

6G 安全架构： 构建基于零信任的 智能安全

OPPO 6G 安全白皮书



6G SECURITY

目录

01

前言

4

02

5G 安全小结

- 2.1 5G 安全双向信任模型 6
- 2.2 5G 安全架构 7
- 2.3 5G 传输安全机制 8

03

6G 时代的发展趋势 及安全需求

- 3.1 新业务的安全需求 12
- 3.2 新终端的安全需求 13
- 3.3 新连接的安全需求 15
- 3.4 新架构的安全需求 17

04

基于零信任的 6G 智能安全架构

- 4.1 零信任背景 19
- 4.2 基于零信任构建智能安全 20

05

6G 时代关键安全技术

5.1	区块链与 6G 安全	24
5.1.1	基于区块链的多方信任	24
5.1.2	区块链支持分布式身份管理与数据授权	27
5.1.3	区块链支持高可靠的频谱共享	29
5.2	物理层安全与 6G 安全	31
5.2.1	无线环境与空口技术	32
5.2.2	6G 典型场景下物理层安全功能	32
5.3	6G 时代的 AI 安全	34
5.3.1	安全的在 6G 中使用 AI 技术	34
5.3.2	智能的安全策略	35
5.4	后量子安全	36
5.4.1	量子计算所带来的安全威胁	36
5.4.2	后量子安全技术研究	36

06

结语

37

参考文献

38



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

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/08802501100006046>