Post-Quantum Cryptography Researcher

We are hiring!

eShard is a global, independent company with world-class expertise in security for embedded and mobile products. Companies like Google, Visa, NXP and other leading vendors around the world use our solutions and services.
We are strengthening our R&D team and are looking for a self-motivated individual ready to contribute to eShard's research on physical attacks applied to Post Quantum Cryptography implementations. The scope includes current and future algorithms selected by the NIST.
Do you have interest in working on PQC and hardware security topics, producing practical knowledge and know-how, publishing scientific articles and technical blog posts, and presenting your research to conferences ?
If so, your work and motivation will significantly contribute to eShard success.

Job description

Your day-to-day at eShard for this position

You mostly work on research topics related to hardware security analysis, such as physical attacks applied to PQC. Typical activities range across the following categories:

- Define and implement side-channel and/or fault injection attacks on innovative techniques or algorithms, such as PQC.
- Integrate research outcomes into the product portfolio in an appealing way, i.e. knowledge, tutorial and use case Python notebooks.
- Present the work to broad audiences from academic to industry.
- Follow the technical developments in the area and summarise your suggested technical orientations to the team.
- Collaborate with our technical partners (e.g. PQ Shield, academics).
- Contribute to hands-on customer and partner projects.

You also contribute to eShard's technical communication on hardware security. It can be writing articles for scientific reviews, blog posts for our website, preparing a poster or paper for a conference or a webinar to present one of your research topics.

You work from our office in Pessac, France; it's important to have a place of work to meet and hang out. Parts of a project may require interacting with customers all over the world. Our office culture is highly technical, our organisation fairly flat and our mindset flexible.

Your skills and experience

- Just graduated with a PhD
- PhD in Cryptography or Mathematics, Computer Science or related field with a strong focus on cryptography
- First experience in cryptography or side-channel analysis
- Master digital processing and statistical tools
- Background knowledge in chip microarchitectures
- Python programming
- Fair written and spoken English
- Good communication skills
- Time management and organisational skills to meet research project deadlines
- Teamwork
- Analytical and problem-solving skills
- Self motivated

Your benefits

- Competitive compensation package
- Flexible working hours, remote-friendly environment
- Strong focus on personal development
- High performance office equipment
- Comprehensive health insurance policy offering extensive medical, dental and vision care coverage
- Meal Vouchers
- Annual company outing plus snacks and drinks

Interested?

Send your resume and motivation letter to:

career@eshard.com

eShard

Get in touch

contact@eshard.com

www.eshard.com

France

Bâtiment GIENAH
11 avenue de Canteranne
33600 PESSAC

7 rue Gaston de Flotte
13012 Marseille