Then, taking into account the interests of the candidate and the progress of the work, the candidate context, we will mainly focus on lightweight block ciphers and on particular stream ciphers. 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 elements of the underlying field, such as integers or bits. Then, we define a function that maps each plaintext to a value, typically a boolean function. If the function returns 0 for all plaintexts in the set, we say that the cipher has the integral distinguisher.

**Todo** [2] generalized the concept of integral and higher order differential distinguishers, 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. In this new approach, we can 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 equal to 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 context, we will mainly focus on lightweight block ciphers and on particular stream ciphers.
could specialize his/her work on one (or several possible subjects):

- 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 criteria 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 cryptanalysis.
- Solid programming experience.
- Solid skills in probability theory and statistics.

**Benefits package**

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

**Remuneration**

Salary: 2653€ gross/month

---

**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.