Céline Blondeau
Aalto University, School of Science,
Department of 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	Blondeau
Marital Name	Wieringa
First Name	Céline
Date of Birth	22th November, 1985
Place of Birth	Saint Quentin, Aisne, France
Nationality	French
Marital Status	Married, 1 child (October 2015)

Education

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

2008 **Master Degree in Coding and 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

Current Position

Sept. 2015- **Researcher funded by Academy of Finland:** *Member of the Secure Systems research group, Department of Computer Science (CS), School of Science, Aalto University, Finland.*
September 2015-June 2016: Maternity leave
January 2017- : Maternity leave

Experience

Sept. 2011-Aug. 2015 **Postdoctoral Researcher:** *Member of the Cryptographic group, Department of Information and Computer Science (ICS), School of Science, Aalto University, Espoo, Finland. Team Leader: Kaisa Nyberg.*

2008-2011 **PhD Student:** *Member of the project-team SECRET, Research center INRIA Paris-Rocquencourt, France. Supervisor: Pascale Charpin. Team Leader: Anne Canteaut.*

Languages

French **Native**

English **Fluent**

Dutch **Learning in family environment**

Finnish **Basic communication skills**

Pedagogical Training

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

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

2011-2012 **French qualification in mathematics, applied mathematics and computer science:** *Required to become* "maître de conférence" *(assistant professor)*.

Teaching Experience

2016-2017 **Lecturer in charge: "Cryptography and Data Security"** *5 ECTS*.
CS Department, School of Science, Aalto University, Espoo, Finland

2016 **Lecturer at the Spring School on Symmetric Cryptography: "Statistical Models in Cryptography"**.
Bochum, Germany, Mars 2016

2014-2015 **Lecturer in charge: "Cryptology"** *5 ECTS*.
CS Department, School of Science, Aalto University, Espoo, Finland

2014-2015 **Assistant in charge of the programming assignments: "Cryptography and Data Security"**.
ICS Department, School of Science, Aalto University, Espoo, Finland

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 **Lecturer in charge: "Mathématiques 1ère année"**.
DUT génie éléctique et information industrielle, IUT de Cachan, Université de Paris Sud, France

Supervision

2016 **Helping in the instruction of a PhD thesis:** *Roberto Civino*.

2014 **Supervision of a Master's student:** *Masoud Naderpour*.

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

External Funding

2015 **Granted an Academy of Finland Postdoctoral project:** *Duration 3 years. Acceptance rate: 9.6%*, includes salary and travel funding.

2015 **Granted funding for a summer intern:** *3 months, full salary*.

2014 **Granted funding to invite a researcher:** *2 weeks, full travel arrangement*.

Publication Record

Publication List: *Provided at the end of this CV*.

H-index: *12*.
Numerical data provided by Google scholar:
`http://scholar.google.com/citations?user=sJgnkqgAAAAJ`

Total number of citations: *412*.

Number of journal publications: *9*.

Number of peer-reviewed conference publications: *20*.

Prominent conferences: *CRYPTO, EUROCRYPT, ASIACRYPT*.
5 publications in these conferences.

Most cited papers: *[25] published in 2011 and cited 62 times, [19] published in 2013 and cited 41 times*.

Number of co-authors: *27*.

Number of international co-authors: *18*.
Co-authors not only in France while I was in France, and not only in Finland while I was in Finland.

Editorial Board

2016 **IACR Transactions on Symmetric Cryptology**.

Program Committees

2016 **SAC 2016:** *Selected Areas in Cryptography, conference*.
INDOCRYPT 2016: *17th International Conference on Cryptology, conference*.

2015 **FSE 2015:** *Fast Software Encryption, workshop*.
INDOCRYPT 2015: *16th International Conference on Cryptology, conference*.

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

International Conferences: *CRYPTO 2016, ASIACRYPT 2016, EUROCRYPT 2015, SAC 2015, ASIACRYPT 2014, ACNS 2014, EUROCRYPT 2014, ASIACRYPT 2013, SAC 2013, FSE 2013, AFRICACRYPT 2013, ACNS 2013, FSE 2012, CRYPTO 2012, SAC 2012, INDOCRYPT 2010.*

International Journals: *ACM Transactions on Information and System Security, Advances in Mathematics of Communications, Applicable Algebra in Engineering, Communication and Computing, Cryptography and Communications, Designs Codes and Cryptography, Discrete Applied Mathematics, Frontiers of Information Technology and Electronic Engineering, Finite Fields and Their Applications, IEEE Transactions on Information Theory, Information Processing Letters, Journal of Computer Science and Technology.*

Other International Duties

2016- **Member of the COST Action IC1306:** *Cryptography for Secure Digital Interaction.*

Miscellaneous

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

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

Referees

Professor Gregor Leander

Affiliation: Professor at Ruhr University Bochum, Germany
Postal address: Gregor Leander
Fakultät für Elektrotechnik und Informationstechnik
Universitätsstr. 150
44780 Bochum
Germany
Email address: gregor.leander@rub.de
Webpage: `https://www.emsec.rub.de/chair/_staff/Gregor_Leander/`

Professor Kaisa Nyberg

Affiliation: Professor Emerita at Aalto University, Finland
Postal address: Kaisa Nyberg
Aalto University, School of Science
Department of Computer Science
P.O. Box 15400
FI-00076 Aalto
Finland
Email address: kaisa.nyberg@aalto.fi
Webpage: https://users.ics.aalto.fi/knyberg/

Professor Bart Preneel

Affiliation	Professor at University of Leuven, Belgium
Postal address	Bart Preneel
	University of Leuven
	Dept. Elektrotechniek-ESAT /COSIC
	Kasteelpark Arenberg 10 Bus 2452
	B-3001 Leuven-Heverlee
	Belgium
Email address	bart.preneel@esat.kuleuven.be
Webpage	`http://homes.esat.kuleuven.be/~preneel/`

List of Publications

Ten publications considered important by the applicant are denoted with the symbol ⋆ before the name of the first author.
For the journal publications given in category A.1, the impact factor is provided.
For the peer-reviewed conference publications given in category A.4, when available the acceptance rate is provided.

A.1 Articles in Refereed Scientific Journals

[1] ⋆ Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. *Journal of Cryptology*, pages 1–30, 2016. JCR Impact Factor 2015: 1.617.

[2] ⋆ Céline Blondeau and Kaisa Nyberg. Joint Data and Key Distribution of Simple, Multiple, and Multidimensional Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity. *Design Codes and Cryptography*, pages 1–31, 2016. Online First 17 August 2016, JCR Impact Factor 2015: 0.781.

[3] Céline Blondeau. Impossible Differential Attack on 13-round Camellia-192. *Information Processing Letters*, 115(3):660–666, 2015. JCR Impact Factor 2015: 0.605, cited 4 times.

[4] ⋆ Céline Blondeau and Kaisa Nyberg. Perfect nonlinear functions and cryptography. *Finite Fields and Their Applications*, 32:120–147, 2015. JCR Impact Factor 2015: 1.292, cited 8 times.

[5] ⋆ Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, and Yanfeng Wang. Reflection Cryptanalysis of PRINCE-like Ciphers. *Journal of Cryptology*, 28(3):718–744, 2015. JCR Impact Factor 2015: 1.617, cited 29 times.

[6] Céline Blondeau and Léo Perrin. More differentially 6-uniform power functions. *Designs, Codes and Cryptography*, 73(2):487–505, 2014. JCR Impact Factor 2015: 0.781, cited 5 times.

[7] ⋆ Céline Blondeau, Benoît Gérard, and Jean-Pierre Tillich. Accurate estimates of the data complexity and success probability for various cryptanalyses. *Design, Codes and Cryptography*, 59(1-3):3–34, 2011. JCR Impact Factor 2011: 0.875, cited 37 times.

[8] ⋆ Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential Properties of Power Functions. *International Journal of Information and Coding Theory*, 1(2):149–170, 2010. Cited 37 times.

[9] ⋆ Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential Properties of $x \mapsto x^{2^t-1}$. *IEEE Transactions on Information Theory*, 57(12):8127–8137, 2011. JCR Impact Factor 2012: 2.621, cited 25 times.

A.4 Articles in Refereed Scientific Conference Proceedings

[10] Céline Blondeau, Thomas Peyrin, and Lei Wang. Known-key Distinguisher on Full PRESENT. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015*, volume 9215 of *Lecture Notes in Computer Science*, pages 455–474. Springer, 2015. Acceptance rate=28%, cited 7 times.

[11] Céline Blondeau and Nyberg Kaisa. On Distinct Known Plaintext Attacks. In Pascale Charpin, Jean-Pierre Tillich, and Nicolas Sendrier, editors, *Pre-proceedings of WCC 2015*, 2015.

[12] Céline Blondeau and Marine Minier. Analysis of Impossible, Integral and Zero-Correlation Attacks on Type-II Generalized Feistel Networks using the Matrix Method. In Gregor Leander, editor, *Fast Software Encryption, FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 92–113. Springer-Verlag, 2015. Acceptance rate: 39%.

[13] Céline Blondeau, Aslí Bay Bay, and Serge Vaudenay. Protecting against Multidimensional Linear and Truncated Differential Cryptanalysis by Decorrelation. In Gregor Leander, editor, *Fast Software Encryption, FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 73–91. Springer-Verlag, 2015. Acceptance rate: 39%.

[14] Céline Blondeau, Andrey Bogdanov, and Meiqin Wang. On the (In)Equivalence of Impossible Differential and Zero Correlation Distinguishers for Feistel- and Skipjack-type Ciphers. In Ioana Boureanu, Philippe Owezarski, and Serge Vaudenay, editors, *ACNS 2014*, volume 8479 of *Lecture Notes in Computer Science*, pages 271–288. Springer-Verlag, 2014. Cited 12 times.

[15] ⋆ Céline Blondeau and Kaisa Nyberg. Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In Elisabeth Oswald and Phong Q. Nguyen, editors, *EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 165–183. Springer-Verlag, 2014. Acceptance rate: 19%, cited 31 times.

[16] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-Linear Cryptanalysis Revisited. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption, FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 411–430. Springer-Verlag, 2014. Best Paper Award, cited 11 times.

[17] Céline Blondeau. Improbable Differential from Impossible Differential: On the Validity of the Model. In Goutam Paul and Serge Vaudenay, editors, *Indocrypt 2013*, volume 8250 of *Lecture Notes in Computer Science*, pages 149–160. Springer-Verlag, 2013. Cited 8 times.

[18] Céline Blondeau, Andrey Bogdanov, and Gregor Leander. Bounds in Shallows and in Miseries. In *CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 204–222. Springer-Verlag, 2013. Acceptance rate: 27%, cited 8 times.

[19] ⋆ Céline Blondeau and Kaisa Nyberg. New Links Between Differential and Linear Cryptanalysis. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 388–404. Springer-Verlag, 2013. Acceptance rate: 20%, cited 41 times.

[20] Céline Blondeau and Léo Perrin. More Differentially 6-uniform Power Functions. In Matthew G. Parker Lilya Budaghyan, Tor Helleseth, editor, *Pre-proceedings of WCC 2013*, pages 223–233, 2013.

[21] Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, and Yanfeng Wang. Reflection Cryptanalysis of PRINCE-like Ciphers. In Shiho Moriai, editor, *Fast Software Encryption, FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 71–91. Springer-Verlag, 2014. Acceptance rate: 25%, Best Paper Award.

[22] Kimmo Järvinen, Céline Blondeau, Dan Page, and Michael Tunstall. Harnessing Biased Faults in Attacks on ECC-based Signature Schemes. In *Proceedings of the 9th Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2012*, pages 72–82. IEEE Computer Society, 2012. Cited 9 times.

[23] Céline Blondeau, Benoît Gérard, and Kaisa Nyberg. Multiple Differential Cryptanalysis Using LLR and χ^2 Statistics. In *Conference on Security and Cryptography for Networks*, volume 7485 of *Lecture Notes in Computer Science*, pages 343–361. Springer, 2012. Cited 24 times.

[24] Mohammed A. Abdelraheem, Céline Blondeau, María Naya-Plasencia, Marion Videau, and Erick Zenner. Cryptanalysis of ARMADILLO2. In D.H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 308–326. Springer, 2011. Acceptance rate: 15%, cited 17 times.

[25] ⋆ Céline Blondeau and Benoît Gérard. Multiple Differential Cryptanalysis: Theory and Practice. In A. Joux, editor, *Fast Software Encryption, FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2011. Acceptance rate: 21%, cited 62 times.

[26] Céline Blondeau and Benoît Gérard. Differential Cryptanalysis of PUFFIN and PUFFIN2. In *ECRYPT Workshop on Lightweight Cryptography 2011*, 2011.

[27] Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential Properties of Power Functions. In *IEEE International Symposium on Information Theory*, pages 2478–2482, 2010.

[28] Céline Blondeau and Benoît Gérard. Links Between Theoretical and Effective Differential Probabilities: Experiments on PRESENT. In *Ecrypt Workshop on Tools for Cryptanalysis*, June 2010. Cited 13 times.

[29] Céline Blondeau and Benoît Gérard. On the Data Complexity of Statistical Attacks against Block Ciphers. In A. Kholosha, E. Rosnes, and M.Parker, editors, *Workshop on Coding and Cryptography - WCC 2009*, pages 469–488, 2009. Cited 13 times.

G.2, G.4 Theses

[30] Céline Blondeau. *La cryptanalyse différentielle et ses généralisations*. Phd thesis, Université Pierre et Marie Curie, Paris, France, November 2011.

[31] Céline Blondeau. *La cryptanalyse différentielle tronquée*. Master thesis, Université de Limoges, France, September 2008.

Others Scientific Publications

[32] Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential Properties of $x \mapsto x^{2^t-1}$. In *The 10th International Conference on Finite Fields and Applications - Fq10*, July 2011.

[33] Céline Blondeau and Benoît Gérard. On the Data Complexity of Statistical Attacks against Block Ciphers. In *Poster at EUROCRYPT*, 2009.

Seminars and Invited Talks

2015 **Remarks on the Data Complexity of Zero-Correlation Linear Attacks** *Early Symmetric Crypto (ESC)*, Luxembourg, January 2015.

2014 **Relations Between the Generalizations of Differential and Linear Cryptanalyses** *Université de Rennes*, France, November 2014.

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.