



山西师范大学

SHANXI NORMAL UNIVERSITY 数学与计算机科学学院

学术报告

2016年5月5日(周四)上午9:00

科学会堂 A710

信息安全理论与技术



蔡永泉

北京工业大学教授、博士生导师

报告人简介:

蔡永泉, 北京工业大学教授、博士生导师, 北京工业大学信息安全交叉学科带头人, 《Chinese Journal of Electronics》、《电子学报》等期刊编委会委员, 密码学会密码普及专业委员会委员。主持和参与国家“863”、“973”、国家自然科学基金和北京市自然科学基金项目等科研项目10多项, 获得国家专利4项、软件著作权16项, 出版专著3部。在国内外期刊上发表有关信息安全的文章53篇, 其中被SCI检索11篇, 被EI检索27篇。

报告摘要:

该报告将围绕网络用户 A 如何在一个不安全的计算网络上将信息 M 如何安全的传输给用户 B 这个主线讲述单密钥加密体制、双密钥加密体制、数字签名技术和信息完整性鉴别技术、相互鉴别技术, 最后介绍对等网 SKYPE 的安全协议。

欢迎广大师生参加!