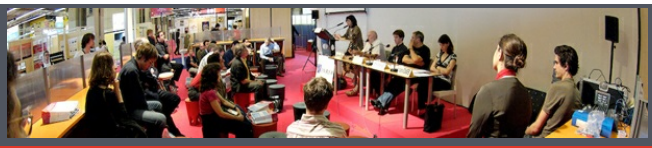
INTERNATIONAL RELATIONS



INTERNSHIP SUBJECT

2898 - NVM-free SRAM Physical Unclonable Function

Historically, securing cryptographic keys within embedded systems typically required storing sensitive secret keys or helper data permanently in Non-Volatile Memory (NVM). However, many resource-constrained devices, such as **Single-Chip micro Motes (SCuM)**, lack integrated NVM, making traditional storage-based methods infeasible. Physically Unclonable Functions (PUFs), particularly SRAM-based implementations, offer a promising alternative by generating device-specific keys directly from hardware variations. Still, most established techniques rely on storing some form of helper data in NVM to ensure reliable key regeneration.

This internship specifically targets this limitation by developing an**NVM-free** SRAM-based PUF implementation on SCuM. In contrast to conventional methods, helper data in this project will not be stored persistently. Instead, it will be dynamically generated on-demand during device initialization or authentication. This approach ensures that even devices lacking NVM, can benefit from secure key generation and authentication.

Your tasks will include building a C-language library that can reliably execute on SCuM chips while being adaptable to other microcontroller platforms. The internship will involve integrating and optimizing privacy amplification techniques, such as compression algorithms, to facilitate secure and robust key generation without persistent storage. Rigorous testing under varying environmental conditions, including temperature and voltage fluctuations, will be essential. Additionally, you'll analyze critical performance metrics, focusing particularly on energy efficiency and time delay.

Finally, you'll use your implementation to develop a secure bootloader that leverages dynamically-generated secret keys, demonstrating practical, real-world applicability for resource-limited microcontrollers.

This internship provides an exciting opportunity to significantly advance embedded systems security, particularly for devices like SCuM that inherently lack NVM.

If you are passionate about embedded programming, security innovation, and solving real-world hardware constraints, this role is ideal for you.

Work Environment

Located at the heart of Europe, Paris is a unique place to work and live in. Inria offers a unique balance between working in a leading research center, and living in one of the most beautiful and bustling cities in the world. A real communication hub, Paris is a gateway to France and Western Europe, and working in the Inria-Paris research center is real asset to your career. Inria Paris is located at the heart of the famous and picturesque Butte aux Cailles neighborhood in Paris.

Thanks to its top-quality researchers and numerous international guests, the Inria-Paris research center plays a leading role in international research, with a strong focus on networking, robotics and communication systems. The 32 research teams of the center are continuously pushing the boundaries in developing new concepts and techniques.

You will be working in a fantastically fun environment, within theAIO team (https://aio.inria.fr/), also in constant collaboration other international research teams, in particular Prof. Pister's team at UC Berkeley. The team is designing Tomorrow's Internet of (Important) Things. It pushes the limits of low-power wireless mesh networking by applying them to critical applications such as robotics, industrial control loops, with harsh reliability, scalability, security and energy constraints. Inria-AIO co-chairs the IETF LAKE standardization working group. Inria-AIO is heavily involved in real-world applications, and oversees over 1,000 sensors deployed on 3 continents for smart agriculture, smart city and environmental monitoring applications. The team's research program is organized around 5 pilars: Smart Dust, Low-Power Wireless Networking, Security in Constrained Systems, Swarm Robotics and Vehicle Area Networking.

Some pointers about the projects theAIO team is involved in:

- Team Homepage: https://aio.inria.fr/

Required Skills

We are looking for a student pursuing a Master's degree in Electronic Engineering, Computer Engineering, Embedded Systems, or an equivalent discipline.

"Hard" skills:

- Proficiency in low-level embedded programming (C language), particularly for microcontrollers.
- Understanding of microcontroller architectures and their operational characteristics.
- Familiarity with cryptographic principles, ideally experience implementing security protocols or mechanisms.
- Hands-on version control systems (Git, GitHub)

"Soft" skills:

- Clear communication and documentation skills.
- Motivated, independent, and proactive.
- Comfortable working in a collaborative environment.
- Proficiency in English required; French is a plus.

General Information

- **Research Theme :** Networks and Telecommunications
- **Locality :** Paris
- **Level :** Master
- **Period :** 1st January 2026 -> 31st March 2026 (3 months)

These are approximative dates. Please contact the training supervisor to know the precise period.

- **Deadline to apply :** 1st July 2025 (midnight)

Contacts

- **Training Supervisor :** Sara Faour / sara.faour@inria.fr
- **Second Training Supervisor :** Vučinić Mališa /

- Thomas Watteyne's homepage: Thomas Watteyne
- Videos of things we have been doing: Videos, Videos
- mm-scale micro-electronics: Welcome! - SCuM - Confluence
- Falco spin-off startup company: Accueil - Falco
- Smart Agriculture deployment in Argentina: PEACH – predicting frost events in peach orchards
- Environmental deployment in California: SNOWHOW – Real-Time Real-World Monitoring Systems
- Smart city deployment in the French Riviera: Smartmarina – Innovation at Work
- open-source 6TiSCH implementation: Confluence

malisa.vucinic@inria.fr
- **Team Manager :** Malisa Vucinic / malisa.vucinic@inria.fr

More information

- **Inria Team :** AIO
- **Inria Center :** Centre Inria de Paris