

## About

29 years old, Single  
Past. van Blitterwijkstr. 31  
6525 SR NIJMEGEN  
THE NETHERLANDS  
☎ (+31) 6 30607282  
✉ benoit@viguier.nl  
🏠 www.viguier.nl  
📺 bevigui  
🐦 @ildyria  
📷 ildyria

## Language

**French** ★★★★★  
**English** ★★★★★  
**German** ★★★★★  
**Dutch** ★★★★★  
**Spanish** ★★★★★  
**Japanese** ★★★★★

## OS Preference

**Debian** ★★★★★  
**Windows** ★★★★★  
**MacOs** ★★★★★

## Activities

**Ballroom Dancing**  
**Piano**  
**Rock climbing**  
**Martial Arts**  
**Sailing**

# Benoît Viguier

SOFTWARE ENGINEER · PHD STUDENT

## Education

### Software Engineer

INSA (NATIONAL INSTITUTE OF APPLIED SCIENCES)

Rennes, France

Sept. 2014 - 2016

### MRes. in Computer Science

UNIVERSITY RENNES 1

Rennes, France

Sept. 2015 - 2016

### MSc. in Mathematics

UNIVERSITY RENNES 1

Rennes, France

Sept. 2006 - 2011

## Skills

### Programming

C/C++, JAVA, Coq, Python, B, PHP, OCaml,  $\LaTeX$

### Dev. Env.

IntelliJ IDEA, Clion, Git, Visual Studio & R#, Xcode

## Experience

### PhD Student

RADBOUD UNIVERSITY

• High Assurance Cryptographic Software.

Nijmegen, The Netherlands

Sept. 2016 - Present

*Coq, ASM, Cryptanalysis*

### Internship : Software Engineer & Researcher

STMICROELECTRONICS

• Formal Methods in differential and linear trail search.

Brussels, Belgium

Feb. - Jun. 2016

*Coq, C++, Differential Cryptanalysis, Hash functions*

### Internship: Software Engineer

MISSION CRITICAL IT

• SNOMED CT, ICD10PCS and NLP parsing.

Brussels, Belgium

Jun. - Sept. 2015

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

### 4th year project

INSA (NATIONAL INSTITUTE OF APPLIED SCIENCE)

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

Rennes, France

2014 - 2015

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

### Internship: Software Developer

BEOTIC

• Development of a prototype of a project management app for iPad

Nantes, France

Feb. 2014

*Objective-C, Xcode*

### Independent Addon developer for online games

• Development of an HUD for World of Warcraft

2011 - 2013

*LUA, Git, User Relationship*

### Independent Web Developer

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

2008 - 2011

### Mathematics Teacher

• Junior Highschool and Highschool

2011 - 2014

*Teamwork, teaching skills, formalism*

### Volunteer

INTERNATIONAL WORK CAMPS WITH CIEE JAPAN

• Restoring a school and teaching English

• Filling a generation gap between elderly people and elementary school students

Hagi, Japan

Jul. - Aug. 2012

## Publications

---

### **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.