Sedat Akleylek, Ph.D.

CONTACT INFORMATION

Department of Computer Engineering
Ondokuz Mayıs University
55139, Kurupelit, Samsun, Turkey.

Mobile: +90 542 8209563
E-mail: akleylek@gmail.com
WWW: goo.gl/ldzhSt
GoogleScholar: goo.gl/hVDYCP

RESEARCH INTERESTS

Cryptography and computer algebra: Efficient cryptographic computations, post-quantum cryptography, applied cryptography for cyber security, arithmetic of finite fields, Boolean functions, machine learning for information security

ACADEMIC APPOINTMENTS

Associate Professor March 2016 to present
Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey
Affiliated Faculty Member October 2011 to present
Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
Assistant Professor March 2011 to March 2016
Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey
Postdoctoral Researcher July 2014 to July 2015
Theoretische Informatik - Kryptographie und Computeralgebra, Technische Universität Darmstadt, Darmstadt, Germany

Visiting Researcher July 2012 to September 2012
Chair for Embedded Security, Ruhr Universität Bochum, Bochum, Germany
Research Assistant January 2005 to March 2011
Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

EDUCATION

Ph.D., Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, December 2010

M.Sc., Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, February 2008

B.Sc., Mathematics (majored in Computer Science), Ege University, Izmir, Turkey, June 2004

REFEREED JOURNAL PUBLICATIONS (SCI-INDEXED)

[1] Sedat Akleylek, Kübra Seyhan, *A Probably Secure Bi-GISIS Based Modified AKE Scheme with Reusable Keys*, IEEE Access, Vol.8, No.2, pp.26210-26222, doi:10.1109/ACCESS.2020.2970537, 2020.

[2] Sedat Akleylek, Nurşah Çevik, *MaTRU-KE Revisited: CCA2 Secure Key Establishment Protocol Based on MaTRU*, International Journal of Communication Systems, Vol.33, No.7, pp.1-14, doi:10.1002/dac.4326, 2020.

[3] Muharrem Tolga Sakallı, Sedat Akleylek, Kemal Akkanat, Vincent Rijmen, *On the Automorphisms and Isomorphisms of MDS Matrices and Their Efficient Implementations*, Turkish Journal of Electrical Engineering & Computer Sciences, Vol.28, No.1, pp.275-285, doi:10.3906/elk-1906-151, 2020.

[4] Sedat Akleylek, Meryem Soysaldı, *A Novel 3-pass Identification Scheme and Signature Scheme Based On Multivariate Quadratic Polynomials*, Turkish Journal of Mathematics, Vol.43, No.1, pp. 241-257,doi:10.3906/mat-1803-92, 2019.

[5] Gülsüm Gözde Güzel, Muharrem Tolga Sakallı, Sedat Akleylek, Yasemin Çengellenmiş, Vincent Rijmen, *A New Matrix Form to Generate All* 3×3 *Involutory MDS Matrices over* $\mathbf{F_{2^m}}$, Information Processing Letters, Vol.147, pp.61-68, doi:10.1016/j.ipl.2019.02.013, 2019.

[6] Sedat Akleylek, Meryem Soysaldı, Djallel Eddine Boubiche, Homero Toral-Cruz, *A Novel Method for Polar Form of Any Degree of Multivariate Polynomials with Applications in IoT*, Sensors, Vol.19, No.4, pp.1-11, doi:10.3390/s19040903, 2019.

[7] Meltem Kurt Pehlivanoglu, Muharrem Tolga Sakallı, Sedat Akleylek, Nevcihan Duru, Vincent Rijmen, *Generalization of Hadamard Matrix to Generate Involutory MDS Matrices for Lightweight Cryptography*, IET Information Security, Vol.12, No.4, pp.348-355, doi:10.1049/iet-ifs.2017.0156, 2018.

[8] Sedat Akleylek, Vincent Rijmen, Muharrem Tolga Sakallı, Emir Öztürk, *Efficient Methods to Generate Cryptographically Significant Binary Diffusion Layers*, IET Information Security, Vol.11, No.4, pp.177-187, doi:10.1049/iet-ifs.2016.0085, 2017.

[9] Sedat Akleylek, Erdem Alkım, Erdal Kılıç, *A Modified Parallel Learning Vector Quantization Algorithm for Real-Time Hardware Applications*, Journal of Circuits, Systems, and Computers, Vol.26, No.10, 175156, doi:10.1142/S0218126617501560, 2017.

[10] Sedat Akleylek, Tolga Sakallı, Emir Öztürk, Andaç Mesut Şahin, Gökhan Tuncay, *Generating Binary Diffusion Layers with Maximum/High Branch Numbers and Low Search Complexity*, Security and Communication Networks, Vol.9, No.16, pp.3558-3569, doi:10.1002/sec.1561, 2016.

[11] Sedat Akleylek, Erdem Alkım, Zaliha Yüce Tok, *Sparse Polynomial Multiplication for Lattice-based Cryptography with Small Complexity*, Journal of Supercomputing, Vol.72, No.2, pp.438-450, doi:10.1007/s11227-015-1570-1, 2016.

[12] Sedat Akleylek, Barış Bülent Kırlar, *New Methods for Public Key Cryptosystems based on XTR*, Security and Communication Networks, Vol.8, No.18, pp.3682-3689, doi:10.1002/sec.1291, 2015.

[13] Sedat Akleylek, Zaliha Yüce Tok, *Efficient Interleaved Montgomery Modular Multiplication for Lattice-Based Cryptography*, IEICE Electronics Express, Vol.11, No.22, pp.1-6, doi:10.1587/elex.11.20140960, 2014.

[14] Sedat Akleylek, Tolga Sakallı, Bora Aslan, Ercan Buluş, Fatma Büyüksaraçoğlu, *On the Construction of* 20×20 *and* 24×24 *Binary Matrices with Good Implementation Properties for Lightweight Block Ciphers and Hash Functions*, Mathematical Problems in Engineering, doi:10.1155/2014/540253, 2014.

[15] Sedat Akleylek, Ferruh Özbudak and Canan Özel, *On the Arithmetic Operations over Finite Fields of Characteristic Three with Low Complexity*, Journal of Computational and Applied Mathematics, Vol.259, pp.546-554, Part B, doi:10.1016/j.cam.2013.08.11, 2014.

[16] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication of Polynomials*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E96-A, No.10, pp.2016-2024, doi:10.1587/transfun.E96.A.2016, 2013.

[17] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *On the Generalisation of Special Moduli for Faster Interleaved Montgomery Modular Multiplication*, IET Information Security, Vol.7, No.3, pp.165-171, doi:10.1049/iet-ifs.2010.0271, 2013.

[18] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *On the Polynomial Multiplication in Chebyshev Form*, IEEE Transactions on Computers, Vol.61, No.4, pp.584-587, doi:10.1109/TC.2011.38, 2012.

[19] Sedat Akleylek and Ferruh Özbudak, *Modified Redundant, Representation for Designing Arithmetic Circuits with Small Complexity*, IEEE Transactions on Computers, Vol.61, No.3, pp.427-432, doi:10.1109/TC.2011.29, 2012.

[20] Sedat Akleylek, Barış Bülent Kırlar, Ömer Sever, Zaliha Yüce, *A New Short Signature Scheme with Random Oracle from Bilinear Pairings*, Journal of Telecommunications and Information Technology, Vol.5, No:1, pp.5-11, 2011.

[21] Sedat Akleylek, Levent Emmungil, Urfat Nuriyev, *A Modified Algorithm for Peer-to-Peer Security*, Applied and Computational Mathematics, Vol.6, No.2, pp.258-265, ISSN:1683-3511, 2007.

SELECTED CONFERENCE PUBLICATIONS

[1] Wai-Kong Lee, Sedat Akleylek, Wun-She Yap, Bok-Min Goi, *Accelerating Number Theoretic Transform in GPU Platform for qTESLA Scheme*, 15th International Conference on Information Security Practice and Experience, LNCS 11879, pp.41-55, November 26-28, 2019.

[2] Wai-Kong Lee, Bok-Min Goi, Denis Chee-Keong Wong, Wun-She Yap, Sedat Akleylek, *Fast NTRU Encryption in GPU for Secure IoP Communication in Post-quantum Era*, IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, pp.1923-1928, November 7-11, 2018.

[3] İlker Özçelik, Sedat Akleylek, İbrahim Özçelik, *TRCyberLab: An Infrastructure for Future Internet and Security Studies*, 6th International Symposium on Digital Forensic and Security (ISDFS 2018), Antalya, Turkey, IEEE Explore Proceedings of ISDFS 2018, pp.431-435, March 22-25, 2018.

[4] Durmuş Özkan Şahin, Oğuz Emre Kural, Sedat Akleylek, Erdal Kılıç, *New Results on Permission Based Static Analysis for Android Malware*, 6th International Symposium on Digital Forensic and Security (ISDFS 2018), Antalya, Turkey, IEEE Explore Proceedings of ISDFS 2018, pp.340-344, March 22-25, 2018.

[5] Sedat Akleylek, Nina Bindel, Johannes A. Buchmann, Juliane Krämer, *Giorgia Azzurra Marson, An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation*, 8th International Conference on Cryptology in Africa (AFRICACRYPT 2016), LNCS Vol.9646, pp.44-60, April 13-15, Fes, Morocco, 2016.

[6] Sedat Akleylek, Ferruh Özbudak, *Multiplication in a Galois Ring*, Proceedings of The Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA'15), IEEE, pp.28-33, September 13-18, Bengaluru, India, 2015.

[7] Sedat Akleylek, Özgür Dağdelen, Zaliha Yüce Tok, *On the Efficiency of Polynomial Multiplication for Lattice-Based Cryptography on GPUs using CUDA*, International Conference on Cryptography and Information Security in Balkan (BalkanCryptSec 2015), Springer LNCS, September 3-4, Koper, Slovenia, 2015.

[8] Sedat Akleylek, Ferruh Özbudak and Canan Özel, *Charlier Polynomial Representation for Finite Fields of Characteristic Three*, 18th International Conference on Applications of Computer Algebra, June 25-28, Varna, Bulgaria, 2012.

[9] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity*, 11th International Conference on Cryptology (INDOCRYPT 2010), G. Gong and K.C. Gupta (Eds.), LNCS 6498, pp.227-237, Springer, 2010.

[10] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication*, 10th Central European Conference on Cryptology, Poznan, Poland, 2010.

[11] Sedat Akleylek, Barış Bülent Kırlar, Ömer Sever, Zaliha Yüce, *Short Signature Scheme from Bilinear Pairings*, Proceedings of Western European Workshop on Research in Cryptology (WEWoRC 2009), pp.57-61, Graz, Austria.

Chapters in a Book

[1] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *Elliptic Curves and Public Key Cryptography*, Handbook of Codes and Sequences with Applications in Communication, Computing and Information Security, S. Boztaş (Editor), to appear, 2021.

[2] Sedat Akleylek, Meryem Soysaldı, *Identification schemes in the post-quantum area based on multivariate polynomials with applications in cloud and IoT*, In Authentication Technologies for Cloud Technology, IoT and Big Data, The Institution of Engineering and Technology (The IET), pp.181-207, 2019.

[3] Meltem Kurt Pehlivanoglu, Muharrem Tolga Sakallı, Sedat Akleylek, Nevcihan Duru, *Lightweight block ciphers with applications in IoT*, In Authentication Technologies for Cloud Technology, IoT and Big Data, The Institution of Engineering and Technology (The IET), pp.153-180, 2019.

[4] Sedat Akleylek, Zaliha Yüce Tok, *Computational Aspects of Lattice-Based Cryptography on Graphical Processing Unit*, Improving Information Security Practices through Computational Intelligence, El Sayed El-Alfy et. al (Eds.), IGI Global, doi:10.4018/978-1-4666-9426-2, 2016.

[5] Sedat Akleylek, Özgür Dağdelen, Zaliha Yüce Tok, *On the Efficiency of Polynomial Multiplication for Lattice-Based Cryptography on GPUs using CUDA*, Cryptography and Information Security in the Balkans, LNCS Vol.9540, pp.155-168, doi:10.1007/978-3-319-29172-7_10, Springer, 2015.

[6] Sedat Akleylek, Murat Cenk and Ferruh Özbudak, *Faster Montgomery Modular Multiplication without Pre-computational Phase For Some Classes of Finite Fields*, Computer and Information Sciences, E. Gelenbe et.al (Eds.), LNEE Vol.62, part.11, pp.405-408, Springer, 2010.

Books

[1] Sedat Akleylek, Besik Dundua, *Handbook of Formal Analysis and Verification in Cryptography*, Taylor & Francis, CRC Press, to appear, 2021.

[2] Canan Çimen, Sedat Akleylek, Ersan Akyıldız, *Şifrelerin Matematiği : Kriptografi* (in Turkish), ODTÜ Geliştirme Vakfı Yayıncılık, ISBN 978-9944-344-27-2, ilk baskı Mayıs 2007.

Scholarships and Awards

- Co-Advisor of the best Ph.D. Thesis at Institute of Applied Mathematics, METU, 2017.
- *Best Research Paper Finalist* at New York University Abu Dhabi Cyber Security Awareness Week (CSAW) 2017 in MENA Region (published paper in 2016-2017).
- *Best Paper Award* at 10th International Conference on Information Security and Cryptology (ISCTURKEY) Conference 2017.
- *Best Research Paper Award* at New York University Abu Dhabi Cyber Security Awareness Week (CSAW) 2016 in MENA Region (published paper in 2015-2016).
- *Best Paper Award* at 9th International Conference on Information Security and Cryptology (ISCTURKEY) Conference 2016.
- TÜBITAK (the Scientific and Technological Research Council of Turkey) 2242 Software Projects Competition, advisor of *SMS-PGP Project* winning second runner up prize among 50 finalists, 2014.

- TÜBITAK (the Scientific and Technological Research Council of Turkey) 2219 Postdoctoral Research Program, 2014-2015.
- ECRYPT Visiting Researcher Scholarship, Ruhr Universität Bochum, 2012.
- *Thesis of the Year Award*, Middle East Technical University, Ankara, Turkey, 2012.
- *Honour Award of Serhat Özyar Young Scientist of the Year*, Turkish Electrical Engineers Association, Middle East Technical University Faculty Association and Science and Utopia Cooperative, Turkey, 2011.
- Scholarship from TÜBITAK (the Scientific and Technological Research Council of Turkey), 2008-2010.
- International Scientific Publications Promotion Program, Ondokuz Mayıs University, 2013-2014-2015.
- International Scientific Publications Promotion Program, TÜBITAK (the Scientific and Technological Research Council of Turkey), 2012-2014-2015.

PROJECTS

- *Design and Analysis of NTRU-based Cryptosystems Using Formal Methods*, Principal Investigator, Funded by Georgian Shota Rustaveli Georgian National Science Foundation and TÜBITAK (the Scientific and Technological Research Council of Turkey), February, 2019 - February, 2021.
- *Lattice-Based Cryptographic Protocol Design and Efficient Implementations*, Principal Investigator, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey) 1003 - Priority Theme: Cryptology, April, 2018 - April, 2020.
- *Efficiency Analysis and Implementation of Post-Quantum Cryptographic Schemes in Software/Hardware*, Principal Investigator, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey) 1001, June, 2017 - June, 2019.
- *Cyber Security and Cryptology Laboratory*, Principal Investigator, Funded by OMU BAP, December, 2017 - May, 2019.
- *Security Requirements of Cryptographic Modules*, Principal Investigator, Funded by OMU BAP, 2012-2014.
- *Some Cryptographic Functions and Efficient Implementations*, Principal Investigator, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey), Accepted, 2014.
- *Mathematical Aspects of Curve-based Cryptography*, Researcher, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey) and BMBF, 2012-2014.
- *Algebraic Curves and Their Applications to Some Problems in Cryptography and Coding Theory*, Researcher, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey), 2010-2013.
- *Certified Electronic Mail*, Researcher, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey), 2010-2011.
- *Finite Geometry, Coding Theory and Cryptography*, Researcher, Funded by METU BAP, 2009-2010.
- *Pairing Based Cryptographic Protocols and Applications*, Researcher, Funded by ASELSAN A.S. 2008-2009.
- *Implementation of Cryptographic Algorithms with Different Security Levels*, Researcher, Funded by TÜRKSAT, 2008.
- *Selecting Secure Elliptic Curves over $GF(p)$ and Implementing a Signature System Based on Elliptic Curves*, Researcher, Funded by ASELSAN A.S. 2007-2008.
- *Development and Implementations in Public Key Infrastructures*, Researcher, Funded by TÜBITAK (the Scientific and Technological Research Council of Turkey), 2006-2008.

PROFESSIONAL ACTIVITIES

Editorial Board Membership

- Member of Editorial Board of IEEE Access (2018-...)
- Member of Editorial Board of Turkish Journal of Electrical Engineering and Computer Sciences (2017-...)

- Member of Editorial Board of Süleyman Demirel University, Journal of Natural and Applied Sciences (2015-...)
- Co-Editor of International Journal of Information Security Science (2012-...)

Consultancy

- Consultant to Rönesans Holding Computer Center Department, (2018-...)
- Panelist of Cyber Security and Cryptology Working Group at Council of Higher Education in Turkey (2017-...)
- Panelist of Ministry of Defence, R&D and Technology Department - Information Technologies (2014-2016)

Technical/Organizing Committee Member

- International Conference on Cryptography and Information Security - BalkanCryptSec (2014, 2015) Steering Committee member
- International Conference on Computer Science and Engineering (UBMK 2016-2017-2018-2019-2020)
- International Conference on Information Security and Cryptology (ISCTURKEY 2007-2008-2010-2012-2013-2014-2015-2016-2017-2018-2019-2020, Ankara, Turkey)
- International Conference on Applied and Computational Mathematics (ICACM October 3-6, 2012, Ankara, Turkey)

Reviewer Service

- **Journals:** IEEE Transactions on Information Forensics and Security, Journal of Super Computing, IEEE Transactions on Computers, Journal of Cluster Computing, Wiley Transactions on Emerging Telecommunications Technologies, IEEE Communications Magazine, Journal of Computational and Applied Mathematics, IEEE Access, IET Signal Processing, The Computer Journal, Electronics Letters, IEEE Transactions on Dependable and Secure Computing, Journal of Cryptographic Engineering, International Journal of Information and Computer Security, Future Generation Computer Systems, IEEE Communications Letters, Mathematical Problems in Engineering, Journal of Circuits, Systems, and Computers, Turkish Journal of Electrical Engineering and Computer Sciences, Journal of Applied Mathematics and Computing, International Journal of Information Security Science, Journal of Applied Mathematics, The Scientific World Journal, Machine Learning, International Journal of Distributed Sensor Networks, IGI Global, International Journal of Computing and Digital Systems, Turkish Journal of Mathematics, Journal of Applied and Computational Mathematics, Journal of Faculty of Engineering and Architecture of Gazi University, etc.

More Information

More information and auxiliary documents can be found at
https://scholar.google.com.tr/citations?user=plpKMjkAAAAJ&hl=tr&oi=ao,
https://sites.google.com/a/bil.omu.edu.tr/akleylek/home and
http://dblp.uni-trier.de/pers/hd/a/Akleylek:Sedat.