基本信息

姓名：张顺生

性别：男

出生年月：1994-08

籍贯：广东梅州

政治面貌：中共党员

电话：15078329621

邮箱：shunszhang@gxnu.edu.cn

外语情况

英语：CET-6(446 分)

获奖情况

1. 2021 年广西师范大学优秀毕业生；
2. 2021 年广西师范大学“十佳学术之星”（全校只有 10 人）；
3. 2020 年国家奖学金；
4. 2020 年广西师范大学三好学生；
5. 2020 年第十一届全国蓝桥杯大赛嵌入式设计与开发广西壮族自治区二等奖
6. 2015-2017 年本科期间连续两年获得国家励志奖学金；
7. 2017 年 6 月获得韶关学院第六届大学生数学竞赛二等奖；
8. 2015-2016 年获得韶关学院三等“优秀奖学金”；
9. 2016 年 10 月获得第七届广东省大学生物理实验设计大赛二等奖和三等奖；
10. 2015-2016 年获得韶关学院“科技创新先进个人；
11. 2015-2016 年获得韶关学院“优秀学生干部”。

个人简历

教育背景

2014.09-2018.06，韶关学院，物理与机电工程学院，物理学专业获学士学位；

2018.09-2021.06，广西师范大学，电子工程学院，电子与通信工程专业获硕士学位。

工作经历

2021.07-至今，广西师范大学，党委教师工作部/人事处，负责学校人事系统信息化建设。

主要研究方向 ： 侧信道攻击、人工智能安全

1.针对 Feistel 结构的混沌分组密码系统，设计一种基于多采样点的相关能量分析攻击。其中包括密码系统攻击点的分析和选择、能量映射模型的选择，给出了基于多兴趣点的能量分析攻击的工作原理，从理论和实际上分析了基于多采样点的相关能量分析攻击的正确密钥区分度。

2.针对 SP 结构的混沌分组密码系统，设计一种基于最大似然准则的模板攻击和一种基于机器学习的相似度攻击。从能量痕迹数量、成功率、攻击成本的角度，分析对比基于最大似然准则的模板攻击和基于机器学习的相似度攻击的性能。

3.针对 AES 分组密码系统，设计一种基于马氏距离的随机攻击方法，该方法克服随机模型和传统模板攻

参与科研项目

1.2020 年广西壮族自治区研究生创新项目 （项目编号：YCSW20201 00；省部级；课题名称：一种基于旁路攻击的混沌分组加密分析研究；第一主持人，已结题）

2.2020 年广西壮族自治区研究生创新项目 （项目编号：YCSW20201 02；省部级；课题名称：基于神经网络的脑电信号情感分类应用研究；第五参与人；已结题）

3.2021 年广西自然科学基金项目（面上项目；项目编号：2021JJA170174；课题名称：基于深度学习的分组密码硬件系统安全分析；第五参与人，项目书主要由本人撰写；在研）

相关成果

[1] Yuling Luo, **Shunsheng Zhang**, Junxiu Liu, and Lvchen. Cao, “ Cryptanalysis of a Chaotic Block Cryptographic System against Template Attacks”, International Journal of Bifurcation and Chaos, 30(15):1-15, 2020.（ 导师第一作者，本人第二作者，SCI 源刊 ， 已见刊）

[2] Dezheng Zhang, **Shunsheng Zhang**, Yuling Luo, and Lvchen Cao,“Cryptanalyzing a Feistel chaotic block cryptosystem using correlation power analysis,” International Journal of Bifurcation and Chaos. [SCI 源刊，与课题组老师共同第一作者，已录用]

[3] Junxiu Li, **Shunsheng Zhang**, Yuling Luo, and Lvchen. Cao, Machine Learning-Based Similarity Attacks for Chaos-based Cryptosystems, IEEE Transactions on Emerging Topics in Computing, 10(2):1-14, 2021. （ SCI 源刊，与课题组老师共同第一作者，已见刊）

[4] **Shunsheng Zhang**, Yuling Luo, Lvchen. Cao, and Junxiu Liu, “Cryptanalysis of a Chaos-based Block Cryptosystem Using Multiple Samples Correlation Power Analysis,”in 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1-15, Guangzhou, China, 29 Dec 2020 – 1 Jan 2021. (本人第一作者，CCF C 类会议，已见刊）

[5] **张顺生**, 罗玉玲, 丘森辉, “面向 AES 密码硬件系统的马氏距离随机旁路攻击方法”, 广西师范大学学报（自然科学版）36(6):1-12, 2021. （本人第一作者，中文核心，已见刊）

[6] 罗玉玲, **张顺生**, 刘俊秀, 丘森辉, 岑明灿, 蔡超波, 一种基于模板攻击的混沌分组加密分析方法,中国国家发明专利, 专利号 ZL201911016102.1.[导师第一作者，本人第二作者，已授权]

[7] Yuling Luo, Shuming Han, **Shunsheng Zhang**, Yanhu Wang and Junxiu Liu,“High Speed True Random Number Generator Controlled by Logistic Map,”HPCC 2021: International Conference on High Performance Computing and Communications. [独自通信作者，CCF C 类会议，已录用]

[8] Yuling Luo, Ce Liang, **Shunsheng Zhang**, and Sheng Qin, “A Combined Features Encoding Network with Semantics Enhancement for Image Tampering Forensics,” 18th IFIP WG 11.9 International Conference on Digital Forensics. [独自通信作者，CCF C 类会议，已录用]

[9] Junxiu Liu, Shunsheng Zhang, et. al,“Mahalanobis Distance-based Template Attacks against Chaotic Block Cryptosystem,”IEEE Transactions on Cybernetics. [SCI 刊源，共同第一作者，一审投稿中]