19 rue Chevreul, 42100 Saint-Étienne, France
(+33) 06 42 31 73 26
nvietsang@gmail.com
https://nvietsang.github.io
nvietsang
04/01/1997
Vietnam

Viet Sang NGUYEN

PhD Candidate in Cryptography

Experiences

2021–2022 **Cryptography Engineer**, *CryptoExperts*, Paris, France
White-Box Cryptography: Design and development of a generic framework for building circuits and generating white-box implementations of cryptographic algorithms.

2021 (6 months) **Cryptography Engineer Intern**, *CryptoExperts*, Paris, France
Secure wallet app for cryptocurrency: Design and development of a wallet capable of sending and receiving coins with considerations of security and privacy. Study of white-box cryptography and countermeasures against physical attacks on ECDSA.

2020 (3 months) **Cryptography Research Intern**, *Research Institute XLIM*, University of Limoges, France
Pre-filtering in Pub/Sub systems: Study and implementation of an encrypted matching scheme. Improvement of speed by pre-discarding costly matching operations known certainly as unmatched using Cuckoo filter.

2018 (3 months) **Machine Learning Intern**, *Knorex*, Ho-Chi-Minh City, Vietnam
Language Detection: Evaluation and improvement of accuracy (60%) when detecting Malaysian and Indonesian. Extension of language detection for 5 new languages.
Keys Mining: Evaluation and improvement of accuracy (10-20%) for extracting keywords related to a certain topic from texts. Extension of keyword extraction for 5 new languages.

Education

2023–* **PhD Candidate in Cryptography**, Expected: 12/2025
University of Lyon, France
Supervisors: Vincent Grosso, Pierre-Louis Cayrel
Secure Implementations of Cryptographic Algorithms against Physical Attacks

2019–2021 **Master Cryptis in Information Security**, GPA: 15.01/20, Rank 2/20
University of Limoges (UNILIM), France
Courses: Cryptology Advanced, Smart Cards and Secure Implementation, Security of ICT Usages, Cryptographic Mechanisms and Applications, Complexity and Computability

2015–2019 **Bachelor Engineer in Computer Science**, *Honors Program*, GPA: 8.35/10
Ho-Chi-Minh University of Technology (HCMUT), Vietnam
Thesis (9.6/10): Development of a Question-Answering model for Vietnamese using Deep Learning (Exact Match: 61.0%, F1-score: 76.6%)

Publications

CHES 2024 **OBSCURE: Versatile Software Obfuscation from a Lightweight Secure Element**
Darius Mercadier, Viet Sang Nguyen, Matthieu Rivain, Aleksei Udovenko

Selected Projects

2022 (4 months) **OBSCURE**: framework for software obfuscation relying on a simple stateless secure element

2022 (4 months) **circkit**: framework for defining, constructing and manipulating computational circuits

2021 (2 weeks) **D-CPA**: Differential Power Analysis and Correlation Power Analysis attacks on AES-128

2020 (3 months) **NIDS-DL**: real-time Network Intrusion Detection System based on a Deep Learning model using Snort, Kafka, Zeek, Spark

Talks

16/10/2023	**Persistent Fault Model: Generalization, Cryptanalysis and Countermeasures** at Journées C2 in Najac, France
22/06/2023	**Linear Cryptanalysis and Countermeasures in Persistent Fault Model** at Laboratoire Hubert Curien in Saint-Étienne, in scope of ANR PROPHY project

External Reviewer

2024	EUROCRYPT

Teaching

2023–2024	**Tutorials of embedding programming on CodeWarrior for second year bachelor students** 27h at IUT Saint-Étienne, France
2023–2024	**Tutorials of C++ programming for first year bachelor students** 27h at IUT Saint-Étienne, France
2022–2023	**Tutorials of embedding programming on CodeWarrior for second year bachelor students** 27h at IUT Saint-Étienne, France

Technical Skills

Programming	Python, C/C++, Sagemath, Java, GPGPU, Android, SQL, MATLAB, Shell Scripts.
Other	Familiar with Unix-like OS, Git, Docker.

Honors/Awards

2021,2022	3rd Prize in International Olympiad in Cryptography NSUCRYPTO with 2 best solutions.

Languages

Vietnamese	Mother tongue
English	Full professional proficiency
French	Level B2