ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/

团 体 标 准

T/XXX XXXX—XXXX

5G 核心网信令数据的采集、处理、传输与隐私保护技术规范

Technical specification for the collection, processing, transmission and privacy protection of 5G core network signaling data

（征求意见稿）

XXXX－XX－XX 发布 XXXX－XX－XX 实施

发 布

目　　次

1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　总体架构 2
5　原理 3
5.1　隐私保护 3
5.2　同态加密算法 4
5.3　威胁流检测分析原理 5
5.4　Hyperledger Fabric 联盟链 5
6　信令数据生成与仿真 6
6.1　正常信令流数据模拟生成 6
6.2　异常信令流数据模拟生成 6
6.3　数据流捕获 7
7　数据加密玉隐私保护 7
7.1　概述 7
7.2　数据加密技术 7
7.3　数据访问控制 9
7.4　身份认证与权限管理 10
7.5　数据完整性验证 10
7.6　零知识证明 10
7.7　数据存储与传输加密 11
8　数据共享与检索 11
8.1　数据共享 11
8.2　共享通道 12
8.3　信令数据管理 14
8.4　身份管理 14
8.5　联盟链管理 14
9　分布式存储管理 15
9.1　分布式存储架构要求 15
9.2　数据存储与访问控制 15
9.3　数据可靠性与完整性 16
9.4　存储性能与效率优化 16
9.5　数据隐私保护措施 16
10　威胁流检测与分析 16
10.1　范围 16
10.2　数据预处理 17
10.3　威胁检测规范 17

10.4 异常行为分析 18
10.5 威胁溯源规范 19
11 建立可视化展示平台 19
11.1 数据库建立 19
11.2 可视化分析平台 20
附录A（资料性） 实验室工作条件 21

5G 核心网信令数据的采集、处理、传输与隐私保护技术规范

1 范围

本文件规定了5G核心网信令数据在采集、处理、传输、存储与隐私保护中的技术要求、实验方法、以及数据的采集、加密、共享、分析等内容。

本文件适用于5G核心网控制面和用户面信令数据的处理与保护，包括信令流的模拟生成、数据的加密与访问控制、隐私保护、威胁检测及可信共享等应用场景。本标准同样适用于基于联盟链技术的数据共享平台和基于零知识证明及同态加密的隐私保护系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术术语

GB/T 22239-2020 信息安全技术 网络安全等级保护基本要求

GB/T 37988-2019 云计算服务安全能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信令数据 signaling data

指5G核心网中的控制面和用户面信令流数据，包括设备间交互的协议消息及流量信息。

3.2

数据采集 data collection

通过探针或其他接口从5G核心网设备中提取信令流数据的过程。

3.3

零知识证明 Zero-Knowledge proof

一种允许证明方在不泄露任何实际信息的情况下向验证方证明某项声明的真实性的密码学技术。

3.4

同态加密 homomorphic encryption

一种允许对加密数据直接执行数学运算的加密技术，解密后结果与对明文执行相同运算的结果一致。

［来源：GB/T 25069-2022］

3.5

联盟链 consortium blockchain

由多个组织共同维护的区块链，仅授权节点参与共识，用于数据共享与访问控制。

3.6

数据完整性 data Intergrity

数据在传输、存储和处理过程中未被篡改的特性，可通过哈希校验或数字签名技术实现。

3.7

数据访问控制 access control

通过技术手段限制对信令数据和系统资源的访问权限的过程，包括基于角色（RBAC）和基于属性（ABAC）的控制方式。

3.8

数据脱敏 data masking

对敏感数据进行伪匿名化或遮盖处理的技术，确保数据内容在共享或存储时不可恢复至原始状态。

3.9

数据共享 data sharing

在授权条件下，在多方之间交换或访问信令数据的过程，需确保数据安全和隐私保护。

3.10

加密 encryption

采用算法将明文数据转换为密文的过程，以保护数据机密性。包括对称加密（如AES）和非对称加密（如RSA）。

［来源：GB/T 25069-2022］

3.11

身份认证 authentication

确认用户身份真实性的过程，常采用密码、数字证书、多因素认证等方式。

3.12

威胁检测 threat detection

通过分析信令流数据，发现和识别潜在网络威胁的技术方法

3.13

威胁检测 threat detection

信令数据在数据库或分布式存储系统中的保存过程，需确保其可用性、安全性和一致性。

3.14

多通道隔离 multi-channel Isolation

一种基于联盟链技术的数据共享机制,通过划分独立的数据通道,实现数据的安全隔离和访问控制。每个通道独立维护成员和数据共享范围,确保不同业务场景下的数据隔离性。通过加密和身份认证技术，多通道隔离可保护敏感数据，防止未授权的访问或数据泄露，同时支持动态调整通道配置，满足复杂的共享需求，如跨组织的敏感数据交换。

3.15

数据传输 data transmission

信令数据在网络中移动或共享的过程，需通过加密协议（如TLS/IPSec）确保安全性。

3.16

分布式存储 distributed storage

将数据分布存储在多个节点中以提高可靠性和可用性的存储方式。

3.17

数据压缩 data compression

采用算法对信令数据进行编码以减少数据存储或传输占用空间的过程。

3.18

数据冗余 data redundancy

通过在多个节点存储相同数据副本来提高数据可靠性和容灾能力的技术手段。该技术广泛应用于分布式存储系统，通过副本策略和地理分布机制，确保即使部分节点故障，数据依然可以被恢复。在5G核心网中，数据冗余可以用于信令数据存储和共享，防止单点故障引发的数据丢失，并保障网络服务的高可用性和持续性。

3.19

区块链 blockchain

分布式账本技术，通过去中心化和不可篡改性实现数据共享和可信记录。

4 总体架构

5G核心网信令数据处理与保护的完整框架如图1所示，涵盖数据生成、存储、保护、分析与平台建设的全流程管理。主要内容包括：正常与异常信令数据的生成；分布式存储的架构优化与数据可靠性管理；通过加密技术、身份认证和零知识证明等手段实现数据访问控制和隐私保护；在确保数据完整性和

安全性的前提下，支持数据共享与检索；通过威胁流检测与分析明确异常行为及潜在风险源；最终构建可视化展示平台，提供安全分析与共享功能，全面保障5G网络数据的安全性、完整性和高效管理。

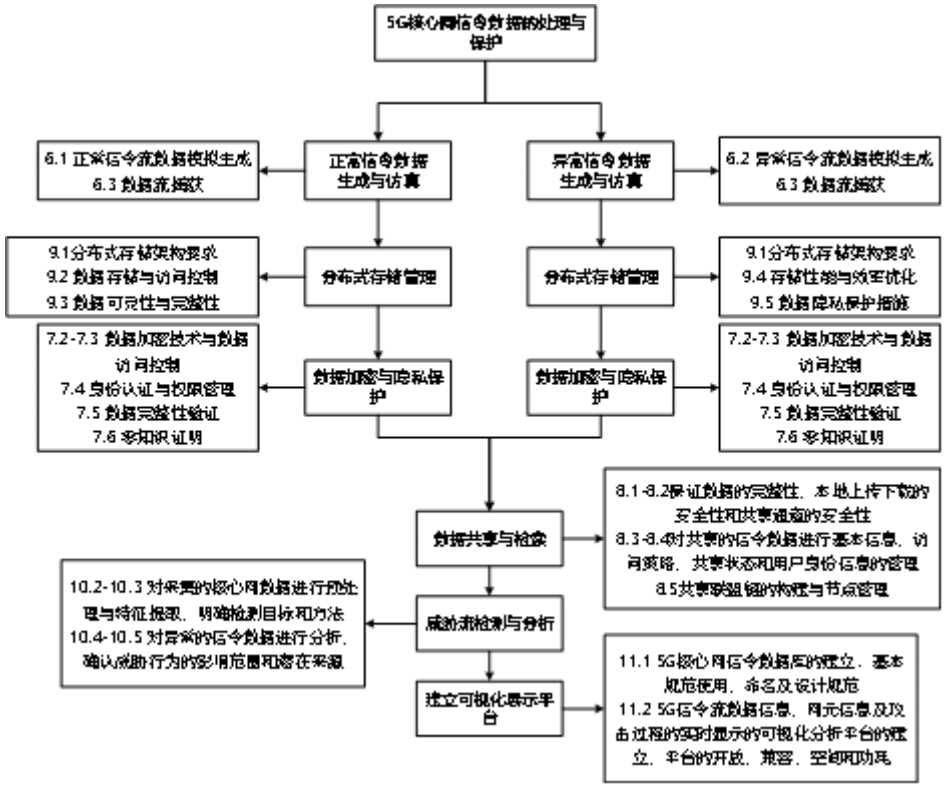


图1　15G 核心网信令数据处理与保护的完整框架图

5　原理

5.1　隐私保护

私保护技术的核心在于确保数据或信息在敏感内容未暴露的情况下，依然能够实现验证、操作或处理。通过数学和密码学方法实现数据的隐私性、安全性和高效性，主要包括零知识证明和同态加密两种关键技术。零知识证明是一种密码学方法，使得证明者可以在不泄露具体信息的前提下，向验证者证明某一声明的真实性。这一技术的核心目标是保护隐私，同时确保信息的真实性和有效性。同态加密是一种允许对加密数据直接进行数学运算的加密技术，运算结果解密后与对明文直接运算的结果一致。这一特性使得数据可以在不解密的情况下进行计算，从而保护数据隐私，如图2、图3所示。

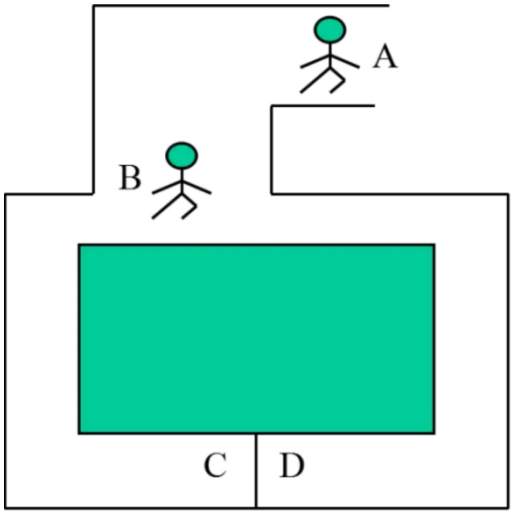


图2　零知识证明

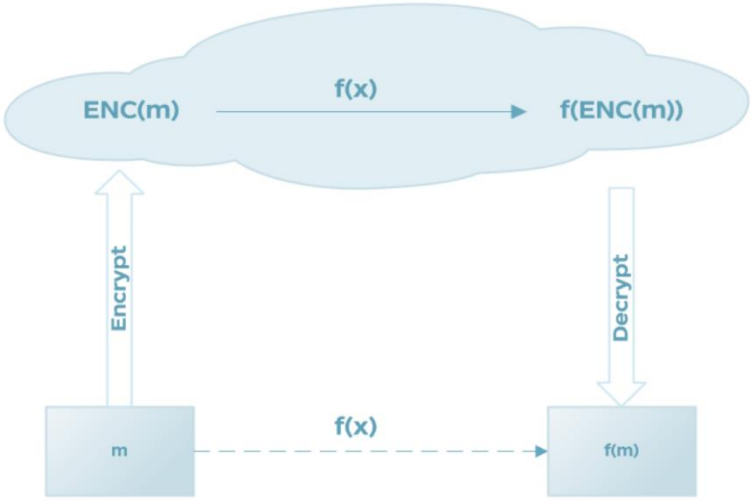


图3　同态加密算法

5.2　同态加密算法

基于联盟链Fabric与多通道机制构建可控的信令网威胁流数据共享环境。联盟链通过认证准入机制建立基础的可控环境，多通道技术在此基础上实现共享数据的隔离，确保数据共享的安全性与可控性。为解决链上存储的高成本和效率低问题，引入IPFS分布式存储系统，构建链上索引与链下数据结合的存储模型，降低存储开销并提升数据管理效率。同时，通过边缘计算技术，将IPFS存储节点动态部署在靠近参与机构的位置，优化数据访问路径，提高数据访问速度和共享效率，从而实现高效、安全、可控的数据共享环境，如图4所示。

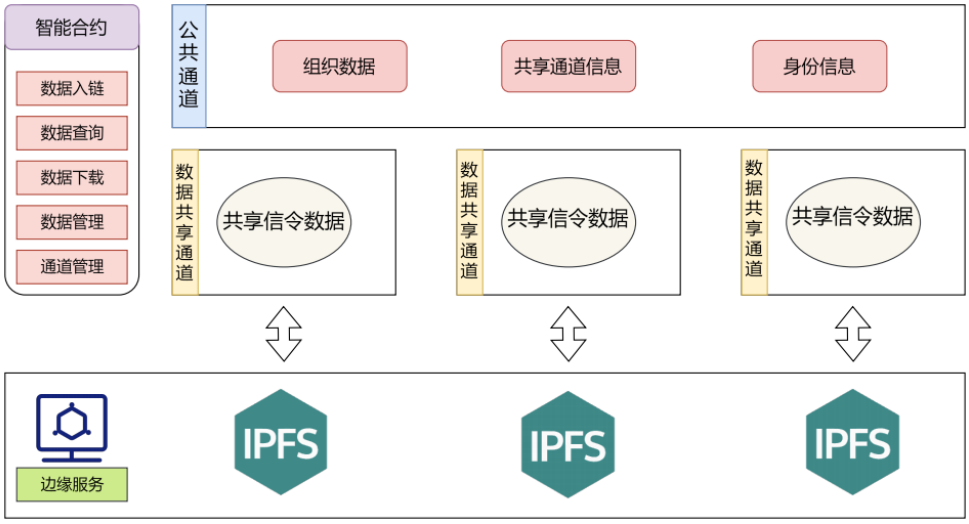


图4　数据共享原理图

5.3　威胁流检测分析原理

基于算法模型和知识图谱技术对信令数据流进行威胁种类检测和行为特征分析。通过比较信令流特征与正常模式的偏离程度或与已知攻击特征的匹配情况，识别异常行为和潜在威胁，生成知识图谱，用于精确描述威胁行为的特性和来源。当信令流表现出异常模式或攻击特征时，将其判断为威胁事件，从而提供有效的技术手段保障5G网络的安全性和稳定性，如图5所示。

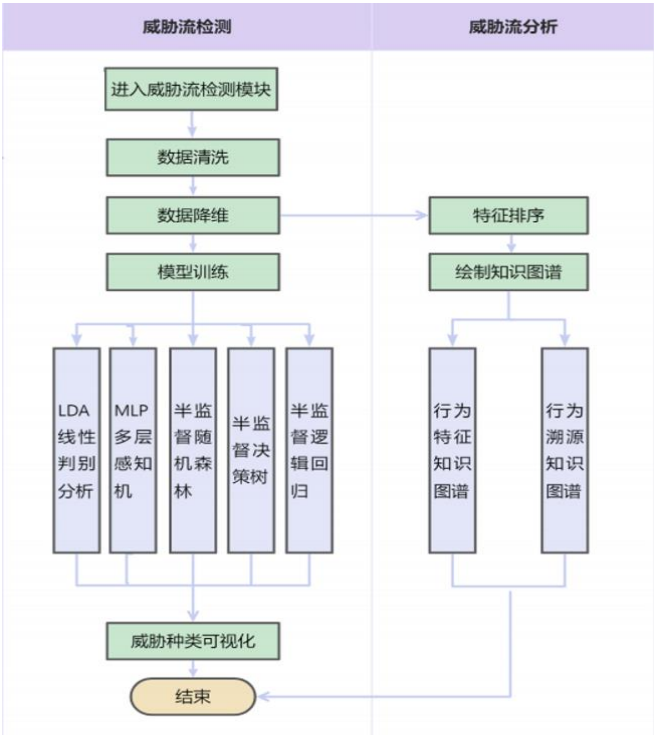


图5　威胁流检测分析原理图

5.4　Hyperledger Fabric 联盟链

Hyperledger Fabric 是一个开源的区块链平台，采用联盟链模式，由一组已知且受信任的参与者共同管理，与公有链和私有链有所不同。其核心是执行-排序-验证（EOV）架构，通过执行、排序和验证三个阶段来高效、安全地处理交易。在执行阶段，交易被模拟和背书；在排序阶段，交易通过共识协

议排序；在验证阶段，根据特定的信任假设进行验证。这种架构不仅提高了性能，还增强了对非确定性和潜在恶意行为的抵抗力。

Fabric 通过访问控制列表（ACL）和成员服务提供（MSP）实现细粒度的权限管理，确保只有授权参与者可以读取或写入账本，同时支持跨组织的数据共享和协作。多通道架构是其显著特点，允许在同一区块链网络上创建多个逻辑隔离的通道，每个通道拥有独立的参与者和智能合约，满足多场景需求。此外，Fabric 采用只追加的区块链和快照机制，保证数据的不可篡改性、高效访问和验证。

Hyperledger Fabric 提供了一种灵活、安全和高效的区块链架构，适用于需要隐私保护、多样化场景和高性能的分布式系统应用。

6 信令数据生成与仿真

6.1 正常信令流数据模拟生成

通过5G 核心网信令风暴仿真测试平台（XPRO 仪表）、开源软件 Free5GC 平台、UERANSIM 模拟器以及 Kali 平台，以模拟生成接近真实的 5G 核心网控制面信令流数据。

正常信令流的模拟生成一方面通过 XPRO 仪表仿照现实网络环境进行配置 AMF、SMF、AUSF、UPF、GNB 网元和 UE，并根据具体需求进行信令负载配置，可以仿真5G 环境；另一方面通过搭建 Free5GC 平台模拟核心网，UERANSIM 模拟网络终端和基站，并通过一定的配置使三者可以互连互通，模拟 UE 、gNB 以及核心网元之间的交互，可以模拟 5G 网络中的各种信令流程，如用户设备 UE 的接入、用户身份的认证、鉴权过程以及数据连接的建立等。这些模拟的信令流数据严格遵循 3GPP 5G 标准，确保了数据的标准化和兼容性。

6.2 异常信令流数据模拟生成

在异常信令流数据的获取方面，主要采用三种方法：

a) 使用 XPRO 仪表可以构建相应的信令风暴业务模型和流量触发，仪表架构如图 6 所示：如 5G UE 上下线、Paging（UE 和网络触发）、多 PDU 会话、Xn 切换、N2 切换、4/5G 互操作以及 PDU Session Modify 等业务组合流程的仿真，如图 6 所示。

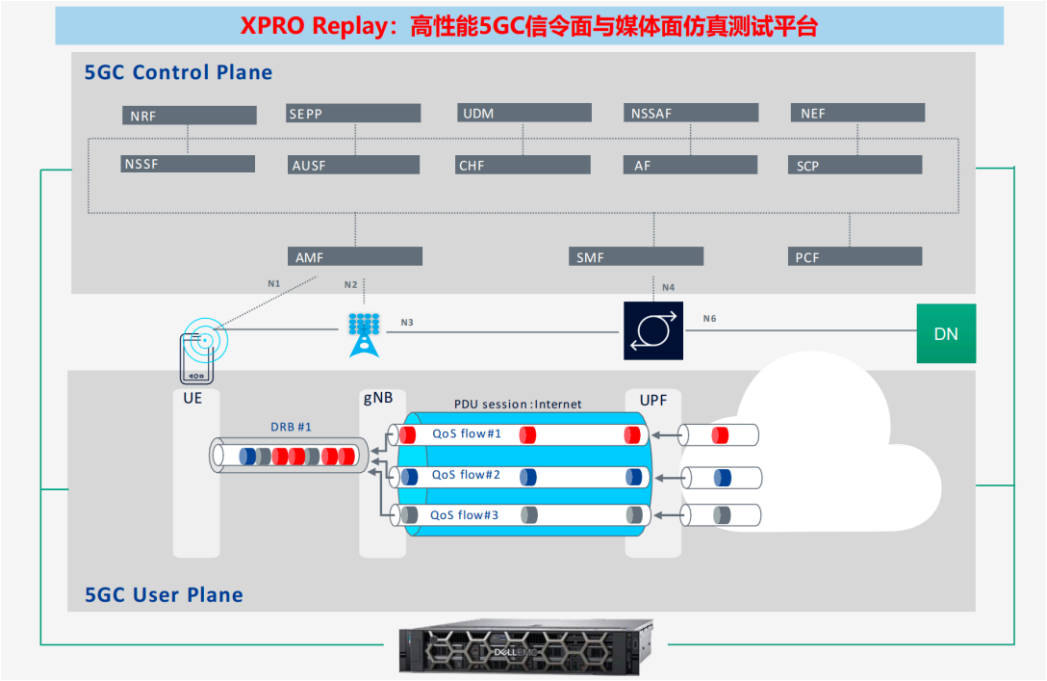


图6 XPRO 仪表架构

b) 基于 Free5GC 和 Kali 攻击系统，在实验环境下模拟外部攻击者发起对核心网的 DDoS 攻击行为，如 ICMP Flood、UDP Flood、SYN Flood 等 DDoS 攻击，并采集分析攻击流量。

c) 基于 Free5GC 实验环境提供的 openAPI，通过深入研究通信信令网的各网元通信机理，对网元通信接口进行分析，利用 5G 通信内部接口间的权限漏洞，推演潜在的逻辑威胁成因，从而发现控制面的异常信令数据。具体的异常信令流数据如下：

1) 基于缺乏身份验证的漏洞，恶意攻击者可以根据此漏洞进行核心网网元数据的窃取。通过伪造一个随机身份，恶意攻击者能够成功冒充合法用户或网元来实现对核心网的非授权访问。访问成功后将会导致网络中的敏感信息和配置数据的曝光，给网络的安全性和隐私保护带来极大威胁。

2) NRF 网元没有实现对请求来源进行有效检查，恶意攻击者根据此漏洞可以冒充 AMF 节点来请求 NRF 网元中存储的关键数据。此类攻击绕过了 5G 核心网的防御机制，攻击者可获得用户数据和网络配置数据。这种敏感信息的获取可能引发用户隐私泄露和网络安全的进一步威胁，同时，攻击者还可将这些数据用于其他恶意活动。

3) 网元接口权限检查缺失的漏洞，会导致恶意攻击者对核心网的虚假 AMF 攻击的风险。通过伪造 AMF 节点加入到网络中并发送删除其他 AMF 节点的请求，攻击者能够绕过权限控制，对核心网实施破坏性操作。此类攻击可能导致核心网的服务中断、网络故障或数据丢失，严重威胁了信令网的可用性和稳定性。

6.3 数据流捕获

在数据流捕获与分析方面，通过使用Wireshark网络协议分析工具对模拟生成的信令流数据进行实时捕获和深入解析。Wireshark能够全面记录网络中的数据包，包括协议类型、源地址、目标地址、数据包长度以及时间戳等信息。在捕获数据的基础上，进一步分析异常信令流中的具体行为特征，例如数据包重复、丢失、异常长度或非法请求等。同时，在模拟的攻击环境下，通过对DDoS攻击流量特征的提取，识别了ICMP Flood、UDP Flood和SYN Flood等攻击的关键模式。这些捕获的数据为后续的异常检测算法开发和安全防护机制的优化提供了高质量的数据支撑。

7 数据加密玉隐私保护

7.1 概述

数据加密与隐私保护是保障数据安全的重要技术手段，贯穿数据的采集、传输、存储及使用的全生命周期。在大数据和云计算等复杂数据环境中，数据加密技术、访问控制策略和隐私保护算法共同构成了防范数据泄露、篡改及未经授权访问的关键防线。本章规定了数据加密与隐私保护的技术要求和应用规范，并明确了适用于不同场景的具体实施方案。

7.2 数据加密技术

7.2.1 加密目标

数据加密技术的主要目标是确保数据在采集、传输、存储和使用过程中的机密性、完整性及不可抵赖性。通过有效的加密手段，防止未经授权的访问，保护数据不被篡改和泄露。如下图所示，数据隐私保护模型结合了AES加密、Paillier加密算法和区块链节点，以确保数据的安全性。业务层使用AES加密保护数据的机密性和完整性，计算层通过Paillier加密算法保护数据隐私，并支持加密计算。区块链节点通过智能合约管理加密数据,确保数据不可篡改,并提供可验证性。此模型有效防止未经授权的访问，确保数据的机密性、完整性与安全性，如图7所示。

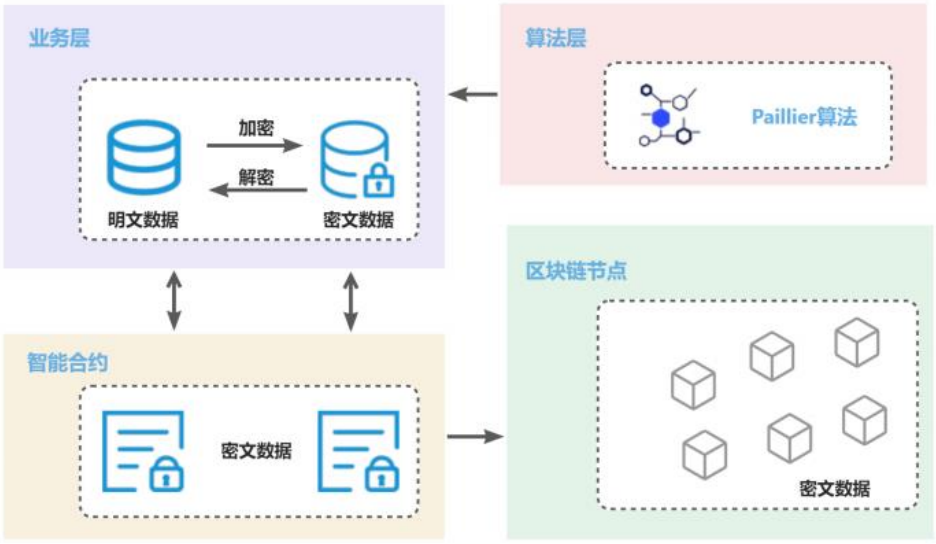


图7　数据隐私保护模型图

7.2.2　加密算法

推荐采用经国家密码管理机构批准的加密算法，以保证安全性和合规性，具体包括以下几种：

——对称加密：推荐使用 AES 算法，用于高效加密大规模数据。AES 算法具有加密速度快、资源占用少等特点，适用于文件存储和批量数据传输的场景。

——非对称加密：推荐使用 RSA 算法，适用于密钥交换和敏感数据加密。非对称加密因其高强度安全性，常用于加密敏感信息如身份凭证。

——同态加密：支持在加密状态下直接对数据进行计算，适用于隐私保护计算和多方协作计算场景。

Paillier 加密算法作为一种同态加密算法，能够在不解密数据的情况下进行计算，非常适合隐私保护计算场景。Paillier 加密算法首先从公钥中提取和，生成随机数，确保它是在范围内的整数，通过下面公式计算密文：

$$C = (g^m \ ?r^n)\bmod n^2 \quad \text{.....(1)}$$

式中：g 为公钥中的参数

M 为明文信息

C 为加密后的密文

密文可以发送给接收方，进行解密操作以获得原始的明文消息。基于 Paillier 的加密算法见示例 1 和示例 2。

示例 1：

Algorithm 7.1 基于 Paillier 加密算法

Input: 明文m ,公钥(n,g)

Output: 密文 C

1：**procedure** $\mathrm{P}_{\mathrm{AILLIER}}\mathrm{E}_{\mathrm{NCRYPT}}(m\ public_key)$

2:　　$(n,g)\neg\ public_key$

3:　　Choose a random r such that 1 < r < n and r is coprime with n

4: Compute ciphertext $C \quad (g^m \quad r^n) \bmod n^2$

5: **return** C

6: **end procedure**

示例 2：

Algorithm 7.2 基于 Paillier 加密的单个属性加密算法

Input: 属性名称 attr_name，属性值 attr_value，公钥(n, g)

Output: 加密后的属性值 enc_attr_value

```
1：procedure PAILLIERATTRIBUTEENCRYPTION (attr_name, attr_value, public_key)
2：    if attr_name = “Src IP” then
3：        enc_attr_value ← PaillierEncrypt(attr_value, public_key
4：    else if attr_name =“Dst IP” then
5：        enc_attr_value ← PaillierEncrypt(attr_value, public_key)
6：    else if attr_name =“Dst Port” then
7：        enc_attr_value ← PaillierEncrypt(attr_value, public_key)
8：    else if attr_name =“Protocol” then
9：        enc_attr_value ← PaillierEncrypt(attr_value, public_key)
10：   else if attr_name =“Timestamp” then
11：       enc_attr_value ← PaillierEncrypt(attr_value, public_key)
12：   end if
13：   return enc_attr_value
14：   end procedure
```

7.2.3 应用要求

数据在传输和存储过程中应全程加密，以防止信息泄露。

系统应支持加密算法的动态更新，以应对新型安全威胁。

密钥管理需采用分布式密钥管理机制，确保密钥的高安全性和高可用性，避免单点失效。

7.3 数据访问控制

7.3.1 控制目标

实现对信令数据访问的严格控制，确保只有授权用户或系统模块能够访问特定数据，防止数据泄露和非法使用。

7.3.2 数据访问控制

基于角色的访问控制（RBAC）：按照用户在系统中的角色分配权限，例如系统管理员、数据分析员、普通用户分别具有不同的数据访问权限。

基于属性的访问控制（ABAC）：通过用户属性和数据属性动态调整权限，适应更复杂的访问需求场景。

区块链智能合约：结合区块链技术，利用智能合约记录和验证访问行为，实现访问过程的透明性和不可篡改性。

7.3.3 应用要求

系统应支持访问权限的动态调整，以适应用户角色和业务需求的变化。
所有访问行为必须记录在系统日志中，并定期对访问记录进行审计。
对敏感数据的访问应支持双重认证或审批流程，进一步提升安全性。

7.4 身份认证与权限管理

7.4.1 认证目标

通过身份认证和权限管理，确保信令数据的安全访问和操作合规性。

7.4.2 身份认证机制

包括以下方式：

a) 单因素认证：采用密码或数字证书的方式进行基础身份验证。
b) 多因素认证：结合密码、生物特征和物理设备，增强认证的安全性。
c) 基于零知识证明的认证：允许用户证明其身份合法性，而无需透露具体的身份信息，从而保护用户隐私。

7.4.3 权限管理

权限分配应遵循最小权限原则，仅授予用户完成其工作所需的最低权限。
系统应支持权限的分级管理和动态调整，满足多层次权限需求。
定期审查权限分配情况，撤销不再需要的权限以减少安全风险。

7.5 数据完整性验证

7.5.1 验证目标

数据完整性验证的主要目标是确保数据在传输、存储和使用过程中的一致性，防止因攻击、错误或意外操作导致的数据篡改或损坏。

7.5.2 验证技术

包括以下方式：

a) 哈希算法：使用 SHA-256 等哈希函数生成数据摘要，用于快速检测数据完整性。
b) 数字签名：结合非对称加密技术，验证数据来源的合法性及数据内容的完整性。
c) Merkle 树结构：在分布式存储环境中，利用 Merkle 树实现多层次的数据完整性校验。

7.5.3 应用要求

对存储和传输的关键数据应定期进行完整性校验，并形成自动化流程。
数据完整性异常时，系统需实时告警并记录异常日志，便于后续追溯。

7.6 零知识证明

7.6.1 原理

零知识证明是一种密码学技术，允许证明方在不透露具体数据内容的情况下，向验证方证明某一声明的真实性。例如，证明用户的身份符合要求，而无需透露具体的身份信息。

7.6.2 应用场景

包括以下场景：

a) 用户身份验证：用户可在不披露个人详细信息的前提下完成身份验证，适用于隐私保护要求较高的场景。
b) 数据共享：在数据共享场景中，数据提供方可证明数据合法性，而无需暴露数据的具体内容。
c) 敏感计算：在医疗、金融等行业，零知识证明可以验证计算结果的正确性，而不泄露输入数据。

7.6.3 技术要求

零知识证明算法应支持交互式和非交互式协议，以适应不同的应用场景。

认证过程需具备高效性，能够满足实时性要求。

7.7 数据存储与传输加密

7.7.1 数据存储安全

数据存储过程中应采用静态加密技术保护其机密性，推荐使用AES算法对静态文件进行加密。

为提高存储可靠性和抗灾难能力，应采用分布式存储系统（如IPFS）存储数据，并设置多副本冗余策略。

7.7.2 数据传输加密

数据传输层应采用TLS或IPSec协议进行加密，确保传输过程中的数据安全性。

传输过程中应支持动态密钥更新机制，避免因密钥泄露导致的安全风险。

在高敏感性场景下，可结合量子安全加密算法，增强数据的抗破解能力。

8 数据共享与检索

8.1 数据共享

8.1.1 数据上传

系统需提供数据上传功能，允许具有共享权限的用户将本地数据上传至共享系统中，以实现数据共享。上传接口应支持多种文件格式，如 .pdf、.docx、.csv、.jpg、.png 以及大文件的上传，单个文件最大支持 1GB。同时，系统应支持多文件批量上传功能，总大小限制可根据业务需求调整。

上传时序图如图8所示上传过程中应对数据进行 AES-256 实时加密，每次上传生成唯一密钥用于文件内容的加密处理，密钥需通过 RSA 公钥加密后安全存储。传输过程需采用 HTTPS 协议，使用 TLS 1.3 或更高版本确保数据传输安全性。上传文件完成后，系统需对文件生成 SHA-256 哈希值，用于后续完整性校验，并对上传记录进行日志化存储，包括上传时间、用户 ID、文件名称和大小等信息，便于后续管理与追踪。如图8所示。

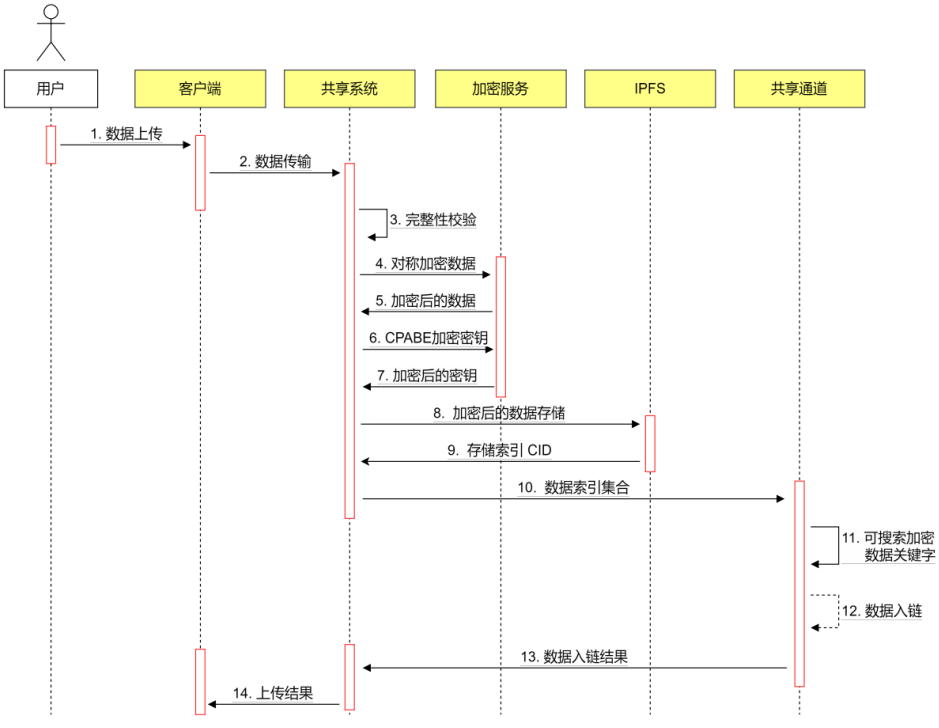


图8 数据上传时序图

8.1.2 数据下载

系统需提供数据下载功能，允许具有访问权限的用户从共享系统中选择并下载所需数据文件至本地。下载接口和界面应支持按需选择文件，并可显示文件基本信息（如文件名称、大小、格式和上传时间）。

为保证数据安全性，下载过程中需对文件内容进行传输加密（使用 HTTPS/TLS），并验证下载数据的完整性，确保文件未被篡改。系统应根据访问者的权限控制下载范围，未授权用户无法下载文件。每次下载需生成访问日志，包括访问者 ID、下载时间、文件名称和大小等信息，供数据提供者了解其共享数据的使用情况。

8.1.3 数据检索

系统需提供多种方式的数据检索功能，以方便用户快速定位所需的数据文件。检索方式包括但不限于：

a) 通过数据 ID 检索：用户可通过文件的唯一标识符（ID）直接精确定位到单项数据，避免检索误差。
b) 通过关键词检索：系统应支持基于文件名称、描述、上传者、日期或其他标签的关键词模糊检索功能，并按相关度返回符合条件的多项数据。
c) 权限限制： 检索功能应基于用户权限，仅返回用户有权访问的数据文件，屏蔽无权限数据。

系统还需在每次检索成功时生成访问日志，记录访问者 ID、访问时间、检索关键词及结果等信息，便于数据提供者监控其数据的访问和使用情况。

8.1.4 完整性校验

系统需提供完整性校验功能，以确保数据在上传、下载和存储过程中未被篡改。具体实现包括：

a) 文件上传校验：在上传完成后对文件内容生成 SHA-256 哈希值，并与本地文件的哈希值进行比对，确认文件内容一致性。
b) 文件存储校验：系统定期对存储中的文件进行哈希校验，确保存储过程中数据未被修改或损坏。
c) 文件下载校验：在用户完成下载后，系统需生成下载文件的哈希值并与存储中的哈希值比对，确保下载数据的完整性。

若发现完整性校验失败，系统需立即向管理员发送警告通知，记录相关文件信息和操作详情，并在用户界面提示操作失败，避免使用被篡改的数据。

8.2 共享通道

8.2.1 创建通道

多通道技术是实现信令数据可控共享的重要标准。用户可以根据自身需求创建多个独立的数据共享通道，每个通道都允许用户定义数据共享范围和相关规则，以确保数据的安全性和隐私性。

标准要求通道的创建应具备以下能力：

a) 支持独立配置：每个通道可独立设置共享范围、参与节点、共识规则和出块策略，以满足不同的业务需求。
b) 严格权限控制：在创建通道时，需明确规定通道成员的访问权限，避免数据被未授权的成员访问。
c) 配置透明：通道的配置应可记录并公开在联盟链的公共部分，以便其他授权成员了解通道存在及其基本配置信息。

每个通道应被视为一个独立的逻辑区块链，通道成员在其中共享数据的同时，不会对通道外的成员产生信息泄露的风险。通道创建的流程图如图9所示。

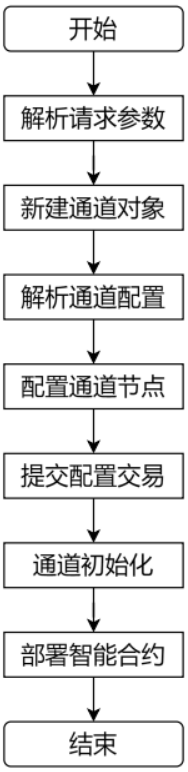


图9　创建共享通道流程图

8.2.2　通道管理

通道的灵活管理是数据共享标准的重要部分。用户应能动态调整通道配置，以适应数据共享需求的变化。标准要求通道管理包括以下功能：

a) 成员管理：用户可动态调整通道成员，包括添加或移除成员，以及调整成员的访问权限级别。
b) 共识规则修改：系统应支持通道共识算法的动态调整，例如从 RAFT 改为 PBFT，以满足不同业务场景下的性能要求。
c) 配置变更记录：所有对通道配置的修改操作（如成员调整、共识规则修改等）应生成完整的日志，记录操作时间、操作人及变更内容。

通道管理功能应具备高适应性，满足不同业务规模和需求场景的调整能力，同时确保变更操作的安全性和可追踪性。

8.2.3　通道配置查看

系统提供实时可视化的通道配置查看功能，方便用户全面了解通道的运行状态。用户应能随时查看通道的基本信息、参与成员、共识算法以及共享数据范围等详细配置。此外，通道还需支持区块数据的解析与查询功能，帮助用户获取通道内的区块信息和交易记录。通过直观的可视化界面，用户能够快速了解当前通道中的数据共享情况，掌握通道运行的整体状况。

8.2.4　通道数据查看

基于联盟链的技术特点，在共享通道中采用双重认证机制。首先，组织需获得公共通道的授权，才能进入系统并了解网络中的基本配置信息。其次，组织需获得数据共享通道的授权，方可访问通道内的共享数据。这种机制确保了数据共享权限的分级管理，仅加入公共通道的组织可查看网络公共信息，而只有加入特定数据共享通道的组织才具有获取相关数据的权限。通过双重认证和通道隔离技术，标准为信令数据的可控共享提供了高效、安全的解决方案。

8.2.5　智能合约管理

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/638100043113007047