

Thomas C. Ristenpart

Department of Computer Science and Engineering
University of California San Diego
EBU3B, Room 4242
9500 Gilman Drive, Mail Code 0404
La Jolla, CA 92093-0404, USA

Phone: 858-405-1740
Email: tristenp@cs.ucsd.edu
Web: <http://www.cse.ucsd.edu/~tristenp/>

Education

- 09/2005–present **University of California San Diego**
PhD Student in Computer Science.
Advisor: Professor Mihir Bellare
- 09/2003–08/2005 **University of California Davis**
Masters in Computer Science, 08/2005.
Advisor: Professor Matt Bishop
- 09/1999–07/2003 **University of California Davis**
Bachelors of Science in Computer Science and Engineering GPA: 3.84/4.00

Research areas

Cryptography and computer security

Publications

- Refereed
- [1] M. Bellare, M. Fischlin, A. O’Neill, and T. Ristenpart. Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. *Advances in Cryptology – CRYPTO ‘08*, to appear, 2008.
 - [2] T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno. Privacy-preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs. *USENIX Security ‘08*, to appear, 2008.
 - [3] T. Ristenpart and T. Shrimpton. How to Build a Hash Function from any Collision-Resistant Function. *Advances in Cryptology – ASIACRYPT ‘07*, LNCS vol. 4833, pp. 147–163, 2007.
 - [4] M. Bellare and T. Ristenpart. Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms. *International Colloquium on Automata, Languages, and Programming – ICALP ‘07*, LNCS vol. 4596, pp. 399–410, 2007.
 - [5] T. Ristenpart and S. Yilek. The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks. *Advances in Cryptology – EUROCRYPT ‘07*, LNCS vol. 4515, Springer, pp. 228–245, 2007.

- [6] T. Ristenpart and P. Rogaway. How to Enrich the Message Space of a Cipher. *Fast Software Encryption – FSE ‘07*, LNCS vol. 4593, Springer, pp. 101–118, 2007.
- [7] F. Hsu, H. Chen, T. Ristenpart, J. Lee, and Z. Su. Back to the Future: A Framework for Automatic Malware Removal. In *Proc. of Annual Computer Security Applications Conference*, 2006.
- [8] M. Bellare and T. Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. *Advances in Cryptology – ASIACRYPT ‘06*, LNCS vol. 4284, Springer, pp. 299–314, 2006.
- Manuscripts [9] T. Ristenpart. Insecurity of Tweak Hash Chaining. Unpublished manuscript, 2003.
- Masters thesis [10] T. Ristenpart. Time Stamp Synchronization of Distributed Sensor Logs: Impossibility Results and Approximation Algorithms. UC Davis Masters thesis, September 2005.

Selected talks

- 06/2008 “Design Paradigms for Building Multi-Property Hash Functions”
Lorentz Center Workshop on
Hash Functions in Cryptology: Theory and Practice
- 05/2008 “Privacy-Preserving Location Tracking of Lost or Stolen Devices”
Ecole Polytechnique Fédérale de Lausanne
- 01/2008 “Design Paradigms for Building Multi-Property Hash Functions”
Echternach Symmetric Cryptography Seminar
- 08/2007 “New Approaches for Building Cryptographic Hash Functions”
Microsoft Research
- 05/2007 “New Approaches for Building Cryptographic Hash Functions”
University of Bristol
- 03/2007 “New Approaches for Building Cryptographic Hash Functions”
University of California Davis

Employment history

- 09/2007–present, 09/2005–06/2007 Graduate student researcher, University of California San Diego
- 06/2007–09/2007 Visiting summer researcher, University of Washington
- 09/2003–08/2005, 07/2003–06/2004 Graduate student researcher, University of California Davis
- 06/2004–08/2004 Software security intern, Center for Computing Sciences

06/2002–09/2002, Software development engineering intern, Microsoft
06/2001–09/2001

06/2000–09/2000, Software engineer intern, Micron Technologies, Inc.
06/1999–09/1999

Teaching

Winter 2008 Modern Cryptography (CSE 107) – teaching assistant for undergraduate course
in CSE department, UC San Diego.

Winter 2006 Modern Cryptography (CSE 107) – teaching assistant for undergraduate course
in CSE department, UC San Diego.

Spring 2001 Introduction to Programming and Problem Solving (ECS 30)– undergraduate
teaching assistant for undergraduate course in CS department, UC Davis.

Awards

2001–2003 UC Regents Scholarship
2000 Albert W. Bijou Scholarship
 Edward Frank Kraft Prize
 UC Davis College of Engineering Annual Fund Scholarship
1999 San Francisco Bay Area Engineering Council Scholarship
 Wakeman Scholarship from the UC Regents
 UC Davis Alumni Association Leadership Scholarship

References

Professor Mihir Bellare

Department of Computer Science & Eng.
University of California San Diego

EBU3B, Room 4244
9500 Gilman Drive
La Jolla, CA 92093-0404, USA
858-534-4544
mihir@cs.ucsd.edu

Professor Matt Bishop

Department of Computer Science
University of California Davis

3059 Kemper Hall
One Shields Avenue
Davis, CA 95616
530-752-8060
bishop@cs.ucdavis.edu

Professor Phillip Rogaway

Department of Computer Science
University of California Davis

3063 Kemper Hall
One Shields Avenue
Davis, CA 95616
530-752-7583
rogaway@cs.ucdavis.edu