François Dupressoir

Post-Doctoral Researcher
IMDEA Software Institute

https://fdupress.net https://www.github.com/fdupress
francois.dupressoir@imdea.org

T: +34-91-101-2202 Ext. 4147 F: +34-91-101-1358

Research Experience

October 2012 - Present Post-doctoral researcher at IMDEA Software Institute (Spain).
February - August 2012 Intern at Microsoft Research Cambridge (UK).
August - November 2011 Intern at Microsoft Research Redmond (USA).
April - July 2010 Intern at the European Microsoft Innovation Center (Germany).

Education

Ph.D. in Computer Science Awarded on April 23, 2013 (Defended February 6, 2013).
The Open University (UK).
Supervisors: Andrew D. Gordon, Jan Jürjens and Bashar Nuseibeh.

M.Sc. in Computer Science Awarded in September 2008. (Normalien)
École Normale Supérieure de Cachan – Antenne de Bretagne (France).

B.Sc. in Theoretical Computer Science Obtained in September 2006. (Auditeur)
École Normale Supérieure de Lyon (France).

Service

Program Committees
- PROOFS (2014, 2015)
- ESSOS (2014)

Journal Reviews
- Journal of Computer Security (×2)

Organization
- 1st EasyCrypt Summer School and Workshop (June 2013)

Academic Juries
- Ph.D. Examiner for *Pablo Rauzy* (ParisTech): July 13, 2015

- Ph.D. Pre-Defence Examiner for *Goran Doychev* (IMDEA Software Institute): February 5, 2016

Grants and Scholarships

2015 ONR Grant – SynCrypt (researcher)
2015 NIST Award #60NANB15D248 – Verified Standards: SHA3 (researcher)
2014 Madrid Regional Project #S2013/ICE-2731 – N-GREENS Software-CM (researcher)
2012 Madrid Regional Project #TIN2012-39391-C04-01 – StrongSoft (researcher)
2012 ONR Grant #N000141210914 – AutoCrypt (researcher)
2012 FP7 Marie Curie Actions-COFUND 291803 grant – AMAROUT II (recipient)
2008 Microsoft Research Cambridge Ph.D. Scholarship (recipient)

Teaching

June 2015 IACR School on Computer-Aided Cryptography
Lectures (5 hours) and tutorials (5 hours).
November 2014 Joint EasyCrypt-F*-CryptoVerif School
Lectures (2 hours) and tutorials (6 hours)
June 2014 Ph.D. Course on Computer-Aided Cryptography (University of Pisa)
Lectures (4 hours) and tutorials (4 hours)
June 2013 First EasyCrypt School
Lectures (1 hour) and tutorials (8 hours)

Supervisions

Martin Moreau October 2015–Present (Ph.D. student)
Lavinia Damian September 2013–July 2014 (B.Sc. intern, now SDE at Endava)
Guillaume Davy with P-Y Strub, May–June 2013 (M1 intern, now PhD student at LAAS)

List of Publications

Journal Publications and Book Chapters

[1] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Benedikt Schmidt, and Pierre-Yves Strub. "Computer-Aided Proofs in Cryptography: An overview". In: *All about Proofs, Proofs for All (APPA)*. Ed. by Bruno Woltzenlogel Paleo and David Delahaye. Vol. 55. Mathematical Logic and Foundations. London, UK: College Publications, Jan. 2015. ISBN: 978-1-84890-166-7.

[2] *François Dupressoir*, Andrew D. Gordon, Jan Jürjens, and David A. Naumann. "Guiding a General-Purpose C Verifier to Prove Cryptographic Protocols". In: *Journal of Computer Security (JCS)* 22.5 (2014). Also appears as tech. rep. MSR-TR-2011-50, pp. 823–866.

[3] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, César Kunz, Benedikt Schmidt, and Pierre-Yves Strub. "EasyCrypt: A Tutorial". In: *Foundations of Security Analysis and Design VII (FOSAD)*. Vol. 8604. Lecture Notes in Computer Science. Springer International Publishing, 2013, pp. 146–166. ISBN: 978-3-319-10081-4.

International Conferences

[4] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and *François Dupressoir*. "Verifiable side-channel security of cryptographic implementations: constant-time MEE-CBC". In: *23rd International Conference on Fast Software Encryption (FSE)*. To appear. Available from https://fdupress.net/files/seccomp.pdf. 2016.

[5] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub. "Verified Proofs of Higher-Order Masking". In: *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Vol. 9056. Lecture Notes in Computer Science. Sofia, Bulgaria: Springer Berlin Heidelberg, 2015, pp. 457–485. ISBN: 978-3-662-46800-5.

[6] Gilles Barthe, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, and Jean-Christophe Zapalowicz. "Synthesis of Fault Attacks on Cryptographic Implementations". In: *Proceedings of the 2014 ACM SIGSAC conference on Computer & Communications security (ACM CCS)*. Scottsdale, Arizona, USA: ACM, 2014, pp. 1016–1027. ISBN: 978-1-4503-2957-6.

[7] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Pierre-Alain Fouque, Mehdi Tibouchi, and Jean-Christophe Zapalowicz. "Making RSA-PSS Provably Secure against Non-Random Faults". In: *Cryptographic Hardware and Embedded Systems (CHES)*. Vol. 8731. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, pp. 206–222. ISBN: 978-3-662-44708-6.

[8] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and *François Dupressoir*. "Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations". In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (ACM CCS)*. Berlin, Germany: ACM, 2013, pp. 1217–1230. ISBN: 978-1-4503-2477-9.

[9] *François Dupressoir*, Andrew D. Gordon, Jan Jürjens, and David A. Naumann. "Guiding a General-Purpose C Verifier to Prove Cryptographic Protocols". In: *Proceedings of the 2011 IEEE 24th Computer Security Foundations Symposium (CSF)*. Washington, DC, USA: IEEE Computer Society, 2011, pp. 3–17. ISBN: 978-0-7695-4365-9.

Keynote and Invited Talks

[10] *François Dupressoir. Formal Methods for the Secure Masking of Large Algorithms.* Keynote Talk. Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), Apr. 2016.

[11] *François Dupressoir. Computer-Aided Cryptographic Proofs for Low-Level Implementations.* Keynote Talk. Workshop on Implementation: Security and Evaluation (WISE), Sept. 2015.

In Submission

[12] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, *François Dupressoir*, and Michael Emmi. *Verifying Constant-Time Implementations.* In submission. Available from https://fdupress.net/files/ctverif.pdf. Feb. 2016.

[13] Gilles Barthe, *François Dupressoir*, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub. *The Bounded Moment Masking Security Model and its Application to Parallel Implementations.* In submission. Available from https://fdupress.net/files/bmoment.pdf. Feb. 2016.

[14] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub. *Compositional Verification of Higher-Order Probing Security – Application to a Verifying Masking Transformation.* In submission. Available from https://fdupress.net/files/mlt.pdf. Feb. 2016.

Invited Papers and Workshops

[1] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Benedikt Schmidt, and Pierre-Yves Strub. "Computer-Aided Proofs in Cryptography: An overview". In: *All about Proofs, Proofs for All (APPA)*. Ed. by Bruno Woltzenlogel Paleo and David Delahaye. Vol. 55. Mathematical Logic and Foundations. London, UK: College Publications, Jan. 2015. ISBN: 978-1-84890-166-7.

[15] The EasyCrypt Team. *EasyCrypt Reference Manual.* Distributed with the EasyCrypt tool. 2015.

[16] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Guillaume Davy, *François Dupressoir*, Benjamin Grégoire, and Pierre-Yves Strub. "Towards an EasyCrypt Formalization of Garbling Schemes". In: *The Workshop on Language Support for Privacy-Enhancing Technology (PETShop)*. Nov. 2013.

[3] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, César Kunz, Benedikt Schmidt, and Pierre-Yves Strub. "EasyCrypt: A Tutorial". In: *Foundations of Security Analysis and Design VII (FOSAD)*. Vol. 8604. Lecture Notes in Computer Science. Springer International Publishing, 2013, pp. 146–166. ISBN: 978-3-319-10081-4.

[17] *François Dupressoir*, Cédric Fournet, and Andrew D. Gordon. "Proving Computational Security with a General-Purpose C Verifier". In: *Workshops on Formal and Computational Cryptography (FCC) and Analysis of Security APIs (ASA)*. July 2012.

[18] Mihhail Aizatulin, *François Dupressoir*, Andrew D. Gordon, and Jan Jürjens. "Verifying Cryptographic Code in C: Some Experience and the Csec Challenge". In: *Formal Aspects of Security and Trust (FAST)*. Vol. 7140. Lecture Notes in Computer Science. Invited Paper, also appears as tech. rep. MSR-TR-2011-118. Springer Berlin Heidelberg, 2012, pp. 1–20. ISBN: 978-3-642-29419-8.

[19] *François Dupressoir*, Andrew D. Gordon, and Jan Jürjens. "Verifying Authentication Properties of C Security Protocol Code Using General-Purpose Verifiers". In: *Workshop on Analysis of Security APIs (ASA)*. June 2010.

Technical Reports and ePrints

[20] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and *François Dupressoir*. *Verifiable side-channel security of cryptographic implementations: constant-time MEE-CBC*. Cryptology ePrint Archive, Report 2015/1241. http://eprint.iacr.org/. 2015.

[1] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Benedikt Schmidt, and Pierre-Yves Strub. "Computer-Aided Proofs in Cryptography: An overview". In: *All about Proofs, Proofs for All (APPA)*. Ed. by Bruno Woltzenlogel Paleo and David Delahaye. Vol. 55. Mathematical Logic and Foundations. London, UK: College Publications, Jan. 2015. ISBN: 978-1-84890-166-7.

[21] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub. *Verified Proofs of Higher-Order Masking*. Cryptology ePrint Archive, Report 2015/060. http://eprint.iacr.org/. 2015.

[15] The EasyCrypt Team. *EasyCrypt Reference Manual*. Distributed with the EasyCrypt tool. 2015.

[22] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Guillaume Davy, *François Dupressoir*, Benjamin Grégoire, and Pierre-Yves Strub. *Verified Implementations for Secure and Verifiable Computation*. Cryptology ePrint Archive, Report 2014/456. http://eprint.iacr.org/. 2014.

[23] Gilles Barthe, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, Mehdi Tibouchi, and Jean-Christophe Zapalowicz. *Making RSA-PSS Provably Secure Against Non-Random Faults*. Cryptology ePrint Archive, Report 2014/252. http://eprint.iacr.org/. 2014.

[24] Gilles Barthe, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, and Jean-Christophe Zapalowicz. *Synthesis of Fault Attacks on Cryptographic Implementations*. Cryptology ePrint Archive, Report 2014/436. http://eprint.iacr.org/. 2014.

[25] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and *François Dupressoir*. *Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations*. Cryptology ePrint Archive, Report 2013/316. http://eprint.iacr.org/. 2013.

[3] Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, César Kunz, Benedikt Schmidt, and Pierre-Yves Strub. "EasyCrypt: A Tutorial". In: *Foundations of Security Analysis and Design VII (FOSAD)*. Vol. 8604. Lecture Notes in Computer Science. Springer International Publishing, 2013, pp. 146–166. ISBN: 978-3-319-10081-4.

[26] *François Dupressoir*, Andrew D. Gordon, Jan Jürjens, and David A. Naumann. *Guiding a General-Purpose C Verifier to Prove Cryptographic Protocols*. Tech. rep. MSR-TR-2011-50. Microsoft Research, Nov. 2011.

[27] Mihhail Aizatulin, *François Dupressoir*, Andrew D. Gordon, and Jan Jürjens. *Verifying Cryptographic Code in C: Some Experience and the Csec Challenge*. Tech. rep. MSR-TR-2011-118. Microsoft Research, Nov. 2011.

Theses

[28] *François Dupressoir*. "Proving Cryptographic C Programs Secure with General-Purpose Verification Tools". Ph.D. thesis. The Open University, 2013.

[29] *François Dupressoir*. "Code and Proof Obfuscation". M.Sc. thesis. École Normale Supérieure de Cachan – Antenne de Bretagne, 2008.

Selected Talks and Lectures

[30] *François Dupressoir. Computer-Aided Cryptographic Proofs for Low-Level Implementations*. Invited Lecture. IACR School on Computer-Aided Cryptography, June 2015.

[31] *François Dupressoir. Towards Provably-Secure Optimizing Masking Compilers*. Contributed Workshop Talk. Real-World Cryptography Workshop (RWC), Jan. 2015.

[32] *François Dupressoir. Verifiable Cryptographic Security for Low-Level Code – From Black-Box Security of Specifications to Side-Channel Security of Executable Code*. Invited Talk. Séminaire Marelle — Inria Sophia-Antipolis – Méditerranée, Dec. 2015.

[33] *François Dupressoir. Verifiable Cryptographic Security for Low-Level Code – From Black-Box Security of Specifications to Side-Channel Security of Executable Code*. Invited Talk. Séminaire Méthodes Formelles et Sécurité – Irisa, Rennes, July 2015.

[34] *François Dupressoir. Efficient Provably Secure Machine Code from High-Level Implementations*. Invited Talk. Real-World Cryptography Workshop (RWC), Jan. 2014.

[35] *François Dupressoir. Formal Adventures in the Land of Masking-Based Side-Channel Countermeasures*. Contributed Talk. Dagstuhl Seminar, Nov. 2014.

[36] *François Dupressoir. A side-channel aware IND-CCA secure implementation of the PKCS#1 v2.1 RSA encryption standard.* Invited Talk. CryptoForma Workshop, Microsoft Research Cambridge, Apr. 2013.

[37] *François Dupressoir. Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations.* Contributed Conference Talk. ACM Conference on Computer and Communications Security (CCS), Nov. 2013.

[38] *François Dupressoir. Proving Computational Security with a General-Purpose C Verifier.* Contributed Plenary Talk (Joint Session). Workshops on Formal, Computational Cryptography (FCC), and Analysis of Security APIs (ASA), July 2012.

[39] *François Dupressoir. Guiding a General-Purpose C Verifier to Prove Cryptographic Protocols.* Contributed Conference Talk. IEEE Computer Security Foundations Symposium (CSF), June 2011.

[40] *François Dupressoir. Proving Security Properties of C Programs Using VCC.* Invited Talk. Workshop on Formal Methods and Tools for Security (FMATS), Microsoft Research Cambridge, Apr. 2011.