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; GPA 3.9

Columbia University in the City of New York, New York, USA
M.Sc. in Applied Mathematics
Advisors: Richard S. Hamilton & Michael I. Weinstein; GPA: 3.9

The University of Western Ontario, London, Canada
B.Sc. Honours Specialization in Mathematics, with Distinction; GPA: 4.0+

McGill University, Montréal, Canada
Visiting Scholar, Honours Mathematics

PEER-REVIEWED PUBLICATIONS

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 two-round, Schnorr threshold signature scheme FROST.
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 (*Under submission.*)

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

Studied partial differential equations, such as mean curvature flow and the Ricci flow, used in Richard S. Hamiton's program for solving the Poincaré Conjecture (Millennium Prize Problem).

Presentations

CRYPTO 2022

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

University of California Santa Barbara, 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

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

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

Services

I have reviewed papers for the following conferences and journals: SCN 2022, CRYPTO 2022, Designs, Codes and Cryptography (DESI) 2022, ACM Transactions on Privacy and Security (TOPS) 2021, Applied Cryptography and Network Security (ACNS) 2021, IEEE International Conference on Distributed Computing Systems (ICDCS) 2021, ACM Advances in Financial Technologies (AFT) 2020.

Honours, Awards, and Scholarships

Brown-IMPA Watson Brazil Initiative Travel Award

Brown-Kobe Exchange in High Performance Computing Travel Award

US Department of Veterans Affairs Scholarship

Columbia University Admission Scholarship

Dean's Honour List, The University of Western Ontario

The University of Western Ontario Admission Scholarship

Languages

English (native), French (basic, passed Brown University Mathematics language exam)