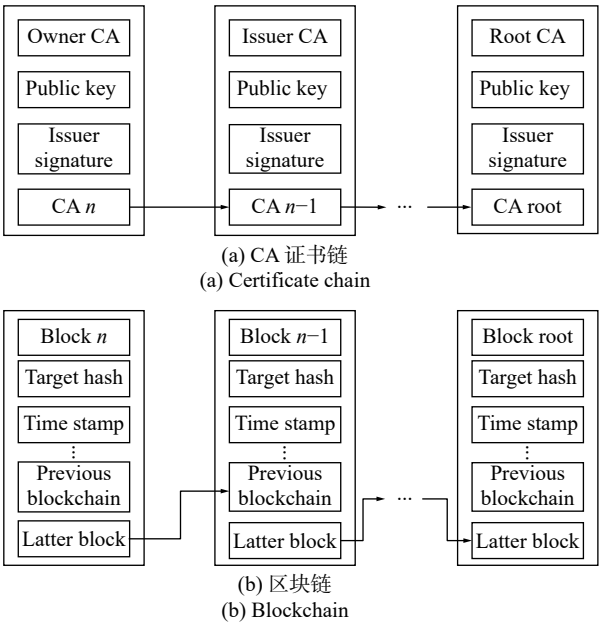

图 5 证书链和区块链对比图

Fig. 5 Comparison of certificate chain and blockchain

SMSSS-CA 原理,首先医生和患者在智能合约生成一组用户，通过采用 SM2 椭圆曲线公钥密码算法[16] 对一组用户生成密钥对，私钥 PK 和公钥 PW。在本文中为提高 Shamir 门限算法安全性，加入了指数型函数。在门限算法中，将 PK 或 PW 切分成 n 个影子秘密，并使用高级加密标准(Advanced Encryption Standard, AES)算法对影子秘密进行加密存入私有区块链中，同时颁发给不同的医患持有者，从而提高密钥管理的安全性和可靠性。最后只有超过 t 个 AES 算法解密后的影子秘密执行才能恢复完整 PK 或 PW 对医疗数据签名或验签。若一组用户中新增医生时，会对以往的影子秘密进行合并，并且对 t 进行加 1 操作。在整个阶段由智能合约对用户进行访问控制，限制用户操作和功能防止人为对数据造成安全问题。

通过 SMSSS-CA 无 CA 机制原理和智能合约的访问控制，避免了传统的 CA 和可信任第三方的高昂维护成本，并且保护 PK 和 PW 的安全性。PK 和 PW 分别分成 n 个影子秘密，避免了一个持有者区块中加密后影子秘密被泄露导致 PK 或 PW 完全泄露的风险。我们将这种去掉 CA 的方法称为 SMSSS-CA，过程如图 6 所示。

在每一笔交易过程中，只有参与治疗的医生和当前患者才可组成一组用户共享密钥，对发起交易的用户进行签名。接收方会通过 SMSSS-CA 签名机制验证签名并核查对方的真实以及时效性。如果签名无效或过期，组织和用户将没有权限发布交易或查看区块链数据。这种机制可以解决远程医疗中 CA 维护成本高和数据安全性低的问题和跨平台服务信息更新延迟的问题。

3.3 基于 NDN 的数据传输

NDN 和区块链具有相似结构，都采用了分布式结构，并且具有以内容为中心的分发机制。NDN 的信息传输机制自然比 IP 网络更能支持数据分布。利用 NDN 的优势替代传统的 P2P 转发流程，采用内容反向路径转发、路由灵活等优点，可以提高转发网络的整体性能和降低区块链广播开销和传输延迟。NDN 上传数据时都会给数据包再次进行数字签名，数据传输时会给数据包解签，使得 NDN 更加安全可靠。

本文的设计模型如图 7 所示，在数据上传过程中，首先通过智能合约获取用户的完整密钥，并使用 SMSSS-CA 签名机制对数据进行签名。在通过 NDN 上传数据包时，将再次对数据包进行签名，最后将多签名的密文存储至 IPFS 中，IPFS 将返回唯一哈希值给区块链。在数据传输过程中，用户发出感兴趣的文件访问请求，该请求经过智能合约进行无效信息检测和用户访问控制。如果检测无误，请求会被发送到私有链验集群节点。NDN 收到兴趣请

求后，会按顺序查询本地的 CS 表、PIT 表和 FIB 表以获取所需内容，如图 2 和图 3 所示。如果成功获取到内容，SMSSS-CA 签名机制恢复完整公钥分别对 NDN 和签名数据进行第一次和第二次解签。

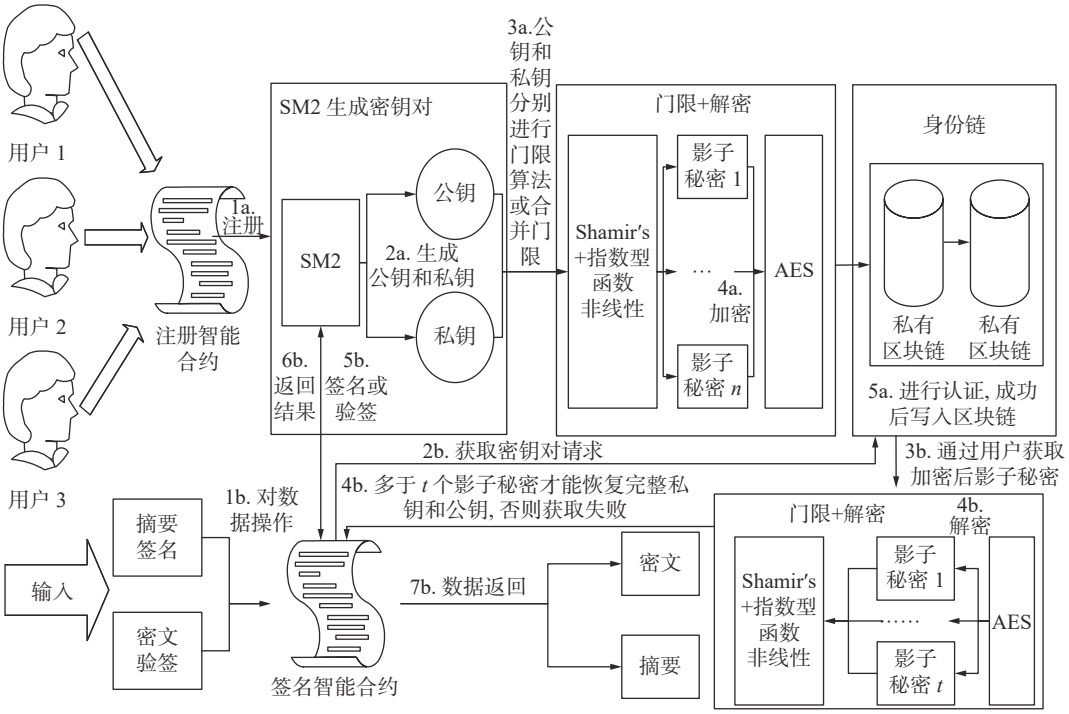

图 6　SMSSS-CA 签名

Fig. 6 SMSSS-CA signature

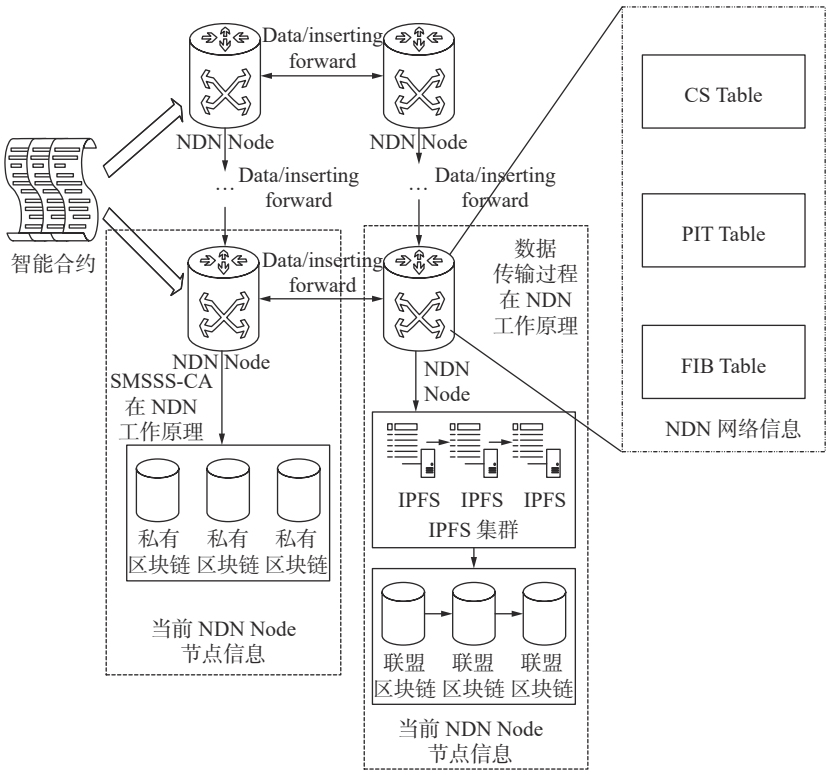

图 7　远程医疗 NDN 网络

Fig. 7 Telemedicine NDN network

通过这样的设计模型，可以有效解决远程医疗中医生和患者共享数据时响应慢和转发率低的问题，

同时提高了数据的安全性和可追溯性。区块链技术保障了数据的不可篡改性和可信度，智能合约技术实现了数据访问的精细控制和对无效搜索进行拦截，同时 NDN 多路径传输技术提高了数据传输的效率和可靠性。因此，这种设计模型对医疗数据的响应速度和数据传输的高效性都具有优秀的表现。

4 算法实现设计

4.1 注册阶段

在注册过程中，系统参数包括有限域F_q的规模 q 的椭圆曲线方程$y^2 = x^3 + ax + b \bmod p$中的参数 a、b、p，其中 p 为大素数。系统还需要选择一个椭圆曲线 $E(F_p)$上的非无穷远的基点 $G(x,y)$及其阶 n。

私钥为 PK，随机生成一个 256 位的整数 d，其取值范围应在 1 到 $n-1$ 之间。公钥则通过将基点 $G(x,y)$与 PK 进行点乘运算，得到$\mathrm{PW} = \mathrm{PK}[*]G(x,y)$，其中 [*] 表示点乘法。医患用户之间将生成一对密钥，包括 PK 和 PW。PK 通过 Shamir 门限算法在结合的同时引进指数型函数非线性计算使得门限算法具有更高的安全性，将 PK 划分成 m 个影子秘密，门限值为 t，通过多项式计算影子秘密，即

$$F(x)_{\mathrm{PK}} = \sum_{i=0} i^{k-1} s_i * \exp(b,i) + \sum_{j=0} j^{t-1} a_j * \exp(x,j) \tag{1}$$

式中：s_i为 PK 第 i 个影子秘密；b 为一个正整数的基数；a_j为门限多项式的系数。在存入区块链前必须对 PK 分片$F(x_i)_{\mathrm{PK}}$进行 AES 加密保护，由$F(x_i)_{\mathrm{PK}}$影子秘密第 i 个对字节生成$S_{\mathrm{PK},i}[v_d][v_e]$矩阵，开始进行行移位，即

$$S_{\mathrm{PK},i}[v_d][v_e] = S_{\mathrm{PK},i}[d,(e+d)\bmod 4] \tag{2}$$

然后再对数值进行列混淆，即

$$\begin{aligned} S'''_{\mathrm{PK},i}[v_d][v_e] = \{&[02 * S'_{\mathrm{PK},i}(d,e) + 03 \\ &* S'_{\mathrm{PK},i}(d,e+1)\bmod 4] + [01 * S'_{\mathrm{PK},i}(d,e+2)\bmod 4 \\ &* S'_{\mathrm{PK},i}(d,e+3)\bmod 4]\}\bmod 0x1b \end{aligned} \tag{3}$$

再进行轮密钥加，即

$$S'''_{\mathrm{PK},i}[v_d][v_e] = S''_{\mathrm{PK},i}[v_d][v_e] \oplus K[v_d][v_e] \tag{4}$$

其中$K[v_d][v_e]$表示当前的轮密钥，最后将加密后的$S'''_{\mathrm{PK},i}[v_d][v_e]$影子秘密存入区块链中。同时 PW 也需要划分 m 个影子秘密公式如上一致，$S'''_{\mathrm{PK},i}[v_d][v_e]$影子秘密存入区块链中。

4.2 SMSSS-CA 数字签名阶段

首先由 invsBox 方法对$S_{\mathrm{PK},i}[v_d][v_e]$密文逆盒，$S'[v_d][v_e] = \mathrm{InvsBox}[S_{\mathrm{PK},i}(d,e)]$，再对$S''_i[v_d][v_e] = S'[d,(e-d+4)\bmod 4]$逆行移位，然后进行逆列混淆，表达式为

$$\begin{aligned} S'''_i[v_d][v_e] = \{&0e * S''_i(d,e) + *0bS''_i[d,(e+1)\bmod 4] \\ &+ 0d * S''_i[d,(e+2)\bmod 4] * S''_i(d,e+3)\bmod 4\}\bmod 0x1b \end{aligned} \tag{5}$$

最后对S'''_i进行轮密钥加，即

$$S_i[v_d][v_e] = S'''_i(i,j) \oplus W(k,i,j) \tag{6}$$

在影子秘密恢复过程中，收集 t 个影子秘密持有者时通过对私钥进行恢复，即

$$\mathrm{PK} = \sum_{i=1}^{t} F(x_l) \prod_{v=1}^{t} \frac{-x_v}{x_l - x_v \bmod p} \quad l \neq v \tag{7}$$

由 SM2 签名计算杂凑值 Z 和 message 的哈希整数值为

$$r = [x + \mathrm{hash}(Z \| \mathrm{message})] \bmod q \tag{8}$$

式中：x 表示椭圆曲线的安全点；q 为系统公开参数，从而计算出签名值一部分 r。再计算签名数据为

$$\mathrm{Msg}_{\mathrm{pri}} = (1 + \mathrm{PK})^{-1}(k - r \cdot \mathrm{PK}) \bmod q \tag{9}$$

式中：k 为 $[1, q-1]$ 范围内随机值。计算的签名值一部分$\mathrm{Msg}_{\mathrm{pri}}$和 r 一起打包作为签名值。

4.3 SMSSS-CA 数字验签阶段

在公钥获取阶段如签名过程获取完整私钥公式一致。在获取到完整公钥 PW 为

$$(x_1, y_1) = \mathrm{Msg}_{\mathrm{pri\_1}G}(r_1 + \mathrm{Msg}_{\mathrm{pri\_1}}) \bmod q * \mathrm{PW} \tag{10}$$

获取到椭圆曲线验签坐标，其中$r_1, \mathrm{Msg}_{\mathrm{pri_1}}$是验签前的签名值，PK 是用户的公钥，$G$ 为有限域椭圆曲线 E 上阶为 q 的生成元点。然后进行验签，即

$$r_2 = [x_1 + \mathrm{hash}(Z \| \mathrm{message})] \bmod q \tag{11}$$

如果$r_1 == r_2$，则表示验签成功。

4.4 新增人员时门限合并阶段

重新为其生成一组密钥对，例如 PK 影子秘密，假设在一组医患用户之间已经生成了 t 个影子秘密$(x_1,y_1),(x_2,y_2),\cdots,(x_t,y_t)$，其中影子秘密$x_i$是已有的，门限私钥分片的 x 值，影子秘密y_i是对应的门限私钥分片的 y 值，然后合并一个新的影子秘密(x_{t+1},y_{t+1})进行计算，即

$$F'(x)_{\mathrm{PK}} = F(x)_{\mathrm{PK}} + F_{t+1}(x)_{\mathrm{PK}} \tag{12}$$

将新的门限值 t+1 更新到门限条件中，表示现在需要 t+1 个参与者才能恢复密钥。公钥 PW 也如上述过程。后续密钥对加密操作如注册阶段$F(x_i)_{\mathrm{PK}}$一致，加密后存入区块链中。

5 实验分析

5.1 实验配置

本系统使用 Inter(R) Core(TM) i7-10875H

CPU@2.30 GHz，内存容量为 32 G(英睿达铂胜 DDR4 3200 MHz)，Nvidia GeForce GTX 2080(6 GB)。采用虚拟机使用 Ubuntu 操作系统，通过 NS3[17] 和 NDNSIM[18] 仿真平台进行测试 3 种网络的负载均衡。系统构架使用以太坊框架，使用 Ganache 来搭建区块链的建立，通过 solodity 语言进行智能合约开发，使用 Node JS 提供以太坊和 IPFS 链接。使用开源的 Golang Ethereum Client(Geth)版本 1.8 作为本项目的代码基础。

5.2　结果分析

实验开启了多个节点，并进行了文件上传和下载测试，同时对医疗数据共享系统的性能和安全性进行了测试。实验测试对 SMSSS-CA 与文献 [19-22] 签名算法方案的安全性进行对比。在安全性的基础上，SMSSS-CA 再与文献 [23-26] 签名成本方案进行对比，最后进行 NDN 实验对比。

5.2.1　安全性分析

SMSSS-CA 安全性对比如表 1 所示。

表 1　主要安全性指标评估

Tab. 1　Evaluation of key safety indicators

方案	不可伪造性	追踪性	模拟攻击抗性	前向安全性	加密文件安全性
文献[19]	√	√	–	√	√
文献[20]	√	√	–	√	√
文献[21]	√	√	√	√	√
文献[22]	√	√	√	–	√
CA	√	√	√	√	√
SMSSS-CA	√	√	√	√	√

不可伪造性：SMSSS-CA 采用多层保护方式，通过使用 AES 算法对分割后的影子秘密 $F(x_i)_{\mathrm{P}}$ 加密为 $S_{\mathrm{p}}'''[v_d][v_e]$，并存入私有区块链中，有效地保护密钥信息免受未授权访问和篡改。同时，利用 SM2 算法的不可逆性和难解性，确保密钥对的完整性和不可篡改性。

追踪性：所有操作在智能合约的基础上对数据日志审计，得到智能合约管理级授权接收到签名信息时，可通过影子秘密查找追踪列表，寻找追踪签名者身份信息，实现追溯目的。

模拟攻击抗性：攻击者无法通过模拟攻击获取完整的 PK 和 PW 信息。由于 PK 和 PW 以加密后的影子秘密 $S_{\mathrm{p}}'''[v_d][v_e]$ 分散存储在多个部分和私有区块链上，攻击者无法单独获取完整的 PK 和 PW。这提高了系统的安全性，并增加了攻击者模拟攻击的难度。

向前安全性：在未来的时间里，即使攻击者获取了一部分影子秘密信息，攻击者也无法推导出其他部分的影子秘密，也无法通过已知的影子秘密信息预测或计算出其他未知的影子秘密。这增强了系统的安全性，防止了向前推导攻击。

加密文件安全性：在通过 SMSSS-CA 对摘要签名或密文验签，通过超过 t 个影子秘密才能做相应操作，防止医疗数据造成隐私安全威胁和泄露造成用户组损失。

如表 1 所示，所提出的 SMSSS-CA 算法满足于主要安全性指标评估，安全性可以得到保证。

5.2.2　SMSSS-CA 签名实验对比

在签名和解签时，实验中将一笔交易进行广播，并执行 200 次。T_{ML} 与 gas 成正比，gas 消耗越少其维护成本越低，其结果如表 2 和表 3 所示，在保证安全性基础上，所提出的 SMSSS-CA 签名总体开销是最低的，优于其他现有方案的。

表 2　名称含义

Tab. 2　Name meaning

方案	签名所用
T_{ML}	执行模乘运算所需时间
T_{M}	椭圆曲线标量点乘 $\approx 29T_{\mathrm{ML}}$
T_{H}	映射到点到点哈希函数 $\approx 23T_{\mathrm{ML}}$
T_{E}	幂运算 $\approx 21T_{\mathrm{ML}}$
T_{I}	模逆运算 $\approx 11.6T_{\mathrm{ML}}$
T_{PE}	基于配对的求幂 $\approx 43.5T_{\mathrm{ML}}$
T_{P}	配对评估 $\approx 87T_{\mathrm{ML}}$
T_{PA}	点相加 $\approx 0.12T_{\mathrm{ML}}$
T_{F}	哈希函数的求值 $\approx 29T_{\mathrm{ML}}$

表 3 主要业务评估

Tab. 3 Major business evaluation

方案	签名(T_{ML})	验签(T_{ML})	总消耗(T_{ML})
文献[8]	$2T_M+T_I+T_H\approx92.6$	$3T_M+T_I+T_H\approx121.6$	$5T_M+T_I+T_H\approx214.2$
文献[23]	$3T_M+T_P+T_{PE}+T_{PA}+4T_F\approx333.62$	$4T_P+T_{PA}+2T_F\approx406.12$	$3T_M+5T_P+T_{PE}+T_{PA}+6T_F\approx739.74$
文献[24]	$8T_M+2T_{PA}+3T_F\approx319.24$	$3T_P+2T_F\approx319$	$8T_M+2T_{PA}+5T_F+3T_P\approx638.24$
文献[25]	$3T_E\approx63$	$2T_E+2T_P+2T_f\approx239.2$	$5T_E+2T_P+2T_f\approx302.2$
文献[26]	$2T_P\approx174$	$3T_P\approx261$	$5T_P\approx435$
CA	$3T_M+T_I+T_H\approx121.6$	$3T_M+T_I+T_H\approx121.6$	$6T_M+2T_I+2T_H\approx243.2$
SMSSS-CA	$T_H+T_M+T_E+T_I+20T_{PA}\approx87$	$2T_M+2T_H+T_I+20T_{PA}\approx118$	$3T_H+3T_M+T_E+2T_I+40T_{PA}\approx205$

5.2.3 NDN 实验对比

在本研究中，基于 NS3 和 NDNSIM 仿真环境，搭建了带宽为 10 Mbps、传输时延为 1ms 的网络拓扑来模拟区块链大小建立错误率为 0.000 01 的 IP、P2P 和 NDN 模拟网络。通过进行 1 000 次测试，评估不同网络的响应延时和方向转发率。

图 8 和图 9 展示了在 NS3 和 NDNSIM 环境下的转发率实验结果。在 NS3 环境下，IP 网络不具备转发条件，而 P2P 和 NDN 的实验结果显示，NDN 的转发率平均高出 P2P 网络转发率 9.84%。在 NDNSIM 环境下的实验结果也表明，NDN 的转发率平均高出 P2P 网络转发率 9.74%。

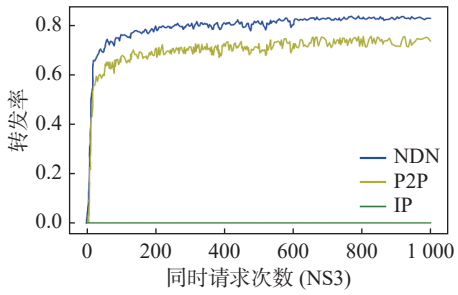

图 8 NS3 环境下 3 种网络的转发率对比

Fig. 8 Comparison of forwarding rates of three networks in NS3 environment

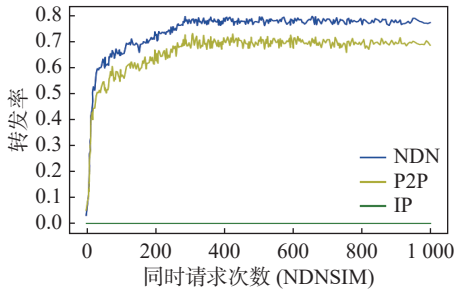

图 9 NDNSIM 环境下 3 种网络的转发率对比

Fig. 9 Comparison of forwarding rates of three networks in NDNSIM environment

响应时间在 NS3 和 NDNSIM 两种环境下实验结果如图 10 和图 11 所示。在 NS3 环境下不同区块链大小对比实验中，NDN 响应时间平均低于 IP 网络的 28.75%，低于 P2P 网络的 7.65%。在 NDNSIM 环境下不同区块链大小对比实验中，NDN 响应时间平均低于 IP 网络的 27.19%，低于 P2P 网络的 7.23%。

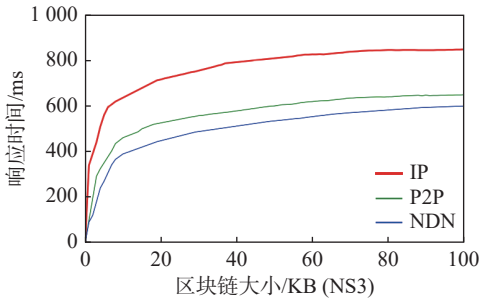

图 10 NS3 环境下 3 种网络响应时间对比

Fig. 10 Comparison of the corresponding time of three networks in NS3 environment

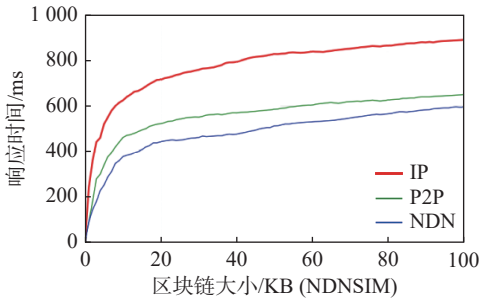

图 11 NDNSIM 环境下 3 种网络响应时间对比

Fig. 11 Comparison of the corresponding time of three networks in NDNSIM environment

经过实验，本文提出的区块链和 SM2 算法代替签证机构颁发公钥和私钥在保证安全性的基础上，确实可以降低远程医疗数据签证的成本开销。同时，在远程医疗数据共享方面，NDN 结合 IPFS 集群表现出更高的转发率和更低的响应时间，特别是在远

程会诊过程中，患者病例的快速获取和医生之间的会诊数据共享方面，具有显著的优势。相比目前市面上的集中式存储方式，NDN 结合 IPFS 集群的方案更加符合当前环境下的需求，同时也降低了潜在的风险。

6　结束语

经过新冠疫情的冲击，远程医疗成为了一种有利的辅助手段。本文提出 SMSSS-CA 签名机制、NDN 命名数据网络集成智能合约等相关技术，并将其应用于远程医疗领域。通过使用 SMSSS-CA 签名机制，实现高效的密钥管理方式。实验结果表明，比现有研究远程医疗方法具有降低的医院 CA 维护成本，同时也提高远程医疗数据的安全性。而通过采用 NDN 和智能合约技术，成功解决了 IP 网络区块链传播慢、网络响应低和 P2P 网络转发慢等问题，从而大大提高了数据的响应速度和传播效率。这一方案不仅能够满足远程医疗的需求，为城乡居民提供更好的医疗服务，减轻医院压力，也能够应对疫情等突发情况，为社会稳定发展做出了积极贡献。

参考文献:

[1] MUBASHAR A, ASGHAR K, JAVED A R, et al. Storage and proximity management for centralized personal health records using an IPFS-based optimization algorithm[J]. Journal of Circuits, Systems and Computers, 2022, 31(1): 2250010. DOI: 10.1142/S0218126622500104.

[2] THIBAC D, MINH N H. Design of network security storage system based on under cloud computing technology[J]. Computers and Electrical Engineering, 2022, 103: 108334. DOI: 10.1016/j.compeleceng.2022.108334.

[3] WIESE F, BALDINI M. Conceptual model of the industry sector in an energy system model: a case study for Denmark[J]. Journal of Cleaner Production, 2018, 203: 427-443. DOI: 10.1016/j.jclepro.2018.08.229.

[4] CHEN Q K, HUANG W J, PENG Y Z, et al. A reinforcement learning-based framework for solving the IP mapping problem[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2021, 29(9): 1638-1651. DOI: 10.1109/TVLSI.2021.3097712.

[5] HASAN H R, SALAH K, JAYARAMAN R, et al. Blockchain-enabled telehealth services using smart contracts[J]. IEEE Access, 2021, 9: 151944-151959. DOI: 10.1109/ACCESS.2021.3126025.

[6] 关志涛, 杨亭亭, 徐茹枝, 等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报, 2015, 36(6): 2015142. DOI: 10.11959/j.issn.1000-436x.2015142.
GUAN Z T, YANG T T, XU R Z, et al. Multi-authority attribute-based encryption access control model for cloud storage[J]. Journal on Communications, 2015, 36(6): 2015142. DOI: 10.11959/j.issn.1000-436x.2015142.

[7] NZANYWAYINGOMA F, HUANG Q M. Improving energy efficiency in M2M healthcare systems using CP-ABE schemes[C]//Proceedings of 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops. Piscataway: IEEE, 2015: 1243-1248. DOI: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.225.

[8] CHEN T H, ZHU T L, JENG F G, et al. Blockchain as a CA: a provably secure signcryption scheme leveraging blockchains[J]. Security and Communication Networks, 2021, 2021: 6637402. DOI: 10.1155/2021/6637402.

[9] 张利华, 付东辉, 万源华. 基于区块链的车联网汽车身份认证方案[J]. 现代电子技术, 2021, 44(8): 77-80. DOI: 10.16652/j.issn.1004-373x.2021.08.017.
ZHANG L H, FU D H, WAN Y H. Blockchain-based Internet of Vehicles authentication scheme[J]. Modern Electronics Technique, 2021, 44(8): 77-80. DOI: 10.16652/j.issn.1004-373x.2021.08.017.

[10] KHALID R, JAVAID N, ALMOGREN A, et al. A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid[J]. IEEE Access, 2020, 8: 47047-47062. DOI: 10.1109/ACCESS.2020.2979051.

[11] DIVÁN M J, SÁNCHEZ-REYNOSO M L. Metadata-based measurements transmission verified by a Merkle Tree[J]. Knowledge-Based Systems, 2021, 219: 106871. DOI: 10.1016/j.knosys.2021.106871.

[12] SONG T T, CUI B, LI R, et al. Smart contract-based trusted content retrieval mechanism for NDN[J]. IEEE Access, 2020, 8: 85813-85825. DOI: 10.1109/ACCESS.2020.2992115.

[13] ZAFAR W U I, REHMAN M A U, JABEEN F, et al. Context-aware naming and forwarding in NDN-based VANETs[J]. Sensors, 2021, 21(14): 4629. DOI: 10.3390/s21144629.

[14] DWIVEDI S K, AMIN R, VOLLALA S. Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(12): 1913-1922. DOI: 10.1109/JAS.2021.1004225.

[15] ABDEL HAKEEM S A, KIM H. Centralized threshold key generation protocol based on Shamir secret sharing and HMAC authentication[J]. Sensors, 2022, 22(1):

331. DOI: 10.3390/s22010331.

[16] 杨龙海, 王学渊, 蒋和松. 改进 SM2 签名方法的区块链数字签名方案[J]. 计算机应用, 2021, 41(7): 1983-1988. DOI: 10.11772/j.issn.1001-9081.2020081220.
YANG L H, WANG X Y, JIANG H S. Blockchain digital signature scheme with improved SM2 signature method[J]. Journal of Computer Applications, 2021, 41(7): 1983-1988. DOI: 10.11772/j.issn.1001-9081.2020081220.

[17] KHATTAK H A, RAJA F Z, ALOQAILY M, et al. Efficient in-network caching in NDN-based connected vehicles[C]//Proceedings of 2021 IEEE Global Communications Conference. Piscataway: IEEE, 2021: 1-6. DOI: 10.1109/GLOBECOM46510.2021.9685200.

[18] UEDA K, KATO T, SASAKI C, et al. Revisiting loss detection in NDN: detecting spurious timeout using probe interest[C]//Proceedings of 2022 IEEE Global Communications Conference. Piscataway: IEEE, 2022: 4455-4460. DOI: 10.1109/GLOBECOM48099.2022.10001095

[19] 欧海文, 雷亚超, 王湘南. 一种安全高效的群签名方案[J]. 计算机应用与软件, 2020, 37(7): 309-312. DOI: 10.3969/j.issn.1000-386x.2020.07.051.
OU H W, LEI Y C, WANG X N. A secure and efficient group signature scheme[J]. Computer Applications and Software, 2020, 37(7): 309-312. DOI: 10.3969/j.issn.1000-386x.2020.07.051.

[20] 洪璇, 张绪霞. 基于中国剩余定理的前向安全群签名方案[J]. 计算机应用研究, 2020, 37(9): 2806-2810. DOI: 10.19734/j.issn.1001-3695.2019.03.0150.
HONG X, ZHANG X X. Forward secure group signature scheme based on Chinese remainder theorem[J]. Application Research of Computers, 2020, 37(9): 2806-2810. DOI: 10.19734/j.issn.1001-3695.2019.03.0150.

[21] ZHONG H, HAN S S, CUI J, et al. Privacy-preserving authentication scheme with full aggregation in VANET[J]. Information Sciences, 2019, 476: 211-221. DOI: 10.1016/j.ins.2018.10.021.

[22] KAMIL I A, OGUNDOYIN S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks[J]. Journal of Information Security and Applications, 2019, 44: 184-200. DOI: 10.1016/j.jisa.2018.12.004.

[23] KIM T H, KUMAR G, SAHA R, et al. CASCF: certificateless aggregated signcryption framework for internet-of-things infrastructure[J]. IEEE Access, 2020, 8: 94748-94756. DOI: 10.1109/ACCESS.2020.2995443.

[24] PIUS OWOH N, MAHINDERJIT SINGH M. SenseCrypt: a security framework for mobile crowd sensing applications[J]. Sensors, 2020, 20(11): 3280. DOI: 10.3390/s20113280.

[25] KARATI A, FAN C I, HSU R H. Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices[J]. IEEE Internet of Things Journal, 2019, 6(6): 10431-10440. DOI: 10.1109/JIOT.2019.2939204.

[26] LUO W, MA W P. Secure and efficient data sharing scheme based on certificateless hybrid signcryption for cloud storage[J]. Electronics, 2019, 8(5): 590. DOI: 10.3390/electronics8050590.

作者简介:

史爱武 博士, 副教授, saw@wtu.edu.cn

韩 超(通信作者) 硕士, 287811015@qq.com