Yarkin Doroz

Cybersecurity · High-Performance Computing · FPGA · Embedded Systems

53 William Street, Apt 3, Worcester, MA 01609, USA

+1-347-682-9787 | ydoroz@njit.edu | http://doroz.org | yarkindoroz

Summary

I am a Research Scientist in New Jersey Institute of Technology working on secure computation of regression algorithms. Prior to that, my Ph.D. research had a focus on implementation and **acceleration** of embedded cybersecurity software using **FPGAs** and **GPUs**. I have a solid experience on hardware, software, embedded system and multi-core designs of security protocols and applications over 8 years. Currently, I am looking for cybersecurity and embedded system design positions.

Education

Worcester Polytechnic Institute (WPI) *Worcester, USA*

Ph.D. in Electrical and Computer Engineering *Jan. 2012 - June. 2017*

- Ph.D. Title: New Approaches for Efficient Fully Homomorphic Encryption
- Research Assistant under supervision of Prof. Berk Sunar.

Sabanci University (SU) *Istanbul, Turkey*

M.S. in Computer Science and Engineering *Sept. 2009 - Dec. 2011*

- Teaching Assistant

Sabanci University (SU) *Istanbul, Turkey*

B.S. in Electronics Engineering *Sept. 2004 - June. 2009*

Skills

Software Programming	C/C++, C#, Assembly, Java, Python, Matlab, Sage
Software Tools	Microsoft Visual Studio, Eclipse, Git, GNU GCC, GNU Make, GNU Debugger,
Hardware Programming	Verilog, VHDL
Hardware Tools	Xilinx Vivado Design Suite, Xilinx ISE & XPS (EDK/SDK), Synopsys Design Compiler

Experience

New Jersey Institute of Technology *Newark, NJ*

Research Scientist *June 2017 - present*

- Implemented regression algorithms (probit, logistic, negative binomial and poisson regression) using homomorphic encryption. The algorithm is implemented using the Palisade library and developed a Server/Client model in order to compute heavy operations efficiently, i.e. matrix inversion. The prototype supports large database inputs (larger than 10,000) with many regression coefficients (larger than 10). The computation of regression algorithms homomorphically for large databases is achieved in couple minutes.

Ph.D. Research, Cybersecurity Lab (Prof. Berk Sunar) *Worcester, MA*

Research Assistant *Jan. 2012 - June. 2017*

- Conducted research on Fully Homomorphic Encryption Algorithms. The main focus was to accelerate FHE algorithms using **GPUs** and **FPGAs**. Also, I focused on new applications that can be implemented using FHE schemes and work on optimizations to take them one step closer to real-time implementations.
- Implemented AES and PRINCE algorithms homomorphically in CPU and GPU. The designs achieved significant **speedup** up to **2-3 orders of magnitude**.
- Designed and implemented million-bit and large polynomial multiplier (32K degree) in hardware using Number Theoretic Transform. The designs achieved **2-3 orders of magnitude speedup** compared to software implementations.
- Using the million-bit multiplier, I present the first full realization of FHE in hardware. It is realization of the Gentry-Halevi(GH) fully homomorphic encryption (FHE) scheme. I reduced the Recryption operation by an order of magnitude.

Intel Corp. *Hudson, MA*

Internship *May. 2015 - July. 2015*

- The focus of the internship is to design a hardware architecture to accelerate compression algorithms. The architecture is developed as a co-processor to be used by the Intel CPUs.

Security Lab. (Prof. Erkay Savaş) *Istanbul, Turkey*

Research/Teaching Assistant *Sept. 2009 - Dec. 2011*

- Implemented a Tate Pairing algorithm on an IBM processor Cell Blade using C/C++ that is optimized and **parallelized** for the **multi-core** functionality. **Single Instruction, Multiple Data (SIMD) instructions** are used to achieve a higher throughput for the Tate Pairing operation.
- Designed an **FPGA cluster** infrastructure that can be utilized in implementing cryptanalytic attacks and accelerating cryptographic operations. The FPGA cluster was controlled by a server (PC) using a software interface through TCP/IP protocol. On the FPGA end, a soft-core processor Microblaze was used to handle TCP/IP protocols.

Publications

Journals

- Wei Dai, Wei Dai, Yarkın Doröz, Yuriy Polyakov, Kurt Rohloff, Hadi Sajjadpour, Erkay Savaş, Berk Sunar Implementation and Evaluation of a Lattice-Based Key Policy Attribute-Based Encryption Scheme. ***Transactions on Information Forensics and Security***, TIFS 2017.
- Yarkın Doröz, Berk Sunar, Flattening NTRU for Evaluation Key Free Homomorphic Encryption. (submitted to IEEE Designs, Codes and Cryptography 2016).
- Erdinç Öztürk, Yarkın Doröz, Berk Sunar, Erkay Savaş, A Custom Accelerator for Homomorphic Encryption Applications. ***IEEE Transactions on Computers,*** 2016.
- Yarkın Doröz, Yin Hu, Berk Sunar, Homomorphic AES Evaluation Using the Modified LTV Scheme. ***Designs, Codes and Cryptography,*** DCC 2015.
- Yarkın Doröz, Erdinç Öztürk, Berk Sunar, Accelerating Fully Homomorphic Encryption in Hardware. ***IEEE Transactions on Computers,*** 2014.
- Yarkın Doröz, Erdinç Öztürk, Berk Sunar, A Million-bit Multiplier Architecture for Fully Homomorphic Encryption. ***Microprocessors and Microsystems: Embedded Hardware Design,*** MICPRO 2014.

Conference

- Yarkın Doröz, Jeffrey Hoffstein, Joseph H. Silverman, Berk Sunar, Zhenfei Zhang, Fully Homomorphic Encryption from the Finite Field Isomorphism Problem, ***Public Key Cryptography***, PKC 2018.
- Gizem Selcan Çetin, Wei Dai, William J. Martin, Yarkın Doröz, Berk Sunar, Blind Web Search: How far are we from a privacy preserving search engine? ***Eprint Archive 2016***.
- Gizem Selcan Çetin, Wei Dai, Yarkın Doröz, Berk Sunar, Homomorphic Autocomplete. ***Eprint Archive 2016***.
- Gizem Selcan Çetin, Yarkın Doröz, Berk Sunar, William J. Martin, Arithmetic Using Word-wise Homomorphic Encryption. (presented in ArcticCrypt 2016).
- Yarkın Doröz, Gizem Selcan Çetin, Berk Sunar, On-the-fly Homomorphic Batching/Unbatching. ***Workshop on Applied Homomorphic Cryptography and Encrypted Computing,*** WAHC 2016.
- Yarkın Doröz, Erdinç Öztürk, Berk Sunar, Erkay Savaş, Accelerating LTV Based Homomorphic Encryption in Reconfigurable Hardware. ***Cryptographic Hardware and Embedded Systems,*** CHES 2015.
- Gizem Selcan Çetin, Yarkın Doröz, Berk Sunar, Erkay Savaş, Depth Optimized Efficient Homomorphic Sorting. ***Latincrypt,*** 2015.
- Wei Dai, Yarkın Doröz, Berk Sunar, Accelerating SWHE based PIRs using GPUs. ***Applied Homomorphic Cryptography and Encrypted Computing,*** WAHC 2015.
- Yarkın Doröz, Aria Shahverdi, Thomas Eisenbarth, Berk Sunar, Toward Practical Homomorphic Evaluation of Block Ciphers Using Prince. ***Workshop on Applied Homomorphic Cryptography and Encrypted Computing,*** WAHC 2014.
- Yarkın Doröz, Berk Sunar, Ghaith Hammouri, Bandwidth Efficient PIR from NTRU. ***Workshop on Applied Homomorphic Cryptography and Encrypted Computing,*** WAHC 2014.
- Wei Dai, Yarkın Doröz, Berk Sunar, Accelerating NTRU based Homomorphic Encryption using GPUs. ***IEEE High Performance Extreme Computing,*** HPEC 2014.
- Ciara Moore, Máire O'Neil, Elizabeth O'Sullivan, Yarkın Doröz, Berk Sunar, Practical homomorphic encryption: A survey. ***IEEE International Symposium on Circuits and Systems,*** ISCAS 2014.
- Yarkın Doröz, Erdinç Öztürk, Berk Sunar, Evaluating the Hardware Performance of a Million-bit Multiplier. ***Digital System Design (DSD)***, Euromicro 2013.
- Yarkın Doröz, Erkay Savaş, Constructing Cluster of Simple FPGA boards for Cryptologic Computations. ***International Symposium on Applied Reconfigurable,*** ARC 2012.

References

Berk Sunar, Worcester Polytechnic Institute sunar@wpi.edu

Kurt Rohloff, New Jersey Institute of Technology rohloff@njit.edu

Jeffrey Hoffstein, Brown University jhoff@math.brown.edu

Erkay Savaş, Sabanci University erkays@sabanciuniv.edu