Benoît **Viguier**

Software Engineer · PhD Student

About

31 years old, Single
Past. van Blitterwijckstr. 31
6525 SR NIJMEGEN
THE NETHERLANDS
☎ (+31) 6 30607282
✉ benoit@viguier.nl
⌂ www.viguier.nl
in beviguier
@ildyria
ildyria

Language

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

OS Preference

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

Activities

Ballroom Dancing
Piano
Rock climbing
Martial Arts
Sailing

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++, JAVA, Coq, Python, B, PHP, Laravel, OCaml, LaTeX
Dev. Env.	IntelliJ IDEA, Clion, Git, Visual Studio & R#, Xcode

Experience

PhD Student — *Nijmegen, The Netherlands*
Radboud University — *Sept. 2016 - Present*

- High Assurance Cryptographic Software.

Coq, ASM, Cryptanalysis

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

- Formal Methods in differential and linear trail search.

Coq, C++, Differential Cryptanalysis, Hash functions

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

- SNOMED CT, ICD10PCS and NLP parsing.

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

4th year project — *Rennes, France*
INSA (National Institute of Applied Science) — *2014 - 2015*

- Building a generic A.I. for board games over a distributed network

Agile Methods, Monte Carlo Tree Search, C++, OpenMP, MPI, Teamwork

Internship: Software Developer — *Nantes, France*
Beotic — *Feb. 2014*

- Development of a prototype of a project management app for IPad

Objective-C, Xcode

Independent Addon developer for online games — *2011 - 2013*

- Development of an HUD for World of Warcraft

LUA, Git, User Relationship

Independent Web Developer — *2008 - 2011*

Cryptography, SQL injection, PHP, MySQL, HTML, CSS, JS

Mathematics Teacher — *2011 - 2014*

- Junior Highschool and Highschool

Teamwork, teaching skills, formalism

Volunteer — *Hagi, Japan*
International Work Camps with CIEE Japan — *Jul. - Aug. 2012*

- Restoring a school and teaching English
- Filling a generation gap between elderly people and elementary school students

Publications

Cryptanalysis of MORUS
Brisban, 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
The Netherlands

Member & Administrator *Aug. 2018 - PRESENT*

- Complete rewrite of the Lychee image server with Laravel.

DSV Sway of Life
The Netherlands

Member *Mar. 2018 - PRESENT*

- 2018 - Dutch Champions in Formation Dancing