
# 韦永壮 教授 (walker_wyz@guet.edu.cn)

计算机与信息安全学院

研究领域：对称密码算法设计与分析、加密芯片侧信道攻击与防御技术、网络安全协议分析等


## 个人简介

韦永壮，男，博士，教授，博士生导师。

目前主持（在研）项目：国家自然科学基金（面上）项目、广西自然科学基金杰出青年基金项目等。

近几年在《IEEE Transactions on Information Theory》等国内外重要学术期刊和会议发表学术论文50余篇，其中多篇被SCI检索或EI检索。

## 教育背景

2004年毕业于西安电子科技大学获密码学专业（工学）硕士学位；

2009年毕业于西安电子科技大学获密码学专业（军事学）博士学位；

2011年至2015年间：曾在中国科学院软件研究所从事博士后研究、获国家留学基金委项目资助到赫瑞瓦特大学（英国）进行一年的学术访问。

## 工作经历

## 主要荣誉

2014年入选“广西高等学校优秀中青年骨干教师培养工程（第2期）”成员。

2015年获得广西自然科学基金杰出青年基金项目资助。

2016年度桂林电子科技大学优秀硕士学位论文指导教师。

## 学术活动

主要学术兼职：中国密码学会算法专委会委员、美国数学杂志《数学评论》(Mathematical Reviews)评论员等。

担任国内外期刊：《Information Sciences》、《IEEE Transactions on Wireless Communications》等的审稿人。

## 教学信息

《信息编码与加密》、《密码算法与设计》、《计算机网络》、《通信网的保密技术》

## 主要论文

**代表性论文：**


[1]**Yongzhuang Wei**, Enes Pasalic, Yupu Hu. A new correlation attack on nonlinear combining generators. ***IEEE Transactions on Information Theory***, 57(9): 6321-6331, 2011. (**IF: 3.009**)

[2]**Yongzhuang Wei**, Enes Pasalic, Yupu Hu. Guess and determine attacks on filter generators-revisited. ***IEEE Transactions on Information Theory***, 58(4): 2530-2539, 2012.

[3]Enes Pasalic, **Yongzhuang Wei**. On the construction of cryptographically significant Boolean functions using objects in projective geometry spaces. ***IEEE Transactions on Information Theory***, 58(10): 6681-6693, 2012.

[4]Fengrong Zhang, **Yongzhuang Wei**, Enes Pasalic. Constructions of bent—negabent functions and their relation to the completed Maiorana-MCFarland class. ***IEEE Transactions on Information Theory***, 61(3): 1496-1506, 2015.

[5] Fengrong Zhang, Enes Pasalic, **Yongzhuang Wei**, Nastja Cepak. Constructing Bent Functions Outside the Maiorana-McFarland Class Using a General Form of Rothaus. ***IEEE Transactions on Information Theory***, 63(8): 5336-5349, 2017.

[6] Fengrong Zhang, **Yongzhuang Wei***, and Enes Pasalic, et al. Large sets of disjoint spectra plateaued functions inequivalent to partially linear functions, ***IEEE Transactions on Information Theory***, DOI (identifier) 10.1109/TIT.2018.2795608

[7] **Yongzhuang Wei**, Enes Pasalic, Fengrong Zhang, Samir Hodzic. Efficient probabilistic algorithm for estimating the algebraic properties of Boolean functions for large n. ***Information Sciences***. 402(9): 91-104, 2017.(**IF：4.832**)

[8] **Yongzhuang Wei**, Enes Pasalic, Fengrong Zhang, Wenling Wu, Cheng-xiang Wang. New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions, ***Information Sciences***, 415–416(11): 377-396, 2017. (**IF：4.832**)

[9] **Yongzhuang Wei**, Wenbin Yin, Enes Pasalic, Fengrong Zhang. On algebraic properties of S-boxes designed by means of disjoint linear codes. ***International Journal of Computer Mathematics***, 93(1): 55-66(12), 2016. (**SCI**)

[10] **Yongzhuang Wei**, Enes Pasalic. On the approximation of S-boxes via Maiorana -McFarland functions. ***IET Information Security***,7(2): 134-143, 2013. (**SCI**)

[11] **WEI YongZhuang**, HU YuPu. New related-key rectangle attacks on reduced AES-192 and AES-256. ***Sci China Ser F-Inf Sci*** (中国科学F辑信息科学(英文)), 52(4): 617-626, 2009. (**SCI**)

## 学术著作

## 科研项目

**在研的部分项目：**

[1]“密码核心部件新型分解方法及应用研究”，国家自然科学基金（面上项目），2016.01-2019.12.

[2] “密码学与信息安全”, 广西自然科学基金（杰出青年基金）项目, 2015.09-2018.08.

## 知识产权

专利申请与授权：

[1] 非线性挤压保护密码S盒的方法，发明专利，授权号：201410784299.4.

[2] 变元分解限门掩码新方法,发明专利，申请号：CN201611265089.X

[3] 密码S盒评估新方法，发明专利，申请号：CN201611265264.5.

[4] 密钥可变的内轮置换流密码加密方法，发明专利，授权号：201310099408.4.

[5] 4个非线性驱动的轻量级流密码加密方法, 发明专利，授权号：201310098768.7.

## 联系信息

电子邮箱：

walker_wyz@guet.edu.cn

或 walker_wei@msn.com

## 常用链接