Valérie NACHEF-TARDIVEL

Publications

1 International journal and conference papers

- Differential Attacks on Generalized Feistel Schemes
  Valérie Nachef, Emmanuel Volte, Jacques Patarin
  CANS 2013- Lectures Notes in Computer Sciences, 8257, Springer-Verlag 2013, 1-19

- Zero Knowledge with Rubik's Cubes
  Emmanuel Volte, Valérie Nachef, Jacques Patarin
  CANS 2013- Lectures Notes in Computer Sciences, 8257, Springer-Verlag 2013, 1-19

- Zero-Knowledge for Multivariate Polynomials
  Valérie Nachef, Jacques Patarin, Emmanuel Volte
  LATINCRYPT 2012- Lectures Notes in Computer Sciences, 7533, Springer-Verlag 2012, 74-91

- Indifferentiability beyond the Birthday Bound for the XOR of Two Public Permutations.
  Avradip Mandal, Jacques Patarin, Valérie Nachef
  INDOCRYPT 2010- Lectures Notes in Computer Sciences, 6498, Springer-Verlag 2010, 69-81

- Improved Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions
  Emmanuel Volte, Valérie Nachef, Jacques Patarin
  ASIACRYPT 2010- Lectures Notes in Computer Sciences, 6477, Springer-Verlag 2010, 94-111

- Generic Attacks on MISTY Schemes
  Valérie Nachef, Jacques Patarin, Joana Treger
  LATINCRYPT 2010- Lectures Notes in Computer Sciences, 6212, Springer-Verlag 2010, 220-240

- I shall love you until death.
  Valérie Nachef, Jacques Patarin
  Cryptologia, 34, n° 2 (2010), 104-114

- Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions
  Jaques Patarin, Valérie Nachef, Côme Berbain
  ASIACRYPT 2007- Lectures Notes in Computer Sciences, 4833, Springer-Verlag 2007, 325-341

- Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions
  Jaques Patarin, Valérie Nachef, Côme Berbain
  ASIACRYPT 2006 - Lectures Notes in Computer Sciences, 4284, Springer-Verlag 2006, 396-414

- Sobolev Algebras on Lie Groups and Riemannian Manifolds
  Thierry Coulhon, Emmanuel Russ, Valérie Tardivel-Nachef

Amer.J.Math , 123, (2001), 283-342

- Haar Invariant Sets
  Catherine Finet, Valérie Tardivel-Nachef
  Journal of Mathematical Analysis and Applications,197, (1996), 138-152

- Lacunary Sets on Transformation Groups
  Catherine Finet, Valérie Tardivel-Nachef
  Hokkaido Math. J., 23, (1994), 1-19

- A Variant of a Yamaguchi's Result
  Catherine Finet, Valérie Tardivel-Nachef
  Hokkaido Math. J., 21, (1992), 483-489

- The Class of Synthezisable Pseudo-measures
  A.S.Kechris, Alain Louveau, Valérie Tardivel
  Illinois J. Math., Vol 35, n^o 1, (1991), 107-146

- Ensembles de Riesz
  Valérie Tardivel
  Trans. Amer. Math. Soc., 305 n^o 1(1988), 167-174

- Fermés d'Unicité dans les Groupes Localement Compacts
  Valérie Tardivel
  Studia Mathematica, 91, (1988), 1-15

2 NIST (National Institute of Standard and Technology) Submission : SHA-3 Competition

- CRUNCH
  Louis Goubin, Mickael Ivasco, William Jalby, Olivier Ly, Valérie Nachef, Jacques Patarin, Joana Treger, Emmanuel Volte.
  Submission to NIST, 2008.

3 Vulgarisation papers

- Marie-Antoinette... Reine de la cryptographie.
  Valérie Nachef, Jacques Patarin
  Pour la Science - n^o 382, Août 2009, 74-78

4 Papers posted on eprint Archive

- 4-point Attacks with Standard Deviation Analysis on A-Feistel Schemes
  Valerie Nachef, Jacques Patarin, Emmanuel Volte
  Cryptology ePrint Archive 2014/446 : Listing for 2014

– Zero-Knowledge for Multivariate Polynomials
Valerie Nachef, Jacques Patarin, Emmanuel Volte
Cryptology ePrint Archive 2012/239 : Listing for 2012

– Zero Knowledge with Rubik's Cubes and Non-Abelian Groups
Emmanuel Volte, Jacques Patarin and Valérie Nachef
Cryptology ePrint Archive 2012/174 : Listing for 2012

– Differential Attacks on Generalized Feistel Schemes
Valérie Nachef, Emmanuel Volte, Jacques Patarin
Cryptology ePrint Archive 2011/750 : Listing for 2011

– Generic Attacks on Misty Schemes -5 rounds is not enough-
Valérie Nachef, Jacques Patarin, Joana Treger
Cryptology ePrint Archive 2009/405 : Listing for 2009

– Generic Attacks on Alternating Unbalanced Feistel Schemes
Valérie Nachef
Cryptology ePrint Archive 2009/287 : Listing for 2009

– I shall love you up to the death
Valerie Nachef, Jacques Patarin
Cryptology ePrint Archive 2009/166 : Listing for 2009

– Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions - Extended Version
Jaques Patarin, Valérie Nachef, Côme Berbain
Cryptology ePrint Archive 2007/449 : Listing for 2007

5 Communications

– Pseudo-mesures et Synthèse
Valérie Tardivel
Séminaire d'Initiation à l'Analyse (G.Choquet-M.Rogalski-J.Saint Raymond)
27 ^{e} année 1987-1988

– Unicité et Synthèse
Valérie Tardivel
Séminaire d'Initiation à l'Analyse(G.Choquet-M.Rogalski-J.Saint Raymond)
27 ^{e} année 1987-1988

– Construction d'Ensembles de Type U_0 qui ne sont pas de Type U
Valérie Tardivel
Séminaire d'Initiation à l'Analyse (G.Choquet-M.Rogalski-J.Saint Raymond)
25 ^{e} année 1985-1986 Communication n^{o} 1

– Ensembles d'Unicité d'après R.M. Solovay
Valérie Tardivel
Séminaire d'Initiation à l'Analyse (G.Choquet-M.Rogalski-J.Saint Raymond)

6 Preprints

– The different cases for Random Feistel schemes when $m = 4$
Valérie Nachef
Preprint 2005

– Random Feistel schemes for $m = 3$
Valérie Nachef
Preprint 2004