

Loïc Masure

Born on 08/08/1994 at Salon-de-Provence (Bouches-du-Rhône), France
14, rue Durand, 34000 Montpellier
loic.masure@lirmm.fr • +33 (0) 6 10 79 56 44 • LinkedIn • DBLP • Google Scholar • Web page
CV compiled on 2025-04-07

RESEARCH EXPERIENCE

CNRS

- Research Scientist, LIRMM, Montpellier, FRANCE Oct 2023 – Now
 - Laboratory co-hosted by Univ. Montpellier, and CNRS Informatics
 - Member of the SmartIES research team (Microelectronics dept.)

UCLouvain - ICTEAM, Louvain-la-Neuve, BELGIUM

- Postdoctoral Fellow, Crypto Group Apr 2021 – Aug 2023
 - Research on the use of Machine Learning for security evaluation against Side-Channel Attacks.
 - Research on counter-measures (masking) against Side-Channel Attacks.
 - Teaching: Discrete Math & Probability (30 hours)

CEA - Leti, Grenoble, FRANCE

- PhD student & Side-Channel Analysis Evaluator, ITSEF Nov 2017 – Mar 2021
 - Laboratory involved in the french certification scheme for cyber-security evaluation on hardware devices.
 - Work in R&D on several tools using deep learning for open samples evaluations.
- Graduate Research Intern, System Department Feb 2017 – Jul 2017
 - Project: Application of deep neural networks in context awareness signals measured by smartphone sensors.
 - Application: deep learning based human activity recognition

EDUCATION

Sorbonne Université, Paris, FRANCE

- Ph.D. in Computer Science Nov 2017 – Dec 2020
 - Thesis: Towards a Better Understanding of Deep Learning for Side-Channel Analysis
 - Advisers: Emmanuel Prouff (ANSSI), Cécile Dumas (CEA - Leti)

Grenoble Institute of Technology - ENSIMAG, Grenoble, FRANCE

- Engineering degree in Computer Science and Applied Mathematics Sep 2014 – Sep 2017
 - Graduated with Honors
 - Option: Mathematical Modelisation, Image Processing, Simulation

FUNDINGS

Chair SCA for Post-Quantum Cryptography Applications

- Amount : 343,000 € Apr 2024 – Dec 2028
 - Within Project PQ-TLS (PEPR Quantique)

PUBLICATIONS

JOURNALS

In chronological order, bold name indicates main authorship.

- [1] **Masure, L.**, Dumas, C., & Prouff, E:
A Comprehensive Study of Deep Learning for Side-Channel Analysis.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1), 348-375.
- [2] O. Bronchain, F. Durvaux, L. Masure and F.-X. Standaert:
Efficient Profiled Side-Channel Analysis of Masked Implementations, Extended.
In IEEE Transactions on Information Forensics and Security, vol. 17, pp. 574-584, 2022.
- [3] **Masure, L.**, Cristiani, V., Lecomte, M. & Standaert, F-X:
Don't Learn What You Already Know: Scheme-Aware Modeling for Profiling Side-Channel Analysis against Masking.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(1), 32–59.
- [4] Cassiers, G., Masure, L., Momin, C., Moos, T. & Standaert, F-X:
Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(2), 482-518.
- [5] **Masure, L.**, Cassiers, G., Hendrickx, J. & Standaert, F-X:
Information Bounds and Convergence Rates for Side-Channel Security Evaluators
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3), 522–569.

- [6] **Masure, L., & Strullu, R.:**
Side-channel analysis against ANSSI's protected AES implementation on ARM: end-to-end attacks with multi-task learning
J Cryptogr Eng 13, 129–147 (2023)
- [7] Cassiers, G., & Masure, L., & Momin, C., & Moos, T., & Moradi, A., & Standaert, F.-X.:
Randomness Generation for Secure Hardware Masking - Unrolled Trivium to the Rescue
IACR Communications in Cryptography, Volume 1, issue 2 (2024)

CONFERENCES

- [1] **Masure L.,** Dumas C., & Prouff E:
Gradient Visualization for General Characterization in Profiling Attacks.
Constructive Side-Channel Analysis and Secure Design. COSADE 2019.
- [2] **Masure L.,** Belleville N., Cagli E., Cornélie M., Couroussé D., Dumas C., & Maingault L:
Deep Learning Side-Channel Analysis on Large-Scale Traces: A Case Study on a Polymorphic AES.
European Symposium on Research in Computer Security. ESORICS 2020.
- [3] **Masure, L.,** Rioul, O. Standaert, F-X.
A Nearly Tight Proof of Duc et al.'s Conjectured Security Bound for Masked Implementations.
Smart Card Research and Advanced Applications. CARDIS 2022.
- [4] Béguinot, J., Cheng, W., Guilley, S., Liu, Y., **Masure, L.,** Rioul, O. Standaert, F-X.:
Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings
Constructive Side-Channel Analysis and Secure Design. COSADE 2023.
- [5] Liu, Y., Béguinot, J., Cheng, W., Guilley, S., Masure, L., Rioul, O. & Standaert, F.-X.:
Improved Alpha-Information Bounds for Higher-Order Masked Cryptographic Implementations
IEEE Information Theory Workshop, ITW 2023
- [6] **Masure, L.,** Méaux, P., Moos, T. & Standaert, F-X.:
Effective and Efficient Masking with Low Noise using Small-Mersenne-Prime Ciphers
Advances in Cryptology–EUROCRYPT 2023.
- [7] **Masure, L., & Standaert, F-X.:**
Prouff & Rivain's Formal Security Proof of Masking, Revisited: Tight Bounds in the Noisy Leakage Model
Advances in Cryptology–CRYPTO 2023.
- [8] Grassi, L., Masure, L., Méaux, P., Moos, T., & Standaert, F-X.:
Generalized Feistel Ciphers for Efficient Prime Field Masking
Advances in Cryptology–EUROCRYPT 2024.
- [9] Faust, S., **Masure, L.,** Micheli, E., Orlt, M., & Standaert, F-X.:
Connecting Leakage-Resilient Secret Sharing to Practice: Scaling Trends and Physical Dependencies of Prime Field Masking
Advances in Cryptology–EUROCRYPT 2024.
- [10] Belleville, N., & **Masure, L.:**
Hiding Behind the One that I Hide – Combining Loop Shuffling and Code Polymorphism for Enhanced AES Side-Channel Security
Constructive Side-Channel Analysis and Secure Design. COSADE 2024.

POSTERS

- [1] **Masure L.,** Dumas C., & Prouff E.:
Understanding a CNN Attack: as Crucial as Succeeding it. CHES 2018, Amsterdam, NL. Sep 2018

PRESENTATIONS

- [1] Au bal des implémentations masquées : comment protéger une implémentation cryptographique contre les attaques par canaux auxiliaires
LIRMM, Montpellier, France. Jan 2024
- [2] Masking implementations of symmetric crypto in a low noise environment : analysis and evaluation
10th ASK Workshop, Guangzhou, China. Dec 2023
- [3] Deep-Learning for Side-Channel Analysis: Where are We ?
CNRS/ Université Jean Monnet, Laboratoire Hubert Curien, Saint-Étienne, France. Nov 2022

- [4] Information Bounds and Convergence Rates of Profiling Attacks for Side-Channel Security Evaluators.
PHISIC 2022, Gardanne, France. May 2022
- [5] Deep Learning Side-Channel Analysis on Large-Scale Traces: A Case Study on a Polymorphic AES. GdR SoC2 workshop on Machine learning & Hardware security, Online. Dec 2020
- [6] Vers une meilleure compréhension de l'apprentissage profond appliqué aux attaques par observation. Journées C2, Online. Nov 2020
- [7] Vers une meilleure compréhension de l'apprentissage profond appliqué aux attaques par observation. Seminar SemSecuElec, INRIA Rennes, France. Jan 2020
- [8] A Comprehensive Study of Deep Learning for Side-Channel Analysis.
PHISIC 2019, Gardanne, France. Oct 2019
- [9] Convolutional Neural Networks with Data Augmentation against Jitter-Based Counter-measures. C&ESAR Conference. Nov 2018

PROGRAM COMMITTEE

- TCHES 2024, 2025
- Eurocrypt 2025

REVIEWS (EXTERNAL REVIEWER OR REFEREE)

- TCHES 2019, 2021-2023,
- Asiacrypt 2020, 2021, 2023, 2024,
- Crypto. & Communications,
- Crypto 2021, 2023, 2024, 2025,
- Cosade 2021, 2024,
- LatinCrypt 2021,
- JCEN,
- ICLR 2021,
- TVLSI,
- The Computer Journal,
- Journal of Cryptology,
- NeurIPS 2022, 2023
- IEICE TFECCS

OTHER WORK EXPERIENCE

Grenoble École de Management, Grenoble, France

- Lecturer Jan 2019 – Jul 2020
 - Advanced Decision: 30 hours
 - Advanced Quantitative Methods for Finance: 15 hours

NXP, Remote

- Free-lance Consultant Vulnerability Assessment Team Jan 2022 – May 2023
 - Help transferring technology from research to industry
 - Giving seminars around my recent works

LANGUAGES

- French: Native language.
- English: Fluent (speaking, reading, writing). TOEIC: 870
- German, Swedish: basic (reading)

SKILLS

- **Advanced:** Python, Numpy, Scipy, Matplotlib, scikit-learn Pytorch, Keras, $\text{\LaTeX}$, Git.