# 会议日程

**第二届密码学与云计算安全国际研讨会（CCCS2014）**

**日 程 表**

会议日期：6月20日-23日

地点：广州市番禺大学城中环西路230号广大商务酒店大堂

会议地点：广州大学行政西楼2楼会议厅

| 时间 | 内容 | 主持人 |
|---|---|---|
| 6月20日 | 报到 | 蔡云鹭 |
| 晚餐 18：00-20：00（北雪湘园） | | |
| 6月21日 | | |
| 7:30-8:30 | 早餐 | |
| 8:30-9:00 | 开幕式、照相 | 唐春明 |
| 主持人：裴定一教授（9：00-10：30） | | |
| 9：00-10：00 | Key Management in Real-World Security Systems | 丁存生（香港科技大学） |
| 10:00-10:30 | 从二次剩余到k次剩余的密码体制 | 曹珍富（上海交通大学） |
| 茶歇：10：30-10：45 | | |
| 主持人：胡磊教授（10：45-12：15） | | |
| 10：45-11：15 | On secret sharing with nonlinear product reconstruction | 邢朝平（南洋理工大学） |
| 11：15-11：45 | How to Collaborate between Threshold Secret Sharing Schemes | 王道顺（清华大学） |
| 11：45-12：15 | How to run the automata in the ciphertext/key spaces under the leakage situation | 张明武（湖北工业大学） |
| 中餐：12：15-13：00 （大学新厨） | | |
| 主持人：林东岱教授（14：00-16：00） | | |
| 14：00-15：00 | Arbitrary-State Attribute-Based Encryption with Dynamic Membership | 范俊逸（台湾中山大学） |
| 15：00-15：30 | Compositional inverces of permutation polynomials over finite fields | 刘卓军（中国科学院数学与系统科学研究院） |

## 会议地点

*广大商务酒店（番禺区大学城中环西路230号）*
*广东科学中心学术交流中心（番禺区大学城西六路168号）*


放大地图:广大商务酒店;广东科学中心学术交流中心

## 联系我们

**联系人: 唐 春 明**

**电话: +86-13342884959**

**传真: +86-20-39366859**

**电子邮箱: ctang@gzhu.edu.cn**

**地址: 广东省广州市番禺区大学城外环西路230号 广州大学数学与信息科学学院**

**邮政编码: 510006**

| | | |
|---|---|---|
| 15：30-16：00 | The weight distributions of two classes of p-ary cyclic codes | 郑大彬（湖北大学） |
| 茶歇：16：00-16：15 | | |
| 主持人：徐茂智教授（16：15-17：45） | | |
| 16：15-16：45 | Some Open Problems and Conjectures in Quantum Integer Factorization | 颜松远（武汉大学） |
| 16：45-17：15 | 抵御量子计算机的新型密码安全性与适用性研究 | 向宏（重庆大学） |
| 17：15-17：50 | A New Method to Compute the 2-Adic Complexity of Binary Sequences | 屈龙江（国防科技大学） |
| 招待晚宴18：00-20：00 （粤园餐厅） | | |
| 6月22日 | | |
| 早餐7:30-8:30 | | |
| 主持人：容淳铭教授（8：30-10：00） | | |
| 8：30-9：30 | 全同态加密的研究 | Shuhong Gao （美国Clemson大学） |
| 9：30-10：00 | Efficient Non-Interactive Verifiable Outsourced Computation for Arbitrary Functions | 陈月乃（广州大学） |
| 茶歇10：00-10：20 | | |
| 主持人：刘卓军教授（10：20-11：50） | | |
| 10：20-10：50 | 基于属性集的加密方案实现与进展 | 朱岩（北京科技大学） |
| 10：50-11：20 | New Publicly Verifiable Databases with Efficient Updates | 陈晓峰（西安电子科技大学） |
| 11：20-11：50 | Secure Cloud Storage Meets with Secure Network Coding | 陈飞（香港中文大学） |
| 11：50-12：05 | 电子政务PaaS平台及其安全应用技术研究 | 刘镭（广东数字证书认证中心有限公司） |
| 中餐12：15-13：00 （大学新厨） | | |
| 主持人：赵淦森教授（14：00-16:00） | | |
| 14：00-15：00 | 可信的云计算 | 赵波（武汉大学） |
| 15：00-15：30 | SNARKS and Its Application to Delegation of Computation | 赵运磊（复旦大学） |
| 15：30-16：00 | 云数据安全审计理论模型与新方法探讨 | 郑相涵（福州大学） |
| 茶歇：16：00-16：20 | | |
| 主持人：杨中皇教授（16：20-17：50） | | |
| 16：20-16：50 | On a conjecture for the girth of the bipartite graph D(k,q) | 唐元生（苏州大学） |
| 16：50-17：20 | A matrix approach for constructing quadratic APN functions | 余玉银（广州大学） |

| | | |
|---|---|---|
| 17：20-17：50 | Memory Leakage-Resilient Searchable Symmetric Encryption | 代署光（中山大学） |
| 晚餐 18：00-19：00（北雪湘园） | | |
| 6月23日：专家返回 | | |