Benoît **Viguier**

PhD. · Software Engineer

I am passionate about symmetric cryptography, formal methods, and beautiful code.
I am also a competitive ballroom dancer and a photographer.

About

36 years old
Zwanenveld 9150
6538 SJ NIJMEGEN
THE NETHERLANDS
(+31) 6 30607282
benoit@viguier.nl
viguier.nl
beviguier
ildyria

Language

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

OS Preference

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

Activities

Ballroom Dancing
Photography
Sailing

Education

PhD in Cryptography & Formal Methods — *Nijmegen, The Netherlands*
Radboud Universiteit — *Sept. 2016 – Dec. 2021*

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 Java, PHP, TypeScript, SQL, Python, C/C++, Coq, RISC-V asm, ARM Asm, LaTeX
Dev. Env. Visual Studio Code, IntelliJ IDEA, Git

Experience

Information Security Expert – DevOps Eng. Crypto. — *Amsterdam, The Netherlands*
ABN AMRO Bank — *Apr. 2021 – current*

- Member of the Crypto Services team.
- Member of the Secure Coding team.
- Member of the Quality Assurance board.
- Member of the Cryptographic Working Group.
- Design & implementation of the Registration Authority (RA) for the bank Public Key Infrastructure (PKI)
- Certificate Authority migration from Single-tier CA to Two-tier CA..
- Standardization of best practices in cryptography.
- Standardization of best practices in software Development.

Java, PKI, Python, Ts, Git, Agile & Scrum, CICD

PhD Researcher — *Nijmegen, The Netherlands*
Radboud Universiteit — *Sep. 2016 – Feb. 2021*

- Designing and breaking 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++, Cryptanalysis, Hash functions

Mathematics Teacher — *France*
Lycée d'Estournelles de Constant & Collège La Madeleine — *2011 – 2014*

- Junior Highschool and Highschool

Teamwork, teaching skills, formalism

Publications

KangarooTwelve and TurboSHAKE

IRTF — CFRG

Internet-Draft — RFC *In review*

- This document defines the TurboSHAKE128, TurboSHAKE256, KT128 and KT256 eXtendable Output Functions (XOF), i.e., a hash function generalization that can return an output of arbitrary length. Both TurboSHAKE128 and TurboSHAKE256 are based on a Keccak-p permutation specified in [FIPS202] and have a higher speed than the SHA-3 and SHAKE functions.

A Panorama on Classical Cryptography

Nijmegen, The Netherlands

PhD Thesis *Dec. 2021*

Designing, Implementing, Breaking, Verifying, and Standardizing Cryptography

- *In this thesis we cover a large part of the classical cryptography world: we examine the design of new symmetric primitive; we explore implementation strategies of lightweight schemes; we analyze a new high performance algorithm; we use formal verification to prove the correctness of Elliptic Curve Cryptography implementations; and finally we describe one of the way algorithms are standardized.*

A Coq proof of the correctness of X25519 in TweetNaCl

Dubrovnik, Croatia

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, Austria

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

LycheeOrg — Lychee.

The Netherlands

Lead Dev. & Team admin *Aug. 2018 - PRESENT*

Lychee is a privacy-friendly self-hosted photo gallery with a simple look & feel.

- *Full rewrite of the PHP core server with Laravel.*
- *Adopt best industry practices with PHP.*
- *Support of WebAuthn and Oauth.*
- *Full rewrite of front-end from Jquery to Livewire & Alpine in TypeScript.*

Landscapes & Ballroom Photography

The Netherlands

Photographer *Jul. 2018 - PRESENT*

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

Standard Ballroom & Formation Dancer

The Netherlands

Member of DSV Sway of Life

Mar. 2018 - PRESENT

- 2023 — **1^{st} place** — Dutch Championship in Formation Dancing — Rotterdam
- 2023 — **3^{rd} place** — Dutch Championship in couple A-class Standard — Steenwijk
- 2022 — **1^{st} place** — Dutch Championship in Formation Dancing — Dalfsen
- 2022 — **5^{th} place** — World Championship in Formation Dancing — Braunschweig
- 2022 — **3^{rd} place** — European Championship in Formation Dancing — Nürnberg
- 2022 — **Semi-Finalist** — Dutch Championship in couple A-class Standard — Steenwijk
- 2021 — **2^{nd} place** — Dutch Championship in couple C-class Standard — Dalfsen
- 2021 — **1^{st} place** — Dutch Championship in Formation Dancing — Rotterdam
- 2020 — **4^{th} place** — Dutch Championship in couple C-class Standard — Dalfsen
- 2019 — **1^{st} place** — Dutch Championship in Formation Dancing — Almere
- 2019 — **Finalist** — World Championship in Formation Dancing — Moskow
- 2018 — **1^{st} place** — Dutch Championship in Formation Dancing — Almere