Yarkin **Doroz**

Security Researcher · Post-Quantum Cryptography · Homomorphic Encryption · Hardware Design

53 William Street, Apt 1, Worcester, MA 01609, USA

☎ +1-347-682-9787 | ✉ yarkindoroz@gmail.com | doroz.org | yarkindoroz

Summary

I am a Security Researcher with more than 12 years of experience. My research area includes **Fully Homomorphic Encryption**, **Post-Quantum Cryptography**, and **Hardware/Software Accelerators**. I am one of the **co-founders** of **QuantumSafe** which is a Post-Quantum Blockchain startup for securing blockchains against quantum computers. Prior to that, I worked as a researcher in implementation and acceleration of Fully Homomorphic Encryption Algorithms on FPGA and GPU platforms, and in secure computation of machine learning algorithms using homomorphic encryption. I have solid experience on hardware, software and multi-core designs of security protocols and applications over 12 years. I published numerous peer-reviewed academic papers in prestigious conferences and journals.

Experience

Worcester Polytechnic Institute — *Worcester, MA*

Consultant / Assistant Teaching Professor — *September 2018 - present*

- Designing **hardware accelerator** for **T-FHE** bootstrapping algorithm (work in progress).
- Implementated **side-channel fault attacks** on most popular TLS libraries to recover ECDSA and RSA keys from a server as a client.
- Received NSF grant as a co-PI for Next-Gen Post-quantum Schemes ($\$600K$).
- Expert witness in patent infringement cases.
  - Perform forensic analysis on devices by capturing network traffic using Wireshark.
  - Forensic analysis of Bluetooth and Bluetooth LE traffic between devices using ubertooth.
- Constructed an Ethereum rig and performed a hardware/software analysis to **increase performance of the hash calculations**.
- Implemented SHA-256 for performance analysis of Bitcoin using Nvidia GPUs (Cuda-C).

QuantumSafe — *MA*

Co-founder/Researcher — *January 2019 - June 2021*

- Worked with a research team to design efficient **post-quantum** cryptographic algorithms for blockchain applications.
- Developed prototypes for the cryptographic libraries.
- Win a spot at Alchemist Accelerator (startup accelerator program).
- Performed many fund raising, pitch and networking activities.

New Jersey Institute of Technology — *Newark, NJ*

Research Scientist — *June 2017 - August 2018*

- Implemented **machine learning** algorithms (probit, logistic, negative binomial and poisson regression) using homomorphic encryption.
- Developed a Server/Client model for computation of homomorphic encryption and implemented on C++ and Python (wrapper).

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

Research Assistant — *Jan. 2012 - June. 2017*

- Designed **acceleration** techniques for Fully Homomorphic Encryption Algorithms using **GPUs** and **FPGAs**.
- Implemented a lattice-based Attribute-Based Encryption (ABE) scheme using GPU.
- Designed and implemented million-bit and large polynomial multipliers using **Fast Fourier Transform** in hardware. The designs achieved **2-3 orders of magnitude speedup** compared to software implementations.
- Implemented many algorithms in FHE: homomorphic AES/PRINCE, homomorphic sort, blind search, and homomorphic autocomplete.
- Introduced a new mathematical hard problem based on the secret finite field isomorphism (FFI) which can be used for cryptographic scheme constructions. Also, construct a fully homomorphic public-key encryption scheme using FFI problem.

Intel Corp. — *Hudson, MA*

Internship — *May. 2015 - July. 2015*

- Designed 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 paralellized Tate Pairing algorithm on an IBM processor Cell Blade using **SIMD**.
- Designed an **FPGA cluster** infrastructure that utilizes cryptanalytic attacks or accelerates cryptographic operations over TCP/IP protocols.

Skills

Software Programming	C/C++, C#, Assembly, Nvidia Cuda-C/C++, Java, Python, Matlab, Sage, Solidity
Software Tools	Microsoft Visual Studio, Eclipse, Git, CCS, GNU GCC, GNU Make, GNU Debugger, Wireshark, OllyDbg
Hardware Programming	Verilog, VHDL
Hardware Tools	Xilinx Vivado Design Suite/Vitis, Synopsys Design Compiler

Education

Worcester Polytechnic Institute (WPI) *Worcester, USA*

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

Sabanci University (SU) *Istanbul, Turkey*

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

Sabanci University (SU) *Istanbul, Turkey*

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

Publications

Google Scholar Citation: 845 H-Index: 16

Journals

1. Y. Doröz, J. Hoffstein, J. H. Silverman, B. Sunar, **MMSAT: A Scheme for Multimessage Multiuser Signature Aggregation.** *Eprint*, 2020.
2. Y. Doröz, B. Sunar, **Flattening NTRU for Evaluation Key Free Homomorphic Encryption.** *Journal of Mathematical Cryptology*, 2020.
3. W. Dai, Y. Doröz, Y. Polyakov, K. Rohloff, H. Sajjadpour, E. Savaş, B. Sunar, **Implementation and Evaluation of a Lattice-Based Key Policy Attribute-Based Encryption Scheme.** *Transactions on Information Forensics and Security*, 2017.
4. E. Öztürk, Y. Doröz, B. Sunar, E. Savaş, **A Custom Accelerator for Homomorphic Encryption Applications.** *IEEE Tran. on Computers,* 2016.
5. Y. Doröz, Y. Hu, B. Sunar, **Homomorphic AES Evaluation Using the Modified LTV Scheme.** *Designs, Codes and Cryptography,* 2015.
6. Y. Doröz, E. Öztürk, B. Sunar, **Accelerating Fully Homomorphic Encryption in Hardware.** *IEEE Transactions on Computers,* 2014.
7. Y. Doröz, E. Öztürk, B. Sunar, **A Million-bit Multiplier Architecture for Fully Homomorphic Encryption.** *Microprocessors and Microsystems: Embedded Hardware Design,* MICPRO 2014.

Conference

1. K. Mus, Y. Doröz, C. Tol, K. Rahman, B. Sunar, **Jolt: Recovering TLS Signing Keys via Rowhammer Faults.** *(under review)*.
2. Y. Doröz, J. Hoffstein, J. H. Silverman, B. Sunar, Z. Zhang, **Fully Homomorphic Encryption from the Finite Field Isomorphism Problem.** *Public Key Cryptography*, 2018.
3. G. S. Çetin, W. Dai, W. Martin, Y. Doröz, B. Sunar, **Blind Web Search: How far are we from privacy preserving search engine?** *Eprint*, 2016.
4. G. S. Çetin, W. Dai, Y. Doröz, B. Sunar, **Homomorphic Autocomplete.** *Eprint,* 2016.
5. G. S. Çetin, Y. Doröz, B. Sunar, W. Martin, **Arithmetic Using Word-wise Homomorphic Encryption.** *ArcticCrypt*, 2016.
6. Y. Doröz, G. S. Çetin, B. Sunar, **On-the-fly Homomorphic Batching/Unbatching.** *Workshop on Applied Homomorphic Cryptography and Encrypted Computing*, 2016.
7. Y. Doröz, E. Öztürk, B. Sunar, E. Savaş, **Accelerating LTV Based Homomorphic Encryption in Reconfigurable Hardware.** *Cryptographic Hardware and Embedded Systems*, 2015.
8. G. S. Çetin, Y. Doröz, B. Sunar, E. Savaş, **Depth Optimized Efficient Homomorphic Sorting.** *Latincrypt,* 2015.
9. W. Dai, Y. Doröz, B. Sunar, **Accelerating SWHE based PIRs using GPUs.** *Applied Homomorphic Cryptography & Encrypted Computing*, 2015.
10. Y. Doröz, A. Shahverdi, T. Eisenbarth, B. Sunar, **Toward Practical Homomorphic Evaluation of Block Ciphers Using Prince.** *Workshop on Applied Homomorphic Cryptography and Encrypted Computing*, 2014.
11. Y. Doröz, B. Sunar, G. Hammouri, **Bandwidth Efficient PIR from NTRU.** *Workshop on Applied Homomorphic Crypt. & Enc. Computing*, 2014.
12. W. Dai, Y. Doröz, B. Sunar, **Accelerating NTRU based Homomorphic Encryption using GPUs.** *IEEE High Perf. Extreme Computing*, 2014.
13. C. Moore, Máire O'Neil, E. O'Sullivan, Y. Doröz, B. Sunar, **Practical homomorphic encryption: A survey.** *IEEE International Symposium on Circuits and Systems,* 2014.
14. Y. Doröz, E. Öztürk, B. Sunar, **Evaluating the Hardware Performance of a Million-bit Multiplier.** *Digital System Design, Euromicro*, 2013.
15. Y. Doröz, E. Savaş, **Constructing Cluster of Simple FPGA boards for Cryptologic Computations.** *International Symposium on Applied Reconfigurable,* 2012.

Presentations

International Workshop on Post-quantum Cryptography - IWPQC *Online*

New Applications Based On PQ-Schemes *Dec. 2021*

Cryptographic Hardware and Embedded Systems 2015 *Saint-Malo, France*

Accelerating LTV Based Homomorphic Encryption in Reconfigurable Hardware *Sept. 2015*

Workshop on Applied Homomorphic Cryptography and Encrypted Computing 2014 *Barbados*

Bandwidth Efficient PIR from NTRU *March 2014*

Euromicro 2013 *Santander, Spain*

Evaluating the Hardware Performance of a Million-bit Multiplier *Sept. 2013*