未来网络信息体系密码技术研究

刘笑凯，王文东，杨鹏飞，杨江帅，孟祥斌
（华北计算机系统工程研究所，北京 100083）

摘　要： 网络空间战略意义日益突出，人工智能、边缘计算、动态重构等技术广泛应用于网络空间，未来网络信息体系在引入新兴技术的同时也面临新型威胁和攻击风险。围绕未来网络信息体系多域融合、泛在感知、智慧化、服务定制和内生安全的特点，进行安全保密需求分析和安全威胁与风险分析，设计了一种包括密码软硬件平台技术、密码算法和协议、密码应用和安全目标，层次化的且面向未来网络信息体系的密码体系结构。

关键词： 未来网络信息体系；密码技术；安全保密需求；安全威胁；安全风险
中图分类号： TN918；TP309　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.211582

中文引用格式： 刘笑凯，王文东，杨鹏飞，等. 未来网络信息体系密码技术研究[J].电子技术应用，2022，48(2)：65-68.
英文引用格式： Liu Xiaokai，Wang Wendong，Yang Pengfei，et al. Research on cryptographic technology of future network information system[J]. Application of Electronic Technique，2022，48(2)：65-68.

Research on cryptographic technology of future network information system

Liu Xiaokai，Wang Wendong，Yang Pengfei，Yang Jiangshuai，Meng Xiangbin
（National Computer System Engineering Research Institute of China，Beijing 100083，China）

Abstract： This article focuses on network information cryptography technology.The strategic significance of cyberspace has become increasingly prominent. Technologies such as artificial intelligence，edge computing，and dynamic reconfiguration are widely used in cyberspace. In the future，network information systems will also face new threats and attack risks while introducing emerging technologies. This paper focuses on the characteristics of future network information system multi-domain integration，ubiquitous perception，intelligence，service customization and endogenous security，conducts security and confidentiality demand analysis and security threat and risk analysis，and designs a technology including cryptographic software and hardware platform technology，cryptography algorithms and protocols，cryptographic applications and security goals，hierarchical cryptographic architecture oriented to the future network information system.

Key words： future network information system；cryptographic technology；security requirements；security threats；security risks

0 引言

随着前沿技术的发展和推动，网络空间与物理空间、人类社会的融合发展日新月异，未来网络信息体系发展应不断满足网络空间对于融合、智能、安全的需求[1]。人工智能、边缘计算、动态重构等技术广泛应用于网络空间，未来网络信息体系应具备多域融合、泛在感知、智慧化、服务定制、内生安全等特点。为了支撑未来网络信息体系诸多新特性带来的功能和性能需求，以及面临网络空间安全威胁日益严峻的挑战，本文围绕未来网信体系的特点与面临安全威胁的特点，对安全保密需求深入分析，进行密码防护技术体系架构设计。

1 未来网络信息体系的特点

1.1 多域融合

未来网络信息体系将实现不同领域的异构融合。在空间层面，随着卫星互联网技术、水下通信技术、移动通信技术的不断发展，陆海空天一体化融合程度将不断提高，全球泛在接入、全网无缝连接将成为可能。在信息和现实层面，物理域、信息域、认知域、社会域融合将更加紧密，跨异构域的互联互通不断完善。

1.2 泛在感知

未来网络信息体系能够实现对泛在接入元素的环境感知、内容感知、需求感知，并提供泛在服务。环境感知包括元素的物理空间环境信息、网络地址、身份标识等信息；内容感知包括元素自身以及元素的流量、行为等信息域数据；需求感知包括元素的需求倾向和行为预判。基于以上泛在感知，可实现元素的泛在服务。

1.3 智慧化

未来网络信息体系各层面具有智慧化的特点，智慧化是智能化的高级阶段，智慧能够根据外界输入和自身演进生成智能。通过智慧化，网络信息体系的功能和性能能够按需进行动态演进，能够根据泛在感知的情况提供智能服务，同时可以根据感知情况进行智能运维管

理，持续进行状态调整、问题改进。

1.4 服务定制

未来网络信息体系具有软件定义、按需服务、动态重构等服务定制特点。服务定制是实现智慧服务的基础和路径，软件定义和动态重构技术能够实现保持硬件平台不变的情况下，满足对于不同功能和性能服务需求变化的支撑，可以解决传统网络空间设备一旦上线部署无法升级演进的问题，从而提供按需服务。

1.5 内生安全

未来网络信息体系具有先天免疫、自主安全等内生安全特点。多域融合和泛在感知带来了新的威胁风险，同时，传统打补丁式的安全防护也无法满足未来网络信息体系的安全需求。因此，未来网络信息体系需要具有先天免疫的特点，从源头上保证内生式安全，通过自主安全手段进一步保障安全。

2 安全威胁与风险分析

未来网络信息体系具有重大的战略价值和现实意义，随着信息技术的不断发展，新型网络空间攻击威胁手段层出不穷，未来网络信息体系面临的安全威胁攻击将呈现国家级、智能化、武器化等特点。此外，量子计算等技术的发展也对未来网络信息体系的安全保密防护手段提出了新的挑战。

2.1 量子计算攻击

量子计算领域的创新突破和量子计算机超强的计算能力将为未来网络信息体系安全带来全新的挑战，也将威胁当前广泛应用的经典加密算法[2]。量子计算能够对基于大数分解难题和离散对数难题的密码算法进行破解，同时，能够降低分组、序列和杂凑算法的算法安全性、工作模式安全性。

2.2 国家级攻击

国家网络空间安全作为各国战略博弈的全新领域，其面临的安全威胁攻击呈现出国家级攻击的特点。专职攻击的网络部队使用军事级的技术，掌握着大量未曾披露的系统漏洞与后门，网络武器具备侦察、渗透、情报、指挥、打击等多种能力，攻击方式朝着精确化、智能化的方向发展，网络武器逐渐实现型谱齐全、全域覆盖。

2.3 高级可持续威胁攻击

未来网络信息体系将面临高级可持续威胁攻击[3]。该攻击利用非常规攻击手段对具有重要价值资产或重要战略意义的特定对象展开持续有效的攻击，攻击具有较强的针对性，能够根据特定对象的特点，通过复杂多样的攻击技术，进行长时间的持续性攻击；且攻击具有较强的隐蔽性和无孔不入的渗透性。

2.4 隔离网络攻击

未来网络信息体系同样面临隔离网络攻击，物理隔离[4]手段无法完全解决信息系统遭受威胁攻击的问题。隔离网络攻击能够突破物理隔离的界限，可通过光盘、U 盘等 IO 设备进行摆渡攻击，可通过芯片、固件升级进行植入攻击，也可通过社会工程方式对没有及时封堵潜在漏洞和缺陷进行攻击。

2.5 未知威胁攻击

网络空间攻击和防护的不对称性使未来网络信息体系面临大量未知威胁攻击[5]。靠安全设备堆叠的传统方式无法有效应对复杂未知的网络安全威胁。规则和特征匹配等基于机器学习的攻击检测技术需要大量的先验样本训练和实时数据分析才能识别已知威胁攻击，但无法满足应对未知威胁攻击的检测需求。

3 安全保密需求分析

安全保密是未来网络信息体系的重要组成部分，为了支撑未来网络信息体系诸多新特性带来的功能和性能需求，以及网络空间安全威胁日益严峻的挑战，未来网络信息体系安全保密具有一体化安全防护需求、内生式安全可信需求、智能化密码防御需求、后量子时代支撑需求、密态功能计算需求、全网统一信任需求、高速多模保密需求、陆海空天一体化密码管理需求等。

3.1 一体化安全防护需求

现有安全保密机制通常是在网络信息体系建立之后，采用打补丁的形式应对已知的安全威胁，是一种静态的、被动的、滞后的安全防护方式。未来网络信息体系应与安全保密体系一体化设计、同步设计，将安全保密机制与网络信息体系进行深度融合，实现网络空间安全到安全网络空间的转变。

3.2 内生式安全可信需求

未来网络信息体系应具有与生俱来的安全免疫能力，其中安全保密机制能够提供机密性、完整性、不可否认性等功能，但作为安全保密机制运行的软硬件底层环境的可信可控是决定安全保密机制发挥预定功能的保障，未来网络信息体系通过动态的、智能的可信度量，实现内生安全[6]。

3.3 智能化密码防御需求

未来网络信息体系软件定义、动态变化的特点需要智能化的密码防御机制，基于安全态势感知，通过人工智能分析决策制定密码防御策略，满足不同功能和性能的指标需求。应对已知和未知的安全威胁进行密码防御效能评价，智能动态地调整密码防御策略，不断优化演进密码防御能力。

3.4 后量子时代支撑需求

随着量子计算技术和量子密码技术的发展和应用，未来网络信息体系具有后量子时代支撑需求，各类密码算法、算法工作模式和密码协议需要具备抗量子计算攻击能力，也需要具备量子密钥管理能力，并融合传统密钥管理体系，实现未来网络信息体系在后量子时代密码机制的有效性[7]。

3.5 密态功能计算需求

未来网络信息体系广泛使用大数据、云计算等技术。数据加密能够保障数据安全和用户隐私，密态数据需要

具有搜索、统计、分析等功能计算能力，以支撑数据可用性[8]。跨异构网系、跨安全域的数据交换需要密态路由、密态数据重加密、密态态势感知等功能计算能力，实现密态条件下的互通和防御。

3.6 全网统一信任需求

未来网络信息体系具有异构融合、广域互联的特点，需要具备对用户进行全网统一访问控制的能力，为用户提供全网统一的身份标识和认证管理体系，实现用户的泛在接入安全；需要具备对软硬件进行全网统一信任管理的能力，为硬件设备和软件应用提供全网统一的身份标识和信任管理体系[9]。

3.7 高速多模保密需求

未来网络信息体系需要密码技术能够支撑更高速的骨干通信、更广泛的网络接入和更复杂的网络管理等需求[10]。密码防护设备能够通过软件定义的方式，自适应地支撑不同速率、多种模式的密码业务，密码处理单元与网络处理单元解耦合，具备速率线性增长、统一管理部署、高可靠性的能力。

3.8 陆海空天一体化密码管理需求

未来网络信息体系覆盖陆海空天等空间，为保障加密防护的有效性、访问控制的时效性和安全链路建立的高效性，需要覆盖广、高效灵活和多通信途经的密码管理保障能力，融合传统陆基密码管理、基于卫星互联网的天基密码管理以及基于舰载和水声通信网的海基密码管理[11]。

4 面向未来网络信息体系的密码体系结构

面向未来网络信息体系的密码体系结构，围绕未来网络信息体系特点、面临安全威胁的特点，对安全保密需求进行深入分析，进行密码防护的一体化设计，包括密码软硬件平台技术、密码算法和协议、密码应用和安全目标四部分，如图 1 所示。

4.1 密码软硬件平台技术

以自主安全的芯片、模块、板卡、整机、系统和软件技术体系为基础[12]，从软硬件平台底层实现内生安全；可重构芯片技术实现密码算法和协议的动态可重构加载，增强密码模块的功能的可用性和业务的适应性；平台加模块架构分离通信业务处理和密码计算处理，支撑设备的可扩展性和性能的线性增长；智能感知决策技术能够感知平台的业务、威胁、管理等态势，智能分析决策，按需调整业务功能和性能；软件柔性配置技术通过软件定义的方式增强平台的动态性和灵活性。

4.2 密码算法和协议

公钥算法、分组算法[13]（及工作模式）、序列算法、杂凑算法、各种密码协议具有加解密速率高、资源占用率小、时延低、轻量级等特点，以适应不同的场景需求；具有可密态计算的功能，实现隐私保护下的数据计算、搜

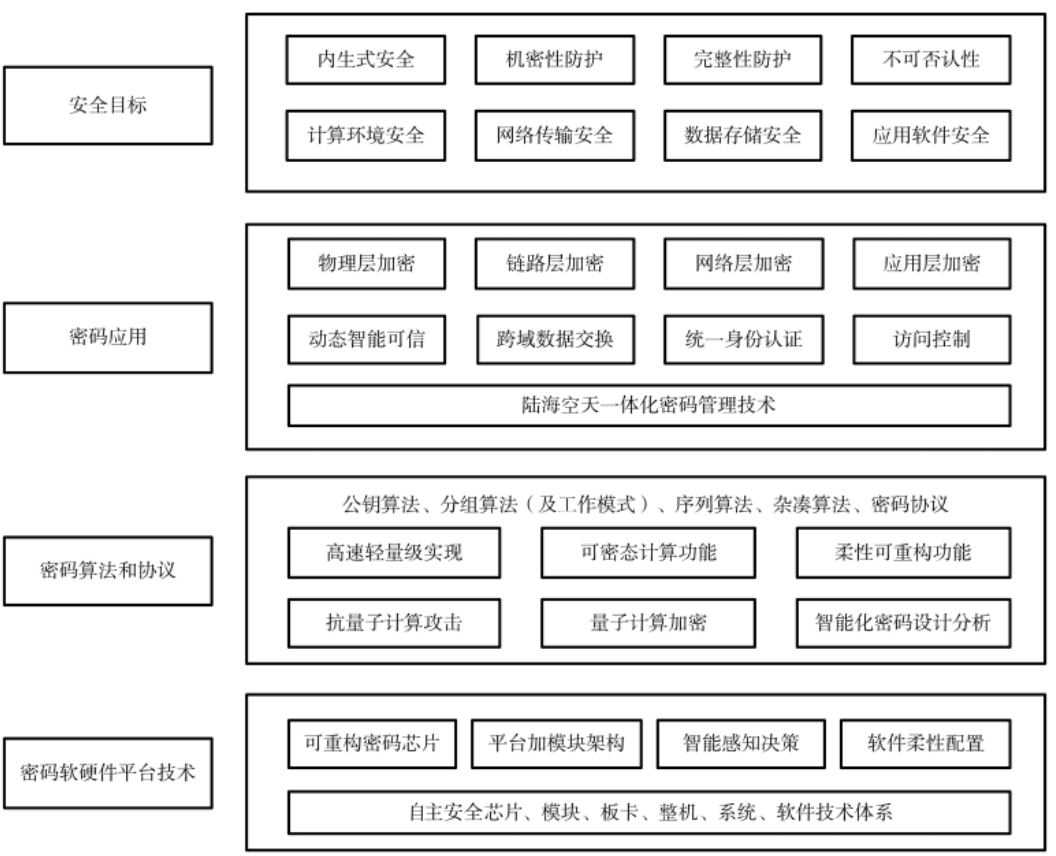

图 1 面向未来网络信息体系的密码体系结构

索等功能；密码算法具有柔性可重构能力[14]，在性能、带宽等方面按需重构；具有基于人工智能的密码算法设计、算法关键环节模块设计，以及密码算法的分析破译功能；具备抗量子计算攻击的能力、基于量子计算的加密能力，以及量子计算下的传统算法实现能力。

4.3 密码应用

基于软硬件平台、密码算法和协议构建密码应用。物理层加密[11]包括信号隐藏、波形频率密码调制等技术，链路层加密包括对 SDH、OTN 等的密码防护，网络层加密主要是 IPSec VPN[15]等防护技术，应用层加密包括信源加密、SSL VPN 等防护技术。具备动态智能可信度量能力，实现对设备进行实时、动态、可重构的信任度量；支撑跨异构网、安全域的数据交换安全防护；具有全网统一身份标识，支撑统一身份认证，以及细粒度的访问控制；具备陆海空天一体化密码管理能力，实现密码全时、全域的高效动态支撑保障。

4.4 安全目标

基于密码软硬件平台、密码算法和协议、密码应用，实现系列安全目标，从底层软硬件平台和可信计算实现内生式安全，保障密码机制和运行环境的正确性和可用性；实现机密性防护、完整性防护和不可否认性；实现主机服务器等计算环境安全，包括可信启动、授权访问等密码防护；实现网络各层面的传输安全；实现数据的存储、更新、删除、访问等全生命周期的密码防护；实现应用软件可信分发、应用服务的密码防护。

5 结论

本文围绕未来网络信息体系多域融合、泛在感知、智慧化、服务定制、内生安全等特点，分析了未来网络信息体系面临的量子计算攻击、国家级攻击、高级可持续威胁攻击、隔离网络攻击和未知威胁攻击等威胁风险，论述了未来网络信息体系的安全保密需求，并提出了一种多层次、多维度的密码技术体系结构，为解决未来网信体系安全保密问题，发挥网络空间效能提供了支撑。

参考文献

[1] ZHANG J，HUANG T，WANG S，et al.Future Internet：trends and challenges[J]. Frontiers of Information Technology & Electronic Engineering，2019，20(9)：1185-1194.

[2] 刘文瑞.抗量子计算攻击密码体制发展分析[J].通信技术，2017，50(5)：1054-1059.

[3] HAQ T，ZHAI J，PIDATHALA V K. Advanced persistent threat(APT) detection center：US20150096024[P].2015-04-02.

[4] 禹晓庆.网络物理隔离安全防御技术[J].中国电子与网络出版，2000(6)：59.

[5] AHMADINEJAD S H，JALILI S，ABADI M.A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J].Computer Networks，2011，55(9)：2221-2240.

[6] Yu Fajiang，Tang Xianglei，Yu Yue，et al.Trusted computing dynamic attestation by using static analysis based behavior model[C]//2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops，2011.

[7] MOSCA M.Cybersecurity in an era with quantum computers：will we be ready?[J].IEEE Security & Privacy，2018，16(5)：38-41.

[8] DAN B，SAHAI A，WATERS B.Functional encryption：definitions and challenges[C]//TCC2011：Theory of Crypto graphy，2011：253-273.

[9] ZHANG F，JIANG W，SHI B.TAC：a unified trust anchor framework based on consortium blockchain[J].Journal of Physics：Conference Series，2020，1544(1)：012181.

[10] 李凤华，殷丽华，吴巍，等.天地一体化信息网络安全保障技术研究进展及发展趋势[J].通信学报，2016，37(11)：156-168.

[11] LI W，MCLERNON D，WONG K K，et al.Asymmetric physical layer encryption for wireless communications[J].IEEE Access，2019，7：46959-46967.

[12] 石锴.对硬件软件密码技术的对比研究[J].华人时刊(中旬刊)，2013(2)：100，102.

[13] 张晓丰，樊启华，程红斌.密码算法研究[J].计算机技术与发展，2006，16(2)：179-180，184.

[14] 王莉.密码算法的可重构系统实现研究[D].南京：南京航空航天大学，2007.

[15] DAVIS C R.IPSec：VPN 的安全实施[M]. 周永彬，冯登国，徐震，等，译.北京：清华大学出版社，2002.

(收稿日期：2021-03-31)

作者简介：

刘笑凯(1977-)，男，硕士，高级工程师，主要研究方向：信息安全、密码学。

王文东(1979-)，女，本科，工程师，主要研究方向：信息安全。

孟祥斌(1995-)，通信作者，男，硕士，主要研究方向：信息安全、密码学，E-mail：xiangbinmeng@foxmail.com。

扫码下载电子文档

版权声明