项目公示信息

成果名称：后量子安全密码方案的设计

完成单位：陕西师范大学、中国科学院信息工程研究所、上海交通大学、中国科学院大学、河南师范大学

完成人：来齐齐、汪哲东、排尔哈提·阿卜拉、王晗、张恩

成果简介：本项目属于后量子安全的公钥密码学研究领域。在国家自然科学基金青年基金项目（61802241）和陕西省自然科学基础研究计划（2019JQ-360）的资助下，项目组**围绕后量子安全公钥密码方案和协议所面临的安全性弱、效率低等缺点展开深入研究，以格困难问题和哈希函数的抗量子计算特性为基础，突破了后量子安全的函数加密方案的安全性和效率瓶颈、后量子安全的紧归约密码方案必须依赖于超多项式模数的效率瓶颈、后量子安全的多方隐私集合交集（PSI）协议不能抵抗恶意敌手的安全性瓶颈、后量子安全的哈希证明系统必须依赖于随机预言机的安全性瓶颈等关键理论难题**，为设计后量子安全的实用型多功能公钥密码方案和协议提供关键理论支撑。

8篇代表作中包含国际密码学会顶级国际会议论文4篇，美国计算机学会知名国际会议论文 1 篇，SCI 检索期刊论文 2 篇，国内中文权威期刊（EI 检索）论文 1 篇。其中 CCF A 类会议会议论文 1 篇，CCF B 类会议论文 3 篇。

相关研究成果受到国际同行的广泛关注，并多次收到国

际相关研究人员的学术交流邮件。尤其是受到包括 Michel Abdalla（现任国际密码学会主席）、Brent Waters（ACM Fellow）、Hoeteck Wee、David Pointcheval、Benoit Libert、Benny Pinkas、Mike Rosulek、Ni Trieu、Jonathan Mayer、Katsuyuki Takashima、Shota Yamada、Dario Catalano、Romain Gay、David Wu、Sam Kim 等众多国际著名密码和网络安全专家的重点关注，并在他们的 USENIX 2022、TCC 2022、AISACRYPT 2022、EUROCRYPT 2021、CRYPTO 2021、CCS 2021、USENIX 2021、AISACRYPT 2020 等国际顶级会议所分别发表的多篇论文中多次给予极高评价。

完成人合作关系情况汇总表

序号	合作方式	合作关系人及排名	合作时间	合作成果名称	证明材料（代表论著、知识产权、项目、协议等）
1	论文合著	汪哲东(3)	2018-04-27 至 2021-11-30	代表论文 1. (New Lattice Two-Stage Sampling Technique and Its Applications to Functional Encryption – Stronger Security and Smaller Ciphertexts) 代表论文 3. (Almost Tight Security in Lattices with	1-1；1-3

				polynomial modulus - PRF, IBE, All-but-many LTF, and More)	
2	论文合著	排尔哈提·阿卜拉(1)，王晗(3)，汪哲东(4)	2019-04-28 至 2021-11-30	代表论文 2.(Ring-Based Identity Based Encryption – Asymptotically Shorter MPK and Tighter Security)	1-2
3	论文合著	汪哲东(1)	2017-10-7 至 2021.11.30	代表论文 4. (FE for Inner Products and Its Application to Decentralized ABE)	1-4
4	论文合著	张恩(1)，来齐齐(3)	2018-06-30 至 2021-11-30	Efficient Multi-Party Private Set Intersection Against Malicious Adversaries	1-5

主要论文专著目录（限 8 条）

序号	论文专著名称	刊名	第一完成单位（全称）	作者（填全），英文翻译	年卷页码（xx 年 xx 卷 xx 页）	发表时间（某年某月）	通讯作者（中文，按照文中标注的，无标注的不填）	第一作者（中文）
1	New Lattice Two-Stage Sampling Technique and Its Applications to Functional Encryption – Stronger Security and Smaller Ciphertexts	EUROCRYPT 2021	陕西师范大学	Qiqi Lai（来齐齐）, Feng-Hao Liu（刘峰豪）, Zhedong Wang（汪哲东）	2021, LNCS 12696, 498–527	2021 年 10 月	来齐齐	来齐齐
2	Ring-Based Identity Based Encryption – Asymptotically Shorter MPK and Tighter Security	TCC 2021	中国科学院信息工程研究所	Parhat Abla（排尔哈提 •阿卜拉）, Feng-Hao Liu（刘峰豪）, HanWang（王晗）, Zhedong Wang（汪哲东）	2021, LNCS 13044, 157-187	2021 年 11 月	王晗	排尔哈提 • 阿卜拉

3	Almost Tight Security in Lattices with polynomial modulus - PRF, IBE, All-but-many LTF, and More.	PKC 2020	陕西师范大学	Qiqi Lai（来齐齐）, Feng-Hao Liu（刘峰豪）, Zhedong Wang（汪哲东）	2020, LNCS 12110, 652–681	2020 年 5 月	来齐齐 刘峰豪 汪哲东	来齐齐
4	FE for Inner Products and Its Application to Decentralized ABE	PKC 2019	中国科学院大学	Zhedong Wang（汪哲东）, Xiong Fan（范雄）, Feng-Hao Liu（刘峰豪）	2019, LNCS 11443, 97–127	2019 年 5 月	汪哲东	汪哲东
5	Efficient Multi-Party Private Set Intersection Against Malicious Adversaries	CCSW @CCS 2019	河南师范大学	En Zhang（张恩）, Feng-Hao Liu（刘峰豪）, Qiqi Lai（来齐齐）, Ganggang Jin（金刚刚）, Yu Li（李煜）	2019, 93-104	2019 年 11 月	来齐齐	张恩
6	Novel Smooth Hash Proof Systems Based on Lattices	The Computer Journal	陕西师范大学	Qiqi Lai（来齐齐）, Bo Yang（杨波）, Yong Yu（禹勇）, Yuan Chen（陈原）, Jian Bai（白健）	2018, 61, 561-574	2017 年 11 月	杨波	来齐齐

7	Novel Identity-Based Hash Proof System with Compact Master Public Key from Lattices in the Standard Model	International Journal of Foundations of Computer Science	陕西师范大学	Qiqi Lai（来齐齐）, Bo Yang（杨波）, Zhe Xia（夏喆）, Yannan Li（李艳楠）, Yuan Chen（陈原）, Zhenlong Li（李振龙）	2019, 30, 589-606	2019 年 1 月	杨波	来齐齐
8	格上基于身份哈希证明系统的新型构造	软件学报	陕西师范大学	来齐齐, 杨波, 陈原, 韩露露, 白健	2018, 29, 1880-1892	2017 年 10 月	杨波	来齐齐

主要知识产权证明目录（限 10 条）

知识产权类别	知识产权具体名称	国家（地区）	授权号	授权日期	证书编号	权利人	发明人