

# Elizabeth C. Crites, Ph.D.

---


CONTACT INFORMATION      elizabeth\_crites@alumni.brown.edu  
elizabeth-crites.github.io


CITIZENSHIP      Canada, US, UK


CURRENT EMPLOYMENT       **Web3 Foundation**  
*Research Scientist*


PAST EMPLOYMENT       **The University of Edinburgh**, Edinburgh, UK  
*Research Associate*


 **Input Output (IOG/IOHK)**  
*Research Fellow*

 **University College London (UCL)**, London, UK  
*Research Fellow*

EDUCATION       **Brown University**, Providence, USA  
*Ph.D. & M.Sc. in Mathematics*  
Advisor: Anna Lysyanskaya

 **Columbia University in the City of New York**, New York, USA  
*M.Sc. in Applied Mathematics*  
Advisors: Richard S. Hamilton & Michael I. Weinstein

 **The University of Western Ontario**, London, Canada  
*B.Sc. Honours Specialization in Mathematics, with Distinction*

 **McGill University**, Montréal, Canada  
*Visiting Scholar, Honours Mathematics*

A full course list can be found [here](#).

AWARDS & SCHOLARSHIPS      Best Early Career Paper Award, CRYPTO 2023  
US Department of Veterans Affairs Scholarship  
Columbia University Admission Scholarship  
The University of Western Ontario Admission Scholarship

PUBLICATIONS      **On the Adaptive Security of FROST**  
Elizabeth Crites, Jonathan Katz, Chelsea Komlo, Stefano Tessaro, Chenzhi Zhu  
*Provable security of the FROST threshold signature scheme under adaptive corruptions.*  
CRYPTO 2025

**A Plausible Attack on the Adaptive Security of Threshold Schnorr Signatures**  
Elizabeth Crites, Alistair Stewart  
*A plausible efficient attack on adaptive security for large classes of threshold Schnorr signatures.*  
CRYPTO 2025

### **On the Adaptive Security of Key-Unique Threshold Signatures**

Elizabeth Crites, Chelsea Komlo, Mary Maller

*Impossibility results ruling out adaptive security for large classes of threshold signatures.*

*Under submission.*

### **Sybil-Resilient Anonymous Signatures with Applications to Decentralized Identity**

Elizabeth Crites, Markulf Kohlweiss, Aggelos Kiayias, Amirreza Sarencheh

*An approach to digital identity that is Sybil resilient, anonymous, non-interactive, and stateless.*

CCS 2025. <https://eprint.iacr.org/2024/379>

### **Sassafras: Efficient Batch Single Leader Election**

Jeffrey Burdges, Elizabeth Crites, Handan Kılınç Alper, Alistair Stewart, Sergey Vasilyev

*An efficient single leader election protocol from ring verifiable random functions.*

ACNS 2025. <https://eprint.iacr.org/2023/031>

### **Ring Verifiable Random Functions and Zero-Knowledge Continuations**

Jeffrey Burdges, Oana Ciobotaru, Elizabeth Crites, Handan Kılınç Alper, Alistair Stewart, Sergey Vasilyev

*Combining verifiable random functions and ring signatures for leader election and digital identity.*

*Under submission.* <https://eprint.iacr.org/2023/002>

### **Fully Adaptive Schnorr Threshold Signatures**

Elizabeth Crites, Chelsea Komlo, Mary Maller

*First Schnorr threshold signature scheme secure with maximum adaptive corruption.*

CRYPTO 2023. Best Early Career Paper Award. <https://eprint.iacr.org/2023/445>

### **Snowblind: A Threshold Blind Signature in Pairing-Free Groups**

Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, Chenzhi Zhu

*First threshold blind signature scheme in pairing-free groups.*

CRYPTO 2023. <https://eprint.iacr.org/2023/1228>

### **Threshold Structure-Preserving Signatures**

Elizabeth Crites, Markulf Kohlweiss, Bart Preneel, Mahdi Sedaghat, Daniel Slamanig

*First threshold structure-preserving signature scheme.*

ASIACRYPT 2023. <https://eprint.iacr.org/2022/839>

### **Better than Advertised Security for Non-Interactive Threshold Signatures**

Mihir Bellare, Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, Chenzhi Zhu

*Security analysis for the FROST and BLS threshold signature schemes.*

CRYPTO 2022. Springer link

### **How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures**

Elizabeth Crites, Chelsea Komlo, Mary Maller

*Efficient two- and three-round multi- and threshold Schnorr signatures.*

Results included in the FROST IRTF RFC 9591. <https://eprint.iacr.org/2021/1375>

### **Mercurial Signatures for Variable-Length Messages**

Elizabeth C. Crites, Anna Lysyanskaya

*Extended mercurial signatures to allow messages of unbounded length.*

PETS 2021. <https://eprint.iacr.org/2020/979>

## Reputable List Curation from Decentralized Voting

Elizabeth C. Crites, Mary Maller, Sarah Meiklejohn, Rebekah Mercer

*Constructed a token-curated registry from a voting protocol with ballot secrecy.*

PETS 2020. <https://eprint.iacr.org/2020/709>

## Delegatable Anonymous Credentials from Mercurial Signatures

Elizabeth C. Crites, Anna Lysyanskaya

*Constructed first efficient scheme for issuing, presenting, and delegating credentials anonymously.*

CT-RSA 2019. <https://eprint.iacr.org/2018/923>

### DOCTORAL DISSERTATION

## Delegatable Anonymous Credentials from Mercurial Signatures

*Introduced a new type of digital signature, called a mercurial signature, and constructed first efficient delegatable anonymous credential (DAC) scheme. Extended mercurial signatures to allow messages of unbounded length. Constructed DAC scheme for multiple certification authorities.*

Brown University Library 2019. <https://repository.library.brown.edu/studio/item/bdr:918764/>

### MASTER'S RESEARCH

*Conducted research on partial differential equations, such as mean curvature flow and the Ricci flow, used in Richard S. Hamilton's program for solving the Poincaré Conjecture (Millennium Prize Problem). Advisor: Richard S. Hamilton*

### ACTIVITIES AND SERVICE

## NIST Call for Multi-Party Threshold Schemes

Team member submitting to the U.S. National Institute of Standards and Technology (NIST) call for multi-party threshold schemes.

## Research Workshop on Foundations and Applications of Zero-Knowledge Proofs

Organizer, International Centre for Mathematical Sciences (ICMS), Edinburgh, 2024.

## CrossFyre 2024

Organizer, 13th International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers, EUROCRYPT Affiliated Event, Zurich, 2024.

## ZK-Lab

Member, The University of Edinburgh, 2023-2024.

## Program Committees

I am or have been a Program Committee member for EUROCRYPT 2025, ASIACRYPT 2024 (*Distinguished PC Members Award*), CRYPTO 2024, EUROCRYPT 2024, the 27th Information Security Conference (ISC 2024), the 1st Workshop on Proofs and Proof Techniques for Cryptographic Security (ProTeCS 2024), and the Institute of Mathematics and its Applications (IMA) International Conference on Cryptography and Coding (IMACC 2023).

I am or have been a reviewer for the following conferences and journals: CRYPTO, EUROCRYPT, Security and Cryptography for Networks (SCN), Designs, Codes and Cryptography (DESI), ACM Transactions on Privacy and Security (TOPS), Applied Cryptography and Network Security (ACNS), IEEE International Conference on Distributed Computing Systems (ICDCS), ACM Advances in Financial Technologies (AFT).

### PRESENTATIONS

**Web3 Summit 2024**, Berlin, Germany

“Recent Developments on Multi-Party Schnorr Signatures”

**CRYPTO 2023**, University of California Santa Barbara, USA

“Fully Adaptive Schnorr Threshold Signatures” (Best Paper Plenary)

**CrossFyre 2023**, Lyon, France

“Multi-Party Schnorr Signatures”

**Real World Crypto 2023**, Tokyo, Japan

“From Theory to Practice to Theory: Lessons Learned in Multi-Party Schnorr”

**London Crypto Day 2022**, London, UK

“Recent Developments on Multi-Party Schnorr Signatures”

**IOG - UEdinburgh Research Week 2022**, Edinburgh, UK

“Multi-Party Schnorr Signatures”

**CRYPTO 2022**, University of California Santa Barbara, USA

“Better than Advertised Security for Non-Interactive Threshold Signatures”

**Zcon3 Conference 2022**, Las Vegas, USA

“Research Updates on FROST”

**Future of PI: Challenges and Perspectives of Personal Identification 2021**

“Delegatable Anonymous Credentials from Mercurial Signatures”

IEEE European Symposium on Security and Privacy (EuroS&P)

**University of Waterloo Cryptography, Security, and Privacy Seminar 2021**

“Delegatable Anonymous Credentials from Mercurial Signatures”

**PETS 2021 Privacy Enhancing Technologies Symposium**

“Mercurial Signatures for Variable-Length Messages”

**PETS 2020 Privacy Enhancing Technologies Symposium**

“Reputable List Curation from Decentralized Voting”

**CT-RSA 2019 The Cryptographers’ Track at the RSA Conference**, San Francisco, USA

“Delegatable Anonymous Credentials from Mercurial Signatures”

#### TEACHING

**COMP0141 Security**

Teaching Assistant, University College London

**CSCI 1510 Introduction to Cryptography and Computer Security**

Teaching Assistant, Brown University

**ENGN 1570 Linear System Analysis**

Teaching Assistant, Brown University

**MATH 0100 Introductory Calculus, Part II**

Teaching Assistant, Brown University

**MATH 0520 Linear Algebra**

Teaching Assistant, Brown University

#### PAST ACTIVITIES

**CAPS @ Brown : Cryptography Anonymity Privacy Security**

Brown University, Providence, USA

**Brown-IMPA Watson Brazil Initiative**

*Hyperbolic Geometry and Minimal Surfaces*

Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, Brazil

**Brown-Kobe Summer School in High Performance Computing**

*K computer, 3D visualization of peridynamic theory of fracture in solid mechanics.*

Kobe University, Kobe, Japan

**The Mathematics Scholars Group**

The University of Western Ontario, London, Canada