计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(5):124−130 [doi: 10.15888/j.cnki.csa.008503]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 基于 SM9 算法的跨区域医疗协同双向身份验证方案①

方　婷[1], 王晓华[2], 杨　敏[2]

[1](贵州大学 计算机科学与技术学院, 贵阳 550025)
[2](遵义医科大学 医学信息工程学院, 遵义 563003)
通信作者: 王晓华, E-mail: wangxiaohua@zmu.edu.cn

**摘　要**: 为保障跨区域医疗协同服务的安全, 鉴别交换双方的身份至关重要. 本文将 DH 算法和国密 SM9 算法相结合, 把 DH 算法协商的共同密钥作为验证因子, 结合数字签名实现加密传输和用户的双向验证. 本文以医院间电子病历的访问过程中用户之间的身份验证作为案例, 对跨区域信息共享中通信双方的身份验证进行分析和研究, 通过实验验证方案的可行性和正确性, 具有一定的实际应用价值.

**关键词**: 验证因子; SM9; 身份验证; 数字签名; 密码算法

引用格式: 方婷,王晓华,杨敏.基于 SM9 算法的跨区域医疗协同双向身份验证方案.计算机系统应用,2022,31(5):124–130. http://www.c-s-a.org.cn/1003-3254/8503.html

## Bidirectional Identity Verification Scheme of Cross-regional Medical Collaboration Based on SM9 Algorithm

FANG Ting[1], WANG Xiao-Hua[2], YANG Min[2]

[1](School of Computer Science and Technology, Guizhou University, Guiyang 550025, China)
[2](School of Medical Information Engineering, Zunyi Medical University, Zunyi 563003, China)

**Abstract**: For the safety of cross-regional medical collaborative services, it is crucial to identify the identities of the exchange parties. This study combines the Diffie-Hellman (DH) algorithm with the SM9 algorithm published by the State Cryptography Administration of China, uses the common key negotiated by the DH algorithm as a verification factor, and integrates digital signatures to achieve encrypted transmission and bidirectional verification of users. Taking the identity verification of users in the access of electronic medical records between hospitals as a case, this study analyzes the identity verification of both communicating parties in cross-regional information sharing and verifies the feasibility and correctness of the scheme through experiments, demonstrating that the scheme has practical application value.

**Key words**: verification factor; SM9; identity verification; digital signature; cryptographic algorithm

电子病历的发展从提升效率, 到信息集成共享, 再到提升医疗质量与安全, 发生了质的变化, 而随着远程医疗技术的发展, 学者们又对电子病历的跨区域共享展开了大量的研究. 其中, 身份验证作为信息系统安全的第一道关卡, 对于电子病历的跨区域[1]安全共享至关重要.

用户身份验证[2–7]的方法基本上可分为: 基于口令的身份验证、基于令牌的身份验证、基于生物学特征的身份验证和基于公开密钥加密算法的身份验证, 在网络通信中最常见的是基于公开密钥加密算法的身份验证. 文献 [8] 针对用户异地访问系统中存在用户身份鉴别和用户数字证书[9]信息交互的问题, 提出采用分

① 基金项目: 国家自然科学基金 (61861047)
收稿时间: 2021-07-23; 修改时间: 2021-08-18, 2021-09-29; 采用时间: 2021-10-09; csa 在线出版时间: 2022-04-11

布式 PKI/CA 架构, 通过数字证书对两地操作系统、应用系统提供统一的安全支撑, 形成面向业务应用和数据管理的统一身份、统一认证的信任体系, 实现异地信息资源的整合利用和业务协同. 但是该方案中的证书管理中心 (CA) 并不是完全安全, 其颁发的主密钥对都相同, 若主密钥泄露, 那么入侵者将冒充 CA 来颁发证书. 文献 [10] 提出了一种通过将大文件分块, 采用多线程传输, 并支持文件断点续传的方案, 解决了异地环境下大文件传输的稳定性问题. 该方案制定了基于 SSL 协议的传输安全策略, 首先, 通过数字证书和电子签名验证通信双方的身份信息, 阻止与非法用户的通信; 其次, 使用对称/非对称加密算法对密钥和数据信息加密, 防止传输过程中密钥和数据信息被非法窃取. 上述方案中都是用第三方 CA 认证中心颁发的数字证书来实现客户与服务器之间的双向认证, 但是证书申请成本高, 还有使用期限限制, 随着用户的增多, 证书的管理难度也越来越大. 文献 [11] 为触觉互联网辅助远程手术应用程序设计了一种超高效的相互认证和密钥协商协议, 外科医生和机械臂之间通过网关进行相互认证, 然后这 3 个实体生成一个公共的秘密会话密钥, 用于当前登录会话中的未来通信, 从而实现远程手术操作期间的安全通信. 国密 SM9 算法[12] 也去除了以 CA 签发数字证书作为凭证的过程, 用户不需要通过第三方来保证其公钥来源的真实性, 这一措施极大地拓宽了 PKI[13−15] 的应用范围和场景, 也节省了传统 PKI 身份认证体制在密钥产生、证书签发、密钥管理等方面的花销. 对于认证, 私钥的分发和安全是整个流程安全性的核心, 文献 [16] 对 SM9 算法的私钥分发给出了具体的解决方案, 在安全分发私钥的同时实现了客户端与服务器的双向认证.

为保障跨区域医疗信息的安全共享, 鉴别通信双方的身份至关重要, 本文提出了一种基于 SM9 的双向身份验证方案 (bidirectional authentication scheme based on SM9, BAS) 实现了用户之间的身份信息认证, 为安全有效的实现电子病历的共享奠定基础.

## 1 相关工作

### 1.1 Diffie-Hellman (DH) 密钥协议

DH 密钥协商算法的具体流程如下:

(1) 用户 $A$ 与用户 $B$ 共享一个素数$p$以及该素数的本原根$g$, 且有$2 \leqslant g \leqslant p-1$;

(2) 用户 $A$ 产生一个私有的随机数$x$, 满足$1 \leqslant x \leqslant p-1$, 计算$Y_A$为:

$$Y_A = g^x \bmod p \tag{1}$$

将式 (1) 计算的结果$Y_A$发送给用户 $B$.

(3) 用户 $B$ 产生一个私有的随机数$y$, 满足$1 \leqslant y \leqslant p-1$, 计算$Y_B$为:

$$Y_B = g^y \bmod p \tag{2}$$

将式 (2) 计算的结果$Y_B$发送给用户 $A$.

(4) 用户 $A$ 接收到$Y_B$后计算得到$K_A$. 同理, 用户 $B$ 接收到$Y_A$计算得到$K_B$. 计算如下:

$$K_A = Y_B^x = g^{xy} \bmod p \tag{3}$$

$$K_B = Y_A^y = g^{xy} \bmod p \tag{4}$$

(5) 式 (3) 和式 (4) 计算得到的结果满足 $K$=$K_A$=$K_B$, 因此双方经过协商后得到了相同的密钥 $K$, 达成密钥协商的目的.

本文将 DH 算法协商的共同密钥作为验证因子, 并将其应用到验证流程中.

### 1.2 双线性群

双线性对定义在椭圆曲线群上, 主要有 Tate 对、Ate 对、R-ate 对和 Weil 对. SM9 算法中使用的双线性对为 R-ate 对[17,18], 其安全性和运算速率较高.

设有$(G_1,+)$、$(G_2,+)$和$(G_T,\cdot)$3 个阶均为素数 $N$ 的循环群. $G_1$和$G_2$的生成元分别为$P_1$和$P_2$, 存在$G_2$到$G_1$的映射$\psi$ 使得$\psi(P_2)=P_1$, 双线性对$e$ 是 $G_2 \times G_1 \to G_T$ 的映射, 满足下列性质:

(1) 双线性性: 对任意的$P \in G_1$, $Q \in G_2$, $a,b \in Z_N$, 有$e(aP,bQ)=e(P,Q)^{ab}$;

(2) 非退化性: $e(P_1,P_2) \neq 1$;

(3) 可计算性: 对任意的$P \in G_1$, $Q \in G_2$, 存在有效的算法计算$e(P,Q)$.

## 2 方案设计

### 2.1 符号定义

表 1 为本文方案所用符号定义.

### 2.2 BAS 方案

本文以医院间电子病历的访问过程中用户之间的身份验证作为案例, 提出 BAS 方案来对跨区域信息共享中通信双方的身份验证进行分析和研究.

BAS 方案采用了“验证因子+数字签名”的验证方式, 该方法区别于传统的公钥加密身份验证方式, 本文将通信双方通过 DH 算法产生的共同密钥作为验证因

子来完成第 1 阶段的身份验证, 再通过数字签名完成第 2 阶段的身份验证. 图 1 为 BAS 方案详细认证流程图.

表 1　符号定义

| 符号 | 代表的意义 |
|---|---|
| $G_T$ | 阶为素数$N$的乘法循环群 |
| $G_1$ | 阶为素数$N$的加法循环群 |
| $G_2$ | 阶为素数$N$的加法循环群 |
| $N$ | 大于$2^{191}$的素数 |
| $P_1$ | $G_1$的生成元 |
| $P_2$ | $G_2$的生成元 |
| $KGC$ | 密钥生成中心 |
| $ID_A$ | 用户$A$的标识, 可以唯一确定用户$A$的公钥 |
| $de_A$ | 用户$A$的加密私钥 |
| $ds_A$ | 用户$A$的签名私钥 |
| $Pub_m$ | 加密主公钥 |
| $Pub_s$ | 签名主公钥 |
| $M$ | 待签名消息 |
| $M'$ | 待验证消息 |
| $V_i$ | 验证因子($i$=1, 2) |

认证流程具体步骤如下:

(1) 医院 $A$ 向医院 $B$ 申请所需患者的电子病历, 医院 $B$ 收到医院 $A$ 的请求后做出响应. 同时, 双方通过 DH 算法分别产生验证因子$V_1$和$V_2$并将其保存.

(2) 医院 $B$ 保存验证因子$V_2$后, 使用 SM9 算法中的公钥加密算法加密$V_2$得到密文$C$, 并将其发送到医院 $A$, 医院 $A$ 对密文$C$进行解密后得到明文$V_2'$. 对比分析$V_2$与$V_2'$的值, 若二者数值相同则继续执行验证流程; 若二者数值不同则结束验证.

(3) 医院 $A$ 对比分析$V_2$与$V_2'$的数值相同, 则将患者的身份信息作为待签名的消息$M$, 获取$M$的数字签名$(h,S)$, 最后将$M$及其数字签名$(h,S)$一起发送到医院 $B$. 医院 $B$ 检验收到的消息$M'$及其数字签名$(h',S')$, 验证成功则根据消息$M'$发送与之身份信息相匹配的患者电子病历到医院 $A$; 验证失败则驳回医院 $A$ 的申请, 结束验证流程.

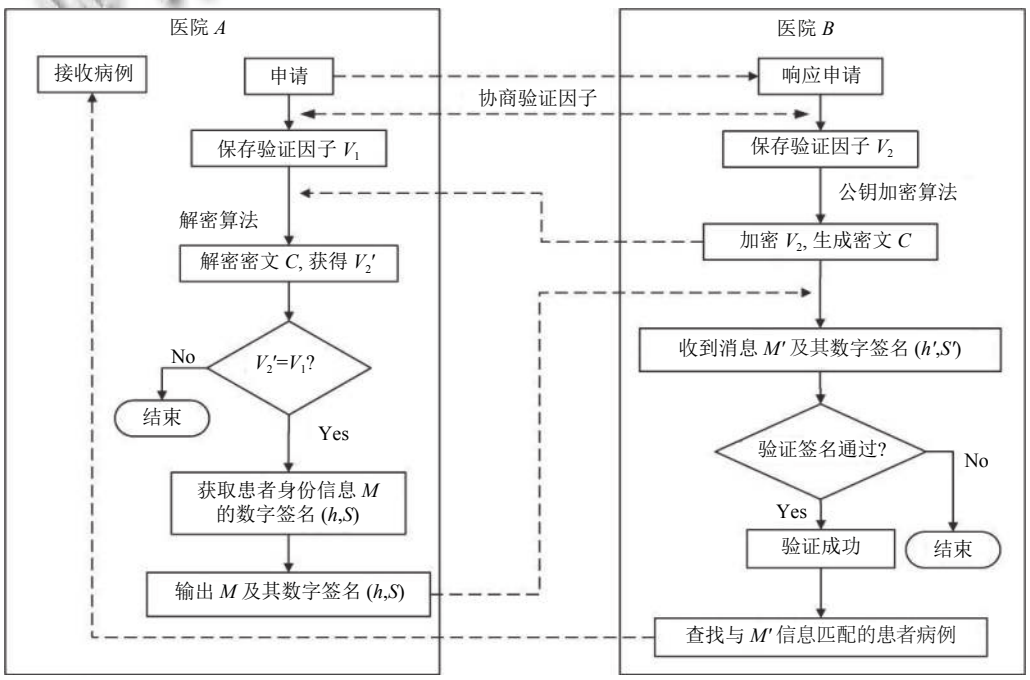


图 1　BAS 方案认证流程图

### 2.3　方案描述

(1) 系统初始化

系统选取两个循环加法群$G_1$、$G_2$和一个循环乘法群$G_T$, 这 3 个群的阶均为素数$N$, $P_1$是$G_1$的生成元, $P_2$是$G_2$的生成元, 存在$G_2$到$G_1$的同态映射$\psi$使得$\psi(P_2)=P_1$, 双线性对$e$是$G_2\times G_1\to G_T$的映射.

系统的密钥生成中心 ($KGC$) 产生随机数$m\in[1, N-1]$作为加密主私钥, 计算$G_1$中的元素$Pub_m=mP_1$作为加密主公钥, 则加密主密钥对为$(m, Pub_m)$. 秘密保存$m$, 公开$Pub_m$.

系统的密钥生成中心 ($KGC$) 产生随机数$s\in[1, N-1]$作为签名主私钥, 计算$G_2$中的元素$Pub_s=sP_2$作为签名主公钥, 则签名主密钥对为$(s, Pub_s)$. 秘密保存$s$, 公开$Pub_s$.

(2) 用户 $B$ 身份验证阶段

用户 $A$ 与用户 $B$ 使用 DH 算法协商验证因子保存后, 用户 $B$ 需将自己的验证因子$V_2$加密并发送到用户 $A$ 进行身份验证. 图 2 为用户 $B$ 身份验证.

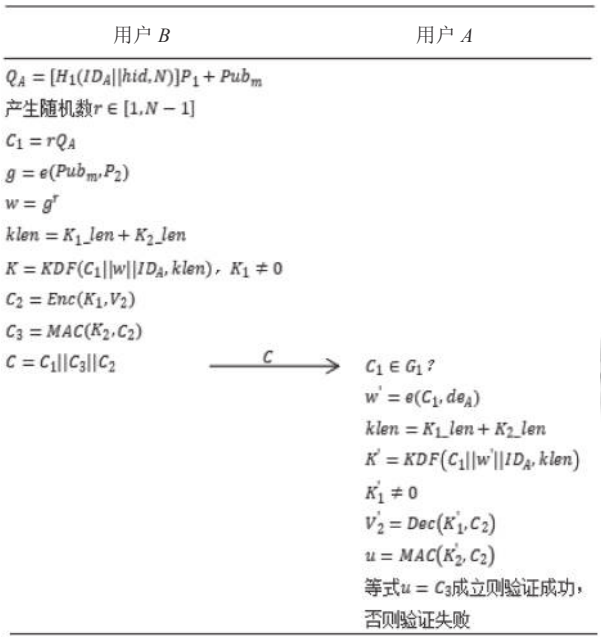


图 2 用户 $B$ 身份验证

1) 加密验证因子

用户 $B$ 使用用户 $A$ 的标识$ID_A$来计算用户 $A$ 的公钥$Q_A=[H_1(ID_A||hid,N)]P_1+Pub_m$, 再产生一个随机数$r\in[1,N-1]$用于加密. 首先, 计算$C_1=rQ_A$、$g=e(Pub_m,P_2)$、$w=g^r$、$klen=K_1\_len+K_2\_len$ (令$K_1$为 $K$ 最左边的$K_1_len$比特, $K_2$为剩下的$K_2_len$比特串, 注意$K_1$是否为全 0 比特串) 和$K=KDF(C_1||w||ID_A)$. 最后输出$(K,C_1)$, 至此密钥封装完成. 继续计算$C_2=Enc(K_1,V_2)$和$C_3=MAC(K_2,C_2)$, 即用密钥$K_1$对验证因子$V_2$进行加密生成密文$C_2$, 然后在密钥$K_2$的控制下产生$C_2$的消息认证码$C_3$, 防止$C_2$被篡改. 最后, 输出密文$C=C_1||C_3||C_2$, 并将其发送给用户 A 进行验证.

2) 验证

用户 $A$ 收到密文$C$后, 从中取出$C_1$, 并验证$C_1\in G_1$是否成立, 若不成立则立即报错并退出; 若成立, 则计算$w'=e(C_1,de_A)$、$klen=K_1\_len+K_2\_len$ (令$K_1'$为$K'$最左边的$K_1_len$比特, $K_2'$为剩下的$K_2_len$比特, 注意$K_1'$是否为全 0, 是则报错退出) 和$K'=KDF(C_1||w'||ID_A,klen)$, 最后输出密钥$K'$, 至此密钥解封装完成. 继续计算$V_2'=Dec(K_1',C_2)$, 即使用密钥$K'$对密文$C_2$进行解密得到明文$V_2'$. 然后使用密钥$K_2'$计算消息认证码$u=MAC(K_2',C_2)$, 从密文$C$中取出$C_3$, 分析对比$u$与$C_3$, 若二者数值不同, 则表示密文被篡改并报错退出; 若二者数值相同, 则输出明文$V_2'$. 最后, 对比分析$V_1$和$V_2'$的值, 若二者数值不同则用户 $B$ 的身份验证失败, 结束验证流程; 若二者数值相同则用户 $B$ 的身份验证成功, 可继续执行下一步验证.

(3) 用户 $A$ 身份验证阶段

用户 $B$ 的身份验证成功后, 用户 $A$ 需要获取消息$M$(患者身份信息) 的数字签名$(h,S)$发送给用户 $B$, 以此来验证用户 $A$ 的身份. 图 3 为用户 $A$ 身份验证.

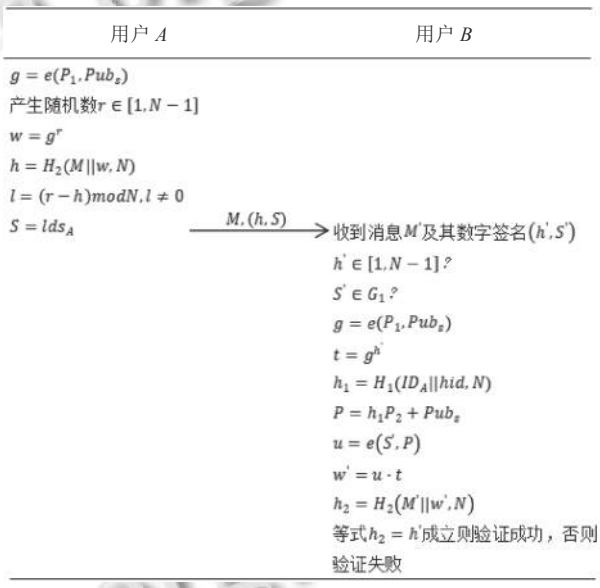


图 3 用户 $A$ 身份验证

1) 数字签名

首先, 计算$g=e(P_1,Pub_s)$并保存结果. 其次, 产生随机数$r\in[1,N-1]$, 然后计算$w=g^r$、$h=H_2(M||w,N)$和$l=(r-h)\bmod N$(注意$l$是否为 0). 在$l$不为 0 的情况下, 计算$S=ldS_A$, 确定消息$M$的数字签名为$(h,S)$. 最后输出$M$及其数字签名$(h,S)$并将其发送到用户 $B$ 处进行验证.

2) 验证数字签名

用户 $B$ 收到消息$M'$及其数字签名$(h',S')$后, 先检验等式$h'\in[1,N-1]$是否成立, 若不成立则验证不通过; 若成立, 则继续检验等式$S'\in G_1$是否成立, 若$S'\in G_1$不成立则验证不通过; 若$S'\in G_1$成立, 则计算$g=e(P_1,Pub_s)$、$t=gh'$、$h_1=H_1(ID_A||hid,N)$、$P=h_1P_2+Pub_s$、$u=e(S',P)$、$w'=ut$和$h_2=H_2(M'||w',N)$. 最后,

检验等式$h_2 = h'$是否成立, 若成立则验证通过; 否则验证失败.

### 2.4 数字签名及验签正确性证明

数字签名及验签的正确性关键是考虑签名时$w$的生成以及验签时$w$的生成, 这两个阶段$w$的计算如式 (5) 和式 (6):

(1) 签名时:

$$w = g^r = e(P_1, Pub_s)^r = e(P_1, sP_2)^r = e(P_1, P_2)^{rs} \tag{5}$$

(2) 验签时:

$$\begin{aligned} w &= ut \\ &= e(S, h_1P_2 + Pub_s)\cdot e(P_1, Pub_s)^h \\ &= e((r-h)dsA, h_1P_2 + sP_2)\cdot e(P_1, sP_2)^h \\ &= e\left(\left[(r-h)\cdot s\cdot (h_1+s)^{-1}\right]P_1, [h_1+s]P_2\right)\cdot e(P_1, P_2)^{sh} \\ &= e(P_1, P_2)^{\frac{(r-h)s}{h_1+s}(h_1+s)}\cdot e(P_1, P_2)^{sh} \\ &= e(P_1, P_2)^{(r-h)s+sh} \\ &= e(P_1, P_2)^{rs} \end{aligned} \tag{6}$$

根据式 (5) 和式 (6) 推导可知, 签名和验签计算的$w$相等, 所以由$w$计算出来的$h$相等.

### 2.5 方案安全性分析

(1) 密钥安全

本文方案中的主密钥对都是通过随机数产生, 用户的私钥是由密钥生成中心通过主私钥与用户的标识计算生成, 且私钥由用户加密后存储在自己的设备上, 只用于数字签名和公钥加密, 既不会被泄露, 也避免被窃取.

(2) 中间人攻击

本文方案是基于 DH 算法和标识密码技术的双向认证方案. 在第 1 阶段的身份验证中, 通信双方通过 DH 算法协商的验证因子经过了非对称加密过后进行传输, 用户的私钥都存储在本地, 不在网络上进行传输, 可以有效地防止攻击者的窃听行为. 在第 2 阶段的身份验证中, 主私钥与用户标识产生的签名私钥对数据产生数字签名, 中间人即使伪造了标识, 也无法伪造数字签名. 因此, 不能通过仿冒或欺骗等手段达到窃取用户间的通信信息这一目的.

(3) 重放攻击

本文方案中验证因子和密钥对都是由随机数计算而来, 加密验证因子产生的密文也是由随机数计算而来, 可通过随机数的信息来识别和确定是否是重放信息, 从而避免重放攻击.

(4) 前向安全

本文方案中, 密钥是由 KGC 通过主私钥和用户的标识结合产生, 而每次加密密钥或签名密钥都是随机的、不同的, 且每次认证时必须使用对方的标识, 标识若是伪造的将造成认证失败. 密钥的随机性以及标识的全过程参与成为了系统安全的保障. 信息也都是经过加密后再进行传输, 所以不会造成以前通信时产生的会话密钥被泄露, 也不会泄露以前通信的内容.

## 3 实验结果及分析

服务器的基本配置: CPU i3-2120U, 主频 3.30 GHz, 内存 4.00 GB, 硬盘 931.51 GB, IP 地址为 202.101.72.84. 同时在服务器上部署了一个基于 Java 开发的双向身份验证系统, 该系统主要用于 BAS 方案的实验论证.

在 BAS 方案的可行性及正确性测试中, 选取两个用户 $A$ 和 $B$ 进行认证测试, 其中用户 $A$ 和用户 $B$ 计算验证因子后由用户 $B$ 加密自己的验证因子发送给用户 $A$ 进行验证. 表 2 为实验具体参数.

用户 $A$ 收到用户 $B$ 加密的密文 $C$ 后, 对其进行解密并验签, 解密成功后得到用户 $B$ 的验证因子$V_2'$, 用户 $A$ 将$V_2'$与自己的验证因子$V_1$进行分析比较, 二者数值相同即为验签成功. 表 3 为具体实验参数.

用户 $B$ 的身份验证成功后, 用户 $A$ 获取消息$M$(患者身份信息) 的数字签名并发送给用户 $B$ 以验证自己的身份, 表 4 为用户 $A$ 数字签名实验具体参数.

用户 $B$ 收到消息$M'$及其数字签名$(h', S')$, 通过计算得到$h_2$, 且若等式$h_2 = h'$成立, 即为验证成功. 表 5 为详细验签内容.

## 4 结语

对于电子病历的跨区域共享中通信双方身份验证的需求, 本文提出的基于 SM9 算法的双向身份验证方案, 改变了传统 PKI 身份验证的流程, 使用“验证因子+数字签名”的方式实现了用户的双向认证. 且该方案中, SM9 算法无需预先与协商密码者交换 CA 证书, 减少了申请和验证环节, 满足跨域用户安全通讯的需求. 本文方案在满足正确性的基础上安全可靠, 在跨域医疗协同这一应用场景下具有一定的研究价值和应用前景, 能够有效的避免因用户的身份验证问题造成患者的就诊信息被泄露. 在接下来的研究中将将继续对 SM9 算法的相关计算进行优化, 提高验证效率.

表 2 BAS 方案用户 *B* 加密验证因子实验参数

| 名称 | 数据 |
|---|---|
| 加密主私钥 | 229EAAB40498E2F1094554644EA520C27E6CF885EEABFFC5E633FD104AEDCBDF |
| 加密主公钥 | 7A1B58ECB8B4433415B6D7D2AC49EA91179B9B3665FC44F073CF0D5FCFD7F459A215B1CFC8936D262C91262E96C84483B5DB84BD7F2E04D171BCED6D7AA2A1F8 |
| 加密私钥 | A2F8A22D01870F12EE5E8B704A0FA0725FC64B4274E47D61E23C4D1DDCA8C76863524078F5D5F4EE8E970A07AD78BD352F7FC19C38F882FECE90002D157BE79F2C7B341B5F770DC9376AB9443436023B86DE591D93C11654D42FC932B65F49C964FE21C45FD6E7C30F582AED58ABAFB07754BE703C98D3DD8E7256FFEEF5AEE2 |
| 待加密验证因子$V_2$ | 72252EB99811B2D459262E2429E35BC5E318A02EBF0C4E34EAC351B6DC5BD1A13F786B61ADABBEBCA707E27542F55EF6963EB2422B93AFE28A0416183D32587D08A137D88FBEC6D99A786FCFD2B4909CA0BF237FBBC4344649BF0F555337514A95FB20D2233E28F2183CF99FD279EEE6D5DC4E13CEA1F5683E02F565A24AB3EC |
| 密文$C$=$C_1$‖$C_3$‖$C_2$ | 9D2FC7C5F8A1863372D759D78A614536B20747CDD83CB61242A583D80279F5B7A2A36CEB9FB341A8A5ABD2B0EC3F4823C9A26097E7014E15EAAD529C6C0172BA6CE51BC736D51728F229AA78DC14CF478F1B8370D35C527520697E73866A73AF8C0DEA7750F3F2E8643F39AA5025DD6FA070E02FCB600528A7719EBE8CBE822CCD17A82E9F3E9C427D348BE64EC44CB8F1C7647E65E9AB9BAFE937CDB6F4E9ECA01160AB70E0E525AB535396FFE40A5248DDCF43D281EF628E19444690E2BCB0E9E0844CE60EE8DF50D9C7EC9363BB6F590AB213E2B0BDC2BB2562EA360E82FF79559B16E5BCBCA08F7A1426561FCE64DD596F06437C14D255F37722F9C406557FAD2C16520D327D9AED3C86C40F8F6BA8EBF5331442E0104AED3CEB9BE7F2FF8050DD8B445742E3447F9750245A0A28B00DA2138F55C1A3D24E64F13500FC2D8B2DE8B90FC10883B83B21BAD2CCD8AD2204903BD2D1E8A98B9D0E3AF1855925D0D74E9D0E452A82D2C6F59CB90DE6C9 |

表 3 用户 *A* 解密实验参数

| 名称 | 数据 |
|---|---|
| 密文$C$数据$C = C_1‖C_3‖C_2$ | 9D2FC7C5F8A1863372D759D78A614536B20747CDD83CB61242A583D80279F5B7A2A36CEB9FB341A8A5ABD2B0EC3F4823C9A26097E7014E15EAAD529C6C0172BA6CE51BC736D51728F229AA78DC14CF478F1B8370D35C527520697E73866A73AF8C0DEA7750F3F2E8643F39AA5025DD6FA070E02FCB600528A7719EBE8CBE822CCD17A82E9F3E9C427D348BE64EC44CB8F1C7647E65E9AB9BAFE937CDB6F4E9ECA01160AB70E0E525AB535396FFE40A5248DDCF43D281EF628E19444690E2BCB0E9E0844CE60EE8DF50D9C7EC9363BB6F590AB213E2B0BDC2BB2562EA360E82FF79559B16E5BCBCA08F7A1426561FCE64DD596F06437C14D255F37722F9C406557FAD2C16520D327D9AED3C86C40F8F6BA8EBF5331442E0104AED3CEB9BE7F2FF8050DD8B445742E3447F9750245A0A28B00DA2138F55C1A3D24E64F13500FC2D8B2DE8B90FC10883B83B21BAD2CCD8AD2204903BD2D1E8A98B9D0E3AF1855925D0D74E9D0E452A82D2C6F59CB90DE6C9 |
| 用户$A$的验证因子$V_1$ | 72252EB99811B2D459262E2429E35BC5E318A02EBF0C4E34EAC351B6DC5BD1A13F786B61ADABBEBCA707E27542F55EF6963EB2422B93AFE28A0416183D32587D08A137D88FBEC6D99A786FCFD2B4909CA0BF237FBBC4344649BF0F555337514A95FB20D2233E28F2183CF99FD279EEE6D5DC4E13CEA1F5683E02F565A24AB3EC |
| 用户$B$的验证因子$V_2'$ | 72252EB99811B2D459262E2429E35BC5E318A02EBF0C4E34EAC351B6DC5BD1A13F786B61ADABBEBCA707E27542F55EF6963EB2422B93AFE28A0416183D32587D08A137D88FBEC6D99A786FCFD2B4909CA0BF237FBBC4344649BF0F555337514A95FB20D2233E28F2183CF99FD279EEE6D5DC4E13CEA1F5683E02F565A24AB3EC |

表 4 BAS 方案用户 *A* 数字签名实验参数

| 名称 | | 数据 |
|---|---|---|
| 签名主公钥 | | 938A991257C64A39DCAD11151FF32D078F25C3E5B440B2255222CD25AA79C08E1DD5C78DB316EFDD73D15BA5B35319EDFAA771C56AEC5B50B163A1D33F4A18DE7457988E45BBC1071C30435B73E2E2935D4957E37A4B3C3F230DAF107D8AD156B3CD56F4DDAB1F9B0A8EB340041B0056FF6A2389F118E7045B12D4D1221AEADC |
| 签名主私钥 | | 4F5A23580005A9D318FAA97C18F1FE082BBABA6620AF6AA4D60D9D77157D1B44 |
| $A$的签名私钥 | | A5702F05CF1315305E2D6EB64B0DEB923DB1A0BCF0CAFF90523AC8754AA6982078559A844411F9825C109F5EE3F52D720DD01785392A727BB1556952B2B013D3 |
| 待签名消息$M$ | | 张三, 3354672 |
| 消息$M$的数字签名($h$, $S$) | $h$ | 2F306A69D0E7525C54077942254C2FE314B98578FC2AC1E92E0CFEF920CE8714 |
| | $S$ | 1C3846EFFA43BBCF5B92BCD5B645CD453EBF88D848EF530BD59C4FF77581FE736A1FC3AD82ACDB4705E8A1D89FCA9869ECF50B745CE9558DB70B5BDB25176D50 |

表 5 用户 $B$ 验证数字签名实验参数

| 名称 | | 数据 |
|---|---|---|
| 用户$A$的标识 | | Alice |
| 用户$B$收到的数字签名$(h',S')$ | $h'$ | 2F306A69D0E7525C54077942254C2FE314B98578FC2AC1E92E0CFEF920CE8714 |
| | $S'$ | 1C3846EFFA43BBCF5B92BCD5B645CD453EBF88D848EF530BD59C4FF77581FE736A1FC3AD82ACDB4705E8A1D89FCA9869ECF50B745CE9558D B70B5BDB25176D50 |
| 用户$B$计算的$h_2$ | | 2F306A69D0E7525C54077942254C2FE314B98578FC2AC1E92E0CFEF920CE8714 |

## 参考文献


1 刘欢. 跨域认证与授权系统的设计与实现 [ 硕士学位论文 ]. 西安: 西安电子科技大学, 2014.

2 赵玉超. 一种基于非对称加密算法的安全高效身份认证协议. 工业技术创新, 2020, 7(6): 103–107.

3 刘怀兰, 侯昕, 王佳. 改进的基于 USBKey 的动态身份认证方案. 华中科技大学学报 (自然科学版), 2010, 38(11): 41–43.

4 董艳花, 张树美, 赵俊莉. 基于深度神经网络的有遮挡身份验证. 青岛大学学报 (自然科学版), 2021, 34(2): 45–52.

5 王霏, 陈明. 完美前向安全的基于身份认证密钥协商方案. 密码学报, 2020, 7(1): 56–68.

6 封化民, 孙铁茹, 孙莹. 基于身份认证加密的私钥共享方案及其应用. 计算机应用研究, 2014, 31(5): 1507–1510. [doi: 10.3969/j.issn.1001-3695.2014.05.054]

7 李郁林. 一种基于动态令牌的双向认证方案. 信息与电脑, 2019, 31(24): 211–212.

8 宋芹芹, 袁泉. PKI/CA 系统异地统一身份认证研究与实现. 网络安全技术与应用, 2017, (6): 54–55. [doi: 10.3969/j.issn.1009-6833.2017.06.033]

9 光笑黎, 张露露, 刘继增. 一种轻量级基于证书的认证密钥协商方案. 计算机系统应用, 2021, 30(1): 264–269. [doi: 10.15888/j.cnki.csa.007806]

10 方明. 异地协同研发过程中基于分布式 PLM 的数据交换研究 [ 硕士学位论文 ]. 武汉: 华中科技大学, 2017.

11 Kamil IA, Ogundoyin SO. A lightweight mutual authentication and key agreement protocol for remote surgery application in tactile Internet environment. Computer Communications, 2021, 170: 1–18. [doi: 10.1016/j.comcom.2021.01.025]

12 赖建昌, 黄欣沂, 何德彪, 等. 基于商密 SM9 的高效标识签密. 密码学报, 2021, 8(2): 314–329.

13 Sharma K, Agrawal A, Pandey D, *et al*. RSA based encryption approach for preserving confidentiality of big data. Journal of King Saud University—Computer and Information Sciences. In Press. [doi: 10.1016/j.jksuci.2019.10.006]

14 Dijesh P, Babu SS, Vijayalakshmi Y. Enhancement of e-commerce security through asymmetric key algorithm. Computer Communications, 2020, 153: 125–134. [doi: 10.1016/j.comcom.2020.01.033]

15 Hoobi MM, Sulaiman SS, AbdulMunem IA. Enhanced multistage RSA encryption model. IOP Conference Series: Materials Science and Engineering, 2020, 928(3): 032068.

16 赵奕捷. 基于标识密码 (IBC) 的私钥分发和双向认证研究. 江苏通信, 2020, 36(6): 70–75. [doi: 10.3969/j.issn.1007-9513.2020.06.018]

17 甘植旺, 廖方圆. 国密 SM9 中 R-ate 双线性对快速计算. 计算机工程, 2019, 45(6): 171–174.

18 王明东, 何卫国, 李军, 等. 国密 SM9 算法 R-ate 对计算的优化设计. 通信技术, 2020, 53(9): 2241–2244. [doi: 10.3969/j.issn.1002-0802.2020.09.025]