CryptoExperts

WE INNOVATE TO SECURE YOUR BUSINESS

# Offre de Stage – Intership Offer

*Secure wallet application for cryptocurrency*
*and blockchain transactions*

Novembre 2018

| | |
|---|---|
| **Type of internship:** | Master 2 or last year engineer student (6 months) |
| **Field:** | Software development, Cryptography |
| **Company:** | CryptoExperts |
| **Workplace:** | 41 boulevard des Capucines, 75002 Paris |

# 1 Company presentation

CryptoExperts is an SME providing outsourced R&D services in cryptography. The company is composed of experts from the industry and the academy, all with a Ph.D. in cryptography, and specialized in various fields (including public key cryptography, symmetric cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, and security of embedded systems). CryptoExperts develops innovative technologies for smart cards, pay-TV, payment, cloud and mobile phone security, and offers services of custom design, security audit, development and training in cryptography. The company is also very active in the field of scientific research in cryptography, producing every year several publications in the main conferences of the field, and taking part in various academic and industrial projects on advanced research issues (white-box cryptography, homomorphic encryption, proven security against physical attacks, pairings, lattices-based cryptography, group signatures and anonymous accreditations, etc.).

# 2 Proposed internship

## 2.1 Context

A cryptocurrency is an electronic currency that is based on a decentralized peer-to-peer network and that uses cryptography to validate transactions and create new coins. The cornerstone of a cryptocurrency is the so-called *blockchain* which is at the heart of the peer-to-peer network controlling the money. In a nutshell, the blockchain is a ledger that contains all the transactions since the origin of the cryptocurrency. The blockchain hence reveals the amount held in each account. A cryptocurrency account is identified by a hexadecimal string encoding a public key and the corresponding private key can then be used by its (anonymous) owner to sign a transaction that transfers coins to another account. Many cryptocurrencies are based on ECDSA (Elliptic Curve Digital Signature Algorithm). In order to be acknowledged as valid, a transaction must be included in the blockchain. This is achieved through the so-called mining process which consists in gathering several transactions into a block and by computing a *proof of work* on this block (which is linked to previous blocks as well). Each time a new block with valid proof of work is pushed to the peer-to-peer network, it is added to the blockchain and all the nodes must take it into account in the mining of the next blocks. The incentive for this validation work comes from the fact that mining a new block is rewarded with new coins for the miner and with transactions fees.

Cryptocurrencies have emerged in the last decade after the publication and development of the Bitcoin system [4]. As of today, there exists more than a hundred cryptocurrencies with a capitalization beyond 25 million US$, and the capitalization of the Bitcoin (the highest one) exceeds 50 billion US$. But more than solving the longstanding e-cash issue, many new applications have emerged from the blockchain technology. In particular, the ledger capability offered by the blockchain enables a reduction of the cost attributed to the verification of transactions by removing the need for a trusted third party in many applications.

The main security issue with cryptocurrencies resides on the protection of the users' secret keys, which reveals to be a hard task in practice, especially in an open environment like a smartphone. Even the most ephemeral key exposure allows an adversary to sign a transaction transferring all the coins on the account to another (pirate) account. The signed transaction is then instantly pushed to the peer-to-peer network and quickly added to the blockchain, which makes it irreversible. Many malware programs have been identified that steals cryptocurrencies from owners who use weak protection mechanisms.

## 2.2 Description

The goal of the internship is to develop a secure cryptocurrency wallet application running on Android devices. The first milestone will consist in a first version of the application enabling the storage and spending of cryptocurrency coins (and in particular bitcoins). In parallel we will investigate different ways of securing the storage and handling of the secret keys, possibly using white-box cryptography [1], software obfuscation [2] and multiparty computation [3].

In a second phase, a hardened version of the application will be developed possibly in conjunction with a cloud service. The foreseen architecture makes use of a dynamic ECDSA white-box implementation that can operate transactions from *tokens*. A token can be seen as a secure container for an ECDSA private key which can only be operated by a pre-determined white-box implementation and which might be locked by a password and various data (e.g. some environmental fingerprint depending on the phone, biometric data, etc.). Additionally, a token might be constrained to be bounded on the transaction amount. The demonstrator will then include a token generation program turning unprotected ECDSA keys into tokens from a secure platform (protected desktop computer or dedicated server). Figure 1 gives an overview of the foreseen architecture.

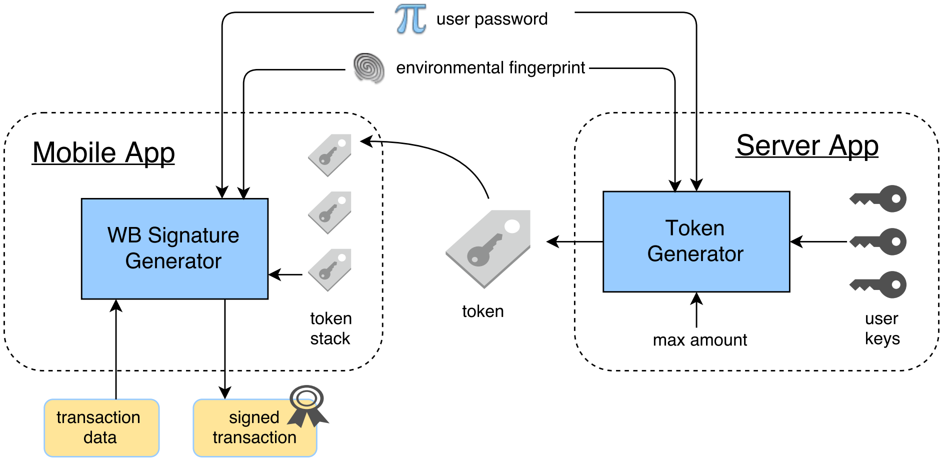

Figure 1: Overview of the cryptocurrency wallet architecture.

The white-box signature generator as well as the token generator should be user dependent and they should be linked so that generated tokens can only be operated by the corresponding white-box implementation. Moreover, the tokens should be useless without the associated white-box implementation, and without the password and environmental data that lock them. In particular, a token alone should not leak any information on the underlying private ECDSA key.

If time allows, we will also investigate how to extend the application to support multisignatures which require more than one key to authorize a transaction and further security features to be gained by using multiparty computation.

## 3 Candidates

This internship offer is for a Master 2 or final year engineer student who has a taste for cryptography and software development. The candidate will have to demonstrate a solid background in computer science, programming, and (preferably) in cryptography. The candidate will have to demonstrate autonomy and dynamism. A good level of English is also desired.

## 4 Contact

To apply, please send your resume to Matthieu Rivain: matthieu.rivain@cryptoexperts.com

## References

[1] Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. White-box cryptography and an AES implementation. In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 250–270. Springer, Heidelberg, August 2003.

[2] Christian Collberg, Clark Thomborson, and Douglas Low. A taxonomy of obfuscating transformations, 1997. https://researchspace.auckland.ac.nz/bitstream/handle/2292/3491/TR148.pdf.

[3] Ronald Cramer and Ivan Damgard. Multiparty computation, an introduction, 2004. https://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/cramer/mpc.ps.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. bitcoin.org.