

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

CONTACT INFORMATION	Microsoft Research Cambridge, Roger Needham Building, 7 J J Thomson Avenue, Cambridge, CB3 0FB, U.K.	Voice: +44 (1223) 479812 Ext: 3812 E-mail: gdane@microsoft.com WWW: research.microsoft.com/users/gdane/
RESEARCH INTERESTS	Computer security, privacy enhancing technologies, traffic analysis, peer-to-peer networking, Bayesian inference and probabilistic modelling.	
EDUCATION	2000 – 2004, Ph.D., Computer Laboratory, University of Cambridge, UK Doctoral thesis in computer security entitled “Better Anonymous Communications”, supervised by Professor Ross J. Anderson. 1997 – 2000, B.A. (Hons), Queens’ College, University of Cambridge, UK B.A. (Hons) in Computer Science with a first class pass grade, with the 50% physics option in the first year (1997-98). 1997, European Baccalaureate, European School of Brussels I, Belgium.	
HONOURS AND AWARDS	<ul style="list-style-type: none">- Shortlisted for best paper in the Privacy Enhancing Technologies field for the year 2005 (2006).- “Most notable publication” award by the (Cambridge) Computer Laboratory Lab Ring (2006).- Cambridge Master of Arts degree, M.A. (Cantab) (2004).- Prize for best paper in the Privacy Enhancing Technologies field for the year 2002 (2003).- Nominated for the “Prix Voltaire” at the Big Brother Awards France (2003)- Cambridge European Union Trust scholarship (2000 – 2003).- Foundation Scholar of Queens’ College Cambridge (2000).	
ACADEMIC EXPERIENCE	Microsoft Research Cambridge, UK Sept. 2009 – present Researcher Sept. 2007 – Aug. 2009 Post-doctoral researcher Full time researcher in security and privacy, under the Luca Cardeli. 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, to work on traffic analysis, covert communications and anonymity in the COSIC group headed by Prof. Bart Preneel. The position involves independent research and frequent involvement with national and EU funded projects. 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, ‘ <i>Next generation peer-to-peer networks</i> ’ on peer-to-peer privacy and censorship resistant technologies. Frequent collaboration and travel to MIT.	

POSITIONS OF
RESPONSIBILITY

- Co-program chair of the Privacy Enhancing Technologies Workshop (PET 2006) and (PET 2005).
- Member of the Privacy Enhancing Technologies Workshop Board (2004–).
- Chair of the Privacy Enhancing Technologies Award committee (2007).
- Publication Chair for IEEE SecureComm (2007).
- Member of the editorial board of Transactions on Data Privacy (2008–).
- Program committee member of
 - EUROSEC Workshop (2010), ISoc Network and Distributed Systems Security (NDSS 2010), IEEE Symposium on Security & Privacy (2006, 2009), ACM Computers and Communications Security (CCS 2007–2010), USENIX Security Symposium (2008–2010) Privacy Enhancing Technologies Symposium (PET 2004, 2007–2009), ACM Symposium on Information, Computer & Communication Security (ASIACCS 2007, 2009), Financial Cryptography (FC 2008–2010) IEEE Computer Security Foundations Symposium (CSF 2007, 2010), European Symposium on Research in Computer Security (ESORICS 2005–2006, 2010), WWW (Security, Privacy and Ethics Track, 2006–2007), ACM Workshop on Privacy in the Electronic Society (WPES 2004–2005), Current Trends in Theory and Practice of Computer Science (SOFSEM 2008), Workshop on Applications of Private and Anonymous Communications (AIPACa 2008), European Conference on Computer Network Defense (EC2ND 2007–2008), International Workshop on Security (IWSEC 2007), ACM CCSW (2009), ACM AISec (2009), WECSR (2010), NetEcon (2006), Information Security Conference (ISC2006)

SELECTED INVITED
TALKS

- Panelist: Privacy – A Fine Balance (Nov. 2008, London, UK)
- Keynote: Anonymity and Cryptography (WEWoRC, Jun. 2007, Bochum, Germany)
- Privacy as a Security Property (CALIT Business event Oct. 2006, IPICS Summer School Jul. 2006, Microsoft Redmond Feb. 2006)
- An Overview of the State of the Art in Anonymous Communications (ITE, Crete, Sept. 2006)
- Keynote: Introducing Traffic Analysis: Attacks, Defences and Public Policy Issues (Santa’s Crypto Get-together. Prague, Dec. 2005, Chaos Communication Congress (CCC) Dec. 2006 and SEC 2007, Prague.)
- The MixMinion packet format (Dagstuhl School, Oct. 2005)
- Towards a discipline of Traffic Analysis (UMass Amherst, UMass Lowell, Nov. 2004)
- An Introduction to Privacy Enhancing Technologies (Internet Society Geneva, Jul. 2004).
- The Economics of Security (Communications Innovation Institute launch event, Jun. 2004).
- Anonymous communications and systems (University of Cambridge, Security Course, Oct. 2003).
- Traffic Data Retention: Its impact on Civil Society (UN World civil society forum, Jul. 2002).
- Chaffinch (MIT LCS Applied Security Reading Group, Mar. 2002).

TEACHING

- Queens’ College Cambridge teaching affiliate (2008).
- Privacy and Anonymous credentials (4 hours, Security application development, Mar. 2008, Leuven, Belgium)
- Lecture series on Privacy Technology (6 hours, Dec. 2007, Tartu, Estonia)
- Data Matters: Technical Aspects of Privacy in Communications and Privacy Preserving Data Analysis (3 hours, Tutorial. Computers Freedom and Privacy (CFP), May 2007, Montreal, Canada)
- ‘Privacy Technology’ & ‘Computer Security’ (2 lectures. COSIC Course Jul. 2007, Leuven, Belgium)

Supervised Cambridge University courses on *computer security, introduction to security, concurrent systems and applications, further java, software engineering and ethics*, as well as over six final year projects on security.

OTHER

Nationality: Dual Greek / French, *Date of Birth:* 6 December 1979, *Language skills:* Greek (native), French (native, DELF/DALF), English (IELTS).

EDITOR

- 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

KEY
PEER-REVIEWED
PUBLICATIONS

The computer security community publishes in international high-impact peer-reviewed conferences with acceptance rates often lower than 20%–15%. The most prestigious venues in the field are the IEEE Symposium on Security and Privacy, ACM Computer and Communications Security (CCS), USENIX Security Symposium and the European Symposium on Research in Computer Security (ESORICS). Key publications comprise papers published in journals, these selected venues, as well as publications with more than 25 citations according to *Google scholar*.

- [DG09] George Danezis and Ian Goldberg. Sphinx: A compact and provably secure mix format. In *IEEE Symposium on Security and Privacy*, San Diego, USA, May 17–20 2009. IEEE (to appear)
- [Dan07] George Danezis. Breaking four mix-related schemes based on universal re-encryption. *Int. J. Inf. Sec.*, 6(6):393–402, 2007 (9 citations)
- [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 (4 citations)
- [DA05] George Danezis and Ross J. Anderson. The economics of resisting censorship. *IEEE Security & Privacy*, 3(1):45–50, 2005 (11 citations)
- [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 (36 citations)
- [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 (90 citations)
- [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 (35 citations)
- [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 (56 citations)
- [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 (48 citations)
- [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 (46 citations)
- [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 (231 citations)
- [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 (270 citations)

- [DM09] George Danezis and Prateek Mittal. Sybilinifer: Detecting sybil nodes using social networks. In *16th Annual Network & Distributed System Security Symposium (NDSS 2009)*, San Diego, USA, February 7–12 2009. Internet Society
- [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
- [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
- [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
- [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
- [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
- [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
- [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
- [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
- [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
- [DD07] George Danezis and Claudia Diaz. Space-efficient private search. In *Financial Cryptography (FC 2007)*, Lowlands, Scarborough, Trinidad/Tobago, February 12–15 2007. Springer
- [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
- [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
- [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
- [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
- [CKMD06a] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. A study on the value of location privacy. In *WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 109–118, New York, NY, USA, 2006. ACM Press
- [CKMD06b] 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

- [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
- [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
- [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
- [DDG⁺04] Claudia Díaz, George Danezis, Christian Grothoff, Andreas Pfitzmann, and Paul F. Syverson. Panel discussion - mix cascades versus peer-to-peer: Is one concept superior? In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, pages 242–242. Springer, 2004
- [BDD⁺04] Rainer Böhme, George Danezis, Claudia Díaz, Stefan Köpsell, and Andreas Pfitzmann. On the pet workshop panel "mix cascades versus peer-to-peer: Is one concept superior?". In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, pages 243–255. Springer, 2004
- [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
- [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
- [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
- [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
- [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
- [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

ACADEMIC
REFERENCES

The following people can be contacted to provide references about my work at any time, and without prior arrangement.

Prof. R.J. Anderson
(PhD & Post-doc supervisor)
University of Cambridge
Computer Laboratory
15 J J Thomson Avenue
Cambridge CB3 0FD, UK

email: rja14@cl.cam.ac.uk
Voice: +44 1223 33 47 33
Fax: +44 1223 33 46 78

Dr Tuomas Aura
(Line manager)
Microsoft Research
Roger Needham Building
7 J J Thomson Avenue
Cambridge, CB3 0FB, UK.

email: tuomaura@microsoft.com
Voice: +44 1223 479708

Prof. B. Preneel
(Post-doc supervisor)
Katholieke Universiteit Leuven
Dept. Elektrotechniek-ESAT /COSIC
Kasteelpark Arenberg 10 Bus 2446
B-3001 Leuven-Heverlee, Belgium.

email: bart.preneel@esat.kuleuven.be
Voice: +32(0)16 32 11 48
Fax: +32(0)16 32 19 69