

Internship M/F – Embedded Fully Homomorphic Encryption



Rousset (Fr) / Milano (It)



WHY JOIN US

At ST, we are more than 50,000 creators and manufacturers of microelectronic technologies. We collaborate with over 200,000 customers and thousands of partners. Together, we design and create products and solutions that meet their challenges and the need to contribute to a more sustainable world. Our advanced technologies enable smarter mobility, more energy efficiency and power management, and large-scale deployment of the Internet of Things (IoT) and 5G. ST has received the Top Employer France and HappyTrainees 2023 certifications. They recognize us as a reference employer and demonstrate our commitment to making people a priority.

OUR FUTURE COLLABORATION

Cloud computing, blockchain smart contracts and online applications dealing with massive data are commonplace today. Nevertheless, it remains important to preserve data privacy during the end-to-end process, which is proving to be a complex task. Homomorphic encryption is one way of solving this problem. But it is clear that performance is the main bottleneck preventing its widespread deployment. On the other hand, IoT devices are increasingly deployed in the field and are becoming more and more powerful.

So much so, that we're seeing the emergence of embedded artificial intelligence and, in particular, hardware-accelerated embedded neural networks. Of course, the problem of maintaining the privacy of the data being manipulated remains. Hardware acceleration is undoubtedly the key to success for the advent of homomorphic cryptography in this field of application, and particularly the acceleration of fully homomorphic cryptography over the torus (TFHE). TFHE offers a bootstrapping function that makes it easy to implement a univariate function using a LUT, which is perfectly suited to implement activation functions used in neural networks.

Within a R&D team specialized in security, this 6-month internship will tackle the implementation of hardware acceleration for TFHE in a more general way without using FPGA hardware resources, but with a focus on embedded systems.

This internship could lead to a PhD thesis proposal.

Our technology starts with you. Come join our team!

YOUR PROFILE

- Last year of a master degree in cryptography, computer science.
- Knowledges in Hardware Description Language is a plus.
- Good level of written and spoken English (Resume and cover letter in English).

LOCATION

This internship can take place in Rousset, which is close to Aix-en-Provence, in France or in Agrate, close to Milano, in Italy.

HOW TO APPLY

In English, through STCareers portal:

- <https://stcareers.talent-soft.com>
- Reference: 2023-35644
- Title: "STAGE – Chiffrement entièrement homomorphe intégré H/F".



Ready to become
a Futurestarter?

Join ST and start the future #Futurestarters