Prof. George Danezis, B.A. (Hons), M.A. (Cantab), Ph.D., FBCS

CONTACT INFORMATION

University College London,	*E-Mail:* g.danezis@ucl.ac.uk	*Twitter:* @gdanezis
Dept. of Computer Science,	*Web:* `http://danez.is`	*LinkedIn:* gdanezis
London WC1E 6BT, U.K.		*Skype:* george_danezis

RESEARCH INTERESTS

Computer security, privacy technologies, traffic analysis, peer-to-peer and distributed systems, inference and probabilistic modelling, applied cryptography, smart grids and transportation security.

EMPLOYMENT

MystenLabs, London, UK

Nov. 2021 – present   **Co-founder & Chief Scientist**
Co-designer and engineer for the Sui smart contract platform, and the Narwhal / Tusk consensus core products by Mysten Labs; co-founder and member of the business leadership team.

Dept. of Computer Science, University College London, London, UK

Oct. 2016 – present   **Professor of Security and Privacy Engineering**
Oct. 2016 – Nov. 2020   **Turing Institute Faculty Fellow**
Oct. 2013 – Oct. 2016   **Reader in Security and Privacy Engineering**
Full-time research in security and privacy, teaching duties and holding grants funding 8 doctoral and 2 post-doctoral researchers.

Facebook & Novi Financial, London, UK

Feb. 2019 – Jul. 2021   **Research Scientist, Director Level (IC8)**
Co-designed the Diem payment system and its regulatory compliance mechanism (DIP-1). Led advanced R&D on distributed systems performance and security.

Chainspace.io, London, UK

Sept. 2018 – Feb. 2019   **Co-founder & Head of Research**
Co-founded the blockchain start-up and acted as Head of Research. Successful exit, with the team moving to Facebook.

Microsoft Research, Cambridge, UK

Sept. 2009 – Sept. 2013   **Researcher**
Sept. 2007 – Aug. 2009   **Post-doctoral researcher**
Researcher in security and privacy, under Andy Gordon, Byron Cook, Luca Cardelli and Tuomas Aura: full time research; managing post-doctoral researchers and interns; and privacy lead for the lab.

ESAT, Katholieke Universiteit Leuven, Belgium

Oct. 2005 – Sept. 2007   **Post-doctoral visiting fellow**
Post-doctoral fellowship funded by the Flemish research council (FWO) and the Katholieke Universiteit Leuven, at the COSIC group headed by Prof. Bart Preneel.

Computer Laboratory, University of Cambridge, UK

June 2004 – Oct. 2005   **Research associate**
Sept. 2003 – June 2004   **Research assistant**
Post-doctoral work funded by the Cambridge-MIT Institute project, *'Next generation peer-to-peer networks'* on peer-to-peer privacy and censorship resistant technologies.

EDUCATION

Oct. 2000 – June 2004,   Ph.D., **Computer Laboratory, University of Cambridge**, UK
PhD thesis on "Better Anonymous Communications", supervised by Prof. Ross J. Anderson.

Oct. 1997 – June 2000,   B.A. (Hons), **Queens' College, University of Cambridge**, UK.
B.A. (Hons) in Computer Science (first class grade), with the 50% Part I Physics.
Foundation Scholar of Queens' College (2000). M.A. (Cantab) (2004).

June 1997   European Baccalaureate, **European School of Brussels I**, Belgium.

POSITIONS OF RESPONSIBILITY

- **Program chair** of ACM Computers and Communications Security (CCS 2011 & 2012).

- Member of the **steering committee** of ACM Computers and Communications Security (2012–2019).
- **Program chair** of Financial Cryptography & Data Security (FC 2011).
- **Program chair** of the Privacy Enhancing Technologies Workshop (PET 2006) and (PET 2005).
- Member of **Board** of the Privacy Enhancing Technologies Symposium (2004–).
- **General chair** of IEEE European Symposium on Security and Privacy (IEEE EuroS&P 2018).
- **Management Board** of the UK Cybersecurity Body of Knowledge Project (CyBOK) (2017–2019).
- Selected **program committee** membership
    IEEE Symposium on Security & Privacy (2006, 2009, 2013–2014, 2017),
    ACM Computers and Communications Security (CCS 2007–2010, 2014–2016, 2020–2021),
    USENIX Security Symposium (2008–2010, 2014–2016, 2019–2021),
    ISoc Network and Distributed Systems Security (NDSS 2010–2011),
    Privacy Enhancing Technologies Symposium (PET 2004, 2007–2009, 2011–2013, 2015–2017)
    Other conferences: ACM Symposium on Information, Computer & Communication Security (ASI-ACCS 2007, 2009), Financial Cryptography (FC 2008–2010, 2013–2014, 2016, 2019–2021), Information Hiding (2011–2015), IEEE Computer Security Foundations Symposium (CSF 2007, 2010), European Symposium on Research in Computer Security (ESORICS 2005–2006, 2010–2011, 2021), Euro S&P (2015-2016),
- Member of the **steering committee** of ACM Information Hiding and Multimedia Security (2012–2019).
- Member of the **editorial board** of Transactions on Data Privacy (2008–2011).
- **Expert** for the European Union Agency for Network and Information Security (ENISA) (2014–). Provided expertise for the EU and UK Parliament, UK law commission, UK Government Office for Science.
- Member of the **advisory board** of Privacy International (2011–2014), Simply Secure project (2014–), GOV.UK Verify Consumer & Privacy (2015–2019), The Open Rights Group (2017–).
- **Advisor** to Privitar (2016–), DeepMind Transparency, Security and Privacy (2018–2019), Spherical Defence (2018–), Vega Protocol (2018–2019), NYM Technologies (2018–2019, 2021–), Celestia (2021–).
- **Doctoral thesis examiner** of *Carmela Troncoso* (KU Leuven), *Markulf Kohlweiss* (KU Leuven), *Prateek Mittal* (UIUC), *Reza Shokri* (EPFL), *Nicolás Bordenabe* (École Polytechnique), *Linna Kamm* (Tartu), *Enrique Larraia* (Bristol), *Brandon Wiley* (Texas, Austin), *Antony Morton* (UCL), *Sune Jakobsen* (QMUL), *Sebastian Meiser* (Saarland), *Anna Krasnova* & *Wouter Lueks* (Radboud University), *Chen Chen* (CMU), *Jeremiah Onaolapo* (UCL), *Apostolos Pyrgelis* (UCL), *Jonathan Bootle* (UCL), *Arnis Parsovs* (Tartu), *Bristena Oprisanu* (UCL).

Honours and Awards
- Prize for best paper in the Privacy Enhancing Technologies field for the year 2002 & 2018.
- Fellow of the British Computing Society (FBCS) (2014–).
- Data Protection by Design Award, Catalan Data Protection Authority (2017).
- Most notable publication award by the (Cambridge) Computer Laboratory Lab Ring (2006).

Funding
- EPSRC Smart Meter Research Portal (co-I, EPSRC £67,240) (2017–)
- EU Horizon 2020 Project DECODE (PI, EU £419,062) (2016–)
- EPSRC Glass Houses Project (co-I, EPSRC £969,096) (2016–)
- EU Horizon 2020 Project PANORAMIX (PI, EU £368,766) (2015–)
- EU Horizon 2020 Project NEXTLEAP (PI, EU £229,000) (2015–)
- Joint UK-Israel Cyber-security Project (PI, EPSRC £177,435) (2015–)

Selected Teaching & Student Supervision
- University College London **Lecture Series** and labs on *Computer Security I* (40 hours, UCL COMPGA01 2013–2016) and *Privacy Technologies* (40 hours with Labs, UCL COMPGA17 2014–2018), *Design and Professional Practice* (40 hours, UCL ENGS102P, 2017–2018).
- Queens' College Cambridge **teaching affiliate** (2008) and **supervisor** (2000–2008) in *computer security, introduction to security, concurrent systems, further java, software engineering* and *ethics*.
- Supervised **seven undergraduate projects** (Cambridge) and **countless MSc/MEng theses** (UCL).

Patents
Named inventor on four U.S. patents (US20120297198A1, US20110307551A1, US20120089494A1, US20140101053A1, US20200327252A1) filed on the topics of social networking and privacy technologies.

Selected Publications in Top Conferences & Journals

1. [DKSS22] George Danezis, Lefteris Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman. Narwhal and tusk: a dag-based mempool and efficient BFT consensus. In *EuroSys '22: Seventeenth European Conference on Computer Systems, Rennes, France, April 5 - 8, 2022*, pages 34–50. ACM, 2022

2. [SD21] Maria Anna Schett and George Danezis. Embedding a deterministic BFT protocol in a block DAG. In *PODC '21: ACM Symposium on Principles of Distributed Computing, Virtual Event, Italy, July 26-30, 2021*, pages 177–186. ACM, 2021

3. [SAB+19] Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, Sarah Meiklejohn, and George Danezis. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*, 2019

4. [ASB+18] Mustafa Al-Bassam, Alberto Sonnino, Shehar Bano, Dave Hrycyszyn, and George Danezis. Chainspace: A sharded smart contracts platform. In *Network and Distributed Systems Security (NDSS)*, 2018

5. [RDK18] Alfredo Rial, George Danezis, and Markulf Kohlweiss. Privacy-preserving smart metering revisited. *Int. J. Inf. Sec.*, 17(1):1–31, 2018

6. [HD17] Jamie Hayes and George Danezis. Generating steganographic images via adversarial training. In *Advances in Neural Information Processing Systems 30 (NIPS)*, pages 1951–1960, 2017

7. [MCS+17] Vasilios Mavroudis, Andrea Cerulli, Petr Svenda, Dan Cvrcek, Dusan Klinec, and George Danezis. A touch of evil: High-assurance cryptographic hardware from untrusted components. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, October, 2017*, 2017

8. [PHE+17] Ania M. Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The loopix anonymity system. In *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017.*, pages 1199–1216, 2017

9. [HD16] Jamie Hayes and George Danezis. k-fingerprinting: A robust scalable website fingerprinting technique. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 1187–1203, 2016

10. [DM16] George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies. *Network and Distributed Systems Security (NDSS)*, 2016

11. [LMC16] George Danezis Luca Melis and Emiliano De Cristofaro. Efficient private statistics with succinct sketches. *Network and Distributed Systems Security (NDSS)*, 2016

12. [CAB+15] Chen Chen, Daniele E. Asoni, David Barrera, George Danezis, and Adrian Perrig. Hornet: High-speed onion routing at the network layer. In *Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security, October, 2015*, 2015

13. [EDG14] Tariq Elahi, George Danezis, and Ian Goldberg. Privex: Private collection of traffic statistics for anonymous communication networks. In Gail-Joon Ahn, Moti Yung, and Ninghui Li, editors, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pages 1068–1079. ACM, 2014

14. [FKDL13] Cédric Fournet, Markulf Kohlweiss, George Danezis, and Zhengqin Luo. ZQL: A Compiler for Privacy-Preserving Data Processing. In Samuel T. King, editor, *USENIX Security*, pages 163–178. USENIX Association, 2013

15. [TDK+11] Carmela Troncoso, George Danezis, Eleni Kosta, Josep Balasch, and Bart Preneel. Pripayd: Privacy-friendly pay-as-you-drive insurance. *IEEE Trans. Dependable Sec. Comput.*, 8(5):742–755, 2011

16. [DG09] George Danezis and Ian Goldberg. Sphinx: A compact and provably secure mix format. In *IEEE Symposium on Security and Privacy*, pages 269–282. IEEE Computer Society, 2009

17. [DM09] George Danezis and Prateek Mittal. Sybilinfer: Detecting sybil nodes using social networks. In *NDSS*. The Internet Society, 2009

18. [TD09] Carmela Troncoso and George Danezis. The bayesian traffic analysis of mix networks. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *ACM Conference on Computer and Communications Security*, pages 369–379. ACM, 2009

19. [Dan07] George Danezis. Breaking four mix-related schemes based on universal re-encryption. *Int. J. Inf. Sec.*, 6(6):393–402, 2007

20. [BDMT07] Nikita Borisov, George Danezis, Prateek Mittal, and Parisa Tabriz. Denial of service or denial of security? In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 92–102. ACM, 2007

21. [DA05] George Danezis and Ross J. Anderson. The economics of resisting censorship. *IEEE Security & Privacy*, 3(1):45–50, 2005

22. [MD05] Steven J. Murdoch and George Danezis. Low-cost traffic analysis of tor. In *IEEE Symposium on Security and Privacy*, pages 183–195. IEEE Computer Society, 2005

23. [DDM03] George Danezis, Roger Dingledine, and Nick Mathewson. Mixminion: Design of a type III anonymous remailer protocol. In *IEEE Symposium on Security and Privacy*, pages 2–15. IEEE Computer Society, 2003

Top Cited in Specialized Venues

24. [SD02] Andrei Serjantov and George Danezis. Towards an information theoretic metric for anonymity. In Roger Dingledine and Paul F. Syverson, editors, *Privacy Enhancing Technologies*, volume 2482 of *Lecture Notes in Computer Science*, pages 41–53. Springer, 2002

25. [DLLKA05] George Danezis, Chris Lesniewski-Laas, M. Frans Kaashoek, and Ross J. Anderson. Sybil-resistant dht routing. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, *ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 2005

26. [Dan03b] George Danezis. Statistical disclosure attacks. In Dimitris Gritzalis, Sabrina De Capitani di Vimercati, Pierangela Samarati, and Sokratis K. Katsikas, editors, *SEC*, volume 250 of *IFIP Conference Proceedings*, pages 421–426. Kluwer, 2003

27. [RD11] Alfredo Rial and George Danezis. Privacy-preserving smart metering. In Yan Chen and Jaideep Vaidya, editors, *WPES*, pages 49–60. ACM, 2011

28. [STD+11] Reza Shokri, George Theodorakopoulos, George Danezis, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Quantifying location privacy: The case of sporadic location exposure. In Simone Fischer-Hübner and Nicholas Hopper, editors, *PETS*, volume 6794 of *Lecture Notes in Computer Science*, pages 57–76. Springer, 2011

29. [Dan04] George Danezis. The traffic analysis of continuous-time mixes. In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2004

30. [KDK11] Klaus Kursawe, George Danezis, and Markulf Kohlweiss. Privacy-friendly aggregation for the smart-grid. In Simone Fischer-Hübner and Nicholas Hopper, editors, *PETS*, volume 6794 of *Lecture Notes in Computer Science*, pages 175–191. Springer, 2011

31. [DLA05] George Danezis, Stephen Lewis, and Ross J. Anderson. How much is location privacy worth. In *Fourth Workshop on the Economics of Information Security*, 2005

32. [BAD09] Joseph Bonneau, Jonathan Anderson, and George Danezis. Prying data out of a social network. In Nasrullah Memon and Reda Alhajj, editors, *ASONAM*, pages 249–254. IEEE Computer Society, 2009

33. [DS04] George Danezis and Andrei Serjantov. Statistical disclosure or intersection attacks on anonymity systems. In Jessica J. Fridrich, editor, *Information Hiding*, volume 3200 of *Lecture Notes in Computer Science*, pages 293–308. Springer, 2004

34. [CKMD06b] Daniel Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. A study on the value of location privacy. In Ari Juels and Marianne Winslett, editors, *WPES*, pages 109–118. ACM, 2006

35. [Dan03a] George Danezis. Mix-networks with restricted routes. In Roger Dingledine, editor, *Privacy Enhancing Technologies*, volume 2760 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2003

Other Peer-Reviewed Publications

36. [SBAD20] Alberto Sonnino, Shehar Bano, Mustafa Al-Bassam, and George Danezis. Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers. In *IEEE European Symposium on Security and Privacy, EuroS&P 2020, Genoa, Italy, September 7-11, 2020*, pages 294–308. IEEE, 2020

37. [BDS20] Mathieu Baudet, George Danezis, and Alberto Sonnino. Fastpay: High-performance byzantine fault tolerant settlement. In *AFT '20: 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, October 21-23, 2020*, pages 163–177. ACM, 2020

38. [ADN20] Sarah Azouvi, George Danezis, and Valeria Nikolaenko. Winkle: Foiling long-range attacks in proof-of-stake systems. In *AFT '20: 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, October 21-23, 2020*, pages 189–201. ACM, 2020

39. [ABC+20] Nadia Alshahwan, Earl T. Barr, David Clark, George Danezis, and Héctor D. Menéndez. Detecting malware with information complexity. *Entropy*, 22(5):575, 2020

40. [HMDC19] Jamie Hayes, Luca Melis, George Danezis, and Emiliano De Cristofaro. LOGAN: membership inference attacks against generative models. *PoPETs*, 2019(1):133–152, 2019

41. [BSA+19] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. Sok: Consensus in the age of blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019*, pages 183–198, 2019

42. [LPDH19] Hemi Leibowitz, Ania M. Piotrowska, George Danezis, and Amir Herzberg. No right to remain silent: Isolating malicious mixes. In *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*, pages 1841–1858, 2019

43. [RDC$^+$18] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, 16(3):96–102, 2018

44. [HD18] Jamie Hayes and George Danezis. Learning universal adversarial perturbations with generative models. In *2018 IEEE Security and Privacy Workshops, SP Workshops 2018, San Francisco, CA, USA, May 24, 2018*, pages 43–49, 2018

45. [KLI$^+$18] Bogdan Kulynych, Wouter Lueks, Marios Isaakidis, George Danezis, and Carmela Troncoso. Claimchain: Improving the security and privacy of in-band key distribution for messaging. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society, WPES@CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 86–103, 2018

46. [CAP$^+$18] Chen Chen, Daniele Enrico Asoni, Adrian Perrig, David Barrera, George Danezis, and Carmela Troncoso. TARANET: traffic-analysis resistant anonymity at the network layer. In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*, pages 137–152, 2018

47. [TDE17] Raphael R. Toledo, George Danezis, and Isao Echizen. Mix-oram: Using delegated shuffles. In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society, Dallas, TX, USA, October 30 - November 3, 2017*, pages 51–61, 2017

48. [PHG$^+$17] Ania M. Piotrowska, Jamie Hayes, Nethanel Gelernter, George Danezis, and Amir Herzberg. Annotify: A private notification service. In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society, Dallas, TX, USA, October 30 - November 3, 2017*, pages 5–15, 2017

49. [PPM$^+$17] John P. Podolanko, Revanth Pobala, Hussain Mucklai, George Danezis, and Matthew Wright. Lilac: Lightweight low-latency anonymous chat. In *IEEE Symposium on Privacy-Aware Computing, PAC 2017, Washington, DC, USA, August 1-4, 2017*, pages 141–151, 2017

50. [TDIH17] Carmela Troncoso, George Danezis, Marios Isaakidis, and Harry Halpin. Systematizing decentralization and privacy: Lessons from 15 years of research and deployments. In *Proceedings of the Privacy Enhancing Technologies Symposium (PoPETs)*, page Issue (4):307329, 2017

51. [IHD16] Marios Isaakidis, Harry Halpin, and George Danezis. Unlimitid: Privacy-preserving federated identity management using algebraic macs. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, pages 139–142. ACM, 2016

52. [HTD16] Jamie Hayes, Carmela Troncoso, and George Danezis. Tasp: Towards anonymity sets that persist. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, pages 177–180. ACM, 2016

53. [TDG16] Raphael R. Toledo, George Danezis, and Ian Goldberg. Lower-cost $\in$-private information retrieval. *PoPETs*, 2016(4):184–201, 2016

54. [BCDA15] Luís Brandão, Nicolas Christin, George Danezis, and Anonymous. Toward mending two nation-scale brokered identification systems. *Proceedings on Privacy Enhancing Technologies*, 2015(2):135–155, 2015

55. [HD15] Jamie Hayes and George Danezis. Guard sets for onion routing. *Proceedings on Privacy Enhancing Technologies*, 2015(2):1–21, 2015

56. [BDG15] Nikita Borisov, George Danezis, and Ian Goldberg. Dp5: A private presence service. *Proceedings on Privacy Enhancing Technologies*, 2015(2):1–21, 2015

57. [DFGK14] George Danezis, Cédric Fournet, Jens Groth, and Markulf Kohlweiss. Square span programs with applications to succinct NIZK arguments. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 532–550. Springer, 2014

58. [DC14] George Danezis and Emiliano De Cristofaro. Fast and private genomic testing for disease susceptibility. In Ahn and Datta [AD14], pages 31–34

59. [SD14] Kumar Sharad and George Danezis. An automated social graph de-anonymization technique. In Ahn and Datta [AD14], pages 47–58

60. [MDH$^+$14] Rebecca Roisin Murphy, George Danezis, Mathew Harry Horrocks, Sophie E Jackson, and David Klenerman. Bayesian inference of accurate population sizes and fret efficiencies from single diffusing biomolecules. *Analytical chemistry*, 2014

61. [DFKP13] George Danezis, Cédric Fournet, Markulf Kohlweiss, and Bryan Parno. Pinocchio coin: building zerocoin from a succinct pairing-based proof system. In Martin Franz, Andreas Holzer, Rupak Majumdar, Bryan Parno, and Helmut Veith, editors, *PETShop@CCS*, pages 27–30. ACM, 2013

62. [DFKB13] George Danezis, Cédric Fournet, Markulf Kohlweiss, and Santiago Zanella Béguelin. Smart meter aggregation via secret-sharing. In Benessa Defend and Klaus Kursawe, editors, *SEGS@CCS*, pages 75–80. ACM, 2013

63. [BDG+13] Gilles Barthe, George Danezis, Benjamin Grégoire, César Kunz, and Santiago Zanella Béguelin. Verified computational differential privacy with applications to smart metering. In *CSF*, pages 287–301. IEEE, 2013

64. [DT13] George Danezis and Carmela Troncoso. You cannot hide for long: de-anonymization of real-world dynamic behaviour. In Ahmad-Reza Sadeghi and Sara Foresti, editors, *WPES*, pages 49–60. ACM, 2013

65. [DK12] George Danezis and Emilia Käsper. The dangers of composing anonymous channels. In Matthias Kirchner and Dipak Ghosal, editors, *Information Hiding*, volume 7692 of *Lecture Notes in Computer Science*, pages 191–206. Springer, 2012

66. [MMDF+12] Andres Molina-Markham, George Danezis, Kevin Fu, Prashant J. Shenoy, and David E. Irwin. Designing privacy-preserving smart meters with low-cost microcontrollers. In Angelos D. Keromytis, editor, *Financial Cryptography*, volume 7397 of *Lecture Notes in Computer Science*, pages 239–253. Springer, 2012

67. [DKLR12] George Danezis, Markulf Kohlweiss, Benjamin Livshits, and Alfredo Rial. Private client-side profiling with random forests and hidden markov models. In Simone Fischer-Hübner and Matthew Wright, editors, *Privacy Enhancing Technologies*, volume 7384 of *Lecture Notes in Computer Science*, pages 18–37. Springer, 2012

68. [DL11] George Danezis and Benjamin Livshits. Towards ensuring client-side computational integrity. In Christian Cachin and Thomas Ristenpart, editors, *CCSW*, pages 125–130. ACM, 2011

69. [DKR11] George Danezis, Markulf Kohlweiss, and Alfredo Rial. Differentially private billing with rebates. In Tomás Filler, Tomás Pevný, Scott Craver, and Andrew D. Ker, editors, *Information Hiding*, volume 6958 of *Lecture Notes in Computer Science*, pages 148–162. Springer, 2011

70. [DDTL10] George Danezis, Claudia Díaz, Carmela Troncoso, and Ben Laurie. Drac: An architecture for anonymous low-volume communications. In Mikhail J. Atallah and Nicholas J. Hopper, editors, *Privacy Enhancing Technologies*, volume 6205 of *Lecture Notes in Computer Science*, pages 202–219. Springer, 2010

71. [DACK10] George Danezis, Tuomas Aura, Shuo Chen, and Emre Kiciman. How to share your favourite search results while preserving privacy and quality. In Mikhail J. Atallah and Nicholas J. Hopper, editors, *Privacy Enhancing Technologies*, volume 6205 of *Lecture Notes in Computer Science*, pages 273–290. Springer, 2010

72. [Dan09] George Danezis. Inferring privacy policies for social networking services. In Dirk Balfanz and Jessica Staddon, editors, *AISec*, pages 5–10. ACM, 2009

73. [DT09] George Danezis and Carmela Troncoso. Vida: How to use bayesian inference to de-anonymize persistent communications. In Ian Goldberg and Mikhail J. Atallah, editors, *Privacy Enhancing Technologies*, volume 5672 of *Lecture Notes in Computer Science*, pages 56–72. Springer, 2009

74. [DDKT09] George Danezis, Claudia Díaz, Emilia Käsper, and Carmela Troncoso. The wisdom of crowds: Attacks and optimal constructions. In Michael Backes and Peng Ning, editors, *ESORICS*, volume 5789 of *Lecture Notes in Computer Science*, pages 406–423. Springer, 2009

75. [LAD+09] Janne Lindqvist, Tuomas Aura, George Danezis, Teemu Koponen, Annu Myllyniemi, Jussi Mäki, and Michael Roe. Privacy-preserving 802.11 access-point discovery. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *WISEC*, pages 123–130. ACM, 2009

76. [Dan08] George Danezis. Covert communications despite traffic data retention. In *Proceedings of the Security Protocols Workshop (SPW 2008)*, Sidney Sussex College, Cambridge, UK, 2008. Springer

77. [CD08] Daniel Cvrcek and George Danezis. Fighting the good internet war. In *Proceedings of the Security Protocols Workshop (SPW 2008)*, Sidney Sussex College, Cambridge, UK, 2008. Springer

78. [MDBP08] Yoni De Mulder, George Danezis, Leila Batina, and Bart Preneel. Identification via location-profiling in gsm networks. In *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society, WPES 2008, Alexandria, VA, USA, October, 2008*. ACM, 2008

79. [DS08b] George Danezis and Paul F. Syverson. Bridging and fingerprinting: Epistemic attacks on route selection. In *Privacy Enhancing Technologies, 8th International Symposium, PETS 2008, Leuven, Belgium, July 23-25, 2008, Proceedings*, volume 5134 of *Lecture Notes in Computer Science*, pages 151–166. Springer, 2008

80. [DS08a] George Danezis and Len Sassaman. How to bypass two anonymity revocation schemes. In *Privacy Enhancing Technologies, 8th International Symposium, PETS 2008, Leuven, Belgium, July 23-25, 2008, Proceedings*, volume 5134 of *Lecture Notes in Computer Science*, pages 187–201. Springer, 2008

81. [TDKP07] Carmela Troncoso, George Danezis, Eleni Kosta, and Bart Preneel. Pripayd: privacy friendly pay-as-you-drive insurance. In Peng Ning and Ting Yu, editors, *Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society, WPES 2007, Alexandria, VA, USA, October 29, 2007*, pages 99–107. ACM, 2007

82. [DTD07] Claudia Díaz, Carmela Troncoso, and George Danezis. Does additional information always reduce anonymity? In Peng Ning and Ting Yu, editors, *Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society, WPES 2007, Alexandria, VA, USA, October 29, 2007*, pages 72–75. ACM, 2007

83. [DDF$^+$07] George Danezis, Claudia Díaz, Sebastian Faust, Emilia Käsper, Carmela Troncoso, and Bart Preneel. Efficient negative databases from cryptographic hash functions. In Juan A. Garay, Arjen K. Lenstra, Masahiro Mambo, and René Peralta, editors, *ISC*, volume 4779 of *Lecture Notes in Computer Science*, pages 423–436. Springer, 2007

84. [DDT07] George Danezis, Claudia Díaz, and Carmela Troncoso. Two-sided statistical disclosure attack. In Nikita Borisov and Philippe Golle, editors, *Privacy Enhancing Technologies, 7th International Symposium, PET 2007 Ottawa, Canada, June 20-22, 2007, Revised Selected Papers*, volume 4776 of *Lecture Notes in Computer Science*, pages 30–44. Springer, 2007

85. [DD07] George Danezis and Claudia Diaz. Space-efficient private search. In *Financial Cryptography (FC 2007)*, Lowlands, Scarborough, Trinidad/Tobago, February 12–15 2007. Springer

86. [BD06] Mike Bond and George Danezis. A pact with the devil. In *ACM New Security Paradigms Workshop (NSPW 2006)*, Schloss Dagstuhl, Germany, September 19–22 2006. ACM

87. [DC06] George Danezis and Richard Clayton. Route fingerprinting in anonymous communications. In *P2P '06: Proceedings of the Sixth IEEE International Conference on Peer-to-Peer Computing*, pages 69–72, Washington, DC, USA, 2006. IEEE Computer Society

88. [DW06] George Danezis and Bettina Wittenben. The economics of mass surveillance and the questionable value of anonymous communications. In *Workshop on Economics and Information Security (WEIS 2006)*, Cambridge, UK, June 2006

89. [Dan06] George Danezis. Breaking four mix-related schemes based on universal re-encryption. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 46–59. Springer, 2006

90. [CKMD06a] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. The value of location information: A european-wide study. In Bruce Christianson, Bruno Crispo, and Michael Roe, editors, *Security Protocols Workshop*, Lecture Notes in Computer Science. Springer, 2006

91. [BD05] Mike Bond and George Danezis. The dining freemasons (security protocols for secret societies). In Bruce Christianson, Bruno Crispo, and Michael Roe, editors, *Security Protocols Workshop*, Lecture Notes in Computer Science. Springer, 2005

92. [DC05] George Danezis and Jolyon Clulow. Compulsion resistant anonymous communications. In Mauro Barni, Jordi Herrera-Joancomartí, Stefan Katzenbeisser, and Fernando Pérez-González, editors, *Information Hiding*, volume 3727 of *Lecture Notes in Computer Science*, pages 11–25. Springer, 2005

93. [DA04] George Danezis and Ross J. Anderson. The economics of censorship resistance. In *Workshop on Economics and Information Security (WEIS 2004)*, Minneapolis, MI, May 2004

94. [DL04] George Danezis and Ben Laurie. Minx: a simple and efficient anonymous packet format. In Vijay Atluri, Paul F. Syverson, and Sabrina De Capitani di Vimercati, editors, *WPES*, pages 59–65. ACM, 2004

95. [DS03] George Danezis and Len Sassaman. Heartbeat traffic to counter (n-1) attacks: red-green-black mixes. In Sushil Jajodia, Pierangela Samarati, and Paul F. Syverson, editors, *WPES*, pages 89–93. ACM, 2003

96. [Dan02] George Danezis. Forward secure mixes. In Jonsson Fisher-Hubner, editor, *Nordic workshop on Secure IT Systems (Norsec 2002)*, pages 195–207, Karlstad, Sweden, November 2002

97. [CD02] Richard Clayton and George Danezis. Chaffinch: Confidentiality in the face of legal threats. In Fabien A. P. Petitcolas, editor, *Information Hiding*, volume 2578 of *Lecture Notes in Computer Science*, pages 70–86. Springer, 2002

98. [CDK01] Richard Clayton, George Danezis, and Markus G. Kuhn. Real world patterns of failure in anonymity systems. In Ira S. Moskowitz, editor, *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 230–244. Springer, 2001

99. [Dan00] George Danezis. An anonymous auction protocol using "money escrow" (transcript of discussion). In Bruce Christianson, Bruno Crispo, and Michael Roe, editors, *Security Protocols Workshop*, volume 2133 of *Lecture Notes in Computer Science*, pages 223–233. Springer, 2000

BOOK CHAPTERS

- George Danezis. *Trust, Computing, and Society*, chapter Trust as a methodological tool in security engineering. Cambridge University Press, May 2014

- George Danezis, Claudia Diaz, and Paul Syverson. Systems for anonymous communication. *Handbook of Financial Cryptography and Security, Cryptography and Network Security Series*, pages 341–389, 2009

- George Danezis and Richard Clayton. *Digital Privacy: Theory, Technologies and Practices*, chapter Introducing Traffic Analysis, pages 95–116. Auerbach Publications, 2007

- George Danezis and Richard Clayton. *Digital Privacy: Theory, Technologies and Practices*, chapter Byzantine Attacks on Anonymity Systems, pages 73–94. Auerbach Publications, 2007

Editor

- Ting Yu, George Danezis, and Virgil D. Gligor, editors. *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012.* ACM, 2012

- George Danezis, Sven Dietrich, and Kazue Sako, editors. *Financial Cryptography and Data Security - FC 2011 Workshops, RLCPS and WECSR 2011, Rodney Bay, St. Lucia, February 28 - March 4, 2011, Revised Selected Papers*, volume 7126 of *Lecture Notes in Computer Science*. Springer, 2012

- Yan Chen, Vitaly Shmatikov, and George Danezis, editors. *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011.* ACM, 2011

- George Danezis, editor. *Financial Cryptography and Data Security, 15th International Conference, FC 2011, St. Lucia, February 28 - March 4, 2011, Revised Selected Papers*, volume 7035 of *Lecture Notes in Computer Science*. Springer, 2011

- George Danezis and David Martin, editors. *Privacy Enhancing Technologies, 5th International Workshop, PET 2005, Cavtat, Croatia, May 30-June 1, 2005, Revised Selected Papers*, volume 3856 of *Lecture Notes in Computer Science*. Springer, 2006

- George Danezis and Philippe Golle, editors. *Privacy Enhancing Technologies, 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers*, volume 4258 of *Lecture Notes in Computer Science*. Springer, 2006

Commissioned Reports

- M. Angela Sasse, George Danezis, Sarah Meiklejohn, Daniel Shiu, and Phil Godsiff. *Distributed Ledger Technology: beyond block chain*, chapter Security and Privacy. Government Office for Science, Dec 2015

- George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, and Stefan Schiffner. Privacy and data protection by design - from policy to engineering. *ENISA Technical Report*, January 2015