山大四教授获08年度国家自然科学奖二等奖

2009-01-10 20:28

［本站讯］2009年1月9日，2008年度国家科学技术奖励大会在北京人民大会堂隆重举行。中共中央总书记、国家主席、中央军委主席胡锦涛等国家领导人出席奖励大会并为获奖人员颁奖。山东大学王小云教授研究的“国际通用Hash函数的破解”项目获国家自然科学奖二等奖，另外由山东大学药学院张建教授、控制科学与工程学院张焕水教授和王玉振教授各自分别位列第四完成人参与研究的3个项目也获得国家自然科学奖二等奖。国家自然科学奖一等奖继2007年度空缺后本年度再次出现空缺。

Hash函数是现代密码学三类基础密码算法之一，是电子签名和身份认证的关键技术。王小云教授创建了国际通用Hash函数分析与破解的系统理论体系，成功破解了系列国际通用Hash函数算法MD4、SHA-0、HAVAL、RIPEMD、MD5与SHA-1，解决了“Hash函数标准MD5与SHA-1碰撞难”两大科学问题，动摇了Hash函数及相关密码应用的理论根基。为此美国国家标准技术所NIST发表了多次正式评论、公布了新的数字签名政策以及组织国际密码领域开始了长达5年的新的Hash函数算法设计计划。该研究成果的4篇论文被授予2005年最佳论文，并囊括了密码领域最权威年会欧密会与美密会的最佳论文。此项目的另一位获奖人于红波系王小云教授的博士生。

王小云教授，女，1966年出生，中国致公党党员。曾获2006年陈嘉庚科学奖、求是杰出科学家奖、中国青年女科学家奖以及中国青年科学家提名奖。

根据《国家科学技术奖励条例》的规定，经国家科学技术奖励评审委员会评审、国家科学技术奖励委员会审定和科技部审核，国务院批准并报请国家主席胡锦涛签署，授予王忠诚、徐光宪两位院士2008年度国家最高科学技术奖；2008年度国家自然科学奖二等奖授奖项目34项；国家技术发明奖授奖项目55项，其中一等奖3项、二等奖52项；国家科学技术进步奖授奖项目254项，其中特等奖3项、一等奖26项、二等奖225项；授予3名外籍科学家中华人民共和国国际科学技术合作奖。

{作者:刘杰　来自:科技处　编辑:新闻中心总编室　责任编辑:张青}

■ 发表评论

你的称呼 （注：可以不填，不填视为匿名）

发送 重填 查看评论