# Elizabeth C. Crites, Ph.D.

CONTACT INFORMATION

The University of Edinburgh
Bayes Centre
47 Potterrow
Edinburgh EH8 9BT
United Kingdom

elizabeth_crites@alumni.brown.edu
elizabeth-crites.github.io

APPOINTMENTS

**The University of Edinburgh**, Edinburgh, UK     2021 –
*Research Associate*

**University College London (UCL)**, London, UK     2019 – 2021
*Research Fellow*

EDUCATION

**Brown University**, Providence, USA     2019
*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*

PUBLICATIONS

**Threshold Structure-Preserving Signatures**
Elizabeth Crites, Markulf Kohlweiss, Bart Preneel, Mahdi Sedaghat, Daniel Slamanig
*First threshold structure-preserving signature scheme.*
IACR ePrint 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

**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.*
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.

Presentations
**London Crypto Day 2022**

TBD

London, UK

**CRYPTO 2022**

"Better than Advertised Security for Non-Interactive Threshold Signatures"

University of California Santa Barbara, USA

**Zcon3 Conference 2022**

"Research Updates on FROST"

Las Vegas, USA

**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**

"Delegatable Anonymous Credentials from Mercurial Signatures"

San Francisco, USA

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

OTHER
SERVICES

I have been a reviewer for the following conferences and journals: CRYPTO, 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).

OTHER
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**