

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 <i>Research Associate</i>	2021 –
	 University College London (UCL) , London, UK <i>Research Fellow</i>	2019 – 2021
EDUCATION	 Brown University , Providence, USA <i>Ph.D. in Mathematics</i> Advisor: Anna Lysyanskaya; GPA: 3.9	2013 – 2019
	 Columbia University in the City of New York , New York, USA <i>M.Sc. in Applied Mathematics</i> Advisors: Richard S. Hamilton & Michael I. Weinstein; GPA: 3.9	2011 – 2013
	 The University of Western Ontario , London, Canada <i>B.Sc. Honours Specialization in Mathematics, with Distinction; GPA: 4.0+</i>	2006 – 2010
	 McGill University , Montréal, Canada <i>Visiting Scholar, Honours Mathematics</i>	2008
PEER-REVIEWED PUBLICATIONS	How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures. Elizabeth Crites, Chelsea Komlo, Mary Maller <i>New proving framework for more efficient multi- and threshold Schnorr signatures.</i> <i>Under submission.</i> IACR ePrint 2021. 39 pgs.	
	Mercurial Signatures for Variable-Length Messages. Elizabeth C. Crites, Anna Lysyanskaya <i>Extended mercurial signatures to allow messages of unbounded length.</i> 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 <i>Constructed a token-curated registry from a voting protocol with ballot secrecy.</i> 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 <i>Constructed first efficient scheme for issuing, presenting, and delegating credentials anonymously.</i> The Cryptographers' Track of the RSA Conference – CT-RSA 2019. 47 pgs.	

DOCTORAL DISSERTATION	Delegatable Anonymous Credentials from Mercurial Signatures. <i>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.</i> Brown University Library 2019. 202 pgs.	
MASTER'S RESEARCH	<i>Studied 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).</i>	
PRESENTATIONS	Future of PI: Challenges and Perspectives of Personal Identification "Delegatable Anonymous Credentials from Mercurial Signatures" IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria Sept. 2021	
	University of Waterloo Cryptography, Security, and Privacy Seminar "Delegatable Anonymous Credentials from Mercurial Signatures" University of Waterloo, Canada Aug. 2021	
	PETS 2021 Privacy Enhancing Technologies Symposium "Mercurial Signatures for Variable-Length Messages" July 2021	
	PETS 2020 Privacy Enhancing Technologies Symposium "Reputable List Curation from Decentralized Voting" Concordia University & Université du Québec à Montréal, Canada July 2020	
	CT-RSA 2019 The Cryptographers' Track at the RSA Conference "Delegatable Anonymous Credentials from Mercurial Signatures" San Francisco, USA Mar. 2019	
	Women in Theory (WIT) "Delegatable Anonymous Credentials from Mercurial Signatures" Harvard University, Boston, USA June 2018	
OTHER ACTIVITIES	CAPS @ Brown : Cryptography Anonymity Privacy Security Brown University, Providence, USA 2016 – 2019	
	Brown-IMPA Watson Brazil Initiative <i>Hyperbolic Geometry and Minimal Surfaces</i> Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, Brazil Jan. 2015	
	Brown-Kobe Summer School in High Performance Computing <i>K computer, 3D visualization of peridynamic theory of fracture in solid mechanics.</i> Kobe University, Kobe, Japan Aug. 2014	
	The Mathematics Scholars Group The University of Western Ontario, London, Canada 2008-2010	

SERVICES	I have reviewed papers for the following conferences and journals: Crypto 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.	
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
HONOURS, AWARDS, AND SCHOLARSHIPS	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	
HONOURS, 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
	Dean's Honour List, The University of Western Ontario	2006 – 2010
	The University of Western Ontario Admission Scholarship (\$10,000)	2006 – 2010
LANGUAGES	English (native), French (basic, passed Brown University Mathematics language exam)	2017