文章编号:1671-4598(2025)02-0095-08 DOI:10.16526/j.cnki.11-4762/tp.2025.02.013 中图分类号:TP393 文献标识码:A

基于国密算法的5G移动通信网络远程终端控制系统设计

张燕平，马晓凯，陈冠祯
（中移互联网有限公司，广州 510640）

摘要：通信数据错误加密是导致移动网络主机无法合理控制信息传输行为的主要原因，针对上述问题，设计基于国密算法的5G移动通信网络远程终端控制系统；基于5G移动通信单元结构连接模型，联合通信网络CAN总线仲裁结构、远程移动控制终端，完成硬件模块的设计；按照国密算法模型，生成必要密钥文本，通过定义数字签验的方式，求解具体的杂凑函数；在此基础上，分析通信数据传输行为，完成基于国密算法的5G移动通信网络数据加密；在移动通信网络表决面中，实施5G协议与远程终端协议的转换，并制定具体的通信控制任务划分标准，实现网络远程终端内控制程序的执行，完成基于国密算法的5G移动通信网络远程终端控制系统的设计；实验结果表明，所设计系统可将通信数据编码码源长度、译码码源长度之间的误差控制在0～0.15 bit的误码允许范围之内，有效减少因通信数据错误加密而导致移动网络主机无法合理控制信息传输行为的问题。

关键词：国密算法；5G移动通信网络；远程终端；CAN总线；协议转换

Design of Remote Terminal Control System of 5G Mobile Communication Network Based on State Secret Algorithm

ZHANG Yanping, MA Xiaokai, CHEN Guanzhen
(China Mobile Internet Co., Ltd., Guangzhou 510640, China)

Abstract: Communication data encryption errors are the main reason why mobile network hosts cannot reasonably control information transmission behavior. In response to the above issues, a 5G mobile communication network remote terminal control system based on the national security algorithm is designed. Based on the connection model of 5G mobile communication unit structure, combined with the CAN bus arbitration structure of the communication network and remote mobile control terminal, the hardware module design is completed. According to the national security algorithm model, generate the necessary key text, and solve the specific hash function by defining a digital signature. On this basis, analyze the communication data transmission behavior and complete the 5G mobile communication network data encryption based on the national security algorithm. In the voting surface of mobile communication networks, implement the conversion of 5G protocol and remote terminal protocol, and develop specific communication control task division standards to achieve the execution of control programs within network remote terminals, and complete the design of 5G mobile communication network remote terminal control system based on national security algorithm. Experimental results show that the designed system can control the error between the length of the communication data encoding code source and the length of the decoding code source within an allowable error rate range of 0～0.15 bit, effectively reducing the problem of mobile network hosts being unable to reasonably control information transmission behavior due to the errors of communication data.

Keywords: state secret algorithm; 5G mobile communication network; remote terminal; CAN bus; protocol conversion

收稿日期:2023-11-29； **修回日期**:2024-04-25。

作者简介:张燕平(1985-),男,硕士。

引用格式:张燕平,马晓凯,陈冠祯. 基于国密算法的5G移动通信网络远程终端控制系统设计[J]. 计算机测量与控制,2025,33(2):95-102.

0 引言

5G 移动通信是实现人机物互联的基础网络设施[1]，具有连接速率快、时延水平低、数据传输量大的特点。相较于其他类型的通信网络，5G 移动通信采用全新的服务架构模型，可对数据节点进行更加灵活的部署，在差异化业务场景下，只要保证主机元件的连接稳定性，客户端主机对于通信平台的响应行为就不会发生中断。基层 5G 单元配件支持灵活性的部署，在 NFV/SDN 模型中，硬件组织与软件程序的相互解耦实现了通信程序的转发与分离，且由于通信网络始终保持较为稳定的连接状态，所以已输出数据信息参量能够在信道组织的配合下，顺利传输至目标通信节点之中。在远程终端体系中，5G 移动网络具有独立的通信环境，可将目标用户划分为多个服务区域，且由于信道组织的连接符合唯一指向性原则，所以该类型网络结构能够避免数据信息参量出现错传或误传的情况。随着通信技术的快速变革，5G 移动网络的布局形式也在不断发生变化，使得通信数据的实时累积量持续增加，如何避免出现通信数据的错误加密行为成为一项亟待解决的问题。

文献［2］设计的反馈控制系统，利用 HL-2A 装置开发独立的通信网络连接环境，配合步进式脉冲调节通信数据传输行为，又联合可编程门阵列器件组合，调度处于空闲状态的 DSP 单元，从而避免通信数据在远程终端体系中表现出错误传输行为。文献［3］设计的面向数据可用性的通信控制系统，依照会话层单元与物理层单元之间的层间映射依赖关系，建立通信传输模型，又分别从自上向下、自下向上两个方向，完成对 5G 通信数据实时传输行为的建模，并根据运算结果，制定具体的通信控制方案。

国密算法是一种非对称性加密原则，以 SM2 数字签名作为编码基础，按照椭圆曲线对公钥密码进行排序处理，打破了原有的 256 位阶数限制条件，可以在定义高级源码的同时，完成密码模板的验签与识别。相较于其他类型的密码编译方案，国密算法不要求码源密钥定义长度的一致性，无论是 233 比特、679 比特还是 181 比特的码源密钥，只要其编码形式符合国密算法的定义形式，依照当前模板编译所得的信息参量就符合国密算法的认定标准[4]。在实际应用过程中，反馈控制系统、数据可用性控制系统对于数据编码码源、译码码源之间长度误差的控制能力相对有限，并不能有效解决移动网络主机无法合理控制信息传输行为的问题。为避免上述情况的发生，利用国密算法应用优势，设计一种新型的 5G 移动通信网络远程终端控制系统，并通过对比实验的方式，突出该系统的实际应用价值。

1 5G 移动通信网络远程终端控制系统设计

5G 移动通信网络远程终端控制系统的硬件应用部分包括 5G 移动通信单元、通信网络 CAN 总线仲裁结构、远程移动控制终端，本章节针对其具体设计方法展开研究。

1.1 5G 移动通信单元

5G 移动通信单元由上层发送端、5G 通信主机、通信网络及 OSI 移动通信组织 4 部分组成。其中，上层发送端负责向外发送通信数据参量，在远程终端体系中，该部件单元中所有数据信息都保持未加密的编码形式。5G 通信主机作为移动通信网络上层发送端的下级负载结构，其内部存储了大量的移动信息参量。在 5G 移动通信网络远程终端控制系统中，只有得到加密编码的数据信息才能得到远程终端的认证，所以通信主机在区分首帧、连续帧与尾帧对象时，必须遵循国密算法原则。5G 移动通信单元不具有全域性覆盖的能力，因此在传输数据文本的过程中，只有保持局域性组网状态的通信网络才符合编码后通信数据的传输需求[5]。完整的 5G 移动通信单元结构连接模型如图 1 所示。

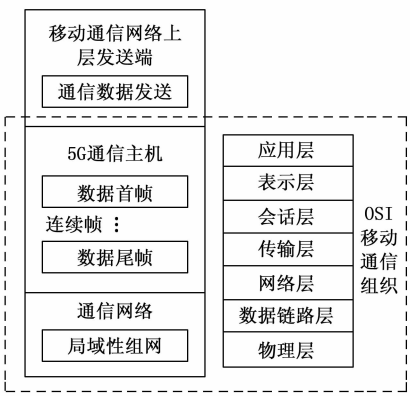

图 1 5G 移动通信单元的结构连接模型

OSI 移动通信组织是复杂的单元型部件结构，其内部包含 7 个不同的层级模块组织，上部应用层、表示层、会话层内所传输通信数据的编码格式完全相同，从功能性角度来看，属于未经国密算法认证的源码信息参量；中部传输层、网络层具有一定的加密认证能力，可以按照功能性的不同，对上层单元输出的通信数据进行初步加密处理；下部数据链路层、物理层负责对通信数据进行整合处理，在功能性角度，属于经过国密算法认证的密码信息[6]参量。

1.2 通信网络 CAN 总线仲裁结构

在 5G 移动通信网络中，CAN 总线对于远程终端体系的控制仲裁是非破坏性的，通信数据帧中的 ID 信息定义了当前数据对象在 CAN 总线中的传输优先级。为

保证数据信息的稳定传输，通信设备之间保持并列连接关系，每一个设备部件占据一条独立的 CAN 总线和一条独立的 REQ 线路，前者可将通信设备输出的数据信息参量反馈至仲裁器部件之中，后者则可以将远程终端内保持线性传输状态的通信数据参量整合成包状传输形式，以便于仲裁器部件对其进行直接调取与利用[7]。CAN 总线中有多个通信设备在同一时间节点向外输出信息参量，且在经过仲裁器部件的裁定处理后，这些信息参量可被直接存储于远程终端组织之中。对于仲裁器部件而言，CAN 总线、REQ 线路的连接状态完全相反，CAN 总线接入、REQ 线路中断，表示通信数据由 5G 移动网络汇入远程终端组织；CAN 总线中断、REQ 线路接入，表示通信数据由远程终端组织反馈回 5G 移动网络[8]。具体的 CAN 总线仲裁结构连接情况如图 2 所示。

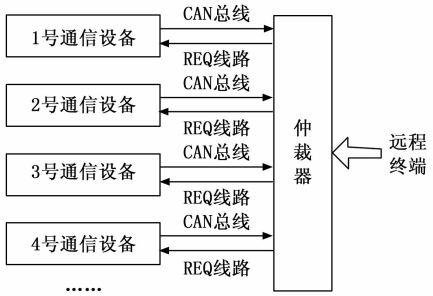

图 2　5G 移动通信网络中 CAN 总线仲裁结构连接示意图

为配合 5G 移动通信单元的运行需求，仲裁器单元必须保持实时响应状态。由于 CAN 总线、REQ 线路是两条完全独立的信息传输通路，且其内部所传输信息参量的编码格式并不相同。所以仲裁器在依照国密算法加密通信数据时，应具有双向识别信息参量的能力。

1.3　远程移动控制终端

远程移动控制终端直接接收 5G 移动通信网络输出的数据信息参量，是控制系统的核心运行部件，可以配合多字节通信模块、控制模块等多个单元性组织，完成对通信数据的加密处理，由于 5G 移动通信网络对于数据信息参量的筛选较为严格，所以远程移动控制终端所执行的加密处理完全遵循国密算法原则。数据信息传输的过程中，5G 移动通信网络、多字节通信模块之间存在明显的双向反馈关系，且无论信息远程识别模块、控制模块、通信数据存储终端三类下级部件结构是否保持开放状态，这种信息参量的双向传输反馈行为都不会受到影响[9]。多字节通信模块完成对 5G 通信数据的录入后，数据信息参量随着信道组织进入信息远程识别模块中，此传输行为不会造成数据消耗。控制模块可对通信数据进行移动协调处理，但这种操作行为具有一定的时效性，简单来说就是在 CAN 总线开放的情况下，只有以仲裁器刚刚选取的通信数据作为处理对象，所得控制指令才能得到远传终端设备的认可。详细的远程移动控制终端模块组成形式如图 3 所示。

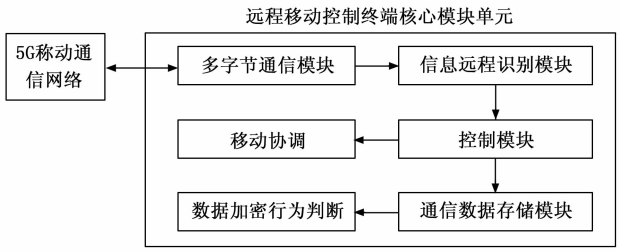

图 3　远程移动控制终端的模块组成结构

通信数据存储模块相当于移动控制终端的数据库单元，对于控制模块输出的通信数据信息进行无差别存储，但由于其额定存储能力相对有限，所以只有满足国密算法加密原则的信息参量才能在此单元中生成长期存储文件，该过程就是存储模块对于数据加密行为[10]的判断。

2　基于国密算法的 5G 移动通信网络数据加密

对于国密算法模型的定义就是依照密钥文本，完成数字签验，从而求得具体的杂凑函数，本章节在该算法模型的基础上，针对 5G 移动通信网络中符合远程终端控制需求的数据信息参量实施加密处理。

2.1　国密算法模型的定义

2.1.1　国密密钥的生成

国密密钥是通过输入私钥来生成的，将通信数据与 5G 移动通信网络中的节点相匹配，得到的信息定义模板即为国密密钥。在 5G 移动通信网络中，主机元件对每一个通信数据都进行赋值处理，即便是在两个数据对象信息格式与存储长度完全相同的情况下，由于其所处传输周期不同，网络主机给予两个数据对象的赋值结果也不相同[11]。数据文本在 5G 移动通信网络中所处的实时传输位置影响远程终端控制主机对信息参量的加密处理能力，通常情况下，数据文本在系统数据库主机中的存储位置越靠前，就表示远程终端在控制该类型信息参量时所需消耗的密钥源码越少，与当前数据对象匹配的实时通信速率也就越快[12]。

ω 表示数据文本在 5G 移动通信网络中的实时传输位置定义参数，其取值满足公式（1）所示的条件：

$$\omega \in (0,+\infty) \tag{1}$$

在公式（1）的基础上，推导移动通信数据的国密密钥生成条件表示为：

$$M_{\omega}=\frac{1}{\omega^{2}-1}\cdot\sqrt{\frac{\sum\limits_{\psi\to\infty}^{\infty}|\xi\times\vec{b}|^{\psi}}{m_{1}^{2}+m_{2}^{2}+\cdots+m_{n}^{2}}} \tag{2}$$

m_1、m_2、…、m_n 表示 5G 移动通信网络中 n 个不相等也不为零的数据文本定义参量，ψ 表示密码码源查询系数，$\vec{b}$ 表示国密密钥条件下的移动通信数据传输向量，ξ 表示通信数据实时编码参数。国密密钥对于 5G 移动通信数据的加密依照随机性原则筛选必要信息参量，因此单位加密周期内，极易出现两个完全相同的数据对象，但为保证编码结果的唯一性，应分别针对两个数据样本定义源码参量，并将其放置在不同的通信周期之中。

2.1.2 国密密码的数字签验

数字签验就是利用已经得到的密码向量，对符合国密密码的 5G 移动通信网络数据数字签名进行验证处理。远程终端内通信数据的输入具有明显的连贯性特征，且相邻信息参量的间隔周期必然小于网络体系的额定跳频周期时长[13]。5G 移动通信网络的额定跳频周期就是指数据参量由实时传输状态转变为稳定加密状态所需消耗的时间，一般来说，该项时间条件的数值水平越高，就表示远程终端体系在单位时间内所能存储的通信数据样本总量越多[14]。国密算法规定数字签验是加密通信数据的必要环节，为实现对远程终端体系的有效控制，只有先在 5G 移动通信网络中定义唯一的密码模板，并按照该模板整合所有需要加密的信息参量，才能保证数字签验结果符合国密算法模型的加密标准。

设 ΔC 表示单位加密周期内 5G 移动通信网络数据的单位累积量，$\dot{X}$ 表示基于国密算法模型的通信数据认证特征，σ 表示 5G 移动通信网络中数据样本的额定跳频参量，ζ 表示 5G 移动通信网络数据的数字化标定参数，且 $\zeta \neq 0$ 的不等式取值条件恒成立，$\boldsymbol{v}_{\max}$ 表示通信数据密码码源向量的最大取值，$\boldsymbol{v}_{\min}$ 表示码源向量的最小取值。在上述物理量的支持下，联立公式（2），可将国密密码的数字签验表达式定义为：

$$B=\sqrt{\sigma\frac{\dot{X}}{\zeta\cdot|\Delta C|}}\cdot[M_{\omega}\cdot(\boldsymbol{v}_{\max}-\boldsymbol{v}_{\min})] \tag{3}$$

5G 移动通信网络的开放具有持续性特征，所以依照国密算法完成数字签验处理时，应在远程终端内选择连续传输的数据样本作为运算对象。

2.1.3 国密算法杂凑函数求解

国密算法杂凑函数是散列函数的一种，由于其无法按照散列函数的反函数条件推导出原始输入数据是什么，所以杂凑函数是具有单向运算特征的加密算法函数。在 5G 移动通信网络中，满足国密算法杂凑函数输入条件的数据样本被称为直接控制信息，既可以是任意有限长度的比特串，也可以是长度水平保持定值状态的字符或字段[15-16]。依照国密算法完成 5G 移动通信网络数据加密处理时，远程终端控制主机输出结果被称为摘要或消息摘要，而杂凑函数对于任意一个给定摘要都必须运算出其散列水平，特别是在数据样本散列值较为接近的情况下，只有保证密码码源的不可修正性，才能够保证数据加密结果的准确性。对于国密算法杂凑函数的求解参考如下表达式：

$$Z=(\tau+1)^2\cdot\frac{\upsilon B}{\prod\limits_{\varpi=1}^{+\infty}\hat{l}\widetilde{x}} \tag{4}$$

其中：τ 表示 5G 移动通信网络中的消息摘要定义参数，υ 表示远程终端内的通信数据输出系数，ϖ 表示通信数据字段长度定义参数，$\widetilde{x}$ 表示国密算法密码码源的非可修正数值指征，$\hat{l}$ 表示基于国密算法所认证的通信数据传输长度标准值。如果将 5G 移动通信网络看作一个非完全封闭的空间环境，那么在实时数据加密的过程中数据输入、数据输出行为也就同时存在，这就表示网络单元的动态化等级相对较高，远程终端体系为实现对数据通信行为的有效控制，只能依照国密算法杂凑函数对所涉及信息参量进行分级加密处理。

2.2 5G 移动通信网络传输信息的实时加密

5G 移动通信网络对于传输信息的实时加密就是按照国密算法模型完成对通信数据的认证处理。从功能性角度来看，控制系统的实时加密服务主要包括如下几方面内容：

1）确认服务：此服务被通信网络 CAN 总线仲裁结构使用，主要是用来向远程移动控制终端等硬件应用装置所接收到的通信数据参量进行确认处理，在制定确认标准时，控制系统对于信息参量的处理遵循国模算法原则。

2）指示服务：此服务被 5G 移动通信网络所使用，用来描述通信数据的具体传输状态，服务对象为国密算法的直接加密目标，每一个指示参量都能够得到系统控制主机的直接调取与利用[17-18]。

3）请求服务：此项服务为国密算法原则的基础服务权限，在 5G 移动通信网络中，请求服务指令的实时执行量越大，就表示远程终端所需处理的通信数据总量越多，每一条控制指令的传输只对应一类完成加密的数据信息参量[19-20]。

基于国密算法的 5G 移动通信网络数据加密处理表达式如下：

$$L=\int_{-\infty}^{+\infty}\left(\frac{\overline{A}}{\dot{K}}\right)^2\cdot Z\cdot\vartheta\times\frac{1}{\sum|\theta\vec{j}|^{-2}} \tag{5}$$

$\dot{K}$ 表示 5G 移动通信网络数据的加密指代特征，$\overline{A}$ 表示单位时间内的密码码源定义量均值，ϑ 表示远程终端内的通信数据认证系数，$\vec{j}$ 表示国密算法密码码源的请求向量，θ 表示国密算法密文码源对于通信数据的响

应参数。

3　实现网络远程终端控制

国密算法是政府制定并推广使用的密码算法标准，其目的是保护通信网络中的数据安全。通过使用国密算法对通信数据进行加密，可以防止未经授权的访问者获取或篡改数据，为实现网络远程终端控制提供了安全的数据基础。网络远程终端控制程序只有在移动通信网络表决面中才能得到运行，因此本章节研究内容根据选取所得通信网络表决面，完成 5G 协议与远程终端协议的转换处理，再根据通信控制任务划分标准，定义具体的控制执行程序，从而完成基于国密算法的 5G 移动通信网络远程终端控制系统的设计。

3.1　移动通信网络表决面选取

移动通信网络表决面是保持套叠关系的数据样本加密平面，每一平面内都有一部分数据信息参量会被下一个平面组织完全覆盖，但这些被覆盖的信息参量并不会完全消失，而是会以数值映射的方式表现在下一平面组织之中，因此移动通信网络表决面中的数据样本具有循环传输能力，这就表示系统主机在对数据信息文本进行控制时，可对远程终端所获得的数据对象进行多次加密处理。此外，国密算法规定移动通信网络表决面之间的覆盖关系应大于单一平面组织物理面积的 25%，但又不得超过单一平面组织物理面积的 50%[21-22]。在不超过上述数值限制范围的情况下，相邻移动通信网络表决面的套叠程度越大，就表示数据样本在远程终端内的传输行为越频繁。具体的移动通信网络表决面套叠关系如图 4 所示。

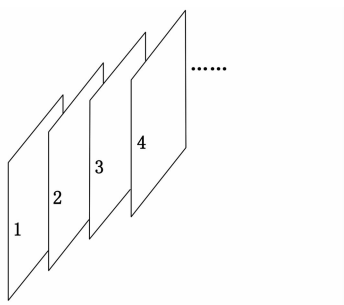

图 4　移动通信网络表决面

在公式（5）的基础上，推导移动通信网络表决面选取表达式如下：

$$D=\mu\times\frac{(d_1+d_2+\cdots+d_n)}{\frac{\hat{S}^2}{fL}} \tag{6}$$

d_1、d_2、…、d_n 为依照国密算法定义的 n 个移动通信网络表决面对象，$\hat{S}$ 为套叠网络表决面的面积限制阈值，μ 为移动通信网络表决面组织内数据信息参量的循环传输向量，f 为表决面覆盖区域内的通信数据套叠参数。关于国密算法的 5G 移动通信网络数据加密总量不为零，所以表决面完全覆盖区域内不可能存在通信数据零套叠的情况。

3.2　5G 协议与远程终端协议转换

5G 协议与远程终端协议转换是 5G 移动通信网络中一种普遍存在的信息处理行为。远程终端主机在完成通信数据加密处理后所筛选出的所有通信数据参量都符合 5G 协议认证条件，在控制信息传输行为的过程中，这些数据参量并不具有普遍传输的能力，故而也就不满足实时控制的系统运行需求[23]。符合远程终端协议认证条件的通信数据参量的实时传输能力较强，在 5G 移动通信网络中其传输行为不受到任何的限制作用，因此较为符合控制系统的实际运行需求。

规定 ν 表示依照 5G 协议所定义的通信数据认证向量[24-25]，$\boldsymbol{o}$ 表示依照远程终端协议所定义的通信数据认证向量，且 $\nu>\boldsymbol{o}$ 的不等式取值条件恒成立，联立公式（6），推导基于国密算法的 5G 协议与远程终端协议转换表达式为：

$$G_{\nu\to o}=\lambda\times\left|\frac{h_\nu g_\nu-h_{\boldsymbol{o}}g_{\boldsymbol{o}}}{D}\right|^{\sqrt{1-\nu/o}} \tag{7}$$

g_ν 表示 5G 协议下的通信数据定义项，h_ν 表示基于参数 ν 的数据传输行为控制指征，$g_{\boldsymbol{o}}$ 表示远程终端协议下的通信数据定义项，$h_{\boldsymbol{o}}$ 表示基于参数 $\boldsymbol{o}$ 的数据传输行为控制指征，λ 表示基于国密算法的协议文本转换系数。远程终端控制系统的运行同时匹配 5G 移动通信数据的输入与输出行为，所以网络体系的开放状态也会影响主机元件对信息传输行为的控制[26-27]能力。

3.3　5G 移动通信网络远程终端控制方法

通信控制任务划分就是按照国密算法原则确定远程终端控制程序在 5G 移动通信网络中所必须经过的行为区域，通常情况下，控制程序必须经过的行为区域越多，就表示通信数据样本的实时传输序列越快，通信控制任务的当前划分等级也就越高。5G 移动通信网络的单位传输周期内，远程终端对于信息参量的选择遵循国密算法原则，且每一个加密信息只能对应唯一的控制任务划分标准[28-30]。依照国密算法对于通信控制任务划分条件，实现网络远程终端控制，参考公式（8）：

$$Q=\kappa G_{\nu\to o}-\dot{E}\sqrt{\left(\frac{q_1}{\iota_1}\right)^2+\left(\frac{q_2}{\iota_2}\right)^2+\cdots+\left(\frac{q_n}{\iota_n}\right)^2} \tag{8}$$

其中：$\dot{E}$ 为 5G 移动通信网络单位传输周期内的数据样本认证特征，q_1，q_2，…，q_n 为 n 个不相等的控制任务执行等级判定参数，ι_1、ι_2、…、ι_n 分别表示与判定参数相关的控制执行指令划分阈值，κ 表示通信数据传输行为

的实时控制参数。至此，完成对相关参数指标的计算与处理，在各级硬件应用结构的配合下，按照国密算法原则，实现对 5G 移动通信网络远程终端的控制。

4 实例分析

选择基于国密算法的 5G 移动通信网络远程终端控制系统、反馈控制系统、面向数据可用性的通信控制系统 3 种不同方法进行实验，根据通信数据编码码源长度、译码码源长度之间的差值水平，判断所应用方法的应用可行性。

4.1 实验准备

5G 移动通信网络负载了大量的传输数据，且这些数据对象的目标传输位置并不相同，在保证网络体系运行稳定性的前提下，选择 6 类不同的通信数据作为实验对象，并将这些数据参量输入 TensorFlow 软件之中，测量通信数据的编码码源长度，具体测量结果如表 1 所示。

表 1 通信数据编码码源长度

通信数据分类	编码码源长度/bit
第一类	0.48
第二类	0.35
第三类	0.57
第四类	0.42
第五类	0.63
第六类	0.39

选择 A02B-0319-D565 型号的通信主机作为实验对象，根据公式（9），求解该型号主机元件所能承载的码源长度误差。

$$\beta = \frac{3\varphi}{\gamma} \tag{9}$$

φ 为通信数据的标准编码参数，γ 为通信数据传输周期。对于 A02B-0319-D565 型号通信主机而言，φ 参数取值恒为 0.1 bit/ms，γ 参数取值恒为 2 ms，所以码源长度误差 β 的计算数值为 0.15 bit，因此本次实验过程中，只要通信数据编码码源长度、译码码源长度之间的误差保持在 0～0.15 bit 之内，就表示所应用系统的控制能力较强。

4.2 实验流程

本次实验的具体实施流程如下：

1）闭合开关开始实验，利用 JTY-GD-A20 装置检测通信主机的实时运行稳定性。

2）将基于国密算法的 5G 移动通信网络远程终端控制系统执行程序输入 TensorFlow 软件，记录该系统作用下，通信数据译码码源长度的数值水平，所得结果为实验组变量。

3）将反馈控制系统执行程序输入 TensorFlow 软件，记录该系统作用下，通信数据译码码源长度的数值水平，所得结果为对照 A 组变量。

4）将面向数据可用性的通信控制系统执行程序输入 TensorFlow 软件，记录该系统作用下，通信数据译码码源长度的数值水平，所得结果为对照 B 组变量。

5）分别计算实验组、对照 A 组、对照 B 组译码码源长度与表 1 所示编码码源长度的差值，并根据求解结果总结实验结论。

4.3 数据与结论

4.3.1 网络远程终端控制能力分析

译码码源长度较长意味着需要传输和处理的数据量更大，传输数据量大，则表明系统的控制能力越好。实验组、对照 A 组、对照 B 组通信数据译码码源长度的具体实验数值如图 5 所示。

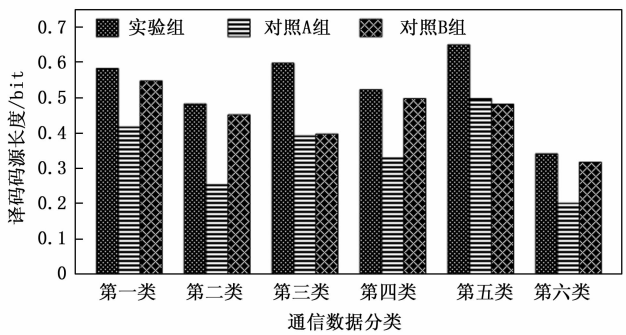

图 5 通信数据译码码源长度

分析图 5 可知，实验组、对照 A 组、对照 B 组通信数据译码码源长度均未与数据编码码源长度保持完全相等的数值状态，但明显实验组译码码源的均值水平相对较高。

4.3.2 网络远程终端控制效果分析

基于表 1、图 5 所示的实验结果，求解通信数据编码码源长度、译码码源长度之间的数值差，具体计算结果如表 2 所示。

表 2 通信数据编码码源长度、译码码源长度差

数据分类	实验组/bit	对照 A 组/bit	对照 B 组/bit
第一类	0.03	0.06	0.07
第二类	0.03	0.09	0.11
第三类	0.03	0.16	0.17
第四类	0.01	0.09	0.08
第五类	0.03	0.13	0.20
第六类	0.05	0.18	0.07

分析表 2 可知，整个实验过程中，实验组通信数据

编码码源长度、译码码源长度差最大值只能达到 0.05 bit，所有实验结果全部属于 0～0.15 bit 的数值范围之内；对照 A 组系统作用下，第三类、第六类通信数据编码码源长度、译码码源长度差均超过了 0～0.15 bit 的数值范围，实验过程中其均值水平高于实验组；对照 B 组系统作用下，第三类、第五类通信数据编码码源长度、译码码源长度差的超过了 0～0.15 bit 的数值范围，其实验均值也明显高于实验组数值。

综上可知，反馈控制系统、面向数据可用性的通信控制系统的应用并不能实现对通信数据编码码源长度、译码码源长度误差的有效控制，故而这两类系统并不能解决通信数据错误加密的问题；应用基于国密算法的 5G 移动通信网络远程终端控制系统，可将通信数据编码码源长度、译码码源长度误差完全控制在 0～0.15 bit 的数值范围之内，能够解决通信数据错误加密的问题，在促进移动网络主机合理控制信息传输行为方面具有突出作用价值。

5　结束语

基于国密算法的 5G 移动通信网络远程终端控制系统设置了独立的 5G 移动通信单元、通信网络 CAN 总线仲裁结构与远程移动控制终端，对于主机元件而言，其在各级硬件单元结构的配合下，完成对通信数据的加密处理，从而保障控制执行指令的顺利实施。相较于反馈控制系统、面向数据可用性的通信控制系统，该系统的应用能够解决通信数据错误加密的问题，从而在促进移动网络主机合理控制信息传输行为的同时，避免通信数据编码码源长度、译码码源长度出现较大误差，与实际应用需求相符合。

参考文献：

[1] 刘春林，秦　进. 面向 5G 网络的移动边缘计算节点部署算法设计 [J]. 计算机仿真，2022，39 (12)：436－439.

[2] 陈　勇，王英翘，李华俊，等. 脉冲步进调制高压电源远程通讯与反馈控制系统研究 [J]. 核聚变与等离子体物理，2021，41 (3)：252－257.

[3] 王梓宇，王镜毓，谢　俊，等. 面向数据可用性的电力通信系统静态分层建模方法 [J]. 电力系统自动化，2021，45 (20)：9－17.

[4] 何之煜，朱建设，李治岩. 基于国密算法的 IPSec VPN 技术在 LKJ 无线换装系统中的实现 [J]. 铁道标准设计，2021，65 (12)：141－145.

[5] 于　浩，汪筱巍，王　韬，等. 基于 SDN 与 NFV 的电力 5G 网络切片差异化资源分配方案 [J]. 电测与仪表，2021，58 (9)：89－95.

[6] 陈　亮，高　洁，李亚军，等. 用于 5G 移动终端 N77 频段的低噪声放大器设计 [J]. 固体电子学研究与进展，2022，42 (6)：498－504.

[7] 周芳芳，毛索颖，黄跃文，等. 基于线阵 CCD 和 CAN 总线通信的引张线仪的设计与实现 [J]. 长江科学院院报，2021，38 (4)：150－154.

[8] 张之森，李　芳，王丽芳，等. 基于 HMAC 和 TEA 算法的 CAN 总线身份认证方法研究 [J]. 电工电能新技术，2021，40 (9)：57－63.

[9] 朱志忠，袁　鑫，赵　丰，等. 考虑作动器输出饱合的光电平台终端滑模神经网络控制 [J]. 振动与冲击，2022，41 (21)：161－167.

[10] 江道根，吕龙进，潘世华，等. 移动机器人轨迹跟踪快速终端滑模自抗扰控制 [J]. 控制工程，2022，29 (1)：91－100.

[11] 李楠楠，韩　瑜，高　宁，等. 基于幅度和相位联合分区的无线物理层密钥生成方法 [J]. 电信科学，2021，37 (5)：100－112.

[12] 唐　杰，文　红，宋欢欢，等. 基于智能反射表面辅助的 MIMO 无线通信密钥快速生成 [J]. 电子与信息学报，2022，44 (7)：2264－2272.

[13] 卫宏儒，黄靖怡. SOTS：一个基于哈希函数更短的后量子数字签名方案 [J]. 计算机研究与发展，2021，58 (10)：2300－2309.

[14] 赖建昌，黄欣沂，何德彪，等. 国密 SM9 数字签名和密钥封装算法的安全性分析 [J]. 中国科学：信息科学，2021，51 (11)：1900－1913.

[15] 王凯光，高岳林，刘航宇，等. 基于广义罚函数可行性准则的 DE 算法对不确定数据的处理 [J]. 控制与决策，2021，36 (2)：498－504.

[16] 张晓亚，刘建勋，倪元相，等. 基于反正切函数的 LMS 自适应滤波算法及应用 [J]. 弹箭与制导学报，2022，42 (1)：114－117.

[17] 崔琪楣，赵文静，顾晓阳，等. 面向 B5G 网络的高效切换认证与安全密钥更新机制 [J]. 通信学报，2021，42 (12)：96－108.

[18] PADMA B，BABU E. End-to-end communication protocol in IoT-enabled ZigBee network：investigation and performance analysis [J]. Internet Things，2023，22：100796.

[19] 周贤韬，江英华，郭晓军，等. 带双向身份认证的基于单光子和 Bell 态混合的量子安全直接通信方案 [J]. 物理学报，2023，72 (13)：17－25.

[20] SETH B，DALAL S，JAGLAN V，et al. Integrating encryption techniques for secure data storage in the cloud [J]. Transactions on Emerging Telecommunications Technologies，2022，33 (4)：e4108.

[21] 张露维，顾荣斌，李　静，等. FSD：增量压缩中局部特

征表决的快速相似性检测 [J]. 小型微型计算机系统，2021，42 (5)：977－983.

[22] 陈健锋，崔 苗，张广驰，等. 双智能反射平面辅助无线携能通信系统的安全通信优化 [J]. 电信科学，2022，38 (1)：47－60.

[23] 张协力，祝跃飞，顾纯祥，等. C2P：基于 Pi 演算的协议 C 代码形式化抽象方法和工具 [J]. 软件学报，2021，32 (6)：1581－1596.

[24] SUN J，KHAN F，LI J，et al. Mutual authentication scheme for the device-to-server communication in the Internet of medical things [J]. IEEE Internet of Things Journal，2021，8 (21)：15663－15671.

[25] FENG C，YU K，BASHIR A K，et al. Efficient and secure data sharing for 5G flying drones：a blockchain-enabled approach [J]. IEEE Network，2021，35 (1)：130－137.

[26] 孙 汉，杨亚联，周 林，等. 基于正则表达式与多叉树的 DBC 网络协议解析方法 [J]. 重庆大学学报，2022，45 (8)：78－86.

[27] CAI W，NIU X. Analysis and research of communication network system based on low power loss routing protocol [J]. International Journal of Global Energy Issues，2024，46 (1/2)：59－68.

[28] 郑 重，何 锋，李浩若，等. 基于贪婪随机自适应搜索法的 TTE 通信调度算法 [J]. 北京航空航天大学学报，2021，47 (11)：2268－2276.

[29] 李本良，李显鑫，侯树政，等. 高压输电线路共享杆塔的 5G 通信设备表面电场计算方法 [J]. 南方电网技术，2021，15 (10)：65－71.

[30] AL-HRAISHAWI H，MATURO N，LAGUNAS E，et al. Scheduling design and performance analysis of carrier aggregation in satellite communication systems [J]. IEEE Transactions on Vehicular Technology，2021，70 (8)：7845－7857.

(上接第 87 页)

[10] 皮 骏，黄江博，黄 磊，等. 基于改进 QPSO-SVR 的航空发动机排气温度预测 [J]. 振动·测试与诊断，2019，39 (2)：267－272.

[11] 皮 骏，马 圣，张奇奇，等. 基于改进果蝇算法优化的 GRNN 航空发动机排气温度预测模型 [J]. 航空动力学报，2019，34 (1)：8－17.

[12] 杨洪富，贾晓亮. 基于 LSTM 的航空发动机排气温度预测 [J]. 航空计算技术，2018，48 (4)：61－65.

[13] JI Z，GAN H，LIU B. A deep learning-based fault warning model for exhaust temperature prediction and fault warning of marine diesel engine [J]. Journal of Marine Science and Engineering，2023，11 (8)：240－152.

[14] WENGANG Z. Aero-engine exhaust gas temperature prediction based on adaptive disturbance quantum-behaved particle swarm optimization [J]. Advances in Mechanical Engineering，2022，14 (8)：50－64.

[15] LI D，PENG J，HE D. Aero-engine exhaust gas temperature prediction based on light GBM optimized by improved bat algorithm [J]. Thermal Science，2021，25 (2A)：845－858.

[16] GUANG B，YU G. Aeroengine exhausted gas temperature prediction by process extreme learning machine [J]. Journal of Convergence Information Technology，2013，8 (6)：1－8.

[17] LI G Q，QI X B，CHEN B，et al. Fast learning network with parallel layer perceptrons [J]. Neural Processing Letters，2017，13 (3)：237－251.

[18] MIRJALILI S，MIRJALILI S M，LEWIS A. Grey wolf optimizer [J]. Advances in Engineering Software，2014，69 (7)：46－61.

[19] NIU P F，WANG Q Y，MA Y P，et. al. Study on NOx emission characteristics of boiler based on quantum adaptive bird swarm algorithm [J]. Acta Metrologica Sinica，2017，38 (6)：770－775.

[20] FENG L H，GUI W H，YANG F. Low nox combustion optimization of utility boiler based on improved POS [J]. Journal of System Simulation，2011，23 (12)：2812－2815.

[21] LAI M，CHEN G S，LIU C，et. al. Application of ca-woa-elm hybrid model in boiler no _ X emission forecast [J]. Journal of Chinese Society of Power Engineering，2018，38 (11)：874－879.

[22] 王晓燕，白贤明，宋 辞，等. 基于 EMD-LSTM 模型的 APU 排气温度预测 [J]. 航空动力学报，2024，39 (8)：393－399.

[23] 皮 骏，马 圣，张奇奇，等. 基于改进果蝇算法优化的 GRNN 航空发动机排气温度预测模型 [J]. 航空动力学报，2019，34 (1)：8－17.

[24] 陈庆贵，李洪伟，李 明，等. 基于径向基过程神经网络的航空发动机排气温度预测 [J]. 兵器装备工程学报，2019，40 (6)：154－157.

[25] 于广滨，丁 刚，姚 威，等. 基于支持过程向量机的航空发动机排气温度预测 [J]. 电机与控制学报，2013，17 (8)：30－36.