

# Prof. Dr. KEMAL BIÇAKCI

## PERSONAL DATA

---

NAME: Kemal Biçakci  
GENDER: Male  
ADDRESS: ITU Ayazaga Kampusu, Bilisim Enstitüsü Maslak-34469, Istanbul Turkey  
HOMEPAGE: <http://www.kemalbicakci.com>  
FAMILY STATUS: Married with three children

## WORK EXPERIENCE

---

since 12/2020 Faculty member at Istanbul Technical University,  
current position: Founding Head of cybersecurity vocational school  
and Full Professor in Informatics Inst. and Computer Engineering Dept.

since 03/2016 Co-Founder of Securify Inc. (a grow-up company in cyber security do-  
main providing identity and access management solutions and special-  
ized in behavioral biometrics)  
current position: Chairman of the Board.

08/2007–12/2020 Faculty member at TOBB University,  
09/2011–11/2011 Visiting Scholar, Carleton University, Canada  
04/2006–07/2007 IT Coordinator, National Agency, Turkey  
08/2004–01/2006 Postdoc Researcher, Vrije University, The Netherlands  
05/2000–03/2006 Teaching Assistant / Instructor, METU, Turkey  
01/1998–03/2000 Graduate Research Assistant, USC/Information Sciences Institute, USA  
08/1996–07/1997 Teaching Assistant, METU, Turkey

## ACADEMIC TITLES

---

02/2015 Full Professor  
06/2009 Associate Professor (Computer Engineering)  
08/2007 Assistant Professor

## EDUCATION

---

09/2003 PH.D. DEGREE, Information Systems  
Informatics Institute, Middle East Technical University (METU)  
Ankara, Turkey

05/1999 M.S. DEGREE, Electrical Engineering (Computer Networks)  
University of Southern California (USC)  
Los Angeles, USA

06/1996 B.S. DEGREE, Electronics Engineering  
Hacettepe University  
Ankara, Turkey

06/1992 HIGH SCHOOL DIPLOMA  
Ankara Atatürk Anatolian High School  
Ankara, Turkey

## RESEARCH INTERESTS

---

Cybersecurity (usable security, user authentication, behavioral biometrics)  
Applied cryptography (digital signatures, white-box cryptography, post-quantum crypto)  
Wireless and sensor networks (security, optimization, modeling)

## RESEARCH PROJECTS

---

Authentication Anomaly Detection with User Behavioral Analytics, (TUBITAK 1501, completed), Role: Principal Investigator (PI)

SECURIFYID-FACE: Privacy Preserving Verification of Real-World Identities with Face Recognition Technology, (TUBITAK 1501, completed), Role: Principal Investigator (PI)

Design and Implementation of a Passwordless Password Manager System with Single Sign On Feature, (TUBITAK 1501, completed), Role: Principal Investigator (PI)

Establishing a National Face Database and Measuring the Performance of Various Face Recognition and Face Detection Algorithms (ITU BAP, completed), Role: Principal Investigator (PI)

Development of Mobile-Identity Solution based on White-Box Cryptography, (TUBITAK 1501, finished), Role: Principal Investigator (PI).

Implementation of a Secure, Quickly-Adaptable and Portable Remote Working System, (TUBITAK 1501, finished), Role: Co-Principal Investigator (PI).

Development of a HSM-based Crypto Asset Wallet, (TUBITAK 1501, finished), Role: Co-Principal Investigator (PI).

WARNING: A Defense-in-depth Cyber Intelligence Platform to Defend against Emerging Cyber Attacks (TUBITAK 2556 – QNRF Joint Funding Program, finished), Role: PI.

Security in Insecure Environment: Design and Development of White-Box Cryptography Library (TUBITAK 1505, finished), Role: PI.

Development of Authentication System Based on Behavioral Biometrics (TUBITAK 1507, finished), Role: PI.

Pilot Study on Validating Academic Credentials (ICT PSP STORK 2.0, TUBITAK BILGEM, finished), Role: PI.

Accessible and Usable Human Interaction Proofs (TUBITAK 1002, finished), Role: PI.

Design and Implementation of Secure and Usable Graphical Password Methods (TUBITAK 1001, finished), Role: PI.

Advanced Training Hands-on, Cyber Defense Training Course for System/Network Administrators, Funded by NATO Emerging Security Challenges (ESC) Division, SPS Programme, Role: Specialist.

Avicenna - Network of universities for open distance learning. Responsible for producing an online computer security and cryptography course, Funded by UNESCO, Role: Tutor.

SecurE-Justice, Secure Communication and Collaboration Framework for the Judicial Co-operation Environment, Funded by EU FP6, Role: Postdoctorate Researcher.

SAS - Server Assisted Signatures, Funded by National Science Foundation (NSF), Role: Graduate Research Assistant.

FLOTS - Flexible One-Time Signatures, Funded by NSF, Role: Graduate Research Assistant.

CRISIS - Critical Resource Allocation and Intrusion Response for Survivable Information Systems, Funded by NSF, Role: Graduate Research Assistant.

## JOURNAL PUBLICATIONS

---

Mahnamfar, Amin, **Bicakci, Kemal** and Yusuf Uzunay. ROSTAM: A passwordless web single sign-on solution mitigating server breaches and integrating credential manager and federated identity systems. *Computers & Security* 139 (2024): 103739.

Burakgazi Bilgen, M., Abul, O., **Bicakci, Kemal**, Authentication-enabled attribute-based access control for smart homes. *International Journal of Information Security*, (2023) 1-17.

Tekin, Salih, **Bicakci, Kemal**, et al., Optimal data backup policies for information systems subject to sudden failure. *Journal of Quality in Maintenance Engineering*, (2023): 338-355.

**Bicakci, Kemal**, et al., "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid", *IEEE Access*, 8 (2020), 177447-177470..

Yildiz, Huseyin Ugur, **Bicakci, Kemal**, et al. "The impact of incomplete secure connectivity on the lifetime of wireless sensor networks." *IEEE Systems Journal*, volume 12, issue 1, March 2018, (2018): 1042-1046.

**Bicakci, Kemal**, and Hakan Ezgi Kiziloz. "A Closer Look at Pure-Text Human-Interaction Proofs." *IEEE Transactions on Human-Machine Systems*, volume 47, issue 6, Dec. 2017 (2017): 994-1004.

**Bicakci, Kemal**, and Hakan Ezgi Kiziloz. "Leveraging human computation for pure-text Human Interaction Proofs." *International Journal of Human-Computer Studies*, volumes 92-93 (2016): 44-54.

Yildiz, Huseyin Ugur, **Bicakci, Kemal**, et al. "Maximizing Wireless Sensor Network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies." *Ad Hoc Networks*, volume 37 (2016): 301-323.

Incebacak, Davut, **Bicakci, Kemal**, and Bulent Tavli. "Evaluating energy cost of route diversity for security in wireless sensor networks." *Computer Standards and Interfaces*, volume 39 (2015): 44-57.

Pala, Zeydin, **Bicakci, Kemal**, and Mustafa Turk. "Effects of node mobility on energy balancing in wireless networks." *Computers and Electrical Engineering*, volume 41 (2015): 314-324.

Uzun, Erkam, **Bicakci, Kemal**, et al. "The impact of scalable routing on lifetime of smart grid communication networks." *Ad hoc networks*, volume 22 (2014): 27-42.

Cotuk, Huseyin, **Bicakci, Kemal**, et al. "The impact of transmission power control strategies on lifetime of wireless sensor networks." *IEEE Transactions on Computers*, volume 63, issue 11 (2013): 2866-2879.

**Bicakci, Kemal**, Bruno Crispo, and Gabriele Oligeri. "LAKE: A Server-Side Authenticated Key-Establishment with Low Computational Workload." *ACM Transactions on Internet Technology (TOIT)*, volume 13, issue 2 (2013): 1-27.

Incebacak, Davut, **Bicakci, Kemal**, et al. "Optimal number of routing paths in multi-path routing to minimize energy consumption in wireless sensor networks." *EURASIP Journal on Wireless Communications and Networking*, 252 (2013).

**Bicakci, Kemal**, et al. "Neighbor sensor networks: Increasing lifetime and eliminating partitioning through cooperation." *Computer Standards and Interfaces*, volume 35, issue 4 (2013): 396-402.

Tavli, Bulent, **Bicakci, Kemal**, et al. "A survey of visual sensor network platforms." *Multimedia Tools and Applications*, volume 60, issue 3 (2012): 689-726.

Uzun, Yasin, and **Bicakci, Kemal**. "A second look at the performance of neural networks for keystroke dynamics using a publicly available dataset." *Computers & Security* 31.5 (2012): 717-726.

**Bicakci, Kemal**, Ibrahim Ethem Bagci, and Bulent Tavli. "Communication/computation tradeoffs for prolonging network lifetime in wireless sensor networks: The case of digital signatures." *Information Sciences*, volume 188, (2012): 44-63.

**Bicakci, Kemal**, et al. "Maximizing lifetime of event-unobservable wireless sensor networks." *Computer Standards and Interfaces*, volume 33, issue 4 (2011): 401-410.

**Bicakci, Kemal**, Ibrahim Ethem Bagci, and Bulent Tavli. "Lifetime bounds of wireless sensor networks preserving perfect sink unobservability." *IEEE Communications Letters*, volume 15, issue 2 (2011): 205-207.

Tavli, Bulent, M. Burak Akgun, and **Bicakci, Kemal**. "Impact of limiting number of links on the lifetime of wireless sensor networks." *IEEE Communications Letters*, volume 15, issue 1 (2010): 43-45.

Tavli, Bulent, M. Mikail Ozciloglu, and **Bicakci, Kemal**. "Mitigation of compromising privacy by transmission range control in wireless sensor networks." *IEEE Communications Letters*, volume 14, issue 12 (2010): 1104-1106.

Guerrero-Zapata, Manel, **Bicakci, Kemal**, et al. "The future of security in wireless multimedia sensor networks." *Telecommunication Systems*, volume 45, issue 1 (2010): 77-91.

**Bicakci, Kemal**, and Bulent Tavli. "Prolonging network lifetime with multi-domain cooperation strategies in wireless sensor networks." *Ad Hoc Networks*, volume 8, issue 6 (2010): 582-596.

**Bicakci, Kemal**, Hakan Gultekin, and Bulent Tavli. "The impact of one-time energy costs on network lifetime in wireless sensor networks." *IEEE Communications Letters*, volume 13., issue 12 (2009): 905-907.

**Bicakci, Kemal**, and Bulent Tavli. "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks." *Computer Standards and Interfaces*, volume 31, issue 5 (2009): 931-941.

**Bicakci, Kemal**. "One-time proxy signatures revisited." *Computer Standards and Interfaces*, volume 29, issue 4 (2007): 499-505.

**Bicakci, Kemal**, and Nazife Baykal. "Improved server assisted signatures." *Computer Networks*, volume 47, issue 3 (2005): 351-366.

**Bicakci, Kemal**, and Nazife Baykal. "Improving the security and flexibility of one-time passwords by signature chains." *Turkish Journal of Electrical Engineering and Computer Sciences*, volume 11, issue 3 (2003): 223-236.

**Bicakci, Kemal**, Gene Tsudik, and Brian Tung. "How to construct optimal one-time signatures." *Computer Networks*, volume 43, issue 3 (2003): 339-349.

## CONFERENCE PUBLICATIONS (INTERNATIONAL)

---

**Bicakci, Kemal**, and Yusuf Uzunay. "Is FIDO2 Passwordless Authentication a Hype or for Real?: A Position Paper." 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY). IEEE, 2022.

Özbay, Abdullah, and **Kemal Bıçakcı**. "Android Pre-installed Applications Effects On User's Privacy." 2021 International Conference on Information Security and Cryptology (ISCTURKEY). IEEE, 2021.

Aydin, Mustafa, **Bicakci, Kemal**, et al. "Using Attribute-based Feature Selection Approaches and Machine Learning Algorithms for Detecting Fraudulent Website URLs." 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2020.

**Bicakci, Kemal**, et al. "Open-TEE is No Longer Virtual: Towards Software-Only Trusted Execution Environments Using White-Box Cryptography." 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2019.

Aksu, M. Ugur, **Bicakci, Kemal**, and Enes Altuncu. "A First Look at the Usability of OpenVAS Vulnerability Scanner." Workshop on Usable Security (USEC) 2019. NDSS, 2019.

Huseinovic, Alvin, **Bicakci, Kemal**, et al. "A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures." 2018 26th Telecommunications Forum (TELFOR). IEEE, 2018.

**Bicakci, Kemal**, et al. "How Safe Is Safety Number? A User Study on SIGNAL's Fingerprint and Safety Number Methods for Public Key Verification." International Conference on Information Security. Springer, 2018.

Aksu, M. Ugur, **Bicakci, Kemal**, et al. "Automated generation of attack graphs using NVD." Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018.

Aksu, M. Ugur, **Bicakci, Kemal**, et al. "A quantitative CVSS-based cyber security risk assessment methodology for IT systems." 2017 International Carnahan Conference on Security Technology (ICST). IEEE, 2017.

**Bicakci, Kemal**, et al. "TwinCloud: secure cloud sharing without explicit key management." 2016 IEEE Conference on Communications and Network Security (CNS). IEEE, 2016.

Kiziloz, Hakan Ezgi, and **Bicakci, Kemal**. "Towards making accessible human-interaction proofs more secure and usable." 2015 IEEE Symposium on Computers and Communication (ISCC). IEEE, 2015.

**Bicakci, Kemal**, and Tashtanbek Satiev. "charPattern: Rethinking Android Lock Pattern to Adapt to Remote Authentication." International Conference on Passwords. Springer, 2014.

**Bicakci, Kemal**, et al. "Mobile authentication secure against man-in-the-middle attacks." 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. IEEE, 2014.

Cotuk, Huseyin, **Bicakci, Kemal**, et al. "The impact of bandwidth constraints on the energy consumption of wireless sensor networks." 2014 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2014.

Uzunay, Yusuf, and **Bicakci, Kemal**. "Trusted3Ballot: Improving Security and Usability of Three Ballot Voting System Using Trusted Computing." 2014 5th International Conference on Intelligent Systems, Modelling and Simulation. IEEE, 2014.

Yildiz, Huseyin Ugur, **Bicakci, Kemal**, and Bulent Tavli. "Communication/computation trade-offs in wireless sensor networks: Comparing network-level and node-level strategies." 2014 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet). IEEE, 2014.

Akpulat, Murat, **Bicakci, Kemal**, and Ugur Cil. "Revisiting graphical passwords for augmenting, not replacing, text passwords." Proceedings of the 29th Annual Computer Security Applications Conference. 2013.

Pala, Zeydin, **Bicakci, Kemal**, and Bulent Tavli. "Mobility helps energy balancing in wireless networks." MILCOM 2013, Military Communications Conference. IEEE, 2013.

Batmaz, Anil Ufuk, **Bicakci, Kemal**, et al. "The impact of link unidirectionality and reverse path length on wireless sensor network lifetime." IEEE International Conference on Communications (ICC). IEEE, 2013.

Soylev, Arda, **Bicakci, Kemal**, and Bulent Tavli. "Uncovering the Impact of Minimum-Energy Routing on Lifetime of Wireless Sensor Networks." IEEE International Conference on Distributed Computing in Sensor Systems. IEEE, 2013.

Cil, Ugur, and **Bicakci, Kemal**. "gridwordx: Design, implementation, and usability evaluation of an authentication scheme supporting both desktops and mobile devices." Workshop on Mobile Security Technologies (MoST'13). 2013.

Incebacak, Davut, **Bicakci, Kemal**, and Bulent Tavli. "Energy Cost of Mitigating Physical Attacks in Wireless Sensor Networks." 2012 5th International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2012.

**Bicakci, Kemal**, et al. "Exploration and field study of a password manager using icon-based passwords." International Conference on Financial Cryptography and Data Security, Workshop on Real-Life Cryptographic Protocols and Standardization. Springer, Berlin, Heidelberg, 2011.

**Bicakci, Kemal**, Nart Bedin Atalay, and Hakan Ezgi Kiziloz. "Johnny in internet café: user study and exploration of password autocomplete in web browsers." Proceedings of the 7th ACM workshop on Digital identity management. 2011.

**Bicakci, Kemal**, and Paul C. Van Oorschot. "A multi-word password proposal (gridWord) and exploring questions about science in security research and usable security evaluation." Proceedings of the 2011 New security paradigms workshop. 2011.

Incebacak, Davut, **Bicakci, Kemal**, and Bulent Tavli. "Investigating the tradeoffs between spatial granularity and energy requirements in wireless sensor networks." 2010 Fourth UKSim European Symposium on Computer Modeling and Simulation. IEEE, 2010.

Unlu, Seckin Anil, and **Bicakci, Kemal**. "Notabnab: Protection against the "tabnabbing attack"." 2010 eCrime Researchers Summit. IEEE, 2010.

**Bicakci, Kemal**. "Pushing the limits of one-time signatures." Proceedings of the 2nd international conference on Security of information and networks. ACM, 2009.

**Bicakci, Kemal**, et al. "Towards usable solutions to graphical password hotspot problem." 2009 33rd Annual IEEE International Computer Software and Applications Conference. Vol. 2. IEEE, 2009.

**Bicakci, Kemal**, et al. "Graphical passwords as browser extension: Implementation and usability study." IFIP International Conference on Trust Management. Springer, Berlin, Heidelberg, 2009.

**Bicakci, Kemal**. "Optimal discretization for high-entropy graphical passwords." 2008 23rd International Symposium on Computer and Information Sciences. IEEE, 2008.

Uzunay, Yusuf, and **Bicakci, Kemal**. "SHA: A secure voice activated smart home for quadriplegia patients." 2007 IEEE International Conference on Bioinformatics and Biomedicine Workshops. IEEE, 2007.

Uzunay, Yusuf, Davut Incebacak, and **Bicakci, Kemal**. "Towards Trustable Digital Evidence with PKIDEV: PKI Based Digital Evidence Verification Model." EC2ND 2006. Springer, London, 2007. 105-114.

Gamage, Chandana, **Bicakci, Kemal**, et al. "Security for the mythical air-dropped sensor network." 11th IEEE Symposium on Computers and Communications (ISCC'06). IEEE, 2006.

Gulkesen, Kemal H., **Bicakci, Kemal**, et al. "Reliability of Health Information on the Turkish Web Sites; Fever in Children at Home.", Medical Informatics 2006, European Notes in Medical Informatics, (2006).

Gamage, Chandana, **Bicakci, Kemal**, et al. "A cost-efficient counter-intrusion scheme for one-time sensor networks." 2005 International Conference on Intelligent Sensors, Sensor Networks and Information Processing. IEEE, 2005.

Uuzunay, Y., and **Bicakci, Kemal**. "UNIDES: an efficient real-time system to detect and block unauthorized Internet access." 11th International Conference on Parallel and Distributed Systems (ICPADS'05). Vol. 2. IEEE, 2005.

**Bicakci, Kemal**, et al. "One-time sensors: A novel concept to mitigate node-capture attacks." European Workshop on Security in Ad-hoc and Sensor Networks. Springer, Berlin, Heidelberg, 2005.

**Bicakci, Kemal**, Bruno Crispo, and Andrew S. Tanenbaum. "Counting abuses using flexible off-line credentials." Australasian Conference on Information Security and Privacy. Springer, Berlin, Heidelberg, 2005.

**Bicakci, Kemal**, Bruno Crispo, and Andrew S. Tanenbaum. "How to incorporate revocation status information into the trust metrics for public-key certification." Proceedings of the 2005 ACM symposium on Applied computing. 2005.

**Bicakci, Kemal**, and Nazife Baykal. "A new design of privilege management infrastructure with binding signature semantics." European Public Key Infrastructure Workshop. Springer, Berlin, Heidelberg, 2004.

**Bicakci, Kemal**, and Nazife Baykal. "Server assisted signatures revisited." Cryptographers' Track at the RSA Conference. Springer, Berlin, Heidelberg, 2004.

**Bicakci, Kemal**, and Nazife Baykal. "EVEREST: an efficient method for verification of digital signatures in real-time teleradiology." MedInfo. 2004.

**Bicakci, Kemal**, and Nazife Baykal. "Saots: A new efficient server assisted signature scheme for pervasive computing." Security in pervasive computing. Springer, Berlin, Heidelberg, 2004. 187-200.

**Bicakci, Kemal**, and Nazife Baykal. "One-time passwords: Security analysis using BAN logic and integrating with smartcard authentication." International Symposium on Computer and Information Sciences. Springer, Berlin, Heidelberg, 2003.

**Bicakci, Kemal**, and Nazife Baykal. "Design and performance evaluation of a flexible and efficient server assisted signature protocol." Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003. IEEE, 2003.

**Bicakci, Kemal**, and Nazife Baykal. "Infinite length hash chains and their applications." Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. IEEE, 2002.

**Bicakci, Kemal**, and Nazife Baykal. "Wireless and mobile security.", 5th International Conference on Knowledge-Based Intelligent Information Engineering Systems and Allied Technologies, 2001.

**Bicakci, Kemal**, Brian Tung, and Gene Tsudik. "On constructing optimal one-time signatures." Proceedings of Fifteenth International Symposium on Computer and Information Sciences, ISCIS, 2000.

## CONFERENCE PUBLICATIONS (IN TURKISH)

Enes Altuncu, **Bicakci, Kemal**. "BLOCKSIGNAL: A Secure Messaging Application Eliminating Authentication Ceremonies using Blockchain Technology, National Blockchain Workshop, 2019.

Kaan Kucuk, **Bicakci, Kemal**. "Development of Mobile ID application using Trusted Execution Environment Technology", Academic Informatics, Akademik Bilisim 2019, Ordu, Turkey, 2019.

Muhammet Sakir Sahkulubey, Enes Altuncu, **Bicakci, Kemal**. "How Safe is Safety Number in Public Key Verification: An Investigation of Usability and Security of Fingerprints and Safety Numbers", Academic Informatics, Akademik Bilisim 2018, Karabuk, Turkey, 2018.

Ersen Balcisoy, **Bıçakcı, Kemal**. "Optimization of SHA256 Hash Algorithm for High Performance Bitcoin Mining", ISCTURKEY 2016, pp.201-209, Ankara, Turkey, 2016.

Batmaz, Anıl Ufuk, **Bıçakcı, Kemal**, et al. "Effects of handshake hop length of unidirectional links on the lifetime of wireless sensor networks." 21st Signal Processing and Communications Applications Conference (SIU). IEEE, 2013.

Uzun, Erkam, **Bıçakcı, Kemal**, et al. "Network lifetime maximization and localized routing tradeoff in wireless sensor networks." 2013 21st Signal Processing and Communications Applications Conference (SIU). IEEE, 2013.

M. Akpulat, **Bıçakcı, Kemal**, U. Çil, "A New Password based Authentication Method Combining Text and Graphical Elements", ISCTURKEY 2012, pp.75-80, Ankara, Turkey, 2012.

Akgün, M. Burak, Bülent Tavlı, and **Bıçakcı, Kemal**. "Number of connection restriction in wireless sensor networks and its influence on network lifetime." National Conference on Electrical, Electronics and Computer Engineering. IEEE, 2010.

**Bıçakcı, Kemal**, "Fundamental Principles for Usable Security", ISCTURKEY 2010, Ankara, Turkey, 2010.

**Bıçakcı, Kemal**, "Reverse SSL: A New Solution for the Performance Problem in SSL Servers", ABG 2008: 2nd National Network and Information Security Symposium, North Cyprus, 2008.

K.H. Gulkesen, **Bıçakcı, Kemal**, et al., "An Evaluation on Technology Use of Diabetic Patients", 4. Academic Informatics Conference, Denizli, Turkey, 2006.

Y. Uzunay and **Bıçakcı, Kemal**, "A3D3M: A Digital Evidence Verification Model Supported with Public Key Infrastructure", In Proc. ABG 2005: National Network and Information Security Symposium, Istanbul, Turkey, 2005.

**Bıçakcı, Kemal**, "Alternative Digital Signature Methods", Internet Conference, INET-TR, Istanbul, Turkey, 2000.

## OTHER PUBLICATIONS

---

Mevlut Serkan Tok, Osman Tufan Tekin, **Bıçakcı, Kemal**. "Analyzing Turkish F and Turkish E keyboard layouts using learning curves", CoRR abs/1905.11791, 2019.

**Bıçakcı, Kemal**, Davut Deniz Yavuz, Sezin Gurkan. "TwinCloud: A Client-Side Encryption Solution for Secure Sharing on Clouds Without Explicit Key Management", CoRR abs/1606.04705, 2016.

Yasin Uzun, **Bıçakcı, Kemal**: "Could We Distinguish Child Users from Adults Using Keystroke Dynamics?", CoRR abs/1511.05672, 2015.

Yusuf Uzunay, **Bıçakcı, Kemal**. "Trust-in-the-Middle: Towards Establishing Trustworthiness of Authentication Proxies using Trusted Computing", CoRR abs/1511.05682, 2015.

**Bıçakcı, Kemal**, et al. "Exploration and Field Study of a Browser-based Password Manager using Icon-based Passwords", Technical Report TR-11-07 (Jan.21, 2011), School of Computer Science, Carleton University, 2011.

**Bıçakcı, Kemal**, "Optimal Discretization for High-Entropy Graphical Passwords", Cryptology ePrint Archive, Report 2008/178, 2008.

**Bıçakcı, Kemal**, et al., "Reverse SSL: Improved Server Performance and DoS Resistance for SSL Handshakes", Cryptology ePrint Archive, Report 2006/212, 2006.

**Bıçakcı, Kemal**, B. Crispo and A.S. Tanenbaum, "How to Incorporate Revocation Status Information into the Trust Metrics for Public-Key Certification", International Journal of Infonomics, Special Issue on Selected papers of the ACM SAC 2005 TRECK Track, 2006.

## SUPERVISED THESIS

---

Yusra Albarazi, Improvement of face recognition performance through transfer learning: A comprehensive study using identity card biometric photographs and mobile phone selfie images, 2024.

Ahmad Droubi, Design and Development of a Secure and Accessible Web Authentication Alternative to FIDO2 Passwordless Standard, 2024.

Kemal Karacuha, Analysis and Evaluation of USB-Based Social Engineering Attacks with User Study, 2024.

Murat Gumus, Systematic Review of Use Cases of Internet Identity Provider Services and Evaluation of Related Design Paradigms, 2024.

Amin Mahnamfar, ROSTAM: A Passwordless Web Single Sign-On Solution Integrating Credential Manager and Federated Identity Systems, 2023.

Murat Sekmen, Face recognition: data collection, testing, evaluation and comparison with id card, biometric photo and phone camera selfie, 2023.

Kaan Küçük, Developing a mobile identity application by using trusted execution environment, M.S. thesis, 2019.

Enes Altuncu, Developing a secure messaging application that eliminates authentication ceremony by using blockchain, M.S. thesis, 2019.

Muhammet Sakir Sahkulubey, Study on the usability and security of the fingerprint and safety number methods used in public key verification, M.S. thesis, 2018.

Ersen Balcısoy, Optimization of SHA256 hash algorithm for high performance bitcoin mining, M.S. thesis, 2017.

Hakan Ezgi Kızılöz, Leveraging human computation for pure-text human interaction proofs, Ph.D. thesis, 2016.

Tashtan Satiev, Charpattern: rethinking android lock pattern to adapt to remote authentication, M.S. thesis, 2015.

Yusuf Uzunay, Increasing trustworthiness of security critical applications using trusted computing, Ph.D. thesis, 2014.

Hüseyin Ugur Yıldız, Communication/computation tradeoffs in wireless sensor networks: Comparing node-level and network-level strategies, M.S. thesis, 2013.

Ugur Cil, Design, implementation, and usability evaluation of a novel knowledge-based authentication scheme supporting both desktops and mobile devices, M.S. thesis, 2013.

Hüseyin Çotuk, Analyzing network lifetime of wireless sensor networks with mathematical programming, Ph.D. thesis, 2013.

Davut Incebacak, Analysis and modeling of routing and security problems in wireless sensor networks with mathematical programming, Ph.D. thesis, 2013.

Yasin Uzun, User authentication and distinguishing child users from adults with keystroke dynamics, Ph.D. thesis, 2013.

Murat Akpulat, A new password based authentication method combining textual and graphical elements, M.S. thesis, 2012.

Ibrahim Ethem Bağcı, The impact of non-repudiation and preserving perfect sink unobservability on the lifetime of wireless sensor networks, M.S. thesis, 2011.

Muhammed Rasit Yıldız, Graphical password: Experimental comparing and field study, M.S. thesis, 2010.

Mehmet Burak Akgün, Investigation of the impact of limiting number of links on the lifetime of wireless sensor networks, M.S. thesis, 2010.

Bahadır İsmail Aydın, Electronic voting with trusted computing, M.S. thesis, 2009.

Davut Incebacak, Design and implementation of a secure and searchable audit logging system, M.S. thesis, 2007.

## SERVICES AND CONSULTANCY WORK

---

Member of Editorial Board - Computer Standards and Interfaces (Elsevier), continuing.

Member of Turkish Cyber Security Cluster supported by the Presidency of the Republic of Turkey Presidency of Defence Industries, continuing.

Member of Science, Technology and Innovation Policy Board Cyber Security and Communication Infrastructure Working Group, 2019-2020.

Member of Administrative Committee of Graduate School of Natural and Applied Sciences, 2013 - 2018.

Member of TUBITAK TEYDEB (Industrial R&D Program) BILTEG (Information Technologies Group) Committee, 2012 - 2016.

Member of Editorial Board - Turkish Journal of Electrical Engineering and Computer Sciences, 2009 - 2010.

Consultancy for various defense industry and IT companies including Havelsan, STM, Comodo, Turktrust, ICTerra, Innova, Procenne, Ofisimcom, Ozgur Entegrasyon, Javatar, GETEK, ILG, and others.

Consultancy for TUBITAK BILGEM (Turkish National E-ID Card project)

Consultancy for the Turkish Electronic Signature Law (date: 15/1/2004, no: 5070)

## TEACHING EXPERIENCE

---

### Free Courses On Youtube

Introduction to Cyber Security, Data Communication and Computer Networks, Operating Systems, Introduction to Computer Science and others (watched 25K+ hours in total)

### Taught Courses in Istanbul Technical University

Information and Computer Security

Information Security Management

Machine Learning Techniques in Cyber Security

Blockchain Technologies

### Taught Courses in TOBB University of Economics and Technology

Usable Security and Privacy

Introduction to Cyber Security / Information Security and Cryptography

Introduction to Computer Science

Operating Systems

Data Communication and Computer Networks

Human-Computer Interaction

Discrete Mathematics

Wireless Communication / Communication Systems

Digital Electronics / Digital Electronics Lab.

### Taught Courses in Middle East Technical University

Computer Security and Cryptography

Information Systems

Networking for Health Information Systems and Telehealth

## HONORS AND AWARDS

---

Securify Inc. received a demand of 11 million TL from 1700 investors in 327 minutes in the investment round organized through the Fonbulucu, a share-based crowdfunding platform.

Award, Adviser of Kaan Kucuk, 3rd Place, Turkey Cyber Security Cluster, Cyber Security Graduation Project Competition.

Award, 2nd Place (among 500 start-ups), for the BiyoSecure product of Securify Inc., TechAnkara 2018, organized by Ankara Development Agency.

MS Thesis Supervisor of Yusuf Uzunay, 2005 - 2006 Academic Year Middle East Technical University Best Thesis Award Winner.

First PhD graduate of Informatics Institute in Middle East Technical University.

## REFERENCES

---

Paul van Oorschot, Prof. Dr., Professor of Computer Science, Canada Research Chair in Authentication and Computer Security, Carleton University, Ottawa, Canada.

Andrew S. Tanenbaum, Prof. Dr., Head of Computer Systems Section, Department of Computer Science, Vrije Universiteit, Amsterdam, The Netherlands.

Nazife Baykal, Prof. Dr., Rector of North Cyprus Campus, Middle East Technical University, Ankara, Turkey.

Gene Tsudik, Prof. Dr., Associate Dean of Research and Graduate Studies, University of California, Irvine, USA.