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

Contract type: Public service fixed-term contract
Level of qualifications required: PhD or equivalent
Other valued qualifications: PhD
Fonction: Post-Doctoral Research Visit

Context
Environment of the position

The post-doctoral researcher will be hosted by the Caramba research group (http://caramba.loria.fr/) of Inria NancyGrand 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;

Assignment
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.

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 mean 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


Main activities
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.

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

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

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

Remuneration
Salary: 2653€ gross/month

General Information
- Theme/Domain : Algorithmics, Computer Algebra and Cryptology
- Town/city : Villers-lès-Nancy
- Inria Center : CRI Nancy - Grand Est
- Starting date : 2018-11-01
- Duration of contract : 1 year, 4 months
- Deadline to apply : 2018-06-06

Contacts
- Inria Team : CARAMBA
- Recruiter : Minier Marine / marine.minier@inria.fr

About Inria
Inria, the French National Institute for computer science and applied mathematics, promotes “scientific excellence for technology transfer and society”. Graduates from the world’s top universities, Inria’s 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

The keys to success

Application deadline
June 6th, 2018 (Midnight Paris time)

How to apply
Upload your file on jobs.inria.fr in a single pdf or zip file, and send it as well by email to marine.minier@inria.fr. Your file should contain the following documents:

- CV including a description of your research activities (2 pages max) and a short description of what you consider to be your best contributions and why (1 page max and 3 contributions max); the contributions could be theoretical or practical. Web links to the contributions should be provided. Include also a brief description of your scientific and career projects, and your scientific positioning regarding the proposed subject.
- The report(s) from your PhD external reviewer(s), if applicable.
- If you haven't defended yet, the list of expected members of your PhD committee (if known) and the expected date of defense (the defense, not the manuscript submission).

In addition, at least one recommendation letter from your PhD advisor should be sent directly by their author(s) to
Applications are to be sent as soon as possible.

**Conditions for application**

**Defence Security :**
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

**Recruitment Policy :**
As part of its diversity policy, all Inria positions are accessible to people with disabilities.

**Warning :** you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.