

**Prof. David J. Pym.**

**April 2018.**

d.pym@ucl.ac.uk (UCL)

<http://www.cs.ucl.ac.uk/people/D.Pym.html> (UCL)

+44 (0)20 3108 1193 (UCL)

*Education & Professional Qualifications.*

- **Sc.D.**, Mathematics, King's College, University of Cambridge, 2009.
- **Ph.D.**, Computer Science, University of Edinburgh, 1991.
- **B.A. (M.A.)**, Mathematics, King's College, University of Cambridge, 1985 (M.A. 1989).
- The Institute of Mathematics and Its Applications: **C.Math, FIMA.**
- British Computer Society: **CITP, FBCS.**

*Academic Appointments & Industry Positions.*

- Nov 2013–Present: **Professor of Information, Logic, and Security, University College London.** Head of the Programming Principles, Logic, and Verification Research Group (PPLV, <http://pplv.cs.ucl.ac.uk/>), Department of Computer Science. Also a member of the Information Security Research Group. At UCL, Head of Group is a core management role, with HR responsibility.
- Nov 2016–Present: **University Liaison Director for UCL, The Alan Turing Institute.** Member of Turing's senior management team with responsibility for liaison with UCL.
- Oct 2016–Present: **Turing Fellow, The Alan Turing Institute.** Inaugural Faculty (now renamed Turing) Fellow of the UK's National Institute for Data Science.
- Mar 2013–Aug 2016: **Cyber-security Research, National Grid.** Engagement to develop a cybersecurity research agenda for National Grid, covering UK and US operations. In practice, the focus has been on security architecture and policy.
- Apr 2010–Oct 2013: **6th Century Chair in Logic and SICSA Professor of Computing Science**, University of Aberdeen. Cybersecurity and cloud computing consultancy for Hewlett-Packard Laboratories, Bristol for two TSB-funded projects.
- November 2010–November 2011: **Head of School of Natural & Computing Sciences**, University of Aberdeen. Four departments (*Chemistry, Computing, Mathematics, Physics*). Responsibility for academic (staffing, strategy, etc.) and general management (finance, HR, etc.). Contributions to College of Physical Sciences and University management. About 150 staff in the School. Turnover about £10M.
- Jan 2006–April 2010: **Principal Scientist, Systems Security Laboratory, Hewlett-Packard Laboratories, Bristol.** Led and managed a range of large UK-US multi-site projects internal and external projects, with a mix of funding from HP and the UK Technology Strategy Board (TSB), and a mix of academic and industry partners. Responsibility for strategic planning of research directions and projects and obtaining internal and external funding. Major projects included:
  - Trust Economics: UK TSB funding, about £1.3M plus industry matching; industry and academic partners, UK and US. Lead scientist; project manager;
  - Cloud Stewardship Economics: UK TSB funding, about £1.3M plus industry matching. Lead scientist;

- Security Analytics: Internal HP-funded project, about 20 internal staff, UK and US. Lead scientist. These projects strongly influenced the establishment and agenda of the UK's Research Institute in the Science of Cybersecurity, funded by GCHQ.
- Jan 2002–April 2010: **Professor of Logic & Computation, University of Bath.**
- Sep 2000–Dec 2001: **Professor of Logic, QMUL.**

Previously: Sep 1998–Aug 2000: Reader in Logic, QMUL; Sep 1997–Aug 1998: Senior Lecturer in Computer Science, QMUL; Sep 1994–Aug 1997: Lecturer in Computer Science, QMUL; Sep 1993–Aug 1994: Lecturer in Artificial Intelligence, University of Birmingham; Oct 1990–Aug 1993: Research Fellow, University of Edinburgh; Oct 1989–Aug 1990: Research Associate, University of Edinburgh; Sep 1985–Jul 1986: Research Officer, BR Research, Derby.

*Fellowships & Honorary Positions.*

- Mar 2016–Present: Faculty Fellow, The Alan Turing Institute (<https://turing.ac.uk>).
- Aug 2012–Jul 2019: Honorary Professor, School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh.
- Oct 2003–Dec 2005: Royal Society Industry Fellow, Hewlett-Packard Laboratories, Bristol.
- Jan 1997–Dec 2001: Honorary Fellow, University of Edinburgh.
- Jan 1997–Dec 2001: EPSRC Advanced Fellow.

*Editorships.*

- *Editor-in-Chief*, Journal of Cybersecurity. OUP.
- *Semantics Corner Editor*, Journal of Logic & Computation. OUP.
- *Editorial Board*, Journal of Computer and System Sciences. Elsevier.
- *Editorial Board*, IFCoLoG Journal of Logics and Their Applications.
- *Editorial Board*, Systems Series, College Publications
- *Editorial Board*, International Journal of Service Science, Management, Engineering and Technology. IGI.

*Main Research Contributions.* My research is mostly in two areas: logic (mathematical and computational) and security (policy and economics).

- Resource semantics: process algebra, bunched, and modal logics as a basis for mathematical systems and security modelling, including models of access control in systems contexts; logical theory and connections with game theory and strategic reasoning.
- Access control logics that account for system architecture (connects my work in logic and information security).
- Information security economics: connecting economic models of security behaviour and investments to mathematical system models.
- Public policy in information security: the concept of information stewardship.
- Categorical models of classical logic/sequent calculus: long-standing open problem solved.
- The semantics and proof theory of bunched logic: provided the basis for separation logic and its subsequent developments: resource semantics.
- The logical theory of reductive logic and proof-search: summarized in an Oxford Logic Guide.

- Proof theory, computational logic, and categorical model theory for dependent type theory and logical frameworks.

#### *Books. Current book project:*

- The Economics of Information Security and Privacy (working title). This project is intended to deliver an accessible, graduate-level text.
- D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Springer, 2002.
- D. Pym and E. Ritter. *Reductive Logic and Proof-search: Proof Theory, Semantics, and Control*. Oxford Logic Guides. OUP, 2004.
- M. Collinson, B. Monahan, and D. Pym. *A Discipline of Mathematical Systems Modelling*. College Publications, 2012.

#### *Main Recent Research Grants.*

- EPSRC Programme Grant: Interface Reasoning for Interacting Systems (IRIS). PI, Jan 2018–; c. £7.5M + studentships and some industry support.
- EPSRC Programme Grant: Resource Reasoning. PI, Nov 2013–Jun 2016; c. £3.7M.
- EPSRC CEReS Grant: Algebra and Logic for Policy and Utility in Information Security. Overall PI, Nov 2013–Apr 2018; c. £1M.
- EPSRC/GCHQ Research Institute in the Science of Cybersecurity: Productive Security. PI at Aberdeen site, co-I at UCL, Oct 2012–March 2016; c. £300K.

Previously: TSB: Trust Domains (PI at Aberdeen/UCL site); TSB: Cloud Stewardship Economics (Chief Scientist; c. £1.3M); TSB: Trust Economics (Chief Scientist and Project Manager; c. £1.3M); EPSRC: The Semantics of Classical Proofs (Overall PI); EPSRC: Bunched ML (PI, concluded by E. O'Neill when I joined HP Labs); EPSRC: Local Reasoning about State.

Trust Economics strongly influenced the establishment by EPSRC and GCHQ of the Research Institute in the Science of Cybersecurity.

Scientific leadership of a major project—Security Analytics—within HP Labs, running alongside Trust Economics. Commercialized by HP Enterprise Services.

#### *Ph.D. Students.*

- *Graduated:* Alex Simpson, Samin Ishtiaq, Pablo Armelín, Jules Bean, Richard McKinley, Mark Price, Adam Beutement, Barry Taylor, Kevin McDonald.
- *Current:* Thomas Cattermole, Albesë Demjaha, Simon Docherty, Hasiba Afzalzada (M.Phil.), Nilufer Tuptuk, Jonathan Spring.

#### *Community.*

- Programme Committee, LPAR 2018, Ethiopia.
- Invited participant, Schloss Dagstuhl Seminar on Logics for Dependence and Independence, January 2019.
- Invited Speaker, FLoC 2018 Workshop on Separation Logic, July 2018.
- External examiner for MSc in Computer Science and MSc in Cybersecurity, University of Southampton, 2018–2022.
- External assessor for appointment of Chair in Cybersecurity, King's College London.
- Lecturer, SYSMICS Logic Summer School, Les Diablerets, Switzerland, August 2018.
- Invited Speaker, 2nd SYSMICS Workshop, Vienna, February 2018.

- Invited participant, Shonan seminar on 'Intensional and extensional aspects of computation: From computability and complexity to program analysis and security', National Institute of Informatics, Japan, January 22-25, 2018.
- Invited speaker, Cyber-risk Conference, Laboratoire de Statistique Théorique et Appliquée, Sorbonne, Paris, 6-7 November 2017.
- House of Commons Science & Technology Committee: Presentation on 'Algorithms in decision-making', October 2017.
- Invited speaker, WoLLIC 2017, London.
- Invited speaker, Simons Institute Workshop on Compositionality, Berkeley, 2016.
- Invited speaker, LICS 2016 Logic Mentoring Workshop, New York, 2016.
- Programme Committees/Chair for conferences in logic and security, including WEIS (2009–2018), GameSec, GraMSec, Service Computation, ACySe, DALT, LRPP, WoLLIC, and ICIS (Associate Editor, 'Cyber-security, privacy, and ethics of IS' track).
- Many invited papers/presentations, including: ALCOP, 2015; HCI International, 2014; The Royal Society, 2014; Security & Cloud Computing, Bletchley Park, 2014; Microsoft Security & Digital Crimes Forum, 2012; Keynote at Information Security Leaders, Edinburgh, 2011; Logics for Action and Mobility (LAM), FLoC 2010.
- External examiner for CS and EE, Oxford University, 2004–2006. PhD examiner in UK, France, and Australia.
- Member of UKCRC (UK Computing Research Committee, UK equivalent of the US CRA).
- EPSRC College; ESRC Reviewer; ACU Assessor.
- Reviewer for research funding agencies in Australia, Austria, Canada, France, Norway.
- UK Home Office Working Group: Costs of Cybercrime.
- Contributor to ENISA's report on the economics of information security.

#### *Teaching.*

I am interested in developing research-based teaching methods and in breaking barriers between mathematical, engineering, and social science aspects of teaching in computing. I believe this is particularly important for teaching information security and cybersecurity effectively.

- Currently/recently, at UCL:
  - Establishing a 'Politics, Philosophy, and Economics of Security and Privacy' module in UCL's information security Master's programme. This module is intended to introduce students to knowledge and skills in the style of social sciences as applied to security.
  - Establishing a new Master's programme in 'Logic, Semantics, and Verification of Programs'.
  - Supervision of Master's projects in the 'Business Analytics' programme.
- Previously, at Aberdeen:
  - Established 4th year module in 'Security'. This module for advanced undergraduates was quite interdisciplinary in nature and emphasized research-based learning.
  - Combined 2nd year and Master's modules in information systems.
- Previously, at Bath:
  - 1st year 'Computability and Decidability', joint CS/Math module.

- 3rd/4th year ‘Logic and Its Applications’, joint CS/Math module.
- Previously, at QMUL and Birmingham:
  - 3rd year and Master’s modules in computability and automated reasoning.
  - 1st year and Master’s modules in AI.

#### Recent Main Publications.

Here is a selection of recent main publications — since 1999 — in each of my two main current research areas. Please note that in my areas it is normal to list authors alphabetically and that (refereed) conference publications are considered significant. I am the author of over 100 publications. Current drafts and older papers may be found via my website.

#### Logic and Systems Modelling.

- (1) F. Dahlqvist and D. Pym. Coalgebraic completeness-via-canonicity for distributive substructural logics. *Journal of Logical and Algebraic Methods in Programming* 93 (2017) 1–22.
- (2) S. Docherty and D. Pym. Intuitionistic layered graph logic. Short version of IJCAR paper to appear in IJCAI 2017 Sister Conference Best Paper Track.
- (3) S. Docherty and D. Pym. A Stone-type duality theorem for Separation Logic via its underlying bunched logics. *Proc. MFPS 2017*, To appear.
- (4) D. Galmiche, P. Kimmell, and D. Pym. A Substructural Epistemic Resource Logic. *Proc. ICLA 2017*. LNCS 10119: 106–122, 2017.
- (5) G. Anderson, G. McCusker, and D. Pym. A logic for the compliance budget. *Proc. GameSec 2016*, LNCS 9966: 370–381, 2016.
- (6) S. Docherty and D. Pym. Intuitionistic layered graph logic. *Proc. IJCAR 2016, Coimbra Portugal*. LNCS 9706: 469–486, 2016.
- (7) G. Anderson and D. Pym. A Substructural Modal Logic of Utility. Accepted, *J. of Logic & Computation*, 2016.
- (8) J.-R. Courtault, D. Galmiche, and D. Pym. A Logic of Separating Modalities. *Theoretical Computer Science*, 637, 30–58, 2016.
- (9) G. Anderson and D. Pym. A Calculus and Logic of Bunched Resources and Processes. *Theoretical Computer Science* 614:63-96, 2016.
- (10) T. Caulfield and D. Pym. Modelling and Simulating Systems Security Policy. Joint work with Tristan Caulfield. In *Proc. SIMUTools 2015*, ACM Digital Library, <http://dl.acm.org/citation.cfm?id=2832181>. doi: ja href="http://dx.doi.org/10.4108/eai.24-8-2015.2260765";10.4108/eai.24-8-2015.2260765;aj.
- (11) F. Dahlqvist and D. Pym. and Completeness via canonicity for distributive substructural logics: a coalgebraic perspective. *Proc 15th Int. Conf. on Relational and Algebraic Methods in Computer Science (RAMiCS 2015)*, LNCS 9348: 119-135, 2015.
- (12) G. Anderson and D. Pym. Substructural modal logic for optimal resource allocation. Paper 5, *Proc. Strategic Reasoning 2015*, St. Catharine’s College, Oxford, September 21-22, 2015.
- (13) G. Anderson and D. Pym. Trust Domains in system models: algebra, logic, utility, and combinators. *J. of Logic & Computation*, 2015: doi: 10.1093/logcom/exv030.

- (14) M. Collinson, K. McDonald, and D. Pym. Layered Graph Logic as an Assertion Language for Access Control Policy Models. *J. of Logic & Computation*, 2015. doi: 10.1093/logcom/exv020.
- (15) M. Collinson, K. McDonald, and D. Pym. A Substructural Logic for Layered Graphs. *J. of Logic & Computation* 24 (4):953-988, 2014. doi: 10.1093/logcom/exu002. Erratum: *J. of Logic & Computation*, 2015. doi: 10.1093/logcom/exv019.
- (16) D. Pym, E. Ritter, and E. Robinson. A Proof-theoretic Analysis of the Classical Matrix Method. *J. of Logic & Computation* 24 (1): 283-301, 2014.
- (17) M. Collinson, B. Monahan, and D. Pym. *A Discipline of Mathematical Systems Modelling*. College Publications, 2012.
- (18) M. Collinson, B. Monahan, and D. Pym. Semantics for Structured Systems Modelling and Simulation. *Proc. Simutools 2010*. ACM Digital Library and EU Digital Library. doi: 10.4108/ICST.SIMUTOOLS2010.8631.
- (19) A. Beutement et al. Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. In *Managing Information Risk and the Economics of Security*. M. Eric Johnson (editor), Springer, 2009: 141–163.
- (20) M. Collinson, D. Pym, and E. Robinson. Bunched Polymorphism. *Mathematical Structures in Computer Science* 18(6), 1091–1132, 2008.
- (21) G. McCusker and D. Pym. A Games Model of Bunched Implications. *Proc. CSL ’07*, LNCS 4646: 573–588.
- (22) D. Pym, P. O’Hearn, and H. Yang. Possible Worlds and Resources: The Semantics of BI. *Theoretical Computer Science* 315(1):257–305.
- (23) C. Führmann and D. Pym. On Categorical Models of Classical Logic and the Geometry of Interaction *Mathematical Structures in Computer Science*, 17, 957–1027, 2007.
- (24) C. Führmann and D. Pym. On the Geometry of Interaction for Classical Logic (Extended Abstract). *Proc. LICS 04*, IEEE Comp. Soc. Press, 2004, 211–220.
- (25) C. Führmann and D. Pym. Order-enriched categorical models of the classical sequent calculus. *Journal of Pure and Applied Algebra*, 204(1), 21–78, 2006.
- (26) J. Harland and D. Pym. Resource-distribution via Boolean constraints. *ACM Transactions on Computational Logic* 4(1), 56–90, 2003.
- (27) D. Pym, E. Ritter, and L. Wallen. On the intuitionistic force of classical search. *Theoretical Computer Science* 232 (2000) 299-333.
- (28) D.J. Pym and E. Ritter. On the semantics of classical disjunction. *Journal of Pure and Applied Algebra* 159 (2001) 315–338.
- (29) D. Pym, E. Ritter, and L. Wallen. Proof-terms for classical and intuitionistic resolution. *Journal of Logic and Computation* 10(2), 173–207, 2000.
- (30) P. O’Hearn and D. Pym. The Logic of Bunched Implications. *Bull. Symb. Log.* 5(2), 215–243, 1999.

#### Security economics, security modelling, and policy.

- (1) J.M. Spring, T. Moore, and D. Pym. Practicing a Science of Security: A Philosophy of Science Perspective. To appear: *Proc. New Security Paradigms Workshop, Islamorada, FL, USA, 2-4 Oct., 2017*. doi: 10.475/xxx.x.

- (2) T. Caulfield, C. Ioannidis, and D. Pym. The U.S. Vulnerabilities Equities Process: An Economic Perspective. *Proc. GameSec 2017*, LNCS 10575:131–150, 2017.
- (3) T. Caulfield, C. Ioannidis, and D. Pym. On the adoption of privacy-enhancing technologies. *Proc. GameSec 2016*, LNCS 9996:175-194, 2016.
- (4) C. Ioannidis, D. Pym, and J. Williams. Ioannidis, C., Pym, D., and Williams, J. (2016) Is Public Co-Ordination of Investment in Information Security Desirable? *Journal of Information Security* 7, 60-80, 2016. doi: 10.4236/jis.2016.72005.
- (5) A. Baldwin, I. Gheyas, C. Ioannidis, D. Pym, and J. Williams. Contagion in Cybersecurity Attacks. In press, *J. of the Operational Research Society*, 2016.
- (6) T. Caulfield, C. Ioannidis, and D. Pym. Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption. *Proc. Financial Cryptography and Data Security 2016*. [http://fc16.ifca.ai/preproceedings/16\\_Caulfield.pdf](http://fc16.ifca.ai/preproceedings/16_Caulfield.pdf).
- (7) T. Caulfield and D. Pym. Improving Security Policy Decisions with Models. *IEEE Security and Privacy*, 13(5), 34-41, Sept/Oct 2015.
- (8) T. Caulfield, D. Pym, and J. Williams. Compositional Security Modelling: Structure, Economics, and Behaviour. LNCS 8533: 233–245, 2014.
- (9) C. Ioannidis, D. Pym, J. Williams, and I. Gheyas. Resilience in Information Stewardship. In *Proc. WEIS 2014*, Pennsylvania State University, June 2014. <http://www.econinfosec.org/archive/weis2014/papers/Ioannidis-WEIS2014.pdf>.
- (10) C. Ioannidis, D. Pym, and J. Williams. Sustainability in Information Stewardship: Time Preferences, Externalities, and Social Co-ordination. In *Proc. WEIS 2013*, Georgetown University, June 2013. <http://www.econinfosec.org/archive/weis2013/papers/IoannidisPymWilliamsWEIS2013.pdf>.
- (11) G. Anderson. M. Collinson, and D. Pym. Utility-based Decision-making in Distributed Systems Modelling [Extended Abstract]. *Proc. TARK 2013*, Burkhard C. Schipper (editor), Chennai, 2013. Computing Research Repository (CoRR): <http://arxiv.org/corr/home>. ISBN: 978-0-615-74716-3.
- (12) C. Ioannidis, D. Pym, and J. Williams. Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach. In *Economics of Security and Privacy III*, Bruce Schneier (editor), Springer 2012. pp. 171–192.
- (13) C. Ioannidis, D. Pym, and J. Williams. Information Security Trade-offs and Optimal Patching Policies. *European Journal of Operational Research*, 216(2):434-444, 2012.
- (14) D. Pym and S. Shiu. Information Stewardship in the Cloud. *IISP Pulse* 7 Winter 2011: 6-8. Available at: [http://www0.cs.ucl.ac.uk/staff/D.Pym/PULSE\\_7\\_final.pdf](http://www0.cs.ucl.ac.uk/staff/D.Pym/PULSE_7_final.pdf).
- (15) Contributor to the ENISA report Economics of Security: Facing the Challenges. Luxembourg: Publications Office of the European Union, 2012. ISBN: 978-92-9204-057-4, doi: 10.2824/23063.
- (16) D. Pym and S. Shiu. Security Analytics: Bringing Science to Security Management. *IISP Pulse* 4 Summer 2010: 12-13. Available at <http://www0.cs.ucl.ac.uk/staff/D.Pym/IISPulse4final.pdf>.
- (17) A. Baldwin, D. Pym, M. Sadler, and Simon Shiu. Information Stewardship in Cloud Ecosystems: Towards Models, Economics, and Delivery. *Proc. CloudCom 2011*. IEEE Digital Library, 784–791, 2011. doi: 10.1109/CloudCom.2011.121.
- (18) C. Ioannidis, D. Pym, and J. Williams. Investments and Trade-offs in the Economics of Information Security. *Proc. Financial Cryptography and Data Security 2009*, LNCS 5628: 148-162, 2009.