Dr. Cyrille Wiedling

ICTEAM, UCL Crypto Group,
Place du Levant, 3
1348 Louvain-la-Neuve,
BELGIUM

Phone : (+32) (0)4 89 54 68 34
cyrille.wiedling@uclouvain.be

Nationality : French
Born 08 September 1987

Webpage :
perso.uclouvain.be/
cyrille.wiedling/

Curriculum Vitae

Research Interests

— Formal Methods : symbolic models, behavioural equivalences, type systems.
— Security of Application Programming Interface.
— Verification of Cryptographic Protocols, especially voting protocols.

Work Experience

Sep. 2014 – Today	PostDoc Researcher at ICTEAM UCL Crypto Group. Under the supervision of Olivier Pereira, Université catholique de Louvain, Louvain-la-Neuve, Belgium.
Oct. 2011 – Jun. 2014	Moniteur (Teaching Assistant) for Exercise Sessions and Tutorials in *Informatique* (Computer Science) for 3rd and 4th year students at Ecole Nationale Supérieure d'Eléctricité et de Mécanique (ENSEM), Nancy, France.
Feb. – Aug. 2011	Internship (M.Sc. 2nd year) - *Formal Analysis of an E-Voting Protocol.* Under the direction of V. Cortier, LORIA, Nancy, France. (Formal verification using applied-pi calculus of a Norwegian internet-voting protocol.)
Jun. – Aug. 2010	Internship (M.Sc. 1st year) - *How to secure a shared calendar ?* Under the direction of A. Imine, LORIA, Nancy, France. (Design and implementation of solutions to protect replicated data.)
2007 – 2010	Home tutor (Mathematics). Company Complétude, Strasbourg, France.

Education

2011 – 2014	PhD Student in Computer Science, *Formal Verification of Advanced Families of Security Protocols : E-voting and APIs.* Under the direction of V. Cortier, CNRS-LORIA & Université de Lorraine, Nancy, France.
2009 – 2011	M.Sc. Scientific Computing & IT Security. UFR de Mathématiques et d'Informatique, Université de Strasbourg, France.
2008 – 2009	M.Sc.Fundamental and Applied Mathematics. (First year only.) UFR de Mathématiques et d'Informatique, Université de Strasbourg, France.
2007 – 2008	B.Sc. Mathematics. UFR de Mathématiques et d'Informatique, Université de Strasbourg, France.
2005 – 2007	2-year intensive program preparing for the national competitive exam for entry to French engineering schools (CPGE). Lycée Kléber, Strasbourg, France.
2005	Baccalauréat Scientifique SVT Option Mathématiques (High School Diploma) Lycée Freppel, Obernai (Bas-Rhin), France.

Publications

Conferences

— Type-Based Verification of Electronic Voting Protocols. Véronique Cortier, Fabienne Eigner, Steve Kremer, Matteo Maffei and Cyrille Wiedling. In *Proceedings of the 4th Conference on Principles of Security and Trust (POST'15)*, pp. 303-323, London, UK, April 2015.

— Analysis of a Boardroom Voting System. Mathilde Arnaud, Véronique Cortier and Cyrille Wiedling. In *Proceedings of the 4th International Conference (Vote-ID 2013)*, pp. 109-126, Guildford, UK, July 2013.

— Revoke and let live : A Secure Key Revocation API for Cryptographic Devices. Véronique Cortier, Graham Steel and Cyrille Wiedling. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS'12)*, pp. 918 - 928, Raleigh NC, USA, October 2012.

— A formal analysis of the Norwegian e-voting protocol. Véronique Cortier and Cyrille Wiedling. In *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, pp. 149 - 168, Lecture Notes in Computer Science 7215, Springer, Tallinn, Estonia, March 2012.

Workshops

— A Type Library for Electronic Voting Protocols. Véronique Cortier, Fabienne Eigner, Steve Kremer, Matteo Maffei and Cyrille Wiedling. In *Journées du GT-Vérif 2014*, P. and M. Curie University, Paris, France, June 2014.

— Revoke and Let Live : A Secure Key Revocation API for Cryptographic Devices. Véronique Cortier, Graham Steel and Cyrille Wiedling. In *6th International Workshop on Analysis of Security APIs (ASA'12)*, Harvard University, Cambridge MA, USA, June 2012.

— A Formal Analysis of the Norwegian E-voting Protocol. Véronique Cortier and Cyrille Wiedling. In *Grande Region Security and Reliability Day 2012 (GRSRD'12)*, LORIA, Nancy, France, March 2012.

Seminars

— Presentation of Type-Based Verification of Electronic Voting Protocols at the "Méthodes formelles et sécurité" seminar in Rennes, May 22^{nd} 2015.

— Presentation of Revoke and Let Live : A Secure Key Revocation API for Cryptographic Devices at the "Méthodes formelles et sécurité" seminar in Rennes, May 24^{th} 2013.

Research Reports

— Revoke and Let Live : A Secure Key Revocation API for Cryptographic Devices. Véronique Cortier, Graham Steel and Cyrille Wiedling. Rapport de recherche RR-7949, INRIA, 2012.

— A Formal Analysis of the Norwegian E-voting Protocol. Véronique Cortier and Cyrille Wiedling. Rapport de recherche RR-7781, INRIA, 2011.

Theses

— Formal Verification of Advanced Families of Security Protocols. Cyrille Wiedling. PhD Thesis, CNRS-LORIA & Université de Lorraine, Nancy, 2014. *(Available on request.)*
Thesis defended at LORIA, Nancy, France on 21st November 2014. The jury was composed of :
- Reviewers : Bruno Blanchet (INRIA) and Cas Cremers (University of Oxford).
- President : Frédéric Cuppens (Télécom Bretagne).
- Examiners : Véronique Cortier (CNRS) [Advisor], Ralf Küsters (University of Trier), Yassine Lakhnech (Université Joseph Fournier), Pierre-Etienne Moreau (Université de Lorraine) and Benjamin Morin (ANSSI).

Miscellaneous

— Co-supervision of 4th year students of Ecole des Mines Nancy during a six-month project for the *developpment of an API and the corresponding interface in Javacard*, Nancy, 2013.

— Co-animation of a workshop on cryptography (with a simplified approach for a broad audience of students, parents and kids) during the *Un TIC'et pour la science - Fête de la Science* event, Nancy, 2013.

— Co-animation of workshop on cryptography (introduction to symmetric/asymmetric encryption, authentication protocols, possible attacks, etc.) for high school students of Lycée Jeanne d'Arc, Nancy, 2012.