

数学在网络空间安全中的应用与探索研究

——评《网络空间安全数学基础》

网络空间已成为人们生活、工作不可或缺的一部分,然而,随着网络技术的飞速发展,网络安全问题也日益凸显,数据泄露、黑客攻击等事件频频发生。在这一背景下,数学作为一门严谨而精确的学科,其在网络空间安全领域的应用显得尤为重要。数学加密算法、数据分析等技术手段,可更有效地保护网络数据安全,预防和抵御各种网络攻击。

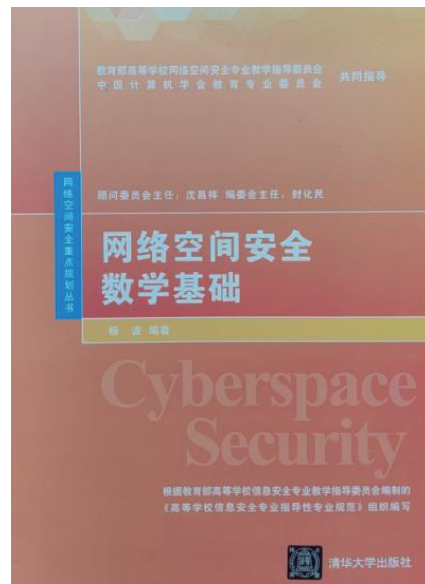
笔者在落实兰州市科技计划项目(2023-ZD-243)的过程中,认真学习了《网络空间安全数学基础》一书,该书全面而深入地探讨了网络空间安全领域所必需的数学知识,全书共分为3大部分。第1部分聚焦数论,详细阐述了整除、数论函数、同余及同余方程等核心概念;第2部分引导读者进入代数系统的世界,涵盖了代数系统和群、环和域以及有限域的重要理论;第3部分则着重于网络空间安全的实用算法,如素性检验、整数分解和离散对数等,该书不仅为网络空间安全和信息安全领域研究者提供了坚实的数学基础,还通过深入浅出的方式将抽象的数学理论与网络安全的实际应用相结合。

编者指出,网络技术更新换代速度快,网络空间安全问题日趋严峻,为了保障网络通信和数据存储的安全性,加强数学加密算法的研究与应用成为一项重要任务。数学加密算法是网络空间安全的核心技术之一,通过加密数据,可以保护数据的机密性和完整性,防止数据被非法获取或篡改。目前,常用的数学加密算法包括对称加密算法、非对称加密算法和哈希算法等,这些算法都基于复杂的数学问题,如大数分解、离散对数等,确保了加密的强度和安全性。为了加强数学加密算法的研究与应用,政府和信息安全企业应加大扶持力度,支持数学家和密码学家对数学加密算法进行深入研究,通过不断探索新的数学理论和方法,设计出更安全、更高效的加密算法,提高网络通信和数据存储的安全性。为推动数学加密算法在实际中的应用,政府、企业和个人都应该重视数据加密的重要性,积极采用先进的加密算法保护自己的数据安全,且相关机构还应加强对加密算法的评估和审核,通过分享经验、交流技术,确保其安全性和可靠性,共同应对网络空间安全挑战,推动数学加密算法的不断进步和创新。

笔者认为,网络空间安全风险评估和预防是确保网络安全的重要环节,利用数学模型科学评估网络安全风险,及时发现潜在的安全隐患,并采取相应的预防措施,可降低网络安全事件的发生概率。信息安全企业可以利用数学模型评估网络系统的脆弱性,通过收集网络系统的相关数据,建立相应的数学模型,定量分析网络系统的各个组成部分,确定可能存在的安全漏洞和风险点,如此可以有针对性地加强安全防护措施,提高网络系统的整体安全性。数学模型还可用于预测网络安全事件的发展趋势,通过分析历史网络安全事件的数据,建立相应的预测模型,预测和预警未来可能发生的安全事件,提醒安全机构提前采取相应的应对措施,避免或减少安全事件带来的损失。为了利用数学模型提升网络安全风险评估与预防能力,要加强数据采集和分析能力。数学模型的有效性和准确性取决于数据的质量和数量,因此,需要建立完善的数据采集和分析体系,确保数据的真实性和完整性,为数学模型的建立提供有力支持。此外,政府、企业和研究机构应该加大信息安全技术人才的培养和引进力度,推动行业技术交流与合作,共同推动数学模型在网络安全领域的发展与应用。

总之,在数字化时代,网络空间安全至关重要,而数学作为解决网络安全问题的关键工具,其重要性不言而喻。深入研究和应用数学加密算法、数学模型等技术手段,能够更有效地评估和预防网络安全风险,确保网络通信和数据存储的安全性。面对不断变化的网络环境,需要不断创新和完善数学方法,加强国际合作与交流,共同应对网络空间安全的挑战。

(孙玲/兰州资源环境职业技术大学基础教学部/副教授)



书名:网络空间安全数学基础

编者:杨波

出版社:清华大学出版社

ISBN:9787302548171

出版时间:2020年5月

定价:35元