**会议日程**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **日期** | **时间** | **会议内容** | | **主持人** | **地点** |
| 5月  17日 | 15:00-22:00 | 会议注册报到 | | | 蓝海金港 酒店大厅 |
| 20:00-22:00 | 中国密码学会密码算法专业委员会工作会议 | | 张振峰 | 文理楼 会议室 |
| 5月  18日 | 7:30-9:00 | 会议注册报到 | | | 逸夫礼堂  大厅 |
| 8:30-9:00 | 开幕式 | 2019年密码算法学术会议开幕式 | 闫统江 | 逸夫会议中心二楼 |
| 合影 | 全体会议代表合影 | | 创造太阳 广场 |
| 9:00-9:50 | 特邀报告 | 安全多方计算与隐私数据处理（山东大学，**徐秋亮**） | 张振峰 | 逸夫会议中心二楼 |
| 9:50-10:10 | 茶歇 | | |
| 10:10-11:00 | 特邀报告 | 非线性反馈移位寄存器理论与应用（信息工程大学，**戚文峰**） | 张振峰 |
| 11:00-12:00 | 专题报告 | **1.** Modifying Maiorana-McFarland type Bent Functions for good Cryptographic Properties and Efficient Implementation （作者：**Deng Tang**, Selcuk Kavut, Bimal Mandal, and Subhamoy Maitra）  **2.** ARX 密码算法Pilot （作者：**刘韵雯**，刘国强，仝海鹏，沈璇，李超）  **3.** On the k-error linear complexity of binary sequences derived from the discrete logarithm in finite fields（作者：**陈智雄**，王秋艳） | 吴文玲 |
| 11:30-14:00 | 午餐 | | | 蓝海金港蓝钻自助百汇 |
| 14:00-15:40 | 特邀报告 | **1.** LAC算法设计与实现（中国科学院信息工程研究所，**路献辉**）  **2.** 密钥封装机制的抗量子安全性 （中国科学院软件研究所， **江浩东**） | 丁存生 | 逸夫会议中心二楼 |
| 15:40-16:00 | 茶歇 | | |
| 16:00-17:20 | 专题报告 | **1.** SWAN算法（减轮）的分析（作者：张道法，**姚富**，史晓明，刘仁章，潘文伦）  **2.** BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0  （作者：**Chao Lin**, Debiao He, Xinyi Huang, Kim-Kwang Raymond Choo, and Athanasios V. Vasilakos） | 胡予濮 |
| **3.** AFCoin: A framework for digital fiat currency of central banks based on account model（作者：**Haibo Tian**, Peiran Luo,Xiaofeng Chen, and Fangguo Zhang）  **4.** Blockchain-Based Anonymous Reporting Scheme with Anonymous Rewarding（作者：**Huaqun Wang**, Debiao He, Zhe Liu, and Rui Guo） | 张方国 |
| 17:30-21:00 | 晚餐 | | | 蓝海金港蓝钻自助百汇 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **日期** | **时间** | **会议内容** | | **主持人** | **地点** |
| 5月19日 | 8:30-10:10 | 特邀报告 | **1.** Related-Tweak Statistical Saturation Cryptanalysis and Its  Application on QARMA（山东大学，**王美琴**）  **2.** Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS（中国科学院信息工程研究所，**史丹萍**） | 来学嘉 | 逸夫会议中心二楼 |
| 10:10-10:30 | 茶歇 | | |
| 10:30-11:30 | 专题报告 | **1.** 基于格的原像采样算法的研究与应用（作者：**高媛媛**，王鲲鹏）  **2.** An Efficient Certificateless Aggregate Signature Scheme without Pairings for Healthcare Wireless Sensor Network  （作者：**Hongzhen Du**, Qiaoyan Wen, and Shanshan Zhang）  **3.** Revocable certificateless encryption with ciphertext evolution（作者：**Yinxia Sun**, Futai Zhang, and Anmin Fu） | 胡磊 |
| 11:30-11:50 | 闭幕式 | 2019年密码算法学术会议闭幕式 | 张振峰 |
| 12:00 | 午餐，会议代表散会 | | | 蓝海金港蓝钻自助百汇 |

.