Benoît **Viguier**

SOFTWARE ENGINEER · PHD CANDIDATE

About

32 years old
Zwanenveld 9150
6538 SJ NIJMEGEN

THE NETHERLANDS
☎ (+31) 6 30607282
✉ benoit@viguier.nl
⌂ viguier.nl
beviguier
@ildyria
ildyria

Language

French	★★★★★
English	★★★★★
Dutch	★★☆☆☆
German	★★☆☆☆
Spanish	★☆☆☆☆
Japanese	★☆☆☆☆

OS Preference

Debian	★★★★★
Windows	★★★☆☆
MacOs	★★★☆☆

Activities

Ballroom Dancing
Photography
Piano
Rock climbing
Martial Arts
Sailing

I am currently writting my PhD Thesis on Cryptography and Formal Verification.
I am passionate about symmetric cryptography, formal methods, and beautiful code.
I am also a competitive ballroom dancer and a photographer.

Education

Software Engineer — *Rennes, France*
INSA (National Institute of Applied Sciences) — *Sept. 2014 - 2016*

MRes. in Computer Science — *Rennes, France*
University Rennes 1 — *Sept. 2015 - 2016*

MSc. in Mathematics — *Rennes, France*
University Rennes 1 — *Sept. 2006 - 2011*

Skills

Programming	C/C++, Coq, Python, RISC-V asm, ARM Asm, PHP, LaTeX
Dev. Env.	Visual Studio Code, IntelliJ IDEA, Clion, PhpStorm, Git, Atom

Experience

PhD Candidate — *Nijmegen, The Netherlands*
Radboud University — *Sep. 2016 - Dec. 2020*

- Designing symmetric cryptography algorithm.
- Writting optimized implementation for lightweight schemes.
- Using formal methods to verify cryptographic C implementations.

Coq, Formal Approaches, Cryptanalysis, C, Assembly

Internship : Software Engineer & Researcher — *Brussels, Belgium*
STMicroelectronics — *Feb. - Jun. 2016*

- Verification of the truncated tree search using Formal Methods.
- Application to differential and linear trail search.

Coq, C++, Differential Cryptanalysis, Hash functions

Internship: Software Engineer — *Brussels, Belgium*
Mission Critical IT — *Jun. - Sep. 2015*

- SNOMED CT, ICD10PCS and NLP parsing.

Lucene, OpenNLP, Stanford Parser, SWRL, Ontologies, JAVA

Mathematics Teacher — *2011 - 2014*

- Junior Highschool and Highschool

Teamwork, teaching skills, formalism

Publications

A Coq proof of the correctness of X25519 in TweetNaCl — *Dubrovnik*
34th IEEE Computer Security Foundations Symposium — *Jun. 2021*

- We formally prove that the C implementation of the X25519 key-exchange protocol in the TweetNaCl library correctly implements the protocol from Bernstein's 2006 paper, as standardized in RFC 7748, as well as the absence of undefined behavior. We also formally prove that X25519 is mathematically correct, i.e., that it correctly computes scalar multiplica- tion on the elliptic curve Curve25519. The proofs are all computer-verified using Coq.

Assembly or Optimized C for Lightweight Cryptography on RISC-V?

Vienna

Cryptology and Network Security *Dec. 2020*

- In this work, we studied the general impact of optimizing symmetric-key algorithms in assembly and in plain C on RISC-V architectures. Additionally, we present optimized implementations of NIST's lightweight candidates, with speed-ups of up to 81% over available implementations, and discuss general implementation strategies.

Cryptanalysis of MORUS

Brisbane, Australia

Advances in Cryptology – ASIACRYPT 2018, LNCS *Dec. 2018*

- We present a linear correlation in the keystream of full MORUS, which can be used to distinguish its output from random and to recover some plaintext bits in the broadcast setting.

KangarooTwelve: fast hashing based on Keccak-p

Leuven, Belgium

Applied Cryptography and Network Security – ACNS 2018, LNCS *July 2018*

- KangarooTwelve, a fast and secure arbitrary output-length hash function aiming at a higher speed than the FIPS 202's SHA-3 and SHAKE functions.

Gimli: A Cross-Platform Permutation

Taipei, Taiwan

Cryptographic Hardware and Embedded Systems – CHES 2017, LNCS *Sept. 2017*

- Gimli, a 384-bit permutation designed to achieve high security with high performance across a broad range of platforms.

Extra Activities

DSV Sway of Life

The Netherlands

Standard Ballroom Formation Dancer *Mar. 2018 - PRESENT*

- 2020 - **4th place** — Dutch Championship in couple C-class Standard — Dalfsen
- 2019 - **1st place** — Dutch Championship in Formation Dancing — Almere
- 2019 - **Finalist** — World Championship in Formation Dancing — Moskow
- 2018 - **1st place** — Dutch Championship in Formation Dancing — Almere

Landscapes & Ballroom Photography

The Netherlands

Photographer *Jul. 2018 - PRESENT*

- Landscapes & long exposures
- Ballroom Photography – WDSF, NADB, NTDS, ETDS
- Events – PhD Defenses
- Portraiture

LycheeOrg

The Netherlands

Main Developer & Administrator *Aug. 2018 - PRESENT*

- Complete rewrite of the Lychee image server with Laravel.