Proposition de recherche doctorale

Implémentation de fonctions cryptographiques homomorphiques et d'outils de cryptanalyse

Mots clés :

- **Directeur de thèse** : Jean-Claude Bajard
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

{New cryptanalytic techniques for SHE (Somewhat Homomorphic Encryption) computational problems: } Currently the computational problems on which SHE schemes have not been studied in depth; this leaves some doubt on the security and minimum key sizes of SHE. Our cryptanalytic work will concentrate on the following problems which are the basis of most SHE: Approximate GCD computation, Learning with Errors Structured lattice reduction... The PhD will start with the study of the basic computational problems used in FHE schemes from a cryptanalytic standpoint. This task will be studied both from an asymptotic point of view, trying to find algorithms with the lowest possible asymptotic complexity, and from a concrete viewpoint, trying to devise the fastest possible algorithms and implementation optimizations. {Hardware implementations of a selection of SHE schemes: } This task will consider two approaches: the first approach is a full implementation of a selection of SHE schemes capable of handling low depth circuits on FPGAs to assess the resource consumption both in silicon and computing time. Particular focus will be placed on the FFT subroutines and Gaussian samplers. The second approach will consist of a proper SW/HW co-design in the embedded environment, where a dedicated co-processor will be designed to speed-up very specific subroutines such as (part of) the FFT computation or even a big integer multiplier. Since the MCUs used (32 bit e.g. ARM M series) are not so powerful, reasonable execution time and cost can only be achieved by using a dedicated HW accelerator. The PhD will consider also the cryptanalytic implementations. In order to better understand the long-term viability of homomorphic encryption (still a new form of encryption), and to specify security parameters in a much more effective way than currently, the most promising cryptanalytic algorithms designed in the first study will be implemented and their effectiveness assessed. References - Craig Gentry: Fully homomorphic encryption using ideal lattices. STOC 2009: 169-178 - Marten van Dijk, Craig Gentry, Shai Halevi, Vinod Vaikuntanathan: Fully Homomorphic Encryption over the Integers. EUROCRYPT 2010: 24-43 - Zvika Brakerski, Vinod Vaikuntanathan: Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011: 505-524 - Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106

Résumé du projet de recherche (Langue 2)

L'implémentation de fonctions cryptographiques homomorphiques et d'outils de cryptanalyse est un véritable challenge de la cryptologie actuelle.