Baptiste Lambin
baptiste.lambin51@gmail.com
people.irisa.fr/Baptiste.Lambin/

Work address
Office F409, IRISA
Campus Universitaire de Beaulieu
35700 Rennes, France

Baptiste Lambin

Formation

2016-2019, PhD Thesis
Cryptanalysis of lightweight symmetric primitives
Advisors : Pierre-Alain Fouque, Patrick Derbez, at Université de Rennes 1, France

2014 - 2016, Master Degree CRYPTIS, with honors
Université de Limoges, France

2011 - 2014, Bachelor of Science Degree in Pure Mathematics, with honors
Université de Reims Champagnes-Ardennes, France

Teaching

INF1 *Introduction to imperative programming in Java*, Level L1, 100h over 3 years
Theoritical exercices, practical exercices and writing some exercises sheets

OIA *Follow-up course of INF1 for maths students*
Level L1, 24h over 2 years, practical exercices

BCS *Implementation of some cryptographic primitives and attacks for non-crypto students*
Level M2, 16h over 1 year, practical exercices

SECU *Introduction to cryptography and some HTML/PHP vulnerabilities*
Level M1, 36h over 1 year, theoritical exercices and practical exercices

APS *Follow-course of SECU, emphasis on cryptanalysis*
Level M1, 24h over 2 years, practical exercices

Private Lessons *Mathematics for High Schoolers and first year students*
10 students between 2013 and 2015, about 1-2h per week per student

Research

Variants of the AES Key Schedule for Better Truncated Differential Bounds
Patrick Derbez, Pierre-Alain Fouque, Jérémy Jean, Baptiste Lambin
accepted and presented at SAC 2018

On Recovering Affine Encodings in White-Box Implementations
Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, Brice Minaud
accepted and presented at CHES 2018

Talks

Variants of the AES Key Schedule for Better Truncated Differential Bounds
Presented at Journées Codages & Cryptographie 2018 and at the Caen Crypto Seminar

On Recovering Affine Encodings in White-Box Implementations
Presented at Séminaire C2 in Paris and at Journées Codages & Cryptographie 2017

Ma thèse en 180 Secondes
Online video (in french) : `https://youtu.be/u-1Nqg9SSz8`

Skills and Interests

Maths : Linear Algebra, Finite Fields, Arithmetic, Probabilies
Cryptography : Symmetric cryptanalysis : Division Property, Differentials, Boomerang,...
Progamming : C++, Python, SAGE, Gurobi (MILP solver), Minizinc (CP Solver)

Hobbies

Music, Video Games, Kendo, TV Series, Go...