oppo

6G 安全架构：
构建基于零信任的智能安全

OPPO 6G 安全白皮书

目录

05

6G 时代关键安全技术

06

前言

01

前言

6G 时代以工业互联网、泛在的人工智能（Artificial Intelligence，AI）、零功耗通信、通感一体化（Integrated Sensing and Communication，ISAC）为代表的新业务、新终端、新连接、新架构的发展趋势会对当前的通信模式带来巨大改变，越来越多的数据开始从终端侧收集，再传输到网络侧，成为人工智能必不可少的数字资源，6G 系统将针对这些高价值数据资产进行管理。**因此，6G 安全的最大变化趋势是保护的重点从传输逐渐演变为数据与隐私。**在使用高价值数据资产的同时，需要高效的数据授权，防止归属于不同利益相关方的数据资产价值被滥用。考虑到 6G 系统业务和数据来源的多样性，需要考虑多方信任模式，针对多源的、分布式的数据，进行分布式的数据授权，同时针对个人相关数据，做好隐私保护。

随着新终端、新连接技术的发展，数据传输不仅仅局限于传统高层协议，数据安全保护的能力也需要从传统的高层保护向底层保护迁移，从而匹配 6G 新终端、新空口技术的安全需求。

根据“极简多能”的 6G 系统概念设计，对于不同子系统的数据资产，安全保护机制也需多元化，需要对 6G 系统安全功能进行动态的安全编排，用智能安全架构满足不同场景的安全需求。

本文将通过分析 6G 新业务、新终端、新连接、新架构的发展趋势和安全需求，在传统蜂窝安全机制的基础上，探索区块链、物理层安全、AI 安全、后量子安全等技术，提出基于零信任的 6G 智能安全架构。

- 5G 安全双向信任模型
- 5G 安全架构
- 5G 传输安全机制

5G 安全小结

02

5G 安全双向信任模型

2.1

3GPP 5G 安全 [1] 中定义了双向信任模型，如图 2-1 所示，即 UE（User Equipment 用户设备）和运营商 HE（Home Environment 归属环境）双方共享用户根密钥，作为双向信任的安全可信根。 5G 中的安全可信根承载在 UE 的物理防篡改通用集成电路或 UICC（Universal Integrated Circuit Card 通用集成电路卡）中。 在网络侧，安全可信根承载在核心网的 UDM（Unified Data Management 统一数据管理）和 ARPF（Authentication Credential Repository and Processing Function 认证凭证存储库和处理功能）网元中。 随着网络层层向外部署，网元逐渐远离核心网，信任级别降低，其他网元不能再存储安全可信根，同时在这些网元进行的通信处理需要更周全的安全保护。

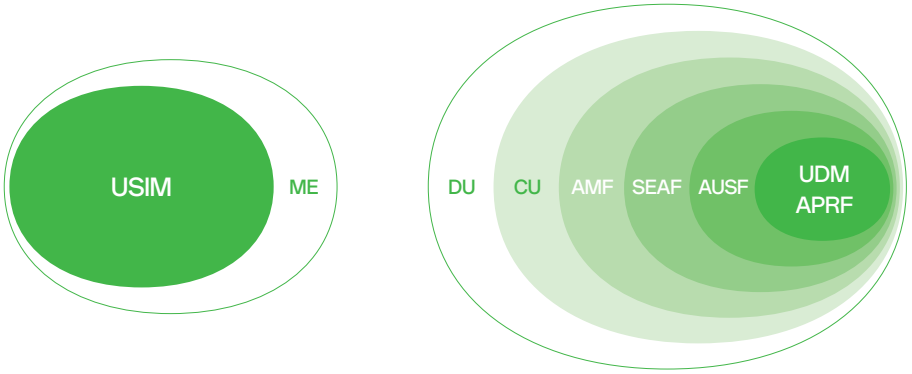

图 2-1: 5G 双向信任模型

当用户设备接入移动网络使用网络资源的时候，用户和移动网络根据用户根密钥执行双向认证。 用户和移动网络各自根据用户根密钥进行密钥衍生计算，得到一系列保护密钥，对双向传输的信令和数据进行加密保护和完整性保护。

除了上述双向信任架构，3GPP 中还存在不同利益相关者（即用户、服务提供方、设备和网络）之间的双向信任关系，这些信任关系未体现在 5G 信任模型中。 例如，还有用户和服务提供方、或服务提供方与移动网络之间的双向服务合约和交互，如何为设备分发身份和凭证，如何基于上述身份和凭证在网络和设备之间进行相互身份验证等。 这些利益相关者之间的信任构成了 5G 服务的基础，但是 5G 中的信任模型都是双向信任模型，5G 不支持这些利益相关者之间的多方信任。

5G 安全架构

2.2

5G 安全架构还定义了五个独立的安全功能域 [2]，如图 2-2 所示，即：

- **网络接入域安全 (I)**

  一组安全功能，为用户提供对服务的安全访问并防止对（无线）接入链路的攻击。

- **网络域安全（II）**

  一组安全功能，使网络节点能够安全地交换信令、用户数据（接入网和服务网络之间以及接入网内部），并防止有线网络受到攻击。

- **用户域安全 (III)**

  保护对终端设备的访问的一组安全功能。

- **应用域安全 (IV)**

  一组安全功能，使用户和提供商域中的应用程序能够安全地交换消息。

- **安全的可见性和可配置性（V）**

  一组功能，使用户能够获知自己安全功能是否正在运行，以及服务的使用和提供是否应依赖于该安全功能。

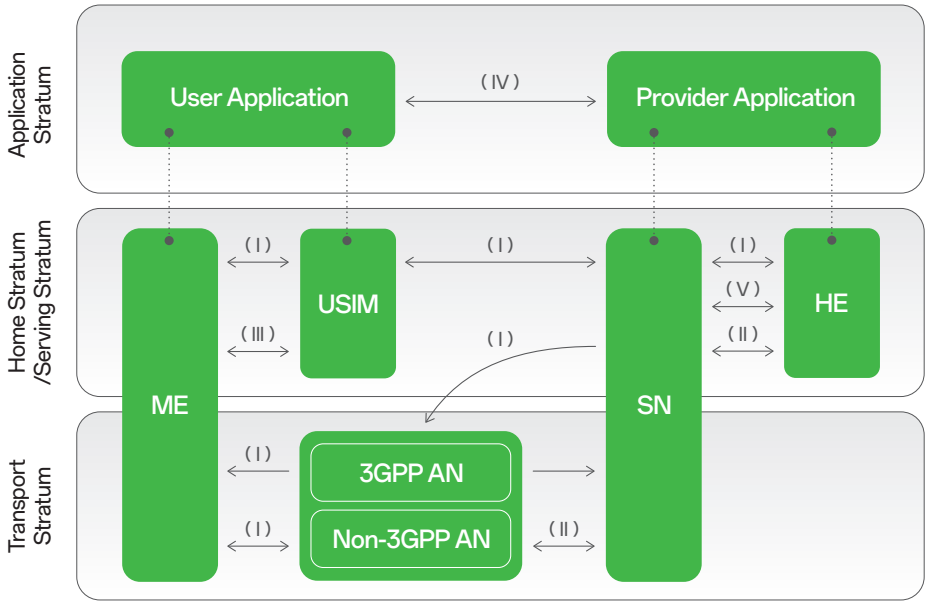

图 2-2: 5G 安全架构

5G安全架构仅包含了归属运营商网络内的安全域，对于漫游服务，归属运营商网络需要与另一个漫游网络交换与漫游相关的UE信息，网络之间通过位于运营商网络边缘的网络功能SEEP（Security Edge Protection Proxy安全边缘保护代理）交互消息。

5G 传输安全机制

2.3

在网络接入域中，UE 通过 AN （Access Network 接入网）接入 5G 网络。接入层（Access Stratum，AS）的安全是基于 5G 密钥层次结构中最低层的密钥和三种密码算法之一（即 AES、Snow 3G、ZUC）实现，对信令面和用户面进行加密和完整性保护。非接入层（Non-Access Stratum，NAS）信令的保护是基于 NAS 层的密钥实现。

网络域安全（Network Domain Security，NDS）是指同一运营商网络内不同网元之间的安全保护，使用 3GPP 指定的 NDS 协议。NDS/IP 使用的是 IETF 标准中的 IPSec（IP Security）和特定的 3GPP 配置文件。5G 网络中服务化架构（Service-Based Architecture，SBA）安全将网络域内的保护提升到更高的协议层，即传输层和应用层，即 5G 网络利用 IETF 定义的 TLS 1.3 进行传输层保护，以及应用层端到端的保护。

5G 支持灵活性和多样化的服务， AF (Application function 应用功能) 或服务器可以通过 5G 网络直接向用户提供服务，用户和 AF 之间的应用域安全性仍基于 5G 安全可信根，由 5G 网络和 UE 基于接入认证（5G Authentication and Key Agreement，5G AKA）生成密钥材料，来保护用户和 AF 之间的端到端应用，从而使得 AF 无需向 UE 提供所需的安全凭证和密钥材料。

- 新业务的安全需求
- 新终端的安全需求
- 新连接的安全需求
- 新架构的安全需求

6G 时代的发展趋势及安全需求

03

6G 将在 5G 基础上进一步赋能各个垂直行业，助力人类社会实现“万物智联、数字孪生”的美好愿景。除了提供个人穿戴、数字健康等以人为本的服务外，6G 能够支持更加多样化的垂直行业与场景部署，如工业互联网、零功耗通信、智能交通、智能物流等。

6G 时代万物互联，新业务形态、新终端设备、新连接方式呈多样化发展：

业务多样化：
相对传统的 2C（To Consumer）业务，新型 2C 业务和 2B（To Business）业务迅猛发展，如数字健康、扩展现实（Extended reality，XR）、智能交通、智能家居、工业互联网、智能物流等。

终端多样化：
上述新业务需要的终端设备形态丰富，如可穿戴设备、零功耗物联网设备、智能汽车等。

连接多样化：
终端设备在 6G 时代会使用通感一体化技术，进一步扩展数字世界对物理世界的探索。大规模连接和频谱共享等新连接形式也会出现。

以上这些发展趋势会对当前的通信模式带来巨大改变，可以看到越来越多的数据开始从终端侧收集，再传输到网络侧，成为人工智能必不可少的数字资源，6G 系统将针对这些高价值数据资产进行管理。

因此，**6G 安全的最大变化趋势是保护的重点从传输逐渐演变为数据与隐私。**6G 系统中对数据进行收集、处理、存储、分析、应用、共享时，这些数据归属于不同的利益相关方，需要解决如何保护数字资产价值，防止数字资源被滥用。此外，当数据从个人终端侧进行收集时，极有可能会涉及到个人终端数据，研究如何在高效的使用这些数据的同时保护好用户隐私，在 6G 中会更加重要。

6G 系统中，存在多样化的终端服务于不同的业务，在 6G 业务、6G 网络、6G 终端之间分享不同的业务数据，因此需要考虑 6G 系统的多信任模式，为不同的终端以及不同的业务数据建立安全域，在高效传输数据的同时保证多源数据按归属进行隔离，防止数据被滥用。

此外，在工业场景中会使用海量物联网终端设备，其中很大一部分物联网终端设备会是低成本零功耗终端 [3]，功耗、存储和处理能力受限，对于这一类终端，需要考虑如何提供安全保护的同时适配轻量级的设备限制。

同时，在使用通感一体化技术时，需要考虑感知信号和传统连接的差别，感知业务利用底层信号进行对物理世界的探索，因此要考虑底层信号的安全保护。如果底层信号感知的是个人敏感信息，还需考虑隐私保护。

针对 6G 业务、终端及连接多样化趋势，OPPO 6G 白皮书提出极简多能的 6G 新架构，6G= 极简核心 +N 个子系统，由一个最小化的极简核心提供内生智能、安全、灵活频谱管理等共性能力；在一个极简的共性技术核心上，设计若干有限融合的子系统，容许各个场景的 6G 系统适度解绑、各自优化，实现一个“能力按需分配、功能灵活组合”的“极简多能”的 6G 系统 [4]。6G 系统可以通过多种 AI 算法的切换和组合，实现多个子系统的切换和组合。**在面对多源的业务数据时，同样需要对安全功能进行智能安全编排，满足不同场景的多样化安全需求。**

6G 系统未来承载的业务应用和数据价值将得到极大提升，驱动着 6G 系统安全技术的发展。6G 安全应重点保护行业数据资产的价值和用户隐私，适配物联网终端的分布式和轻量级安全机制，对新连接进行底层保护，使用 AI 编排智能安全策略，如图 3-1 所示。

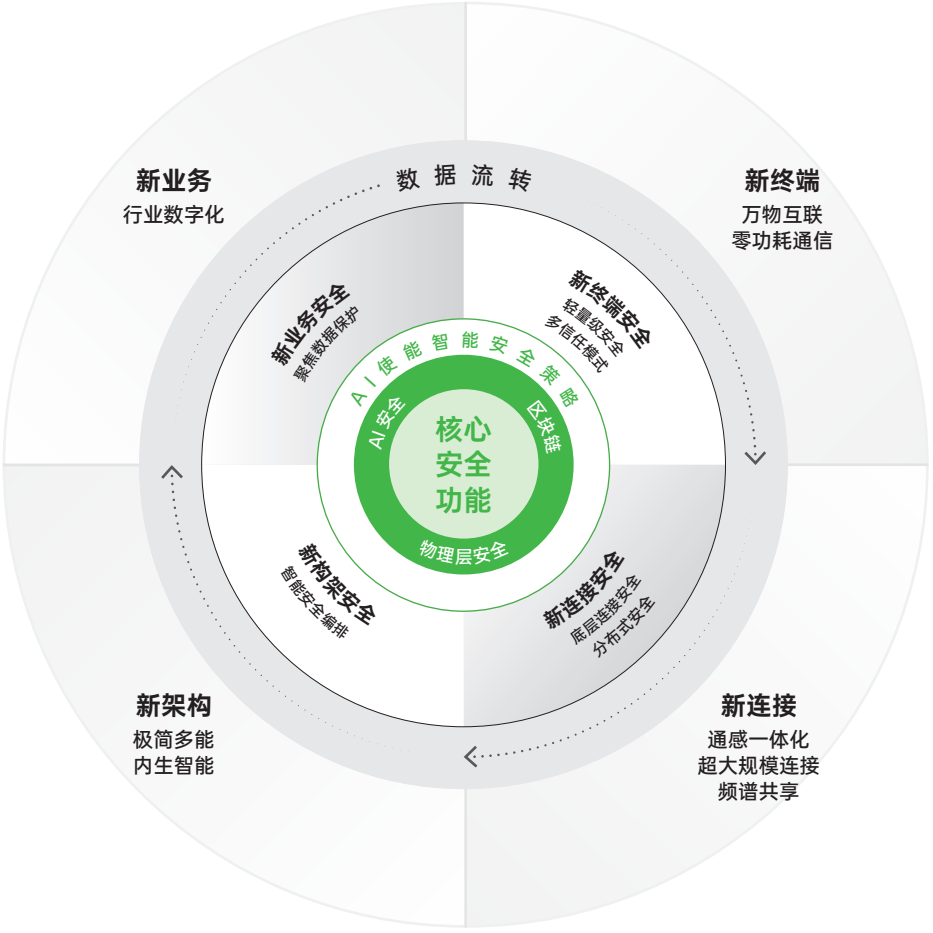

图 3-1: 6G 安全需求概览

接下来会对 6G 安全的关键需求进行讨论，包括

- 新业务的安全需求
- 新终端的安全需求
- 新连接的安全需求
- 新架构的安全需求

新业务的安全需求 3.1

6G 通过大量先进的传感器的部署和人工智能技术的运用，将扩展现实世界在数字世界的应用 [5]。 人工智能将赋能工业互联网、数字健康、数字孪生、XR：

通信与 AI 融合	随着人工智能与机器学习技术的普及与快速发展，图像、语音识别和自然语言翻译技术已被广泛应用于智能终端，渗透到通信系统，并对用户的生产生活产生了深刻影响。 6G 系统中将存在大量具备模型训练、模型推理能力的智能节点，这些节点参与执行本地或分布式的计算过程。 OPPO 提出的 AI-Cube 白皮书 [6] 中描述了通过 AI 功能面、AI 用户面、和 AI 控制面，共同赋予 6G 系统精准决策能力、AI 推理能力、自演进能力和迁移学习能力。
工业互联网场景	随着工业互联网的发展，大量的物联网终端设备可以部署于生产线、仓储管理和物流运输等各业务领域。 数据在物联网设备处采集、生成，并通过网络发送给相应的处理网元和业务服务器，从而达到监测、自动化控制、优化工业流程的有益效果。
数字健康场景	随着传感器、人工智能和通信技术的发展，6G 系统将为数字健康带来巨大的潜力，开启新应用场景： （1）多维感知远程医疗： 采集用户健康信息，实现远程监测与诊断，提供丰富的诊疗数据。 （2）数据积累与分析： 利用人工智能提升健康数据分析的效率，同时提供高质量数据集。 （3）数字孪生： 基于数据、模型和接口对人体进行分析、诊断、模拟和控制，构建人体的数字化镜像，用于模拟患者的生理特点，分析健康状况，预测疾病进展。
沉浸式多媒体和多感官互动场景	该业务旨在扩展多感官信息的完全模拟和实时交互，创造以人为中心的沉浸式人机交互体验，应用包括： （1）沉浸式 XR 体验： 如娱乐、社交和办公等日常活动，通过虚拟现实（Virtual reality，VR）和增强现实（Augmented Reality，AR）技术加强用户沉浸感。 （2）多维感知交互： 结合触觉、味觉、嗅觉等感官信息，用于增强医疗领域、或娱乐体验。 （3）全息通信： 利用全息技术实现 3D 场景的实时互动，适用于娱乐、全息会议等。

新业务的安全需求包括以下内容：

安全保护的重点从传输逐渐演变为数据与隐私	在工业互联网、智能物流等场景中，如果未经授权的通信实体获取到物联网设备的上行业务数据，或者上行传输数据被攻击者窃听，会导致业务数据的泄漏，有损数据拥有者的权利，对业务造成危害。 在数字健康、沉浸式多媒体和多感官互动等场景中，如果泄露的数据涉及个人隐私，这不仅损害了用户的权利，也可能会造成业务运营者或网络运营者的合规风险或法律风险。 因此，新业务安全保护的重点从传统的传输逐渐演变为面向新业务的数据与隐私。

新终端的安全需求 3.2

6G 的大规模通信用例包括智慧城市、交通、物流、卫生、能源、环境监测、农业以及许多其他领域的扩展和新应用，需要各种无电池或长寿命电池的新型物联网设备 [7]，新终端可应用于以下典型场景与技术：

零功耗通信场景

该场景正在推动物联网朝着能量高效和可持续发展进发。 该场景主要建立在三个核心技术基础之上： 射频能量采集、反向散射和低功耗计算。 这些技术允许物联网终端通过捕获环境中存在的无线电波来收集能量，并利用这些能量通信，减少对传统供电方式的需求 [3]。 同时，通过精简的射频和基带电路设计，不仅能够降低生产成本和设备尺寸，还能显著降低电路运行时的能耗。 国际标准组织 3GPP 已经识别出了零功耗（即 Ambient IoT，环境供能的物联网）通信的一些潜在应用场景 [8]：（1）智慧城市建设和工业互联网领域的远程监测； （2）物流和仓储管理中的盘存任务； （3）智能家居环境下的物品定位和智能控制。

室内定位场景

该场景主要面向人流密集的办公楼、机场和商场，以提供导航，优化人流分布，提升服务效率。 该场景还还可以应用于工厂和物流中心，提供精准定位支持智能货物管理和追踪，降低成本。 6G 时代，基于大规模天线、大宽带、零功耗通信等技术，有望实现室内厘米级的定位精度，满足更高的精准定位需求。

智能交通场景

装备了传感器、摄像头和 AI 算法的智能汽车能够自主导航、检测周围环境、防止碰撞，甚至在复杂市区道路状况中自行驾驶。 车辆的传感器、车与车之间、或车与路边基础设施之间的数据，可以用于车与云端的协同计算，从而能够提升车辆的路况检测能力，提前预警潜在危险，优化行驶路径，提升整体交通的效率和安全性。

智能物流场景

随着数字化和自动化技术的发展，智能物流利用物联网、大数据、人工智能与机器学习等技术，正在转变资产和劳动力的管理方式。 例如，通过在设备、产品、车辆和工人间的精准数据交换，能够支持物流节点和仓库中高效的货物的流转、存储、装卸与盘点操作。 6G 系统将支持超大规模的连接和精确的位置定位，提高系统容量，使货物实时追踪成为可能，使能物流自动化和智能化的实现。

新终端的安全需求包括以下内容：

零功耗设备的轻量级安全需求

由于零功耗设备的极简设计、环境供能和超低能耗特性，传统的安全通信机制因高计算复杂性而面临挑战。相比其他类型的物联网设备，如 NB-IoT（Narrow Band Internet of Things 窄带物联网）设备和 RedCap （Reduced Capability）设备，零功耗设备的协议栈设计复杂度与计算能力更低。因此，设计轻量级的安全技术成为保障零功耗通信安全的关键。安全功能应遵循轻量级的设计思路，满足以下安全需求：

01

资源受限条件下的可信接入与数据授权：

因此，需要研究与极低复杂度终端能力相适配的低成本安全可信接入与数据授权机制；

02

简化的数据传输安全：

为避免攻击者在数据传输过程中窃取数据，以及适配低成本的终端特点，需要简化的传输安全保护机制；

03

能够抵御拦截、伪造、重播等网络攻击。

多样化终端设备的多信任模式需求

多样化的终端设备通过 6G 网络服务于不同的业务，需要在 6G 业务、6G 网络、6G 终端之间分享不同的业务数据、模型、指令等消息，对于不同的业务，需要确保使用数据资产的正当权限，即保证其服务于正确的数据拥有者，不能被其他业务和网元滥用。为了保障 6G 系统对多样化终端设备的多源数据进行分类处理，需要考虑 6G 系统的多信任模式，为不同的终端以及不同的业务数据建立安全域，在高效传输数据的同时保证多源数据按归属进行隔离，防止数据被滥用。

新连接的安全需求

3.3

6G 中包含以下新连接的典型场景：

通感一体化场景

作为 6G 新增的典型场景， 通感一体化旨在利用通信信号实现对目标的检测、 定位、识别、 成像等感知功能 [9]。 3GPP 的需求制定组 SA1 已经识别出了一系列感知应用场景 [10]， 对于个人用户而言， 这些潜在的应用包括：

基于设备甚至无设备的超高精度目标定位	基于手势、动作、步态等生物特征的目标识别
智能家居中的访客识别与控制	高分辨率实时地图构建等

此外，通感一体化也将有助于提高通信的性能和效率，例如，通过考虑用户移动轨迹和环境变化来优化无线资源利用率。

超大规模连接场景

6G 系统的连接密度将从 5G 系统的 100 万 / 平方公里增加到 1000 万 / 平方公里 [5]。超大规模连接在 5G 海量物联通信的基础上，拓展设备数量、应用领域和能力边界，支撑数以亿计的设备互联互通，应用于智慧城市、智能农业、和工业互联网等场景 [11]。

频谱共享场景

随着移动业务所需的频谱量的增加，频谱共享和协调是非常有益的。频谱协调的好处包括促进规模经济、实现全球漫游、降低设备设计的复杂性、提高频谱效率(包括潜在地减少跨境干扰)[5]。运营商可以把闲置的频谱共享给另一个运营商使用，以便非签约用户，从而获取额外的收益。

新连接的安全需求包括以下内容：

通感一体化的授权和隐私保护需求

由于感知技术可以跟踪并可能识别环境中的任何事物，包括不携带终端的对象，因此需要考虑隐私保护 [10]。

不同感知对象所产生的感知数据不同，针对特定个体或特定区域的感知可能涉及敏感数据，如感知对象的精确位置、物体的物理特征、感知对象的生命体征。 同时，感知数据的获取亦须遵循地区的法律、法规。 因此，对于不同对象和不同区域的感知，需要不同粒度的授权机制与隐私保护，以避免滥用感知操作和感知数据。

通感一体化的物理层安全需求

由于感知信号和测量的感知数据通常来自底层，攻击者容易获取感知信道状态信息，进而推断涉及目标隐私信息的感知结果，例如，窃听者可能在不解码帧内容的情况下监听无线传输并测量 , 获得智能家居场景或者智能健康 / 医疗场景下人体的相关数据等。 另外，即使感知波形及其信号参数不公开，攻击者仍可以采用参量估计技术获取感知信号参数，从而对感知信号进行重放攻击，导致接收端测量出现时延，甚至提取参数错误。 因此，有必要对感知信号来源的真实性进行检验，并保证感知信号安全传输，考虑物理层的安全保护机制。

超大规模连接的分布式安全需求

对于海量不同形态的终端设备，设计统一的 6G 安全方案具有较大的挑战。 此外，超大规模设备连接到动态异构的网络，需要大量安全信令开销，会给传统中心化的安全管理带来挑战，需要高效、及时的处理海量设备的安全接入。 同时，设备在特定区域范围内接入移动通信系统，业务和系统存在跨区域形态，具有分布式的特点，因此需要考虑海量终端设备的分布式接入认证与数据授权。 对于超大规模连接场景可以考虑高效的、局部自适应的、分布式的安全机制和安全功能。

频谱共享的高可靠安全需求

为了保障闲置频谱的安全共享，保护运营商利益，需要安全的用户接入机制和可靠的跨运营商计费规则。 现有的蜂窝系统漫游机制对频谱共享可能不够高效和可靠，GSMA（全球移动通信系统协会）正在研究基于区块链的漫游优化 [12]，对于频谱共享，可以进一步考虑利用区块链的分布式特性和多方信任特性，进行高可靠的安全设计。

新架构的安全需求

3.4

OPPO《6G： 极简多能，构建移动的世界》白皮书，提出极简多能的 6G 新架构，6G= 极简核心 +N 个子系统，由一个最小化的极简核心提供内生智能、安全、灵活频谱管理等共性能力； 在一个极简的共性技术核心上，设计若干有限融合的子系统，容许各个场景的 6G 系统适度解绑、各自优化，实现一个“能力按需分配、功能灵活组合”的“极简多能”的 6G 系统。 通过多种 AI 算法的切换和组合，实现多个子系统的切换和组合 [4]。

新架构的安全需求包括以下内容：

由于不同的多个子系统的业务场景、终端类型等会产生多样性的安全需求，使用 AI 技术对安全的基本功能和差异化安全功能进行智能编排，围绕数据资产的价值，动态地满足对业务场景的安全需求，使能子系统的安全功能实现。 零信任是一种侧重于数据保护的架构方法，可以制定动态策略以决定对数据和资源的访问 [13]，**6G 需要基于零信任考虑构建智能的、适配不同 6G 子系统的安全保护架构。**

- 零信任背景
- 基于零信任构建智能安全

基于零信任的 6G 智能安全架构

04

零信任背景

4.1

自从 2009 年 Forrester 提出零信任理念以来，零信任安全模型在金融、互联网、云服务等行业中得到广泛应用。 零信任提倡这三个核心原则： 所有实体默认不受信任，强制执行最小权限访问，并实施全面的安全监控。 基于零信任的安全系统设计可以通过动态的身份认证和授权，保证对数据和资源的访问由动态策略决定。

在业界广为人知的零信任架构中 [13]，位于控制平面的策略引擎（PE）根据一系列的信息源（包括持续诊断和缓解（CDM: Continuous Diagnostics and Mitigation）系统、行业合规、威胁情报、活动日志、数据访问策略、公钥基础设施（PKI: Public key infrastructure）、ID 管理、安全事件管理系统）动态地决策授予访问主体对相关资源的访问权限。 策略管理者（PA）将根据 PE 的执行决策，生成访问凭证，建立、维护、终止会话。 策略执行点（PEP）是与访问主体交互的组件，根据 PA 发布的策略指示，建立、终止通信会话。

零信任的架构可能有多种变体，可通过多种方式为特定工作流程定制不同的零信任架构，例如使用网络基础设施和软件定义边界方法，PA 作为网络控制器，根据 PE 做出的决策来设置和重新配置网络，客户端通过 PEP 请求访问，提供基于业务的安全体系结构。

随着零信任技术的发展 , 和政策与标准的涌现，零信任的商业模型走向成熟，市场逐步规模化。 根据中国信息通信研究院在 2023 年发布的《零信任发展研究报告》[14] 中的统计数据显示，零信任在重点行业市场（例如金融、电信）呈现增长态势，在不同应用场景中落地，例如远程办公、远程运维、多分支机构互连等。

基于零信任构建智能安全

4.2

基于多源的业务数据这个关键变化，**安全保护的重点从传输逐渐演变为数据与隐私。为了保护业务的数据资产，满足不同子系统多元化的安全需求，在 6G 时代需要智能安全，对系统、子系统信任模型、数据访问授权、以及传输安全进行更全面的安全评估，实施灵活的、动态的安全策略。**

在 6G 时代，可以考虑基于零信任的安全架构，支持安全策略智能化，灵活地、动态地编排安全策略，根据安全需求智能配置安全功能。**与静态的 5G 安全架构相比，6G 动态的安全智能架构不仅仅能支持当前识别出来的安全需求、子系统及安全能力，配置相应的安全策略，随着 6G 业务场景的丰富、安全技术的发展，还能够灵活的引入新的安全能力，配置新业务场景的安全策略，满足后向兼容的发展需要。**基于零信任的 6G 智能安全架构如图 4-1 所示。

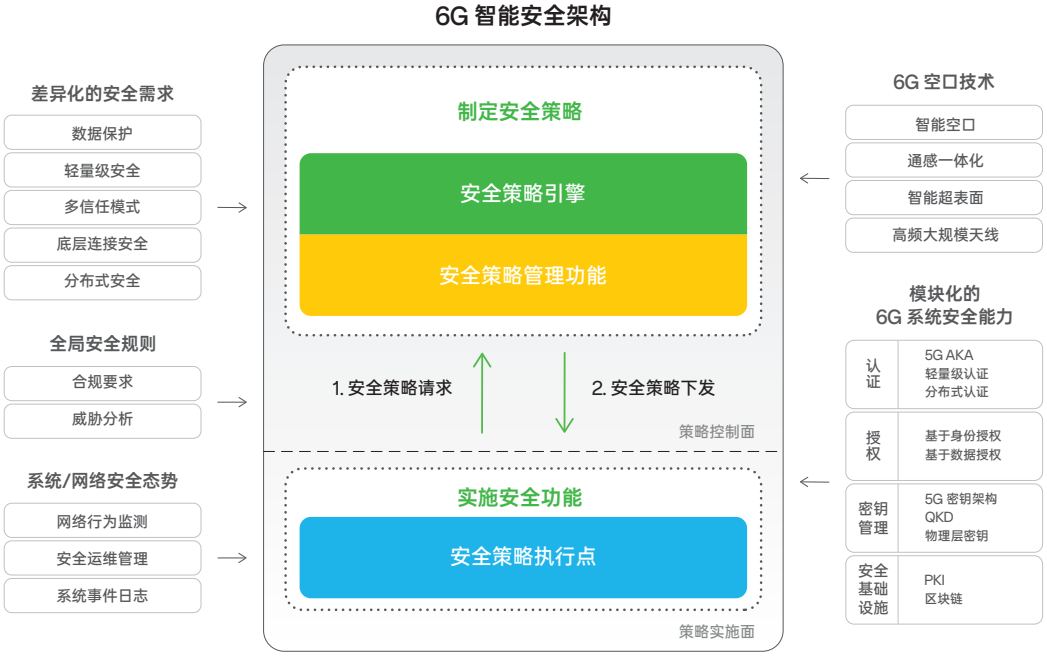

图 4-1: 基于零信任的 6G 智能安全架构

基于零信任的 6G 智能安全架构的核心组件

安全策略引擎 SPE (Security Policy Engine)

借鉴零信任策略引擎功能 PE，根据输入，为“极简多能”的 6G 系统制定安全策略。

安全策略管理功能 SPA (Security Policy Administrator)

借鉴零信任策略管理功能 PA，为策略制定和策略执行之间建立通信路径，提供输入或输出。

安全策略执行点 SPEP (Security Policy Enforcement Point)

借鉴零信任安全策略执行点 PEP，为每个子系统配置差异化的安全功能。

制定安全策略和实施安全功能的原则：

6G 智能安全架构将基于两个变量，安全变量与业务 / 系统变量，智能地制定和调整安全策略：

安全变量

全局安全规则和系统 / 网络安全态势。 在 6G 环境中，由于外部监管要求、网络条件、业务需求和威胁的动态性，这些安全策略需要能够及时适应新出现的法律法规要求和安全威胁。 全局安全规则包括具有普适性的合规要求和业界威胁分析，系统 / 网络安全态势则包括系统和网络实时的攻击态势或网络的安全运行状态。

业务 / 系统变量

业务差异化安全需求、6G 空口具备的网络能力和模块化的安全能力。“极简多能”的 6G 系统支持高效地上线新业务，需要快速为新业务制定所需安全策略，为子系统配置适当的安全功能。 6G 空口具备的能力可以使能或优化安全功能，例如智能超表面（Reconfigurable Intelligent Surfaces，RIS）和智能空口都能提高物理层安全密钥生成的效率和安全性。 6G 中模块化的安全能力包括认证、授权、密钥管理、安全基础设施等，和其他 6G 系统功能和协议解耦，有利于安全功能的按需灵活配置。

制定安全策略和配置安全功能的实例：

如图4-2所示，由SPE为不同的子系统制定差异化的安全策略，并由SPEP配置安全功能：

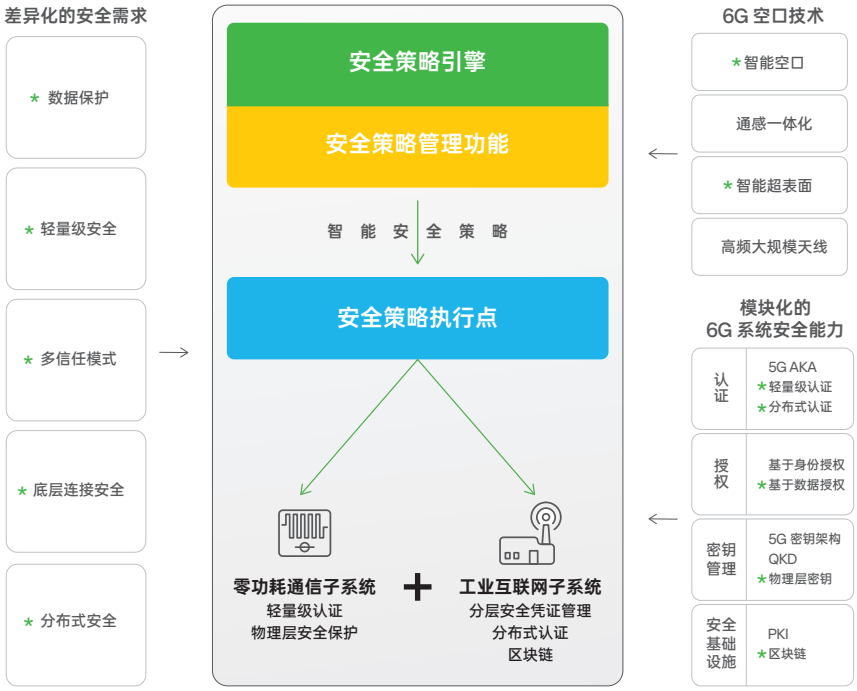

图 4-2: 子系统的差异化安全功能

工业互联网 + 零功耗通信子系统安全策略编排与安全功能配置

SPEP 通过 SPA 向 SPE 请求安全策略。以工业互联网 + 零功耗通信子系统安全功能为例，需要考虑全产业链环节，不同地点的数据搜集与处理，因此需要多信任模式、分布式安全，以及对业务数据的保护。同时，考虑到零功耗设备需要在计算和处理资源受限的情况下完成安全功能，因此需要轻量级安全以及底层连接安全。

SPE 制定安全策略：

SPA 读取模块化的 6G 系统安全能力，并上报给 SPE，SPE 根据上述安全需求，选择安全能力，比如认证功能里的轻量级认证模块、分布式认证模块，授权功能里的基于数据授权模块，密钥管理里的物理层密钥模块，安全基础设施里的区块链，作为该子系统需要的安全能力。SPE 进一步根据选择的安全能力，组合成子系统安全策略。

SPEP 配置安全功能：

SPA 获取 SPE 制定的子系统安全策略，并进一步读取 6G 空口技术列表，发送给 SPEP。SPEP 根据安全策略和空口技术实施安全功能，即根据不同的空口技术对安全能力进行增强。比如，如果安全策略包括物理层密钥，系统具备智能空口及智能超表面技术，那么 SPEP 可以使用这些空口技术加强物理层密钥的安全性能。

最终工业互联网 + 零功耗通信子系统获得的安全功能为： 轻量级认证、分布式认证、基于数据的授权、物理层密钥、区块链。

- 区块链与 6G 安全
- 物理层安全与 6G 安全
- 6G 时代的 AI 安全
- 后量子安全

6G 时代
关键安全技术

05

区块链与 6G 安全

5.1

区块链具有分布式和可信的特点，能够促进数据的共享，在 6G 时代将成为产业数字化的关键基础设施。 在产业应用中，电信运营商和区块链供应商大力发展区块链基础设施网络，并面向各行各业推出区块链服务，其中包括区块链身份管理服务、接入认证服务和安全服务。

区块链分为公有链、私有链和联盟链。 其中联盟链和私有链是可信区块链，联盟链可以由多方参与，通过安全算法实现参与方之间的信任关系，能够用于实现 6G 时代的多方信任模式，构建内生可信的多方信任可信根。 基于区块链的分布式数字身份（Decentralized Identity，DID）技术，能够支持分布式的身份管理，可用于实现分布式认证。

零功耗设备这样的轻量级物联网终端受限于计算、存储资源，可能无法支持传统的认证计算，基于身份的密码算法（identity-based cryptography, IBC）支持轻量级的身份管理和认证机制，可用于低成本认证。

频谱共享需要多方信任和高效的计费机制，基于区块链可信的特点，通过联盟区块链和智能合约，可以支持跨运营商的高可靠频谱共享，确保频谱共享计费的可信度，减少争议。

5.1.1 基于区块链的多方信任

在安全凭证发放阶段，运营商可以和多个业务提供商灵活地建立安全管理，多个业务提供商之间可以相互隔离，独立地管理安全凭证。 基于区块链技术，可以由多方共同维护联盟区块链，区块节点之间相互信任，用于存储物联网终端的凭证，物联网终端的凭证可以跨域上链和获取。 如图 5-1 所示，独立证书存储不能支持多方信任，基于联盟链区块链的证书存储能够支持多方相互信任。

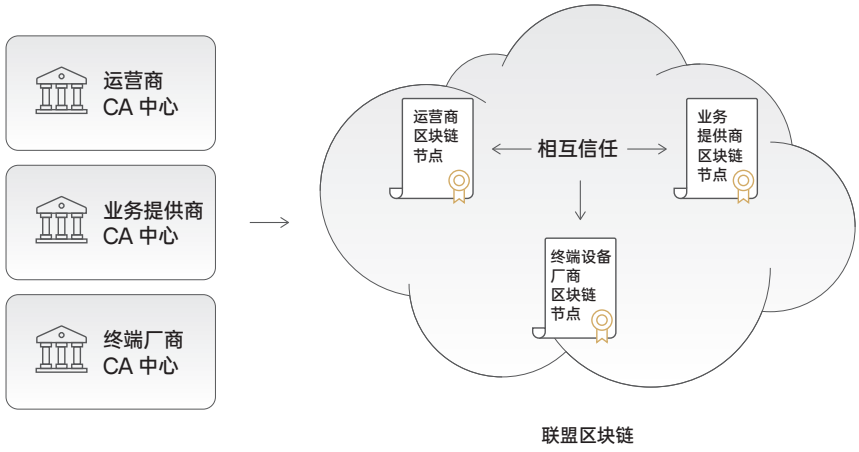

图 5-1: 独立证书存储 VS 基于联盟链区块链的证书存储

结合分层安全凭证管理和区块链，可以实现多方信任和分布式信任。

在安全凭证发放阶段，分层的安全凭证管理机制可以支持移动通信系统对海量物联网终端设备的高效安全管理，以及支持运营商对使用这些物联网终端设备的业务提供商的灵活安全管理策略。

一层 CA（Certificate Authority 证书授权）中心根据安全多方计算，管理和授权各类业务提供商，再由下层 CA 中心为海量物联网终端设备发放安全凭证。 这样的分层管理机制使得业务提供商的安全管理更高效。

分层安全凭证管理架构可以分为二层安全凭证管理架构和三层安全凭证管理架构，二层安全凭证管理架构使用 DID 技术管理联网设备安全凭证，三层安全凭证管理架构使用 IBC 管理物联网设备安全凭证。

以三层安全凭证管理架构为例，包含以下功能主体，如图 5-2 所示：

三层的凭证管理架构

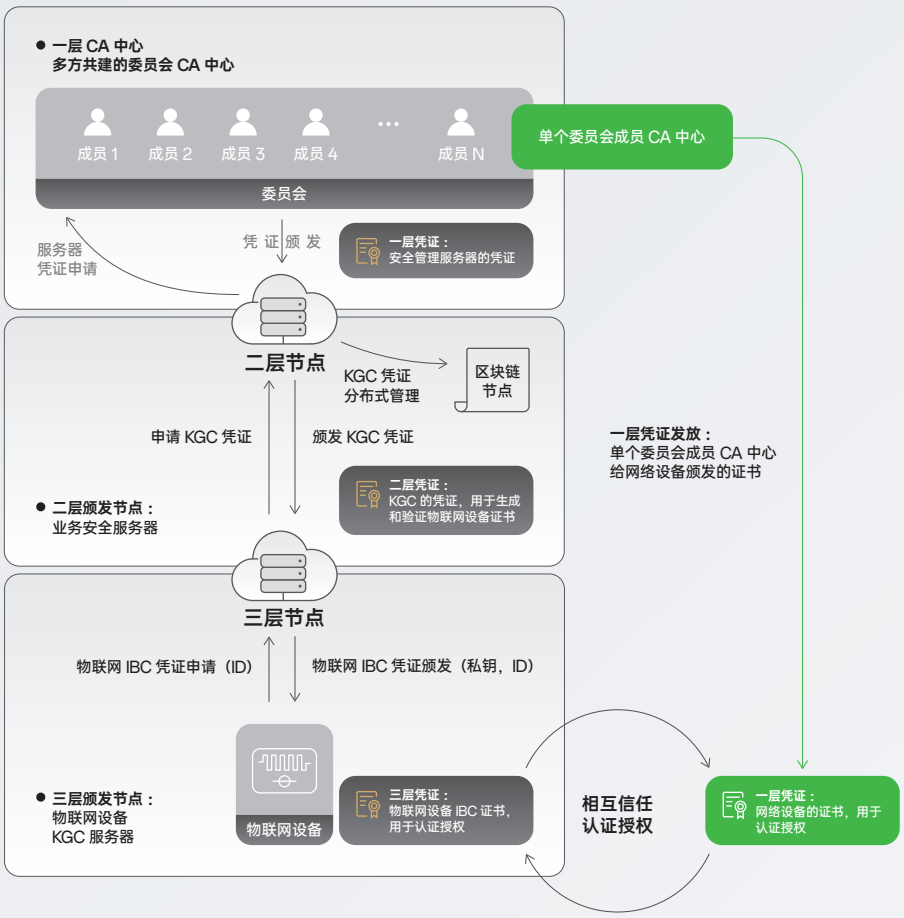

图 5-2: 三层安全凭证管理架构与多方信任

一层凭证颁发方

多方共建委员会 CA 中心节点，可以由国家节点、各大运营商和终端设备厂商共同建立，主要功能是给二层安全凭证管理服务器颁发凭证以及维护撤销列表。这样有益于多方共同构建相互信任的可信根。

共建 CA 中心的其中一个运营商委员，可以单独给该运营商的网络设备发放安全凭证，这个网络设备的安全凭证是一层安全凭证。

二层凭证颁发方

业务安全管理服务器，主要功能是给物联网设备密钥生成中心（Key Generation Center，KGC）服务器发放凭证以及维护撤销列表，同时负责将 KGC 服务器的安全凭证上链。

由于一层多方共建委员会 CA 中心节点为虚拟节点，不具备接入区块链的功能，所以二层凭证颁发方需要接入区块链并完成安全凭证上链的过程，因此需要二层凭证颁发方为 KGC 颁发安全凭证，而不能直接由一层 CA 中心为 KGC 颁发凭证。

三层凭证颁发方

KGC, 即物联网设备安全凭证管理服务器，可以由业务提供商、运营商部署，也可以由他们委托服务平台、终端厂商部署，主要功能是使用 IBC 技术给物联网设备颁发及撤销凭证。KGC 采用 IBC 模式统一对其信任域下的大量物联网设备的安全凭证进行管理，此时，物联网设备的安全凭证被简化为由其所属 KGC 信任背书的 ID，即物联网终端的安全凭证 ={ID, KGC 证书 }。此外，由 KGC 为物联网设备的 ID 维护一个撤销列表，记录被撤销的物联网设备的身份信息，防止已被撤销设备的身份被盗用。

分层管理架构有利于分布式分发、管理移动通信系统中海量物联网设备的安全凭证，提高安全管理效率。由于终端安全凭证管理服务器的证书是运营商参与颁发的，因此分层的安全凭证管理架构可在运营商可控的情况下，提高不同业务物联网终端的安全管理效率，降低管理复杂度。

对于三层安全凭证管理架构，由于一层凭证颁发方是多方委员会共建 CA 中心，可以由移动网络运营商、终端设备厂商等共同建立，并且由共建 CA 中心给 KGC 颁发安全凭证，再由 KGC 给业务提供商颁发安全凭证，最后由业务提供商给物联网设备颁发安全凭证，因此物联网终端的三层凭证和运营商委员发放的运营商设备安全凭证可以相互信任，因此业务提供商颁发凭证的物联网设备可以和运营商设备相互认证授权，也可以和业务提供商服务器相互认证授权，从而建立起运营商、业务商、终端设备厂商的多方信任。

5.1.2 区块链支持分布式身份管理与数据授权

当物联网设备收到数据请求时，需要对请求数据的功能实体完成身份校验和数据授权，确认对方有适当的权限，才能把数据上传。 由于采用了多方信任安全凭证管理，多方相互授权成为可能，物联网设备安全凭证可以和运营商设备的安全凭证以及业务功能的安全凭证相互信任，授权对应的业务实体获得物联网设备上传的数据。

在认证授权阶段，由于区块链支持安全凭证的分布式管理，因此可以实现分布式认证，无需接入集中式节点执行认证，可以由联盟链存储安全凭证，网络边缘节点接入联盟链获取凭证，执行验证授权，在海量物联网终端场景下大大提高认证效率，减轻网络设备的工作负载，避免因单点故障引起的网络认证服务中断。

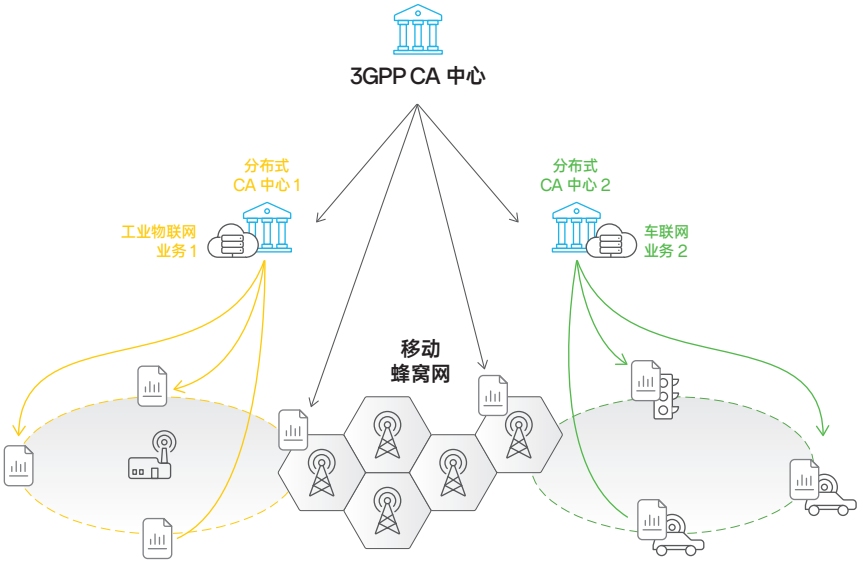

图 5-3: 分布式身份管理

如图 5-3 所示，对于需要分布式接入的业务（如： 跨域物流），物联网终端需要在多个地点接入，可以由联盟链存储安全凭证，网络边缘节点接入联盟链获取凭证，实现分布式的身份认证与数据授权。

对于轻量级物联网设备，物联网设备的安全凭证上链能降低安全管理成本。 此外，还可以采用代理模式完成身份认证与授权，由 UE 或代理设备为轻量级物联网设备验证安全凭证，可以降低轻量级物联网设备的存储开销和计算开销，同时，代理模式可以以群组的方式对物联网设备进行高效管理和安全验证，相比单一物联网设备逐一进行安全校验的过程，可以降低处理的时延。

分布式身份认证

当运营商网络设备或业务服务器需要对物联网终端凭证进行验证时，利用物联网终端发送过来的 ID 和凭证链上位置，即可向分布式的区块链节点获取相应物联网终端凭证，无需到核心网获取凭证，从而执行分布式认证。

多方信任数据授权

当物联网设备需要对运营商网络 / 业务服务器进行身份认证并许可运营商网络设备或业务服务器获取物联网设备的数据时，物联网设备可以接收运营商网络设备或业务服务器发送的安全凭证，校验身份后，根据相关身份的许可授权数据获取，物联网设备只有在授权通过的情况下发送数据，并且只会发送给对应的运营商网络设备或业务服务器。

基于三层安全凭证管理架构的物联网设备与网络设备之间的身份认证与数据授权过程如下图 5-4 所示：

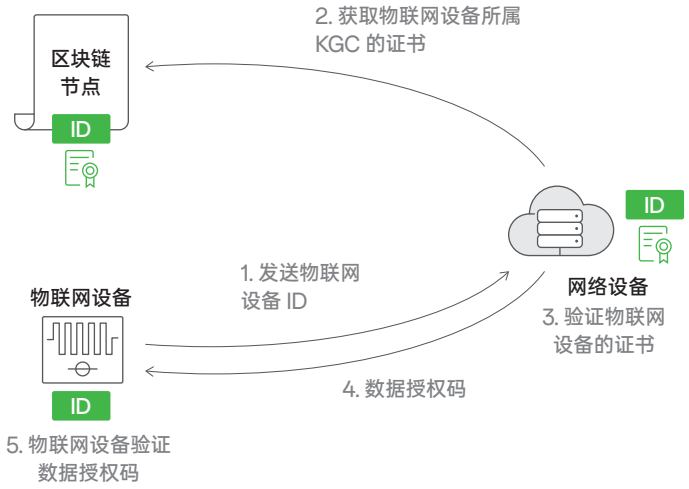

图 5-4: 物联网设备与网络设备的身份认证和数据授权过程

网络设备与物联网终端设备的认证授权过程可以分为以下步骤：

01	物联网设备向网络设备发送物联网设备 ID、所属 KGC 证书在链上的位置信息，用私钥计算身份校验码。
02	网络设备收到 ID 和链上的位置信息后向区块链节点获取物联网设备所属 KGC 的证书。 网络设备是能接入区块链的节点，考虑到区块链节点的分布式属性，网络设备可以是如基站这样的边缘节点，也可以是核心网设备。 联盟链的区块链节点支持多方信任的证书存储。 对于网络设备而言，可以信任从联盟链区块链节点上获取的证书，即使该证书不是网络设备的签发机构所颁发的。
03	根据 IBC 的安全凭证管理技术，物联网终端的安全凭证 ={ID, KGC 证书 }。 网络设备使用物联网设备发来的 ID 以及 KGC 证书验证身份校验码，完成对物联网设备的身份认证。
04	网络设备向物联网设备发送数据请求消息以及数据授权校验码，消息包含网络设备的身份 ID、证书，还可以包含业务方的 ID 和证书，目的是告知物联网设备，什么运营商和什么业务商请求获取相关数据。 数据授权校验码使用与证书对应的私钥生成。
05	物联网设备使用收到的证书验证数据授权校验码。

完成身份认证和数据授权后，物联网设备发送数据，网络设备或业务服务器可以获得物联网设备的数据。

5.1.3 区块链支持高可靠的频谱共享

在频谱共享场景中，运营商可以将部分闲置频谱资源出售给其他运营商使用，允许其他运营商的用户在安全可控的条件下接入闲置频谱资源。 为避免资源滥用和计费争议，确保频谱的授权接入，并执行透明、可靠且实时的计费，可以通过区块链和智能合约的协同作用，建立安全而高效的系统。

区块链和分布式账本保证可信授权

区块链技术为频谱共享提供了分布式安全管理的基础。区块链的分布式账本记录并存储了频谱授权的凭证信息和智能合约。这种分布式存储机制支持透明性和安全性，确保了所有参与方都能够查看和验证凭证的状态，并确保频谱授权信息和智能合约不可篡改。

智能合约保障自动计费

区块链上可以存储智能合约，智能合约通过自动执行预定的规则，实现了频谱授权以及计费过程的自动化。智能合约根据预设条件自动触发频谱授权过程，确保了实时的、可靠的频谱分配。智能合约支持自动化的计费过程，根据频谱使用情况自动扣除预定的费用。这降低了人为错误的可能性，提高了计费的准确性，有效避免运营商之间频谱共享计费的争议。

终端用户的身份管理与频谱共享的认证授权过程描述如图 5-5 下：

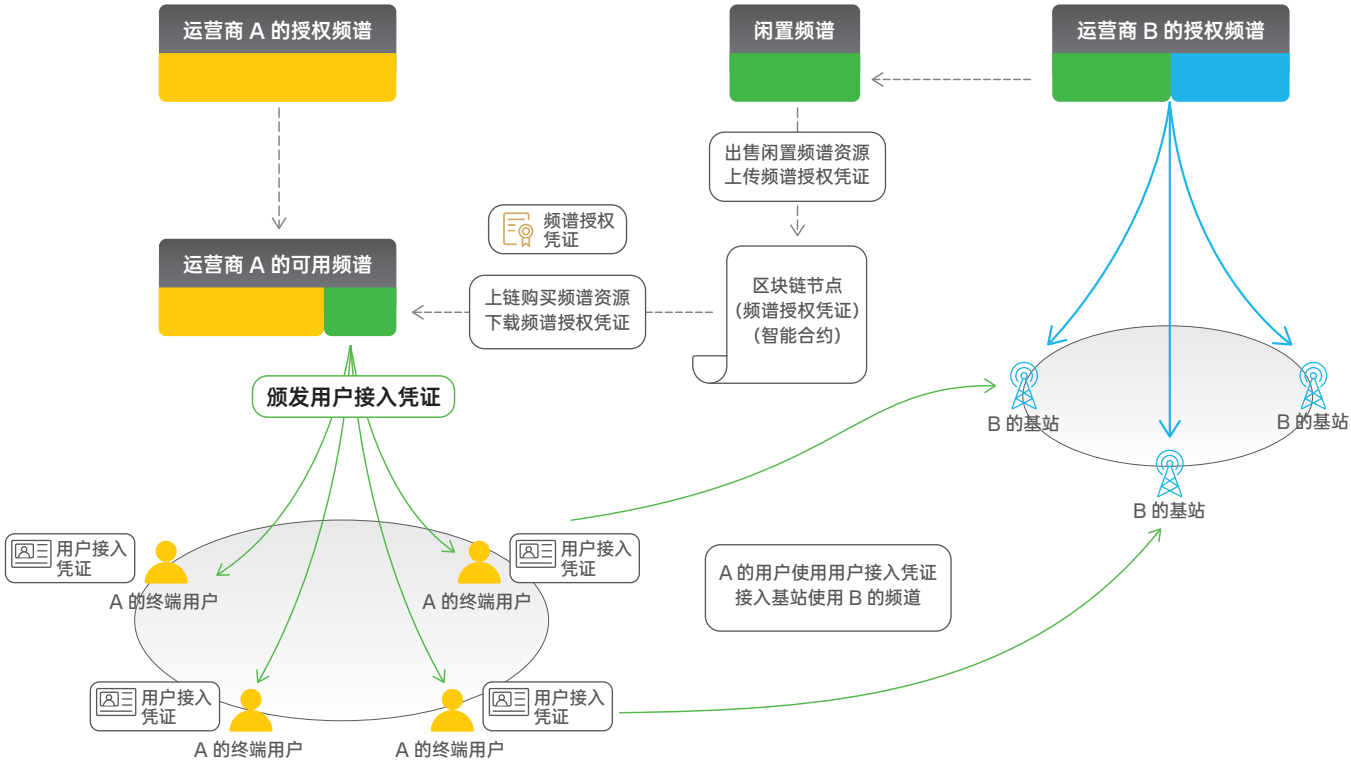

图 5-5: 区块链支持频谱共享的智能计费

如果运营商 B 希望将闲置频谱共享给其他运营商的终端用户使用，运营商 B 可以在区块链节点上存储这一段闲置频谱的授权凭证，由于区块链节点存储机制的透明性和安全性，频谱授权信息可以被联盟链的成员验证，并且不可被篡改。在任何一个分布式的区块链节点上存储的授权凭证，都可以用于用户的接入，从而保证了高效、快速的用户接入授权，如果基站可以接入区块链节点，那么用户可以在基站侧就完成频谱共享的接入授权，无需到核心网进行漫游认证过程。

如果运营商 A 的终端用户希望接入运营商 B 的闲置频谱，基于区块链建立的多方信任，可以直接用终端用户的安全凭证接入运营商 B 的闲置频谱，完成身份认证和频谱授权过程。

运营商 A 和运营商 B 之间的计费可以通过存储在区块链上在智能合约完成。由于区块链节点存储机制的透明性和安全性，智能合约的存储和执行过程可以被联盟链的成员验证，并且不可被篡改。运营商 A 和运营商 B 可以在智能合约中约定好计费规则和计费触发条件，在用户接入到共享频谱后，可以根据约定的规则触发计费，执行计费。

物理层安全与 6G 安全 5.2

以零功耗、通感一体化及超大规模连接为代表的 6G 新终端和新连接方式的出现对现有安全机制提出了挑战。 当前认证机制与密钥协商机制依赖于安全计算，对计算能力有一定要求，零功耗终端设备可能无法支撑。 此外，现有密码安全机制依赖上层协议进行加密和完整性保护，对于底层信号，比如物理层感知信号则无法进行安全保护。 超大规模连接的安全密钥分发机制导致大量安全信令开销，需要考虑更高效的密钥管理方法。 因此，6G 时代需要将现有高层安全机制向底层延伸，考虑在物理层实现通信的真实性、机密性、完整性和可用性。 物理层安全利用无线信道、传播环境和通信设备的特性，能够提供基于信息论的安全防御机制，相比传统安全机制提高密钥协商效率，并能结合现有高层安全机制实现自下而上的全栈安全保障。

随着 6G 空口技术的发展，物理层安全的应用潜力得到了极大的释放。 6G 系统中更高的频段、更高的带宽、更大的天线阵列，以及智能超表面带来的更可控电磁环境，为物理层安全的设计创造了丰富的信道资源。 此外，通感一体化与智能空口的引入，与丰富的信道资源相结合，能进一步增强对无线环境的利用。 基于无线环境，面向 6G 的物理层安全机制能够更好的满足 6G 电信业务场景下的安全需求，选择合适的物理层安全功能，如物理层密钥生成、物理层认证、物理层安全传输、物理层安全加密等。 6G 与物理层安全技术的融合如图 5-6 所示。

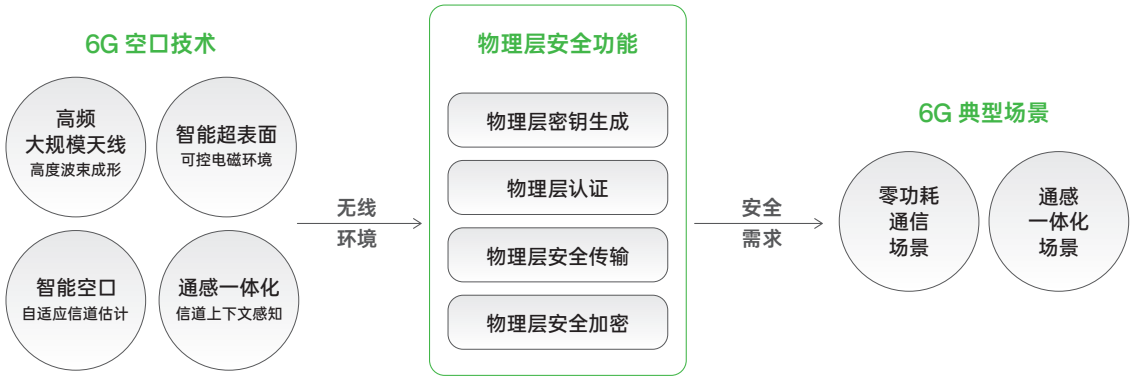

图 5-6： 6G 与物理层安全技术的融合

5.2.1 无线环境与空口技术

6G 的发展将集成各种新型空口技术，这些技术的发展为物理层安全的应用创造了有利的条件。

通感一体化

通感一体化能够动态获取无线信道上下文信息。 通信感知融合将实现通信能力和感知能力的交融互通，一方面，借助于通信系统提升感知精准度、提高感知时效性、实现无缝泛在的感知服务； 另一方面，基于对无线通信信道环境的感知、识别与预测不仅能够进一步提升无线通信系统的性能，还能助力通信双方基于无线信道进行物理层安全技术的实施，如物理层密钥生成。

智能空口

AI 能够帮助 6G 系统在训练空口信道数据集，以获取精确的信道状态信息，提升物理层密钥生成性能。 此外，基于 AI 的波束管理，能够实现精准的安全波束成形，实现无线信号的安全传输。 考虑到 6G 系统在部署场景、频谱、应用需求和设备功能方面的异构性增加，物理层参数的数量将会成倍增加，AI 将在空口中发挥更重要的作用，进一步为物理层安全的应用创造了有利的条件。

高频大规模天线

6G 将通信推向更高的频率和更大的带宽，同时天线规模也越来越大。 由于物理层密钥生成不依赖于特定实体提供的固定参数，而是依赖于无线信道的熵，因此向更高频率的转移为密钥生成提供了更高的熵，从而增加密钥生成速率。 此外，使用毫米波和太赫兹等更高频段的大规模天线系统通常需要定向传输来将能量集中在接收器上，窄波束定向传输有助于抵制窃听攻击。

智能超表面

智能超表面能够可控的调整无线信道传播环境，提升物理层安全传输和密钥生成性能。 通过反射入射波并将其引导到所需的方向，能够操纵和重新配置无线传播环境，促进物理层密钥生成。 此外，利用智能超表面，能够配置铅笔尖波束形成进行安全传输，使攻击者难以窃听。

5.2.2 6G 典型场景下物理层安全功能

物理层安全功能模块能够作为独立的模块嵌入到无线接入网的网元和协议中，并基于无线环境和典型场景的安全需求，选择最优的物理层安全功能，包括物理层密钥生成、物理层认证、物理层安全传输、物理层安全加密等。例如，针对零功耗通信场景，在完成首次认证后，利用信道特征生成物理层密钥保护接入层传输，能够降低零功耗设备的计算功耗。针对通感一体化场景，基于感知发送方和感知接收方的共享信息，设计感知参考信号，能够保护感知结果不被窃取。针对大规模连接场景，物理层认证技术能够优化频繁的认证给网络带来的信令开销，提高安全管理效率。

物理层密钥生成

物理层密钥生成的基本原理是利用无线信道的随机性、时变性和互易性，在收发设备之间生成共享密钥，窃听者由于不同的信道特性而无法获取相同的密钥。物理层密钥生成过程通常包括信道探测与特征提取、比特量化、信息协商和隐私放大，其中信道探测是指合法节点在信道相干时间内相互交换信道探测信号，并利用信道估计等手段提取接收信号特征。考虑到零功耗设备的功耗限制，接收端直接从接收信号中测量信号特征并量化提取密钥，而将信道估计等复杂信号处理手段转移到发送端，如基站或 UE。这种功耗友好的密钥生成方案，能够支持资源受限的零功耗设备生成密钥。此外，针对信道变化缓慢的室内零功耗通信场景，通过人为引入发送信号的随机性，能够提升密钥生成速率。

物理层认证

无线信道具备唯一性、随机性和不可预测性，除非两个通信节点在时域、频域和空域上完全一致，否则无法被仿冒，这就构成了物理层认证的安全内核。物理层认证机制可分为基于设备指纹的认证机制和基于信道特征的认证机制。其中，基于设备指纹的认证机制能够应用到零功耗场景中，利用硬件设备的独有特性提取唯一标识，如物理不可克隆函数（Physical Unclonable Function，PUF），并和设备 ID 进行绑定，作为零功耗设备的安全凭证，无需在非易失性存储器（Non-volatile Memory，NVM）中存储根密钥，从而能够实现轻量级的认证与密钥协商。而基于信道特征的认证机制能够应用到通感一体化场景中感知信号认证，利用不同位置设备的信道特征之间存在的不相干性，感知信号接收端能够计算接收的连续两个感知帧的相似度，判断该感知信号是否来自合法发送端。

物理层安全传输

物理层安全传输是基于香农提出的完美安全性概念以及 Wyner 提出的窃听信道模型 [15]，在不需依赖高层协议及设备的加密计算基础上，来建立传输信道的安全性。零功耗设备受限于计算、存储资源，可能无法支持传统的安全保护，如基于 AES 算法的 256 位加密机制在 PDCP 协议层的安全处理，物理层安全传输可以作为一个很好的补充，实现零功耗设备的轻量级传输安全。例如，为解决上行窃听，在零功耗终端发射曼彻斯特编码上行信息的同时，引入辅助节点同时发送伪随机生成的曼彻斯特波形进行人工加扰，主基站能够依据协商共享信息恢复原数据信息，攻击者缺少协商共享信息，从而无法恢复出原始数据信息。

物理层安全加密

物理层安全加密技术利用相位旋转、幅度调节、符号模糊和符号顺序变化等手段生成物理层信号 , 保护调制方式与调制符号信息，使窃听者无法解出正确信息，能够解决通感一体化场景中感知信号的窃听威胁。一方面，感知信号收发两端能够利用共享信息加解密参考信号序列，窃听者由于没有共享信息，因此无法进行信道估计。另一方面，收发两端还可以利用共享信息生成随机相位、随机幅度、随机子载波等参数，对调制符号进行加密处理，窃听者由于不知道共享信息而无法生成相同随机参数，进而无法获取信道状态信息和感知结果。

6G 时代的 AI 安全 5.3

5.3.1 安全的在 6G 中使用 AI 技术

6G 将把 AI 相关功能整合到通信中，并作为基础设施来支持新的用户和应用趋势。6G 预计将采用 AI 原生新型空口设计，利用 AI 增强无线空口性能。提供支持人工智能服务的无线网络将是 6G 技术设计的基础，以服务于各种人工智能应用 [5]。

因此，安全的在 6G 中使用 AI 技术（Security for AI），即如何增强 6G 系统从而能够安全地使用 AI 技术将是一个基础课题，比如 6G 空口和应用的安全也将包括如何安全的使用 AI 技术为空口和上层应用提供增强，防止攻击者破坏信道估计或者影响业务的判断。

Security for AI 可以按照机器学习的过程大致分为 3 个阶段和 7 类风险，分别为训练阶段、推理阶段和传输阶段，对应数据窃取风险、数据篡改风险、隐私泄露风险、模型破坏风险、对抗攻击风险、模型逆向风险和模型反演风险，如表 5-1 所示。

训练阶段

攻击目标为训练数据的安全与隐私，恶意攻击者在多方合作训练中注入恶意数据，观察其对建模结果的影响，进而推断其它参与方训练数据的隐私，对应数据窃取风险和隐私泄露风险；

攻击目标为训练模型，恶意攻击者在多方合作训练中注入恶意数据，影响模型的准确性和可信度，对应模型破坏风险；

推理阶段

攻击目标为推理结果，恶意攻击者在测试数据里加入一些恶意改动，使模型产生错误的输出，对应对抗攻击风险。

攻击目标为模型，攻击者通过大量的测试样本、推理输出以及一些背景知识，推断出模型的内部结构或参数，对应的是模型逆向风险。

攻击目标为训练数据安全与隐私，攻击者使用已知模型输出和一些背景知识来还原模型的输入，对应模型反演风险。

传输阶段

攻击目标为网络传输中的训练数据、模型、梯度、测试样本、推理结果等，攻击者试图截获、篡改传输中的数据，对应数据窃取风险、数据篡改风险。

机器学习阶段分类 / 攻击目标分类	训练阶段	推理阶段	传输阶段
以数据和隐私为攻击目标	数据窃取风险 隐私泄露风险	模型反演风险	数据窃取风险 数据篡改风险
以模型为攻击目标	模型破坏风险	模型逆向风险	数据窃取风险 数据篡改风险
以推理结果为攻击目标		对抗攻击风险	数据窃取风险 数据篡改风险

表 5-1: 在 6G 中的 AI 安全风险分析

在 6G 中研究 AI 安全，需要考虑 6G 系统本身的能力与需求。 比如，如何利用移动蜂窝系统的用户认证授权机制削减恶意用户风险，在无线空口和上层接口中，如何融合移动蜂窝系统的传输安全机制，应对数据窃取、篡改和隐私泄露风险，是否可以高效的引入新的技术，如隐私计算和同态加密等保护机制，在分布式计算的基础上引入联邦学习等，都是 6G 需要研究的 AI 安全议题。

5.3.2 智能的安全策略

6G 将是智能原生架构，AI 无处不在的为 6G 提供网络能力的增强，包括安全能力的增强，即 AI for Security。

面向 6G 多元的业务、多源的数据，安全策略必须是智能的、灵活的、动态的。 6G 引入新业务并非一蹴而就，差异化的安全需求和多样化的安全能力将长期共存，如零功耗设备和 NB-IoT 设备将长期共存，分布式的信任模式和分布式的认证机制并不能取代中心化的安全机制，轻量级传输安全是在零功耗场景中的一种补充安全机制。

基于零信任的智能安全架构采用了智能的安全策略编排，能够高效的应对差异化的业务安全需求，为不同的子系统提供恰当的安全能力。 具体机制请参考本文 4.2 章节 基于零信任构建智能安全。

后量子安全

5.4

6G 时代的量子传输将日趋成熟，量子计算能力将远远超越现有计算技术，对抗量子计算的密码学研究也将会发展成为一个重要的研究领域，这个领域称为后量子安全，包括对抗量子的密钥生成和密钥分配机制的研究，对抗量子的安全算法（包括加密算法，哈希算法）的研究，对抗量子的安全协议的研究。

5.4.1 量子计算所带来的安全威胁

量子计算的发展将会为 6G 时代中需要大量计算能力的业务开启了新的篇章。 然而，量子计算的发展也给一些行业带来了严重的安全挑战。

当前，业界常用的加密算法大多都是基于整数因式分解和离散对数等高复杂度数学设计而成，这些高复杂度数学计算需要现有超级电脑花上数百甚至数千年才能逆向算出。 随着量子计算的普及和广泛采用，基于量子计算的超级电脑可以做到传统计算机无法在短期内做到的大量计算，现有的加密安全技术面临着前所未有的威胁。 尤其对基于非对称密钥的安全机制，有可能在数天甚至数小时的时间内被攻破。

一旦被量子计算攻破，不仅现有通信信道中的加密信息将会很容易地被攻击者破解，而且以往存储的加密数据也面临被量子计算解密的风险，通信的安全、数据的安全以及个人隐私的安全将受到威胁。 因此，后量子安全成为量子计算里最重要的研究方向之一。

5.4.2 后量子安全技术研究

后量子安全的技术研究主要分为以下几个方面：

后量子密钥生成和分配机制

传统密钥生成和分配是根据通信双方预配的密钥或安全凭证，经过双向认证后获取共享密钥，依赖数学计算。量子密钥分发（Quantum Key Distribution，QKD）则不依赖数学计算，而是利用了光链路发送量子的原理，将密钥从通信一方发送给另外一方，因此任何对密钥传输过程的观测和干扰都将导致密钥不一致，因此通信双方能检测到对密钥的窃取或干扰，从而保证密钥传输的安全性。

后量子的安全算法

一些能够提供一次性的或者有时间限制签名的哈希算法都具有抗量子的功能，根据格密码学，编码密码学和多变量密码学研发出来的加密算法都有着抗量子的功能。

后量子的安全协议

不安全的算法协商，密码长度协商，初始化向量协商等都有可能给安全的加密算法带来潜在的风险和安全漏洞。 安全协议的考虑要从简化做起，默认的配置（如最优选的算法和密钥长度）可以在减少不必要的协商过程，同时提升安全性能。

后量子密钥长度的增强

移动蜂窝系统里既有使用非对称密钥的场景，也有使用对称密钥的场景，对称密钥相对来说使用的更多，例如用户认证和密钥架构的根密钥是对称密钥。 相比非对称密钥加密算法，量子计算对于基于对称密钥算法的影响较小，但后量子计算的发展不容小觑。 为了确保后量子密钥的长期安全性，3GPP 当前已经在研究将对称密钥的长度从 128 位扩展到 256 位 [16]。

结语

随着 6G 新业务、新终端、新连接、新架构的发展与丰富，6G 安全技术与架构也会随之改变，本文讨论了区块链、物理层安全、AI 安全、后量子安全等技术，并引入 6G 智能安全架构，根据安全需求、子系统及安全能力，编排相应的安全策略，并能动态的根据安全规则、安全态势调整安全策略。更重要的是，对于 6G 运营商、厂商、业务商等 6G 系统参与方，不仅能应对当前业务的动态变化，还能够灵活的引入新的安全能力，适应新的安全需求，为新业务子系统编排安全策略、配置安全能力，满足后向兼容的发展需要。

参考文献

[1]. https://www.3gpp.org/news-events/3gpp-news/sec-5g .

[2]. 3GPP TS 33.501 Security architecture and procedures for 5G System.

[3]. OPPO 白皮书 :《零功耗通信》.

[4]. OPPO 6G 白皮书 :《6G： 极简多能，构建移动的世界》.

[5]. ITU Framework and overall objectives of the future development of IMT for 2030 and beyond.

[6]. OPPO 白皮书 :《6G AI-Cube 智能网络》.

[7]. 3GPP TR 22.840 3rd Study on Ambient power-enabled Internet of Things.

[8]. 3GPP TS 22.369 Service requirements for ambient power-enabled IoT.

[9]. IMT 2030 6G 推进组： 《6G 总体愿景与潜在关键技术》.

[10]. 3GPP TR 22.837 Study on Integrated Sensing and Communication.

[11]. IMT 2030 6G 推进组： 《6G 典型场景和关键能力》.

[12].https://www.gsma.com/services/blog/blockchain-technology-and-streamline-roaming-processes/.

[13]. NIST SP 800-207“Zero Trust Architecture”.

[14]. 中国信息通信研究院： 《零信任发展研究报告》.

[15]. Wyner A D. The wire‐tap channel[J]. Bell system technical journal, 1975, 54 (8): 1355-1387.

[16]. SP-231788 SID NEW New Study on enabling a cryptographic algorithm transition to 256-bits.

oppo