CURRICULUM VITAE

Prof. Dr. Ali Aydın Selçuk

PERSONAL DATA

Date & Place of Birth: 1971, Ankara, Turkey
Address: Department of Computer Engineering
TOBB University of Economy and Technology
06560, Ankara, Turkey
Phone: +90 312 292 4382
Fax: +90 312 292 4178
E-mail: aliaydinselcuk@gmail.com

ACADEMIC DEGREES

Ph.D., Computer Science, University of Maryland Baltimore County, 2001.

M.S., Industrial Engineering, Bilkent University, 1995.

B.S., Industrial Engineering, Middle East Technical University, 1993.

EMPLOYMENT HISTORY

05/2014 – Present, Professor, TOBB University of Economy and Technology, Department of Computer Engineering.

09/2013 – 05/2014, Associate Professor, TOBB University of Economy and Technology, Department of Computer Engineering.

09/2002 – 08/2013, Assistant Professor, Bilkent University, Department of Computer Engineering.

09/2001 – 09/2002, Postdoctoral Research Associate, Purdue University, Department of Computer Sciences.

09/1995 – 06/2001, Graduate Assistant, University of Maryland, Baltimore County, Department of Computer Science.

06/2000 – 08/2000, Intern, Novell, Network Security Group.

06/1997 – 08/1997, Intern, RSA Data Security Inc., RSA Laboratories.

09/1993 – 08/1995, Teaching Assistant, Bilkent University, Department of Industrial Engineering.

PROFESSIONAL AWARDS

- Distinguished Teaching Award, Bilkent University, 2008.
- Graduate Merit Award, University of Maryland Baltimore County, 1995-96.

SCHOLARLY PUBLICATIONS

Ph.D. Dissertation:

"Probabilistic Optimization Techniques for Multicast Key Management and Bias Estimation in Linear Cryptanalysis," June 2001, Dr. Deepinder Sidhu, University of Maryland Baltimore County.

Articles in Refereed Journals:

- "Server Notaries: A Complementary Approach to the Web PKI Trust Model." *IET Information Security*, 12 (5), pages 455-461, September 2018. E. Yüce, A. A. Selçuk:
- "Distributed Multi-Unit Privacy Assured Bidding (PAB) for Smart Grid Demand Response Programs." *IEEE Transactions on Smart Grid*, 9 (5), pages 4119-412, September 2018. M. F. Ballı, S. Uludağ, A. A. Selçuk, B. Tavlı.
- "Intractable Problems in Malware Analysis and Practical Solutions." *Journal of Internet Technology and Secured Transactions*, 6 (2), pages 588-595, June 2018. A. A. Selçuk, F. Orhan, B. Batur.
- "A CRT-Based Verifiable Secret Sharing Scheme Secure Against Unbounded Adversaries." *Security and Communication Networks*, 9 (17), pages 4416-4427, November 2016. O. Ersoy, T. B. Pedersen, K. Kaya, A. A. Selçuk, E. Anarım.
- "Improved Improbable Differential Attacks on ISO Standard CLEFIA: Expansion Technique Revisited." *Information Processing Letters*, 116 (2), pages 136-143, February 2016. C. Tezcan, A. A. Selçuk.
- "The Cloaked-Centroid Protocol: Location Privacy Protection for a Group of Users of Location-Based Services." *Knowledge and Information Systems*, 45 (3), pages 589-615, December 2015. M. Ashouri-Talouki, A. Baraani-Dastjerdi, A. A. Selçuk.
- "Punctured Interval Broadcast Encryption Scheme with Free Riders." *Information Sciences*, 305, pages 285-301, June 2015. M. Ak, A. A. Selçuk.
- "IND-CCA Secure Encryption Based on Zheng-Seberry Scheme." *Journal of Computational and Applied Mathematics*, 259, pages 529-535, March 2014. M. Ak, T. Hanoymak, A. A. Selçuk.
- "Anonymous Trace and Revoke." *Journal of Computational and Applied Mathematics*, 259, pages 586-591, March 2014. M. Ak, S. Pehlivanoğlu, A. A. Selçuk.
- "Sharing DSS by the Chinese Remainder Theorem." *Journal of Computational and Applied Mathematics*, 259, pages 495-502, March 2014. K. Kaya, A. A. Selçuk.
- "Preserving Location Privacy for a Group of Users." *Turkish Journal of Electrical Engineering and Computer Sciences*, 21, pages 1857-1870, October 2013. M. Ashouri-Talouki, A. Baraani-Dastjerdi, A. A. Selçuk.

- "GLP: A cryptographic approach for group location privacy." *Computer Communications*, 35 (12), pages 1527-1533, July 2012. M. Ashouri-Talouki, A. Baraani-Dastjerdi, A. A. Selçuk.
- "Efficient Broadcast Encryption with User Profiles." *Information Sciences*, 180 (6), pages 1060-1072, March 2010. M. Ak, K. Kaya, K. Onarlıoğlu, A. A. Selçuk.
- "Optimal Subset-Difference Broadcast Encryption with Free Riders." *Information Sciences*, 179 (20), pages 3673-3684, September 2009. M. Ak, K. Kaya, A. A. Selçuk.
- "A Reputation-Based Trust Management System for P2P Networks." *International Journal of Network Security*, 6 (2), pages 227-237, March 2008. A. A. Selçuk, E. Uzun, M. R. Pariente.
- "On Probability of Success in Linear and Differential Cryptanalysis." *Journal of Cryptology*, 21 (1), pages 131-147, January 2008. A. A. Selçuk.
- "Threshold Cryptography Based on Asmuth-Bloom Secret Sharing." *Information Sciences*, 177 (19), pages 4148-4160, October 2007. K. Kaya, A. A. Selçuk.
- "Probabilistic Optimization Techniques for Multicast Key Management." *Computer Networks*, 40 (2), pages 219-234, October 2002. A. A. Selçuk, D. Sidhu.

Refereed Proceedings (International):

- "An Analysis DRDoS Amplifiers in Europe." *ICONCS 2018: International Conference on Cyber Security and Computer Science*. E. M. Ercan, A. A. Selçuk.
- "Undecidable problems in malware analysis." *ICITST 2017: International Conference for Internet Technology and Secured Transactions*. A. A. Selçuk, F. Orhan, B. Batur.
- "Privacy-Guaranteeing Bidding in Smart Grid Demand Response Programs." *IEEE Globecom 2015 Workshop on SmartGrid Resilience (SGR)*. S. Uludağ, M. F. Ballı, A. A. Selçuk, B. Tavlı.
- "Trusting SSL in practice." *Security in Information Networks, 2013*. A. A. Selçuk.
- "Generic Trace and Revoke Scheme." *ICACM 2012: International Conference on Applied and Computational Mathematics*. M. Ak, A. Kiayias, S. Pehlivanoğlu, A. A. Selçuk.
- "Joint Compartmented Threshold Access Structures." *ICACM 2012: International Conference on Applied and Computational Mathematics*. A. A. Selçuk, R. Yılmaz.
- "Sharing DSS by the Chinese Remainder Theorem." *ICACM 2012: International Conference on Applied and Computational Mathematics*. K. Kaya, A. A. Selçuk.
- "Practical Threshold Signatures with Linear Secret Sharing." *Africacrypt 2009: Second International Conference on Cryptology in Africa*. LNCS v.5580, Springer-Verlag. İ. N. Bozkurt, K. Kaya, A. A. Selçuk.
- "A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem." *Indocrypt 2008: 9th International Conference on Cryptology in India*. LNCS v.5365, Springer-Verlag. K. Kaya, A. A. Selçuk.
- "Generalized ID-Based Blind Signatures From Bilinear Pairings." *ISCIS 2008*. S. Kalkan, K. Kaya, A. A. Selçuk.
- "Robust Threshold Schemes Based on the Chinese Remainder Theorem." *Africacrypt 2008: First International Conference on Cryptology in Africa*. LNCS v.5023, Springer-Verlag. K. Kaya, A. A. Selçuk.
- "A Meet-in-the-Middle Attack on 8-Round AES." *FSE 2008: 15th Fast Software Encryption Conference*. LNCS v.5086, Springer-Verlag. H. Demirci, A. A. Selçuk.

- “Generalized ID-Based ElGamal Signatures.” *ISCIS 2007*. S. Kalkan, K. Kaya, A. A. Selçuk.
- “Threshold Broadcast Encryption With Reduced Complexity.” *ISCIS 2007*. K. Kaşkaloğlu, K. Kaya, A. A. Selçuk.
- “Threshold Cryptography Based on Asmuth-Bloom Secret Sharing.” *ISCIS 2006*. LNCS v.4263, Springer-Verlag. K. Kaya, A. A. Selçuk, Z. Tezcan.
- “Capture Resilient ElGamal Signature Protocols.” *ISCIS 2006*. LNCS v.4263, Springer-Verlag. H. Acan, K. Kaya, A. A. Selçuk.
- “Improved DST Cryptanalysis of IDEA.” *SAC 2006: 13th Annual Workshop on Selected Areas in Cryptography*. LNCS v.4356, Springer-Verlag. E. S. Ayaz, A. A. Selçuk.
- “A Strong User Authentication Protocol for GSM.” *WETICE'05: 14th IEEE International Workshops on Enabling Technologies*. Ö. Aydemir, A. A. Selçuk.
- “ A Reputation-Based Trust Management System for P2P Networks.” *CCGrid 2004: 4th IEEE/ACM International Symposium on Cluster Computing and the Grid*. A. A. Selçuk, E. Uzun, M. R. Pariente.
- “A Zone-Based Shared-Tree Multicast Routing Protocol for Mobile Ad Hoc Networks.” *VTC2003-Fall: IEEE Semiannual Vehicular Technology Conference*. A. Rangnekar, Y. Zhang, A. A. Selçuk, A. Bıçak, V. Devarapalli, D. Sidhu.
- “Comparison of Zone-Based Multicast Routing Protocols for Ad Hoc Networks.” *ICON 2003: 11th IEEE International Conference on Networks*. Y. Zhang, A. Rangnekar, A. A. Selçuk, A. Bıçak, D. Sidhu.
- “A New Meet in the Middle Attack on The IDEA Block Cipher.” *SAC 2003: Tenth Annual Workshop on Selected Areas in Cryptography*. LNCS v.3006, Springer-Verlag. H. Demirci, A. A. Selçuk, E. Türe.
- “On Probability of Success in Linear and Differential Cryptanalysis.” *SCN'02: Third Conference on Security in Communication Networks*. LNCS v.2576, Springer-Verlag. A. A. Selçuk, A. Bıçak.
- “Probabilistic Methods in Multicast Key Management.” *Information Security: Third International Workshop, ISW 2000*. LNCS v.1975, pages 179-193, Springer-Verlag. A. A. Selçuk, D. Sidhu.
- “On Bias Estimation in Linear Cryptanalysis.” *Indocrypt 2000: First International Conference in Cryptology in India*. LNCS v.1977, Springer-Verlag. A. A. Selçuk.
- “Initialization Vector Attacks on the IPsec Protocol Suite.” *WETICE'00: 9th IEEE International Workshops on Enabling Technologies*. C. McCubbin, A. A. Selçuk, D. Sidhu.
- “New Results in Linear Cryptanalysis of RC5.” *FSE 1998: 5th Fast Software Encryption Conference*. LNCS v.1372, Springer-Verlag. A. A. Selçuk.

Refereed Proceedings (National):

- “Atlamalı Aralık Yayın Şifrelemesinde Bedava Alıcıların İyi Yerleştirilmesi.” *ABGS 2011*. M. Ak, A. A. Selçuk.
- “Linear Hierarchical Secret Sharing.” *ISC-TURKEY 2010: Information Security and Cryptology*. A. A. Selçuk, R. Yılmaz.
- “Secret Sharing for General Access Structures.” *ISC-TURKEY 2010: Information Security and Cryptology*. İ. N. Bozkurt, K. Kaya, A. A. Selçuk.
- “Threshold Cryptography Based on Blakley Secret Sharing.” *ISC-TURKEY 2008: Information Security and Cryptology*. İ. N. Bozkurt, K. Kaya, A. A. Selçuk, A. M. Güloğlu.

- "An Analysis of the Generalized ID-Based ElGamal Signatures." *ISC-TURKEY 2008: Information Security and Cryptology*. H. Koyuncu, K. Kaya, A. A. Selçuk.
- "Generalized ID-Based ElGamal Signatures with Message Recovery." *ISC-TURKEY 2007: Information Security and Cryptology*. S. Kalkan, K. Kaya, A. A. Selçuk.
- "Threshold Paillier and Naccache-Stern Cryptosystems Based on Asmuth-Bloom Secret Sharing." *2nd National Cryptology Symposium*. K. Kaya, B. G. Dündar, S. Kalkan, A. A. Selçuk.
- "Similar State Tables and Related Keys in RC4." *2nd National Cryptology Symposium*. H. Demirci, E. S. Ayaz, A. A. Selçuk.
- "Experiments on Probability of Success in Linear and Differential Cryptanalysis." *First National Cryptology Symposium*. M. Ak, K. Kaya, A. A. Selçuk, Z. Tezcan.

SCHOLARLY AND PROFESSIONAL DUTIES

- Program co-chair for *LightSec 2011: Workshop on Lightweight Security & Privacy*.

- Referee for the following journals:
  1. IEEE Trans. on Information Theory
  2. IEEE Trans. on Wireless Communications
  3. Designs, Codes and Cryptography
  4. International Journal of Network Security
  5. Cryptologia
  6. Turkish Journal of Electrical Engineering and Computer Sciences
  7. TBV Bilgisayar Bilimleri ve Mühendisliği Dergisi

- Technical program committee member for the following international conferences/workshops:
  1. CT-RSA 2015: RSA Conference 2015–Cryptographers' Track. San Fransisco, USA, 2015.
  2. BalkanCryptSec 2014: International Conference on Cryptography and Information Security. Istanbul, Turkey, 2014.
  3. LightSec 2014: Third International Workshop on Lightweight Cryptography for Security & Privacy. Istanbul, Turkey, 2014.
  4. SIN 2013: The 6th International Conference on Security of Information and Networks. Aksaray, Turkey, 2013.
  5. LightSec 2013: Workshop on Lightweight Security & Privacy. Gebze, Turkey, 2013.
  6. ICACM: International Conference on Applied and Computational Mathematics. Ankara, Turkey, 2012.
  7. LightSec 2011: Workshop on Lightweight Security & Privacy. Istanbul, Turkey, 2011.
  8. ISCIS'09: The 24th International Symposium on Computer and Information Sciences. Famagusta, Cyprus, 2009.
  9. Africacypt 2009: Second African International Conference on Cryptology. Gammarth, Tunisia, 2009.
  10. Africacypt 2008: First African International Conference on Cryptology. Casablanca, Morocco, 2008.

11. ISCIS'07: The 22nd International Symposium on Computer and Information Sciences. Ankara, Turkey, 2007.
12. ISCIS'06: The 21st International Symposium on Computer and Information Sciences. Istanbul, Turkey, 2006.
13. WETICE'06: 15th IEEE International Workshops on Enabling Technologies. Manchester, UK, 2006.
14. IEEE WirelessCom'05: Symposium on Mobile Computing. Maui, Hawaii, 2005.

- Technical program committee member for the following national conferences/workshops:
  1. ISC-Turkey 2016: 9th Information Security and Cryptology Conference. Ankara, Turkey, 2016.
  2. ISC-Turkey 2015: 8th Information Security and Cryptology Conference. Ankara, Turkey, 2015.
  3. ISC-Turkey 2014:7th Information Security and Cryptology Conference. Istanbul, Turkey, 2014.
  4. ISC-Turkey 2013: 6th Information Security and Cryptology Conference. Ankara, Turkey, 2013.
  5. ISC-Turkey 2012: 5th Information Security and Cryptology Conference. Ankara, Turkey, 2012.
  6. IPv6 Conference. Ankara, Turkey, 2011.
  7. ISC-Turkey 2010: 4th Information Security and Cryptology Conference. Ankara, Turkey, 2010.
  8. ISC-Turkey 2008: 3rd Information Security and Cryptology Conference. Ankara, Turkey, 2008.
  9. Second National Cryptology Symposium. Ankara, Turkey, 2006.
  10. First National Cryptology Symposium. Ankara, Turkey, 2006.

INVITED LECTURES AND INVITED TALKS

- "Trusting SSL in Practice," Department of Computer Engineering, Karadeniz Technical University, January 2017.
- "Trusting SSL in Practice," Department of Computer Engineering, Fırat University, April 2015.
- "Trusting SSL in Practice," Department of Computer Science, Kuwait University, December 2014.
- "Trusting SSL in Practice," Department of Computer Engineering, Koç University, October 2014.
- "Trusting SSL in Practice," keynote address, in *SIN 2013: The 6th Int. Conf. on Security of Information and Networks*, Aksaray, Turkey, November 2013.
- "SSL Security & Trust," invited lecture, in *CryptoDays*, Gebze, Turkey, June 2013.
- "Fundamentals of Cryptographic Protocols," Technical University of Berlin, Berlin, Germany, May 2013.
- "Cryptography and Internet Security," Technical University of Berlin, Berlin, Germany, May 2013.
- "SSL Security & Trust," Technical University of Berlin, Berlin, Germany, May 2013.

- "Threshold Cryptography with Linear Secret Sharing Schemes," Department of Mathematics, TOBB ETU, March 2011.
- "Practical Threshold Signatures with Linear Secret Sharing Schemes," Faculty of Computing, Kingston University, UK, September 2010.
- "Threshold Cryptography based on the Chinese Remainder Theorem," Faculty of Computing, Kingston University, UK, September 2010.
- "An Introduction to Cryptography and Cryptological Problems," Dept. of Industrial Engineering, METU, May 2009.
- "Threshold Cryptography," UEKAE, TUBITAK, November 2008.
- "ID-Based Encryption and Signatures," UEKAE, TUBITAK, November 2007.
- "Threshold Cryptography with Asmuth-Bloom Secret Sharing," Inst. of Applied Mathematics, METU, May 2006.
- "Cryptography," Dept. of Mathematics, Hacettepe University, April 2005.
- "Threshold Cryptography," Dept. of Computer Engineering, Galatasaray University, May 2005.
- "IPsec and Protocol Cryptanalysis," Dept. of Computer Engineering, Galatasaray University, May 2005.
- "Differential and Linear Cryptanalysis of Block Ciphers," Informatics Institute, METU, May 2004.
- "Reputation-Based Trust Management in P2P Networks," Dept. of Computer Sciences, Purdue University, April 2004.
- "A New Meet-in-the-Middle Attack on the IDEA Block Cipher," Inst. of Applied Mathematics, METU, October 2003.
- "Security of Cryptographic Protocols," UEKAE, TUBITAK, June 2003.
- "Applications of Cryptography in Computer Science," Inst. of Applied Mathematics, METU, April 2003.
- "Protocol Cryptanalysis and IPsec," Faculty of Engineering and Natural Sciences, Sabanci University, March 2003.
- "Probabilistic Optimization Techniques for Multicast Key Management," Dept. of Computer Science, University of Texas at San Antonio, April 2002.
- "Probabilistic Optimization Techniques for Multicast Key Management," Dept. of Computer Sciences, Purdue University, May 2001.
- "New Results in Linear Cryptanalysis of RC5," T.J.Watson Research Center, IBM, July 1998.

GRADUATE STUDENT SUPERVISION

Ph.D. Students:

- Emre Yüce, "Server Notaries: A Complementary Approach to the Web PKI Trust Model," 01/2016. (co-supervisor)
- Murat Ak, "Optimization Techniques and New Methods for Broadcast Encryption and Traitor Tracing Schemes," 01/2013.
- Turgut Hanoymak, "On Provable Security of Some Public Key Encryption Schemes," 09/2012. (co-supervisor)
- Kamer Kaya, "Threshold Cryptography with Chinese Remainder Theorem," 07/2009.

M.S. Students:

- Hakan Kılıç, "Evasion Techniques' Efficiency over Intrusion Prevention and Detection Technologies" , 08/2019.
- Mevlüt Serkan Tok, "IoT Botnets: A Case Study on Mirai Malware", 08/2019.
- Osman Tufan Tekin, "Anti-Virtualization Techniques Used by Malware and Measures That Can Be Taken Against Them", 12/2018.
- Emre Murat Ercan, "An Analysis of DRDoS Amplifiers in Turkey and Europe", 08/2018.
- Yunus Çağrı Yurdakul, "A Technical Analysis of Proof of Stake Based Blockchain Systems", 08/2018.
- Gamze Akman, "User Interaction with Change of Authentication and Encryption Key in Popular Instant Messaging Applications", 04/2018.
- Hasan Hüseyin Subaşı, "Development of Integrated And Hybrid TSM Model For the New Generation Cash Registers," 12/2016.
- Erhan Turan, "Designing Pades Test Suite and Testing Adobe Reader Signature Mechanisms," 04/2015.
- Serkan Sarıtaş, "Analysis of Android Random Number Generator," 05/2013.
- Satiye Albakır, "Random Delay Techniques for Location Privacy in VANETs," 05/2013.
- Bahar Berna Akkoç, "OpenID with Certificate-Based User Authentication on Smartcard," 05/2013.
- Utku Ozan Yılmaz, "Insights Into User Behavior in Dealing with Common Internet Attacks," 08/2011.
- Ramazan Yılmaz, "Some Ideal Secret Sharing Schemes," 08/2010.
- Kaan Onarlıoğlu, "Immunizing Binary Executables Against Return-Oriented Programming," 07/2010.
- İlker Nadi Bozkurt, "Function and Secret Sharing Extensions for Blakley and Asmuth-Bloom Secret Sharing Schemes," 08/2009.
- Ömer Sezgin Uğurlu, "Stealth Sandbox Analysis of Malware," 08/2009.
- Leyla Bilge, " Generating Content-Based Signatures for Detecting Bot-Infected Machines," 07/2008.
- Said Kalkan, "Generalized ID-based ElGamal Signatures and Extentions," 07/2008.
- Murat Ak, "Optimal Broadcast Encryption with Free Riders," 09/2006.
- Cumhur Doruk Bozağaç, "Ghostware and Rootkit Detection Techniques for Windows," 09/2006.
- Özer Aydemir, "GUAP: A Strong User Authentication Protocol for GSM," 01/2005.

GRANTS

As Principal Investigator:

- "Secret Sharing Schemes and Extensions Based on the Chinese Remainder Theorem," TÜBİTAK project no. 108E150, 112,000 TL, 10/2008 – 10/2010.
- "Development of Trace and Revoke Systems based on Broadcast Encryption," TÜBİTAK project no. 111E213, 82,600 TL, 03/2012 – 03/2013.

As Researcher:

- "BTT-Türkiye: New Information Society Technologies for Turkey," TÜBİTAK project no. 105E065, 550,000 YTL, 12/2005 – 12/2008.
- "Bluetooth Scatternet Construction and Bluetooth Applications," TÜBİTAK project no. 103E014, 9,048 MTL, 09/2003 – 09/2005.

CONTRIBUTION TO SOCIETY AT LARGE

Guest lectures given at different institutions:

- "Cryptographic Protocols," TÜBİTAK Cryptology Summer School, September 2016.
- "Cryptography and Communications Security," ACM Student Seminar, Bilkent University, April 2016.
- "Cryptography and Communications Security," ACM Student Seminar, TOBB-ETU, November 2015.
- "Cryptography and Protocols," TÜBİTAK Cybersecurity Summer School, September 2014.
- "Cryptographic Protocols," TÜBİTAK Cryptology Summer School, September 2013.
- "Cryptographic Protocols," TÜBİTAK Cryptology Summer School, September 2012.
- "Differential and Linear Cryptanalysis," TÜBİTAK Cryptology Summer School, September 2011.
- "Cryptographic Protocols," TÜBİTAK Cryptology Summer School, September 2011.
- "An Introduction to Cryptography and Cryptological Problems," Dept. of Industrial Engineering, METU, May 2009.
- "Threshold Cryptography," Dept. of Computer Engineering, Galatasaray University, May 2005.
- "IPsec and Protocol Cryptanalysis," Dept. of Computer Engineering, Galatasaray University, May 2005.
- "Cryptography," Dept. of Mathematics, Hacettepe University, April 2005.
- "Differential and Linear Cryptanalysis of Block Ciphers," Informatics Institute, METU, May 2004.