区块链技术支持下通信数据实时加密算法的设计研究

樊帆[1]，周妍婷[2]
1. 中国空间技术研究院，北京 100094
2. 中国空间技术研究院西安分院，陕西 西安 710100
DOI: 10.61369/TACS.2025080039

摘　　要： 为防止通信数据发生泄露、提高通信数据加密安全性，提出一种区块链技术支持下的通信数据实时加密算法。在数字签名、同态加密的基础上，通过计数器模式，对通信数据进行安全加密。通过验证分析可以看出，该算法在通信数据加密中表现出较高的安全性与可靠性，具有良好的应用价值。
关 键 词： 通信数据；区块链技术；数字签名；同态加密；计数器模式

Research on the Design of Real-Time Encryption Algorithm for Communication Data Supported by Blockchain Technology

Fan Fan[1], Zhou Yanting[2]
1.China Academy of Space Technology, Beijing 100094
2.China Academy of Space Technology, XI'AN Branch, Xi'an, Shaanxi 710100

Abstract: To prevent the leakage of communication data and improve the encryption security of communication data, this paper proposes a real-time encryption algorithm for communication data supported by blockchain technology. Based on digital signature and homomorphic encryption, the algorithm performs secure encryption on communication data through the counter mode. Verification and analysis show that the algorithm exhibits high security and reliability in communication data encryption, and has good application value.
Keywords: communication data; blockchain technology; digital signature; homomorphic encryption; counter mode

引言

通信数据实时加密是一种保障网络通信数据安全性的技术，它通过对传输数据以及传输过程进行实时动态加密，确保数据在传输过程和读写中不被未授权第三方截获以及明码解读。这种技术通常应用于移动应用和网络服务中，以防止数据泄露和篡改，从而保护用户的隐私和数据的安全。有学者基于加权傅里叶变换数学模型对数据帧进行替换处理，设定通信数据加密传输密钥，设计加密传输流程，实现了通信数据加密传输，但加密及解密的时效性不理想[1]。还有学者采用混沌映射技术进行通信加密，实现了安全加密，然而如果在较复杂的解密环境中，该方法容易发生解密失误的情况[2]。因此，下文设计一种通信数据实时加密算法，通过发挥区块链技术的应用优势，来提高通信数据加密的时效性与安全性。

一、基于区块链的实时加密算法

（一）身份认证数字签名

公钥机制是一种基于非对称加密技术的密码学方法，主要包括公钥和私钥两个密钥对。公钥用于加密信息，而私钥用于解密信息，在实际通信中即使公钥被公开，攻击者也无法从公钥推导出私钥，从而保证了通信数据安全[3]。本文运用公钥机制开展认证活动，在 A 与 B 的双方通信中，A 使用私钥 S，K 为数据 m 通信过程的签名，$<V>$ 作为认证证书，向 B 发送 m、K、$<V>$。对 $B<V>$、m、K、$<V>$ 的有效性进行是或否的验证。并进一步通过身份认证的引导，实时加载数字签名，其次从各区域的数据中对身份认证机制进行二次引导加载，实现对于 A、B 身份信息全面获取，而后 B 向 A 发送随机数，A 生成身份认证数字签名：

$$K:SIG(r,S) \tag{1}$$

其中，r 表示随机数。

A 发送 K、$<V>$ 给 B，对 $<V>$、$V(K,m,PK)$ 的有效性进行是或否的验证，二者同时有效则完成身份认证时，双方通信活

动可开展。

（二）构建同态加密四元组

同态加密是一种密码学技术，允许在不解密数据的情况下对密态数据执行特定的计算操作，使得计算结果仍是密文状态，对密态结果解密后可以得到与直接用明文数据计算相同的结果[4]。设定通信数据 x 、 y 的加密过程：

$$E(x)\circ E(y)=E(x\circ y),\forall x,y\in M \quad (2)$$

其中，$\circ$ 表示运算符； E 表示实时加密算法； $E(x)$ 表示 x 数据的密文； $E(y)$ 表示 y 数据的密文； $E(x\circ y)$ 表示同态密文。

同态加密的四元组表达式为：

$$H=(H.keygen,H.E,H.r,H.S) \quad (3)$$

其中， $H.keygen$ 表示密钥生成函数； $H.E$ 表示加密函数； $H.r$ 表示计算函数； $H.S$ 则表示解密函数。

区块链技术在通信数据自动、实时加密中表现出较强的安全性与可信性。从中心化方面来看，区块链不依赖于任何中心机构或服务器，是由多个独立节点共同维护和更新，每个节点都保存着完整且相同的账本副本，通过共识机制确保数据一致性。从不可篡改的方面来看，区块链中的实时数据一旦开始写入，过程则很难被篡改或直接删除，每个数据块的连续性上都具有上一个数据块的哈希值，任何修改都会影响后续所有数据块的哈希值，使得篡改行为容易被网络中的其他节点发现。在安全性和可追溯性方面，区块链使用加密技术保护数据的安全性，使用公私钥加密进行验证和授权，确保只有拥有私钥的人可以进行有效的数字签名和交易，还会通过记录历史数据追溯到最初的创世区块[5]。在此基础上，本文从通信方 A 方面建立数据加密空间：

$$S(L(A))=S(B) \quad (4)$$

其中， $L(A)$ 表示数据的加密空间； $S(L(A))$ 表示数据空间内的密文； $S(B)$ 表示加密后接收的数据。 B 在 $L(A)$ 上的任意区域为满足式（5），并设置空间向量 t ，进一步得到区域内与 t 最接近的向量之一，满足 $L(A)$ 区域上任意非零向量，则得到式（6）。

$$P(B)=\left\{Bx\middle|x\in A_n,0\le x\le 1\right\} \quad (5)$$

$$d(t,B)=d(x) \quad (6)$$

其中， A_n 表示 $L(A)$ 中任意一个数据； $d(t,B)$ 表示 t 与 B 的距离； $d(x)$ 表示 $L(A)$ 上 x 数据的通信距离。

区块链技术支持下的通信数据加密首先依托共识机制保证加密安全，接着以激励方式开展实时加密活动，而后通过设置智能合约来优化加密服务，最后在不同区块中对不同数据进行独立加密。

（三）计数器初值的随机生成

计数器是一种对称加密算法的工作模式，通过将逐次累加的计数器进行加密来生成密钥流，然后将密钥流与明文进行异或操作得到密文，可以实现加密，并支持并行处理，提高了加密效率[6]。本文通过图1的流程生成计数器的第一初值，初始密文从 $a0$、$a1$ ... $a127$ 开始设置，设定随机数为2，转变初始密文用循环位移的形式。通信数据加密的安全性表现在：如果不掌握随机数则无法得到位移密码；通过更新随机数可以对计数器初值进行调整；通过调整初值便能够完成单次加密活动[7]。

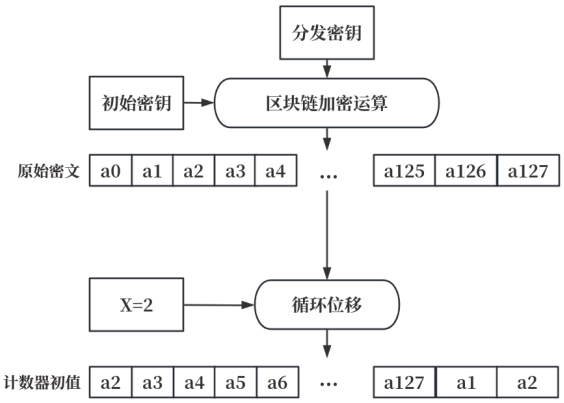

图1 生成计数器初值

二、验证分析

（一）前期准备

结合实验需求，选择开发环境为 *CCS* 。使用 *I2C _config* 对总线进行配置，主 / 从 (*maater / slave*) 设置接收函数 *I2C _read*( ) ；并设置禁止指定 *I2C* 中断函数为 *I2C _eventDisable*(。变量交互条件下的密钥，以及随机生成的数据使用存储芯片进行存储，进行对相关库函数参数的配置，并确定 *TCP* 的连接状态是否良好，最后完成通信双方身份的验证，即可开始通信数据实时加密任务。图2为主要数据加密流程。

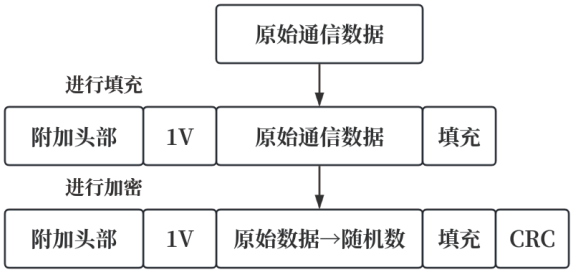

图2 数据加密流程

P2、*P3* 作为数据长度的表示，利用16进制数据形成并开始发出加密指令， *CRC* 的校验则通过原始加密数据基础上 +1 字节后进行，并即时头部字节填充 0×80 ，其他所有字节则按 0×0 填充处理。若通信数据的字节为16的倍数（如0、16、32、64等），则以16字节进行填充，长度 $\le 2048bit$ ，后进行加密处理。在解密时将 0×80 与之后数据进行去除，重复身份认证操作后获取原始报文[8]。

（二）结果分析

基于前文表述的实验准备情况，随机选择12组通信数据对加密解密的安全性能进行研判。在严格保持其他条件一致的前提下，将本文所提到的方法与方法 a（基于加权傅里叶变换数学模型的通信数据加密传输方法）、方法 b（基于混沌映射算法的电力物联网加密通信认证方法）进行对比分析，进而得出安全性结论。通过分析表1实验结果，首先能看到方法 a 的密文与明文差异不

大，易于被破解的概率较高，并且进一步发现，解密后的密文与明文内容与实际内容差异性较大，因此推断出该技术方法在加密与解密过程的安全性中无法充分保证，并且易于出现解密失误，与明文不匹配；第二，通过方法 b 的明文与密文的差异较大，且解密得到的密文内容与实际内容具有一致性，然而最终解密的明文却与实际内容具有一定差异，同时存储开销已超出200M（存储开销越小，说明数据处理量较少，可以扩大加密算法的应用范围），数据的处理量和应用范围上仍有待优化。通信数据经由本文所提出方法进行实时加密后，明文与密文之间表现出较大差异，完成解密后的明文、密文等内容与实际内容相一致，且存储开销均保持在50MB 范围内，所取得的加密效果较为理想 [9]。

表2 不同方法的对比结果

技术方法	加密		解密		存储开销
	明文	密文	密文	明文	
方法 a	29201A	2920C9	2920C9	29202B	250MB
	2A2B2C	2ACBC9	2ACBC9	2A2C2B	350MB
	282A2F	45CA2F	45CA84	272F2F	150MB
	272B2E	790623	790623	202E1E	300MB
方法 b	2542AZ	VA5864	VA5864	2542AA	150MB
	2C2D2F	Z4Z5Z8	Z4Z5Z8	2C2D2F	100MB
	2K568M	A2K4P5	A2K4P5	2K569M	200MB
	2EU857	E4568Z	E4568Z	2EU857	100MB
方法 c	292A2B	52500B	52500B	292A2B	50MB
	2C2D2E	E9106F	E9106F	2C2D2E	20MB
	222A2B	6E8960	E8960	222A2B	40MB
	2E2F2G	5FF2O6	5FF2O6	2E2F2G	30MB

三、结语

本文设计和提出的区块链技术支持下通信数据实时加密算法，在通信数据的安全加密上表现出优异性能，具有良好的应用前景和应用价值 [10]。在未来的研究中，要重点关注物联网与区块链的融合，探寻去中心化架构和加密工具的持续建设，打造更加透明、自动化的工作流程，还要通过云基础设施允许部署和利用技术解决方案，使技术方法更加可用和适应性更强。

参考文献

[1] 李婧彬，郑真真 . 基于加权傅里叶变换数学模型的通信数据加密传输方法 [J]. 长江信息通信 ,2024,37(02):99-101.

[2] 张颖军，蒙静，古松，彭凯，朱鹏，孙静，方进勇 . 空间 X 射线通信技术研究现状分析 [J]. 长江信息通信 ,2024,37(02):99-101.

[3] 赵国杰，文华，刘成浩 . 基于混沌映射算法的电力物联网加密通信认证方法 [J]. 电子设计工程 ,2024,32(02):143-146+151.

[4] 陈闻宇，李晓东，杨学，等 . 一种基于区块链的 DNSSEC 公钥验证机制 [J]. 自动化学报 ,2023,49(04):731-743.

[5] 李秋贤，周全兴 . 基于全同态加密的联邦学习隐私保护技术研究 [J]. 现代信息科技 ,2024,8(23):170-174.

[6] 靖海，吴进国，袁嘉骏 . 改进区块链的数据库信息可搜索加密算法研究 [J]. 电子设计工程 ,2025,33(02):145-148+153.

[7] 孙凡，雷文鑫，文红，等 .CCMP 加密协议的密钥信息泄漏问题 [J]. 网络安全技术与应用 ,2024,(03):23-26.

[8] 方海，赵扬，王显煜，高媛，杨旭 .6G 时代卫星算力网络发展思考 [J]. 空间电子技术 ,2023,20(2):08-14.

[9] 李冲霄，李卓 . 量子通信技术及应用研究综述 [J]. 空间电子技术 ,2024,21(1):72-80.

[10] 陈中原 . 基于区块链技术的通信数据实时加密算法 [J]. 长江信息通信 ,2024,37(11):56-58.

