Foteini Baldimtsi

Curriculum Vitae, February 2014

Contact

Department of Computer Science
Brown University
115 Waterman St., 4th floor
Providence, RI 02912 USA

Cell: (+1) 401-499-6494
e-mail: foteini@cs.brown.edu
www.cs.brown.edu/people/foteini

Research Interests

Cryptography, Privacy, Data security.

Education

05/'11 - now PhD Candidate Computer Science, **Brown University**, USA
Advisor: Anna Lysyanskaya

09/'09 - 05/'11 M.Sc. Computer Science, **Brown University**, USA
Advisor: Anna Lysyanskaya

09/'04 - 06/'08 B.Sc. Applied Informatics , **University of Macedonia**, Greece
Gpa: 8.87/10, Top 1% of class, Advisor: George Stephanides

Awards

- Paris Kanellakis Fellowship, 2010-2011, Spring 2014.
- Gerondelis Foundation Scholarship, 2011-2012.
- Brown University Fellowship, 2009-2010.
- Bodossaki Foundation Scholarship, 2009.
- Greek National Scholarship Foundation Scholaship and Award for academic achievements 2004-2005, 2005-2006 (Rank 1st), Dept. of Applied Informatics, University of Macedonia, Greece.
- Greek National Scholarship Foundation Award for outranking in the Panhellenic Examinations and entering *1st* in the Dept. of Applied Informatics, University of Macedonia, Greece, 2004. (GPA 19.297/ 20.000)
- 3rd award in the "Innovative Ideas" competition organized by the Region of Central Macedonia with the business plan titled "EasySeCrypt - Innovative services for secure web transactions", 2008.
- Travel grants: Ecrypt Summer School on Advanced topics in Cryptography, Greece 2008 · Women in Theory, Princeton, 2010 · Google CS grad forum 2012, San Francisco · HotPETS 2012, Vigo, Spain · 3rd bar-Ilan Winter School in Cryptography (Bilinear Pairings), Tel-Aviv, 2013 · Eurocrypt 2013, Athens, Greece · ACM-CCS 2013, Berlin, Germany · Asiacrypt 2013, Bangalore, India · Real World Crypto 2014, NYC.

Research Experience

09/'09 - now Research Assistant, **Brown University**, Providence, RI, USA
Working with prof. Anna Lysyanskaya on various projects on anonymous credentials, e-cash, blind signature security, group signatures etc. Member of the PAYG project team that investigates security and privacy in Integrated Transportation Payment Systems.

09/'13 - 12/'13 Research Intern, **Microsoft Research**, Redmond, WA, USA
Worked with Melissa Chase on fully anonymous, transferable electronic cash without a judge.

06/'12 - 08/'12 Research Intern, **IBM Research**, Zurich, Switzerland
Worked together with Jan Camenisch, Anja Lehmann and Gregory Neven as a member of the Cryptography and Security team on anonymous credentials.

01/'07 - 08/'09 Research Assistant, **University of Macedonia**, Thessaloniki, Greece
Worked as a student member of the Computational Systems & Software Engineering (CSSE) Lab on key agreement protocols and timed release encryption.

Teaching Experience

Brown University, CS Dept., Providence, RI, USA

Spring 2014 Teaching Assistant, Introduction to Cryptography and Computer Security
Design of homework problems, grading, one-to-one tutoring.

Spring 2013 Teaching Assistant, Introduction to Computer Systems Security
Guest Lectures, design of homework problems, grading, one-to-one tutoring.

Fall 2011 Teaching Assistant, Introduction to Cryptography and Computer Security
Design of homework problems and exams, grading, one-to-one tutoring.

Brown University, Sheridan Teaching Center, Providence, RI, USA

Spring 2013 Certificate I: Sheridan Teaching Seminar - Reflective Teaching

University of Macedonia, Applied Informatics Dept., Thessaloniki, Greece

Spring 2009 Teaching Assistant, Cryptography
Guest Lectures, design of homework problems, grading.

Fall 2008 Teaching Assistant, Introduction to Informatics
Guest Lectures, grading.

Publications

[1] "On the security of One-Witness Blind Signature Schemes", F. Baldimtsi and A. Lysyanskaya, **ASIACRYPT**, 2013.

[2] "Anonymous Credentials Light", F. Baldimtsi and A. Lysyanskaya, **ACM-CCS**, 2013.

[3] "Efficient E-cash in Practice: NFC-based Payments for Intelligent Transportation Systems", G. Hinterwalder, C. T. Zenger, F. Baldimtsi, A. Lysyanskaya, C. Paar and W. P. Burleson, Privacy Enhancing Technologies Symposium (**PETS**), 2013.

[4] "P4R: Privacy-Preserving Pre-Payments with Refunds for Transportation Systems", A. Rupp, G. Hinterwalder, F. Baldimtsi and C. Paar, Financial Cryptography and Data Security (**FC**), 2013.

[5] "Pay as you go", F. Baldimtsi, G. Hinterwalder, A. Rupp, A. Lysyanskaya, C. Paar and W. P. Burleson, Workshop on hot topics in privacy enhancing technologies, **HotPETS** 2012, Vigo, Spain, 2012.

[6] "Two types of Key- Compromise Impersonation Attacks against One- Pass Key- Establishment protocols", K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis and G. Stephanides, In 'E-business and Telecommunication', Volume 23, pp. 227-238, Springer, 2009.

[7] "An Implementation Infrastructure for Server-Passive Timed-Release Cryptography", K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, G. Stephanides, Information Assurance and Security Conference, 2008 (**IAS** '08), IEEE Proceedings, pp.89-94, 2008.

[8] "Mathematical problems and algorithms for timed-release encryption", K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis and G. Stephanides, in Bulletin of the Transilvania University of Brasov, Vol 15(50) Series B - 2008, 1-4, 2008.

[9] "On the Key-Compromise Impersonation vulnerability of One-pass key establishment protocols", K. Chalkias, F. Mpaldimtsi, D. Hristu-Varsakelis and G. Stephanides, In International Conference on Security and Cryptography (**SECRYPT**), 2007.

Manusrcipts

[1] "Efficient and Privacy-Preserving Payments in Transportation Systems: Cryptographic Theory Meets Practice", A. Rupp, F. Baldimtsi, G. Hinterwalder and C. Paar, ACM Transactions on Information and System Security (**TISSEC**) (under review), 2014.

[2] "A Convenient Building Block for Efficient Anonymous Revocation", F. Baldimtsi and A. Lysyanskaya, 2014.

[3] "Anonymous Transferable E-Cash Without a Judge", F. Baldimtsi, M. Chase, G. Fuchsbauer, M. Kolhweiss, 2014

Technical Reports

[1] "Attacks on the AKACP protocol", K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, S. Halkidis and G. Stephanides, IACR Cryptology Eprint Archive, 2010/500, 2010.

Posters

[1] "Pay-As-You-Go: E-cash for Intelligent Public Transporation", New York Computer Science and Economics Day (NYCE), December 2012.

[2] "Security and Privacy for integrated Transportation Payment Systems", Google Grad CS Forum, January 2012.

Invited Talks

"Lightweight Credentials, E-cash with attributes and an Application to Public Transit Systems"

- MSR Privacy Workshop, Redmond, October 2013.

"Anonymous Credentials Light"

- Crypto Group, Microsoft Research, Redmond, October 2013.
- Athens Cryptography Day, NTUA, January 2013.

"On the security of One-Witness Blind Signature Schemes"

- Crypto Group, Microsoft Research, Redmond, November 2013.
- Ruhr Universität Bochum, Germany, July 2012.
- IBM Research Zurich, June 2012.
- Cryptography Seminar at UCSD, January 2012.
- X-Theory Day, University of Athens, December 2011.

Professional Activities

- External Reviewer: Asiacrypt 2013, Eurocrypt 2012, TCC 2011, CT-RSA 2011.
- Volunteer: Eurocrypt 2013 (web site, registration), TCC 2011 (registration, local arrangements).
- Dec. 2013 - Jan. 2014: Student member of PhD Admissions Committee, Brown University, Department of Computer Science.
- Oct. 2013 - now: CS Blog Merc, Organizing the department's blog, Brown University, Department of Computer Science.
- Sep. 2009 - now: Organizer of the Cryptography Group Meetings, Brown University, Department of Computer Science.
- Sep. 2009 - Feb. 2012: Communications Officer of the Hellenic Students Association (HSA) at Brown University.

Memberships

2008 - now: International Association for Cryptologic Research (IACR).
2010 - now: Greek Association of Computing Professionals.