Offre de Stage - Internship Offer

*Homomorphic Encryption of Neural Networks*

September 2021

<table>
<thead>
<tr>
<th><strong>Type of internship:</strong></th>
<th>Master 2 or last year engineer student (6 months)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field:</strong></td>
<td>Cryptography</td>
</tr>
<tr>
<td><strong>Company:</strong></td>
<td>CryptoExperts</td>
</tr>
<tr>
<td><strong>Workplace:</strong></td>
<td>41 boulevard des Capucines, 75002 Paris</td>
</tr>
</tbody>
</table>
1 Company presentation

CryptoExperts is an SME providing outsourced R&D services in cryptography. The company has a team of experts from industry and the academy, all with a Ph.D. in cryptography, and specialized in various fields. They include public key cryptography, symmetric cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, and security of embedded systems. CryptoExperts develops innovative solutions for smart cards, pay-TV, payment and secure messaging services, and offers security auditing, certification support, and training services 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 Internship description

2.1 Context

The increasing use of deep learning techniques raises new privacy issues. If the inference computation is outsourced to an external server, then the data owner is expected to share their unencrypted data to initiate their analysis. On the contrary, if the inference computation is managed locally, then the (proprietary) model can be revealed by software disassembly.

Homomorphic encryption (FHE), introduced in 2009 by Gentry [4] offers a cryptographic solution to this paradox. This innovative technique makes it possible to perform calculations directly on encrypted data, without revealing any information. Namely, certain operations can be carried out directly on encrypted data, while preserving the confidentiality of the request and of the result. Many works have been published to improve and extend the first construction of 2009 but their complexity often remains prohibitive.

A few years ago, the cryptographic community began to take an interest in the application of deep learning techniques to neural networks [5]. In particular, CryptoExperts partly designed one of the first FHE systems of this type [1]. Specifically adapted to certain classes of neural networks, this system is able to operate on encrypted data with linear complexity in the size of the network.

2.2 Subject

CryptoExperts has been recently involved in a collaborative project where one of the challenges is to both preserve the confidentiality of a company’s neural network and the confidentiality of users’ data to analyze. While homomorphic encryption typically offers a relevant solution, several techniques can be employed according to the target neural networks and the data structure.
In this internship, the candidate will be asked to focus on a specific category of convolutional networks that are widely used to classify documents and exhibit chosen fields. Together with his/her supervisor, the candidate will investigate different homomorphic methods to protect the confidentiality of the model (e.g., weights, number of layers) as well as the confidentiality of the input data to analyze that must remain encrypted.

In particular, he/she will start by studying CKKS [2] (named after its designers Cheon, Kim, Kim, and Song) and TFHE [3] (Fully Homomorphic Encryption over the Torus) and implement them both in Python for basic operations (e.g., additions, multiplications). Both techniques theoretically make it possible to transform an arithmetic circuit into a functionally equivalent circuit which operates directly on encrypted data.

Then, the candidate will instantiate and apply both techniques to a specific convolutional network that is yet to be defined. Some more operations will probably be required, like the ReLU and softmax non-linear activation functions and the max pooling convolution process. Tests will be defined and carried out to select good approximations for these functions and relevant homomorphic parameters (e.g., noise, precision, data size) for both techniques in order to obtain the best possible trade-offs in terms of security of the encryption, concrete performances, and network accuracy when processing encrypted data.

Finally, the intern will try to find theoretical and practical optimizations to improve both the final accuracy and the global performances while preserving the scheme security. At this step, variants of CKKS and TFHE can also be studied.

3 Candidates

This internship offer is for a Master student who has a taste for cryptography and applied research. The candidate will have to demonstrate a solid background in mathematics and/or computer science with a specialization in cryptography. The technical background required for this internship combines skills in algebra (finite fields, polynomials, etc.) as well as ease in programming. The candidate will have to demonstrate autonomy and dynamism. A good level of English is also desired.

4 Contact

To apply for this internship offer, please send your résumé to

Sonia Belaïd: sonia.belaid@cryptoexperts.com.

References


