PAUL HUYNH

PHD WITH A SPECIALIZATION IN LIGHTWEIGHT CRYPTOGRAPHY

DETAILS

Born on 11/08/1993
27 years old
French

47 rue Bargue
75015, Paris, France

+33 6 66 81 82 51
paul.h@outlook.com
members.loria.fr/PHuynh

SKILLS

Mathematics:
Linear algebra
Galois theory
Error correction codes
Information theory

Cryptography:
Design of secret-key encryption primitives
Classical cryptanalysis techniques
Authentication modes
Basic knowledge of public-key cryptography and Side-Channel Analysis

Programming languages/tools:
Java, C, Python, SageMath
Choco solver, Gurobi solver, MiniZinc
LaTeX, Bash, Git

Foreign languages:
English (C1 level)
German (B1 level)
Vietnamese (fluent)

INTERESTS

Traditional & digital art, film and music making, mountaineering, sport climbing

EDUCATION

2017 - 2020 **PhD in Computer Science**
Under the supervision of Prof. Marine Minier
Université de Lorraine, CNRS, INRIA, LORIA, Nancy, France

2014 - 2016 **Master's degree in Mathematics & CS applied to Cryptology**
Summa cum laude
Université de Paris, Paris, France

2011 - 2014 **Bachelor's degree in Fundamental Mathematics**
Summa cum laude
Université de Paris, Paris, France

EXPERIENCE

Dec. 2020 - present **Research Engineer - Cryptanalyst**
LORIA, Nancy, France
Study of boomerang and differential attacks using automated tools (Constraint Programming, MILP, SAT solvers).

2017 - 2020 **PhD Candidate**
LORIA, Nancy, France
"Analysis and Design of Lightweight Encryption Schemes"
funded by the PACLIDO project (collaboration between academia and industry aiming for IoT security)

Co-designer of Lilliput-AE, a lightweight authenticated encryption algorithm submitted to the international standardization open process initiated by NIST (National Institute of Standards & Technology).
Cryptanalysis of various NIST proposals. Application of automated tools to solve symmetric cryptography problems.

4 published papers in international conferences/journals
2 papers in preparation.
Full list and presentations available at https://members.loria.fr/PHuynh/publications.

2016 - 2017 **Engineer**
CRAN, Nancy, France
Co-designer of a self-synchronizing stream cipher based on control theory. Provided SageMath and C implementations as well.

2016 **Intern in Cryptology**
Airbus Defence & Space - CyberSecurity, Élancourt, France
Provided a theoretical fault injection analysis of a self-synchronizing stream cipher as well as a simulation of the resulting attack in C language.

linkedin.com/in/lephucpaulhuynh