# 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


**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 — 2013 – 2019
*Ph.D. in Mathematics*
Advisor: Anna Lysyanskaya; GPA: 3.9

**Columbia University in the City of New York**, New York, USA — 2011 – 2013
*M.Sc. in Applied Mathematics*
Advisors: Richard S. Hamilton & Michael I. Weinstein; GPA: 3.9

**The University of Western Ontario**, London, Canada — 2006 – 2010
*B.Sc. Honours Specialization in Mathematics, with Distinction*; GPA: 4.0+

**McGill University**, Montréal, Canada — 2008
*Visiting Scholar, Honours Mathematics*

**Peer-Reviewed Publications**

**How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures.**
Elizabeth Crites, Chelsea Komlo, Mary Maller
*New proving framework for more efficient multi- and threshold Schnorr signatures.*
*Under submission.* IACR ePrint 2021. 39 pgs.

**Mercurial Signatures for Variable-Length Messages.**
Elizabeth C. Crites, Anna Lysyanskaya
*Extended mercurial signatures to allow messages of unbounded length.*
Privacy Enhancing Technologies Symposium – PETS 2021.
IACR ePrint 2020. 41 pgs.

**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. 23 pgs.
Concurrent version (major differences) IACR ePrint 2020. 52 pgs.

**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. 47 pgs.

**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**

**Future of PI: Challenges and Perspectives of Personal Identification** Sept. 2021
"Delegatable Anonymous Credentials from Mercurial Signatures"
IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria

**University of Waterloo Cryptography, Security, and Privacy Seminar** Aug. 2021
"Delegatable Anonymous Credentials from Mercurial Signatures"
University of Waterloo, Canada

**PETS 2021 Privacy Enhancing Technologies Symposium** July 2021
"Mercurial Signatures for Variable-Length Messages"

**PETS 2020 Privacy Enhancing Technologies Symposium** July 2020
"Reputable List Curation from Decentralized Voting"
Concordia University & Université du Québec à Montréal, Canada

**CT-RSA 2019 The Cryptographers' Track at the RSA Conference** Mar. 2019
"Delegatable Anonymous Credentials from Mercurial Signatures"
San Francisco, USA

**Women in Theory (WIT) 2018** June 2018
"Delegatable Anonymous Credentials from Mercurial Signatures"
Harvard University, Boston, USA

**CRYPTO 2017 Rump Session** Aug. 2017
"Delegatable Anonymous Credentials from Mercurial Signatures"
University of California, Santa Barbara, USA

**Other Activities**

**CAPS @ Brown : Cryptography Anonymity Privacy Security** 2016 – 2019
Brown University, Providence, USA

**Brown-IMPA Watson Brazil Initiative** Jan. 2015
*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** Aug. 2014
*K computer, 3D visualization of peridynamic theory of fracture in solid mechanics.*
Kobe University, Kobe, Japan

I have reviewed papers for the following conferences and journals: 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.

## Teaching

**COMP0141 Security** — Spring 2021
Teaching Assistant, University College London

**CSCI 1510 Introduction to Cryptography and Computer Security** — Spring 2018
Teaching Assistant, Brown University

**ENGN 1570 Linear System Analysis** — Fall 2015
Teaching Assistant, Brown University

**MATH 0100 Introductory Calculus, Part II** — Spring 2015
Teaching Assistant, Brown University

**MATH 0520 Linear Algebra** — Fall 2014
Teaching Assistant, Brown University

## Awards and Scholarships

**Brown-IMPA Watson Brazil Initiative Travel Award** — 2015

**Brown-Kobe Exchange in High Performance Computing Travel Award** — 2014

**US Department of Veterans Affairs Scholarship** ($\$65,000$) — 2011 – 2014

**Columbia University Admission Scholarship** ($\$15,000$) — 2011 – 2013

**The University of Western Ontario Admission Scholarship** ($\$10,000$) — 2006 – 2010

## Languages

English (native), French (basic, passed Brown University Mathematics language exam) — 2017