Scott Griffy

✉ *scottgriffy@gmail.com*
🌐 *scottgriffy.com*
Updated: Sep 25, 2024

Publications

ASIACRYPT 2024 — **Delegatable Anonymous Credentials From Mercurial Signatures With Stronger Privacy**, *Scott Griffy, Anna Lysyanskaya, Omid Mir, Octavio Pérez Kempner, and Daniel Slamanig*, ASIACRYPT 2024, Conference paper
`https://iacr.org/cryptodb/data/paper.php?pubkey=34667`

CIC 2024 — **PACIFIC: Privacy-preserving automated contact tracing scheme featuring integrity against cloning**, *Scott Griffy and Anna Lysyanskaya*, IACR Communications in Cryptography (CIC) Issue 1 Volume 2, Journal paper
`https://cic.iacr.org/p/1/2/12`

FC 2024 — **SoK: Signatures With Randomizable Keys**, *Sofía Celi, Scott Griffy, Lucjan Hanzlik, Octavio Perez Kempner, Daniel Slamanig*, Financial Cryptography and Data Security 2023, Conference paper
`https://eprint.iacr.org/2023/1524`

ACM CCS 2023 — **Aggregate signatures with versatile randomization and issuer-hiding multi-authority anonymous credentials**, *Omid Mir, Balthazar Bauer, Scott Griffy, Anna Lysyanskaya, Daniel Slamanig*, ACM Conference on Computer and Communications Security 2023, Conference paper
`https://eprint.iacr.org/2023/1016`

Patent 2021 — **Circuitry And Methods For Supporting Encrypted Remote Direct Memory Access (ERDMA) For Live Migration Of A Virtual Machine**, *Scott Griffy, David Bronleewe, Hormuzd Khosravi, Siddhartha Chhabra*, Patent, Status: Pending, Application US17/359,117
`https://patents.google.com/patent/US20220413886A1`

DIMACS 2020 — **Abradable Key Wrapping**, *Scott Griffy, Charles V. Wright, Mayank Varia*, DIMACS Workshop on Co-Development of Computer Science and Law, Poster session and lightning talk
`http://dimacs.rutgers.edu/events/details?eID=1787`

IEEE DSN 2019 — **The Strength of Weak Randomization: Easily Deployable, Efficiently Searchable Encryption with Minimal Leakage**, *David Pouliot, Scott Griffy, and Charles V. Wright*, 49th IEEE/IFIP International Conference on Dependable Systems and Networks, Conference paper
`https://eprint.iacr.org/2017/1098`

Master's Thesis 2019 — **Crumpled and Abraded Encryption: Implementation and Provably Secure Construction**, *Scott Griffy*, Portland State University Master's Thesis, Advisor: Charles V. Wright
`https://pdxscholar.library.pdx.edu/compsci_fac/242/`

Education

2021 to current — **PhD, Computer Science**, *Brown University*, Providence, RI, *3.83 GPA*
- Advisor: Anna Lysyanskaya
- Taking classes on cryptography, probability, and algebra.
- Researching anonymous credentials and structure-preserving signatures.
- Running a cryptography reading group.

2017 to 2019 — **Master of Science, Computer Science**, *Portland State University*, Portland, OR, *3.95 GPA*
- Advisor: Charles V. Wright
- Took classes in computer security and cryptography.
- Researched searchable encryption, co-authoring a paper at DSN 2019.
- Defended my thesis relating to exceptional access in June, 2019.
- Wrote an educational Windows 10 32-bit rootkit that included a keylogger.
- Helped create the Portland State University video game development club.
- Configured and performed database benchmarks such as TPC-C and SPARTA, a framework from MIT Lincoln Laboratory.
- Wrote a script to crawl Github and put security related information in a PostgreSQL database.

2010 to 2016 **Bachelor of Science, Computer Science**, *Oregon State University*, Corvallis, OR, *3.0 GPA*

- Computer Systems Option, ABET Accredited
- Awarded best capstone project. This project used single board computers for computer vision.
- Member of the computer security club.
- Took classes on Applied Cryptography.
- Implemented a searchable encryption library on Android in C.
- Simulated and benchmarked GPUs running a cryptographic algorithm.

Service

September 2022 to present **Weekly Brown Crypto Reading Group Organizer**, *Brown University*, Providence, RI

Work experience

September 2021 to present **Research/Teaching Assistant**, *Brown University*, Providence, RI

- TA for cryptography.
- Researching cryptography and anonymous credentials.

July 2019 to July 2021 **Security Engineer/Researcher**, *Intel Corporation*, Hillsboro, OR

- Worked with memory encryption, virtualization-based security, nested virtualization, and other OS technologies.
- Debugging operating systems and hardware.
- Filed a patent.
- Wrote exploits for Intel products.
- Researching timing attacks through hardware power signal analysis.

September 2018 to June 2019 **Research/Teaching Assistant**, *Portland State University*, Portland, OR

- Designed new cryptographic protocols for privacy and exceptional access
- Worked on symbolic execution in ethereum contracts
- TA for computer security

June 2018 to September 2018 **Graduate Technical Intern**, *Intel Corporation*, Hillsboro, OR

- Developed a proof of concept, securing a virtual machine with new technologies
- Worked with memory encryption and TPMs
- Worked with Windows virtualization technologies

July 2016 to December 2016 **Software Contractor**, *Empirical Inc*, Portland, OR

- Added voice recognition to an existing python project
- Developed a test suite for a React/Redux web application

Skills

Programming Languages:
Java, C/C++, HTML/CSS, JavaScript, Node.js, PHP, SQL, Python, OpenGL, CUDA, Haskell

Utilities/Tools:
bash, git, ssh, Apache HTTP, ftp/scp, vim, Debian/Ubuntu, CentOS/Fedora, LaTeX, gdb, Metasploit, PowerShell, Visual Studio, Eclipse, WinDBG, Android SDK/NDK, PostgreSQL, Libvirt, qemu