

中国密码学会 2017 年青年论坛通知

为促进我国密码学青年学者的交流与合作，中国密码学会 2017 年青年论坛将于 2017 年 5 月 17 日在北京万寿庄宾馆召开。本次会议由中国密码学会青年工作委员会主办，中国科学院软件研究所可信计算与信息保障实验室承办。会议届时将邀请 9 位在密码学各研究领域的优秀青年学者作报告，旨在为从事密码研究的广大青年学者、技术人员和在校研究生提供学术交流合作平台。现将会议有关事项通知如下：

主办单位：中国密码学会青年工作委员会

承办单位：中国科学院软件研究所可信计算与信息保障实验室

会议时间：2017 年 5 月 17 日

会议地点：北京市海淀区万寿路西街 7 号万寿庄宾馆

会议报到：2017 年 5 月 16 日 16:00-22:00，5 月 17 日 7:00-8:00

组织方式：会议以特邀报告和自由论坛为主，会期一天，不接受征文

会议报名：请于 5 月 10 日前填写报名回执表（见附件 2），并通过邮件

反馈 baikunpeng@tca.iscas.ac.cn

注册费：通过银行汇款或现场刷卡方式交纳

密码学会已缴费会员 960 元/人，学生：860 元/人

其他：1060 元/人

户名：中国密码学会

开户行：中国工商银行北京公主坟支行

账号：0200 1864 1920 0001 727

注意：请在汇款附言中写清楚会议名称“青年论坛+姓名”（若有多人同时缴费，则写清楚全部缴费人员姓名）。

交费凭证发：cacr02@cacrnet.org.cn

财务联系人：贺老师：010—59703621

会议住宿：会议提供北京万寿庄宾馆住宿，费用自理。

标间：460 元/天（含双早）；单间：440 元/天（含单早）。

会务工作联系方式：

白琨鹏 15201306046, baikunpeng@tca.iscas.ac.cn

张奕芝 13810258429, zhangyizhi@tca.iscas.ac.cn

附：1. “中国密码学会 2017 年青年论坛”议程

2. “中国密码学会 2017 年青年论坛”回执

3. 北京万寿庄宾馆路线

中国密码学会青年工作委员会

2017年4月28日



附件 1:

“中国密码学会 2017 年青年论坛”议程

| 序号 | 报告人 | 题目 |
|----|---------------------|--|
| 1 | 邓焱 中国科学院信息工程研究所 | Magic Adversaries Versus Individual Reduction: Science Wins Either Way |
| 2 | 张江 密码科学技术国家重点实验室 | 基于格的短签名设计 |
| 3 | 陈荣茂 国防科学技术大学 | Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions |
| 4 | 喻杨 清华大学 | 可证明安全 NTRU 加密体制的研究 |
| 5 | 陈宇 中国科学院信息工程研究所 | Non-Malleable Functions and Their Applications |
| 6 | 杨糠 中国科学院软件研究所 | Anonymous Password Authentication with Applications to Privacy-Preserving TLS |
| 7 | 王安宇 中国科学院信息工程研究所 | 分布式存储系统中可并行局部修复码的构造 |
| 8 | 郑群雄 解放军信息工程大学 | 基于不同代数结构设计大周期二元非线性 序列 |
| 9 | 李新宇 中国科学院软件研究所 | TLS 握手机制安全模型及其在下一代 TLS 标准中的应用 |
| 10 | 自由论坛: 密码货币与新型密码 | |