会 议 日 程

10 月 19 日	星期六	
上午	**8:00-16:00**	会议签到（三层多功能厅）
	8:50-09:00	开幕式、领导致辞
	9:00-09:15	参会人员合影
	9:20-10:10	特邀报告 1：哈希证明系统与 CCA 安全的公钥加密（刘胜利 教授）
	10:10-10:30	休息
	10:30-11:20	特邀报告 2：超导量子计算（朱晓波 教授）
	11:20-12:10	特邀报告 3：Space-Depth Tradeoff of CNOT circuits（孙晓明 研究员）
	12:10-13:40	午餐（三层咖啡厅）
下午	**13:40-14:30**	特邀报告 4：Searchable Encryption: Recent Progress and Beyond（王骞 教授）
	14:30-15:20	特邀报告 5：支持删除操作的数字签名（黄欣沂 教授）
	15:20-15:40	休息
	15:40-16:30	特邀报告 6：A Timing Side-Channel Attack on Deep Neural Networks（胡红钢 教授）
	16:30-17:20	特邀报告 7： 格密码体制攻击方法综述（郑中翔 博士）
	18:00 -19:30	晚餐（三层咖啡厅）
10 月 20 日	星期日	
上午	**9:00-09:50**	特邀报告 8：对称密码算法的新型分析与设计方法（王美琴 教授）
	9:50-10:10	休息
	10:10-11:00	特邀报告 9：杂凑函数 RIPEMD-160 的安全性分析（王高丽 教授）
	11:00-11:50	特邀报告 10：Boomerang Connectivity Table and Boomerang Distinguishers（宋凌 副研究员）
	11:50-13:40	午餐（三层咖啡厅）
下午	**13:40-14:30**	特邀报告 11：A Brief Survey on Secure Multiparty Computation（邢朝平 教授）
	14:30-15:20	特邀报告 12：Valiant's Universal Circuits Revisited: an Overall Improvement and a Lower Bound（郁昱 教授）
	15:20-15:40	休息
	15:40-16:30	特邀报告 13：非线性反馈移位寄存器串联结构综述（田甜 副教授）
	16:30-17:20	特邀报告 14：非线性反馈密码系统安全性分析（刘美成 副研究员）