Kamyar Mohajerani

PhD Student

Interests

- Digital Design
- Cryptography
- Post-Quantum Cryptography
- Side-Channel Analysis
- Electronic Design Automation
- Embedded Systems
- System-on-Chip
- Hardware Accelerators
- Hardware Security
- Computer Architecture
- Low-Power Design

Contact

9537 Barkwood Ct
Fairfax VA 22032
kamyar@ieee.org
703.832.2648
kammoh
kammoh
kamyar.xyz
kamyar....
3D9C D145 64DB 057A

Education

- PhD in Electrical & Computer Engineering . . . . . Sep 2017 – Present
  George Mason University, Fairfax, VA
  • Computer Arithmetic • Advanced Algorithms • Microprocessor Architecture • Machine Learning
  • Digital System Design • Applied Cryptography • VLSI • Distributed Systems
- Master of Science in Computer Architecture . . . . . Sep 2012 – Sep 2016
  University of Tehran, Tehran, Iran
  Thesis: An Action-Oriented Approach to Hardware Description and Synthesis
  (Proposed and implemented an HDL, integrating Bluespec atomic-actions into Chisel eDSL)
- Bachelor of Science in Computer Engineering . . . . . Sep 2006 - Sep 2012
  Isfahan University of Technology, Isfahan, Iran

Experience

- Research Assistant . . . . . Jan 2019 – Present
  Cryptographic Engineering Research Group (CERG)
  George Mason University, Fairfax, VA
  • Performed FPGA benchmarking of 26 LWC candidates in terms of performance, area, and energy
  • Developed VHDL and Bluespec implementations of Round 2 LWC candidates:
  Ascon, GIFT-COFB, Gimli, Grain, Sparkle, Subterranean, and Xoodyak
  • Developed high-speed hardware implementation of the NIST PQC finalist CRYSTALS-Kyber
  • Contributed to the grant proposal on RISC-V instruction-set extensions & accelerators for PQC
  • Developed Xeda: a Cross-EDA automation tool (used in LWC FPGA benchmarking)
  • Contributed to LWC Hardware API Development Package
- Teaching Assistant . . . . . Aug 2017 – Dec 2018
  George Mason University, Fairfax, VA
  • Digital Design Course & Lab, Cybersecurity
- Developer . . . . . Oct 2015 – May 2016
  Research Institute for Robotics, AI, and Information Science, Tehran, Iran
  • Developed a data-center HVAC monitoring and control unit with web interface (RaspberryPi/C++)
- Project Lead . . . . . Sep 2014 – Oct 2015
  iWin Eng. Co., Tehran, Iran
  • Led the development team of a high-performance Hardware Security Module
- Developer . . . . . Mar 2014 – Sep 2014
  iWin Eng. Co., Tehran, Iran
  • Developed high-speed implementation of configurable Elliptic-curve cryptography (ECC) processor
  • Developed high-speed FPGA implementations of AES (CTR/CFB/OFB/CBC) and 3DES
  • Developed network PKCS11 client/server, Zynq-based server utilizing Arm TrustZone/TEE
  • Developed verification harness for hardware cryptographic implementations
- Developer . . . . . Mar 2009 – Jan 2013
  Padid-Avaran Narmafzar Apadana (PANA), Isfahan, Iran
  • Network-tap and VPN tunnel Linux kernel modules • High-availability UTM

Skills

Python	Rust	C++
VHDL	SystemVerilog	Bluespec
Scala/Chisel	FPGAs	ASIC flows
Linux	RISC-V	Tcl/sh

References

Kris Gaj, PhD
George Mason University
kgaj@gmu.edu

Jens-Peter Kaps, PhD
George Mason University
jkaps@gmu.edu