

会议日程

2013年7月20日

8:50—9:00	973 项目首席科学家致辞	
9:00—10:20	Chair: Daqing Wan	
9:00—9:40	Shuhong Gao (Clemson University)	Solving polynomial systems from cryptography
9:40—10:20	王明生 (中国科学院信息工程研究所)	多输出布尔函数的代数免疫度的刻画
10:20—10:40	茶 歇	
10:40—12:00	Chair: Shuhong Gao	
10:40—11:20	Daqing Wan (University of California)	Rational points on Kloosterman hypersurfaces
11:20—12:00	冯荣权 (北京大学)	待定
12:00—13:00	午 餐 (雅谷西餐厅)	
14:30—15:50	Chair: 王明生	
14:30—15:10	Qiang Wang (Carleton University)	Permutation Polynomials over finite fields
15:10—15:50	曾祥勇 (湖北大学)	Several Classes of Complete Permutation Polynomials
15:50—16:10	茶 歇	
16:10—18:00	Chair: 王丽萍	
16:10—16:50	陆玫 (清华大学)	The linear guessing number of directed graphs
16:50—17:30	曹喜望 (南京航空航天大学)	On expander graphs and Cayley graphs
17:30—18:00	李永强 (中国科学院信息工程研究所)	$GF(2^{2n})$ 上 4 差分均匀置换的构造
18:00—20:00	晚 宴	

2013年7月21日

8:30—9:40	Chair: Qiang Wang	
8:30—9:10	张晓东（上海交通大学）	A Novel Class of Reciprocal-orthogonal Jacket Transformation With Many Parameters
9:10—9:40	黄振宇（中国科学院信息工程研究所）	布尔非线性含错方程组求解及其应用
9:40—10:00	茶 歇	
10:00—11:30	Chair: 冯荣权	
10:00—10:30	孙瑶（中国科学院信息工程研究所）	推广的 GVW 算法
10:30—11:00	单进勇（中国科学院信息工程研究所）	Algebraic Immunities of Nested Functions and the Boolean Function in Hitag2 Stream Cipher
11:00—11:30	宋凌（中国科学院信息工程研究所）	PRINCE is a new lightweight block cipher proposed
11:30—11:40	总 结	
12:00—13:00	午 餐	
下午	自由讨论	

2013年7月22日

上午	自由讨论、离开会场
----	-----------