基于区块链和轻量级秘密共享的IoMT高效隐私保护

Privacy Preserving in IoMT With Blockchain and Lightweight Secret Sharing

Chaoyang Li , Mianxiong Dong , Member, IEEE, Xiangjun Xin , Jian Li , Xiu-Bo Chen , and Kaoru Ota , Member, IEEE

目录 CONTENT

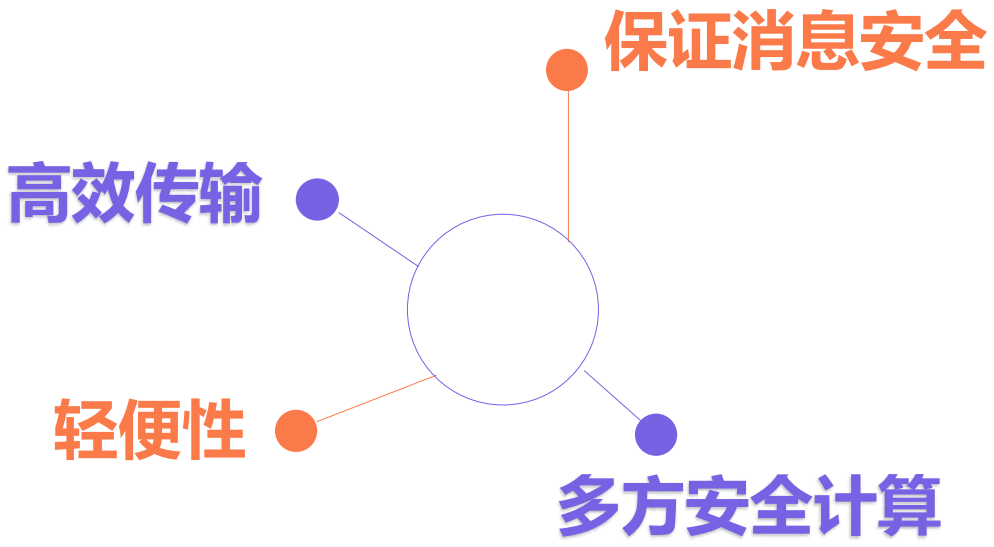
PART 01

背景与动机

Background and motivation for the study.

隐私泄露的威胁

IoMT数据共享过程中：**隐私泄露**、**数据丢失**和**低效共享**问题仍然很严重



当前共享方法的**局限性**：

- 基于高效共享：非加密设计易受攻击，导致隐私泄露
- 基于安全多方计算：复杂性较高，不适用于医疗设备

(t/n)-SS 方案的思路

思路：利用交错编码技术将原始消息的长度分割到 n 个小份额中，适用于更节能的数据传输和处理，它可以通过破坏数据的语义来保护隐私。
同时，它只需要少于 t（t ≤ n） 个份额即可恢复原始密钥，使共享过程更加高效。

效果：对 IoMT 中事务处理的性能评估表明，所提出的模型非常稳定。仿真和性能评估结果表明，与同类文献相比，该 t/n-SS 方案具有节能、节省存储和较强的容错性。

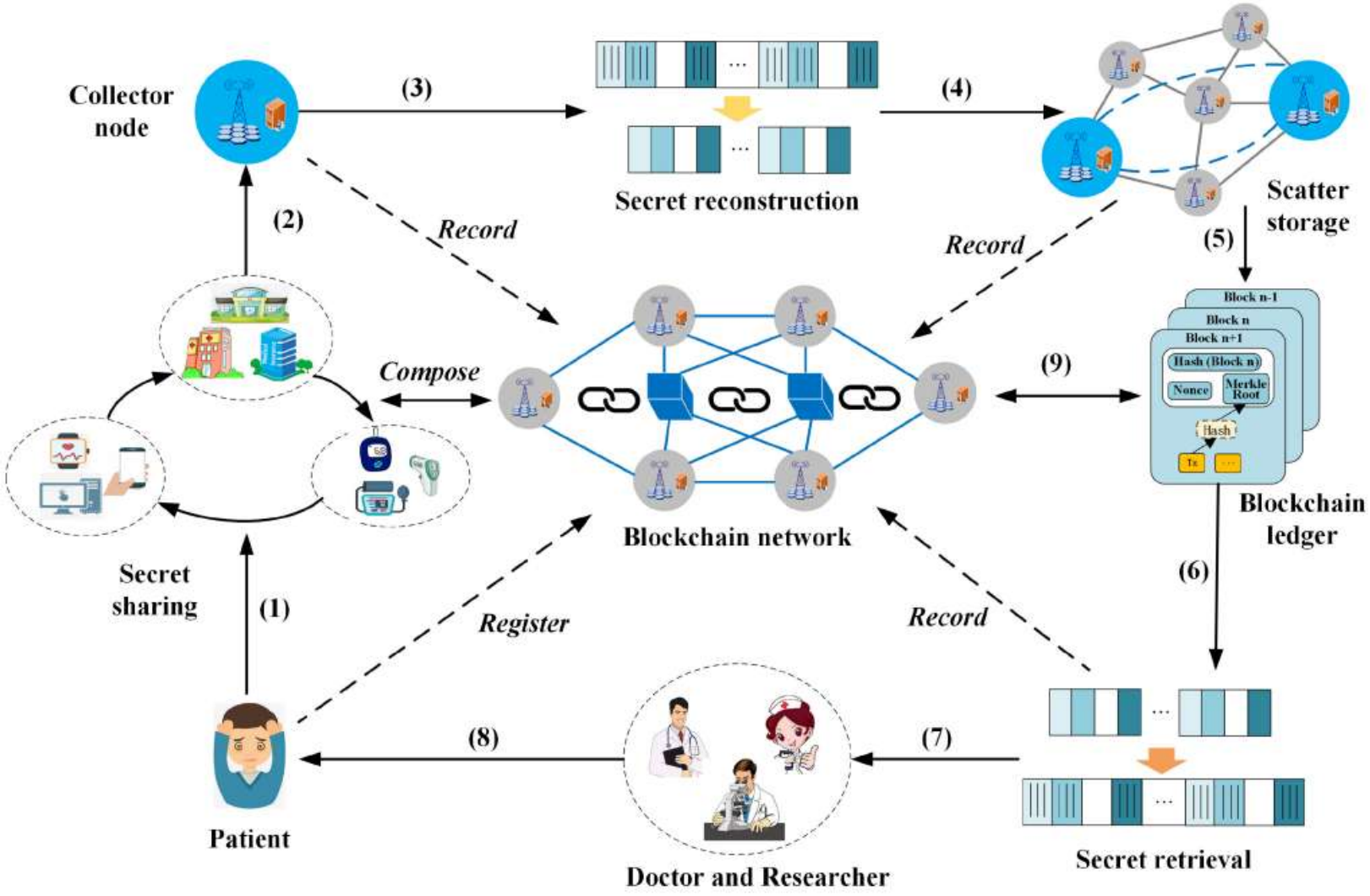
PART 02

设计模型

Try to design a model.

IoMT的数据隐私保护模型框架

主要思想：利用区块链技术和轻量级秘密共享构建了一个数据隐私保护模型，如图所示。
它改变了传统 IoMT 系统中的数据管理形式，应用轻量级的秘密共享机制，实现健康的数据存储和共享。



方案模型- SHAMIR 协议

目的：尽可能保护重要信息不被单一参与方泄露或丢失，将原始消息分割成若干子消息，实现阈值分割。

方法：

A.秘密重构：该阶段包含7个步骤，将原始消息划分为若干子消息。

1. 选取一个素数p。
2. 确认子密钥持有者n。
3. 确定阈值t。
4. 选取t - 1个数a1，a2，..，at - 1∈[1 , p] 。
5. 对于秘密s，设定一个多项式$f(x) = s + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$。
6. 将$s_i = f(i), (\mathrm{i} = 1,2,\ldots,\mathrm{n})$分别分配给n个持有者$p_1$，$p_2$，..，$p_n$。
7. 消除多项式$f(x)$。

B.秘密检索：该阶段包含3个步骤，在不低于预设子消息数的情况下恢复原始消息。

1. 聚合t个子密钥$\{s_1, s_2, .., s_t\} \rightarrow \{f(1), f(2), .., f(t)\}$。
2. 建立了秘密检索多项式$f(x) = \sum_{j=1}^{t} f(i_j) \prod_{l=1,l!=j}^{t} (x - i_l)/(i_j - i_l) \ mod \ p$。
3. 计算并输出$s = f(0)$。

安全模型

目的： 尽可能抵抗敌手的攻击，保证健康信息的安全性。

敌手类型：

类型①-半诚实敌手：这类敌手会遵守协议要求，但会主动收集子密钥。

类型②-恶意敌手：这类敌手不再诚实地遵循协议，会向其他参与者发送虚假或伪造的计算结果。

方法： 对于抵抗这两类敌手的方案容错性，必须证明不少于 t 个子密钥可以恢复 s，而少于 t 个子密钥则无法恢复 s。将其安全性归结于以下两个引理：

引理 1: 用 $j(t \le j \le n)$ 个子密钥 $\{s_{i_1}, s_{i_2}, \ldots, s_{i_j}\} \subseteq \{s_1, s_2, \ldots, s_n\}$ $(i_j \in \{1, 2, \ldots, n\})$可以恢复原始秘密s。

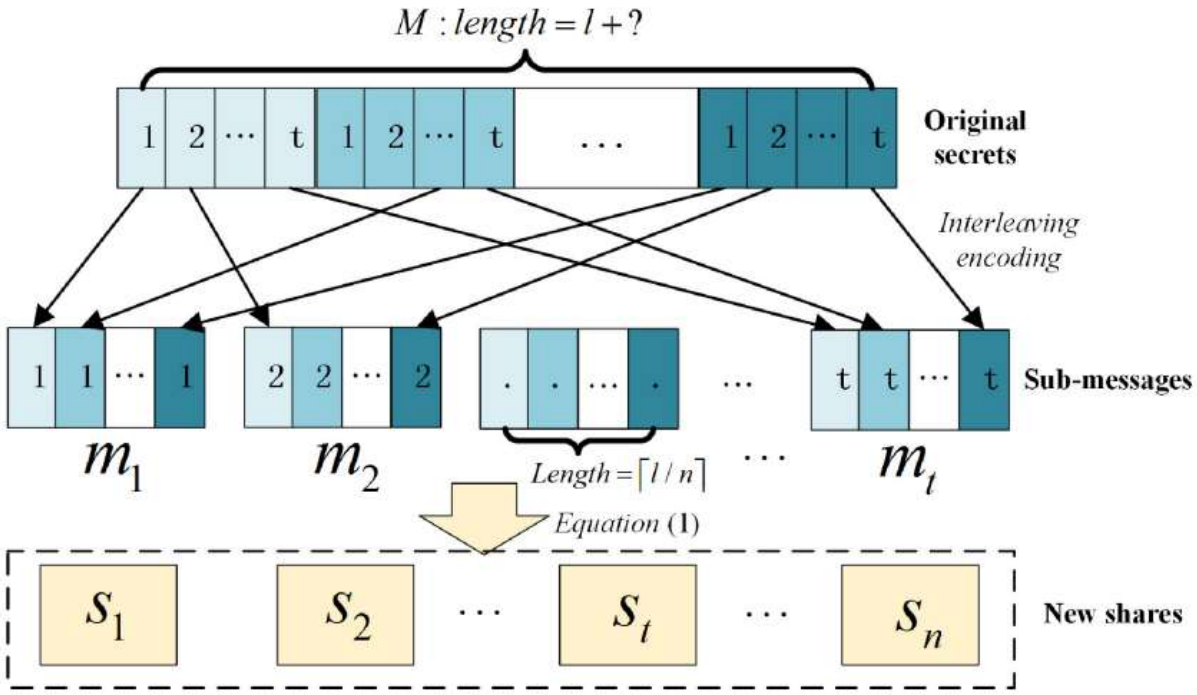
引理2: 用j'(j'< t)个份额 $\{s_{i_1}, s_{i_2}, \ldots, s_{i_{j'}}\} \subseteq \{s_1, s_2, \ldots, s_n\}$ $(i_{j'} \in \{1, 2, \ldots, n\})$无法恢复原始秘密s。

(t/n)-SS 方案概览

1、密码重构（分割）

①交织编码

交织编码器算法将秘密M编码为t个子消息$\{m_1, m_2, .., m_t\}$，每个子消息的长度为$\lceil l/t \rceil (1 < t \leq n)$。这种编码算法破坏了原始秘密的语义，防止了不知道代码规则的敌手的统计攻击。



(t/n)-SS 方案概览

②消息重组

新的小份额可以使秘密数据共享方案更加轻量级，因为它需要更少的存储空间和数据处理时间。

具体过程

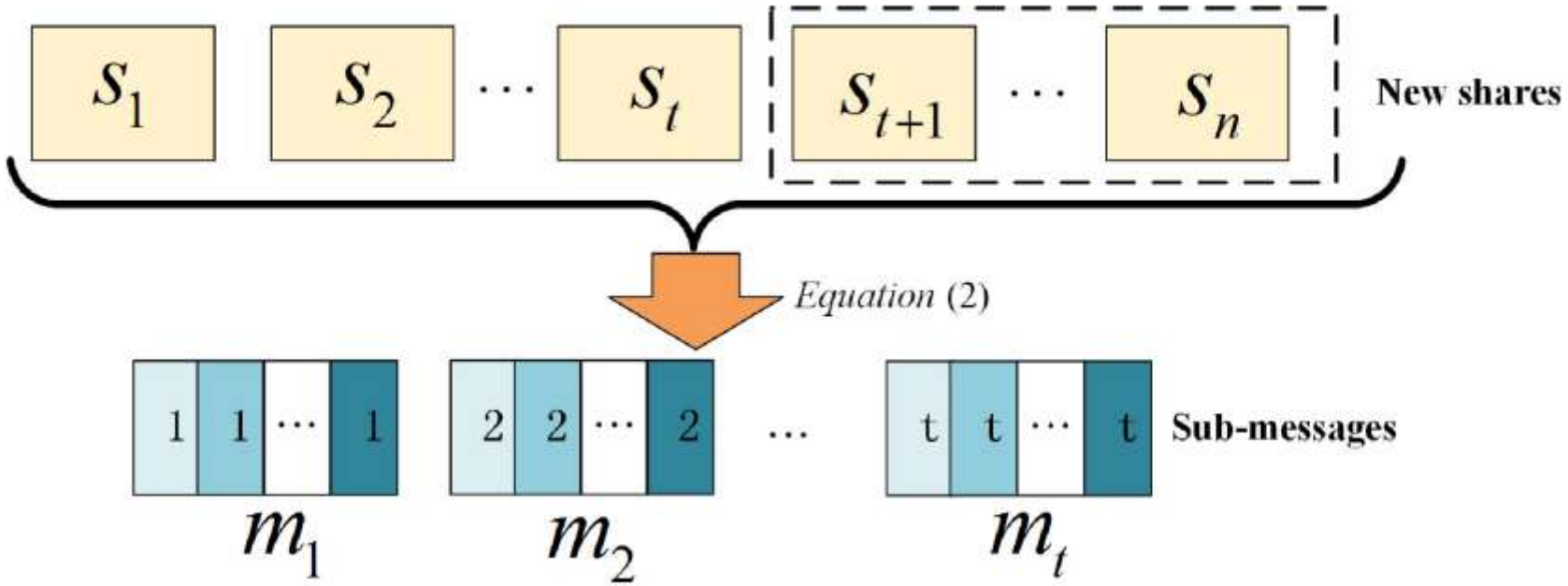
将t个子消息$\{m_1, m_2, .., m_t\}$按照下面给出的原则重组为n个新的份额$s_i(i = 1,2,\ldots,n)$。

$$s_i = \begin{cases} m_1 + \cdots + im_i + \cdots + m_t \bmod p, if\ 1 \le i \le t \\ 2^{i-t+1}s_1 + \cdots + 2^{i-t+t}s_t \bmod p, if\ t < i \le n \end{cases}$$

(t/n)-SS 方案概览

2、秘密检索

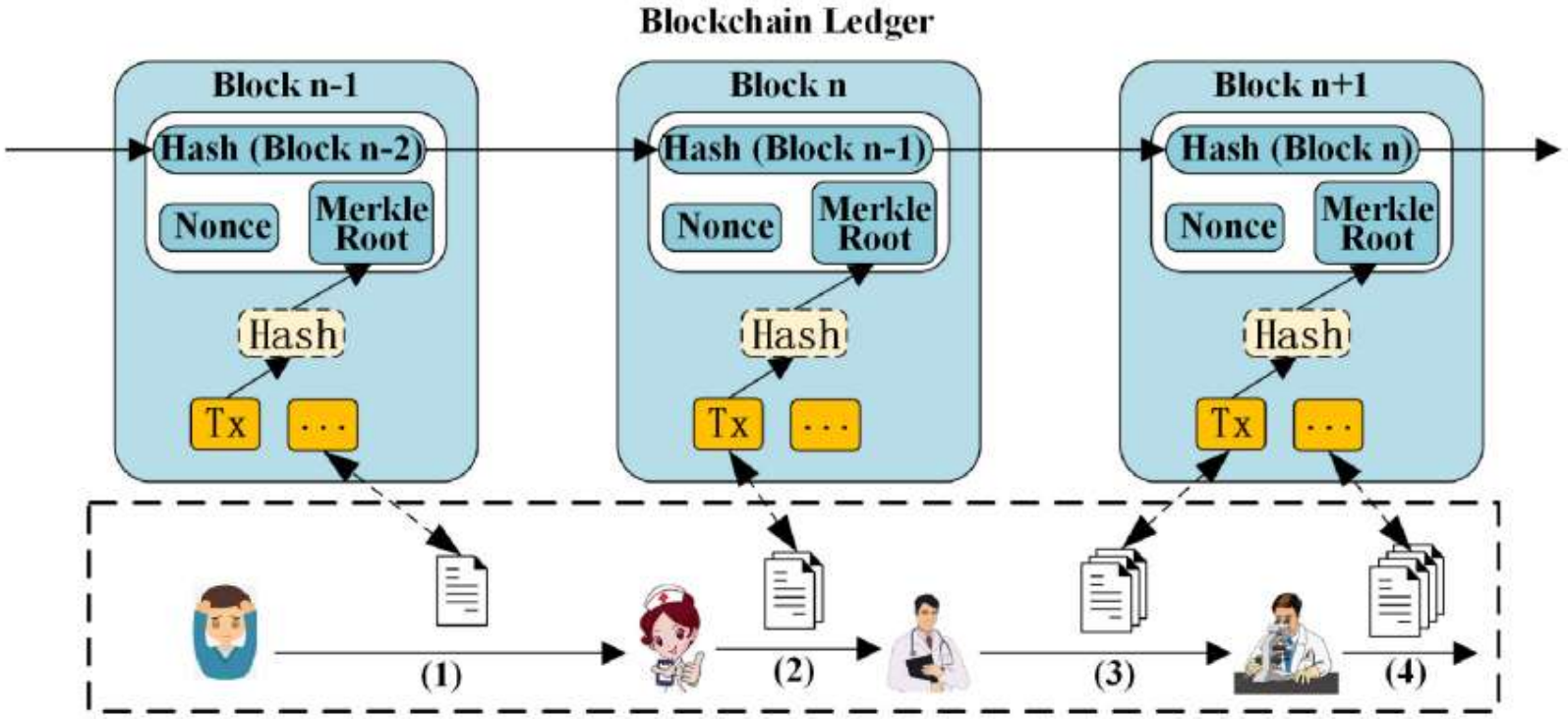
用不少于预设数量的份额恢复原始数据，提供了在某些共享块被篡改或破坏的情况下的容错能力，可以提高检索效率



区块链账本中的数据记录

目的：使用区块链账本负责记录基于区块链的IoMT中健康数据的存储地址和操作记录。

方法：交易记录被组织为默克尔树的叶节点，根节点代表该区块中所有交易数据的哈希值，对数据读取进行逐层哈希操作，保证安全性。



(t/n)-SS 方案的安全性证明

定理1证明：用 J（T ≤ J ≤ N）个份额**可以**恢复原始秘密 M

证明用 t 个份额可以恢复秘密 M，如果这是最坏情况成功，那么多于 t 个份额的情况也有效。**情况1**：用前 t 个份额进行检索，通过上方分割的原则进行重构，因此可描述为：

$$\begin{cases} s_1 = m_1 + m_2 + \cdots + m_t \bmod p \\ s_2 = m_1 + 2m_2 + \cdots + m_t \bmod p \\ \vdots \\ s_t = m_1 + m_2 + \cdots + tm_t \bmod p \end{cases}$$

系数矩阵D_1如下所示：$D_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & t \end{pmatrix}$

然后，计算D_1的行列式，发现$|D_1| = (t-1)!$。因此，系数矩阵D_1是可逆的，非零行列式$(t-1)!\ (t>1)$

子消息$\{m_1, m_2, .., m_t\}$可以通过矩阵D_1^{-1}恢复，t份额为$\{s_1, s_2, .., s_t\}$。

(t/n)-SS 方案的安全性证明

情况2：从两部分中分别选择份额，其中，方程是从同余方程中随机选取的，根据分割的原则进行重构，其中$t < i \leq n$:

$$2^{i-t+1}s_1 + \cdots + 2^{i-t+t}s_t \ mod\ p$$

现在，我们不需要直接证明子消息集合和原份额之间的关系。只需要证明是否可以用原份额求出前t个份额，就转化为了第一种情况。如下式所示

$$\left\{s_{k_1}, \ldots, s_{k_i}, s_{t+k_{i+1}}, \ldots, s_{t+k_t}\right\}^T = F \cdot (s_1,\ s_2,\ \ldots,\ s_t)^T$$

接下来，系数矩阵F可以描述为:

$$F = \begin{pmatrix} 0 & \cdots & 1 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 1 & \ldots & 0 \\ 1 & \ldots & k_1^{k_{i+1}+k_1} & \ldots & k_i^{k_{i+1}+k_i} & \ldots & t^{k_{i+1}+t} \\ \vdots & & \vdots & & \vdots & & \vdots \\ 1 & \ldots & k_1^{k_t+k_1} & \ldots & k_i^{k_t+k_i} & \ldots & t^{k_t+t} \end{pmatrix}$$

计算其行列式可得F可逆，即可恢复原消息。

综上，引理1得证。

(t/n)-SS 方案的安全性证明

定理2证明：若有J′(J′<T)个份额，则**无法**恢复原始秘密M

假设一个敌手可以获得一个份额集合A:$\{s_{k_1}, s_{k_2}, \dots, s_{k_{j'}}\}$，他尝试用系数矩阵$D_{j'\times t}$恢复子消息集合B:$\{x_1, x_2, \dots, x_t\}$，如上述式所示：

$$A = D_{j'\times t}B$$

此时，问题就变成了上述同余方程是否有解的问题。我们认为最好的情况是获得$j' = t - 1$个份额的对手可以推导出M，那么少于t - 1份的情况也是不成立的。

由于系数矩阵$D_{(t-1)\times t}$在域F上，我们在F_p上设定一个新的矩阵D'。$D_{j'\times t}$的增广矩阵可以表示为$(D'|A)_{(t-1)\times(t+1)}$，且$(D'|A)_{(t-1)\times(t+1)} = D'_{(t-1)\times t}A$

这里存在两种情况：一种是$D_{(t-1)\times t}$的秩小于$(D'|A)_{(t-1)\times(t+1)}$

另一种是$D_{(t-1)\times t}$的秩等于$(D'|A)_{(t-1)\times(t+1)}$。

第一种情况同余方程没有解。第二种情况由于同余式在$D_{(t-1)\times t}$的秩和$(D'|A)_{(t-1)\times(t+1)}$小于变量t的个数的条件下有无穷多个解，无法得到合法解。

因此，t - 1份额不能成功恢复原始秘密，少于t - 1份额不能成功。

PART 03

性能分析

Conducting experiments and analyzing results.

性能指标

交易处理时间 (TSP)

从交易发起至交易完成所经历的时长。

交易延迟 (TL)

从交易指令发出到该指令被执行或交易被确认所超出的正常时间间隔。

查询 (Query)

交易 (Transaction)

比较对象

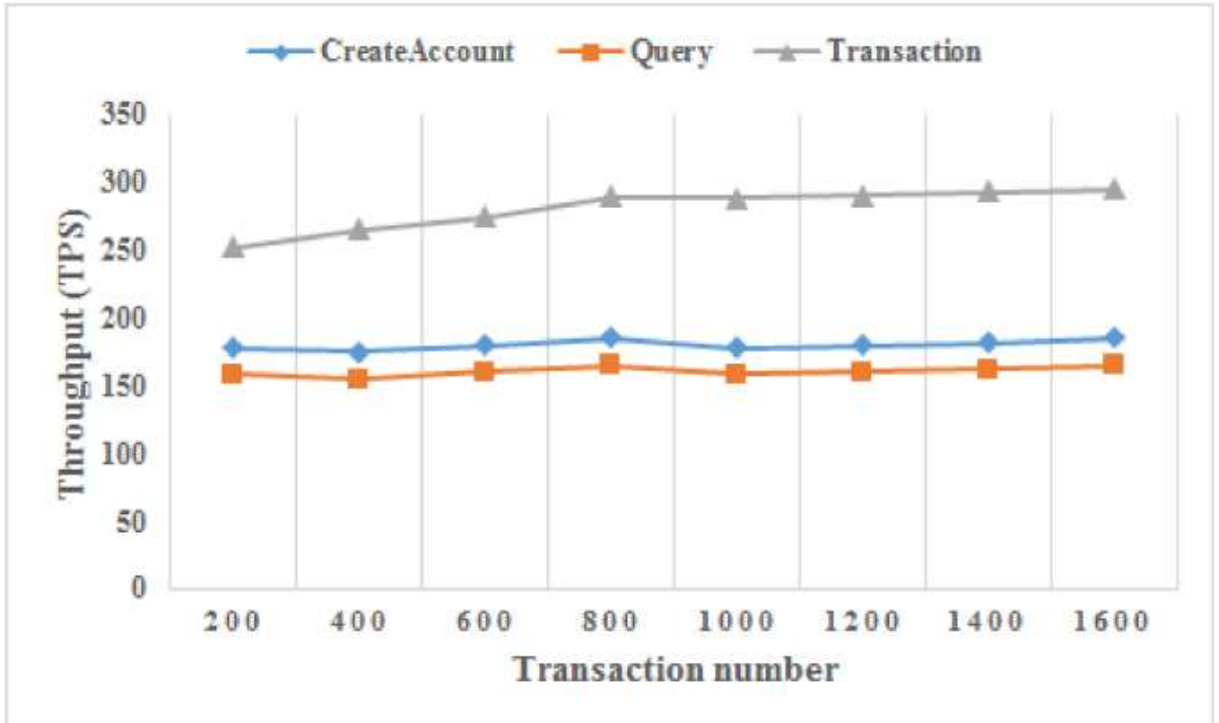
1.基于云的秘密共享css方案
2.完美秘密共享pss方案
3.基于中国剩余定理的crss方案

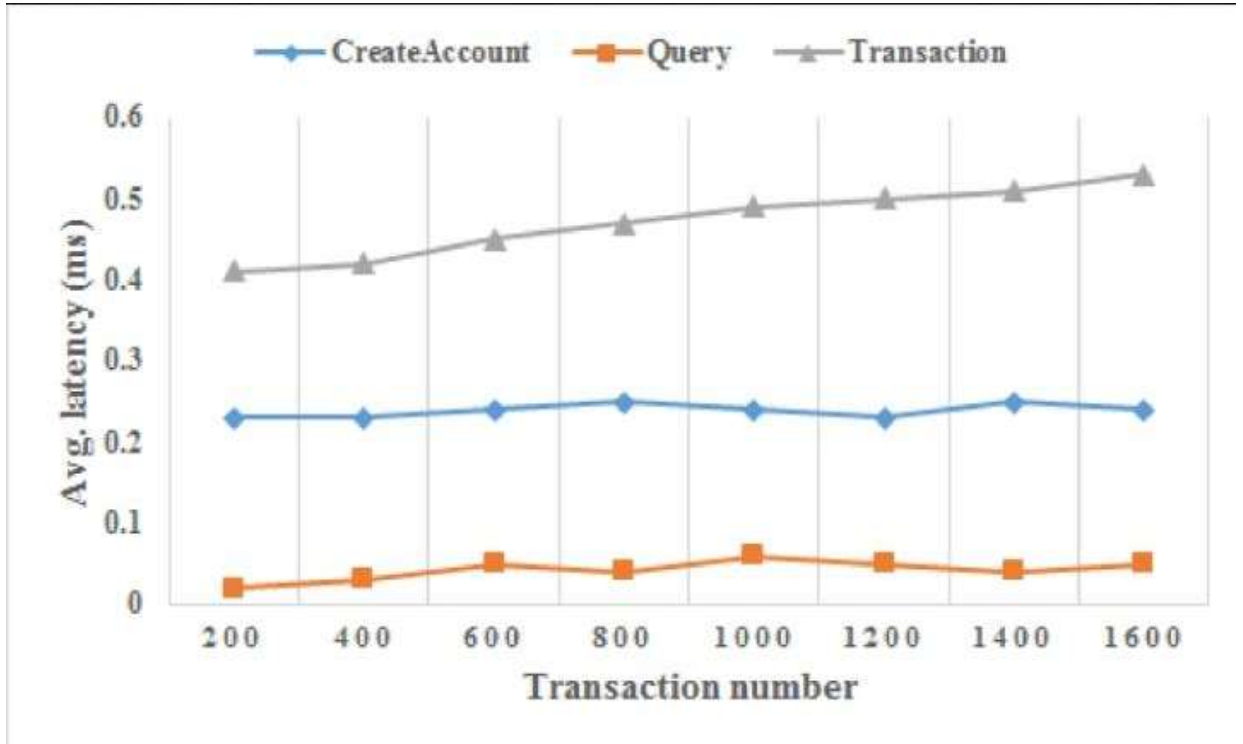
性能分析

基于区块链的IoMT中的事务处理

随着交易次数从200次增加到1600次进行模拟，只有Transaction项的TSP略有增加。

因此可以得出TSP和TL**受测试环境的影响较小**

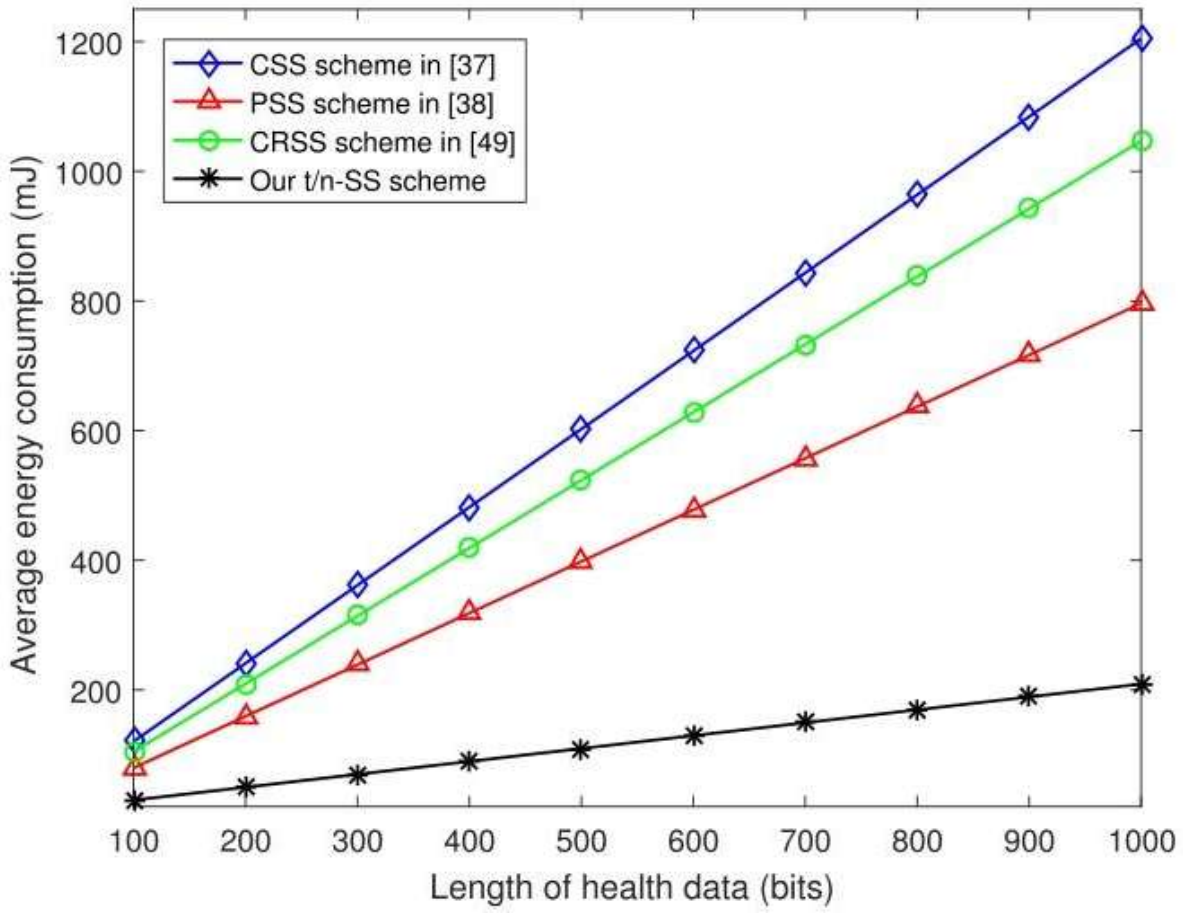




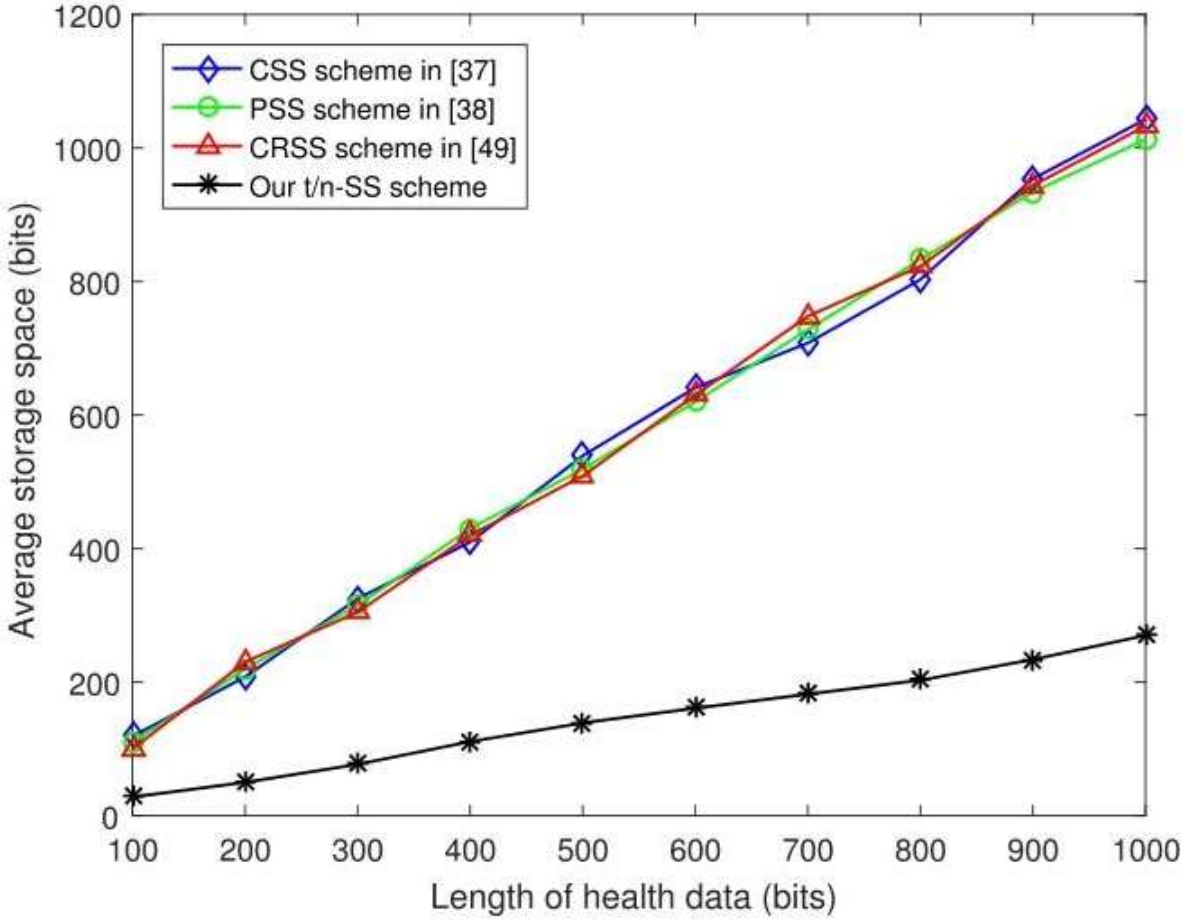
性能分析

性能比较

能耗对比



存储空间对比



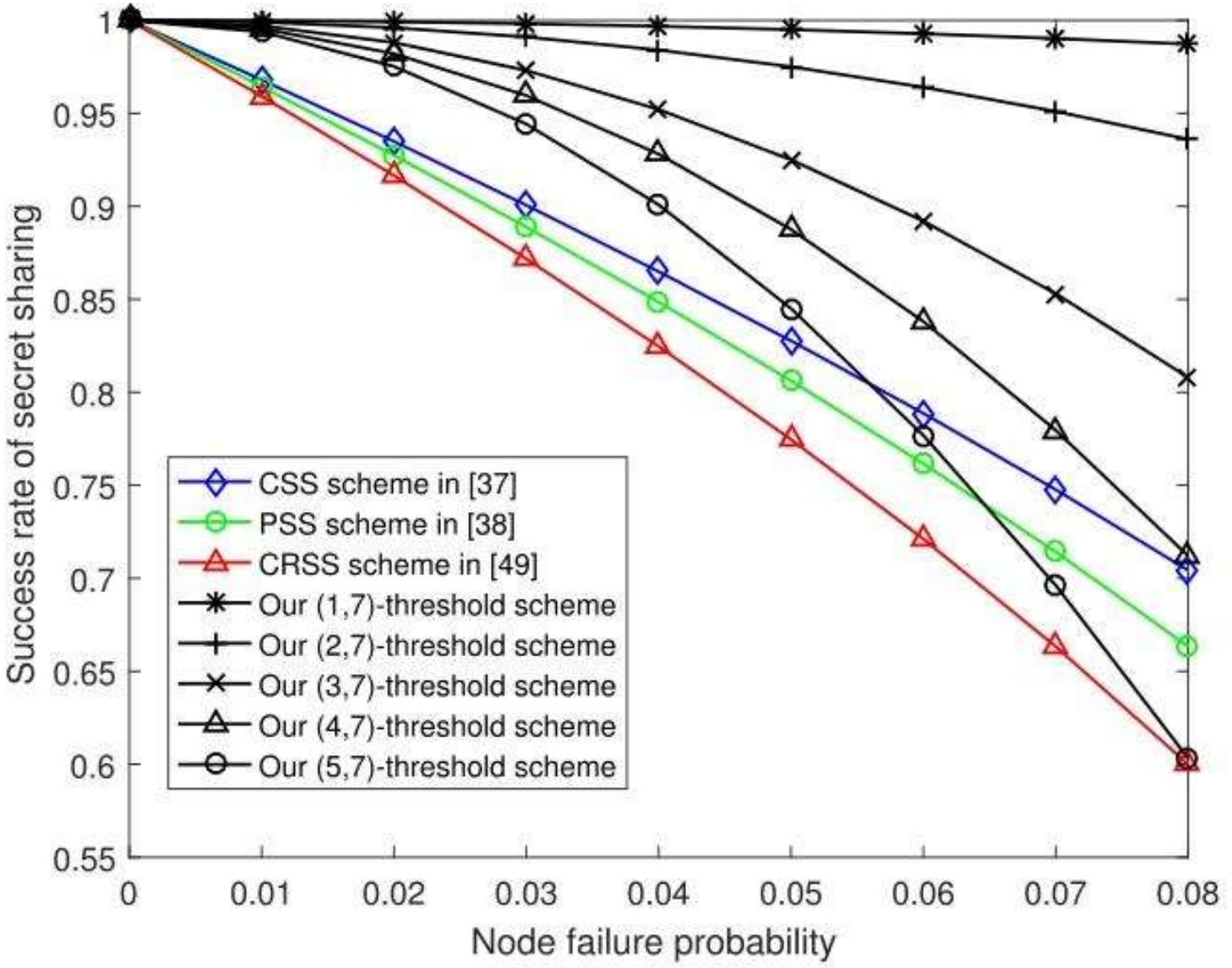
性能分析

性能比较

网络容错性对比

当1≤t≤4时，节点失效概率为[0,0.08]
但当t增加到5时，成功率迅速下降，不再具有实际意义。

在实际情况中，该方案可以提高网络的容错能力，使共享的健康数据更加可靠。



安全性分析

基于区块链的IoMT中用户的隐私问题：

01 健康数据秘密共享；

02 用户隐私保护；

03 健康数据轻量级存储；

04 网络故障容忍；

- 基于区块链
- 通过重构破坏语义
- 划分原数据
- t/n-ss算法

PART 04

总结展望

Summary of the thesis and outlook for the future.

总结展望

贡献总结：

01 聚焦于不同智能医疗设备之间数据共享过程中的隐私保护问题，设计了一种基于区块链技术的数据隐私保护模型，用于安全的数据共享。

02 该模型在数据传输时，能够保证健康数据的安全和用户的隐私。

03 提出了一种方案将原始秘密分割成小份额进行存储和共享，显著节省了存储空间，并保证了公共账本中的隐私安全。

04 安全性证明表面该方案是正确且具有理论安全性的，性能结果表明隐私保护模型节能、存储空间高效且具有网络容错性。

未来展望：

感谢聆听

Thanks for your listening