Curriculum Vitae

Ali Aydın Selçuk

Department of Computer Engineering
Bilkent University, Ankara, 06800, Turkey
E-mail: selcuk@cs.bilkent.edu.tr
URL: http://www.cs.bilkent.edu.tr/∼selcuk/

Personal Data

- Date of birth: 1971
- Place of birth: Ankara, Turkey
- Citizenship: Turkey
- Marital status: Married

Research Interests

Network security, cryptography, protocol security analysis, block cipher cryptanalysis, wireless protocol security, P2P security, group key management, security of medical information systems, mobile ad hoc networks, data compression.

Educational Background

- Ph.D., Computer Science, University of Maryland, Baltimore County, Baltimore, Maryland, USA, 2001. Thesis Title: *Probabilistic Optimization Techniques for Multicast Key Management and Bias Estimation in Linear Cryptanalysis.* Thesis Advisor: Dr. Deepinder Sidhu.
- M.S., Industrial Engineering, Bilkent University, Ankara, Turkey, 1995. Thesis title: *Word-Based Compression in Full-Text Retrieval Systems.* Thesis advisor: Dr. Akif Eyler.
- B.S., Industrial Engineering, Middle East Technical University, Ankara, Turkey, 1993.
- H.S. Diploma, Ankara High School of Science, Ankara, Turkey, 1989.

Work Experience

- 2002–Present. Assistant Professor. Department of Computer Engineering, Bilkent University, Ankara, Turkey.
- 2001–2002. Postdoctoral Research Fellow. Department of Computer Sciences, Purdue University, West Lafayette, IN.
- 1997–2001. Research Assistant. Maryland Center for Telecommunications Research, and the Department of Computer Science, University of Maryland, Baltimore County, Baltimore, MD.
- 2000. Intern. Novell, Inc., Provo, Utah.
- 1997. Intern. RSA Laboratories, RSA Data Security Inc., Redwood City, CA.
- 1995–1997. Teaching Assistant. Department of Computer Science, University of Maryland, Baltimore County, Baltimore, MD.
- 1993–1995. Teaching Assistant. Department of Industrial Engineering, Bilkent University, Ankara, Turkey.

Professional Activities

- Program co-chair, *LightSec 2011*, Istanbul Turkey, 2011.
- Program committee member, *4th International Conference on Information Security and Cryptology (ISC-Turkey 2010)*, Ankara, Turkey, 2010.
- Program committee member, *Africacrypt 2009*, Gammarth, Tunisia, 2009.
- Program committee member, *3rd International Conference on Information Security and Cryptology (ISC-Turkey 2008)*, Ankara, Turkey, 2008.
- Program committee member, *Africacrypt 2008*, Casablanca, Morocco, 2008.
- Program committee member, *The 22nd International Symposium on Computer and Information Sciences (ISCIS'07)*, Istanbul, Turkey, 2007.
- Program committee member, *Second National Cryptology Symposium*, Ankara, Turkey, 2006.
- Program committee member, *The 21st International Symposium on Computer and Information Sciences (ISCIS'06)*, Istanbul, Turkey, 2006.
- Program committee member, *IEEE WETICE'06–Workshop on Security Technologies*, Manchester, England, 2006.
- Program committee member, *IEEE International Conference on Wireless Networks, Communications, and Mobile Computing (WirelessCom'05)–Symposium on Mobile Computing*, Maui, Hawaii, 2005.
- Program committee member, *First National Cryptology Symposium*, Ankara, Turkey, 2005.
- Program committee member, *The 19th International Symposium on Computer and Information Sciences (ISCIS'04)*, Antalya, Turkey, 2004.
- Consultant, *TUBITAK-UEKAE*, 2003–2005, 2006–2007, 2008–2010.
- Consultant, *Banking Regulation and Supervision Agency (BDDK)*, 2003-2004.

Journal Publications

- M. Ak, K. Kaya, K. Onarlıoğlu, A. A. Selçuk, "Efficient Broadcast Encryption with User Profiles," *Information Sciences*, 180 (6), pages 1060-1072, March 2010.
- M. Ak, K. Kaya, A. A. Selçuk, "Optimal Subset-Difference Broadcast Encryption with Free Riders," *Information Sciences*, 179 (20), pages 3673-13684, September 2009.
- A. A. Selçuk, E. Uzun, M. R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," *Int. Journal of Network Security*, 6 (2), pages 227-237, March 2008.
- A. A. Selçuk, "On Probability of Success in Linear and Differential Cryptanalysis," *Journal of Cryptology*, 21 (1), pages 131-147, January 2008.
- K. Kaya, A. A. Selçuk, "Threshold Cryptography Based on Asmuth-Bloom Secret Sharing," *Information Sciences*, 177 (19), pages 4148-4160, October 2007.
- A. A. Selçuk, D. Sidhu, "Probabilistic Optimization Techniques for Multicast Key Management," *Computer Networks*, 40 (2), pages 219-234, October 2002.

Conference Publications

- A. A. Selçuk, R. Yılmaz "Linear Hierarchical Secret Sharing," *Information Security and Cryptology*, Ankara, Turkey, May 2010.

- I. N. Bozkurt, K. Kaya, A. A. Selçuk, "Secret Sharing for General Access Structures," *Information Security and Cryptology*, Ankara, Turkey, May 2010.
- I. N. Bozkurt, K. Kaya, A. A. Selçuk, "Practical Threshold Signatures with Linear Secret Sharing," *Africacrypt 2009*, Lecture Notes in Computer Science, Springer-Verlag. Gammarth, Tunisia, June 2009.
- I. N. Bozkurt, K. Kaya, A. A. Selçuk, A. M. Güloğlu, "Threshold Cryptography Based on Blakley Secret Sharing," *Information Security and Cryptology*, Ankara, Turkey, December 2008.
- H. Koyuncu, K. Kaya, A. A. Selçuk, "An Analysis of the Generalized ID-Based ElGamal Signatures," *Information Security and Cryptology*, Ankara, Turkey, December 2008.
- S. Kalkan, K. Kaya, A. A. Selçuk, "Generalized ID-Based Blind Signatures From Bilinear Pairings," *The 23rd International Symposium on Computer and Information Sciences (ISCIS 2008)*, Istanbul, Turkey, October 2008.
- K. Kaya, A. A. Selçuk, "Robust Threshold Schemes Based on the Chinese Remainder Theorem," *Africacrypt 2008*, Lecture Notes in Computer Science, Springer-Verlag. Casablanca, Morocco, June 2008.
- K. Kaya, B. G. Dündar, S. Kalkan, A. A. Selçuk, "Threshold Paillier and Naccache-Stern Cryptosystems Based on Asmuth-Bloom Secret Sharing," *2nd National Cryptology Symposium*, Ankara, Turkey, December 2006.
- H. Demirci, S. Ayaz, A. A. Selçuk, "Similar State Tables and Related Keys in RC4," *2nd National Cryptology Symposium*, Ankara, Turkey, December 2006.
- K. Kaya, A. A. Selçuk, Z. Tezcan, "Threshold Cryptography Based on Asmuth-Bloom Secret Sharing," *The 21st International Symposium on Computer and Information Sciences (ISCIS 2006)*, Lecture Notes in Computer Science, Springer-Verlag. Istanbul, Turkey, November 2006.
- H. Acan, K. Kaya, A. A. Selçuk, "Capture Resilient ElGamal Signature Protocols," *The 21st International Symposium on Computer and Information Sciences (ISCIS 2006)*, Lecture Notes in Computer Science, Springer-Verlag. Istanbul, Turkey, November 2006.
- S. Ayaz, A. A. Selçuk, "Improved DST Cryptanalysis of IDEA," *13th Annual Workshop on Selected Areas in Cryptography (SAC 2006)*, Lecture Notes in Computer Science, Springer-Verlag. Montreal, Canada, August 2006.
- M. Ak, K. Kaya, A. A. Selçuk, Z. Tezcan, "Experiments on Probability of Success in Linear and Differential Cryptanalysis," *First National Cryptology Symposium*, Ankara, Turkey, November 2005.
- Ö. Aydemir, A. A. Selçuk, "A Strong User Authentication Protocol for GSM," *14th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE'05)*, Linköping, Sweden, June 2005.
- A. A. Selçuk, E. Uzun, M. R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," *4th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid 2004)*, Chicago, USA, April 2004.
- H. Demirci, A. A. Selçuk, E. Türe, "A New Meet in the Middle Attack on The IDEA Block Cipher," *Tenth Annual Workshop on Selected Areas in Cryptography (SAC 2003).* Lecture Notes in Computer Science v.3006, pages 117-129, Springer-Verlag. Ottowa, Canada, August 2003.

- Y. Zhang, A. Rangnekar, A. A. Selçuk, A. Bıçak, D. Sidhu, "Comparison of Zone-Based Multicast Routing Protocols for Ad Hoc Networks," *11th IEEE International Conference on Networks (ICON 2003)*, Sydney, Australia, September 2003.
- A. Rangnekar, Y. Zhang, A. A. Selçuk, A. Bıçak, V. Devarapalli, D. Sidhu, "A Zone-Based Shared-Tree Multicast Routing Protocol for Mobile Ad Hoc Networks," *IEEE Semiannual Vehicular Technology Conference (VTC2003-Fall)*, Orlando, USA, October 2003.
- A. A. Selçuk, A. Bıçak, "On Probability of Success in Linear and Differential Cryptanalysis," *Third Conference on Security in Communication Networks (SCN'02).* Lecture Notes in Computer Science v.2576, pages 177-188, Springer-Verlag. Amalfi, Italy, September 2002.
- A. A. Selçuk, D. Sidhu, "Probabilistic Methods in Multicast Key Management," *Information Security Workshop 2000.* Lecture Notes in Computer Science v.1975, pages 179-193, Springer-Verlag. Wollongong, Australia, December 2000.
- A. A. Selçuk, "On Bias Estimation in Linear Cryptanalysis," *Indocrypt 2000 Conference.* Lecture Notes in Computer Science v.1977, pages 52-66, Springer-Verlag. Calcutta, India, December 2000.
- C. McCubbin, A. A. Selçuk, D. Sidhu, "Initialization Vector Attacks on the IPsec Protocol Suite," *5th IEEE International Workshop on Enterprise Security* (in *WETICE'00*). Gaithersburg, Maryland, June 2000.
- A. A. Selçuk, "New Results in Linear Cryptanalysis of RC5," *5th Fast Software Encryption Conference.* Lecture Notes in Computer Science v.1372, pages 1-16, Springer-Verlag. Paris, France, March 1998.

Internet Drafts

- A. A. Selçuk, C. McCubbin, D. Sidhu. *Probabilistic Optimization of LKH-based Multicast Key Distribution Schemes.* draft-selcuk-probabilistic-lkh-01.txt, January 2001.
- V. Devarapalli, A. A. Selçuk, D. Sidhu. *MZR: A Multicast Protocol for Mobile Ad Hoc Networks.* draft-vijay-manet-mzr-00.txt, November 2000.

Awards & Achievements

- June 2008, Distinguished Teaching Award, Bilkent University.
- September 1995–May 1996, $2000, Graduate Merit Award, University of Maryland, Baltimore County.
- October 1989–July 1993, Middle East Technical University Fellowship.
- August 1989, Türkiye İş Bankası Award, in recognition of the success in the National University Entrance Examination (Was placed 49th among 770,000 participants).

Professional Memberships

- International Association for Cryptologic Research
- Institute of Electrical and Electronics Engineers, Computer Society

Hobbies

History, music, volleyball.