Si Gao

Personal Information

Gender	Male
Date of Birth	5th February,1989
Place of Birth:	Tianjin, China
Email	si-gao@outlook.com
Work Address	Digital Age Research Center (D!ARC), Universität Klagenfurt Universitätsstraße 65-67, Klagenfurt 9020, Austria
Home Address	Flat 6, Jesserniggstraße 10. 9020 Klagenfurt am Wörthersee, Austria.

Education& Work Experience

2019.12–present **Postdoc**, *Alpen-Adria-Universität Klagenfurt, Austria*.
Research Interests: Cryptographic implementations, Side Channel Analysis, Embedded Security

2017.7–2019.12 **Research Associate**, *Department of Computer Science, University of Bristol*.

2011.9–2017.6 **PhD, Computer Science**, *Institute of Software, Chinese Academy of Sciences*.
Computer Application Technology
Thesis: Security evaluation of cryptographic modules in a 'Gray-box' model

2007.9– 2011.6 **BS, Computer Science**, *School of Computer Science, Wuhan University*.
Information Security
Thesis: Research and Design of Unknown Nonlinear Cryptographic Component Analysis based on DPA

Open Projects & Utilities

ELMO Maintaining/Refining the ARM M0 simulator ELMO
https://github.com/sca-research/ELMO

DPAdemo A demo of power analysis for education purpose
https://github.com/gs1989/DPAdemo

Trace Acquisition Acquisition script (python) for Lecroy oscilloscope
https://github.com/gs1989/Trace-Acquisition-for-Lecroy
Acquisition project (c#) for Picoscope
https://github.com/gs1989/AcquisitionProject

COSMIC a Complication of Open-Source Masked Implementations for Crypto-software
https://github.com/sca-research/COSMIC inc.
A Thumb Assembly based Byte-wise Masked AES implementation
https://github.com/sca-research/ASM_MaskedAES
Evaluation/analysis of the masked AES implementations from Virginia Tech
https://github.com/gs1989/Masked-AES-Implementation

RISC-V with masking Software masking scheme with/without instruction set extension on RISC-V
https://eprint.iacr.org/2020/773

Publication List

CHES 21 Si Gao, Johann Großschädl, Ben Marshall, Dan Page, Thinh Pham, Francesco Regazzoni. *An Instruction Set Extension to Support Software-Based Masking* IACR Trans. Cryptogr. Hardw. Embed. Syst. 2021(4): xxx-xxx (2021)

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

Awards

2010 **National Undergraduate Electronic Design Contest, third prize**.

2010 **National Undergraduate Information Security Contest, second prize**.