JASON GOERTZEN

jason.goertzen@uwaterloo.ca
https://goertzen.dev
https://github.com/martyrshot

SUMMARY

An extremely passionate and performance-driven software engineer with experience developing and maintaining bleeding edge open-source cryptographic libraries as well as conceptualizing, implementing, and experimenting with protocol changes to the Domain Name System. Having completed my Master of Mathematics in Computer Science in Fall 2022, I am looking for career opportunities to apply my expertise in designing and developing novel solutions to complex problems.

EDUCATION

Master of Mathematics
Thesis: Enabling Post-Quantum Signatures in DNSSEC: One ARRF at a time
University of Waterloo, Computer Science — **December 2022**
Advisor: Douglas Stebila

Bachelor of Science (Honours)
University of Saskatchewan, Computer Science — **May 2020**
Graduated with High Honours

Bachelor of Science (3 Year)
University of Saskatchewan, Mathematics — **May 2019**
Graduated with Great Distinction

PUBLICATIONS

Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation
Jason Goertzen, *Douglas Stebila* — **November 2022**
Preprint ArXiv

Densities of bounded primes for hypergeometric series with rational parameters
Cameron Franc, Brandon Gill, ***Jason Goertzen****, Jarrod Pas, Frankie Tu* — **March 2020**
Research in Number Theory

Illuminating the Hidden Elements and Future Evolution of Opioid Abuse using Dynamic Modeling
Xiaoyan Li, Bryce Keeler, Rifat Zahan, Lujie Duan, Anahita Safarishahrbijari, ***Jason Goertzen****, Yuan Tian, Juxin Liu, Nathaniel Osgood* — **July 2018**
SBP-BRiMS 2018

PROJECTS AND EXPERIENCE

University of Waterloo
Research Assistant; — **September2020-December 2022**

Applying post-quantum cryptography to DNSSEC

- Designed protocol changes to DNS to achieve a 20% performance improvement in delivering post-quantum signatures in a reliable manner
- Used OpenSSL to add Falcon-512, CRYSTALS-Dilithium2, and SPHINCS+-128s support into a forked version of BIND9 DNS software
- Designed and built a C based daemon to intercept DNS traffic and implement protocol changes transparently using raw UDP sockets and libnetfilter-queue
- Constructed a DNS testing environment using Docker to evaluate protocol modifications
- Collaborated with DNS experts to maximize backwards compatibility

Open Quantum Safe

- Integrated ARMv8 optimized implementations of SHA-2 suite of hashing algorithms and CRYSTALS-Dilithium and CRTYSTALS-KYBER post-quantum algorithms into the open-source C based library liboqs
- Updated Python3 build scripts to support pulling post-quantum algorithms from multiple upstreams
- Added CPU extension detection for FreeBSD into open-source library
- Extended Open Quantum Safe's OpenSSL fork to support exporting keys as bytes through the OpenSSL API

Computational Epidemiology and Public Health Informatics Laboratory (CEPHIL)
Undergraduate Research Assistant **January 2018-September 2020**

COVID-19 Model Pipeline

- Constructed an automated model pipeline for generating reports daily to be sent to the Saskatchewan Health Authority and Public Health Agency of Canada
- Greatly reduced the amount of manual effort required to initiate and aggregate results
- Used a combination of Python3 and Bash scripts to distribute models across multiple servers to maximize parallelization and constructed an automated archival system using Python3 and git
- Teamed up with machine learning and infrastructure experts to deliver pipeline features for the modeling team

Fully Homomorphic Encryption (FHE) FPGA Experimentation

- Primary researcher for evaluating the feasibility of FHE
- Implemented BFV FHE scheme's multiplication operation using OpenCL, for Intel FPGAs
- Performed a security analysis relating RSA's security level to BFV's equivalent security level
- Constructed several C-based proof of concept applications to evaluate FHE feasibility

University of Saskatchewan Cyber Security Team
Founding President **September 2017-April 2020**

- Founded student run competitive hacking club focusing on education and awareness of cybersecurity
- Utilized hacking competitions and challenges to reenforce various cybersecurity topics
- Responsible for planning and organizing weekly meetings, recruiting, and onboarding new members, and coordinating with other club executives
- Networked and interfaced with potential club sponsors, and spoke at sponsored events
- While president team was ranked the third best competitive hacking team in Canada

University of Saskatchewan
Teaching Assistant **September 2019-April 2020**

- Led and designed labs for senior level courses including Operating Systems and Programming Paradigms