文章编号:1671-4598(2023)04-0246-06 DOI:10.16526/j.cnki.11—4762/tp.2023.04.038 中图分类号:TP393 文献标识码:A

基于区块链的通信网络节点位置隐私加密控制模型设计

马亚蕾,张 怡
(陕西职业技术学院 电子信息工程学院,西安 710000)

摘要:为解决因通信网络加密执行能力有限而造成的隐私信息识别异常问题,提升网络体系对于隐私文本的加密处理能力,设计基于区块链的通信网络节点位置隐私加密控制模型;在区块链技术的支持下,建立密码共识机制,再根据智能合约中协议条文的编码形式,求解节点加密差值,完成基于区块链的通信网络节点加密验证;按照信息序列定义条件,建立P盒、S盒两类信息数列处理结构,完成对通信网络节点位置隐私信息数列产生器的设计;规范隐私信息的数据帧格式,根据密钥内容查询结果,确定熵值控制系数的取值范围,再实施熵值校验处理,实现基于区块链的通信网络节点位置隐私加密控制模型的设计;实验结果表明,区块链技术作用下,通信网络在单位时间内所能加密处理的信息样本总量达到了9.8×10^{13} bit,因加密执行能力有限造成的隐私信息识别异常问题得到较好解决,隐私信息样本加密准确性为96.5%,能够加强网络体系在加密处理隐私文本方面的能力。

关键词:区块链;通信网络;隐私加密;密码共识;智能合约;信息序列;数据帧;熵值校验

Design of Node Location Privacy Encryption Control Model in Communication Network Based on Blockchain

MA Yalei, ZHANG Yi
(School of Electronic Information Engineering, Shaanxi Vocational and Technical College, Xi'an 710000, China)

Abstract: In order to solve the abnormal identification problem of privacy information caused by the limited implementation capacity of a communication network encryption, and improve the network system's ability to encrypt private texts, a communication network node location privacy encryption control model based on blockchain is designed. With the support of the blockchain technology, this paper establishes a password consensus mechanism, solves the node encryption difference by the encoding form of the protocol clauses in the smart contract, and completes the encryption verification of communication network nodes based on the blockchain. According to the definition condition of information sequence, two information sequence processing structures (P box and S box) are established to complete the privacy information sequence generator design for the communication network node location. By standardizing the data frame format of the privacy information, the entropy control coefficient range is determined by the query result of the key content, and then the entropy verification processing is implemented to achieve the design of the location privacy encryption control model of the communication network nodes based on the blockchain. The experimental results show that the total number of the information samples that the communication network can encrypt and process in a unit time reaches 9.8×10^{13} bits by using the blockchain technology, the privacy information identification anomaly caused by the limited encryption execution ability has been well solved, and the accuracy of privacy information sample encryption reaches 96.5%, which can strengthen the ability of network system to encrypt and process privacy text.

Keywords: blockchain; communication network; privacy encryption; password consensus; smart contract; information sequence; data frame; entropy check

0 引言

区块链就是由多个区块组织联合起来形成的链条状结构。每一个区块组织都接受区域性主机的直接调度,故而每一区块中所保存的信息参量既可以相同也可以不同,它们可以按照各自需求制定出多种不同的时间序列条件。在互联网环境中,所有服务器设备都具有保存链条序列的能力,且只要大规模区块环境中有一台服务器设备能够保持正常工作状态,整个区块链组织的安全运行能力就可以得到保障[1-2]。服务器主机在通信网络区块链组织中被称为连接节点,在互联网体系保持稳定运行的情况下,这些节点对象可以为数据信息样本提供大量的存储空间。如果通信网络区块链组织中存在信息错误的情况,在进行修改处理时,必须征得半数以上节点对象的同意,但并不是所有节点对象都掌握主动允准权,所以篡改通信网络区块链组织

收稿日期:2022-12-14; **修回日期**:2023-01-17。
基金项目:陕西省教育厅专项科研计划项目课题名称(21Jk0590)。
作者简介:马亚蕾(1985-),女,陕西咸阳人,硕士研究生,副教授,主要从事计算机网络安全、物联网方向的研究。
引用格式:马亚蕾,张 怡.基于区块链的通信网络节点位置隐私加密控制模型设计[J].计算机测量与控制,2023,31(4):246-251.

中的信息样本是一件非常困难的事情。相较于其他类型的网络体系，区块链可以在去中心化处理的同时，维护数据信息的独立性，因此该类型链条结构可以有效解决信息样本之间相互不信任的问题。

通信是指可以借助媒介实现的信息交流与传递关系，而网络则是指由物理链路连接起来的工作站集群。通信网络是通信关系与网络体系的综合表现形式，可以在链路体系的作用下，将节点与节点连接起来，从而达到资源传输与共享的目的。由于通信网络的覆盖范围较为广泛，所以在信息快速传输的情况下，主机元件对于个别节点处隐私文本的加密处理能力可能会出现一定程度的下降，这也是导致通信网络中出现隐私信息识别异常情况的主要原因。为此，相关学者纷纷对通信网络节点位置隐私加密控制方法做出了研究。文献［3］提出使用模糊关键字可搜索同态加密的区块链隐私保护方案。同态加密保护方案以模糊关键字为标准，对通信数据进行搜索，又联合中间节点，制定完整的加密执行算法。文献［4］提出基于群签名与属性加密的区块链可监管隐私保护方案。基于群签名与属性加密的保护方案通过公钥文本、私钥文本来回交互的方式，判断通信网络中当前数据信息的隐私等级，再根据溯源机制，定义与该信息相关的加密条件。然而上述两种方法在单位时间内所能加密处理的信息样本总量相对较少，并不能有效提升通信网络的加密执行能力。为解决上述问题，设计基于区块链的通信网络节点位置隐私加密控制模型。

1　基于区块链的通信网络节点加密验证

对于通信网络节点的加密验证，应按照区块链组织所要求的密码共识机制，建立智能合约协议，再以此为基础，确定节点加密差值的实际取值范围。

1.1　密码共识机制

密码共识机制决定了通信网络对于节点对象的去中心化处理能力。在区块链组织单元中，为满足通信网络节点的高速运行需求，要求密码共识机制必须对数据信息的存储形式进行精准定义[5]。所谓密码共识就是指密文模板的普遍存在形式，在通信网络环境中，密文模板对于数据信息样本的定义越细致，就表示主机元件在单位时间内所能处理的隐私信息总量越多。

共识向量常表示为 $\vec{E}$，定义密码共识机制时，该项物理量的取值影响通信数据明文信息与密文信息之间的转换关系。对于共识向量的求解满足式（1）：

$$\vec{E}=\frac{\sum_{w=1}^{+\infty}\left|\boldsymbol{Q}_{\max}-\boldsymbol{Q}_{\min}\right|^{2}}{\dot{E}\times(\Delta\boldsymbol{Q})} \tag{1}$$

式中，w 表示密文信息编码系数，$\boldsymbol{Q}_{\max}$ 表示去中心化向量的最大取值，$\boldsymbol{Q}_{\min}$ 表示去中心化向量的最小取值，$\Delta\boldsymbol{Q}$ 表示去中心化参数的单位累积量，$\dot{E}$ 表示密文样本编码系数。在式（1）的基础上，设 $\bar{\chi}$ 表示隐私信息的单位转码均值，e 表示密码编译系数，α 表示密文表达系数，β 表示通信网络节点对于密码信息的提取参数，$\dot{q}$ 表示隐私信息加密特征，δ 表示实时加密系数，联立上述物理量，可将密码共识机制表达式定义为：

$$W=\delta\dot{q}\left[\beta\left(e-\frac{\sqrt{\vec{E}\left|\chi\right|}}{\alpha^{2}}\right)\right] \tag{2}$$

对于通信网络节点位置隐私信息的编码必须遵循密码共识机制，且由于区块链组织的存在，各个节点区域的共识主机都可对数据信息样本进行独立处理，因此即便是在明文信息、密文信息传输方向不一致的情况下，通信网络主机也不会陷入错误编码的行为局面之中[6]。

1.2　智能合约

智能合约包括与主动执行方、被动执行方、中间过渡单位相关的协议文本，能够按照密码共识机制对隐私信息加密行为进行约束，从而使得通信网络节点能够准确记录信息文本传输行为，并可以在已存储数据信息文本的基础上，完善区块链组织中的信息编码形式[7]。对于智能合约的规范主要从如下几方面进行。

1）主动执行方的智能合约：主动执行方就是指通信网络中具有自主编码能力的节点对象，为使位置隐私信息得到精准加密，在定义智能合约时，待加密的通信网络节点位置隐私信息不需经过数据库主机的存储，可以由网络体系传输环境直接进入加密编码主机。

2）被动执行方的智能合约：被动执行方是指通信网络中与主动执行方保持映射连接关系的节点对象，由于节点位置隐私信息的编码必须同时具有完整性与特殊性，所以合约文本必须对密文模板的编码形式进行准确定义。

3）中间过渡单位的智能合约：中间过渡单位是存在于主动执行方与被动执行方之间的信息传输节点，在通信网络环境中，中间过渡单位所处位置受到执行方节点的直接影响[8]。与中间过渡单位相关的智能合约文本应对执行方节点之间的连接关系进行注释，且为保证密码共识机制的完整性，合约条款还要求节点加密差值的赋值区间必须与密码共识机制中节点位置隐私信息样本的取值区间相匹配。

1.3　节点加密差值

节点加密差值可用来验证加密控制模型对于通信网络节点位置隐私信息的加密处理能力，对于区块链组织而言，确保节点加密差值结果的合理性，是实现通信网络节点加密验证的关键执行环节。所谓差值就是指实际加密结果与密码共识机制所规定结果具有一定的数值差，且为适应智能合约对于区块链组织的约束需求，标准加密差的取值不宜过大[9-10]。对于节点加密差值的求解需同时考虑通信网络节点度量值与隐私性参数。通信网络节点度量值常表示为 γ，在区块链组织之中，该项物理量的取值属于 $[1,+\infty)$ 的数值区间。隐私性参数常表示为 y，在通信网络环境中，该项物理量的取值越大，就表示数据信息样本的隐私性等级越高。在上述物理量的支持下，联立式（2），推导节点加密差值计算表达式为：

$$\hat{R}=\int_{r=1}^{+\infty}\frac{\sqrt{\gamma\cdot\left|\bar{y}^{2}W-y^{2}\right|}}{\left|\frac{\overline{\overline{u}}}{\overline{\overline{u}}}\right|^{1/\varepsilon^{2}}} \tag{3}$$

其中：r 表示基于区块链算法的加密信息约束系数，$\tilde{y}$ 表示隐私性参数在特定情况下的取值结果，$\overleftarrow{u}$ 表示顺序传输情况下的隐私信息加密特征，$\overrightarrow{u}$ 表示逆序传输情况下的隐私信息加密特征，ε 表示位置隐私信息融合系数。如果 $\overleftarrow{u}=\overrightarrow{u}$ 的取值条件成立，表示通信网络环境中，隐私信息顺序、逆序传输量相等，通信节点处于相对平衡的分配状态。

2 通信网络节点位置隐私信息的数列产生器

在加密验证机制的基础上，定义信息序列条件，并分别借助 P 盒、S 盒结构，完善数列产生器对于通信网络节点位置隐私信息的处理能力。

2.1 信息序列定义

信息序列是一项广义定义条件，决定了通信网络主机对于节点位置隐私信息的深度与广度加密处理能力，在重复处理环节中，保障信息序列条件的完整性，才有可能实现对通信网络节点位置隐私信息的准确加密[11]。从概率统计的角度来看，节点位置隐私信息序列的定义具有随机性，两个随机选取的数据信息样本在不同密文模板的作用下，有可能对应一个完全相同的加密结果，而在区块链组织作用下，通信网络主机对于相似信息样本的辨别能力较弱，所以为使加密结果保持唯一性，还要在定义信息序列时，尽量避免随机数据样本的出现[12]。规定 ε 表示通信网络环境中的隐私信息加密映射系数，I 表示原始加密数据，I' 表示数据 I 的一次求导结果，I'' 表示数据 I 的二次求导结果，联立上述物理量，可将基于区块链组织的隐私信息密文向量表示为：

$$U=\hat{R}\times\lim_{\varepsilon\to\infty}\mid I\mid\times\left|\frac{I''}{I'}\right| \tag{4}$$

在式（4）的基础上，求解信息序列定义式如下：

$$O=\left|\frac{U^{\mp}-1}{\varphi\cdot\widetilde{Y}^{2}}\right|_{\varphi\neq 0} \tag{5}$$

式中，φ 表示不为零的信息序列参数，φ 表示节点位置隐私取值系数，$\widetilde{Y}$ 表示信息样本的隐私特征。由于信息序列定义式必须适应区块链组织对于隐私数据样本的编码需求，所以为保证加密结果的真实性，在推导序列表达式时，可对信息样本进行多次取值。

2.2 信息数列处理结构

2.2.1 P 盒结构

P 盒结构的功能是维持通信网络节点位置隐私信息的初始编码序列，从而在保障区块链主机对于隐私信息样本辨识能力的同时，实现对数据信息的精准加密[13-14]。遵循 P 盒结构的信息数列处理原则如图 1 所示。

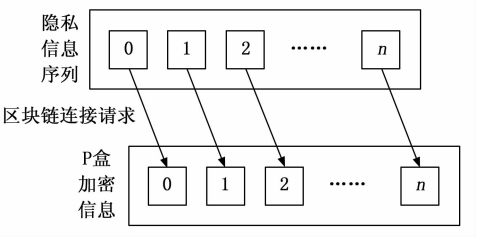


图 1 基于区块链的 P 盒处理原则

由于一个隐私信息序列只能对应一个 P 盒加密信息，所以在 P 盒结构中，不会出现单一信息多次加密的情况。

2.2.2 S 盒结构

S 盒结构的功能是打乱通信网络节点位置隐私信息的原有加密序列，并按照区块链编码原则，将这些数据信息样本组合成全新的序列模型，从而在保证加密内容机密性的同时，改写加密信息的存储内容，使得区块链主机能够对这些信息参量进行直接调取与利用[15-16]。由隐私信息序列指向加密信息的区块链连接请求保持“一对多”的映射状态，即通信主机所捕获到的一个节点位置隐私信息样本可以同时对应多个加密信息文本，因此 S 盒结构负责处理大规模输出的隐形信息数列。遵循 S 盒结构的信息数列处理原则如图 2 所示。

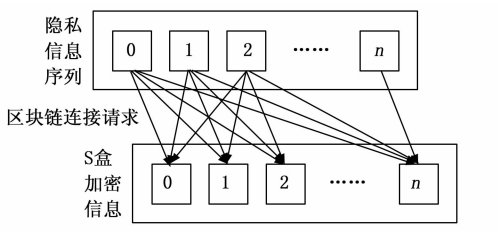


图 2 基于区块链的 S 盒处理原则

对于区块链主机而言，待加密的通信网络节点位置隐私信息不可能同时满足 P 盒、S 盒两种处理原则。

3 加密控制方法

利用数列产生器，对通信网络节点位置隐私数据的帧格式进行定义，再遵循区块链组织的连接形式，确定密钥内容，从而使得网络主机设备能够根据熵值控制系数的取值结果，完成对熵值指标的准确校验。

3.1 数据帧格式

数据帧格式就是指通信网络节点位置隐私信息样本的存储格式[17]。在区块链组织之中，数据帧格式决定了完成加密处理后隐私信息的存储形式，由于 P 盒结构、S 盒结构对于数据信息样本的处理原则并不相同，所以已定义的数据帧参量必须具有双重适应性[18]。规 λ 定表示帧信息标记系数，ι 表示帧信息查询参数，关于两项物理指标的取值满足式（6）。

$$\begin{cases}\lambda\neq 0\\ \iota\neq 1\end{cases} \tag{6}$$

在式（6）的基础上，设 $\dot{S}$ 表示区块链主机中的通信网络节点位置隐私信息加密特征，A 表示通信网络对于隐私信息样本的实时控制参量。在上述物理量的支持下，联立式（5），可将基于区块链的通信网络节点位置隐私数据帧格式定义结果表示为：

$$P=\frac{1}{\lambda}\int_{-\infty}^{+\infty}O\dot{S}^{2}\mid A\mid^{-\iota} \tag{7}$$

如果区块链主机对于两个隐私信息参量的识别结果相

同，那么通信网络对于这两类信息样本的加密处理结果也相同，作为过渡条件的数据帧格式定义结果也就完全相同。

3.2　密钥内容

密钥内容可以理解为通信网络节点位置隐私数据密文信息的编码形式，对于区块链主机而言，确保密钥内容的完整性是实现隐形信息精准加密处理的基础环节。完整的密钥内容需要对隐私信息样本帧对象进行精准定义[19-20]。κ 表示隐私信息样本的帧对象参量，其取值属于 $(-\infty,0)\cup(0,+\infty)$ 的数值区间。但由于区块链主机无法识别帧对象为负的隐私信息样本，所以在定义密钥内容时，应以 κ^2 作为基础判别条件。关于系数 κ^2 的取值满足如下表达式：

$$\kappa^2 \in (0,+\infty) \tag{8}$$

联立式（7）、（8），推导密钥内容定义式为：

$$D = P \cdot \left(1 - \frac{|d_{\kappa^2}|^2}{\sqrt{f}}\right) \tag{9}$$

其中：d_{κ^2} 表示 κ^2 条件下的隐私数据加密指征参量，f 表示密文信息查询参数。区块链主机为保证加密后信息与初始隐私信息传输方向的一致性，要求密钥内容中不可以出现取值为零的物理参量。

3.3　熵值控制系数

熵值控制系数可以理解为区块链主机对通信网络节点位置隐私信息进行加密处理时，所遵循的控制处理标准，一般来说，熵值计算结果越大，就表示节点位置隐私信息的单位累积量越大[21-22]。$\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n$ 表示 n 个不相等的信息样本加密控制向量，其求解表达式满足式（10）：

$$\begin{cases} \boldsymbol{g}_1 = \dfrac{\sum\limits_{\mu=1}\nu_1 \cdot h_1}{D} \\ \boldsymbol{g}_2 = \dfrac{\sum\limits_{\mu=1}\nu_2 \cdot h_2}{D} \\ \vdots \\ \boldsymbol{g}_n = \dfrac{\sum\limits_{\mu=1}\nu_n \cdot h_n}{D} \end{cases} \tag{10}$$

式中，$\boldsymbol{\mu}$ 表示通信网络节点位置隐私信息的单位累积向量，ν_1、ν_2、$\cdots$、ν_n 分别表示 n 个不相等的熵值指标，h_1、h_2、$\cdots$、h_n 分别表示与 ν_1、ν_2、$\cdots$、ν_n 匹配的主机控制权限。

利用式（10），求解熵值控制系数，定义式如下：

$$K = \frac{\sqrt{g_1 \times g_2 \times \cdots \times g_n}}{n! \times (l^2-1) \times |\vec{j}|^2} \tag{11}$$

其中：$\vec{j}$ 表示由区块链主机端指向通信网络主机端的加密控制指令执行向量。$\vec{j}>0$ 成立，表示加密后信息参量的传输方向与隐私信息源码的传输方向一致；$\vec{j}<0$ 成立，表示加密后信息参量的传输方向与隐私信息源码的传输方向相反；$\vec{j}=0$ 成立，表示区块链主机不能对通信网络节点位置隐私信息进行加密处理。

3.4　熵值校验

熵值校验就是对求解所得熵值控制系数的有效性进行核实。在熵值控制系数求解结果不等于零的情况下，只有校验结果与实际求解结果完全符合的熵值指标才能对应绝对精准的节点位置隐私信息加密处理结果[23-24]。在式（12）恒成立的情况下，联立式（11），求解熵值校验表达式为：

$$K \neq 0 \tag{12}$$

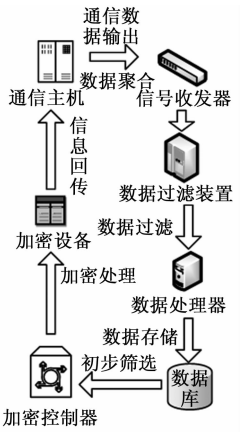
$$M = \log_K\left(1 - \left|\frac{\dot{b}^2}{\boldsymbol{\theta} \times \boldsymbol{C}}\right|\right) \tag{13}$$

式中，$\dot{b}$ 表示熵值控制系数在区块链主机中的存储特征，$\boldsymbol{\theta}$ 表示隐私信息加密文本定义向量，$\boldsymbol{C}$ 表示隐私信息加密文本的转码向量。在区块链组织中，根据式（13）对熵值控制系数进行校验处理，从而实现通信网络节点位置隐私加密控制模型的顺利应用。

4　实验分析

4.1　通信网络实验环境

搭建如图 3 所示的通信网络作为实验环境，在确保不存在外界信息干扰行为的情况下，闭合通信主机控制开关，使网络节点位置隐私数据保持自由传输状态。当加密设备中已存储信息样本达到一定数值标准后，正式开始实验。



（a）通信网络机柜实物图　　（b）通信网络布局

图 3　通信网络系统示意图

具体的实验元件设备型号如表 1 所示。

表 1　设备元件型号

编号	设备元件	名称
1	通信主机	HJ-4000FL
2	数据处理器	ZX-51VHK-3232
3	信号收发器	MT-viki HDMI
4	网络主机	RTX2060
5	加密芯片	FOR SMEC98SP
6	数据过滤装置	GTJ2021
7	数据库设备	SR558H 2U
8	加密设备	MFC-L8900CDW

为保证实验结果的公平性，实验组、对照组所选实验设备型号始终保持一致。

4.2　变量与实验步骤

通信网络在单位时间内所能加密处理的隐私信息样本总量决定了网络体系对于隐私文本的加密处理能力，为实

现对隐私信息的精准识别，要求单位时间内加密处理的隐私信息样本总量应保持在高数值水平状态。验证本文方法对通信网络节点位置隐私加密控制的有效性，具体实施流程如下：

步骤一：按需连接通信网络实验环境，闭合相关控制开关，满足通信网络节点位置隐私数据的传输需求；

步骤二：以基于区块链的通信网络节点位置隐私加密控制模型作为实验组方法，记录在该方法作用下，网络主机在通信网络节点处所能加密处理的隐私信息样本总量；

步骤三：以同态加密保护方案作为对照（1）组实验组方法，重复步骤二，记录隐私信息样本的加密总量；

步骤四：以基于群签名与属性加密的保护方案作为对照（2）组实验组方法，再次重复步骤二，记录隐私信息样本的加密总量；

步骤五：在此基础上，测试通信网络节点位置隐私加密的准确性；

步骤六：对比实验组、对照组实验结果，总结实验规律。

4.3 结果与讨论

图 4 反映了低峰、高峰传输情况下，网络主机在单位时间内所能加密处理的隐私信息样本总量。

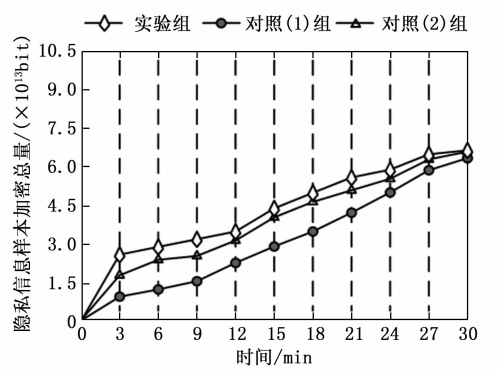


图 4 隐私信息样本加密总量（低峰传输）

信息样本低峰传输情况下，实验组、对照组隐私信息样本加密总量都呈现出不断增大的数值变化态势，整个实验过程中，实验组隐私信息样本加密总量均值水平明显更高。前 27 min 的实验时间内，实验组数值远高于对照（2）组实验数值，到第 30 min，二者差值水平开始缩小。前 9 min 的实验时间内，实验组数值明显高于对照（2）组实验数值，从第 12 min 开始，二者之间的数值差开始不断缩小。

信息样本高峰传输情况下，实验组隐私信息样本加密总量依然保持不断增大的数值变化态势，至实验结束，其最大值达到了 9.8×10^{13} bit。对照（1）组隐私信息样本加密总量保持先增大、再趋于稳定的数值变化态势，全局最大值仅能达到 7.5×10^{13} bit，明显小于实验组数值。第 21 min，对照（2）组隐私信息样本加密总量出现了明显下降趋势，除此时间节点外，其他实验数值均保持不断增大的数值变化态势，全局最大值为 6.8×10^{13} bit，也远小于实验组数值。

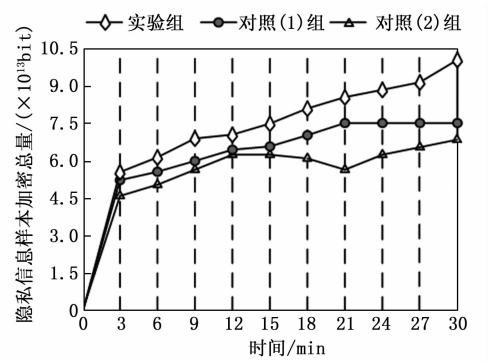


图 5 隐私信息样本加密总量（高峰传输）

在此基础上，测试 3 种方法的通信网络节点位置隐私加密的准确性，得到实验结果如图 6 所示。

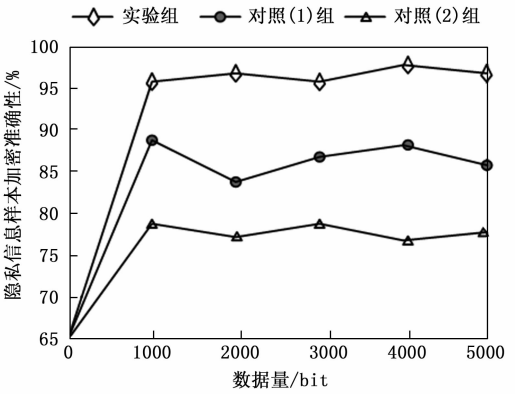


图 6 隐私信息加密准确性

分析图 6 可知，在 5 000 bit 实验数据的隐私加密实验中，实验组隐私信息样本加密准确性为 96.5%，对照（1）组隐私信息样本加密准确性为 85.5%，对照（2）组隐私信息样本加密准确性为 77.5%。

综上可知本次实验结论为：

1）同态加密保护方案、基于群签名与属性加密的保护方案在单位时间内所能加密处理的隐私信息样本总量相对较少，故而并不能较好解决因通信网络加密执行能力有限而造成的隐私信息识别异常问题，隐私信息样本加密准确性较差；

2）基于区块链的通信网络节点位置隐私加密控制模型在单位时间内所能加密处理的隐私信息样本总量较多，隐私信息样本加密准确性较高，更符合解决因通信网络加密执行能力有限而造成的隐私信息识别异常问题、提升网络体系对于隐私文本的加密处理能力的实际应用需求。

5 结束语

本文设计了基于区块链的通信网络节点位置隐私加密控制模型。在区块链组织的作用下，从隐私信息识别异常问题的角度入手，在建立密码共识机制的同时，精准定义信息序列，从而实现对熵值控制系数的校验处理。实验结果表明，该方法可以大幅提升通信网络在单位时间内所能

加密处理的信息样本总量，提升隐私信息样本加密准确性，对于提升网络体系对于隐私文本的加密处理能力，可以起到一定的促进性影响作用。

参考文献：

[1] 穆程刚，丁　涛，曲　明，等．基于区块链的表后微网系统及其点对点能量块交易模型设计［J］．中国电机工程学报，2021，41（20）：6927－6941.

[2] 吉　斌，昌　力，朱丽叶，等．区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计［J］．电力自动化设备，2021，41（12）：87－94.

[3] 蔡玉涵，王静宇．使用模糊关键字可搜索同态加密的区块链隐私保护方案［J］．小型微型计算机系统，2022，43（11）：2406－2413.

[4] 李　莉，杜慧娜，李　涛．基于群签名与属性加密的区块链可监管隐私保护方案［J］．计算机工程，2022，48（6）：132－138.

[5] 邹　贤，沈　力，张　伟，等．基于信用评分的电力交易区块链改进 RAFT 共识机制［J］．南方电网技术，2022，16（6）：132－139.

[6] 王瑞锦，唐榆程，裴锡凯，等．基于轻量级同态加密和零知识证明的区块链隐私保护方案［J］．计算机科学，2021，48（S2）：547－551.

[7] 谢昕怡，应黎明，田书圣，等．基于 MADDPG 和智能合约的微电网交易决策优化［J］．电力建设，2022，43（11）：142－150.

[8] 郭伟嘉，刘敦楠，王　文，等．基于智能合约的电动汽车充电服务费自适应调整机制［J］．电力自动化设备，2022，42（10）：13－20.

[9] 仝　军，田洪生，吴翠红．考虑节点能量特征的无线传感数据加密传输方法［J］．传感技术学报，2022，35（9）：1277－1281.

[10] 赵梓婷，徐　银，宋祥福，等．基于差分隐私的多模式隐藏动态对称可搜索加密方案［J］．计算机研究与发展，2021，58（10）：2287－2299.

[11] 周　杨，张天骐．多径环境下异步长码直接序列码分多址信号伪码序列及信息序列盲估计［J］．电子与信息学报，2021，43（4）：1137－1144.

[12] 叶　铃，沈伟国，徐建良，等．基于特征值分解的直扩信号信息序列和伪码序列盲估计方法［J］．信号处理，2022，38（7）：1442－1449.

[13] 马春波，石俊杰，王　莹，等．一种自由空间光通信中自适应光电阵列信号处理算法［J］．电子学报，2021，49（10）：1908－1912.

[14] 鲁　军，张源鑫，冯凯旋，等．MSMA 自感知执行器结构设计与信号处理研究［J］．电机与控制学报，2021，25（5）：131－138.

[15] 沈梦萍，段　然，张海燕，等．基于图形处理器的转变边缘传感器读取系统信号处理技术研究［J］．北京师范大学学报（自然科学版），2022，58（2）：203－208.

[16] 曹鹏宇，杨承志，石礼盟，等．基于 PSO－DBSCAN 和 SC-GAN 的未知雷达信号处理方法［J］．系统工程与电子技术，2022，44（4）：1158－1165.

[17] 王忠远，李玉文，王小雨．西门子 S7－200 PLC PPI 通信协议读写命令帧格式的数据解析［J］．无线互联科技，2021，18（21）：1－2.

[18] 高　志，樊锐轶，耿少博，等．基于大数据技术的电力数据质量评估数据框架研究［J］．电子器件，2022，45（1）：194－198.

[19] 贾春福，哈冠雄，武少强，等．加密去重场景下基于 AONT 和 NTRU 的密钥更新方案［J］．通信学报，2021，42（10）：67－80.

[20] 肖　勇，许　卓，罗鸿轩，等．基于属性基加密与阈值秘密共享的智能电表密钥管理方法［J］．南方电网技术，2020，14（1）：31－38.

[21] 陈天伟，康传利，陈　明，等．顾及空间相关特征的最大熵 DEM 插值权系数计算［J］．桂林理工大学学报，2020，40（3）：546－550.

[22] 李家祥，汪凤翔，柯栋梁，等．基于粒子群算法的永磁同步电机模型预测控制权重系数设计［J］．电工技术学报，2021，36（1）：50－59，76.

[23] 林歆悠，郑清香，吴超宇．基于 GA－ECMS 电机转矩优化的混合动力系统协调控制［J］．机械工程学报，2020，56（2）：145－153.

[24] 李耀华，陈桂鑫，王孝宇，等．一种优化感应电机无权重系数无差拍模型预测控制［J］．电机与控制应用，2022，49（3）：18－27.

（上接第 218 页）

[18] 刘　燕．基于 BERT-BiGRU 的中文专利文本自动分类［J］．郑州大学学报（理学版），2023，55（2）：33－40.

[19] ZHU X，SOBHANI P，GUO H，et al. Long short-term memory over recursive structures［C］//International Conference on International Conference on Machine Learning JMLR. org，2015.

[20] ZHOU C，SUN C，LIU Z，et al. A C-LSTM Neural Network for Text Classification［J］. Computer Science，2015，1（4）：39－44.

[21] PETERS M E，NEUMANN M，IYYER M，et al. Deep contextualized word representations［C］//Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics：Human Language Technologies，New Orleans，2018：2227－2237.

[22] 徐　雄．基于深度学习的问答系统研究［J］．湖北师范大学学报（自然科学版），2019，39（1）：10－18.

[23] 张周彬，邵党国，马　磊，等．一种循环互作用注意力的属性级情感分类模型［J］．计算机应用与软件，2020，37（5）：140－144，150.

[24] 高　宸，张　璇，韩梦婷，等．网络空间安全命名实体识别综述（英文）［J］．Frontiers of Information Technology & Electronic Engineering，2021，22（9）：1153－1169.

[25] RADFORD A，NARASIMHAN K，SALIMANS T，et al. Improving language understanding by generative pre-training［EB/OL］. OpenAI Blog，2019：1－12.