Cryptography Expert / Engineer

About CryptoExperts

CryptoExperts is a company founded by internationally recognized industrial and academic researchers in IT security and cryptography. Launched in Feb 2009, the company intends to fill the huge gap that exists between the scientific state of the art and the technology level found in current security products. Through both consulting services and business-driven innovation, we help the security industry benefit from the latest available advances in cryptography to improve their products and services. We have gathered - and go on gathering - cryptography experts with complementary skills and knowledge of the field to offer a unique panel of services ranging from product developement to the conception of new security systems. CryptoExperts' clients and partners include leading technology companies from around the world.

For more information: https://www.cryptoexperts.com/

Job description

White-box cryptography turns a keyed cryptographic algorithm into an unintelligible program with the same functionality. This white-box component can then be executed in an untrusted environment without fear of exposing the underlying keys. The code itself is tamper-proof, just as a secure element.

CryptoExperts develops and maintains a **white-box cryptography technology** which aims at producing white-box cryptography software components secure against beyond-state-of-the-art attacks. The technology is made of several ingredients:

- a framework for the design and implementation of white-box components,
- a portfolio of white-box components for the main cryptographic standards,
- a web service for the generation of white-box components,
- an attack toolkit to evaluate white-box components.

We are looking for a candidate who will take part to the design and implementation effort of CryptoExperts' white-box cryptography technology. In particular, the candidate will be asked to:

- improve our white-box generation framework (in terms of performances, diversity of white-box techniques, continuous integration),
- complete the portfolio of cryptographic algorithms covered by the white-box technology,
- monitor the state of the art in terms of practical white-box designs and attacks,
- research new encoding & obfuscation techniques for white-box implementations.

The candidate will also be invited to develop his/her expertise on other crypto related topics, through e.g. the participation to research projects or customer missions for the company.

Preferred experience

The candidate should have:

- good knowledge of cryptography / embedded software security
- deep development skills and experience (in particular in Python, C/C++)
- a particular taste for applied research
- organization and communication skills
- (optionally) a PhD in cryptography / cybersecurity
- (optionally) knowledge or experience with white-box cryptography

Application

To apply please write to jobs@cryptoexperts.com with

- a short description of your profile, story and motivation,
- your CV,
- (optionally) recommendation from (former) co-workers.