一种面向中医药临床数据的区块链安全与隐私保护方案*

余　健，胡孔法**，丁有伟

（南京中医药大学人工智能与信息技术学院　南京　210023）

摘　要：目的　针对中医药医疗大数据实现数据共享，打通各环节流程，提高医疗数据的透明性、可追溯性，同时保障个人医疗数据的安全隐私，提出一种面向临床医疗数据的区块链安全与隐私保护方案。方法　通过区块链技术实现医疗数据的跨平台共享，本文提出一种基于加法的同态加密和基于范围的零知识证明算法，来保证中医药大数据的安全性和合法性。结果　在区块链对临床医疗数据存储场景下，各个中医院和医保中心可以对患者医疗数据进行共享访问，同时本文提供的同态加密和零知识证明算法具备很好的性能。结论　为了满足各个医疗平台之间的患者医疗数据的共享访问诉求，同时保障医疗数据的安全性和满足数据的可追溯性，必须借助于区块链技术才能完成。本文提出的基于paillier加法同态加密与基于环签名的范围零知识证明方案对临床医疗区块链的数据进行隐私保护。

关键词：中医药大数据　区块链　同态加密　零知识证明　离链通道　共识算法

doi: 10.11842/wst.20210319009　　中图分类号：R2-031　　文献标识码：A

1　引言

随着计算机技术和医疗信息技术的发展，各个中医院和中医药医疗机构面临着医疗信息从封闭走向开放共享的诉求，跨平台实现医疗数据的开放与共享互通，可以提升患者的就医效率和医疗信息处理效率。医疗数据包含个人敏感医疗数据，以及重要的中医处方等敏感信息，这些个人敏感数据在网络共享和开放的过程中，存在着较大的个人隐私数据泄露[1]的风险，需要对医疗数据进行隐私保护。同时在患者存在着跨医院和医疗机构的场景，医疗费用需要跨平台结算，所以医疗费用的结算需要满足可追溯的要求。区块链的自身技术特点可以解决医疗数据的隐私保护问题，同时也满足医疗费用跨平台结算的可追溯的要求。

近年来，各国政府机构，开源组织产业联盟等在陆续投入区块链产业的拉通和应用，随着区块链的产业价值的逐渐确定，区块链的应用场景愈发广泛。区块链的应用已由最初的金融延伸到医疗健康、物联网、智能制造、供应链管理、数据存证及交易等多个领域，将为互联网医疗、云计算、大数据、承载网络等新一代信息技术的发展带来新的机遇。区块链因其通过分布式数据存储、点对点传输、共识机制、加密算法等技术的集成[2]，可有效解决传统交易模式中数据在系统内流转过程中的造假行为，从而构建可信交易环境，打造可信社会[3]。最初在比特币等公有链系统中，所有的交易信息都是公开的，因此大部分的区块链没有隐私性。但是在医疗行业，医疗数据和交易信息是

收稿日期：2021-03-19

修回日期：2021-09-16

*　科学技术部国家重点研发计划项目（2017YFC1703500）：中医药大数据中心与健康云平台构建，负责人：李国正；国家自然科学基金委员会青年科学基金（82004499）：基于区块链的中医临床大数据可信分析技术研究，负责人：丁有伟；国家自然科学基金委员会面上项目重点专项（82074580）：基于知识图谱的现代名老中医诊治肺癌用药规律及其机制研究，负责人：胡孔法。

**　通讯作者：胡孔法，博士生导师，教授，主要研究方向：物联网与云计算、中医药人工智能与大数据分析研究。

敏感数据，在区块链的传输和交易中会存在医疗数据泄露的问题，非业务相关方不能查看[4]，但同时需要满足第三方或者监管机构的监管要求。所以中医药临床数据区块链方案的目标是医疗数据和交易在合法的监管下实现数据的明文保护[5]，同时让共识节点可以在密文上检查交易数据的正确性，同时监管机构可以进行解密操作。

区块链是一系列现有成熟技术的有机组合，它对账本进行分布式的有效记录，并且提供完善的脚本以支持不同的业务逻辑。在典型的区块链系统中，数据以区块为单位产生和存储，并按照时间顺序连成链式数据结构，所有节点共同参与区块链系统的数据验证、存储和维护[6]。新区块的创建通常需得到全网多数节点的确认，并向各节点广播实现全网同步，之后不能更改或删除。区块链的这些特点可以有效降低互信的成本，构建去中心化的应用，但是区块链的数据是对全网公开的，对数据的读写是受到全网各个节点的监督[7]。医疗区块链领域的医疗数据是属于隐私数据，需要对医疗链上的医疗数据和交易信息进行加密保护[8-9]。传统的密码学关注的是“数据存储安全”，即在没有秘钥的情况下只有存储和传输加密结果，同态加密关注“数据处理”安全，支持对加密数据进行处理而不泄露任何原始信息[10-12]。医疗区块链中的加密数据处理都在云端高性能处理器上，如果采用传统的本地加密存储和数据处理存在效率低下的问题，而同态加密为医疗区块链的各节点的医疗数据安全和隐私保护提供了完美的解决方案。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一个方法处理未加密的原始数据得到的输出结果是一样的。由于就医高峰期的医疗数据量并发，对链上的加密数据的处理有性能的诉求，为了进一步提升医疗区块链的各节点数据处理的效率[13-14]，本文提出一种基于 paillier 同态加密和零知识证明算法，面向临床医疗数据的区块链安全与隐私保护方案，为医疗数据区块链的安全隐私提供更有效的保障，同时利用安全离链通道对医疗区块链进行传输扩容。

2　方法

全国存在着数量庞大的中医医院和机构，其医疗数据和电子病历数据库系统都是相互隔离和独立的，彼此之间是不能互相开放和共享。这些医疗数据信息包含健康数据、遗传病史、手机号码、身份证号码等病人的个人敏感医疗数据[15-16]，以及重要的中医处方等敏感信息，医疗区块链技术和解决方案可以解决各个中医医院医疗数据共享和安全的问题。

在医疗信息区块链解决方案中，病人在生病入院环节就会把病人的个人信息上链，包括姓名、身份证号码、年龄、性别、手机号等信息输入医疗信息区块链，这些属于个人敏感信息需要加密上链，只有病人自己和得到授权的医院可以进行查询，医生得到授权后就可以对病人的病例进行查询和治疗，患者的治疗信息也是属于敏感信息，同样需要加密后才能上链。如果病人需要治疗费用需要经过医保中心进行结算，

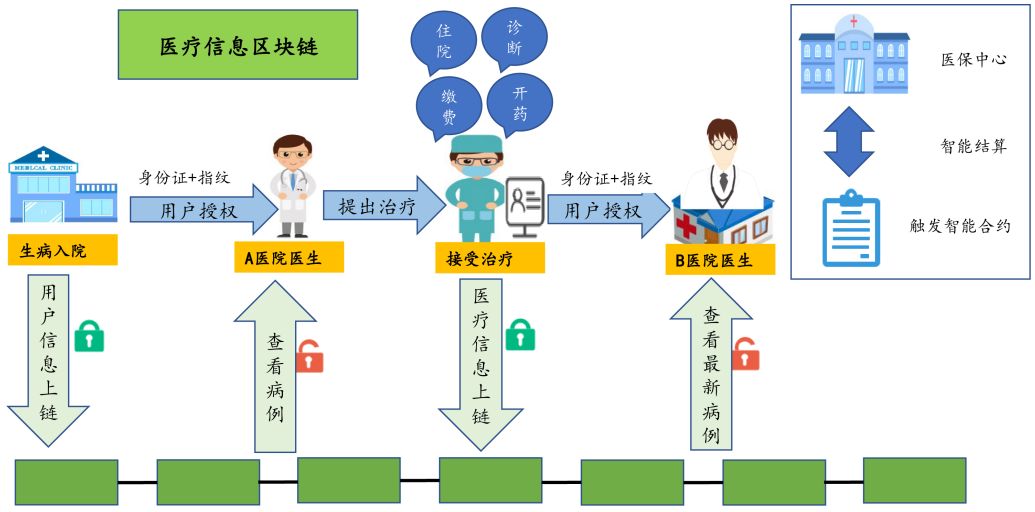

图1　医疗信息区块链

需要把病人个人信息和医疗费用信息授权给医保中心进行检查和结算。病人在各个中医医院、机构医疗的就诊和医疗信息上链的过程图1所示。

通过对医疗区块链的应用场景分析，归结出其主要诉求就是对个人隐私数据和医疗费用交易类的数据进行隐私保护，一般的医疗数据加密方案关注的都是数据存储安全，先对数据进行加密后再发送或者存储，只有拥有密钥的患者或者医疗机构才能够正确解密得到原始的内容，这个过程中是不能对加密数据做任何操作，只能进行存储和传输[17-18]。而同态加密方案关注的是数据处理安全，同态加密提供了一种对加密数据进行处理的功能，医疗信息区块链上的各个节点可以对加密数据进行处理，但是处理过程不会泄露任何原始内容。拥有密钥的医疗机构和患者对处理过的数据进行解密后，得到的正好是处理后的结果。同态加密是将原始的明文数据进行加密，然后在密文上进行各种算术运算，最终得到结果的密文，可以使用如下的形式语言进行描述和表示：

$$x_1, x_2, ..., x_n \xrightarrow{encrypt} [x_1], [x_2], ..., [x_n]$$

$$f([x_1], [x_2], ..., [x_n]) \longrightarrow f(x_1, x_2, ..., x_n)$$

其中$x_1, x_2, ..., x_n$是原始的明文数据，$[x_1], [x_2], ..., [x_n]$是加密后的密文数据，f是运算函数。由此可见，同态加密直接在密文上操作和在明文上操作然后加密，得到的效果是一样的。1999年Paillier发明的概率公钥加密系统就是支持加法同态的加密方案：

$$[x] := g^x r^n$$

$$[x] \cdot [y] = g^{x+y}(r_x r_y)^n$$

目前医疗机构的医疗信息IT化正在迅猛的发展，医疗数据有逐步上云的趋势，同态加密技术比较适用于运行在云计算平台上。患者和医生的电子病历和处方信息需要加密，数据处理和上链，但是移动终端或者计算机计算能力较弱，可以借助云平台来实现[19]。但是直接将数据传输给云端，需要保障数据的安全性，所以可以使用同态加密让云平台对加密数据进行直接处理，并将处理结果返回[20]。在医院就医的场景下，高峰期病人就医人数较多，对区块链系统的实时性要求较高。本文提出一种基于paillier加法同态加密与范围零知识证明算法的方案，对临床医疗区块链的数据进行进行隐私保护。

在本文提出的医疗区块链的系统方案中，零知识证明验证密文数据的合法性，使用同态加密[20-23]实现对密文数据进行更新。将同态加密和零知识证明算法应用到区块链，首先由系统加密算法对输入的个人隐私数据进行同态加密，同时生成相应的范围证明数据，这些范围证明数据可以用来证明医疗费用交易数据的合法性。这样在后续的医院和社保中心处理数据过程中，背书节点，链码端，提交节点看到的都是密文数据，同时背书节点可以通过零知识证明技术验证过程数据是否合法，非法伪造的数据将无法通过检验。链码端可以对同态加密后的数据进行同态加操作，完成病人账户的数据更新。整个交易过程只有病人自己可以看到明文数据，如果医院的医生需要查看，病人可以把公钥的授权给医生或者社保中心，医生和社保中心可以拿到公钥进行密文的解密操作，从而获得病人的个人医疗数据的明文数据，链上其他用户无法看到明文数据，为医疗区块链提供有效的隐私保护能力。

3 算法和方案

3.1 同态加密和零知识证明方案

假设有一个加密函数f，把医疗数据的明文A通过加密后变成密文数据A′，把明文B通过加密后变成密文数据B′，也就是存在函数f使得f(A) = A′，f(B) = B′，同时解密函数f^{-1}能够将f加密后的密文解密成加密前的明文。如果A′+ B′ = C′，使用解密函数f^{-1}对C′进行解密得到C，同时满足C = A + B，那么我们称f是个加法同态的加密函数，即满足f(A) + f(B) = f(A + B)的函数为加法同态加密函数，同理满足f(A) x f(B) = f(A x B)的函数为乘法同态加密函数，既满足加法同态又满足乘法同态的加密函数称为全同态加密函数。在满足医疗区块链的隐私安全的前提下，本文提出一种基于paillier加法同态加密算法和零知识证明的隐私保护方案，步骤如下：

①秘钥生成：

(1) 选取2个不同的素数p和q，取2个数的乘积$n = p \times q$

(2) 根据欧拉函数，当p和q为不同的素数时，有$\psi(n) = (p-1)(q-1)$,记为λ

(3) 选择随机整数g，$2 < g < n^2$，并且g和n互质

(4) 取$\mu = [L(g^{\lambda} \bmod n^2)]^{-1} \bmod n$，其中$L(x) = (x-1)/n$

(5) 令(n, g)为解密的公钥，(λ, μ)为加密的私钥

②加密函数Encrypt，待加密的数据为m，r为随机数，满足$0 < r < n$，并且和n互质，paillier加密函数为：$c = (g^m \ x \ r^n) \bmod n^2$

m为医疗数据的明文，包含电子病历、处方信息等数据，一般数据较大，在此对该大数据进行切割，然后把切割的数据进行加法同态加密，比如m数据切割为k段，切割后的数据为$m_1,\cdots,m_k$，然后对切割后的数据分别进行加密，得到加密后的数据$c_1,\cdots,c_k$。

③解密函数Decrypt

$m_i = L(c_i^{\lambda} \bmod n^2) \times \mu \bmod n$

④计算函数Evaluate

$D(E(m_1,r_1) \times E(m_2,r_2) \bmod n^2) = s_1 + s_2 \bmod n$

而对于切割后的分段明文数据来说，满足解密后的明文等于解密前各个切割段明文相加$m_1+m_2,+\cdots+m_k = s_1+s_2,+\cdots+s_k$。此处只验证一次所有输入明文之和等于所有的解密后的输出明文之和。

⑤零知识证明

同时零知识证明对每一次输入和输出的明文数据进行验证。

3.2 医疗客户端交易数据创建

在本文提出的基于同态加密和零知识证明的医疗数据隐私保护方案中，使用同态加密实现对密文数据进行更新，零知识证明验证密文数据的合法性；包含AHE（Additive Homomorphic Encryption，加法同态加密），EL-AHE（Proof of the equality of additive homomorphic encryption，加法同态加密相等性证明），EL-ENC（Proof of the equality of encrypted data，加密数据相等性证明）和ZKRP（Zero-Knowledge Range Proof，零知识范围证明）四个方面。

在医疗客户端，病人A输入生成包含个人敏感信息的医疗数据，在医疗数据上链之前，病人A需要具备：公钥（PK A），密钥（SKA）和本次医疗机构就诊的交易金额（T），同时从区块链中获取病人A医保卡的加密余额A 和医疗机构的公钥（PKB）。通过这些数据，病人A将计算以下内容：

3.2.1 创建新的加密余额：①使用SKA对余额进行解密；②余额A′ = 余额A-T；③使用PKA加密余额A′

3.2.2 创建余额证明：①余额A′的零知识范围证明（ZKRP），余额A′ > 0；②余额A′的加法同态加密相等性证明（EL-AHE），余额A′ = 余额A-T

3.2.3 创建交易：①交易A，通过PKA加密T；②交易B，通过PKB加密T

3.2.4 创建交易证明：①交易A的零知识证明（ZKRP），T>0；②交易A和交易B的加密数据相等性证明（EL-Enc），解密后的交易B =-解密后的交易A。

计算完成后，交易数据包括交易A，交易B，加密余额A′，EL-AHE，EL-Enc，ZKRP余额，ZKRP交易都发送给对等医疗机构点进行验证，病人客户端的加密和数据交易流程如图2所示。

3.3 对等医疗机构点验证

在病人客户端完成交易的数据创建之后，医疗数据区块链的隐私保护下一步动作就是对等医疗机构点接收医疗交易数据并对其进行验证。对等医疗点会从医疗数据区块链中提取以下内容：

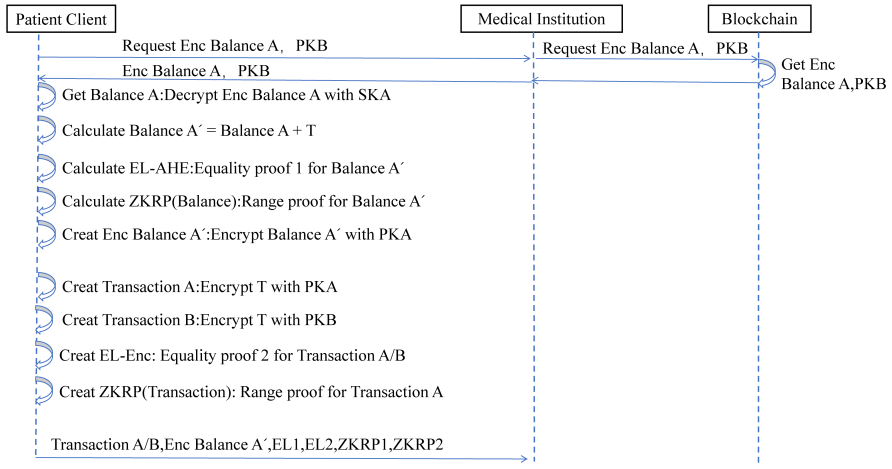

图2 客户端创建交易流程图

加密余额A，用于验证EL-AHE，交易数据校验包括：①范围验证（2a，使用交易ZKRP）：转入金额大于0；②范围验证（2b，使用余额ZKRP）：客户端病人A的新余额大于0；③相等性检查（2c，使用EL-Enc）：从发送方客户端病人提取的转移金额与存入接收医疗机构B的转移金额相匹配；④相等性检查（2d，使用EL-Enc）：客户端病人A的新余额等于其旧余额减去转移的金额；⑤交易来源（2e，使用EL-Enc）：只有客户端病人A才能从其余额中提取。在完成以上的验证流程后，需要对医疗区块链进行创建交易和新的加密余额，并将它们追加到区块链中，对等点会从区块链中提取对应的内容（图3）。

加密余额B，用于计算新的加密余额B，对等点将计算新的加密余额：①新的加密余额A由签名人创建，经过对等点的验证，被追加到区块链中；②通过AHE运算，使用旧的加密余额B和交易B计算新的加密余额B。

本方案通过病人医疗数据加密上链，并在医疗机构端进行数据的验证，以及把更新后的数据刷新到医疗区块链上，可以保证病人与医院之间的医疗数据和个人隐私信息的安全性，即医患双方及监管监管可以看到具体的医疗数据和医疗费用的交易信息，而区块链的其他患者和医院是不可见的，同时也配合审计或监管。同时在跨医疗机构平台的场景下，医疗区块链的医疗费用交易结算机制中，可以完成证明病人支付医疗费用输入的交易金额之和等于医院系统输出的交易金额之和，医疗费用输入的交易金额和医院系统输出的交易金额在有效的范围内，同时证明监管机构可以解密交易金额。由此可见，通过加法同态加密算法和零知识证明的区块链技术，可以有效的解决患者和不同医疗机构之间的数据共享和敏感个人医疗数据的隐私保护问题。

3.4 安全离链通道

区块链社区对交易扩容方案的争论与尝试由来已久，现有的主要方案包括区块扩容、共识算法改良、安全硬件辅助、隔离见证、闪电网络、交易状态分片、多层子链等。无论哪种方案都难以兼顾去中心化，可扩展性，安全性三个关键需求。值得注意的是区块链具有强应用相关性，在特定的应用场景仍可找到各要素间的平衡点以满足总体业务需求。在医疗区块链的医院和医保中心的医疗费用的结算中，小额医疗费用支付占据了大部分交易请求，同时存在就医高峰时段，这个时段会对主链的交易性能和延时提出极高的诉求。而小额医疗费用交易并无必要在主链及时获得确认，同样的应用也存在于共享经济中的小额支付场景。如果将海量小额交易在链下通道处理，交易过程不与主链交互，而在交易通道关闭或者交易方退出时才请求主链记录交易的最终状态，这将极大缓解主链的处理压力，这也是离链支付通道的设计思想。

医疗区块链如果要满足医疗数据区块链去中心化，可扩展性和安全性的诉求，也可以采取离链通道方案，在医疗区块链上锁定，在链下执行，交易双方的状态变化(资金分配比例)与交易执行过程由链上合约监督执行。医疗区块链的离链通道具体方案如

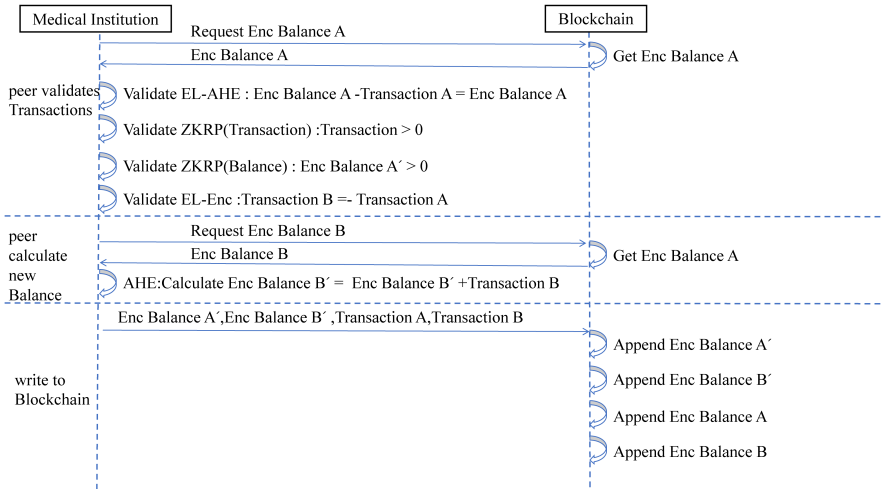

图3 对等点验证交易数据流程图

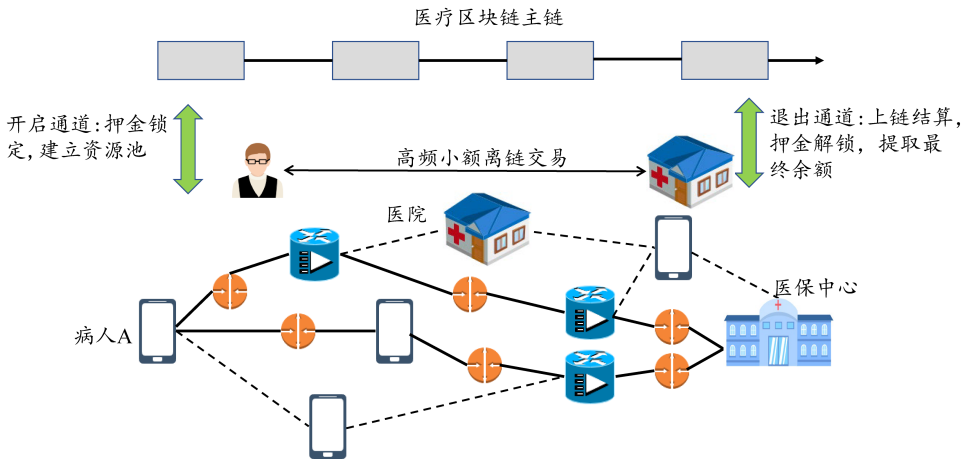

图4　病人A和医院/医保中心之间离链通道实现

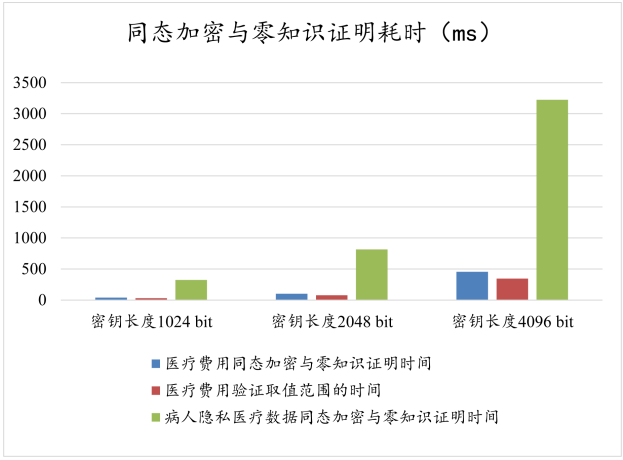

图5　同态加密与零知识证明耗时

下图4。

（1）医院和社保中心建立链下交易通道，由链上合约绑定链上资金形成交易押金池，医患双方初始状态（即交易方各拥有的资金数字）由链上合约锁定。

（2）链下交易过程中产生的新状态将淘汰旧状态，并由双方确认。双方在新状态产生时交换旧状态分配资金的解锁条件。

（3）医疗费用交易方实时监控链上状态，一旦一方将旧状态提交到主链进行退出操作，另一方可在允许的时间段内提交证据（如对方已签名的新状态和已交换的旧状态解锁条件），以扣除押金的方式对恶意行为进行惩罚。

单个离链交易通道是点对点模式，若医患双方没有直接交易通道，可以在其他节点间有交易通道的第三方组建一条临时交易路径，路径中的桥接第三方交易节点可以获取手续费。离链支付通道适用于两类应用场景，一是交易双方有高频小额交易需求，二是交易双方需要立即交易确认的需求。需要注意的是这里的确认仅是链下确认，交易方需要承担一定的风险，因此离链通道一般限制在微支付和双方有频繁交易需求的应用中。

4　实验结果

同态加密与零知识证明性能规格：医疗费用交易金额为256比特，病人隐私医疗数据长度为4096字节，密钥长度分别取1024比特、2048比特和4096比特。硬件配置为intel x86-cpu，i5 3.4GHZ 8GB RAM，cache size（缓存大小）为25600 KB，测试环境为64位的linux商用操作系统suse12 sp4 container内部运行测试，医疗数据集格式如表1所示。

在上述的软硬件环境下，本方案采用相同的数据集格式的基础上，针对不同的密钥长度对医疗数据集进行同态加密和零知识范围证明耗时计算。实验中在不同的密钥长度为1024bit，2048bit和4096bit的情况下，分别对医疗费用同态加密与零知识证明，医疗费用验证取值范围和病人隐私医疗数据同态加密与零知识证明三者的耗时进行计算和性能对比分析，三者的耗时如表2所示。

通过同态加密与零知识证明耗时的数据可以看到（图5），在密钥长度为4096 bit的情况下，病人隐私医疗数据同态加密与零知识证明时间的耗时达到4 s多，在医疗区块链对性能要求较高的场景下，这种耗时是不可行的。同时实验数据发现密钥长度为2048 bit场景下的耗时是密钥长度为1024 bit场景下耗时的

表1　医疗数据集格式

姓名	身份证号码	手机号码	邮箱	地址	交易金额	处方药
张三	1*********	131********	a*****@163.com	北京市朝阳区***	12.11	环丙沙星
李四	2*********	132********	b*****@163.com	北京市海淀区***	12.12	青霉素
王五	3*********	133********	c*****@163.com	南京市鼓楼区***	12.13	盐酸普鲁卡因
赵六	4*********	134********	1*****@qq.com	南京市建邺区***	12.14	头孢噻肟钠
刘七	5*********	135********	2*****@qq.com	南京市秦淮区***	12.15	血塞通
朱八	6*********	136********	3*****@qq.com	南京市玄武区***	12.16	头孢呋辛钠

表2　医疗数据的同态加密和零知识证明耗时

性能规格项	密钥长度1024 bit	密钥长度2048 bit	密钥长度4096 bit
医疗费用同态加密与零知识证明时间	40ms	102ms	453ms
医疗费用验证取值范围的时间	30ms	78ms	347ms
病人隐私医疗数据同态加密与零知识证明时间	359ms	903ms	4112ms

2.5倍，而密钥长度为1024 bit也能够满足医疗区块链的安全性要求，所以本文提出的基于加法同态加密和零知识证明的方案可以采用1024 bit的密钥长度来为医疗区块链提供数据的隐私保护和安全共享。离链通道交易系统，通过交易双方高效安全的握手协议，可以实现用户间单通道1000+TPS（每秒钟处理事务的数量）的交易性能。

在医疗系统的应用场景中，对区块链隐私保护方案的性能要求较高，由以上的实验数据可以看到密钥长度对医疗数据的同态加密和零知识证明的耗时影响较大。如果选择较长的密钥，在医疗区块链的认证节点较多的情况下会造成医疗数据处理和交易性能的急剧下降，所以在满足安全要求的前提下，选择合适的密钥长度对医疗区块链的实际应用非常重要。本文选择长度为1024 bit的密钥既能满足安全保护的要求，又能高效的支撑同态加密和零知识证明技术在医疗区块链场景下的应用。

5　小结

本文针对医疗数据在不同的医疗机构平台上的安全共享和隐私保护的场景，提出一种基于加法同态加密和零知识证明技术的医疗区块链解决方案。通过在软硬件平台上采取不同的密钥长度，对医疗数据进行分类验证和性能对比分析，选取适用于医疗区块链场景的数据集格式和密钥长度，同时对离链通道的系统进行性能测试和验证。本文提出的医疗区块链隐私保护方案是在点对点场景下对医疗数据进行加法同态加密和零知识证明的交易验证，后续将会对多节点的医疗区块链和多节点网络传输场景进行性能测试和方案验证，以继续提升医疗区块链的加密数据的处理性能，同时亦能达到医疗数据共享和隐私保护的目的。

参考文献

1　王利明. 数据共享与个人信息保护. 现代法学, 2019, 41(1):45-57.

2　刘滋润, 王点, 王斌. 区块链隐私保护技术. 计算机工程与设计, 2019, 40(6):1567-1573.

3　Lai J C, Mu Y, Guo F F, *et al*. Privacy-enhanced attributebased private information retrieval. *Inform Sci*, 2018, 454-455:275-291.

4　刘向宇, 王斌, 杨晓春. 社会网络数据发布隐私保护技术综述. 软件学报, 2014, 25(3):576-590.

5　Wang H Q, Wu Q H, Qin B, *et al*. FRR: fair remote retrieval of put sourced private medical records in electronic health networks. *J Biomed Inform*, 2014, 50(8):226 - 233.

6　Dorri A, Luo F, Kanhere S S, *et al*. SPB: A secure private blockchain-based solution for distributed energy trading. *IEEE Commun Mag*, 2019, 57(7):120-126.

7　祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述. 计算机研究与发展, 2017, 54(10):2170-2186.

8　薛腾飞, 傅群超, 王枞, 等. 基于区块链的医疗数据共享模型研究. 自动化学报, 2017, 43(9):1555-1562.

9　徐文玉, 吴磊, 阎允雪. 基于区块链和同态加密的电子健康记录隐私保护方案. 计算机研究与发展, 2018, 55(10):2233-2243.

10　Zheng Z B, Xie S A. Blockchain challenges and opportunities: a survey. *Int J Web Grid Serv*, 2018, 14(4):352-375.

11　Shen B Q, Guo J Z, Yang Y L. MedChain: efficient healthcare data

sharing via blockchain. *Appl Sci*, 2019, 9(6):1207.
12 Chen Y, Ding S, Xu Z, *et al*. Blockchain-based medical records secure storage and medical service framework. *J Med Syst*, 2019, 43(1):5.
13 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from(standard) LWE. *SIAM J Comput*, 2014, 43(2): 831-871.
14 Gentry C, Groth J, Ishai Y, *et al*. Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proof. *J Cryptol*, 2015, 28(4):820-843.
15 Fan K, Nana H, Wang X, *et al*. Secure and efficient personal health record scheme using attribute-based encryption. *Netw Appl*, 2017(2): 1-12.
16 余健, 胡孔法, 丁有伟. 一种面向中医药数据的高效脱敏算法. 世界科学技术-中医药现代化, 2020, 22(12):4169-4174.
17 胡荣磊, 何艳琼, 曾萍, 等. 一种大数据环境下医疗隐私保护方案设计与实现. 信息网络安全, 2018, 18(9):48-54.
18 Tu Y F, Xia F, Yang G. Access control for personal health records and support for attribute revocation. *J Chin Comput Syst*, 2017, 38(4): 834-838.
19 薛燕, 朱学芳. 基于改进加密算法的云计算用户隐私保护研究. 情报科学, 2016, 34(9):145-149.
20 Pass R, Seeman L, Shelat A. Analysis of the blockchain protocol in asynchronous networks. *Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer*, 2017:643-673.
21 陈志伟, 杜敏, 杨亚涛, 等. 基于RSA和Paillier的同态云计算方案. 计算机工程, 2013, 39(7):35-39.
22 李增鹏, 马春光, 周红生. 全同态加密研究. 密码学报, 2017, 4(6): 561-578.
23 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from(standard) LWE. *Proc of the 52nd Annual Symposium on Foundations of Computer Science. IEEE Press*, 2011:97-106.

A Blockchain Security and Privacy Protection Scheme for Traditional Chinese Medicine Clinical Data

Yu Jian, Hu Kongfa, Ding Youwei
(School of Artificial Intelligence and Information Technology, Nanjing University of Chinese Medicine, Nanjing 210023, China)

Abstract: Objective To share the data of Traditional Chinese Medicine (TCM) medical big data, open up all processes, improve the transparency and traceability of medical data, and ensure the security and privacy of personal medical data, and to propose a blockchain security and privacy protection scheme for clinical medical data. Methods Through the blockchain technology, the cross platform sharing of medical data was achieved. This paper proposed a homomorphic encryption algorithm based on addition and zero knowledge proof algorithm based on range to ensure the security and legitimacy of big data of TCM. Results In the scenario of blockchain storing clinical medical data, each hospital of TCM and medical insurance center shared and accessed the patient's medical data. At the same time, the homomorphic encryption and zero knowledge proof algorithm provided in this paper had good performance. Conclusion In order to meet the demands of patients' medical data sharing and access between various medical platforms, ensure the security of medical data and meet the traceability of data, it must be completed with the help of blockchain technology. This paper proposes a range zero knowledge proof scheme based on Paillier addition homomorphic encryption and ring signature to protect the data privacy of clinical medical blockchain.

Keywords: Big data of TCM, Blockchain, Homomorphic encryption, Zero-knowledge proof, Off blockchain channel, Consensus algorithm

（责任编辑：周阿剑、刘玥辰，责任译审：周阿剑，审稿人：王瑀、张志华）