高思

个人信息

出生日期 1989 年 2 月 5 日

移动电话 18810459901

Email si-gao@outlook.com

通讯地址 Flat 6, Jesserniggstraße 10. 9020 Klagenfurt am Wörthersee, Austria

教育/工作背景

2019 至今 **博后**, 克拉根福大学, 奥地利.

研究方向: 密码实现，嵌入式安全，侧信道分析

2017–2019 **博后**, 计算机科学系, 英国布里斯托大学.

PI: Prof. Elisabeth Oswald

2011–2017 **计算机应用技术, 硕博连读**, 中国科学院软件研究所.

研究方向：可信计算与信息保障

导师: 吴文玲研究员

学位论文题目: “灰盒模型”下的密码模块实现安全性分析

2007–2011 **计算机科学技术, 本科**, 武汉大学计算机学院.

专业: 信息安全

GPA 排名– 1/90

教学

2019 助教, *Applied Security*.
英国英国布里斯托大学

开源项目/小工具

ELMO ARM M0 泄漏模拟器 ELMO 的维护与改进
https://github.com/sca-research/ELMO

DPAdemo 教学用能量分析示例
https://github.com/gs1989/DPAdemo

曲线采集 Lecroy 示波器采集脚本 (python)
https://github.com/gs1989/Trace-Acquisition-for-Lecroy
Picoscope 采集工程 (c#)
https://github.com/gs1989/AcquisitionProject

COSMIC 开源软件掩码实现汇总
https://github.com/sca-research/COSMIC 包含
基于 Thumb 汇编的字节级 AES 掩码实现
https://github.com/sca-research/ASM_MaskedAES
针对 Virginia Tech 的 AES 开源掩码实现的分析与评估
https://github.com/gs1989/Masked-AES-Implementation

RISC-V 掩码实现 在使用/不使用指令集扩展条件下 RISC-V 掩码实现范例
https://eprint.iacr.org/2020/773

论文发表列表

CHES 20 Si Gao, Ben Marshall, Dan Page, Elisabeth Oswald. *Share-slicing: Friend or Foe?* IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020(1): 152-174 (2020)

CHES 20 Si Gao, Ben Marshall, Dan Page, Thinh Hung Pham. *FENL: an ISE to mitigate analogue micro-architectural leakage*. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020(2): 73-98 (2020)

RSA 19 Si Gao, Arnab Roy, Elisabeth Oswald. *Constructing TI-Friendly Substitution Boxes Using Shift-Invariant Permutations*. CT-RSA 2019: 433-452

CARDIS 18 Si Gao, Elisabeth Oswald, Hua Chen, Wei Xi. *Non-profiled Mask Recovery: The Impact of Independent Component Analysis*. CARDIS 2018: 51-64

FSE 17 Zhiyuan Guo, Renzhang Liu, Si Gao, Wenling Wu, Dongdai Lin. *Direct Construction of Optimal Rotational-XOR Diffusion Primitives*. IACR Trans. Symmetric Cryptol. 2017(4): 169-187 (2017)

RSA 17 Si Gao, Hua Chen, Wenling Wu, Limin Fan, Weiqiong Cao, Xiangliang Ma. *My Traces Learn What You Did in the Dark: Recovering Secret Signals Without Key Guesses*. CT-RSA 2017: 363-378

CANS 16 Si Gao, Hua Chen, Wenling Wu, Limin Fan, Jingyi Feng, Xiangliang Ma.*Linear Regression Attack with F-test: A New SCARE Technique for Secret Block Ciphers*. CANS 2016: 3-18

ICISC 16 Jingyi Feng, Hua Chen, Si Gao, Limin Fan, Dengguo Feng: *Improved Fault Analysis on the Block Cipher SPECK by Injecting Faults in the Same Round*. ICISC 2016: 317-332

SAC 15 Zhiyuan Guo, Wenling Wu, Si Gao: *Constructing Lightweight Optimal Diffusion Primitives with Feistel Structure*. SAC 2015: 352-372

CANS 13 Si Gao, Hua Chen, Limin Fan: *Padding Oracle Attack on PKCS#1 v1.5: Can Non-standard Implementation Act as a Shelter?* CANS 2013: 39-56