Aalto University, School of Science,
Department of Information and Computer Science,
P.O. Box 15400,
FI-00076 Aalto,
Finland
+358 449706979
celine.blondeau@aalto.fi
http://users.ics.aalto.fi/blondeau/

Céline Blondeau

Curriculum Vitae

Personal Information

Last Name	Wieringa
Maiden Name	Blondeau
First Name	Céline
Date of Birth	22th November, 1985
Place of Birth	Saint Quentin, Aisne, France
Nationality	French
Marital Status	Married

Education

2011 **PhD Thesis**, *Université Pierre et Marie Curie, Paris VI*, France, Title: *Differential cryptanalysis and its generalizations*, Advisor: Pascale Charpin, INRIA Paris-Rocquencourt .
Obtained with honour

2008 **Master Degree in Cryptography**, *Université de Limoges, Limoges*, France.
excellent success

2006 **Bachelor Degree in Mathematics**, *Université Jules Verne, Amiens*, France.
excellent success

2003 **Scientific High School Degree**, *Lycée Gay Lussac, Chauny*, France.
excellent success

Pedagogical Training

2014 **SCYPE course clinic**, *5 credits*, School of Science, Aalto University.

2013 **SCYPE introductionary course**, *5 credits*, School of Science, Aalto University.

Languages

French	**Native**
English	**Fluent**
Finnish	**Learning**

Dutch **Learning**

Actual Position

Sept. 2011- **Researcher**, *Aalto University, School of Science*, Department of Information and Computer Science.
Member of the Cryptographic Team

Experience

Current **Postdoctoral Researcher**.
Researcher in the Cryptographic Group,
Department of Information and Computer Science (ICS),
Aalto University School of Science,
Espoo, Finland
Team Leader: Kaisa Nyberg

2008-2011 **PhD Student**.
Project-team SECRET,
Research center, INRIA Paris-Rocquencourt,
Rocquencourt, France
Team Leader: Anne Canteaut

Teaching Experience

2013-2014 **Assistant in charge of the programming assignments, "Cryptography and Data Security"**.
ICS Department, School of Science, Aalto University, Espoo, Finland

2012-2013 **Teaching assistant, "Computational Complexity Theory"**.
ICS Department, School of Science, Aalto University, Espoo, Finland

2011-2012 **Teaching assistant, "Cryptology"**.
ICS Department, School of Science, Aalto University, Espoo, Finland

Teaching assistant, "Computational Complexity Theory".
ICS Department, School of Science, Aalto University, Espoo, Finland

2010-2011 **Teaching assistant, "Algorithmique et Programmation"** .
Engineering School, ENSTA, Paris, France

Teaching assistant, "Informatique Générale".
Biology Engineering School, Polytech'Paris, Université Pierre et Marie Curie, Paris, France

2009-2010 **Teaching assistant, "Algorithmique et Programmation"**.
Engineering School, ENSTA, Paris, France

Teaching assistant, "Cryptographie et Sécurité".
Master SeCReTS (Computer Science), Université de Versailles-Saint-Quentin-en-Yvelines, France

2008-2009 **Teaching, "Mathématiques 1ère année"**.
DUT génie éléctique et information industrielle, IUT de Cachan, Université de Paris Sud, France

Supervision

2014 **Supervision of a Master's Student**.
Masoud Naderpour

2012-2013 **Supervision of a Master's Student**.
Léo Perrin

Seminars and Invited Talks

2014 **Complexity of Statistical Attacks: On the Relation between Chosen and Known Plaintext Attacks**, *Seminar on Cryptography, Dagstuhl*, Germany, January 2014.

2013 **Using Multiple Differentials... On the LLR and χ^2 Statistical Tests in Differential Context**, *Early Symmetric Crypto (ESC), Mondorf-les-Bains*, Luxembourg, January 2013.

2012 **Utilisation des tests statistiques : LLR et χ^2 pour la cryptanalyse différentielle**, *Journée Codage et Cryptographie, Dinard*, France, October 2012.

Cryptanalysis of Armadillo, *Université de Rennes*, France, February 2012.

Cryptanalysis of Armadillo, *Université de Caen*, France, February 2012.

2011 **Data complexity and success probability of statisticals cryptanalysis**, *Aalto university*, Finland, May, 2011.

2010 **Propriétés différentielles des fonctions puissances**, *Université de Paris VIII* , France, January 2010.

2009 **Data Complexity and Success Probability for various cryptanalysis**, *Darmstadt*, Germany, October 2009.

Program Committee

2015 **FSE 2015**, *Fast Software Encryption, Workshop*.

2014 **YACC 2014**, *Yet Another Conference on Cryptography, Workshop*.

SAC 2014, *Selected Areas in Cryptography, Conference*.

INDOCRYPT 2014, *15th International Conference on Cryptology, Conference*.

Other Reviewing Tasks

2014 **Finite Fields and Their Applications**, *International Journal*.

Advances in Mathematics of Communications, *International Journal*.

Designs, Codes and Cryptography, *International Journal*.

IEEE Transactions on Information Theory, *International Journal*.

ASIACRYPT 2014, *20th Annual International Conference on the Theory and Application of Cryptology and Information Security*.

AFRICACRYPT 2014, *Annual International Conference on the Theory and Applications of Cryptology*.

ACNS 2014, *12th International Conference on Applied Cryptography and Network Security*.

EUROCRYPT 2014, *33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*.

2013 **ASIACRYPT 2013**, *19th Annual International Conference on the Theory and Application of Cryptology and Information Security*.

SAC 2013, *Selected Areas in Cryptography 2013*.

FSE 2013, *19th International Workshop on Fast Software Encryption*.

AFRICACRYPT 2013, *6th International Conference on Cryptology in Africa*.

ACNS 2013, *11th International Conference on Applied Cryptography and Network Security*.

Information Processing Letters, *International journal*.

ACM Transactions on Information and System Security, *International journal*.

Designs, Codes and Cryptography, *International Journal*.

2012 **Finite Fields and Their Applications**, *International journal*.

FSE 2012, *19th International Workshop on Fast Software Encryption*.

CRYPTO 2012, *32th-International Cryptology Conference*.

SAC 2012, *Conference on Selected Areas in Cryptography*.

2011 **Designs, Codes and Cryptography**, *International Journal*.

2010 **Indocrypt 2010**, *11th International Conference on Cryptology in India*.

Other Experience

Summers 2013-2014 — **Kayak Instructor**.
Canoa, Espoo, Finland

Summers 2002–2005 — **Kayak Instructor**.
CKPA, Chauny, France
Thiérache Sport Nature, Hirson, France