



# Elizabeth C. Crites, Ph.D.

---

CONTACT INFORMATION	The University of Edinburgh Bayes Centre, 47 Potterrow, Edinburgh EH8 9BT	elizabeth_crites@alumni.brown.edu elizabeth-crites.github.io
CITIZENSHIP	UK, US, Canada	
APPOINTMENTS	 <b>The University of Edinburgh</b> , Edinburgh, UK <i>Research Associate</i>	2021 –
	 <b>University College London (UCL)</b> , London, UK <i>Research Fellow</i>	2019 – 2021
EDUCATION	 <b>Brown University</b> , Providence, USA <i>Ph.D. &amp; M.Sc. in Mathematics</i> Advisor: Anna Lysyanskaya	2019
	 <b>Columbia University in the City of New York</b> , New York, USA <i>M.Sc. in Applied Mathematics</i> Advisors: Richard S. Hamilton & Michael I. Weinstein	
	 <b>The University of Western Ontario</b> , London, Canada <i>B.Sc. Honours Specialization in Mathematics, with Distinction</i>	
	 <b>McGill University</b> , Montréal, Canada <i>Visiting Scholar, Honours Mathematics</i>	
PUBLICATIONS	<b>Fully Adaptive Schnorr Threshold Signatures</b> Elizabeth Crites, Chelsea Komlo, Mary Maller <i>First fully adaptive security proof for a Schnorr threshold signature scheme.</i> CRYPTO 2023. <b>Best Early Career Paper Award.</b> IACR ePrint 2023/445	
	<b>Snowblind: A Threshold Blind Signature in Pairing-Free Groups</b> Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, Chenzhi Zhu <i>First threshold blind signature scheme in pairing-free groups.</i> CRYPTO 2023. IACR ePrint 2023/1228	
	<b>Threshold Structure-Preserving Signatures</b> Elizabeth Crites, Markulf Kohlweiss, Bart Preneel, Mahdi Sedaghat, Daniel Slamanig <i>First threshold structure-preserving signature scheme.</i> ASIACRYPT 2023. IACR ePrint 2022/839	
	<b>Better than Advertised Security for Non-Interactive Threshold Signatures</b> Mihir Bellare, Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, Chenzhi Zhu <i>Security analysis for the FROST and BLS threshold signature schemes.</i> CRYPTO 2022	
	<b>How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures</b> Elizabeth Crites, Chelsea Komlo, Mary Maller <i>Efficient two- and three-round multi- and threshold Schnorr signatures.</i> Results included in the FROST IETF draft. IACR ePrint 2021/1375	

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

Elizabeth C. Crites, Anna Lysyanskaya

*Extended mercurial signatures to allow messages of unbounded length (e.g., credential attributes).*

Privacy Enhancing Technologies Symposium – PETS 2021

## **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.*

Privacy Enhancing Technologies Symposium – PETS 2020

## **Delegatable Anonymous Credentials from Mercurial Signatures**

Elizabeth C. Crites, Anna Lysyanskaya

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

The Cryptographers' Track of the RSA Conference – CT-RSA 2019

### 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. 202 pgs.

### 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 SERVICES

## **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.

## **Program Committees**

I am a Program Committee member for CRYPTO 2024, EUROCRYPT 2024, and the Institute of Mathematics and its Applications (IMA) International Conference on Cryptography and Coding (IMACC2023).

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

**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

**SCHOLARSHIPS**

**US Department of Veterans Affairs Scholarship**

**Columbia University Admission Scholarship**

**The University of Western Ontario Admission Scholarship**