Viet-Sang Nguyen

(+33) 6 42 31 73 26 | nvietsang@gmail.com | 18 rue Prof Benoît Lauras, 42100 Saint-Etienne
https://nvietsang.github.io | nvietsang | nvietsang
04/01/1997 | Vietnam

About Me

My main interest is in the security analysis of cryptographic implementations. I'm especially motivated by the cycle: analyzing how implementations can be attacked and using those insights to develop protections.

Experience

Jean Monnet University — Saint-Etienne, France
PhD Researcher — 01/2023–12/2025 (Expected)

- Studied and published papers in side-channel and fault attacks.
- Designed countermeasures for secure implementations.

CryptoExperts — Paris, France
Cryptography Engineer — 09/2021–12/2022

- Designed and developed a generic framework for building circuits and generating white-box implementations of cryptographic algorithms.
- Designed and developed a framework for software obfuscation with a simple stateless secure element.

CryptoExperts — Paris, France
Cryptography Intern — 03/2021–08/2021

- Designed and developed of a cryptocurrency wallet with consideration of security protection.
- Studied white-box cryptography and physical attacks on ECDSA.

Research Institute XLIM — Limoges, France
Cryptography Intern — 06/2020–08/2020

- Studied and developed an encrypted matching scheme.
- Improved speed by pre-discarding costly operations using Cuckoo filter.

Knorex — Ho-Chi-Minh City, Vietnam
Machine Learning Intern — 06/2018–08/2018

- Evaluated and improved accuracy in language detection (60%), and keyword extraction (10-20%)

Teaching

Embedded Programming (tutorials) — IUT Saint-Etienne, France
27h×3, for 2nd-year Bachelor Students — 2023–2024

C++ Programming (tutorials) — IUT Saint-Etienne, France
33h, for 1st-year Bachelor Students — 2024

Publications

- **Nguyen**, Grosso and Cayrel, "*Practical Persistent Fault Attacks on AES with Instruction Skip*", IACR CiC, 2025
- **Nguyen**, Grosso and Cayrel, "*Practical Second-Order CPA Attack on Ascon with Proper Selection Function*", CASCADE, 2025
- **Nguyen**, Grosso and Cayrel, "*Correlation Power Analysis on Ascon with Multi-bit Selection Function*", SECRYPT, 2025
- **Nguyen**, Grosso and Cayrel, "*Provable Resistance of Threshold Implementations to S(I)FA*", in submission
- **Nguyen**, Grosso and Cayrel, "*SIFA on Nonce-based Authenticated Encryption: When Does It Fail? Application to Ascon*", in submission
- Mercadier, **Nguyen**, Rivain and Udovenko, "*Versatile Software Obfuscation from a Lightweight Secure Element*", IACR TCHES, 2024

Education

PhD in Cryptography — 2023-2025
Jean Monnet University — France
Supervisors: Vincent Grosso, Pierre-Louis Cayrel

Master in InfoSec & Crypto — 2019-2021
University of Limoges — France
Magna cum laude

Bachelor of Engineering (CS) — 2015-2019
HCM University of Technology — Vietnam
Magna cum laude, honors program

Service

External Reviewer for EuroCrypt (2024,2025)

Honors/Awards

2024 1st Prize in NSUCRYPTO Olympiad
2023 3rd Prize in NSUCRYPTO Olympiad
2018 Award for Outstanding Students

Selected Projects

2024 Incremental 2nd-order CPA (1 month)
2022 Framework for software obfuscation with simple secure element (4 months)
2022 Framework for defining and constructing computational circuits (5 months)
2021 Tutorials for differential power analysis (2 weeks)

Technical Skills

Programming	Python, C/C++, Sagemath, Java, Android, GPGPU
Security	Cryptography, Basics of Reverse Engineering
Others	Unix-like OS, Git, Docker

Languages

English	Full professional proficiency
French	Level B2
Vietnamese	Native

Hobbies

- Playing and watching football
- Playing drums
- Reading, especially biographies and memoirs

Reference

Dr. Vincent Grosso
CNRS Researcher at Jean Monnet University
18 rue Prof. Benoît Lauras, Saint-Etienne
vincent.grosso@cnrs.fr