梁 蓓

研究方向：信息安全 <密码学>

移动电话： （+86）18911186561　　电子邮件： lbei@chalmers.se

出生年月： 1985.9　　政治面貌： 中共党员

教育经历

2016.06毕业

中国科学院信息工程研究所	信息安全	博士	2012.09—2016.07
西安理工大学	应用数学	硕士	2007.09—2010.07
西安理工大学	计算数学	学士	2003.09—2007.07

工作经历

Chalmers University of Technology	Dept. Computer Sciences & Engineering	博士后	2016.08—2020.08

学术访问经历

Tokyo Institute of Technology, Japan	Hosted by Prof. Tanaka Keisuke	2018.05—2018.06
中国科学院信息工程研究所	Hosted by薛锐教授	2017.07—2017.09
Aarhus University, Denmark	Hosted by Prof. Claudio Orlandi	2017.02—2017.04
ETH Zurich, Switzerland	Hosted by Prof. Adrian Perrig	2016.11—2016.12

科研项目

云计算环境下安全高效全同态签名方案的构造	参与人	国家自然基金（主持人王付群）	2020.01—2023.12
基于属性的全同态加密方案的构造	参与人	浙江省自然基金（主持人王付群）	2019.01—2020.12
CryptoQuaC: Cryptography meets Verifiable Quantum Computation Chalmers)	参与人	Chalmers GENIE（主持人Aikaterini Mitrokotsa）	2020.01—至今
Cryptographic-based verification protocols of quantum computation	参与人	Chalmers（主持人Aikaterini Mitrokotsa）	2019.01—2020.01
Security and Privacy in the Internet of Things using Blockchains	参与人	STINT (Sweden-Japan 150 Anniversary Grant)（主持人Aikaterini Mitrokotsa）	2018.01—2019.09
PRECIS: Privacy and Security in Wearable Computing Devices	参与人	Swedish Research Council-VR grant（主持人Aikaterini Mitrokotsa）	2016.09—2019.09
短期访问任务（in COST ACTION IC1403）	申请人	COST ACTION IC1403 CRYPTACUS（主持人Prof. Claudio Orlandi ）	2017.02—2017.04
短期访问任务（in COST ACTION IC1306）	申请人	COST ACTION IC1306	2016.11—2016.12

指导学生经历

共同指导(co-supervisor)博士生:

Carlo Brunetta	2017.09 – 至今	Chalmers University of Technology, Dept. Computer Science & Engineering
Georgia Tsaloli	2017.09 – 至今	Chalmers University of Technology, Dept. Computer Science & Engineering
潘冬雪	2019.01 – 2020.06	中国科学院信息工程研究所

教学经历

2019 年秋季学期	助教	本科课程	密码学	Chalmers University of Technology

2018 年秋季学期	助教	本科课程	密码学	Chalmers University of Technology

获奖情况 Awards

- 2015年 ProvSec 2015 最佳学生论文
- 2007--2010年 一等奖学金
- 2010年 优秀毕业生，三好学生
- 2019年 ISC 2019 最佳论文

学术活动

Session chair of poster session in CySep summer school 2019

Program committee of NordSec2017–The 22rd Nordic Conference on Secure IT Systems

参与会议及期刊审稿：IET Information, Future Generation Computer Systems, Wireless Communications and Mobile Computing, Asiacrypt2020, GameSec 2019, IEEE TrustCom 2019, NordSec 2018, NordSec2017等

学术会议报告

- “What can go wrong with cryptography in the quantum setting”, Applied Quantum Physics Laboratory at Dep. Micro-technology and Nanoscience, Chalmers University of Technology, Sweden, March 2019.
- “Overview on (Distributed) Verifiable Random Functions”, Cryptography and Security Group, Aarhus University, Denmark, March 2017.
- “Robust Distributed Pseudorandom Functions for mNP Access Structures.”, ISC 2019, New York City, NY, USA, September 2019.
- “How to Robustly Distribute the Computation of Pseudorandom for General Access Structures”, CySep 2019, Stockholm, Sweden, June 2019.
- “Distributed Pseudorandom Functions for General Access Structures in NP”, ICICS 2017, Beijing, China, December 2017.
- “Constrained Verifiable Random Functions from Indistinguishability Obfuscation”, ProvSec 2015, Kanazawa, Japan, November 2015.
- “Transformation from Standard Signatures to Identity-Based Aggregate Signatures”, ISC 2015, Trondheim, Norway, September 2015.