Wei CHENG

Curriculum Vitae

Research Interests

- Applied cryptography, Information theory, Embedded system security, Side-channel analysis (SCA), Fault injection analysis (FIA)
- Side-channel countermeasure, Code-based masking scheme, Combined protection against SCA and FIA, Secure crypto impl. (incl. post-quantum ciphers)

Educations

Sep, 2018 – Dec, 2021 **Ph.D. degree**, *Télécom Paris & Institut Polytechnique de Paris*, Paris, France.
Subject: "What Can Information Guess? Towards Information Leakage Quantification in Side-Channel Analysis"

Sep, 2014 – Jul, 2017 **Master degree**, *University of Chinese Academy of Sciences (UCAS)*, Beijing, China.
Subject: "Differential Fault Analysis on Midori & SM4 and Countermeasures"

Sep, 2010 – Jun, 2014 **Bachelor degree**, *Wuhan University*, Wuhan, China.
Subject: "Dynamic Taint Analysis on Android Applications"

Ph.D Thesis

Title ***What Can Information Guess?*** *Towards Information Leakage Quantification in Side-Channel Analysis* Online link: HAL

Supervisors Prof. Olivier Rioul, Prof. Sylvain Guilley and Prof. Jean-Luc Danger

Best Thesis Award (1st) from ICE Dept., Institut Polytechnique de Paris (2022)

Work Experience

Jun, 2022 – Present **Associate Researcher (Invited)**, *LTCI, Télécom Paris & Institut Polytechnique de Paris*, Paris, France.

May, 2022 – Present **Postdoc R&D Researcher**, *Secure-IC S.A.S.*, Paris, France.

Jul, 2017 – Aug, 2018 **Research Engineer**, *Institute of Information Engineering, Chinese Academy of Sciences*, Beijing, China.

Recognitions & Prizes

Jun, 2022 ***Best Ph.D Thesis Award (1st)*** from ICE (Information, Communications and Electronics) Department, Institut Polytechnique de Paris

19, place Marguerite Perey – F-91123 Palaiseau (Paris), France
✉ *wei.cheng AT telecom-paris.fr*
https://perso.telecom-paristech.fr/wcheng/

2020 & 2021 Twice Finalists of CSAW *Applied Research Competition*

Feb, 2021 Nomination of *Best Paper Award* (1-out-of-4) in T-Track of DATE 2021

Dec, 2019 *Best Poster Award* during *Journée de l'ED IP Paris 2019* in the domain of ICE (Information & Communications & Electronics), Institut Polytechnique de Paris

2016 & 2017 *Two Best Proposals* against protected AES-128 impl., submitted to DPA Contest v4.2, that is held by Télécom ParisTech, France.

Selected Publications — Refer to *Google Scholar* for all publications

Journal Papers

IEEE TIFS, 2022 IF: 7.231 Jingdian Ming, Yongbin Zhou, **Wei Cheng**, and Huizhong Li. Optimizing Higher-Order Correlation Analysis against Inner Product Masking Scheme. IEEE Trans. Inf. Forensics Secur. 17: 3555-3568 (2022).

IACR TCHES, 2022 Julien Béguinot, **Wei Cheng**, Sylvain Guilley and Olivier Rioul. Side-Channel Expectation-Maximization Attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(4): 774–799 (2022).

IEEE TIFS, 2022 IF: 7.231 **Wei Cheng**, Sylvain Guilley, and Jean-Luc Danger. Information Leakage in Code-based Masking: A Systematic Evaluation by Higher-Order Attacks. IEEE Trans. Inf. Forensics Secur. 17: 1624–1638 (2022).

IACR TCHES, 2022 Qianmei Wu, **Wei Cheng**, Sylvain Guilley, Fan Zhang, and Wei Fu. On Efficient and Secure Code-based Masking: A Pragmatic Evaluation. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(3): 192–222 (2022).

IEEE TVLSI, 2022 IF: 2.775 Trevor Kroeger, **Wei Cheng**, Sylvain Guilley, Jean-Luc Danger, Naghmeh Karimi. Assessment and Mitigation of Power Side-Channel based Cross-PUF Attacks on Arbiter-PUFs and their Derivatives. IEEE Trans. Very Large Scale Integr. Syst. 30(2): 187-200 (2022).

IACR TCHES, 2021 **Wei Cheng**, Sylvain Guilley, Claude Carlet, Jean-Luc Danger and Sihem Mesnager. Information Leakages in Code-based Masking: A Unified Quantification Approach. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2021(3): 465-495 (2021).

IACR TCHES, 2021 Jingdian Ming, Huizhong Li, Yongbin Zhou, **Wei Cheng**, Zehua Qiao. Revealing the Weakness of Addition Chain Based Masked SBox Implementations. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2021(4): 326-350 (2021).

CCDS, 2021 IF: 1.376 **Wei Cheng**, Sylvain Guilley and Jean-Luc Danger. Categorizing All Linear Codes of IPM over $\mathbb{F}_{2^8}$. Cryptogr. Commun. 13(4): 527-542 (2021).

JCEN, 2021 IF: 1.870 **Wei Cheng**, Claude Carlet, Kouassi Goli, Jean-Luc Danger, Sylvain Guilley. Detecting faults in inner product masking scheme. J. Cryptogr. Eng. 11(2): 119-133 (2021).

IEEE TIFS, 2020 IF: 7.231 **Wei Cheng**, Sylvain Guilley, Claude Carlet, Sihem Mesnager, Jean-Luc Danger. Optimizing Inner Product Masking Scheme by a Coding Theory Approach. IEEE Trans. Inf. Forensics Secur. 16: 220-235 (2020).

IEEE TIFS, 2020 IF: 7.231 Jingdian Ming, Yongbin Zhou, **Wei Cheng**, Huizhong Li, Guang Yang, Qian Zhang. Mind the Balance: Revealing the Vulnerabilities in Low Entropy Masking Schemes. IEEE Trans. Inf. Forensics Secur. 15: 3694-3708 (2020).

Conferences & Workshops

DATE, 2023 Jingdian Ming, Yongbin Zhou, **Wei Cheng**, Huizhong Li. Table Re-Computation Based Low Entropy Inner Product Masking Scheme. DATE 2023: 1-6 (2023).

ISIT, 2022 **Wei Cheng**, Yi Liu, Sylvain Guilley, Olivier Rioul. Attacking Masked Cryptographic Implementations: Information-Theoretic Bounds. ISIT 2022: 654-659 (2022).

CWIT, 2022 **Wei Cheng**, Olivier Rioul, Yi Liu, Julien Béguinot, and Sylvain Guilley. Side-Channel Information Leakage of Code-Based Masked Implementations. CWIT 2022: 51-56 (2022).

PROOFS, 2021 **Wei Cheng**, Yi Liu, Sylvain Guilley, Olivier Rioul. Towards Finding Best Linear Codes for Side-Channel Protections. PROOFS 2021: vol 87, pp 83-99 (2021).

ISIT, 2021 Olivier Rioul, **Wei Cheng**, Sylvain Guilley. Cumulant Expansion of Mutual Information for Quantifying Leakage of a Protected Secret. ISIT 2021: 2596-2601 (2021).

ISIT, 2021 Patrick Solé, **Wei Cheng**, Sylvain Guilley, Olivier Rioul. Bent Sequences over Hadamard Codes for Physically Unclonable Functions. ISIT 2021: 801-806 (2021).

ICCD, 2021 Jingdian Ming, **Wei Cheng**, Yongbin Zhou, Huizhong Li. APT: Efficient Side-Channel Analysis Framework against Inner Product Masking Scheme. ICCD 2021: 575-582 (2021).

DATE, 2021 Trevor Kroeger, **Wei Cheng**, Jean-Luc Danger, Sylvain Guilley and Naghmeh Karimi. Making Obfuscated PUFs Secure Against Power Side-Channel Based Modeling Attacks. DATE 2021:1000-1005 (2021).

DATE, 2020 Trevor Kroeger, **Wei Cheng**, Jean-Luc Danger, Sylvain Guilley and Naghmeh Karimi. Effect of Aging on PUF Modeling Attacks based on Power Side-Channel Observations. DATE 2020: 454–459 (2020).

PROOFS, 2019 **Wei Cheng**, Claude Carlet, Kouassi Goli, Sylvain Guilley, Jean-Luc Danger. Detecting Faults in Inner Product Masking Scheme - IPM-FD: IPM with Fault Detection. PROOFS 2019: 17-32 (2019).

DAC, 2018 Yiwen Gao, Hailong Zhang, **Wei Cheng**, Yongbin Zhou and Yuchen Cao. Electromagnetic analysis of GPU-based AES implementation. DAC 2018: 121:1-121:6 (2018).

ICICS, 2016 **Wei Cheng**, Yongbin Zhou and Laurent Sauvage. Differential Fault Analysis on Midori. ICICS 2016: 307-317 (2016).

** Full list also refer to DBLP page.*

Selected Conference Talks & Posters

IACR CHES, 2022 Presentation on: *On Efficient and Secure Code-based Masking: A Pragmatic Evaluation*, KU Leuven, Leuven, Belgium, Sep 18-21, 2022.

IEEE ISIT, 2022 Presentation on: *Attacking Masked Cryptographic Implementations: Information-Theoretic Bounds*, Aalto Univ., Espoo (Helsinki), Finland, Jun 26-Jul 1, 2022.

PROOFS, 2021 Presentation on: *Towards Finding Best Linear Codes for Side-Channel Protections*, online, Sep. 17, 2021.

IACR CHES, 2021 — Presentation on: *Information Leakages in Code-based Masking: A Unified Quantification Approach*, online, Sep. 13-17, 2021.

IEEE ISIT, 2021 — Two presentations on: *Cumulant Expansion of Mutual Information* and *Bent Sequences for PUFs*, online, Jul. 12-20, 2021.

IP Paris, 2019 — One poster on: *Optimal Linear Codes for Inner Product Masking*. Journée de l'ED IP Paris 2019, Paris, France, Dec. 10, 2019. (Best poster award from IP Paris)

CryptArchi, 2019 — Invited talk on: *Optimal Codes for Inner Product Masking*. Cryptographic Architectures Embedded in Logic Devices (CryptArchi), Prague, Czech, Jun, 2019.

IEEE ESIT, 2019 — One poster on: *Guessing A Secret Cryptographic Key from Side-channel Leakages*. 2019 IEEE European School of Information Theory (ESIT'19), Sophia Antipolis, France, Apr. 15-19, 2019.

Community

Editorial Board — Journal of Cryptographic Engineering (JCEN), since 2023

Reviewer — External Reviewer of IACR Eurocrypt 2023, and IACR CHES 2023

Guest Editor — Entropy, special Issue "An Information-Theoretic Approach to Side-Channel Analysis"

Reviewer — IEEE Transactions on Information Forensics and Security (TIFS), since 2018

Reviewer — Journal of Cryptographic Engineering (JCEN), since 2021

PC Member — IEEE International Conference on Omni-layer Intelligent systems (COINS) 2021

Teaching

MICAS, 2020–2023 — M2 master level in specialized courses MICAS-932: *Information Processing: Machine Learning, Communications and Security*, Télécom Paris, IP Paris