

## Nicolas MORO

34 years old, driving license

 Eindhoven, The Netherlands

French nationality 

nicolas.moro@gmail.com 

www.nicolasmoro.net 

# Cryptography software engineer

---

## Education

### 2011-2014 - PhD in computer science – Sorbonne Université

*Security of assembly programs against hardware attacks on embedded processors*

PhD grant funded by CEA (French Atomic Energy and Alternative Energies Commission)

### 2008-2011 - “Diplôme d’ingénieur” – Mines Saint-Étienne ISMIN

Joint Master in executive management and engineering, graduated with highest honours

Majors in computer science, embedded systems, microelectronics, microcontrollers

### 2006-2008 - “CPGE” – Classe préparatoire aux grandes écoles MP

Intensive preparation for the competitive examination for admission to the top French engineering schools

Undergraduate studies in mathematics, physics and computer sciences

### 2006 - “Baccalauréat scientifique” mention Bien

French high school exam, equivalent to British A-Levels with majors in science and high honours

## Skills

**Programming** C , Python , C++ , C# , Perl , Android , Java SE 

**Hardware** ARM Assembly , Embedded C , Embedded Linux , VHDL 

**Security** Applied cryptography , Software countermeasures for physical attacks ,  
Fault injection & EMFI , Side-channel analysis , Reverse engineering , Threat modelling 

**UNIX Systems** Linux server administration (Debian, Ubuntu) 

**Web** HTML , CSS , PHP 5 , Javascript , Web applications security 

**Other** CMake , Git , LaTeX , TCP/IP , Matlab , UML , Docker , SQL , MongoDB 

**Management** Team management , Requirements management , Project planning 

-  Basic, either used long time ago or for small projects
-  Independent user, able to use with minimal supervision
-  Proficient, recently used on a regular basis

## Languages

 **French** mother language

 **English** fluent

 **Italian** intermediate

 **Dutch** advanced, level CEFR C1

 **Chinese** beginner, 6 months and several trips to Taiwan

## Other interests and hobbies

- Interests: history, strategy video games, Franco-Belgian comics, Chinese culture, badminton
- Former webmaster of a French website about TI-89 calculators (2004-2008, available at fl89.free.fr)
- French hackathon « Nuit de l’info » (web technologies): 4 awards in 3 participations (2009-2011)

## Work experience



### Senior Embedded Software Engineer | Intrinsic ID

Developer, then Software Team Lead (since sep 2021)

Eindhoven, The Netherlands Feb 2020 to now

I worked on (and then led the team working on) the software PUF product and software RNG product of Intrinsic ID. The team is made of 5 engineers (including myself). Together, we drastically improved the quality of the products, in terms of maintainability, testing, requirements management, internal processes and continuous integration.



### R&D Engineer | IMEC-NL

Member of the Solutions4IoT team

Eindhoven, The Netherlands Apr 2018 to Jan 2020, 1 year and 10 months

I mostly worked on two projects, a firmware over-the-air update solution and a secure distance bounding protocol, both using Bluetooth Low Energy (BLE).

My main achievements were coordinating the preparation of a demo for IMEC's biggest event, taking over the task lead on short notice for a EU funded project and giving good quality deliverables on time, and reaching a better than state-of-the-art performance for an authenticated key exchange protocol on an ARM Cortex-M0 board.



### Cryptography Software Engineer | NXP Semiconductors

Innovation Center Crypto & Security, member of the Crypto Software team

Eindhoven, The Netherlands Dec 2014 to Mar 2018, 3 years and 4 months

I worked first as a developer and later as a component owner for the NXP Cryptographic Library. The library provides cryptographic functions hardened against fault attacks and side-channel analysis for NXP's secure microcontrollers. I had to coordinate the activities (software design, task planning, implementation, adaptations for new platforms, test specifications, security evaluation and technical documentation) for the components I was in charge of.

My main achievements were implementing a complex proprietary function which gave a key performance advantage to the library, proposing a code compression solution which became used for code size reduction, reorganizing the code in my component to improve its adaptability, and designing a masking scheme for a proprietary 3G cryptographic primitive.



### Junior researcher in embedded systems security, PhD student | CEA

PhD thesis, supervised by Emmanuelle Encrenaz, Bruno Robisson and Karine Heydemann

Gardanne, France Oct 2011 to Nov 2014, 3 years

My research works focused on performing practical fault injection attacks on ARM microcontrollers, on identifying their effect on embedded programs and on designing assembly-level countermeasures. These activities led to four publications in international peer-reviewed conferences with proceedings and one journal article, and these articles have been cited in many recent research papers (cf. Google Scholar). A detailed list is available on my website.

I also attended some extra classes (on strategic management, management of technology projects, competitive intelligence, European Union funded research projects), and gave MSc courses on cryptography for 2 years (21h/year).



### Junior research engineer | National Taiwan University

Internship, Department of Electrical Engineering

Taipei, Taiwan Mar to Sep 2011, 6 months

I built embedded Linux distributions and root filesystems based on Busybox for ARM development boards.

## Involvement in associations



### President, then board member | Mines Saint-Étienne Alumni – Gardanne Campus

President 2011-2013 (2 years) then board member 2014-2017

During my president term, we managed to revitalize the association, improve its image among the students and alumni, and set up some efficient processes and working tools. I was also in charge of the association's server and website.



### Tutor for the Mob-e3 Contest | Airbus Group Foundation | March to June 2010 (4 months)

With another engineering student, we tutored a 7th grade class for the Mob-e3 national contest "Let's imagine the future's transportation means" organized by the Airbus Group Foundation.



### Treasurer | Association Illu-Mines | 2009-2010 (1 academic year)

Association for the popularization of science, held by students of the school. I was involved into the organization of the Science Festival and did popular science presentations to high school students.