2018-00697 - Post-doctoral position: division property, integral distinguishers, cube testers: some ways to attack block and stream ciphers. [S]

Type de contrat : CDD de la fonction publique
Niveau de diplôme exigé : Thèse ou équivalent
Autre diplôme apprécié : PhD
Fonction : Post-Doctorant

Contexte et atouts du poste

Environment of the position

The post-doctoral researcher will be hosted by the Caramba research group (http://caramba.loria.fr/) of Inria Nancy Grand Est and LORIA. The objective of the Caramba team is to contribute research on the number field sieve algorithm and its siblings, for integer factorization and discrete logarithm in finite fields; algebraic curves for cryptography, in particular genus 2 curves and pairings; Arithmetic in general, from integers to floating-point numbers, in software and hardware;

Mission confiée

Scientific context

Cryptography is a cornerstone of everyday digital security as it aims at ensuring confidentiality and integrity of digital communications. These tasks are achieved by using public key cryptography and symmetric cryptography where the two parties that want to communicate share a common key. Among the primitives in symmetric key cryptography, we could cite block and stream ciphers that ensure confidentiality of information.

As these primitives are widely used, it is of outermost importance to evaluate the actual security level they ensured, and cryptanalysis aims at testing these security levels. This task usually consists in mounting attacks for recovering secret keys or a part of them. Those attacks are most of the times, based on an undesirable property that allows to distinguish a true random permutation from the cipher under analysis. Among the particular distinguishers, we propose to study during this post-doctoral position, we will mainly focus on integral distinguishers, on the so-called division properties and on cube attacks.

Integral or saturation distinguishers has been first introduced in [1]. For identifying an integral distinguisher of a block cipher, we first consider a set of chosen plaintexts that contains all possible values for some bits and constant value for the other bits. Then the corresponding ciphertexts are calculated from plaintexts in the set by using an encryption oracle. If the XOR of the corresponding ciphertexts always becomes 0, we say that this cipher has the integral distinguisher.

Todo [2] generalized the concept of integral and higher order differential distinguisher, and discovered a new distinguishing property against block ciphers, called the division property. This property was used to present new generic distinguishers against block ciphers. More precisely, it means that a set X has the division property \( D(k, n) \), if the sum over all vectors on X of a particular product of terms raised to a certain power lower than k equals 0. The division property then generalizes integral attacks in the sense that \( D(2, n) \) means that the set X is balanced, while \( D(n, n) \) means that it is saturated. The distinguishers described by Todo in [2] thus exploit the classical properties used in integral attacks together with some algebraic properties related to the degree of several iterations of a nonlinear function.

Recently, many research papers have been published based on this new distinguishing property against block ciphers and stream ciphers in leading crypto conferences. Among them, Boura and Canteaut [3], proposed a new approach of...
division property by introducing the notion of parity sets and of intermediate properties that could be easily propagate through the successive rounds of a cipher by capturing some information resulting from the algebraic degree of the round function. This new approach enables to provide a simpler formulation and interpretation of the division property of any order. Moreover, it is proved that the division property of any order can be expressed in an elegant way by using the theory of Reed-Muller codes.

**Bibliography**


**Principales activités**

**Project description**

The objectives of this project will be to first have a global vision on the links between division property, integral distinguishers and cube attacks and then to apply those attacks on block ciphers and stream ciphers. We will mainly focus on lightweight block ciphers and on particular stream ciphers. Moreover, in some particular cases, integral attacks could result into a sum property that is not 0 but equal for two different words, i.e. the higher-order differentials for those two words are equal to the same constant different from 0.

Then, taking into account the interests of the candidate and the progress of the work, the candidate could specialize his/her work on one (or several possible subject):
- Theoretical links between those three attacks.
- Dedicated cryptanalysis on previously chosen stream and block ciphers.
- Improving existing attacks using MILP (Mixed Integer Linear Programming).
- Find other criterias for the basic building blocks of a stream or a block cipher to resist to those attacks.

**Compétences**

We expect the candidate to be familiar with the following subjects:

- Solid knowledge on symmetric key cryptography, in particular boolean functions and/or cryptanalysis.
- Solid programming experience.
- Solid skills in probability theory and statistics.

**Avantages sociaux**

- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- French courses

**Rémunération**

Salary: 2653€ gross/month

In addition, at least one recommendation letter from your PhD advisor should be sent directly by their author(s) to marine.minier@inria.fr.

Applications are to be sent as soon as possible.

**A propos d'Inria**

Inria, institut de recherche dédié au numérique, promeut « l'excellence scientifique au service du transfert technologique et de la société ». Inria emploie 2700 collaborateurs issus des meilleures universités mondiales, qui relèvent les défis des sciences informatiques et mathématiques. Son modèle ouvert et agile lui permet d’explorer des voies originales avec ses partenaires industriels et académiques. Inria répond ainsi efficacement aux enjeux pluridisciplinaires et applicatifs de la transition numérique. Inria est à l’origine de nombreuses innovations créatrices de valeur et d’emplois.

**Conditions pour postuler**

**Sécurité défense :**

Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L’autorisation d’accès à une zone est délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

**Politique de recrutement :**

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

**Attention:** Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.