Scott Griffy

✉ *scottgriffy@gmail.com*
🌐 *scottgriffy.com*
Updated: Aug 12, 2025

Education

2021-2026 **PhD, Computer Science**, *Brown University*, Providence, RI
- Advisor: Professor Anna Lysyanskaya

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

2010-2016 **Bachelor of Science, Computer Science**, *Oregon State University*, Corvallis, OR

Conference publications

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`

2024 **SoK: Signatures With Randomizable Keys**, *Sofía Celi, Scott Griffy, Lucjan Hanzlik, Octavio Perez Kempner, Daniel Slamanig*, Financial Cryptography and Data Security 2024, Conference paper
`https://link.springer.com/content/pdf/10.1007/978-3-031-78679-2_9`

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://dl.acm.org/doi/10.1145/3576915.3623203`

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://ieeexplore.ieee.org/document/8809552`

Journal publications

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

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`

Talks and posters

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://icms.ac.uk/activities/workshop/foundations-and-applications-of-zero-knowledge-proofs/`

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`

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

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/open_access_etds/5067/`

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

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

2022- **Weekly Brown Crypto Reading Group Organizer**, *Brown University*, Providence, RI

2025 **Subreviewer and shepherd**, *CANS*

2025 **Subreviewer**, *Crypto*

2025 **PC Member**, *Priv-crypt*

2024 **Subreviewer**, *Eurocrypt*

2024 **Subreviewer**, *Asiacrypt*

2024 **Subreviewer**, *CANS*

2024 **Subreviewer**, *Crypto*

2023 **Subreviewer**, *IMACC*

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

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

Awards and Scholarships

2025- **Dissertation fellowship**, *Brown University*, Providence, RI

2021-2022 **Entrance fellowship**, *Brown University*, Providence, RI

2016 **Best capstone project**, *Oregon State University*, Portland, OR

2010-2014 **Diversity scholarship**, *Oregon State University*, Corvallis, OR

Work experience

2021- **Research/Teaching Assistant**, *Brown University*, Providence, RI

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

2018-2019 **Research/Teaching Assistant**, *Portland State University*, Portland, OR

2018 **Graduate Technical Intern**, *Intel Corporation*, Hillsboro, OR

2018 **Quality Assurance Intern**, *Iovation*, Portland, OR

2017-2018 **Quality Assurance Analyst**, *PlusQA*, Portland, OR

2016 **Student Mentor and Volunteer**, *PixelArts*, Portland, OR

2016 **Software Contractor**, *Empirical Inc*, Portland, OR

2011 **Intern**, *Crowd Compass*, Portland, OR

2009 **Intern**, *RNA Networks*, Portland, OR