Scott Griffy

scottgriffy@gmail.com
scottgriffy.com
Updated: Oct 31, 2024

Education

2021 to current — **PhD, Computer Science**, *Brown University*, Providence, RI, *3.83 GPA*
- Advisor: Professor Anna Lysyanskaya

2017 to 2019 — **Master of Science, Computer Science**, *Portland State University*, Portland, OR, *3.95 GPA*
- Advisor: Professor Charles V. Wright

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

Peer-reviewed conference 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

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

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

Peer-reviewed journal publications

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

Patents

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

Poster sessions and talks

Edinburgh 2024 — **Privacy-Preserving Blueprints via Succinctly Verifiable Computation over Additively-Homomorphically Encrypted Data**, *Scott Griffy, Markulf Kohlweiss, Anna Lysyanskaya, Meghna Sengupta*, ICMS Foundations and Applications of Zero-Knowledge Proofs, Lightning talk
https://www.icms.org.uk/ZeroKnowledgeProofs

Saarbrüken 2024 — **Delegatable Anonymous Credentials From Mercurial Signatures With Stronger Privacy**, *Scott Griffy, Anna Lysyanskaya, Omid Mir, Octavio Perez Kempner, Daniel Slamanig*, CISPA Summer School on Privacy-Preserving Cryptography, Poster session
https://cispa.de/summer-school-crypto

Online 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

Theses and capstones

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/`

Undergraduate capstone 2016 — **Image Processing Vision System for Manned and Unmanned Aircraft**, *Hailey Palmiter, Scott Griffy, and Ryan Kitchen*, Oregon State University Capstone Project

Pre-printed work

EPRINT 2024 — **Privacy-Preserving Blueprints via Succinctly Verifiable Computation over Additively-Homomorphically Encrypted Data**, *Scott Griffy, Markulf Kohlweiss, Anna Lysyanskaya, and Meghna Sengupta*, IACR Cryptology ePrint Archive, Pre-print
`https://eprint.iacr.org/2024/675`

Service and volunteering

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

Eurocrypt 2024 — **Subreviewer**

Asiacrypt 2024 — **Subreviewer**

CANS 2024 — **Subreviewer**

Crypto 2024 — **Subreviewer**

IMACC 2023 — **Subreviewer**

Crypto 2023 — **Volunteer**, Santa Barabara, CA

September 2018 to June 2019 — **Co-founder of student game development group**, *Portland State University*, Portland, OR

Work experience

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

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

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

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

March to June 2018 — **Quality Assurance Intern**, *Iovation*, Portland, OR

July 2017 to March 2018 — **Quality Assurance Analyst**, *PlusQA*, Portland, OR

September to November 2016 — **Student Mentor and Volunteer**, *PixelArts*, Portland, OR

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

July to September 2011 **Intern**, *Crowd Compass*, Portland, OR

July to September 2009 **Intern**, *RNA Networks*, Portland, OR