İsmail San
Department of Electrical and Electronics Engineering
Anadolu University
Eskişehir, Turkey
Phone: +90 (0)222 321 3550 – 6469
isan@anadolu.edu.tr
isan83@gmail.com
`http://home.anadolu.edu.tr/~isan/`
Place of birth: Denizli, Turkey

Affiliation

Since 2014 **Assistant Professor**
Department of Electrical and Electronics Engineering,
Anadolu University
Eskisehir, Turkey

Current Research Interests

Fault Tolerant Computing
Scalable fault correction mechanisms for the arithmetic operations over finite fields.

Cryptographic Hardware Design
New computational descriptions for symmetric key cryptography, cryptographic hardware accelerators for high-speed communication channels, fast point multiplication for binary elliptic curves, cryptography for ubiquitous computing.

Future Computer Architectures
Instruction set architectures, instruction-level parallelism, pipelining, hardware design languages, future processing technologies, heterogeneous multi core and network-on-chip architectures.

Career Path

2009-2014 **Research Assistant**
Department of Electrical and Electronics Engineering,
Anadolu University,
Eskisehir, Turkey

2013 **Research Intern at IBM Research Zurich**
Reliability issues in digital design, Scalable fault tolerant computing
IBM Research - Zurich Laboratory
Zurich, Switzerland

2011 **Consultant - Global Supercomuting Corporation**
Consulting on hardware based systems specialized in cryptographic engineering research and development, Global Supercomputing Corporation
Eskisehir, Turkey

2008 **Systems Engineer**
Digital Data Recorder Product Family Development Project
SDT Space & Defence Technologies
Ankara, Turkey

2007–2008 **Student Assistant**
Department of Electrical and Electronics Engineering,
Anadolu University,
Eskisehir, Turkey

Education

2009-2014 **Ph.D.**
Department of Electrical and Electronics Engineering,
Anadolu University,
Eskisehir, Turkey
Thesis Topic: *Efficient Hardware Architectures for Cryptographic Algorithms used in Computer and Communication Systems, (May 2014).*

2003-2008 **B.Sc.**
Department of Electrical and Electronics Engineering,
Anadolu University,
Eskisehir, Turkey

and
Department of Avionics
Anadolu University,
Eskisehir, Turkey

Languages

Turkish	Native Speaker
English	Fluent

Awards

2013 **Great Minds Student Internship Program**
Science & Technology Department,
IBM Research - Zurich Laboratory, Switzerland

2008 **Winner of Savronik Project Competition (SPY08)**
Inertial Measurement Unit,
Savronik, Eskisehir, Turkey

2008 **Graduated in the first rank** from Faculty of Engineering,
Anadolu University, Eskisehir, Turkey

2008 **Graduated in the first rank** from Faculty of Aerospace Sciences,
Anadolu University, Eskisehir, Turkey

Grants

2012 **Xilinx University Program**
Granted for donations of Xilinx development tools in terms of software and hardware design tools.

List of Publications

International Journals

1. Ismail San and Nuray At. *Improving the Computational Efficiency of Modular Operations for Embedded Systems*, Journal of Systems Architecture, vol.60, issue.5, pp.440–451, May. 2014

2. Nuray At, Jean-Luc Beuchat, Eiji Okamoto, Ismail San, and Teppei Yamazaki. *Compact Hardware Implementations of ChaCha, BLAKE, Threefish, and Skein on FPGA*. Circuits and Systems I: Regular Papers, IEEE Transactions on, vol.61, no.2, pp.485–498, Feb. 2014

3. Ismail San and Nuray At. *Compact Keccak Hardware Architecture for Data Integrity and Authentication on FPGAs*. Information Security Journal: A Global Perspective, vol.21, issue.5, pp.231–242, 2012

Unpublished Work

1. Ismail San, Nuray At, Ibrahim Yakut, and Huseyin Polat. *Designing Paillier Cryptoprocessor for Improving Privacy-Preserving Applications.*

Work Under Review

1. Nuray At, Jean-Luc Beuchat, Eiji Okamoto, Ismail San, and Teppei Yamazaki. *A Low-Area Unified Hardware Architecture for the AES and the Cryptographic Hash Function Grøstl.* Cryptology ePrint Archive, Report 2012/535, 2012.
   Submitted to Integration, the VLSI Journal *Under Review.*

International Conferences

1. Ismail San and Nuray At. *On Increasing the Computational Efficiency of Long Integer Multiplication on FPGA*. In *Proceedings of the Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE 11th International Conference on, pages.1149-1154, IEEE Press, 2012.

2. Nuray At, Jean-Luc Beuchat, and İsmail San. *Compact Implementation of Threefish and Skein on FPGA*. In *Proceedings of the 5th IFIP International Conference on New Technologies, Mobility and Security.* IEEE Press, 2012.

3. Ismail San and Nuray At. *Lightweight Hardware Architecture for XTEA Cryptographic Algorithm. International Conference on Embedded Systems and Intelligent Technology (ICESIT 2012)*, Japan, January 2012.

4. Ismail San and Nuray At. *Compact Hardware Architecture for Hummingbird Cryptographic Algorithm.* In *Proceedings of the 2011 Field Programmable Logic and Applications (FPL)*, pages 376–381. IEEE Press, 2011.

5. Ismail San and Nuray At. *Hardware Implementation of Spectral Modular Multiplication on FPGAs.* In *Proceedings of the International Symposium on Computing in Science & Engineering (ISCSE 2011)*, pages 403–408. 2011.

6. Ismail San and Nuray At. *Efficient SoC Design for Acceleration of Message Authentication and Data Integrity on FPGAs.* In *Proceedings of the International Symposium on Computing in Science & Engineering (ISCSE 2011)*, pages 409–418. 2011.

Ph.D. Thesis

1. İsmail San. *Efficient Hardware Architectures for Cryptographic Algorithms used in Computer and Communication Systems.* Ph.D. thesis, Anadolu University, 2014.

Research Activities

Since 2010 **Lightweight Cryptography**
Designing symmetric cryptosystem for low cost devices using predefined structures, lightweight hardware design for ubiquitous system devices.

2011-2013 **Cryptographic Hash Algorithm Competition**
Performance analysis of the SHA-3 candidates on FPGA.

2010 **Public Key Cryptography**
Algorithm improvements in computation of modular arithmetic, design practical processor for spectral modular multiplication and exponentiation.

2010 **HW/SW Codesign**
Building a secure framework for high and low-speed communication channels with exploiting both advantages of HW and SW.

Talks

2013 **Fault Tolerant Computing**
Scalable Fault Tolerant GF Multiplication.
IBM Zurich Research Laboratory,
Switzerland, November 2013.

2013 **Cryptographic Hardware Design Approaches**
Cryptographic Engineering for Communication Systems.
USI - Università della Svizzera italiana,
Lugano, Switzerland, July 2013.

2012 **Cryptographic Hardware Research**
Compact hardware architectures for XTEA, Hummingbird and Keccak on FPGAs.
Laboratory of Cryptography and Information Security,
University of Tsukuba, January 2012.

Teaching

2014 **Discrete Computational Structures**
Lecturer. Five important themes are covered in this course: mathematical reasoning, combinatorial analysis, discrete structures, algorithmic thinking, and applications & modeling. It is conceptual foundation for all of computer science.

2009-2013 **Computer Architecture**
Teaching Assistant. Teaching MIPS based single and multi cycle processor architectures on FPGA with various laboratory experiments.

2011–2014 **Communications Laboratory**
Teaching Assistant. Teaching various digital schemes using Matlab and advanced digital measurement tools including spectrum analyzer and signal generator.

Since 2009 **Digital Systems II**
Teaching Assistant. Teaching the fundamentals of hardware description language VHDL by introducing advanced digital system topics.

2007–2008 **Computer Architecture**
Student Assistant.

2007–2008 **Digital Systems II**
Student Assistant.

2007 **Microprocessor I**
Student Assistant.