François Dupressoir

Senior Lecturer in Cryptography
University of Bristol

https://fdupress.net

https://github.com/fdupress https://gitlab.com/fdupress

f.dupressoir@surrey.ac.uk

T: +44 117 33 15200 M: +44 7948 543 281

Professional Experience

September 2019 - Present Senior Lecturer in Cryptography – University of Bristol.
June 2016 - August 2019 University of Surrey.
June 2016 - July 2019 Lecturer in Secure Systems.
July 2019 - August 2019 Senior Lecturer in Secure Systems.
October 2012 - June 2016 Post-doctoral researcher – IMDEA Software Institute (Spain).

Education

October 2008 - September 2012 PhD in Computer Science – Open University (UK).
Awarded April 2013.
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).
2007 - 2008 MSc in Computer Science – École Normale Supérieure de Cachan, Antenne de Bretagne (Rennes, France).
Awarded September 2008.
2005 - 2007 BSc and first year MSc in Theoretical Computer Science at the École Normale Supérieure de Lyon (France).
Summer 2007 Research Intern (6 weeks) – University of Calgary
Sumer 2006 Research Intern (4 weeks) – LIRMM

Grants and Scholarships

Grant Funding (as investigator)

2018 Innovate UK #133294 – SwiftAid (co-investigator, work package leader)
Industrial Lead: David Michael (Streeva)
Applications of formal methods to the design of an industrial system for the processing and financial reporting of charitable donations (GiftAid). Interactions with Government (HMRC), banking industry (Visa) and charities.

2018 H2020 Grant #779391 – FutureTPM (co-investigator, work package leader)
Technical Lead: Liqun Chen (U of Surrey)
Development and integration of post-quantum cryptography into the TPM standard. Development of security models for combined TPM functionalities. Development of a run-time threat assessmnt mechanism. Use cases in electronic payments, activity tracking and device management.

2017 EPSRC Grant #EP/P031811/1 – Trusted and Transparent Voting Systems (co-investigator)
Technical Lead: Steve Schneider (U of Surrey)
Feasibility study into the use of Distributed Ledger Technologies to support verifiability in online voting (with Electoral Reform Services) and shareholding management (with Crowdcube).

2017 Microsoft Research Cambridge PhD Scholarship (as supervisor)
Development and application of formal techniques and tools for the verification of isolated roots of trust and systems that use them.

Grant Funding (as named researcher)

2015 NIST Award #60NANB15D248 – Verified Standards: SHA3 (named researcher, task leader)

2015 ONR Grant #N00014-15-1-2750 – SynCrypt (named researcher)

2014 Madrid Regional Project #S2013/ICE-2731 – N-GREENS Software-CM (named researcher, task leader)

2012 Spanish National Project #TIN2012-39391-C04-01 – StrongSoft (named researcher)

2012 ONR Grant #N00014-12-1-0914 – AutoCrypt (named researcher)

Scholarships

2012 FP7 Marie Curie Actions-COFUND 291803 grant – AMAROUT II

2008 Microsoft Research Cambridge PhD Scholarship

Consultancy Work

2018 Semafone Limited (as technical lead)
Client: Ben Rafferty (Semafone Limited)
Security and prior art evaluation for a multi-factor authentication mechanism for card payments over low-capacity channels

Teaching

Undergraduate and MSc Teaching (University of Surrey)

Further Programming Paradigms Year 2; 2018 (as co-designer and contributor)

Symmetric Cryptography MSc; 2016, 2017, 2018

Software Engineering Project Year 2; 2016 (as contributor), 2017 (as lead of a team of 3 lecturers, 2 library staff and 4 external speakers)

Seasonal Schools and Post-Graduate Courses

October 2017 "Computer-Aided Security Proofs" (Aarhus University)
October 2017 ECRYPT-NET School on Correct and Secure Implementation
June 2017 Summer School on Models and Tools for Cryptographic Proofs
May 2017 Spring School on Security and Correctness in the Internet of Things
June 2015 IACR School on Computer-Aided Cryptography
November 2014 Joint EasyCrypt-F*-CryptoVerif School
June 2014 "Computer-Aided Cryptography" (University of Pisa)
June 2013 First EasyCrypt School

Supervision

PhD Supervision

Sara Zain April 2018–Present

Research Internships

Nick Frymann and Alex Brown Summer 2018 (BSc interns, funded by HMG) – Secure networking and communication protocols for fleets of re-engineered consumer drones. (With Mark Manulis.)

Lavinia Damian September 2013–July 2014 (BSc intern, now SDE at Amazon) – EasyCrypt formalization of a group signature scheme.

Guillaume Davy May–June 2013 (MSc intern, now PhD student at LAAS) – EasyCrypt formalization of Yao's garbled circuits.

BSc and MSc Projects ca. 6/year

Academic Service and Administration

Program Committees

- CHES/TCHES (2019)
- ESORICS (2018)
- PROOFS (2014, 2015, 2016, 2017, 2018)
- ESSOS (2014)

Journal Reviews

- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Information Forensics and Security
- Journal of Computer Security

Event Organization

- 1st Workshop on Computer-Aided Design and Implementations for Security and Cryptography (2016)
- 1st EasyCrypt Summer School and Workshop (June 2013)

Academic Juries

Ph.D. Juries as Examiner

- *Gijs Vanspauwen* (KU Leuven) October 2018
- *Pablo Rauzy* (ParisTech) July 2015
- *Goran Doychev* (IMDEA Software Institute) May 2016

Other Juries

- *Nada El Kassem* (U. of Surrey) July 2017 – Confirmation Examiner
- *Jorden Whitefield* (U. of Surrey) October 2016 – Confirmation Examiner

Teaching Administration

University of Bristol (2019-Present)

PGR Tutor (2019-Present)

University of Surrey (2016-2019)

MSc Programme Leader (2018-2019) Strategic oversight, reporting and review of MSc teaching on both of the Department's MSc programmes. Management of NCSC certification for the MSc in Information Security.

MSc Coordinator (2017-2019) Day-to-day running and coordination of teaching activities across both of the Department's MSc programmes

Academic Integrity Officer (2016-2018) Advising colleagues on academic integrity matters, conducting interviews and participating in Faculty-level panels. Part of a team of 3.

Open Day and Applicant Day Coordinator (2016-2017) Leading a team of 2 in organising and delivering outreach and recruitment activities for open days and applicant days.

Additional Qualifications

Level 3 Award in Leadership and Management Awarded November 2018.
Cherith Simmons L&D Llp and the Institute of Leadership and Management.

Graduate Certificate in Learning and Teaching Awarded September 2018.
University of Surrey (UK).

List of Publications

Significant Publications

[1] José Bacelar Almeida, Cécile Baritel-Ruet, Manuel Barbosa, Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Alley Stoughton and Pierre-Yves Strub. 'Machine-checked proofs for cryptographic standards: Indifferentiability of Sponge and secure high-assurance implementations of SHA-3'. In: *2019 ACM SIGSAC Conference on Computer and Communications Security*. To appear. 2019.

[2] Véronique Cortier, Constantin Cătălin Drăgan, *François Dupressoir*, Benedikt Schmidt, Pierre-Yves Strub and Bogdan Warinschi. 'Machine-Checked Proofs of Privacy for Electronic Voting Protocols'. In: *2017 IEEE Symposium on Security and Privacy*. May 2017, pp. 993–1008.

[3] 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)*. **Best paper award.** Mar. 2016.

[4] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, *François Dupressoir* and Michael Emmi. 'Verifying Constant-Time Implementations'. In: *25th USENIX Security Symposium*. Aug. 2016.

[5] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub and Rébecca Zucchini. 'Strong Non-Interference and Type-Directed Higher-Order Masking'. In: *23rd ACM Conference on Computer and Communications Security*. Oct. 2016.

Journal Publications and Book Chapters

[6] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert and Pierre-Yves Strub. 'Improved Parallel Mask Refreshing Algorithms: Generic Solutions with Parametrized Non-Interference & Automated Optimizations'. In: *Journal of Cryptographic Engineering (JCEN)* (2019). To appear.

[7] 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.

[8] *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.

[9] 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

[1] José Bacelar Almeida, Cécile Baritel-Ruet, Manuel Barbosa, Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Alley Stoughton and Pierre-Yves Strub. 'Machine-checked proofs for cryptographic standards: Indifferentiability of Sponge and secure high-assurance implementations of SHA-3'. In: *2019 ACM SIGSAC Conference on Computer and Communications Security*. To appear. 2019.

[10] Cécile Baritel-Ruet, *François Dupressoir*, Pierre-Alain Fouque and Benjamin Grégoire. 'Formal Security Proof of CMAC and Its Variants'. In: *31st IEEE Computer Security Foundations Symposium*. July 2018, pp. 91–104.

[11] Véronique Cortier, Constantin Cătălin Drăgan, *François Dupressoir* and Bogdan Warinschi. 'Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios'. In: *31st IEEE Computer Security Foundations Symposium*. July 2018, pp. 298–312.

[12] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Vincent Laporte and Vitor Pereira. 'A Fast and Verified Software Stack for Secure Function Evaluation'. In: *2017 ACM SIGSAC Conference on Computer and Communications Security*. Oct. 2017, pp. 1989–2006.

[13] Gilles Barthe, *François Dupressoir*, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert and Pierre-Yves Strub. 'Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model'. In: *Advances in Cryptology – EUROCRYPT 2017*. Vol. 10210. Lecture Notes in Computer Science. Apr. 2017.

[2] Véronique Cortier, Constantin Cătălin Drăgan, *François Dupressoir*, Benedikt Schmidt, Pierre-Yves Strub and Bogdan Warinschi. 'Machine-Checked Proofs of Privacy for Electronic Voting Protocols'. In: *2017 IEEE Symposium on Security and Privacy*. May 2017, pp. 993–1008.

[3] 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)*. **Best paper award.** Mar. 2016.

[4] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, *François Dupressoir* and Michael Emmi. 'Verifying Constant-Time Implementations'. In: *25th USENIX Security Symposium*. Aug. 2016.

[5] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub and Rébecca Zucchini. 'Strong Non-Interference and Type-Directed Higher-Order Masking'. In: *23rd ACM Conference on Computer and Communications Security*. Oct. 2016.

[14] 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*. Vol. 9056. Lecture Notes in Computer Science. Sofia, Bulgaria: Springer Berlin Heidelberg, 2015, pp. 457–485. ISBN: 978-3-662-46800-5.

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

[16] 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.

[17] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe and *François Dupressoir*. 'Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations'. In: *2013 ACM SIGSAC Conference on Computer & Communications Security*. Berlin, Germany: ACM, 2013, pp. 1217–1230. ISBN: 978-1-4503-2477-9.

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

Keynote Talks and Lectures

[19] *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.

Invited Papers and Workshops

[20] 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.

[21] 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.

[22] *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.

[23] *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

[24] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert and Pierre-Yves Strub. *Improved Parallel Mask Refreshing Algorithms: Generic Solutions with Parametrized Non-Interference & Automated Optimizations*. Cryptology ePrint Archive, Report 2018/505. http://eprint.iacr.org/. 2018.

[25] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, *François Dupressoir*, Benjamin Grégoire, Vincent Laporte and Vitor Pereira. *A Fast and Verified Software Stack for Secure Function Evaluation*. Cryptology ePrint Archive, Report 2017/821. http://eprint.iacr.org/. 2017.

[26] Gilles Barthe, *François Dupressoir* and Benjamin Grégoire. *A Note on 'Further Improving Efficiency of Higher-Order Masking Scheme by Decreasing Randomness Complexity'*. Cryptology ePrint Archive, Report 2017/1053. http://eprint.iacr.org/. 2017.

[27] Gilles Barthe, *François Dupressoir*, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert and Pierre-Yves Strub. *Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model*. Cryptology ePrint Archive, Report 2016/912. http://eprint.iacr.org/. 2016.

[28] 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.

[29] Gilles Barthe, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque and Benjamin Grégoire. *Compositional Verification of Higher-Order Masking: Application to a Verifying Masking Compiler*. Cryptology ePrint Archive, Report 2015/506. http://eprint.iacr.org/. 2015.

[30] 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.

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

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] *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.

Theses

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

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

Selected Talks and Lectures

[40] *François Dupressoir. Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios*. Contributed Talk. IEEE Symposium on Computer Security Foundations, July 2018.

[41] *François Dupressoir. Computer-Aided Cryptographic Proofs: EasyCrypt*. Invited Course. Aarhus, Oct. 2017.

[42] *François Dupressoir. Formal Verification of Masking Countermeasures*. Invited Lecture. Spring School on Security and Correctnes in the Internet of Things, May 2017.

[43] *François Dupressoir. Proving Cryptographic Implementations Secure*. Invited Lecture. ECRYPT-NET School on Correct and Secure Implementation, Oct. 2017.

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

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

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

[47] *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.

[48] *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.

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

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

[51] *François Dupressoir. A side-channel aware IND-CCA secure implementation of the PKCS1 v2.1 RSA encryption standard.* Invited Talk. CryptoForma Workshop, Microsoft Research Cambridge, Apr. 2013.

[52] *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.