张焕国

教授

武汉大学
计算机学院

教师简介

张焕国，男，1945.6出生，武汉大学计算机学院教授，博士生导师。主要从事信息安全、可信计算和容错计算方面的研究和教学。担任中国密码学会常务理事，中国计算机学会容错计算专业委员会委员委员，中国电子学会计算机取证专家委员会副主任，教育部信息安全类专业教学指导委员会副主任，湖北省电子学会副理事长，湖北省暨武汉市计算机学会理事，《中国科学》杂志（信息科学版）编委。

⑴ 简历

1964.8 - 1970.7 在西安军事电信工程学院无线电工程系无线电通信专业学习；

1970.8 - 1975.7 在西北电讯工程学院通信研究室，参加“流星余迹通信”研究工作。

1975.8 - 在武汉大学计算机学院任教，主要从事信息安全、密码学、可信计算和容错计算方面的研究和教学。

⑵ 论著

发表学术论文100多篇，著作和译作12部。

⑶ 获奖

[1]张焕国、黄传河、王丽娜、刘玉珍、许卫平，信息安全专业课程体系与人才培养研究，湖北省教学研究成果一等奖，2005。

[2]张焕国、刘毅、韩永桥、毋国庆、覃中平、周强、余发江，SQY-14嵌入密码型计算机，密码科技进步二等奖，2006。

[3]王新梅、张焕国，计算机中的纠错编码技术，人民邮电出版社，全国优秀科技图书三等奖，2001。

⑷ 教学科研成果

① 创建信息安全专业

作为学术带头人创建了全国第一个“信息安全”本科专业、“信息安全”硕士点、博士点和博士后流动站，在武汉大学形成了信息安全人才培养的完整体系。

2006年武汉大学的信息安全本科专业获“湖北省品牌专业”，2007年又获“国家特色专业建设点”。

② 主持制定教育部信息安全专业指导性专业规范

受教育部委托，主持制定了我国第一个“信息安全专业指导性专业规范”。

⑸ 科研成果

1、密码学研究成果：

⑴在抗量子计算密码方面，取得如下阶段性成果：

①提出了一种密码加扰方法，对对欧盟签名标准算法SPLASH进行了改进，改进后的SPLASH可以抵抗已有攻击。

②基于多变量问题，提出了一种扩展多变量Hash函数的构造方法。

③借鉴有理分式密码单向函数链的思想，对MQ密码进行了扩展，构造了一种新的扩展MQ密码，其特点是具有安全的加密和签名功能。

④申请了4项国家发明专利。

⑤发表高质量学术论文十几篇。

⑵提出演化密码的概念和用演化密码的思想实现密码设计自动化和密码分析自动化的方法，并在演化密码体制，演化密码芯片、密码函数的演化分析与设计（如Bent 函数、正型置换），密码部件设计自动化（S盒，P置换和轮函数）以及密码的演化分析等方面获得实际成功，部分研究成果处于国际领先水平。

出版学术专著（国家十一五重点图书）：张焕国，覃中平等著.演化密码引论，武汉大学出版社，2010.

⑶对有限自动机公钥密码（FAPKC）的安全性理论有较深入的研究，成功地破译了FAPKC0和FAPKC3的一个实例，发展了FAPKC的安全理论。

⑷提出变长检错码的概念，并将其用于计算机病毒检测，效果良好。

⑸对纠字节错误码理论有较系统的研究，部分成果用于银河Ⅱ计算机。

2、可信计算研究成果

①与企业合作研制出我国第一款“可信计算机”，通过了国家鉴定。国家科技部等四部委联合授予“国家级重点新产品”，获“国家密码科技进步二等奖”。这一产品在中央办公厅、各级政府部门和军队得到实际应用。

②在国家863计划项目的支持下，研制出我国第一款可信PDA。

③在国家863计划项目的支持下，研制出我国第一个可信计算平台测评系统。

④参加制定了我国一系列可信计算技术标准。

⑤与美国HP公司、EMC公司合作，开展基于可信计算增强网格安全的研究。HP公司评价认为：取得了国际学术界与工业界认可的成果。

⑥出版学术专著（国家十一五重点图书）：张焕国，赵波，等著.可信计算，武汉大学出版社，2010。

3、信息安全应用研究成果

与企业合作研制出多种信息安全产品，为企业产生了很大的经济效益。