IHSAN CICEK, Ph.D.

Address: Dept. of Computer Science, University of California,
Santa Barbara, Goleta, CA 93106, USA
e-mail: ihsancicek@engineering.ucsb.edu
Tel: +1 805 403 4363

EDUCATION

2015 - Present **Post-Doctoral Researcher,** Department of Computer Science, University of California, Santa Barbara**,** USA

Research Topics:

- Advanced TRNG architectures for low power cryptographic systems
- Low power cryptographic IP core design

2007 - 2014 **Ph.D.**, Electronics Engineering, Faculty of Electrical & Electronics Engineering
Bogazici University, Istanbul, Turkey
GPA: 3.72 / 4.00
Thesis: Design Aspects of Discrete Time Chaos Based True Random Number Generators (Prototype chip is implemented in UMC 180nm process technology)

My research was focused on discrete time 1D chaotic maps, evaluation of underlying entropy, and determination of optimum dynamic system parameters for generating maximum randomness. A design method for mapping dynamic system parameters to circuit parameters is developed.

- Published six conference papers and two journal papers.

2002 - 2004 **M.Sc.**, Microelectronics Engineering, Faculty of Engineering and Natural Sciences, Sabanci University, Istanbul, Turkey

GPA: 3.86 / 4.00 (**Ranked 1st in the department**)
Thesis: A CMOS Readout/Drive Front-End Integrated Circuit for Capacitive Micromachined Ultrasonic Transducer Arrays (Prototype chip is implemented in AMS 0.8um 50V process technology)

CMUT is a cost effective alternative to piezoelectric transducers used in ultrasound imaging. I designed a CMOS circuit for both driving the CMUT with a high voltage pulse and a read-out amplifier to read the echo signal. My research was financially supported by TUBITAK.

- Awarded research scholarship by Sabanci University (full tuition and a stipend).
- Published one conference, and one journal paper.
- Best assistant award (two times).

1998 - 2002 **B.Sc.**, Electronics & Telecom. Engineering, Faculty of Electrical Engineering
Istanbul Technical University, Istanbul, Turkey

GPA: 3.6 /4.00 (Ranked 6th in the department**)**
Senior graduation project: Line Follower Mobile Robot "ARIUS"
ARIUS was a line follower robot based on PIC16F84, with infrared optical navigation, PWM motor driver, and power supply monitor for low battery level detection.

- Awarded with high honor degree for outstanding undergraduate academic performance.
- Awarded with the **"Siemens Excellence Prize"** by SIEMENS Corporation (2002) for my undergraduate performance. I am the only student awarded with this prize in the department.
- Awarded NORTEL - NETAS scholarship during my undergraduate education.

1997 **Ranked 4th** (among 250 projects) in the national high school project competition organized by TUBITAK

1995 **Ranked 62nd** in the national scientific high school examination among 300 thousand students.

WORK EXPERIENCE

2015 – 2015 **TUBITAK BILGEM Test and Evaluation Center, Kocaeli, Turkey**
Senior Researcher, Cryptographic Hardware Communication Security (COMSEC) Assessment Specialist,

- Hardware security assessment of cryptographic hardware designs used in government, and military grade applications.
- Consultancy for COMSEC compliant hardware design process.
- Custom hardware design for side-channel attacks and measurements.

2013 - 2015 **TUBITAK National Institute of Electronics and Cryptology (UEKAE), Kocaeli, Turkey**
Senior Researcher, National Secure IP Phone (MILSEC-4),

- NATO COMSEC compliant ARM (TI) CPU based mainboard and peripheral hardware design for secure voice/video over IP terminal.
- NATO COMSEC compliant FPGA (Xilinx) based cryptographic add-on module hardware design for secure voice/video over IP terminal.
- NATO COMSEC compliant microcontroller (TI) based cryptographic key manager hardware design.

2013 - 2014 **TUBITAK National Institute of Electronics and Cryptology (UEKAE), Kocaeli, Turkey**
Senior Researcher, Custom Cryptographic Add-on Module Design For Air Combat Maneuvering Instrumentation (ACMI) Pods,

- Reverse engineering of internal communication signals, and protocols.
- Design of a custom FPGA based cryptographic add-on board for ACMI pod
- Design of a symmetric key cryptographic IP core for the FPGA on board.
- Field testing of the developed hardware on F-16 aircraft, and base station platforms.

2009 - 2013 **TUBITAK National Institute of Electronics and Cryptology (UEKAE), Kocaeli, Turkey**
Project Leader, Random Number Generators Project,

- Project management, coordination, consultancy.
- Modeling, design, simulation, and testing of TRNG modules for government, and military grade applications.
- FPGA (Xilinx Spartan-3/6) Microblaze based DAQ hardware design.
- Discrete time chaotic system modeling, statistical, and spectral characterization.
- FPAA (Anadigm AN231E04) based hardware design of 1D chaotic maps.
- Continuous time chaos based jitter/entropy booster for dual oscillator based true random number generator applications (implemented in 0.25um CMOS technology).

Researcher, Secure Power-Line Modem (PLM) Surveillance System Project,

- Design of transmitter, and receiver hardware units.
- A compact power line modem analog front-end and high voltage line coupler design, modeling, simulation (SPICE), and testing.
- ARM Cortex-M3 (STM32) based embedded system hardware design.

2008 - 2009 **Bahcesehir University, Faculty of Computer Science, Istanbul, Turkey**
Researcher, Current Mode Multivariable Logic Based Arithmetic Logic Unit Project,

- Installation and administration of Mentor Graphics IC Design Suite on workstation.

2007 - 2008 **Eczacibasi Bilisim, Embedded Design Center, Istanbul, Turkey**
Digital Design Engineer

- HDL Design of an automated testbench for a custom high performance AES module for Texas Instruments
- CAD software administration

2005 - 2007 **Istanbul Commerce University, Information Security Research Center, Istanbul, Turkey**
Teaching Assistant,

- Cofounded Information Security Research Center with Prof. Cetin Kaya Koc.
- Assisted courses given in Information Security Research Center.
- Design of a 16 bit experimental CPU in VHDL

2005 **TUBITAK National Institute of Electronics and Cryptology (UEKAE), Kocaeli, Turkey**
Researcher,
- Embedded system design (8051, PIC based single board microcontroller module),
- 10 GHz Wideband Receiver Front End circuit design for RF bug detection application,

2002 - 2005 **Sabanci University, Istanbul, Turkey**
Research Assistant,
- Design of an analog receiver/transmitter front-end for capacitive micromachined ultrasonic transducers (in cooperation with B. K. Yakub's research group at Stanford University)
- Hardware design and fabrication of a photoresist coater/spinner device.
- Hardware design and fabrication of a constant temperature photoresist dryer device for use in PCB manufacturing.
- Assisted in various courses including VLSI System Design, Microcomputer Based System Design, Analog Integrated Circuits, Digital Integrated Circuits and Electronic Circuits.

2001 **ETA ASIC Design Center, Istanbul Technical University, Istanbul, Turkey**
Intern engineer,
- Designed Miller OTA (Cadence IC Design Tools)
- Designed Vending Machine Controller (Verilog)

2000 **Arcelik, Research & Development Center, Istanbul, Turkey**
Intern engineer,
- Trained on Orcad and Accel EDA
- Trained on SMD rework
- Programmed PIC microcontroller

1999 **Turkish Air Force's 2nd Reinforcement Base, Kayseri, Turkey**
Intern engineer,
- Trained on general electronics
- Repaired electrical motors
- Calibrated test and measurement instruments

PUBLICATIONS

- Cicek, I.; Parlak, M.; Koc, C. K.; , "Energy efficient implementation of FIPS140-2 online true random number generator tests," 2016 26th IEEE International Conference on Field Programmable, vol., no., pp. ??-??, 2016 (Under review).

- Parlak, M.; Cicek, I.; Koc, C. K.; , "Power characterization of ring oscillator based random number generator on FPGAs," 2016 26th IEEE International Conference on Field Programmable, vol., no., pp. ??-??, 2016 (Under review).

- Cicek, I.; Pusane, A.E.; Dundar, G.; , "An integerated dual entropy core true random number generator," IEEE Transactions on Circuits and Systems II: Express Briefs, vol., no., pp. ??,?? 2015 (Under review).

- Cicek, I.; Pusane, A.E.; Dundar, G.; , "A new dual entropy core true random number generator," Journal of Analog Integrated Circuits and Signal Processing (AICSP), vol. 81, no. 1, pp. 61-70, 2014 (Invited paper).

- Cicek, I.; Pusane, A.E.; Dundar, G., "A novel design method for discrete time chaos based true random number generators," Integration, the VLSI Journal, vol. 47, no. 1, pp.38-47, 2014.

- Cicek, I.; Pusane, A.E.; Dundar, G.; , "A novel dual entropy core true random number generator," 2013 8th International Conference on Electrical and Electronics Engineering (ELECO), vol., no., pp.1-4, 28-30 Nov. 2013.

- Cicek, I.; Dundar, G.; , "A chaos based integrated jitter booster for true random number generators," 2013 21th IEEE European Conference on Circuit Theory and Design (ECCTD), vol., no., pp.1-4, 08-12 Sep. 2013.

▪ Cicek, I.; Pusane, A.E.; Dundar, G., "Random number generation using field programmable analog array implementation of logistic map," 2013 21st Signal Processing and Communications Applications Conference (SIU), vol., no., pp.1,4, 24-26 April 2013.

▪ Cicek, I.; Pusane, A.E.; Dundar, G., "Field programmable analog array implementation of logistic map," 2013 21st Signal Processing and Communications Applications Conference (SIU), vol., no., pp.1,4, 24-26 April 2013.

▪ Cicek, I.; Pusane, A.E.; Dundar, G.; , "A feasibility study of a 1D chaotic map for True Random Number Generation," 2012 20th Signal Processing and Communications Applications Conference (SIU), vol., no., pp.1-4, 18-20 April 2012.

▪ Cicek, I.; Dundar, G.; , "A hardware efficient chaotic ring oscillator based true random number generator," 2011 18th IEEE International Conference on Electronics, Circuits and Systems (ICECS), vol., no., pp.430-433, 11-14 Dec. 2011.

▪ Cicek, I.; Bozkurt, A.; Karaman, M.; , "Design of a front-end integrated circuit for 3D acoustic imaging using 2D CMUT arrays," IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control, vol.52, no.12, pp.2235-2241, Dec. 2005.

▪ Cicek, I.; Bozkurt, A.; Karaman, M.; , "Transmit/receive front-end electronics for 3D acoustic imaging," Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, vol., no., pp. 438-441, 28-30 April 2004.

CERTIFIED TECHNICAL TRAININGS

2015	▪ Riscure Side Channel Attack Training
	▪ Ergonomy Training
	▪ Embedded Linux on Raspberry Pi Training
2014	▪ Embedded Linux on Beaglebone Black Training
2013	▪ Ansoft SIwave EMC/EMI Simulation Training
	▪ Mentor Graphics High-speed Fundamentals Training
	▪ Mentor Graphics Signal Integrity Analysis using Hyperlynx Training
	▪ Mentor Graphics Advanced High-speed PCB Analysis using Hyperlynx Training
	▪ Xilinx HLS & Vivado for Xilinx 7 series FPGAs Training
2012	▪ Altium Designer Training
2011	▪ Reliasoft RS490 Standards Based Reliability Prediction Training
	▪ Reliasoft RS522 Training Seminar Advanced System Reliability/Maintainability Analysis Training
2010	▪ Programmable Logic Competence Center FPGA Training (www.plc2.de) Xilinx Spartan-6 / Virtex-6
	▪ Programmable Logic Competence Center FPGA Training (www.plc2.de) Implementation of DSP Algorithms on FPGA
2008	▪ HP Project Management Fundamentals Training
2007	▪ Microsoft Project Training
2005	▪ EMC aware PCB Design Training
	▪ Frequency Modulated Continuous Wave Radar Training

TECHNICAL SKILLS

Operating Systems	▪ MS-Windows (Advanced)
	▪ Unix / Linux (Intermediate)
Office Software	▪ MS-Office (Word, Excel, Powerpoint, Project)
	▪ Open Office
	▪ Latex
CAD/EDA Software	▪ Cadence Integrated Circuit Design Framework Software (Composer, Virtuoso, Spectre, Diva etc.)
	▪ Mentor Graphics FPGA Design Software (Modelsim, Precision RTL, HDL Designer)

	▪ Mentor Graphics Hyperlynx Signal Integrity ▪ Xilinx ISE and EDK (XPS, SDK) Software ▪ Cadence Allegro (Schematic, Layout Plus, Pspice) ▪ Altium Designer ▪ Microchip MPLAB IDE ▪ KEIL Embedded IDE ▪ HITEC PICC
Programming Languages	▪ C for Embedded Systems (Keil ARM, C51 and HITEC PICC) ▪ Verilog HDL
Mathematical Software	▪ Matlab, Mathematica, Python
Lab Equipment	▪ Oscilloscope (Agilent 54622D, Tektronix MSO4034, TDS3052B) ▪ Function Generator (Agilent 33120A, 33250A, Tektronix AFG3102) ▪ Spectrum Analyzer (Agilent E4407B) ▪ Impedance Analyzer (Agilent 4294A) ▪ Power Analyzer (Agilent N6705B) ▪ Multimeter (Agilent 344401A, Fluke 87 V) ▪ Universal logic device programmers and JTAG emulators ▪ Soldering and rework stations (Weller WSP-80, WD-1, WRS1002X) ▪ Logic and Protocol Analyzer (Saleae Logic Pro, MSO4034, Bus Pirate)