Research engineer : Authenticated Encryption for a Robust IoT

```
Position: Research engineer CNRS
Contract: fixed-term 9 months, gross salary 28k€/year minimum
Start date: ASAP
Location: Grenoble, Rhône-Alpes, France
Hosting institution: LIG laboratory, Université Grenoble Alpes, Grenoble Institute of Technology
Scientific advisors: Franck Rousseau @LIG/UGA, Marine Minier @LORIA/U.Lorraine, Pascal Lafourcade @LIMOS/UCA
Application deadline: 01/06/2017
```

Context

This project will take place in the scope of the PEPS OCAAA CHARIOT project, in the Drakkar research group at the LIG - Université Grenoble Alpes. LIMOS - Université Clermont Auvergne and LORIA - Université de Lorraine are partners in the project. The Internet of Things will succede only if the many security issues that we witness on a daily basis are solved. The IoT poses many challenges in terms of security. Many of the "Things" are devices with very stringent constraints in terms of energy, memory and processing power, and are often deployed in hard to control harsh environments.

Expected work

In the scope of the CHARIOT project, Chiffrement Authentifié pour la Robustesse de l'IoT, we will study security solutions based on symmetric authenticated encryption proposed in response to the CAESAR competition. We want to test these propositions in real-world conditions on very constrained devices. We will conduct experimentations on a local platform and IoT-lab.

Tasks :

- study various available OSes like Contiki, Riot and OpenWSN to propose a generic solution ; choose and experiment with one of these environments;
- implement some / all the CAESAR propositions;
- setup an experiment protocol and validate implementations;
- performances measurements and results analysis.

Outcome :

- portable implementation of the CAESAR algorithms;
- performance evaluation results in various typical IoT setups.

Skills & Expertise

Applicants for this position must have an engineer, MSc or PhD diploma in computer science.

Expected skills:

- Python and C programming languages;
- good software development practices (version control, tests);
- Unix-like environment.

Good to have:

- embedded systems programming;
- security and cryptography.

Location and Institution

The LIG laboratory is located in Grenoble, the capital of the Alps. Grenoble is one of France's major scientific and industrial centers for computer science and applied mathematics. The city lies amidst three mountain ranges and offers exceptional quality of life, with extensive public transportation and dedicated bikeways.

The Drakkar group investigates various aspects of network protocols, security and multimedia applications with an emphasis on wireless networks and sensors networks. The LIG lab has just moved to the brand new IMAG building, thus offering a very high standard work environment.

How to Apply & Contact Information

If you need additional information on this job offer, please contact Franck.Rousseau@imag.fr

Please apply by sending the following documents to Franck.Rousseau@imag.fr:

- Email subject MUST start with "[IR Chariot]";
- Letter of application;
- Curriculum vitae;
- Transcripts for undergraduate and graduate studies;
- References or letters of recommendation are appreciated.

On the WWW

- https://competitions.cr.yp.to/caesar.html
- https://www.iot-lab.info
- http://walt.forge.imag.fr