

# Emiliano De Cristofaro

Palo Alto Research Center (PARC)  
3333 Coyote Hill Road  
Palo Alto, CA, 94304, U.S.A.  
PARC Email: [edc@parc.com](mailto:edc@parc.com)  
PARC Homepage: <http://www.parc.com/edc>

Personal Email: [edecrist@uci.edu](mailto:edecrist@uci.edu), [me@emilianodc.com](mailto:me@emilianodc.com)  
Personal Homepage: <http://www.emilianodc.com>

## Research Interests

- Network and Systems Security
- Privacy and Applied Cryptography

## Education

- **PhD**, Computer Science Department, University of California, Irvine. Advisor: Gene Tsudik.  
Fall 2007 – Summer 2011.
- **BSc Honors**, Computer Science (*summa cum laude*). University of Salerno, Italy.  
Fall 2000 – Summer 2005.

## Research Experience

- **September 2011 – Ongoing**. Member of the Research Staff at PARC (Security Group).  
Ongoing projects: security, privacy, and verifiability in next-generation cloud architectures; security and privacy vulnerabilities and countermeasures in the smart grid; security aspects of Content Centric Networking.
- **June – September 2010**. Internship at Nokia Research Center, Lausanne, Switzerland.  
Collaboration with Dr. I. Aad and Dr. V. Niemi.  
Designed, implemented, and evaluated several techniques for privacy protection in smartphone applications.  
Consulted on several Nokia projects as cryptography/security expert.
- **September – December 2009**. Internship at INRIA Rhone Alpes, Grenoble, France.  
Collaboration with Dr. C. Castelluccia.  
Discovered and demonstrated an inference attack that reconstructs web search history of Google users.  
Designed and implemented a system for protecting privacy of archived data.
- **January 2009**. Research Visit at Singapore Management University.  
Collaboration with Prof. X. Ding.  
Designed a cryptographic protocol for protecting query privacy in wireless sensor networks.
- **June – September 2008**. Internship at NEC Europe Research Lab, Heidelberg, Germany.  
Collaboration with Dr. D. Westhoff.  
Designed and implemented a framework for resilient data aggregation in wireless sensor networks.
- **2006-2007**. Graduate Researcher at University of Salerno, Italy.  
Collaboration with Prof. C. Blundo and Prof. G. Persiano.  
Worked on EU-funded Ecrypt and Aeolus projects; authored several academic publications and deliverables.

## Honors and Grants

- **Dissertation Fellowship**. University of California, Irvine. \$10,000 for 1-quarter support. Fall 2010.  
(Only 2 fellowships awarded per department).

- **Dean's Fellowship.** University of California, Irvine. 4-year PhD financial support. 2007-2011.
- **Travel Grants.** Selected awards for conference attendance: CCS 2011, PETS 2011, WiSec 2011, S&P 2010, Asiacrypt 2010, PETS 2010, ICCCN 2009, PETS 2009, S&P 2008.
- **Summa Cum Laude Honors.** University of Salerno, Italy. Top 1% in graduating class. July 2005.
- **EU Erasmus Scholarship.** University of Portsmouth, UK. September 2004 - March 2005.

## Publications

1. E. De Cristofaro and G. Tsudik.  
"Experimenting with Fast Private Set Intersection".  
To appear in International Conference on Trust and Trustworthy Computing (TRUST), 2012.  
Related (very) preliminary report appears as ePrint Report 2012/054.
2. E. De Cristofaro, C. Soriente, G. Tsudik, A. Williams  
"Hummingbird: Privacy at the time of Twitter".  
To appear in IEEE Symposium on Security and Privacy ("Oakland"), 2012.
3. E. De Cristofaro, C. Soriente.  
"Participatory Privacy: Enabling Privacy in Participatory Sensing".  
To appear in IEEE Network. (Submitted March 2011, Accepted January 2012).
4. M. Almishari, E. De Cristofaro, K. El Defrawy, G. Tsudik.  
"Harvesting SSL Certificate Data to Identify Web-Fraud".  
To appear in the International Journal of Network Security (IJNS).
5. E. De Cristofaro, R. Di Pietro.  
"Preserving Query Privacy in Urban Sensing Systems".  
International Conference on Distributed Computing and Networking (ICDCN), 2012.
6. C. Castelluccia, E. De Cristofaro, A. Francillon, M.A. Kaafar.  
"EphPub: Toward Robust Ephemeral Publishing".  
IEEE Conference on Network Protocols (ICNP), 2011.
7. P. Baldi, R. Baronio, E. De Cristofaro, P. Gasti, G. Tsudik.  
"Countering GATTACA: Efficient and Secure Testing of Fully Sequenced Human Genomes".  
ACM Conference on Computer and Communications Security (CCS), 2011.  
Media Coverage: MIT Technology Review, New Scientist, Kurzweilai.
8. E. De Cristofaro, Y. Lu, G. Tsudik.  
"Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information".  
International Conference on Trust and Trustworthy Computing (TRUST), 2011.
9. E. De Cristofaro, M. Manulis, B. Poettering.  
"Private Discovery of Common Social Contacts".  
International Conference on Applied Cryptography and Network Security (ACNS), 2011.
10. E. De Cristofaro, C. Soriente.  
"PEPSI: Privacy Enhancing Participatory Sensing Infrastructure".  
ACM Conference on Wireless Security (WiSec), 2011.
11. E. De Cristofaro, A. Durussel, I. Aad.  
"Reclaiming Privacy for Smartphone Applications".  
IEEE International Conference on Pervasive Computing and Communications (Percom), 2011
12. G. Ateniese, E. De Cristofaro, G. Tsudik.  
"(If) Size Matters: Size-Hiding Private Set Intersection".  
IACR International Conference on Practice and Theory of Public Key Cryptography (PKC), 2011.
13. E. De Cristofaro, J. Kim, and G. Tsudik.  
"Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model".  
IACR Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt), 2010.

14. E. De Cristofaro and J. Kim.  
 "Some like it private: Sharing Confidential Information based on Oblivious Authorization".  
 IEEE Security and Privacy, July-August, 2010.
15. C. Castelluccia, E. De Cristofaro, and D. Perito.  
 "Private Information Disclosure from Web Searches".  
 Privacy Enhancing Technologies Symposium (PETS), 2010.  
 Also appeared as a poster at IEEE Symposium on Security and Privacy (S&P), 2010.  
 Media Coverage: MIT Technology Review, ACM News, The Register.
16. E. De Cristofaro and G. Tsudik.  
 "Practical Private Set Intersection Protocols with Linear Complexity".  
 Financial Cryptography and Data Security (FC), 2010.
17. V. Auletta, C. Blundo, A. De Caro, E. De Cristofaro, G. Persiano, and I. Visconti.  
 "Increasing Privacy Threats in the Cyberspace: the Case of Italian e-Passports".  
 Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC), 2010.
18. E. De Cristofaro, S. Jarecki, J. Kim, and G. Tsudik.  
 "Privacy-preserving Policy-based Information Transfer".  
 Privacy Enhancing Technologies Symposium (PETS), 2009.
19. E. De Cristofaro, X. Ding, and G. Tsudik.  
 "Privacy-preserving Querying in Sensor Networks".  
 IEEE International Conference on Computer Communications and Networks (ICCCN), 2009.
20. E. De Cristofaro, J.M. Bohli, and D. Westhoff.  
 "FAIR: Fuzzy-based Aggregation providing In-network Resilience for real-time WSNs".  
 ACM Conference on Wireless Network Security (WiSec), 2009.
21. C. Blundo, E. De Cristofaro, A. Del Sorbo, C. Galdi, and G. Persiano.  
 "A Distributed Implementation of the Certified Information Access Service".  
 European Symposium on Research in Computer Security (ESORICS), 2008.
22. C. Blundo, E. De Cristofaro, C. Galdi, and G. Persiano.  
 "Validating Orchestration of Web Services with BPEL and Aggregate Signatures".  
 IEEE European Conference on Web Services (ECOWS) 2008.
23. E. De Cristofaro.  
 "A Secure and Privacy-Protecting Aggregation Scheme for Sensor Networks".  
 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), 2007.
24. V. Auletta, C. Blundo, E. De Cristofaro, S. Cimato, and G. Raimato.  
 "Authenticated Web Services: A WS-Security Based Implementation".  
 IFIP International Conference on New Technologies, Mobility, and Security (NTMS), 2007.
25. C. Blundo and E. De Cristofaro.  
 "A Bluetooth-based JXME infrastructure".  
 International Symposium on Distributed Objects, Middleware, and Applications (DOA), 2007.
26. V. Auletta, C. Blundo, and E. De Cristofaro.  
 "A J2ME transparent middleware to support HTTP connections over Bluetooth".  
 International Conference on Systems and Network Communications (ICSNC), 2007.
27. V. Auletta, C. Blundo, E. De Cristofaro, and G. Raimato.  
 "A lightweight framework for Web Services invocation over Bluetooth".  
 IEEE International Conference on Web Services (ICWS), 2006.
28. V. Auletta, C. Blundo, E. De Cristofaro, and G. Raimato.  
 "Performance Evaluation for Web Services invocation over Bluetooth".  
 ACM Conference on Modeling and Simulation of Wireless and Mobile Systems (MSWiM), 2006.

## Technical Reports

1. E. De Cristofaro, P. Gasti, G. Tsudik.  
“Fast and Private Computation of Set Intersection Cardinality”, ePrint Report 2011/141.

## Invited Talks

- *UC Berkeley*. Hummingbird: #Privacy at the Time of @Twitter. March 2012.
- *Dagstuhl, Germany*. Secure Computing in the Cloud. Invited Speaker. December 2011.
- *Aarhus University, Denmark*. Sharing Sensitive Information with Privacy. June 2011.
- *Microsoft Research, Redmond*. Sharing Sensitive Information with Privacy. March 2011.
- *Singapore Management University*. Sharing Sensitive Information with Privacy. December 2010.
- *UCLA*. Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model. November 2010.
- *Nokia Research Center, Palo Alto*. Sharing Sensitive Information with Privacy. November 2010.
- *EPFL, Lausanne, Switzerland*. Sharing Sensitive Information with Privacy. October 2010.
- *INRIA Rhone Alpes, France*. Reclaiming Privacy for Smartphone Applications. October 2010.
- *ETH, Zurich, Switzerland*. Sharing Sensitive Information with Privacy. September 2010.
- *EPFL, Lausanne, Switzerland*. Protecting Privacy in Wireless Sensor Networks. December 2009.
- *Katholieke Universiteit Leuven*. Privacy-preserving Policy-based Information Transfer. October 2009.

## Teaching Experience

- **Teaching Assistant:** Network Security (University of California, Irvine, 2011), Cryptographic Protocols (University of Salerno, Italy, 2006).
- **Coordinator:** Privacy Reading Group, University of California, Irvine, 2008–2011.
- **Lecturer:** Network Programming, University of Salerno, Italy, 2007.

## Service

- **Program Co-Chair:** HotPETS 2012.
- **Program Committee Member:** ICNC 2013, CANS 2012, CCSW 2012, PETS 2012, WISEC 2012, DPM 2012, ICCCN 2012, TrustCom 2012, CANS 2011, TrustCom 2011, ISC 2010, ICSNC 2010, ICSNC 2009, ICSNC 2008.
- **Reviewer:**
  - Conferences: ESORICS 2012, EUROCRYPT 2012, CODASPY 2012, NDSS 2012, CT-RSA 2012, CCS 2011, ESORICS 2011, ACNS 2011, WiSec 2011, PKC 2011, Secrypt 2011, PERCOM 2010, WISEC 2010, SESOC 2010, ICDCS 2010, CANS 2009, IFIP SEC 2009, ASIACCS 2009, COMPSAC 2009, ICNP 2009, ICNP 2008, MCN 2008, IEEE S&P 2008, OPODIS 2008.
  - Journals: IEEE Transactions on Mobile Computing, IEEE S&P Magazine, Journal of Systems and Software, Ad Hoc Networks, Computing and Informatics, VLDB Journal, Computer Communications.

## Filed Patents

- Method and Apparatus for Preserving Privacy for Appointment Scheduling. Filed February 2011. US Patent.