密码学和信息安全,量子技术,区块链

来学嘉 教授

（上海交通大学）

报告人简介：

来学嘉，上海交通大学计算机系教授，IDEA 密码的共同发明者。1992 年，他的博士论文“On the Design and Security of Block Ciphers”给出了 IDEA 密码算法(International Data Encryption Algorithm)。如今，这个“国际数据加密算法”已经成为全球通用的加密标准。过去 20 年，主要工作在密码学中，特别是在实际密码系统(包含分组密码和流密码),分组密码的差分分析和密码散列函数的分析和构建。参加了为欧洲的银行使用的信用卡的芯片中的算法的设计。参加了 ISO 标准 13888 不可否认协议，11770 密钥管理和 18033 密码算法的编辑.已出版了"有关分组密码的设计和安全"(Hartung orreVerlag,1992)这本书和不少于 40 篇的相关著作。已经评估、分析和改进了几个为大型商用和欧洲的组织使用的密码系统。研究方向为：密码算法设计和分析、密码技术的应用。

报告摘要：

密码学和信息安全的关系，密码学和量子技术的关系，密码学和区块链的关系。

Practical Computation Outsourcing: The State of the Art

任奎 教授

（浙江大学）

报告人简介：

任奎，浙江大学网络空间安全研究中心主任，国家千人计划特聘教授，研究方向为云安全，物联网安全和隐私保护。IEEE 会士，ACM 杰出会员。

报告摘要：

In this talk, I will give an overview of the field of practical computation outsourcing, which received much attention in recent years due to the rises of cloud computing and mobile computing. Various solutions are discussed and summarized according to a set of metrics that are meaningful in real world practices. The talk will also discuss the future directions.

Cryptanalysis of AES-PRF and Its Dual

王美琴 教授

（山东大学）

报告人简介：

王美琴，山东大学数学学院教授、博士生导师，密码技术与信息安全教育部重点实验室副主任，中国密码学会理事，中国密码学会密码数学理论专委会委员。2013 年获教育部新世纪优秀人才支持计划支持。2014 年获中国密码学会密码创新奖二等奖。2017 年以第一完成人获得国家密码科技进步一等奖（省部级）。主要从事对称密码理论的研究，主持多项国家级项目，近五年在 EUROCRYPT、ASIACRYPT、FSE、DCC 等国际权威期刊和会议发表高水平论文三十余篇。担任亚洲密码年会和 FSE 等顶级会议程序委员，作为联合主席承办国际会议 ASK 2013 和 2017 年中国密码学年会。

报告摘要：

A dedicated pseudorandom function (PRF) called AES-PRF was proposed by Mennink and Neves at FSE 2018 (ToSC 2017, Issue 3). AES-PRF is obtained from AES by feed-forwarding the output of the 5th round to the output state. This talk will presents extensive security analysis of AES-PRF and its variants.

非线性反馈移位寄存器仿射子簇的研究进展

郑群雄 讲师

（解放军信息工程大学）

报告人简介：

郑群雄，现任职于战略支援部队信息工程大学网络空间安全学院，2013 年毕业于解放军信息工程大学，获密码学博士学位。硕士学位论文和博士学位论文分别于 2010 年和 2014 年获评全军优秀学位论文。主要从事对称密码设计与分析方面的研究工作，先后在《IEEE Transactions on Information Theory》、《Designs、Codes and Cryptography》等刊物上发表学术论文近 20 篇。2016 年入选中国科协青年人才托举工程项目。

报告摘要：

非线性反馈移位寄存器（简称 NFSR）已广泛应用于密码算法的设计中，如 Grain 系列算法、Sprout、Fruit 等。本报告首先介绍 NFSR 仿射子簇的概念及其密码意义；随后介绍 NFSR 仿射子簇阶数上界的研究进展；最后介绍求取 NFSR 仿射子簇的若干算法，首重介绍我们团队基于差分技术构建的求取仿射子簇的新算法，并介绍这些算法在 Grain 等算法中的应用。

特征矩阵分析法

孙兵 讲师

（国防科技大学）

报告人简介：

孙兵，空军第 41 期飞行学员，2009 年毕业于国防科技大学获理学博士学位，比利时鲁汶大学访问学者，现为国防科技大学文理学院讲师。长期从事对称密码的设计与分析研究，在 CRYPTO、EUROCRYPT 等密码学国际学术会议和期刊发表学术论文 50 余篇，在科学出版社出版专著 1 部。

报告摘要：

本报告提出布尔函数的特征矩阵概念，并研究其密码学性质，在此基础上建立密码算法针对中间相遇攻击的可证明安全模型，指出在现有分析模型下 AES 等算法具有对中间相遇攻击的可证明安全。

对一个对称全同态密码的攻击

王保仓 教授

（西安电子科技大学）

报告人简介：

王保仓，1979 年 3 月生，河南郸城人，西安电子科技大学通信工程学院/综合业务网理论与关键技术国家重点实验室 密码学专业教授、博士生/硕士生导师，2006 年 12 月获西安电子科技大学密码学专业博士学位。科技部重点研发计划项目课题负责人，主持国家自然科学基金项目 4 项，主持十三五预研项目、十二五预研项目、陕西省自然基金、华为高校合作重点项目、中电集团 30 所、54 所高校合作项目等。中国密码学会会员，中国密码学会算法委员会委员。

报告摘要：

最近，Lichun Li 等人提出了一个对称的全同态加密算法，并使用该算法构造了一个隐私保护的数据库关联规则挖掘外包协议。基于连分式算法，证明了 Lichun Li 等人的全同态加密算法是不安全的。给定 一系列明密文对，可以在多项式时间内恢复 Lichun Li 等人的全同态加密算法的解密密钥。

Key Consensus from Lattice (KCL)

赵运磊 教授

(复旦大学)

报告人简介：

赵运磊，复旦大学计算机学院教授、博士生导师。中国密码学会理事、中国计算机学会区块链专委会委员、中国电子学会区块链专委会委员、。主要研究兴趣：密码理论及应用、零知识、公钥密码、后量子密码、区块链和密码货币、云计算和大数据安全隐私。在密码学与信息安全重要国际会议和期刊（包括 Journal of Cryptology、ACMCCS、EUROCRYPT 等）发表系列论文，获得较大国际影响。多项研究成果得到大规模应用，产生了重大效益。

报告摘要：

在本报告中，我们简要介绍我们提交到 NIST 后量子密码标准征集的 KCL 算法族。介绍 KCL 的设计理念、与 NIST 后量子密码标准征集在主流格基密码算法的比较。

噪音条件下的量子通信协议安全性分析

李剑 教授

（北京邮电大学）

报告人简介：

李剑，北京邮电大学计算机学院教授，博士生导师。一直从事信息安全、量子密码等方面的研究。北京邮电大学“现代密码学”国家级精品课、“信息安全”北京市精品课主要参与人。在《Scientific Reports》、《Physics Letter A》、《Entropy》、《International Journal of Theoretical Physics》、《中国科学》、《科学通报》等国内外期刊发表论文 100 余篇，其中 SCI 检索论文 30 篇余篇，EI 检索论文 40 余篇；出版信息安全方面教材 10 余本，其中包括《信息安全概论》、《信息安全导论》、《信息安全专业英语》《操作系统安全》等国家级规划教材和北京市精品教材。承担多项国家 863、973、自然基金课题。目前是中国互联网协会反恶意软件技术组组长，中国电子学会高级会员。

报告摘要：

多数在理想条件下设计的量子密码协议没有考虑实际通信中噪声的影响，可能造成机密信息不能被准确传输，或可能存在窃听隐藏在噪声中的风险，因此分析噪声条件下量子密码协议的安全性具有重要的意义。本研究分析已有量子密码协议在联合噪声条件下的安全性，针对如何定量地区分量子信道中噪声和窃听的问题，采用粒子偏转模型，对量子信道中的联合噪声进行建模；针对如何定量地分析噪声条件下量子信道的安全性问题，采用冯•诺依曼熵理论建立窃听者能窃取的信息量与量子比特误码率、噪声水平三者之间的函数关系；针对如何证明量子密码协议在联合噪声条件下是否安全的问题，根据联合噪声模型及窃听者能窃取的信息量与量子比特误码率、噪声水平三者之间的关系，定量地分析协议在联合噪声条件下的安全性并计算噪声临界点。本研究成果丰富了量子密码学理论，创新噪声条件下的量子密码协议安全性检测方法，有利于推进量子密码协议的实用化进程。

小模数格密码算法设计

路献辉 副研究员

（中科院信工所）

报告人简介：

路献辉，2009 年于西南交通大学获得信息安全专业博士学位。2009-2012 年进入中国科学院研究生院信息安全国家重点实验室从事博士后研究。2012 年起进入中国科学院信息工程研究所工作。主要研究兴趣包括公钥密码体制的可证明安全性和后量子公钥密码算法设计。设计了后量子公钥加密算法 LAC，参与了美国 NIST 组织的后量子密码算法征集活动，成为全球进入第一轮评估的 69 个候选算法之一。

报告摘要：

格密码是抗量子攻击密码算法中最为活跃的一种类型，也是本次 NIST 后量子公钥密码算法标准征集中提交数量最多的类型。本次报告介绍我们提交到 NIST 的候选算法 LAC。LAC 的核心设计思想是最大限度降低模数的尺寸，为此我们放弃了 NTT 加速技术，并通过 BCH 大分组纠错和 AVX2 向量指令解决了模数降低带来的错误率增大和计算效率问题。

量子密码与量子网络编码研究进展

陈秀波 副教授

（北京邮电大学）

报告人简介：

陈秀波，副教授，博士生导师。在北京邮电大学长期从事信息安全领域的研究工作，中国电子学会量子信息分会委员。主要研究方向为量子密码、区块链技术、大数据安全。

近年来，作为项目负责人主持了 10 余项纵向科研项目，包括国家自然科学基金 3 项、教育部博士点基金、“十二五”国家密码发展基金等。作为研究骨干参加了十余项科研项目，包括国家自然科学基金委创新研究群体项目、国家信息安全 973 项目、863 项目、国家自然科学基金项目等。目前，在国内外著名 SCI 检索期刊上共发表论文 114 篇，共被引 97 篇，总 1382 次，他引 1049 次，单篇他引次数最高为 100 余次。其中 JCR 一区论文 38 篇，二区论文 36 篇。担任国际学术期刊《Information Sciences》、《IEEE Access》、《Quantum Information Processing》、《Soft Computing》、《IEEE communication letters》、《计算机学报》、《通信学报》、《物理学报》等 10 多家国内外杂志的审稿专家。2013 年入选教育部“新世纪优秀人才支持计划”。2012 年获霍英东教育基金会青年教师基金基础性研究课题资助。

报告摘要：

经典密码学和量子力学的量子密码在理论上具有无条件安全性，其目的也是为了有效地保护信息。特别是量子秘密共享，量子信息隐藏，量子安全多方计算等相关协议已成为量子密码的重要研究方向。目前，基于量子密码体制的保密通信逐渐从点对点的两方通信向多用户和网络化方向发展。由于网络中间节点的存在，使得对信息的处理能力大大加强。理论上可以提升通信网络的最大吞吐量，提高带宽利用率。量子网络编码采用量子密码特有的理论与技术，借鉴经典网络编码思想，致力于提供高效、安全、可靠的量子通信解决方案。量子网络编码技术对提升和优化量子网络通信的整体性能具有重要的研究意义。

区块链与隐私保护

张方国 教授

（中山大学）

报告人简介：

张方国，中山大学数据科学与计算机学院的教授、博导。广东省信息安全技术重点实验室副主任，中国密码学会常务理事，中山大学网络空间安全研究所所长。2001 年 12 月，在西安电子科技大学密码学专业获得工学博士学位。曾在美国，韩国，澳大利亚等多个国家进行过学术访问。担任《密码学报》、《信息网络安全》等杂志编委，2018 中密会，Pairing 2013, ProvSec2009, JWIS2011，AsiaJCIS 2012-13 等会议的程序委员会联合主席，以及一百多个密码学领域国内外学术会议的程序委员会委员。

张方国的研究兴趣是密码学理论及其应用，特别是：椭圆曲线和超椭圆曲线密码体制，安全多方计算，隐私性与匿名性，区块链及其应用等。

报告摘要：

报告主要探讨区块链与隐私保护，分两部分内容：一方面探讨一下如何用隐私保护技术实现区块链中的隐私保护；另一方面探讨一下如何用区块链技术实现隐私保护。

InstantCryptoGram: Secure Image Retrieval Service

王骞 教授

（武汉大学）

报告人简介：

王骞，教授，博导，武汉大学国家网络安全学院副院长、“信息安全与可信计算”方向学科带头人。2013 年入选国家中组部第四批“青年千人计划”。获 2014 年 CCF-Intel “青年学者奖”、2016 年 IEEE 通信协会亚太区“杰出青年研究学者奖”。王骞研究涉及云计算安全与隐私、无线网络安全、人工智能安全、大数据安全与隐私、应用密码学等多个领域。发表论文 100 余篇，近五年的引用超过 10000 次，其中 SCI 他引 2000 余次。其中，CCF A 类长文 37 篇，包括 IEEE TDSC、TIFS、JSAC、ACM CCS、MobiCom 等。4 篇论文入选 ESI 高被引论文，1 篇入选 ESI 热点论文，5 篇论文分别获得 ICDCS’17、TrustCom’16、WAIM’14、ICNP’11 和 ChinaCom’09 最佳论文奖。王骞受邀担任网络与信息安全领域重要刊物 IEEE Transactions on Information Forensics and Security (TIFS) (CCF A 类)、IEEE Transactions on Dependable and Secure Computing (TDSC) (CCF A 类)编委。担任国家高技术研究发展计划会评专家、国家自然科学基金委信息科学部重点项目会评专家。

报告摘要：

Image retrieval is crucial for social media sites such as Instagram to identify similar images and make recommendations for users who share similar interests. To get rid of the storage burden and computation for image retrieval, outsourcing to a remote cloud is now a trend. Yet, privacy concerns mandate the use of encryption before outsourcing the images. We need a secure way for retrieving images from a not-fully-trusted server.

In this talk, we introduce InstantCryptoGram, a secure image retrieval service. We first design a new data structure called sub-simhash, which fits for the inverted index used by many searchable symmetric encryption schemes. It leads to our modular solution that supports efficient similarity queries and updates over encrypted images. Our experiments on Amazon AWS EC2 over representative datasets show that our scheme is efficient and accurate in finding similar images while preserving privacy.

Achieve Efficient and Verifiable Conjunctive and Fuzzy Queries over Encrypted Data in Cloud

邵俊 教授

（浙江工商大学）

报告人简介：

邵俊，博士毕业于上海交通大学计算机软件与理论专业，现为浙江工商大学教授，其研究兴趣为应用密码学、云/雾计算安全和区块链等。主持省部级以上项目 10 余项，包括两项国家自然科学基金项目、一项浙江省杰出青年基金项目和一项浙江省重点基金项目。在知名期刊和会议发表多篇论文，包括 IEEE TIFS、IEEE Network、IEEE TVT、PKC、ESORICS、IEEE INFOCOM 等。

报告摘要：

Due to the high demands of searchability over encrypted data, searchable encryption (SE) has recently received considerable attention and been widely suggested in encrypted cloud storage. Typically, the cloud server is assumed to be honest-but-curious in most SE-based cloud storage systems, i.e., the cloud server should follow the protocol to return valid and complete search results to users. However, this trust assumption is not always true due to some unanticipated situations, such as misconfigurations and malfunctions. Therefore, the function of verifiability of search results becomes crucial for the success of SE-based cloud storage systems. For this reason, many verifiable SE schemes have been proposed; however, they either fail to support query operators “OR”, “AND”, “*” and “?” simultaneously, or require many time-consuming operations. Aiming at addressing this problem, in this paper, we propose a new verifiable SE scheme for encrypted cloud storage. The proposed scheme is characterized by integrating various techniques, i.e., bitmap index, radix tree, format preserving encryption, keyed-hash message authentication code and symmetric key encryption, for achieving efficient and verifiable conjunctive and fuzzy queries over encrypted data in cloud. Detailed security analysis shows that our proposed scheme holds the confidentiality of data and verifiability of search results at the same time. In addition, extensive experiments are conducted, and the results demonstrate our proposed scheme is efficient and suitable for users to retrieve their data from the cloud to their mobile devices.

Data Protection Mechanism in Cloud Computing

沈剑 教授

（南京信息工程大学）

报告人简介：

沈剑，江苏南京人，现任南京信息工程大学研究生院副院长、江苏省网络监控工程中心副主任，教授、博导、云计算安全团队学术带头人，2015 年入选江苏省“双创人才”-双创博士、入选江苏省“六大人才高峰”。一直从事信息安全、密码学、网络安全、数据安全等方面的研究工作。沈剑分别于 2009 年 8 月和 2012 年 8 月在韩国获得工学硕士学位和工学博士学位，并于 2012 年 12 月回国任职。主要研究方向包括：密钥协商、公钥加密、数据安全分享、数据审计等方向。沈剑现为 IET Fellow、IEEE、ACM 会员、中国密码学会安全协议专业委员会委员，多个国际期刊编委及多个国际会议程序委员会主席、委员。近年来，已在 IEEE Transactions 等国内外期刊和国际会议上发表学术论文三十余篇。主持国家自然科学基金项目两项、参与国家自然科学基金重点项目一项等。

报告摘要：

With the rapid development of cloud computing, we have carried out many researches on data protection mechanism in cloud computing. In order to strengthen the control of cloud storage data, we propose an efficient public auditing protocol with global and sampling blockless verification as well as batch auditing. Note that, the novel dynamic structure consists of a doubly linked info table and a location array. In order to protect the data security, we propose a trusted third party aided searchable and verifiable data protection scheme utilizing cloud computing technology, where a user differentiated system model and a cube data storage structure are presented. In order to address the security and privacy issues in the vehicle-to-grid, we propose a robust key agreement protocol that can achieve mutual authentication without exposing the real identities of users. In addition, in order to improve the machine-to-machine technology to a higher level of security, we extend the idea of (t, n) secret sharing for information transmission in M2M (machine-to-machine) with high security and efficiency. Specifically, a secret is divided into 2k shares and then transmitted through 2k node-disjoint paths constructed by Latin square.

Collision Resistant Hashing from Learning Parity with Noise

郁昱 研究员

（上海交通大学）

报告人简介：

郁昱，博士，上海交通大学计算机科学与工程系的特别研究员，主要从事密码学相关的研究。2003 年获得复旦大学计算机系学士学位，2006 年获南洋理工大学博士学位，之后在比利时鲁汶大学从事博士后研究工作。2010 年回国后曾分别在华东师范大学和清华大学任教，多项研究成果一作发表在密码三大会和 CCS,TCC,CT-RSA 等密码与信息安全的代表性会议上。目前他还担任了 Asiacrypt Steering Committee 委员。

报告摘要：

Learning Parity with Noise (LPN)是著名的机器学习领域的困难问题，是 Learning With Errors (LWE)在二元域上的版本，也是少数具有最坏意义到平均意义困难性规约的量子困难问题。目前我们已知如何基于 LWE 或格问题构造抗碰撞哈西(CRH)函数，但是如何给予 LPN 构造 CRH 仍是一个公开问题。受到 Ajtai 基于 SIS 问题的 CRH 启发，我们构造了基于 LPN 问题的抗碰撞哈西函数，并利用 RO 或随机置换等理想模型进行进一步的效率优化。

Regular Lossy Functions and Their Applications

陈宇 副研究员

（中科院信工所）

报告人简介：

陈宇，中国科学院信息工程研究所信息安全国家重点实验室副研究员、中国科学院青年创新促进会会员。主要研究方向为公钥密码学，研究兴趣为可证明安全理论、基本密码组件及其应用. 近年在密码学领域高水平期刊 Design, Codes and Cryptography 等及国际会议 SCN 2014、PKC 2016、CRYPTO 2016、CT-RSA 2018 等上发表论文多篇。

报告摘要：

Peikert 和 Waters 在 STOC 2008 上提出了新的密码原语—有损陷门函数. 在正常模式下，函数是单射且可逆的；在有损模式下，函数是有损的(输出丢失输入的信息)。两种模式计算不可区分. 在本研究工作中，我们对有损陷门函数进行弱化，得到新的密码原语—规则有损函数. 与有损陷门函数相比，规则有损函数不要求正常模式下的函数是单射可逆的，仅要求其规则有损. 此外，我们提出规则有损函数的两个扩展，分别是 All-But-One 规则有损函数 (ABO-RLFs) 和一次性规则有损过滤器(OT-RLFs). 在构造层面，我们展示如何分别基于数论困难假设和哈希证明系统给出高效的构造；在应用层面，我们展示了规则有损函数在抗泄漏密码学中的强力应用.

密码方案的不可证明安全性研究

张江 副研究员

（密码科学技术国家重点实验室）

报告人简介：

张江，博士，密码科学技术国家重点实验室副研究员。2015 年博士毕业于中国科学院软件研究所。主要从事公钥密码可证明安全理论、抗量子密码和多方安全计算协议设计与分析研究，近五年以第一作者身份在三大国际密码会议 CRYPTO、EUROCRYPT、AISACRYPT 和 IEEE TMC、TCS 等重要国际期刊上发表了多项研究成果，受邀担任亚洲密码年会 AISACRYPT 2017、CANS 2017、ACISP 2018 等多个国际会议程序委员和多个国际期刊的审稿人，曾获“中国科学院院长优秀奖”，“中国科学院优秀博士论文”，“中国密码学会优秀博士论文”等荣誉，并入选中国科协“2016-2018 青年人才托举工程”。

报告摘要：

许多知名的密码方案往往不存在（或没有找到）安全证明，但同时也没有找到有效的攻击。密码方案的不可证明安全性即利用可证明安全技术来说明某些“安全”的密码方案不能以某种方式被证明是“安全的”，从而一定程度揭示特定安全证明技术的“局限性”。本报告将重点介绍几种用于密码方案不可证明安全性的技术，并通过实例来展示如何运用他们来研究密码方案的可证明安全性。

对称密码的可证明安全

王磊 研究员

（上海交通大学）

报告人简介：

王磊，上海交通大学特别研究员，入选青年千人计划。主要从事密码学研究，集中对于对称密码算法的设计与安全分析。成果多次在密码学三大年会 CRYPTO、EUROCRYPT、ASIACRYPT 发表。多次担任 EUROCRYPT、ASIACRYPT、FSE 等国际会议的程序委员会成员。

报告摘要：

对称密码算法的研究大致分为：标准算法的设计与分析；理论模型的设计和可证明安全。前者往往通过混合一些常见的简单操作，例如模加、异或、循环移位等，达到抵抗已知攻击方法的效果。优点在于高效率。后者理论模型的研究为标准算法的设计提供指导思想和归约安全保障，对于开发改进标准算法具有非常重要的意义。本次报告主要关注对称密码理论模型的可证明安全，介绍主流的方法和工具等，集中于近年密码学领域的新成果，并且针对若干通用理论构造，总结和介绍近年来的科研成果。

新应用中的密码关键技术

李智虎 高级工程师

（国家密码管理局）

报告人简介：

李智虎，国家密码管理局高级工程师，长期从事密码理论，密码工程，商用密码标准和商用密码管理研究，对密码协议安全性分析有深刻的理解，是国家卫生与健康委员会，中国残联，中国防伪协会，公安部等多个部委信息化专家。

报告摘要：

移动互联网时代的到来，各种新应用层出不穷，例如区块链，量子通信，云计算，移动互联网及物联网等，密码在新应用中发挥着身份认证、数据机密性、完整性和个人隐私保护等重要关键作用，本报告介绍了区块链使用的杂凑链，杂凑二叉树，非交互零知识证明，量子通信最基本的 bb84 协议，并对该协议及其工程实现存在的风险进行了分析，对移动互联网、物联网及云计算环境下密码防护关键技术进行了介绍和分析。

基于人工智能的攻防对抗

陈恺 研究员

（中科院信工所）

报告人简介：

陈恺，中国科学院信息工程研究所，研究员、博士生导师，国家“万人计划”青年拔尖人才、北京市“科技新星”，《Cybersecurity》编辑部主任。2010 年获中国科学院研究生院博士学位，美国宾州立大学博士后。中国保密协会隐私保护专业委员会委员，中国计算机学会系统软件专委会委员、中国网络空间安全协会全国高校网安联赛监督委员会委员。主要研究领域包括软件与系统安全、人工智能对抗。在 IEEE S&P、USENIX Security、ACM CCS、ICSE、ASE、TIFS、TDSC、TMC、TRE、RAID、DSN、MobiSys 等发表论文 70 余篇；曾主持和参加国家重点研发计划、国家自然科学基金、863 计划、国家发改委信息安全专项、中科院战略性先导科技专项等国家部委课题 40 余项。

报告摘要：

Patches and related information about software vulnerabilities are often made available to the public, aiming to facilitate timely fixes. Unfortunately, the slow paces of system updates (30 days on average) often present to the attackers enough time to recover hidden bugs for attacking the unpatched systems. Making things worse is the potential to automatically generate exploits on input-validation flaws through reverse-engineering patches.

We seek to generate proof-of-concept (PoC) exploits for the vulnerability types never automatically attacked. Unlike an input validation flaw that is often patched by adding missing sanitization checks, fixing other vulnerability types is more complicated, usually involving replacement of the whole chunk of code. Without understanding of the code changed, automatic exploit becomes less likely. To address this challenge, we present SemFuzz, a novel technique leveraging vulnerability related text (e.g., CVE reports and Linux git logs) to guide automatic generation of PoC exploits. Such an end-to-end approach is made possible by natural-language processing (NLP) based information extraction and a semantics-based fuzzing process guided by such information.

FourQ-based Cryptography for High-performance and Low-power Applications

刘哲 教授

（南京航空航天大学）

报告人简介：

刘哲，南京航空航天大学计算机科学与技术学院教授，博士生导师，中国密码学会青年工作委员会委员。曾在法国巴黎高师信息安全组（ISG）和卢森堡大学安全与信任中心（SnT）和加拿大滑铁卢大学量子研究中心和应用密码研究中心从事博士后研究工作。2015 年 11 月于卢森堡大学(University of Luxembourg)算法、密码与安全实验室获得博士学位。刘哲的博士毕业论文“Lightweight Public-Key Cryptography for Wireless Sensor Nodes”获得卢森堡国家基金委 2016 年评出的唯一杰出博士毕业论文奖(Outstanding Ph.D Thesis Awards)，他也成为了该奖项第一位华人获得者，卢森堡国家基金委，卢森堡大学以及滑铁卢大学量子研究中心进行了专题报道；2017 年获得 ACM 中国新星奖提名奖。刘哲已经在国内外密码学术期刊和会议上发表学术论文 70 多篇，其中 20 多篇发表在安全类著名期刊和会议上，包括 IEEE Transactions on Computers (IEEE TC), IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), IEEE Transactions on Information Forensics and Security (IEEE TIFS); ACM Transactions on Embedded Computing Systems (ACM TECS) 和 IACR Conference on Cryptographic Hardware and Embedded Systems (CHES)，Computers & Security, Science China (中国科学) 等。刘哲目前担任 4 个著名安全类期刊的编委，10 几个期刊的客座编辑（包括 IEEE Transactions on Computers, IEEE Transactions on Emerging Topics in Computing）以及 30 多个安全类国际会议的程序委员会委员。

报告摘要：

This work deals with the energy-efficient, high-speed and high-security implementation of elliptic curve scalar multiplication, elliptic curve Diffie-Hellman (ECDH) key exchange and elliptic curve digital signatures on embedded devices using FourQ and incorporating strong countermeasures to thwart a wide variety of side-

channel attacks.

First, we set new speed records for constant-time curve-based scalar multiplication, DH key exchange and digital signatures at the 128-bit security level with implementations targeting 8, 16 and 32-bit microcontrollers. For example, our software computes a static ECDH shared secret in 6.9 million cycles (or 0.86 seconds @8MHz) on a low-power 8-bit AVR microcontroller which, compared to the fastest Curve25519 and genus-2 Kummer implementations on the same platform, offers 2x and 1.4x speedups, respectively. Similarly, it computes the same operation in 496 thousand cycles on a 32-bit ARM Cortex-M4 microcontroller, achieving a factor-2.9 speedup when compared to the fastest Curve25519 implementation targeting the same platform. A similar speed performance is observed in the case of digital signatures.

Second, we engineer a set of side-channel countermeasures taking advantage of FourQ's rich arithmetic and propose a secure implementation that offers protection against a wide range of sophisticated side-channel attacks, including differential power analysis (DPA). Despite the use of strong countermeasures, the experimental results show that our FourQ software is still efficient enough to outperform implementations of Curve25519 that only protect against timing attacks. Finally, we perform a differential power analysis evaluation of our software running on an ARM Cortex-M4, and report that no leakage was detected with up to 10 million traces.

These results demonstrate the potential of deploying FourQ on low-power applications such as protocols for the Internet of Things.

Countering Cryptographic Subversion in the Post-Snowden Era

陈荣茂 助理研究员

（国防科技大学）

报告人简介：

陈荣茂，博士，国防科技大学计算机学院助理研究员，入选中国科协2017-2019年度青年人才托举工程。2011年和2013年先后在国防科技大学获得计算机专业学士学位和硕士学位，2013-2016年获国家留学基金委资助在澳大利亚卧龙岗大学获得密码学博士学位。主要研究兴趣为网络安全与应用密码技术，现阶段主要从事后斯诺登密码学研究。迄今以第一作者及主要作者身份在CRYPTO，ASIACRYPT，CT-RSA等国际会议以及IEEE TIFS，DCC等多个国际期刊上发表论文近30篇。先后担任多个国际学术会议程序委员会委员以及多个学术会议和期刊审稿人。

报告摘要：

The revelations of Edward Snowden in 2013 demonstrated that cryptography in practice may be surreptitiously weakened by inserting backdoors into cryptosystems. Moreover, these backdoors are usually undetectable for even cryptographic experts due to the extreme complexity of modern cryptographic implementations. Inspired by this issue, a new research direction known as Post-Snowden cryptography has arisen in recent years with the aim of safeguarding the user privacy in face of subversion attacks against cryptosystems in the real world. This talk will first give an overview of formalized subversion attacks against several fundamental cryptographic primitives, and follow with our recent progress on strong subversion attack against digitals signatures. Various Countermeasures to defending subversion attacks will also be discussed.