有限自动机的可逆性

关 键 词：有限自动机　公开钥密码体制　密码分析

所属年份：2001	成果类型：基础理论
所处阶段：	成果体现形式：论文
知识产权形式：	项目合作方式：
成果完成单位：中国科学院软件研究所	

成果摘要：

在有限自动机可逆性理论的基础上，提出了拟线性有限自动机的概念，并用RaRb变换解决了拟线性自动机的可逆性判别、求逆和结构等基本问题。 有限自动机的理论研究成果丰硕，基于有限自动机可逆性理论的密码体制理论基础坚实，所设计的FAPKC3体制构思巧妙、抗攻击能力强、密钥参量适中、易于软硬件实现、速度快、使用方便。在有限自动机可逆性理论及其在密码应用上处于国际领先水平，FAPKC3具有广泛应用前景。

成果完成人：陶仁骥;陈世华

完整信息

推荐成果

· 液压负载模拟器	04-23
· 新一代空中交通服务平台、关...	04-23
· Adhoc网络中的QoS保证(Wirel...	04-23
· 电信增值网业务创意的构思与开发	04-23
· 飞腾V基本图形库的研究与开发...	04-23
· ChinaNet国际(国内)互联的策...	04-23
· 电信企业客户关系管理(CRM)系...	04-23
· “易点通”餐饮管理系统YDT2003	04-23
· MEMS部件设计仿真库系统	04-23

行业资讯

新疆综合信息服务平台
准噶尔盆地天然气勘探目标评价
维哈柯俄多文种操作系统FOR ...
社会保险信息管理系统
塔里木石油勘探开发指挥部广...
四合一多功能信息管理卡MISA...
数字键盘中文输入技术的研究
软开关高效无声计算机电源
邮政报刊发行订销业务计算机...
新疆主要农作物与牧草生长发...

成果交流