金海 —— 主编
徐鹏 邹德清 —— 副主编

中国网络空间安全前沿科技发展报告 2018

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

金海 —— 主编
徐鹏 邹德清 —— 副主编

中国网络空间安全前沿科技发展报告 2018

人民邮电出版社
北京

图书在版编目（CIP）数据

中国网络空间安全前沿科技发展报告. 2018 / 金海主编. — 北京 : 人民邮电出版社, 2019.2
ISBN 978-7-115-50304-6

Ⅰ. ①中… Ⅱ. ①金… Ⅲ. ①计算机网络－安全技术－研究报告－中国－2018 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第274809号

内 容 提 要

本书依据各位杰出青年学者的专长，介绍了近几年来网络空间安全领域的研究热点、国内外研究现状和未来亟需开展的研究建议。内容涉及密码学基础理论、多功能密码算法、后量子密码、网络安全、物联网系统安全、物联网传输与终端安全、云计算安全、大数据隐私保护、区块链、人工智能安全。

本书适合于所有从事网络安间安全领域的科研人员学习和研究。

◆ 主　　编　金　海
副 主 编　徐　鹏　邹德清
责任编辑　邢建春
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：14　　2019 年 2 月第 1 版
字数：341 千字　　2019 年 2 月北京第 1 次印刷

定价：168.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

本书编委会

主　编　金　海

副主编　徐　鹏　邹德清

委　员（按姓氏拼音排序）

陈　洁　陈　晶　陈　恺　陈荣茂　陈　玺　陈晓峰　陈宇飞

程　鹏　段海新　高　飞　葛春鹏　巩俊卿　韩劲松　韩伟力

何道敬　何德彪　胡红钢　胡　志　黄　琼　黄欣沂　纪守领

冀晓宇　赖俊祚　李　进　李　琦　李　珍　林璟锵　刘　烃

刘　哲　罗向阳　屈龙江　任　奎　沈　超　沈　剑　孙　兵

汪　定　汪京培　王　聪　王　磊　温金明　翁　健　肖　亮

徐文渊　许封元　杨　珉　禹　勇　郁　昱　张　超　张　甲

张　江　张　磊　张明武　赵运磊　郑佳佳　周亚金　朱浩瑾

诸葛建伟

推荐序

网络空间安全是国家安全的重要组成部分，人才是网络空间安全学科发展的重要基础。为加强网络空间安全学科建设、加快网络空间安全人才培养、促进网络空间安全科学技术发展，华中科技大学、武汉市网信办、国家网络安全人才与创新基地和武汉网络安全战略与发展研究院共同创办了“网络空间安全喻园青年科学家论坛”。该论坛已经连续举办两届，共邀请来自国内知名高校的83位杰出青年学者参与论坛并做特邀报告。论坛具有受邀嘉宾年轻化、演讲主题前沿化、研讨内容专业化、研究方向多样化、交流讨论对等化等鲜明特色，为广大青年学者提供一个有利于把握学科建设需求、有利于展示科学研究成果、有利于探讨学术发展方向、有利于多安全方向交叉的互动平台。

《中国网络空间安全前沿科技发展报告》作为“网络空间安全喻园青年科学家论坛”的成果与总结，由来自全国27所高校（科学院）的59位杰出青年学者联合倾力编写完成，内容丰富，涵盖了可信计算、密码学、网络安全、物联网安全、云计算与云数据安全、大数据安全、区块链和人工智能等领域的前沿科技。报告中的每篇文章都凝聚了一位或多位优秀科研工作者近年来的科研心得，提纲挈领地阐述了相关领域内的当前研究背景、简明扼要地分析了相关技术在国内外的研究现状，深入浅出地介绍了学者在各自领域的研究成果。每篇文章的最后还启发式地给出了各位优秀学者对各自领域的研究展望与宝贵建议，这为网络空间安全领域的广大学者或学子们提供了很好的借鉴价值。同时，该报告对于各级国家与地方主管部门参考制定网络空间安全发展战略、明确网络空间安全领域的人才培养方向也具有重要参考价值。

报告内涵丰富，既有科普性，也具启发性。阅读本报告，可以了解目前网络空间安全领域面临的各种科学问题与挑战以及众多前沿科技的国内外研究现状、发展特色。

中国工程院院士 沈昌祥

2018年11月20日于北京

前 言

为促进网络空间安全科学技术发展、服务网络空间安全学科建设，华中科技大学、武汉市网信办、国家网络安全人才与创新基地、武汉网络安全战略与发展研究院以主办“网络空间安全喻园青年科学家论坛”为契机，联合全国 27 所高校和科学院的 59 位杰出青年学者，围绕网络空间安全科学技术前沿领域，共同撰写《中国网络空间安全前沿科技发展报告》（以下简称“发展报告”）。发展报告分别从密码学、网络安全、物联网安全、云计算与云数据安全、大数据安全、区块链、人工智能安全 7 个方面，依据各位杰出青年学者的专长，分别介绍近几年来网络空间安全领域的研究热点、国内外研究现状和未来亟需开展的研究建议。

在密码学方面，发展报告以伪随机函数、对称密码、数字签名、功能加密、全同态加密和后量子密码等为核心内容。中国科学技术大学胡红钢教授介绍了抗量子攻击与可验证的伪随机函数构造。上海交通大学王磊研究员、国防科技大学屈龙江教授和孙兵博士等主要介绍了对称加密的可证明安全性、低差分函数与密码分析。福建师范大学黄欣沂教授介绍了可修订的数字签名。华东师范大学陈洁研究员介绍了功能加密。暨南大学赖俊祚研究员介绍了全同态加密。暨南大学翁健教授、复旦大学赵运磊教授、密码科学技术国家重点实验室张江博士和南京航空航天大学刘哲教授等介绍了基于格的抗量子攻击密码，具体包括格规约、格密码及其快速实现等。北京邮电大学高飞教授介绍了量子计算密码分析。

在恶意系统或算法下的安全防护方面，发展报告以旁路攻击、程序混淆、抗颠覆攻击、密钥安全和口令猜测等为核心内容。上海交通大学郁昱研究员介绍了抗泄露与抗篡改密码。湖北工业大学张明武教授介绍了白盒密码安全级的程序混淆。国防科技大学陈荣茂博士介绍了抗颠覆攻击的密码算法构造。中国科学院信息工程研究所林璟锵研究员介绍了可抵御内存数据物理攻击的密钥安全机制和可抵御系统软件零日漏洞的密钥安全机制。北京大学汪定博士介绍了口令中异构个人身份信息的感知、用户口令修改行为的上下文环境感知和小训练样本下的口令定向猜测模型构建。

在网络安全方面，发展报告以网络与系统攻防、频谱安全、软件定义网络安全、网络空间测绘和无线网络安全等为核心内容。清华大学段海新教授等介绍了互联网基础协议不一致问题、自动化攻防场景下的动态决策问题和适用于物联网的标准化安全体系。上海交通大学朱浩瑾教授介绍了认知无线电的阻塞攻击及其防御和频谱分配过程中的用户隐私保护。清华大学李琦副研究员介绍了软件定义网络中网络流量劫持攻击与策略篡改攻击的检测和防御。战略支援部队信息工程大学罗向阳研究员介绍了网络空间资源的探测、地理位置定位及其与社会空间的精准关联。厦门大学肖亮教授介绍了无线网络场景下强化学习技术的高维度危机和基于强化学习的无线网络安全机制的“状态和效用难观察”问题。

在物联网系统安全方面，发展报告以模拟态安全、工控内生安全、软件系统安全、星载电子系统安全和信息物理系统安全等为核心内容。浙江大学徐文渊教授等介绍了物联网模拟态安全机理模型、基于模拟态信息的设备异常检测技术和基于模拟态信息的硬件设备认证技术。浙江大学程鹏教授等介绍了内生安全的工控系统可信防护架构、未知威胁下的工控系统可信协同防护技术研究和基于行为的工控系统可信评估与网络审计。浙江大学周亚金研究员介绍了高交互性的物联网蜜罐系统设计、物联网设备软件未知威胁发现和物联网恶意软件分析。华东师范大学何道敬教授等介绍了高效可用的卫星综合电子系统仿真平台建设及其攻击场景构建、自学习轻量级入侵检测与快速响应方法。西安交通大学刘烃副教授介绍了信息物理融合系统行为模式的异构性、多样性与时空隐蔽性。

在物联网可信认证、保密传输与终端安全方面，发展报告以一体化认证、行为特征识别、安全传输和智能终端安全漏洞等为核心内容。浙江大学韩劲松教授介绍了抗伪造与重放的设备指纹提取与认证、基于活体生物特征的用户认证和计算与通信过程中持续性认证。西安交通大学沈超副教授等介绍了智能终端中人机行为的表示与描述、特征提取与表达、学习与主动认证。华东师范大学张磊研究员介绍了车联网中的高并发签名验证与大规模数据中长距离多条传输。复旦大学杨珉教授介绍了复杂多层次系统架构下的安全漏洞发现机制和程序深层逻辑中的安全漏洞发现机制。复旦大学韩伟力教授介绍了移动终端中的持续感知能力和混合感知数据的安全管控、自动安全策略管理和感知安全管控的优化。

在云计算与云数据安全方面，发展报告以云系统安全、云服务安全、云数据安全等为核心内容。华中科技大学金海教授等介绍了云平台的安全可信基构建、信任传递与可信度量，多层次云服务的安全共享和云数据的安全可控。西安电子科技大学陈晓峰教授介绍了海量密文的可验证多模式检索方法和随机数据流的公开可验证计算机制。陕西师范大学禹勇教授介绍了外包数据完整性保障、云数据审计协议和外包数据损失赔偿机制。南京航空航天大学刘哲教授介绍了抗量子攻击的云数据安全共享方法与用户隐私保护方法。南京信息工程大学沈剑教授等介绍了云数据的访问控制、安全审计和用户权限安全撤销。

在大数据隐私保护与区块链方面，发展报告以隐私保护、安全搜索和区块链等为核心内容。浙江大学任奎教授介绍了大数据中的多元异构敏感数据的安全采集、复杂结构数据中的隐私保护机制、计算与存储过程中的动态保护。香港城市大学王聪副教授介绍了可验证的多功能大数据安全搜索技术、支持细粒度访问控制的大数据安全搜索技术和分布式大数据安全搜索技术。华南农业大学黄琼教授介绍了面向动态数据的安全、快速与多样的加密搜索方法。武汉大学何德彪教授介绍了面向区块链隐私保护安全的模型构建、形式化分析方法、关键技术、系统化解决方案与实现。武汉大学陈晶教授介绍了基于区块链的统一身份认证与管理系统，并提出其亟需进一步解决的高效与公平的共识机制问题和安全可靠的快速响应问题。

在人工智能安全研究方面，发展报告以模型安全、系统安全、隐私与样本保护、语音识别安全、推理安全和漏洞智能检测等为核心内容。南京大学许封元教授介绍了训练数据投毒的高效防御、深度学习任务的可信云计算和在线模型窃取的防护机制。浙江大学纪守领教授介绍了机器学习训练数据的质量保障与隐私保护、对抗环境下机器学习模型的主动防御和开放场景下机器学习应用中的隐私防护与风险评估。广州大学李进教授介绍了机器学习数据的隐私保护、机器学习模型的恶意样本攻击和机器学习的安全模型定义。中国科

学院信息工程研究所陈恺研究员介绍了语音自动识别系统安全，特别是如何为该系统建立实际的对抗攻击、对抗样本是否能够被普通用户察觉或影响大量用户等问题。西安交通大学沈超副教授介绍了人工智能中的训练样本可信、学习模型防窃取防欺骗、机器学习数据的隐私保护。华中科技大学邹德清教授等介绍了软件源代码漏洞数据的有效表征、软件源代码漏洞的细粒度定位和软件源代码漏洞智能检测模型的解释与优化。

发展报告涵盖领域广、内容丰富、内涵深刻。阅读发展报告内容，将有利于了解网络空间安全前沿领域的研究现状与挑战、把握国内外在网络空间安全领域的科技差距、指导各级国家与地方主管部门制订网络空间安全发展战略、明确网络空间安全领域的人才培养方向。

未来，希望更多杰出青年学者积极参与发展报告撰写，进一步改善我国网络空间安全科学技术方面相关科技现状、深刻分析差距与亟需解决的问题，不断促进相关科学技术的研究。

目 录

伪随机函数与密码算法

伪随机函数研究

胡红钢
中国科学技术大学

一　研究背景概述

一簇有效可计算的确定性函数被称为是伪随机的，如果不存在多项式时间的攻击者，能够以不可忽视的概率区分如下两种情况：一个函数是随机地选自该簇，还是选自真随机的函数簇。伪随机函数是密码学的基础性问题。在密码学中，伪随机函数可以用于模拟随机预言机（Random Oracle）。伪随机函数也是构造密码算法和协议极端重要的基本工具。如果不存在伪随机函数，就不可能存在安全的密码算法和协议。通过有效地利用伪随机函数，我们可以构造加密、消息认证码和身份认证等方案。此外，伪随机函数在复杂度理论领域也有重要的应用。

与伪随机函数相比，可验证的伪随机函数除了提供正常的输出以外，还会提供一个非交互的证明 π。利用 π，任何人都可以验证与 π 对应的输出是否正确，这就很好地将不可预测性（Unpredictability）与可验证性（Verifiability）结合到了一起。与带密钥的 Hash 函数相比，可验证的伪随机函数可以看成公钥版本的带密钥 Hash 函数。可验证的伪随机函数与其他密码学基本构件存在着深刻的联系，如基于身份的加密方案、非交互式零知识证明协议等。目前，密码学家还在继续开展这方面的研究。可验证的伪随机函数可应用于区块链领域。在区块链中，有些分布式共识协议在选择 session leader 或者 committee member 时，既需要不可预测性，又需要可验证性（如 Algorand），可验证的伪随机函数正好满足这种需求。

二　主要科学问题

目前，该领域的主要问题是：构造可以抵抗量子计算攻击的伪随机函数，特别是可验证的伪随机函数。量子计算是计算技术的必然发展趋势。首先，这涉及计算复杂度问题：什么样的计算困难问题才能真正抵抗量子计算的攻击？（这个问题的难度非常大）其次，除了 LPN、LWE、Ring-LWE 这些受到广泛关注的问题以外，是否可以找到其他问题，不但支持高效复杂的运算，还具有可证明的难度？这涉及怎样嵌入更好的代数结构，以及怎么处理一般性的噪声模式。最后，面向分布式的网络环境，如 P2P 网络，怎样设计实用的可验证伪随机函数？现在，基于 LWE 等问题的密钥协商、加密、签名、密钥封装等结果已经很多，是否可以将这些结果或者其中的想法用于可验证伪随机函数的构造？

三　国际研究现状

1984 年，Goldreich、Goldwasser 和 Micali[1]提出了伪随机函数的概念。假设伪随机序列发生器存在的前提下，他们给出了第一个伪随机函数的树状构造方法，人们称之为 GGM 构造。1997 年，Naor 和 Reingold[2]给出了两类基于数论的有效构造方法：第一种基于 DDH 假设；第二种基于分解 Blum 整数的困难性。2000 年，Naor、Reingold 和 Rosen[3]给出了另一种基于整数分解的构造方法，效率更高。2012 年，Banerjee、Peikert 和 Rosen[4]提出了 LWR 问题，该问题的难度可以约化到 LWE 问题。基于 LWR 问题，并借鉴 GGH 构造中的技术，他们给出了基于格的伪随机函数构造方法。2013 年，Boneh、Lewi、Montgomery 等[5]给出了基于格的密钥同态伪随机函数。2014 年，Banerjee 和 Peikert[6]改进了这个结果：降低了密钥规模，并提高了效率。2015 年，Brakerski 和 Vaikuntanathan[7]进一步推广了上述两个结果，可以将电路秘密地嵌入伪随机函数中。

1999 年，Micali、Rabin 和 Vadhan[8]提出了可验证伪随机函数的概念。基于 RSA 假设的一个变形，他们构造了第一类可验证的伪随机函数。2003 年，Dodis[9]利用椭圆曲线上的双线性对给出了一种新的构造方法，但效率较低。2005 年，Dodis 和 Yampolskiy[10]改进了这个构造，其安全基础来源于双线性判定 Diffie-Hellman 逆假设（DBDHI）。2009 年，Abdalla、Catalano 和 Fiore[11]发现，基于 ID 的密钥封装机制（IB-KEM）可以用于构造可验证伪随机函数。2014 年，基于双线性判定 L-弱 Diffie-Hellman 逆假设（L-wBDHI*），他们[12]又给出了一种新的构造方法。2017 年，Goyal、Hohenberger、Koppula 等[13]利用非交互证据不可区分证明（NIWI）等技术给出了一种新的构造可验证伪随机函数的方法，并利用 LWE 问题和 LPN 问题给出了具体实例。

四　国内研究现状

在这个领域，国内的相关结果较少。2007 年，为了解决 Barak 等在 2001 年提出的关于可重置零知识证明的猜想，邓燚和林东岱教授[14]提出了依赖于实例（Instance-Dependent）的可验证伪随机函数。他们证明了如果存在陷门置换，那么存在这种特殊的可验证伪随机函数，并给出了具体的构造方法。2016 年，郁昱和 Steinberger[15]首次利用 LPN 构造了一类伪随机函数，因为它是并行的，该类函数效率较高。此外，在国内期刊上，受到 Peikert 和 Rosen 在 2012 年工作的启发，2014 年，陈和风等[16]利用短整数解问题（SIS 问题）给出了两种伪随机函数的构造方法，第一种是并行结构，第二种是串行结构。

五　未来研究建议

面向未来的量子计算时代，构造安全的可验证伪随机函数。新的计算技术会带来新的安全问题和安全需求，对随机性的要求也更加严格。该领域有两个问题具有较大的理论意义和应用价值。

（1）现有构造方法的密码分析

基于格，密码学家已经找到了一些构造方法，但这些构造方法在量子计算下的真实安全水平，还有待进一步的密码分析来衡量。这涉及底层的计算困难问题，在量子计算下的真实困难程度。

（2）抗量子攻击的可验证伪随机函数

基于格来构造可验证的伪随机函数，需要利用底层计算困难问题的更多代数结构，以便嵌入更合适的陷门，同时还要借鉴基于格的数字签名和基于身份的加密方案中的技巧。

参考文献：

[1] GOLDREICH O, GOLDWASSER S, MICALI S. How to construct Randolli functions[C]//IEEE 25th Annual Symposium on Foundations of Computer Science. 1984: 464-479.

[2] NAOR M, REINGOLD O. Number-theoretic constructions of efficient pseudo-random functions[J]. Journal of the ACM (JACM). 2004, 51(2): 231-262.

[3] NAOR M, REINGOLD O, ROSEN A. Pseudorandom functions and factoring[J]. SIAM Journal on Computing. 2002, 31(5): 1383-1404.

[4] BANERJEE A, PEIKERT C, ROSEN A. Pseudorandom functions and lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2012: 719-737.

[5] BONEH D, LEWI K, MONTGOMERY H, et al. Key homomorphic PRFs and their applications[C]//Advances in Cryptology–CRYPTO 2013. 2013: 410-428.

[6] BANERJEE A, PEIKERT C. New and improved key-homomorphic pseudorandom functions[C]// International Cryptology Conference. 2014: 353-370.

[7] BRAKERSKI Z, VAIKUNTANATHAN V. Constrained key-homomorphic PRFs from standard lattice assumptions[C]//Theory of Cryptography Conference. 2015: 1-30.

[8] MICALI S, RABIN M, VADHAN S. Verifiable random functions[C]//IEEE 40th Annual Symposium on Foundations of Computer Science. 1999: 120-130.

[9] DODIS Y. Efficient construction of (distributed) verifiable random functions[C]//International Workshop on Public Key Cryptography. 2003: 1-17.

[10] DODIS Y, YAMPOLSKIY A. A verifiable random function with short proofs and keys[C]//International Workshop on Public Key Cryptography. 2005: 416-431.

[11] ABDALLA M, CATALANO D, FIORE D. Verifiable random functions from identity-based key encapsulation[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2009: 554-571.

[12] ABDALLA M, CATALANO D, FIORE D. Verifiable random functions: relations to identity-based key encapsulation and new constructions[J]. Journal of Cryptology, 2014, 27(3): 544-593.

[13] GOYAL R, HOHENBERGER S, KOPPULA V, et al. A generic approach to constructing and proving verifiable random functions[C]//Theory of Cryptography Conference. 2017: 537-566.

[14] DENG Y, LIN D D. Instance-dependent verifiable random functions and their application to simultaneous

resettability[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2007: 148-168.

[15] YU Y, STEINBERGER J. Pseudorandom functions in almost constant depth from low-noise LPN[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2016: 154-183.

[16] 陈和风，马文平，高胜，等. 基于短整数解问题的伪随机函数新构造[J]. 通信学报，2017，35(10): 138-144.

对称密码算法研究

屈龙江[1]，陈玺[1]，王磊[2]，孙兵[3]
1. 国防科技大学文理学院数学系；
2. 上海交通大学；3. 国防科技大学
（上述作者同等贡献）

一　研究背景概述

1. 低差分函数研究方面

密码函数包含布尔函数与向量函数（S-盒）两大类，是构成序列密码、分组密码和 Hash 函数等对称密码算法的重要组件，其密码学性质的好坏直接关系到密码算法的安全性[1,2]。密码算法对于各种已知攻击的抵抗性可以由它所使用密码函数的相应密码学指标来衡量。差分攻击是攻击迭代分组密码最有效的方法之一，其基本思想是通过分析明文对差值对密文对差值的影响来恢复某些密钥比特。一个密码函数抵抗差分攻击的安全性指标被称为差分均匀度，差分均匀度越小，其抵抗差分攻击的能力越强。密码算法中重要的低差分函数有完全非线性函数（Perfect Nonlinear Function, PN 函数）、几乎完全非线性函数（Almost Perfect Nonlinear Function, APN 函数）和差分均匀度为 4 的函数（4-Uniform Function, 4 差分函数）等。当有限域的特征为奇数时，PN 函数、APN 函数分别达到最优、次优的差分均匀度；而在偶特征的有限域上，差分均匀度必然为偶数，此时 APN 函数、4 差分函数分别达到最优、次优的差分均匀度。由于绝大多数密码算法用的密码函数是定义在偶特征有限域上的，所以密码学研究中更关注 APN 函数和 4 差分函数。

为了抵抗差分攻击、线性攻击和插值攻击等分析方法，一个理想的 S-盒应同时具有低差分均匀度、高非线性度和高代数次数等多种良好密码学性质。在 SPN（Substitution-Permutation-Network）结构分组密码 S-盒的设计中，为了避免熵泄露，一般要求分组密码中使用的向量函数是置换的；而为了软硬件实现时具有较高的效率，又希望其定义在二元域的偶数维扩域上，因此相比一般的 4 差分函数，偶扩张上 4 差分置换的构造与分析近年来受到了更多研究和关注。

2. 可证明安全研究方面

相对于公钥密码算法基于公认的数学难题，对称密码算法往往基于设计者的安全分析经验，通过混合多种常见操作，如模加、循环移位、异或等，强化整体算法的混乱和扩散性能，使其能够通过标准性能测试，同时专门评估对已知攻击方法的抵抗强度。例如，AES 分组密码算法以及该算法设计者提出的宽轨迹策略。然而，这类设计方法和路线并不能为对称密码算法提供严格的安全保障。一方面，新型攻击方法不断涌现，攻击能力日益强化，某些新的攻击方法甚至可导致广泛应用的标准对称算法安全性瞬间崩塌，如 MD5 与 SHA-1 算法的突然破解；另一方面，标准性能测试关注输入和输出之间相关性、随机性等，即通用性测试，缺乏对各个算法特性的挖掘，有很大的局限性，仅提供基本的安全性能测试。