

# Workshop on Boolean functions: Cryptography and Applications

The workshop on Boolean functions Cryptography and applications provides a forum for researchers with interests within all aspects of boolean function theory and applications to cryptography. It is co-organized by the LIFAR and the LIAFA.

## Program Committee

- Claude Carlet (Univ. Paris 8, INRIA)
- Hervé Chabanne (SAGEM)
- Pascal Charpin (INRIA)
- Jean-Charles Faugères (CNRS, LIP6)
- Louis Granboulan (ENS, GRECC)
- Étienne Grandjean (Univ. Caen, GREYC)
- Jean-François Michon (Univ. Rouen, LIFAR)
- Pierre Valarcher (Univ. Rouen, LIFAR)
- Jean-Baptiste Yunes (Univ. Paris 7, LIAFA)

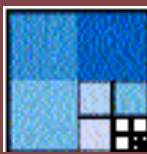
## Organization Committee

- Jean-François Michon (Univ. Rouen, LIFAR)
- Pierre Valarcher (Univ. Rouen, LIFAR)
- Jean-Baptiste Yunes (Univ. Paris 7, LIAFA)

## Support Committee

- Jean-Eric Pin (CNRS, LIAFA)

LIFAR  
LIAFA



LIAFA

Papers on all aspects of cryptography and boolean functions are welcomed, be they theoretical, implementation oriented or experiments reports. The venue for this workshop will be **Rouen University** in Haute-Normandie, FRANCE.

Original papers will be solicited on practical aspects of:

1. *Algebraic geometry over  $F_2$ ,*
2. *Random Generation,*
3. *Boolean Complexity,*
4. *BDD and cryptography,*
5. *Stream Cipher*
6. ...

All speakers attending the workshop are invited to submit a paper for the draft proceedings. This implies (among other things) that:

- \* the paper should be written in English
- \* the paper is well written
- \* the topic of the paper should be stated clearly
- \* the approach to solve the problem should be outlined clearly
- \* a detailed discussion of the solution has to be given
- \* the solution is compared with relevant related work
- \* there is an abstract, introduction and conclusion.
- \* the conclusion should summarize the problem, the solution, and how this solves the problem.
- \* papers must not exceed 16 pages.
- \* the paper should be submitted as a PostScript or PDF file by email to the program co-chairs,

[Pierre.Valarcher@univ-rouen.fr](mailto:Pierre.Valarcher@univ-rouen.fr),  
[Jean-Baptiste.Yunes@liafa.jussieu.fr](mailto:Jean-Baptiste.Yunes@liafa.jussieu.fr)

## Important Dates

- Submission for draft proceedings : **January 10th, 2005**
- Notification of acceptance/rejection : **February 11th 2005**
- Workshop at Rouen University : **March 7, 8 and 9, 2005**

