Computer Science and Application 计算机科学与应用, 2025, 15(4), 252-259
Published Online April 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.154097

Hans汉斯

面向医疗数据共享的匿名认证密钥交换方案

车　航，岳笑含

沈阳工业大学信息科学与工程学院，辽宁 沈阳

收稿日期：2025年3月15日；录用日期：2025年4月14日；发布日期：2025年4月22日

摘　要

随着信息技术的快速发展，数据安全和用户的隐私越发受到重视。本文提出了一种匿名认证密钥交换(Anonymous Key Exchange, AKE)协议，旨在为医疗场景下的医疗数据共享和患者身份隐私提供安全和隐私的保护。该方案通过使用累加器、零知识证明和关联数据加密等技术，实现用户匿名的认证和安全的会话密钥协商，有效防止敌手对于用户和医用物联网设备的攻击，还能抵御诚实且好奇的医疗机构对患者身份的猜测。相较于现有的方案提供了更强的隐私安全保护，并且很好地平衡了性能和安全性，具有重要的理论价值和意义。

关键词

密钥交换，身份认证，累加器，零知识证明

Anonymous Authenticated Key Exchange Scheme for Medical Data Sharing

Hang Che, Xiaohan Yue

School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: Mar. 15th, 2025; accepted: Apr. 14th, 2025; published: Apr. 22nd, 2025

Abstract

With the rapid development of information technology, data security and user privacy have been paid more and more attention. This paper proposes an Anonymous authenticated Key Exchange (AKE) protocol to provide security and privacy protection for medical data sharing and patient identity privacy in medical scenarios. By using accumulator, zero-knowledge proof and associated data encryption technology, the scheme realizes anonymous user authentication and secure session key agreement, which effectively prevents adversaries from attacking users and medical IoT devices, and can resist honest and curious medical institutions from guessing the patient's identity. Compared

文章引用: 车航, 岳笑含. 面向医疗数据共享的匿名认证密钥交换方案[J]. 计算机科学与应用, 2025, 15(4): 252-259.
DOI: 10.12677/csa.2025.154097

with the existing schemes, it provides stronger privacy security protection, and a good balance between performance and security, which has important theoretical value and significance.

Keywords

Key Exchange, Authentication, Accumulator, Zero-Knowledge Proof

Copyright © 2025 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

为了提高医疗资源的利用率，使处在偏远地区的用户能够享受到优质的医疗资源，各种医疗数据共享和协作医疗网络方案被提出。然而，随着隐私保护意识增强，现有方案大多无法满足对更高隐私保护的需求。此外，随着物联网设备在医疗中越来越广泛的研究和使用，物联网设备的安全性也走入了人们的视野，医用物联网设备也存在着丢失和被破坏的可能，会导致身份冒充和医疗数据丢失或被窃取的风险。

建立安全可靠的通信信道是安全的进行数据共享的方式之一，而如何安全地在各个实体之间建立数据共享信道是密钥交换方案主要解决的问题。近年来，国内外在物联网(IoT) [1]-[3]、无线医疗传感器网络(WMSN) [4]-[7]和工业物联网(IIoT) [8]等领域的匿名认证密钥交换方案取得了大量的进展。在物联网环境中，轻量级的密钥交换方案成为研究热点，关联数据加密(AEAD)和物理不可克隆函数(PUF)技术被应用于匿名认证密钥交换方案中。但密钥交换方案在使用物联网设备的场景中仍面临一些安全漏洞和计算开销的挑战。例如，为了保护用户行为不可追溯，Das 等人[9]提出了使用动态 ID 技术的轻量级身份验证协议，但由于设计简单而难以避免很多已知的攻击。随后，提出了许多基于动态 ID 的身份验证方案[10]-[13]。后续改进方案中，Xie 等人[13]使用公钥加密 ID 来实现匿名性，并抵御同步攻击，而 Kumari [14]等人则通过假名来提升方案安全性，但匿名性问题仍未完全解决。在 V2G 网络中，为了实现匿名的身份验证，已经提出了很多认证密钥交换方案，现有认证密钥交换(AKE)方案虽然提供了安全的数据交换机制，但仍普遍存在计算成本高、易受中间人攻击(MITM)和重放攻击等问题。Gope 和 Sikdar [15]提出的隐私 AKE 方案在成本效益上有所突破，但仍存在登录不同步和冒充攻击的漏洞，后续 Irshad 等人[16]则通过改进方案进一步增强了安全性。在无线医疗传感器网络(WMSN)中，针对植入式传感器节点的资源受限特性，研究者提出了基于 PUF 和生理数据的轻量级双向认证与密钥协商方案[17]，显著降低了通信和存储成本。然而，现有方案如 Turkanovic 等人[18]的轻量级认证协议在匿名性和不可链接性保护方面存在不足，Farash 等人[19]和 Yuanbing 等人[20]提出的方案逐步解决了特权内部攻击和离线密码猜测攻击等问题。在工业物联网(IIoT)领域，随着边缘计算的兴起，区块链技术被广泛应用于跨域认证[21]-[23]，解决了传统证书颁发机构(CA)的瓶颈问题。Rani 等人[24]提出的基于区块链的匿名认证密钥交换方案，使用财团区块链实现用户身份跨域认证。

针对现有的隐私安全问题，本文提出了一种基于协作医疗网络的匿名认证密钥交换方案，在满足用户身份认证性的同时也提供了隐私性和不可链接性的保护。本方案首先围绕协作医疗数据共享网络，根据用户、医疗机构和物联网设备等实体的功能需求给出了方案的系统模型并针对相应的安全及隐私需求给出了安全模型和形式化定义。然后利用零知识证明、ASCON 加密、累加器以及区块链等密码学工具给

出了方案的构建。

最后，本文设计并实现了面向医疗数据共享支持匿名性和不可链接性的身份认证方案的系统，给出了性能分析结果，该结果表明所提出的方案较现有同类方法存在安全性、功能性及性能三个维度均有不同的提高，可以有效解决医疗数据共享方案中存在的隐私问题，因此具有一定的实际应用意义。

2. 基础知识

2.1. 零知识证明系统

在零知识证明中，证明者 $\mathcal{P}$ 需要向验证者 $\mathcal{V}$ 证明其持有的陈述是正确的，并且保证验证者除了能够确定陈述的正确性以外，不能从证明中获取任何知识。

令 R 表示一种有效的可计算的关系(Relationship)且满足$(x, w) \in R$，x 是陈述(Statement)，w 是证据(Witness)。$L=\left\{x \middle| \exists w\ s.t. R(x, w)=1\right\}$，其中 L 是满足 R 的 NP 语言。如果一对概率多项式时间内的算法 $\langle\mathcal{P}, \mathcal{V}\rangle$ 是零知识的，则满足以下性质：

1) 完整性(Completeness)：对于任意$(x, w) \in R$，满足 $Pr\left[\langle\mathcal{P}, \mathcal{V}\rangle(x) \rightarrow 1\right]$。

2) 可靠性(Soundness)：对于任意 $x \notin L$，$(x, w) \notin R$ 及任何不诚实的证明者 $\mathcal{P}^*$，都满足 $Pr\left[\left\langle\mathcal{P}^*, \mathcal{V}\right\rangle(\mathrm{x}) \rightarrow 1\right] \leq negl(\cdot)$。

3) 零知识性(Zero-knowledge)：对于任意 $x \in L$，模拟器 $\mathcal{S}$ 及陷门 τ，满足 $P(x, w)$，即验证者不会学到任何关于证据的知识。

2.2. ASCON 加密

ASCON 是一种轻量级的关联数据加密算法，专为资源受限设备设计。它具有单次处理和无逆运算的特点。单次处理意味着在一次操作中同时完成加密和认证，提高了效率；无逆运算的设计避免了复杂的逆运算，适合硬件实现。

ASCON 的加密过程可以描述为：$(CT, MAC)=EK(N, AD, PT)$。

其中，EK 表示加密操作，输入为共享密钥 K、随机数 N、关联数据 AD 和明文 PT，输出为密文 CT 和消息认证码 MAC。

ASCON 的解密过程可以描述为：$(PT, \perp)=DK(N, AD, CT, MAC)$。

其中，DK 表示解密操作，输入为共享密钥 K、随机数 N、关联数据 AD、密文 CT 和消息认证码 MAC。如果 MAC 验证成功，则输出明文 PT；否则，输出错误标志$\perp$。

2.3. 累加器

累加器是一种用于管理和验证集合成员关系的重要密码学工具，累加器将多个元素累加成一个较小的值，并且生成相应的证据$(witness)$，并允许用户通过累加器的成员证据$(witness)$，证明他所持有的元素是累加器的一部分，而不必透露集合中的其他成员。本文的方案中使用了一种基于强 RSA 假设的正动态累加器[25]，本文使用以下算法描述基本类型累加器：

$Gen\left(1^{\lambda}\right) \rightarrow\left(a_0, sk, m_0\right)$：选择两个 λ 位的素数 $p=2p'+1$ 和 $q=2q'+1$，其中 p' 和 q' 也是素数，计算 $n=pq$。累加器的私钥 $sk=p'q'$，随机选择一个整数 $a_0 \leftarrow \mathbb{Z}_n^*$，令 $a_0=a_0{}^2 mod\ n$，输出私钥 sk 和累加器值 a_0，m_0 为维护累加器可能需要的任何辅助值。

$Add\left(sk, a_t, x, m_t\right) \rightarrow\left(a_{t+1}, w_{t+1}^x, m_{t+1}, upmsg_{t+1}\right)$：对于加法和动态累加器，将元素 $x \in D$ 添加到累加器中(D 是累加器的域)，从而产生更新的累加器值 a_{t+1}，并产生元素 x 对应的成员证据 w_{t+1}^x，还要向所有

证据持有人发送一条广播消息 $upmsg_{t+1}$，旨在让所有证据持有人都能更新他们所持有的证据，此外还要更新辅助值 m_{t+1}。

$Del\left(sk, a_t, x, m_t\right) \to \left(a_{t+1}, u_{t+1}^x, m_{t+1}, upmsg_{t+1}\right)$：对于减法和动态累加器，从累加器中删除元素 $x \in D$，产生新的累加器值 a_{t+1} 和非成员证据 u_{t+1}^x，并更新辅助值 m_{t+1}，产生更新消息 $upmsg_{t+1}$。

$VerMem\left(a_t, x, w_t^x\right) \to 0/1$：使用成员证据 w_t^x 验证元素 x 在累加器中的成员资格，若验证成功，则返回 1，否则返回 0。

本文使用正动态累加器，只验证元素的成员证明，支持从累加器中增加和删除元素。

3. 匿名认证密钥交换方案设计

3.1. 初始化阶段

这一阶段是生成全局公共参数和各个实体的公私钥的算法。定义如下：

$\text{Setup}_{\text{RC}}\left(1^\lambda\right) \to pp$：由 RC 执行，以安全参数 λ 为输入，输出全局公共参数 pp。

$RCKeyGen_{RC}\left(pp\right) \to \left(pk_{RC}, sk_{RC}\right)$：由 RC 执行，以 pp 为输入，生成密钥对 $\left(pk_{RC}, sk_{RC}\right)$。

$\text{UsrKeyGen}_{\text{U}}\left(pp\right) \to \left(pk_U, sk_U\right)$：由用户 USER 执行，以 pp 为输入，输出用户的公私钥对 $\left(pk_{Usr_i}, sk_{Usr_i}\right)$。

$\text{HSKeyGen}_{\text{HS}}\left(pp\right) \to \left(pk_{HS}, sk_{HS}\right)$：由医疗机构 HS 执行以 pp 为输入，输出医疗机构的公私钥对 $\left(pk_{HS}, sk_{HS}\right)$。

$\text{ACCSetup}_{\text{HS}}\left(1^\lambda, pp\right) \to \left(a_{ACC}, sk_{ACC}\right)$：医疗机构调用累加器执行，以 pp 和 1^λ 为输入，输出累加器的私钥 sk_{ACC} 和累加器值 a_{ACC}，$\text{ACCSetup}_{\text{HS}}\left(\cdot\right)$ 只需要被调用一次，其生成的秘钥和累加器值由医疗机构成员之间共享。

$\text{IoTKeyGen}_{\text{IoT}}\left(pp\right) \to \left(k_{Dev_{IoT}}\right)$：由 IoT 执行，以 pp 为输入，生成医用物联网设备的加密密钥 k_{IoT}。

3.2. 注册阶段

在注册阶段，用户和物联网设备与医疗机构进行交互，进行身份合法性注册。

$\text{Reg}_{\text{Usr}}\left(pp, ID_i, BIO_i, pk_{Usr_i}, sk_{Usr_i}, rh\right) \to \left(id, a, R_a, pk_{Usr_i}, w_{rh}\right)$：该算法由用户 Usr_i 执行，生成私钥的持有型验证，向医疗机构证明用户拥有 pk_{Usr_i} 所对应的私钥 sk_{Usr_i}，并向医疗机构发送用户所选择的用于添加到累加器的撤销句柄 rh。

$\text{Verify}_{\text{HS}}^{\text{reg}}\left(id, a, R_a, pk_{Usr_i}\right) \to 0/1$：由 HS 调用，通过用户的公钥 pk_{Usr_i}，验证的中间参数 a，R_a，用户名 id_i，验证想要在医疗机构进行身份注册的用户的私钥持有性。

$\text{Add}_{\text{HS}}^{\text{reg}}\left(rh, sk_{\text{ACC}}, a_{\text{ACC}}\right) \to \left(w_{rh}, upmsg\right)$：医疗机构将用户的撤销句柄 rh，利用累加器的私钥 sk_{ACC} 和累加器的累加器值 a_{ACC} 添加到累加器，计算出用户的撤销句柄 rh 对应已添加到累加器的证据 w_{rh} 和更新消息 $upmsg$，本文使用的累加器只有在进行删除操作时才更新累加器的累加值，因此进行添加操作时，$upmsg = \perp$。并且将 $\left(a_{\text{ACC}}, rh, w_{rh}, upmsg\right)$ 返回给用户。

$\text{Reglog}_{\textbf{Usr}}\left(id_i, BIO_i, PW_i, sk_{Usr_i}, rh, w_{rh}\right) \to \left(\tau_i, CT, MAC\right)$：此操作由用户执行，生成用户登录信息，输入用户身份 ID_i、密码 PW_i、生物特征 BIO_i、撤销句柄 rh 和证据 w_{rh}，通过 ASCON 加密计算存储用户的私钥 sk_{Usr_i} 的密文 CT 和用于登录验证的消息认证码 MAC。

$\text{Reg}_{\text{IoT}}\left(ID_{IoT}, ID_{IoT}', k_{IoT}\right)$：由医用物联网设备执行，物联网设备将真实身份 ID_{IoT}，匿名身份 ID_{IoT}' 和加密密钥 k_{IoT} 发送给医疗机构进行注册，医疗机构将注册信息存入区块链。

3.3. 密钥交换阶段

密钥交换阶段包括用户登录，医疗机构与用户、医疗机构与物联网设备身份的相互认证，然后生成会话密钥，用于后续敏感医疗数据在用户、物联网设备和医疗机构三个实体之间的传输。

$\mathrm{Login}_{\mathrm{Usr}}\left(ID_i^*, PW_i^*, BIO_i^*, \tau_i, CT, MAC\right)\rightarrow\left(sk_{Usr_i}, rh, w_{rh}\right)/\perp$：此算法由用户执行，用户首先通过输入用户身份 ID_i、密码 PW_i、生物特征 BIO_i 和用户登录设备内存储的密文 CT 和用于登录验证的消息认证码 MAC，以及协助登录验证的参数，进行用户登录认证，只有拥有正确的用户身份 ID_i、密码 PW_i 和生物特征 BIO_i 的用户才能通过身份验证，并获得由 ASCON 加密方式存储的用户私钥 sk_{Usr_i}、撤销句柄 rh 和证据 w_{rh}，并进行后续的步骤，否则，验证不通过，终止进程。

$\mathrm{Auth}_{\mathrm{Usr}}\left(pp, rh, w_{rh}, a_{\mathrm{ACC}}, pk_{HS}, TS_1\right)\rightarrow\left(c, M_{U-H}, R_1, R_3\right)$：由用户调用，生成身份验证信息，输入用户的撤销句柄 rh、证据 w_{rh} 和累加器值 a_{ACC}，医疗机构的公钥 $pk_{HS,}$，时间戳 TS_1，输出密文 M_{U-H}，以及辅助认证参数 c、R_1 和 R_3。

$\mathrm{VerifyUsr}_{\mathrm{HS}}\left(c, M_{U-H}, R_1, R_3, sk_{HS,}, TS_1\right)\rightarrow 0/1$：此算法由医疗机构执行，输入辅助认证参数 cc、R_1 和 R_3，医疗机构的私钥 $sk_{HS,}$，密文 M_{U-H}，计算对称密钥 k_2，解密密文 M_{U-H}，获得撤销令牌 $RevTok_{rh}$ 与时间戳，通过零知识证明验证撤销令牌和时间戳，如果验证通过则进行后续步骤，否则终止。

$\mathrm{AuthtoIoT}_{\mathrm{HS}}\left(ID_{IoT}, ID_{IoT}^{'}, k_{IoT}, pk_{HS}\right)\rightarrow\left(C, r_4, MAC_1, TS_2, M_1\right)$：此操作由医疗机构执行，生成身份认证信息，输入目标物联网设备的真实身份标识 ID_{IoT}，用于匿名认证的临时身份标识 $ID_{IoT}^{'}$，物联网设备的加密密钥 k_{IoT} 和医疗机构的公钥 pk_{HS}，输出用于验证的消息 $\left(r_4, MAC_1, TS_2, M_1\right)$，$r_4$ 为辅助认证的参数，密文 C，$C:=\left(C_1\|C_2\|C_3\|C_4\right)$ 消息认证码 MAC_1，时间戳 TS_2，密文 M_1，密文 M_1 中包含密钥生成参数 k_2。

$\mathrm{VerifyHS}_{\mathrm{IoT}}\left(r_4, MAC_1, TS_2, M_1, ID_{IoT}^{'}, pk_{HS}, k_{IoT}\right)\rightarrow\left(C', MAC_1', k_2\right)/\perp$：物联网设备首先检验时间戳 TS_2，然后通过输入的辅助参数 r_4，消息认证码 MAC_1，密文 M_1，医疗机构公钥 pk_{HS}，加密密钥 k_{IoT}，输出密文 C'，设置 $C':=\left(C_1^{'}\|C_2^{'}\|C_3^{'}\|C_4^{'}\right)$，密钥生成参数 k_2，消息认证码 MAC_1'，如果 MAC_1' 与 MAC_1 不一致，则终止。

$\mathrm{GenSK}_{\mathrm{IoT}}\left(C_3', k_2, r_5\right)\rightarrow SK$：物联网设备执行，生成会话密钥。

$\mathrm{Auth}_{\mathrm{IoT}}\left(C_3', C_4', r_5, k_2, TS_3\right)\rightarrow\left(c_2, X\right)$：此算法由物联网设备调用，输入辅助参数 r_5，密文 $C_3^{'}$ 和 $C_4^{'}$，密钥生成参数 k_2，时间戳 TS_3，以验证消息 c_2，使用 $C_3^{'}$ 和 $C_4^{'}$ 将 r_5 秘密传输的密文 X 作为输出，并连同时间戳一并发送给医疗机构，作为物联网设备的身份认证信息。

$\mathrm{UpdateIoT}_{\mathrm{IoT}}\left(C_1^{'}, C_2^{'}\right)\rightarrow ID_{IoT}^{''}, k_{IoT}^{'}$：物联网设备更新加密密钥和临时身份。

$\mathrm{VerifyIoT}_{\mathrm{HS}}\left(C_3, C_4, k_2, X, TS_3, c_2\right)\rightarrow 0/1$：此算法由医疗机构执行，在此过程中通过传递过来的 X 和医疗机构计算生成的密文 C_3、C_4 解密出密钥生成参数 r_5，并结合时间戳 TS_3，密钥生成参数 k_2，验证消息 c_2 等验证物联网设备的身份，如果输出 1，则认为物联网设备为目标设备，并传递了正确的密钥生成参数 r_5。

$\mathrm{GenSK}_{\mathrm{HS}}\left(C_3, k_2, r_5\right)\rightarrow SK$：此算法由医疗机构调用，输入密钥生成参数，计算会话密钥。

$\mathrm{Enc}_{\mathrm{HS}}\left(R_1, sk_{HS}\right)\rightarrow M_2$：由医院调用，生成医疗机构向用户证明身份的认证信息。

$\mathrm{UpdateIoT}_{\mathrm{HS}}\left(C_1, C_2\right)\rightarrow ID_{IoT}^{''}, k_{IoT}^{'}$：医疗机构调用此算法更新存储的物联网设备加密密钥和临时身份。

$\mathrm{Dec}_{\mathrm{Usr}}\left(r_3, s_1, pk_{HS}, M_2\right)\rightarrow\left(C_3, ID_{IoT}, r_5\right)$：由用户调用此算法，验证医疗机构身份，并解密获得密钥生成参数 C_3 和 r_5 以及指明收集医疗数据需要使用的物联网设备的身份 ID_{IoT}。

$\mathrm{GenSK}_{\mathrm{Usr}}\left(C_3, s_1, pk_{HS}, r_5\right)\rightarrow SK$：由用户执行此算法，生成用于后续医疗数据在三个实体之间安全

传输的会话密钥 SK 。

4. 方案安全性及性能分析

4.1. 安全性分析

本节将对本文满足的用户匿名性、物联网设备匿名性、用户不可链接性、医疗数据的隐私性、会话密钥的前向安全性、抗重放攻击等进行非正式的安全性分析。

1) 用户匿名性：本方案采用零知识证明的方式实现用户的匿名性，正如 2.3 节所述，零知识证明可以在不泄露任何证据的情况下，使验证者相信该陈述是真实有效的。因此，在用户合法成员身份认证阶段，用户需要生成关于撤销句柄和证据的持有性证明，即撤销令牌 RevTok_{rh} 为证据。

本文通过采用 *Fiat – Shamir* 启发式零知识证明方案构建证明，使得医疗机构相信陈述的真实性。并由难题假设保障在概率多项式时间内不会有任何敌手能够从认证信息中获得用户的身份信息。

2) 身份相互认证性：医疗机构作为医疗服务的提供者，本文方案假设它在加入系统之前已经经过权威机构的身份验证，并具有公开的公钥。在这种情况下，当用户与医疗机构建立连接时，相互认证的安全性取决于认证信息的不可伪造性。在本文的方案中，撤销令牌和对称密钥的不可伪造就意味着用户生成的成员身份认证信息是不可伪造的，而 ASCON 加密很好的保障了物联网设备认证信息的不可伪造性，因此在本方案中只有授权的实体能够成功参加会话密钥的生成过程，协商会话密钥。

3) 物联网设备匿名性：在医疗机构与物联网设备相互认证的阶段，本方案采用 ASCON 加密结合动态更新物联网设备密钥和临时身份的思想，实现物联网设备的匿名性，只有同时持有物联网设备密钥和临时身份与真实身份的实体，才能认证彼此的身份，并通过 ASCON 加密保证认证信息的完整性和不可篡改性，由于在概率多项式时间内不会有任何敌手能够破坏 ASCON 加密，因此在概率多项式时间内不会有任何敌手能够破坏物联网设备的匿名性。

5) 医疗数据的隐私性和前向隐私：在本文方案中，在共享敏感的医疗数据之前，用户、医疗机构和物联网设备会通过密钥交换协商一个会话密钥，以此来加密后续通信的敏感医疗数据，保证医疗数据的隐私。如果敌手获取了当前时刻的会话密钥，敌手也无法通过当前的会话密钥推测出过去时刻的会话密钥并解密过去时刻用会话密钥加密通信的医疗数据。

6) 会话密钥的前向安全性：敌手会通过腐败用户的登录设备、物联网设备和医疗机构来获得实体中长期存储的信息，并且结合监听到的信息来推断过去成功协商的会话密钥，以此解密密文，获得用户的敏感医疗数据。身份认证和密钥协商的过程中，用户使用随机值生成会话密钥的生成参数，且患者的成员证据使用多认证因素加密存储在用户的设备内，增加了攻击的成本和难度。物联网设备使用动态的更新密钥和临时身份，并且敌手即使获得了当前时刻的物联网设备的密钥、临时身份和真实身份，由于 ASCON 加密、随机值和动态更新密钥和身份的思想的结合使用，敌手根据能够获取的信息也无法推测出过去的物联网设备使用的密钥和临时身份，更不能进一步推测出过去的会话密钥。因此，会话密钥的前向安全性得到了保证，进而保护了用户敏感的医疗数据。

7) 用户不可链接性：对于外部敌手，由于加密和随机数的使用，无法将窃听到的密钥交换消息链接到同一个源。而对于诚实且好奇的医疗机构，医疗机构会试图将获得的多个用户身份认证消息链接到同一个信息源，但是由于累加器结合零知识证明的使用，并且每次都使用不同的临时选择的随机子，医疗机构也无法通过获得的信息来推测消息的来源，保证了用户身份更强的隐私。

8) 可以抵御重放攻击、中间人攻击等常见攻击形式。为了抵御这些攻击，使用临时选择的随机值、时间戳和哈希函数，保证消息的新鲜度和完整性，而消息中包含着敌手无法伪造的信息，因此任何一个

敌手都不能采取这些攻击方式冒充合法用户破坏会话密钥的安全性。

4.2. 性能分析

表 1 给出了各个实体的理论时间代价。其中，T_a 代表 ASCON 加密，T_{em} 代表椭圆曲线点乘运算，T_{fe} 模糊提取器，T_{hf} 代表哈希函数，T_{se} 代表对称加密，T_{sd} 代表对称解密，T_{accs} 表示累加器初始化，T_{acca} 表示累加器添加，T_{accv} 表示累加器验证，T_{rtg} 表示撤销令牌生成，T_{rtv} 表示撤销令牌验证。

Table 1. Theoretical time cost
表 1. 理论时间代价

实体	理论时间代价
用户	$T_{fe}+5T_{em}+4T_{hf}+T_a+T_{se}+T_{sd}+T_{rtg}$
医疗机构	$3T_{em}+4T_{hf}+2T_{se}+T_a+T_{sd}+T_{rtv}$
物联网设备	$3T_{hf}+T_a+T_{sd}$
总计	$T_{fe}+8T_{em}+11T_{hf}+3T_a+3T_{se}+3T_{sd}+T_{rtg}+T_{rtv}$

5. 总结

本文提出了一种面向协作医疗网络数据共享的匿名认证密钥交换方案。该方案通过利用累加器、零知识证明、区块链、ASCON 加密而提升了整体安全性。与传统方案相比，本方案提供了更强的安全隐私保护，考虑了更多的实际安全需求。该方案不仅有效提升了用户身份的安全性，还具有较强的灵活性和可扩展性，适应现代医疗数据共享的多样化需求。

参考文献

[1] Chen, J., Zhang, Y. and Su, W. (2015) An Anonymous Authentication Scheme for Plug-In Electric Vehicles Joining to Charging/discharging Station in Vehicle-to-Grid (V2G) Networks. *China Communications*, **12**, 9-19. https://doi.org/10.1109/cc.2015.7084359

[2] Abbasinezhad-Mood, D., Ostad-Sharif, A., Mazinani, S.M. and Nikooghadam, M. (2020) Provably Secure Escrow-Less Chebyshev Chaotic Map-Based Key Agreement Protocol for Vehicle to Grid Connections with Privacy Protection. *IEEE Transactions on Industrial Informatics,* **16**, 7287-7294. https://doi.org/10.1109/tii.2020.2974258

[3] Zhang, Y., Zou, J. and Guo, R. (2020) Efficient Privacy-Preserving Authentication for V2G Networks. *Peer-to-Peer Networking and Applications*, **14**, 1366-1378. https://doi.org/10.1007/s12083-020-01018-w

[4] Wu, F., Xu, L., Kumari, S. and Li, X. (2015) An Improved and Anonymous Two-Factor Authentication Protocol for Health-Care Applications with Wireless Medical Sensor Networks. *Multimedia Systems*, **23**, 195-205. https://doi.org/10.1007/s00530-015-0476-3

[5] Das, A.K., Sutrala, A.K., Odelu, V. and Goswami, A. (2016) A Secure Smartcard-Based Anonymous User Authentication Scheme for Healthcare Applications Using Wireless Medical Sensor Networks. *Wireless Personal Communications*, **94**, 1899-1933. https://doi.org/10.1007/s11277-016-3718-6

[6] Amin, R., Islam, S.H., Biswas, G.P., Khan, M.K. and Kumar, N. (2018) A Robust and Anonymous Patient Monitoring System Using Wireless Medical Sensor Networks. *Future Generation Computer Systems*, **80**, 483-495. https://doi.org/10.1016/j.future.2016.05.032

[7] Ali, R., Pal, A.K., Kumari, S., Sangaiah, A.K., Li, X. and Wu, F. (2018) An Enhanced Three Factor Based Authentication Protocol Using Wireless Medical Sensor Networks for Healthcare Monitoring. *Journal of Ambient Intelligence and Humanized Computing*, **15**, 1165-1186. https://doi.org/10.1007/s12652-018-1015-9

[8] Cui, J., Zhu, Y., Zhong, H., Zhang, Q., Gu, C. and He, D. (2024) Efficient Blockchain-Based Mutual Authentication and Session Key Agreement for Cross-Domain IIoT. *IEEE Internet of Things Journal*, **11**, 16325-16338. https://doi.org/10.1109/jiot.2024.3351892

[9] Das, M.L., Saxena, A. and Gulati, V.P. (2004) A Dynamic Id-Based Remote User Authentication Scheme. *IEEE*

Transactions on Consumer Electronics, **50**, 629-631. https://doi.org/10.1109/tce.2004.1309441

[10] Wang, Y., Liu, J., Xiao, F. and Dan, J. (2009) A More Efficient and Secure Dynamic Id-Based Remote User Authentication Scheme. *Computer Communications*, **32**, 583-585. https://doi.org/10.1016/j.comcom.2008.11.008

[11] Chen, H., Lo, J. and Yeh, C. (2012) An Efficient and Secure Dynamic Id-Based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*, **36**, 3907-3915. https://doi.org/10.1007/s10916-012-9862-y

[12] Wen, F. and Li, X. (2012) An Improved Dynamic Id-Based Remote User Authentication with Key Agreement Scheme. *Computers & Electrical Engineering*, **38**, 381-387. https://doi.org/10.1016/j.compeleceng.2011.11.010

[13] Xie, Q., Wong, D.S., Wang, G., Tan, X., Chen, K. and Fang, L. (2017) Provably Secure Dynamic Id-Based Anonymous Two-Factor Authenticated Key Exchange Protocol with Extended Security Model. *IEEE Transactions on Information Forensics and Security*, **12**, 1382-1392. https://doi.org/10.1109/tifs.2017.2659640

[14] Kumari, S. and Renuka, K. (2019) Design of a Password Authentication and Key Agreement Scheme to Access E-Healthcare Services. *Wireless Personal Communications*, **117**, 27-45. https://doi.org/10.1007/s11277-019-06755-7

[15] Gope, P. and Sikdar, B. (2019) An Efficient Privacy-Preserving Authentication Scheme for Energy Internet-Based Vehicle-to-Grid Communication. *IEEE Transactions on Smart Grid*, **10**, 6607-6618. https://doi.org/10.1109/tsg.2019.2908698

[16] Irshad, A., Usman, M., Ashraf Chaudhry, S., Naqvi, H. and Shafiq, M. (2020) A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet Based Vehicle-to-Grid Technology Framework. *IEEE Transactions on Industry Applications*, **56**, 4425-4435. https://doi.org/10.1109/tia.2020.2966160

[17] Yu, S. and Park, K. (2024) PUF-Based Robust and Anonymous Authentication and Key Establishment Scheme for V2G Networks. *IEEE Internet of Things Journal*, **11**, 15450-15464. https://doi.org/10.1109/jiot.2024.3349689

[18] Turkanović, M., Brumen, B. and Hölbl, M. (2014) A Novel User Authentication and Key Agreement Scheme for Heterogeneous Ad Hoc Wireless Sensor Networks, Based on the Internet of Things Notion. *Ad Hoc Networks*, **20**, 96-112. https://doi.org/10.1016/j.adhoc.2014.03.009

[19] Farash, M.S., Turkanović, M., Kumari, S. and Hölbl, M. (2016) An Efficient User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Network Tailored for the Internet of Things Environment. *Ad Hoc Networks*, **36**, 152-176. https://doi.org/10.1016/j.adhoc.2015.05.014

[20] Yuanbing, W., Wanrong, L. and Bin, L. (2021) An Improved Authentication Protocol for Smart Healthcare System Using Wireless Medical Sensor Network. *IEEE Access*, **9**, 105101-105117. https://doi.org/10.1109/access.2021.3099299

[21] Lian, H., Pan, T., Wang, H. and Zhao, Y. (2021) Identity-Based Identity-Concealed Authenticated Key Exchange. In: *Lecture Notes in Computer Science*, Springer, 651-675. https://doi.org/10.1007/978-3-030-88428-4_32

[22] Libert, B., Paterson, K.G. and Quaglia, E.A. (2012) Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model. In: *Lecture Notes in Computer Science*, Springer, 206-224. https://doi.org/10.1007/978-3-642-30057-8_13

[23] Lin, H. (2017) Indistinguishability Obfuscation from SXDH on 5-Linear Maps and Locality-5 PRGs. In: *Lecture Notes in Computer Science*, Springer, 599-629. https://doi.org/10.1007/978-3-319-63688-7_20

[24] Rani, D. and Tripathi, S. (2023) Design of Blockchain-Based Authentication and Key Agreement Protocol for Health Data Sharing in Cooperative Hospital Network. *The Journal of Supercomputing*, **80**, 2681-2717. https://doi.org/10.1007/s11227-023-05577-6

[25] Baldimtsi, F., Camenisch, J., Dubovitskaya, M., Lysyanskaya, A., Reyzin, L., Samelin, K., *et al*. (2017) Accumulators with Applications to Anonymity-Preserving Revocation. 2017 *IEEE European Symposium on Security and Privacy* (*EuroS & P*), Paris, 26-28 April 2017, 301-315. https://doi.org/10.1109/eurosp.2017.13