Ahmet Can **Mert**

Research Assistant · Ph.D. Candidate

ahmetcanmert@sabanciuniv.edu http://people.sabanciuniv.edu/acmert/

Education

Sabanci University — *Istanbul, Turkey*

Ph.D. in Electronics Engineering — *Sept. 2017 - Current*

- GPA: 4.00/4.00
- Dissertation: "High Performance FPGA-Based Co-Processor Design for Lattice-Based Cryptography with a Hardware-Software Co-Design Approach" supervised by Prof. Erkay Savas and Assist. Prof. Erdinc Ozturk

Sabanci University — *Istanbul, Turkey*

M.Sc. in Electronics Engineering — *Sept. 2015 - June 2017*

- GPA: 4.00/4.00
- Thesis: "High Performance HEVC and FVC Video Compression Hardware Designs" supervised by Assoc. Prof. Ilker Hamzaoglu

Sabanci University — *Istanbul, Turkey*

B.Sc. in Electronics Engineering — *Sept. 2010 - June 2015*

- GPA: 3.95/4.00 (ranked as 3^{rd})
- Senior Project: "A GPS-based Tracking and Accident Reporting System"

Research Experience

Sabanci University — *Istanbul, Turkey*

Full-Time Research Assistant at Electronics Engineering Program — *May 2017 - Current*

- **Research Group:** CISEC – Cryptography & Information Security Group (Advisor: Prof. Erkay Savaş & Assist. Prof. Erdinç Öztürk)
- I am a member of Cryptography & Information Security Group at Sabanci University since 2017. My research interests include designing accelerators for lattice-based cryptography and homomorphic encryption.

North Carolina State University — *Raleigh, NC, USA*

Visiting Scholar at ECE Department — *June 2019 - Sept. 2019*

- **Research Group:** HECTOR – Hardware and Embedded Cybersecurity Research (Supervisor: Assist. Prof. Aydin Aysu)
- I worked as a visiting scholar under the supervision of Dr.Aydin Aysu in HECTOR Lab. My research area was designing hardware accelerators for homomorphic encryption applications.

Sabanci University — *Istanbul, Turkey*

Scholar at TUBITAK Research Project — *Sept. 2015 - Aug. 2017*

- **Research Group:** SoCLab - System-on-Chip Design and Test Lab (Advisor: Assoc. Prof. Ilker Hamzaoglu)
- I was a member of System-on-Chip (SoC) Design and Test Lab. My main research focus was low-power digital hardware design for video compression algorithms. I worked as a scholarship holder in TUBITAK project titled "Low Power High Performance HEVC Video Compression Hardware Designs" for two years where I designed and implemented the hardware for transform, interpolation and motion estimation operations of H.256 (and upcoming VVC) video compression standard.

AVL Turkey — *Gebze, Kocaeli, Turkey*

Intern - Hardware Engineer — *June 2014 - Feb. 2015*

- I worked as a hardware engineer intern. I was part of a team responsible for the design, implementation and test of a motor control unit, an embedded system controlling an electronic motor, satisfying functional safety requirements.

Research Interests

- Lattice-Based Cryptography
- Post-Quantum Cryptography
- Homomorphic Encryption
- Digital Hardware Design, FPGAs

Skills

- **RTL Design**: Verilog HDL
- **Tools**: Xilinx XST/ISE/XPower/Vivado, ModelSim, Mentor Graphics Questa, Synopsys DC, Cadence Innovus/Virtuoso, LTSpice/PSpice
- **Programming**: C/C++, Python, MATLAB, CUDA, HTML/CSS, LaTeX
- **Computer**: MS Office, Linux, Windows, MAC OS
- **Language**: Turkish (Mother-tongue), English (Advanced)

Publications

Journal Articles

- **[7] A. C. Mert**, E. Ozturk, E. Savas, **"Low-Latency ASIC Algorithms of Modular Squaring of Large Integers for VDF Applications"**, *IEEE Transactions on Computers*, 2020 (early access).
- **[6] A. C. Mert**, E.Karabulut, E. Ozturk, E. Savas, A. Aysu, **"An Extensive Study of Flexible Design Methods for the Number Theoretic Transform"**, *IEEE Transactions on Computers*, 2020 (early access).
- **[5] A. C. Mert**, E. Ozturk, E. Savas, **"FPGA Implementation of a Run-time Configurable NTT-based Polynomial Multiplication Hardware"**, *Microprocessors and Microsystems*, vol. 78, 2020.
- **[4] A. C. Mert**, E. Ozturk, E. Savas, **"Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme"**, *IEEE Transactions on VLSI Systems*, vol. 28, no. 2, Feb. 2020.
- **[3]** H. Azgin, **A. C. Mert**, E. Kalali, I. Hamzaoglu, **"Reconfigurable Intra Prediction Hardware for Future Video Coding"**, *IEEE Transactions on Consumer Electronics*, vol. 63, no. 4, Nov. 2017.
- **[2] A. C. Mert**, E. Kalali, I. Hamzaoglu, **"High Performance 2D Transform Hardware for Future Video Coding"**, *IEEE Transactions on Consumer Electronics*, vol. 63, no. 2, May 2017.
- **[1]** E. Kalali, **A. C. Mert**, I. Hamzaoglu, **"A Computation and Energy Reduction Technique for HEVC Discrete Cosine Transform"**, *IEEE Transactions on Consumer Electronics*, vol. 62, no. 2, May 2016.

Peer-Reviewed Conference Publications

- **[13]** F. Yaman, **A. C. Mert**, E. Ozturk, E. Savas, **"A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme"**, *Design, Automation & Test in Europe (DATE) Conference*, 2021. (accepted)
- **[12] A. C. Mert**, E. Karabulut, E. Ozturk, E. Savas, M. Becchi, A. Aysu, **"A Flexible and Scalable NTT Hardware: Applications from Homomorphically Encrypted Deep Learning to Post-Quantum Cryptography"**, *Design, Automation & Test in Europe (DATE) Conference*, Mar. 2020, Grenoble, France.
- **[11] A. C. Mert**, E.Ozturk, E. Savas, **"Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture"**, *Euromicro Conference on DSD*, Aug. 2019, Kallithea, Greece.
- **[10] A. C. Mert**, H.Azgin, E. Kalali, I. Hamzaoglu, **"Novel Approximate Absolute Difference Hardware"**, *Euromicro Conference on DSD*, Aug. 2019, Kallithea, Greece.
- **[9] A. C. Mert**, E. Kalali, I. Hamzaoglu, **"A Low Power Versatile Video Coding Fractional Interpolation Hardware"**, *Conference on Design and Architecture for Signal and Image Processing (DASIP)*, Oct. 2018, Porto, Portugal.
- **[8] A. C. Mert**, H. Azgin, E. Kalali, I. Hamzaoglu, **"A Reconfigurable Fractional Interpolation Hardware for VVC Motion Compensation"**, *Euromicro Conference on Digital System Design (DSD)*, Aug. 2018, Prague, Czech Republic.
- **[7] A. C. Mert**, H. Azgin, E. Kalali, I. Hamzaoglu, **"Efficient Multiple Constant Multiplication Using DSP Blocks in FPGA"**, *International Conference on Field Programmable Logic and Applications, (FPL)*, Aug. 2018, Dublin, Ireland.
- **[6] A. C. Mert**, E. Kalali, I. Hamzaoglu, **"An HEVC Fractional Interpolation Hardware Using Memory Based Constant Multiplication"**, *IEEE International Conference on Consumer Electronics*, Jan. 2018, Las Vegas, USA.
- **[5]** H. Azgin, **A. C. Mert**, E. Kalali, I. Hamzaoglu, **"An Efficient FPGA Implementation of HEVC Intra Prediction"**, *IEEE International Conference on Consumer Electronics*, Jan. 2018, Las Vegas, USA.
- **[4] A. C. Mert**, E. Kalali, I. Hamzaoglu, **"An FPGA Implementation of Future Video Coding 2D Transform"**, *ICCE – Berlin*, Sep. 2017, Berlin, Germany.
- **[3] A. C. Mert**, I. Hamzaoglu, **"Pixel Correlation Based Computation and Energy Reduction Techniques for HEVC Fractional Interpolation"**, *ICCE – Berlin*, Sep. 2017, Berlin, Germany.
- **[2] A. C. Mert**, E. Kalali, I. Hamzaoglu, **"Low Complexity HEVC Sub-Pixel Motion Estimation Technique and Its Hardware Implementation"**, *ICCE – Berlin*, Sep. 2016, Berlin, Germany.
- **[1]** B. Soner, A. Icke, **A. C. Mert**, U. Basaran, S. T. Impram, I. Sahin, **"Development of an electronic control unit for PMSM drives in automotive applications"**, *ELECO*, Nov. 2015, Bursa, Turkey.

Activities & Awards

Scholarships & Awards

Student, Sabanci University

- 2020 - **Best Paper Award** in Design, Automation and Test in Europe (DATE) Conference
- 2019 - IACR **Student Travel Support** for Conference on Cryptographic Hardware and Embedded Systems (CHES)
- 2017 - **Full Graduate Scholarship**, Sabanci University Electronics Engineering Ph.D. Program
- 2015 - **Full Graduate Scholarship**, Sabanci University Electronics Engineering Master Program
- 2012 - Sabanci University **Extracurricular Student Activity Award**
- 2010 - **Sakip Sabanci Scholarship**, Sabanci University for ranking 358^{th} among 1.5 million participants in the Nationwide University Entrance Exam in 2010

Service to Scientific Community

Reviewer

- I reviewed two papers for **IEEE Transactions on Circuits and Systems II: Express Briefs** (IF:2.8, h5-index:44)
- I reviewed one paper for **IEEE Transactions on Emerging Topics in Computing** (IF:6.0, h5-index:41)
- I reviewed one paper for **IEEE Transactions on Information Forensics and Security** (IF:6.0, h5-index:86)
- I reviewed one paper for **Journal of Cryptographic Engineering (JCEN)** (IF:1.6, h5-index:19)
- I reviewed one paper for **2021 IEEE International Symposium on Circuits & Systems (ISCAS)** (h5-index:11)
- I reviewed two papers for **2019 International Conference on Reconfigurable Computing and FPGAs (ReConFig 2019)** (h5-index:13)

Teaching

Teaching Assistant, Sabanci University *Sept. 2015 - Current*

- I taught classes at recitations and led lab sessions. I also helped course material, exam preparations and grading. List of classes:
  - EE58006 - Special Topics in EE: FPGA in Quantum Computing with Superconducting Qubits (Fall 2020)
  - EE401 - VLSI System Design I (Fall 2015,2016,2017)
  - EE310 - Hardware Description Languages (Spring 2016,2017,2019)
  - EE308 - Microcomputer Based System Design (Spring 2015,2019)
  - EE302 - Digital Integrated Circuits (Spring 2019)
  - CS303 - Logic and Digital System Design (Fall 2016,2017,2018,2019,2020)
  - ENS203 - Electronics Circuits I (Summer 2017)
  - MATH204 - Discrete Mathematics (Spring 2018)

Civic Involvement Project

Participant, Sabanci University (cip.sabanciuniv.edu) *2010*

- I was a volunteer at "Youth Movement in Informatics" Civil Involvement Project which includes visiting high school students weekly in order to educate them on informatics.

References

Prof. Erkay Savas, Dean of Faculty of Engineering and Natural Sciences, Sabanci University, Turkey (erkays [at] sabanciuniv.edu)

Asst. Prof. Erdinc Ozturk, Faculty Member at CS Program, Sabanci University, Turkey (erdinco [at] sabanciuniv.edu)

Asst. Prof. Aydin Aysu, Faculty Member at ECE Department, North Carolina State University, USA (aaysu [at] ncsu.edu)