




## Nicolas MORO


30 years old, driving license

 Eindhoven, The Netherlands

 +31.(0)6.24.50.85.90

French nationality 

nicolas.moro@gmail.com 

www.nicolasmoro.net 

## Cryptography software engineer

### Education

#### PhD in computer science - Université Pierre et Marie Curie

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

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

 Gardanne, France  
 2011-2014

#### "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

 Gardanne, France  
 2008-2011



#### "CPGE" - Classe préparatoire aux grandes écoles MP

Intensive preparation for the competitive examination for admission to the top French engineering schools ("Grandes écoles"), Undergraduate studies in mathematics, physics and computer sciences

































 Nice, France  
 2006-2008

#### "Baccalauréat scientifique" mention Bien

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

 Antibes, France  
 2006

### Computer skills

Programming	C  , Python  , C++  , C#  , Perl  , Android  , Java SE 
Hardware	Assembly  (ARM, AVR), Embedded C  , Embedded Linux  , VHDL 
Security	Applied cryptography  , Software countermeasures for physical attacks  , Fault injection & EMFI  , Side-channel analysis  , IDA Pro  , Threat modelling  , Application vulnerabilities on Windows and Linux 
UNIX Systems	Linux server administration (Debian, Ubuntu) 
Web	XHTML 1.0  , CSS 3  , PHP 5  , Javascript  , Web applications security 
Databases	SQL  (MySQL, PostgreSQL)
Other	VCS (SVN, Git)  , LaTeX  , LabVIEW  , TCP/IP networks  , Matlab  , Maxima  , UML 

 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

 <b>French</b>	mother language		
 <b>English</b>	advanced, TOEIC 915		
 <b>Italian</b>	intermediate		
 <b>Dutch</b>	intermediate, level CEFR B2		
 <b>Chinese</b>	beginner, 6 months and several trips to Taiwan		

### Other interests and hobbies

- Hobbies : strategy video games, history, Franco-Belgian comics, pub quizzes
- 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 prizes in 3 participations (2009-2011)

## Work experience



### R&D Engineer | IMEC-NL

Member of the Solutions4IoT team

📍 Eindhoven, The Netherlands 📅 Apr 2018 to now

I am mostly working for two R&D teams, one of them focusing on air quality measurements and the other one on a secure distance bounding protocol using Bluetooth Low Energy (BLE).

My main achievements were building a firmware over-the-air update solution via BLE for a STM32 board, coordinating the preparation of a demo for IMEC's biggest event showing a potential applications for that updater solution, taking over the task lead from a former colleague in a EU funded project on short notice 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 by selecting a fast elliptic curve and optimizing its implementation.



### 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 several cryptographic functions hardened against fault attacks and side-channel analysis for NXP's secure microcontrollers. It is split in several components, and each of them has an owner who coordinates the activities (software design, task planning, implementation, adaptations for new platforms, test specifications, security evaluation and technical documentation).

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

Joint research lab CEA / Mines St-Etienne on Secure Architectures and Systems

📍 Gardanne, France 📅 Oct 2011 to Nov 2014, 3 years

My research works focused on performing fault injection attacks on microcontrollers, on identifying their effect on embedded programs and on designing assembly-level countermeasures. I also conducted practical experiments on electromagnetic fault injection on an ARM Cortex-M3 microcontroller. 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 [www.nicolasmoro.net/my-publications](http://www.nicolasmoro.net/my-publications). I also attended some extra classes (on strategic management, management of technology projects, competitive intelligence, European Union funded research projects), and gave a course for 2 years on 'Cryptography & introduction to embedded systems security' course for 2 years (21h/year) to 1<sup>st</sup> year MSc students from Mines St-Etienne.



### 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.

## Shorter internships

- Android app developer | Corellis (2011, 1 month)
- Web developer | iPuP (2010, 4 months)

## Involvement in associations



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

President 2011-2013 (2 years) then board member since 2013

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 am also in charge of the association's server since 2011.



### 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.