Ryan Henry, PhD

School of Informatics, Computing, and Engineering
Indiana University Bloomington
107 S. Indiana Avenue
Bloomington IN 47405-7000
USA

Office: Luddy Hall (IF)
Room 3030
700 N. Woodlawn Avenue
Bloomington IN 47408-3901

Phone: +1 (812) 856-9972
Cell: +1 (812) 671-0435
Fax: +1 (812) 856-4764

Email: henry@indiana.edu
Website: http://homes.sice.indiana.edu/henry/

Born: January 26, 1985—Brandon MB, Canada
Nationality: Canadian
Language: English

Current position

Assistant Professor
Department of Computer Science
School of Informatics, Computing, and Engineering
Indiana University Bloomington

Areas of specialization

computer security & privacy · privacy-enhancing technologies · efficient constructions · cryptanalysis
applied cryptography · zero-knowledge proofs · private information retrieval · accountable anonymity

Academic background

PhD in Computer Science 08/2014
University of Waterloo
Dissertation: *Efficient Zero-Knowledge Proofs and Applications*
Advisor: Ian Goldberg
Cumulative GPA: 94/100
Outstanding Achievement in Graduate Studies Designation – Doctoral

MMath in Computer Science 01/2011
University of Waterloo
Dissertation: *Nymbler: Privacy-Enhancing Protection from Abuses of Anonymity*
Advisor: Ian Goldberg
Cumulative GPA: 95.25/100
Outstanding Achievement in Graduate Studies Designation – Master's

BSc (4-yr. Honours) in Mathematics and Computer Science *(dbl. major)* 04/2009
Brandon University
Cumulative GPA: 4.21/4.3
Graduated with "Greatest Distinction" (≥3.9/4.3 cumulative GPA)
Silver Medal in Mathematics (highest cumulative GPA among graduating majors)
Silver Medal in Computer Science (highest cumulative GPA among graduating majors)

Diploma (2-yr. Associate Degree) in Computer Systems Technology 05/2005
Assiniboine Community College
Cumulative GPA: 3.89/4.0
Graduated with "Distinction" (≥3.7/4.0 cumulative weighted GPA)

Professional development

Transforming Education, Stimulating Teaching & Learning Excellence (TRESTLE) 04/2017–*present*
NSF-funded STEM course transformation project

Course Design Institute (CDI) 06/2017
Center for Innovative Teaching & Learning, Indiana University

Transformative Learning Collegium (TLC) 05/2017
Center for Innovative Teaching & Learning, Indiana University

Faculty Success Program (FSP) 01/2016–04/2016
National Center for Faculty Development and Diversity

Graduate Certificate in University Teaching (CUT) 08/2014
Centre for Teaching Excellence, University of Waterloo

Teaching squares 09/2013–12/2013
Centre for Teaching Excellence, University of Waterloo

Graduate Certificate in Fundamentals of University Teaching (CUT) 08/2012
Centre for Teaching Excellence, University of Waterloo

Certificate in Student Leadership 10/2010
Office for Organizational & Human Development, University of Waterloo

Competitive research grants

Total personal share: US$1.42M; Total value: US$3.96M

As Principal Investigator (PI)

NSF SaTC, IU Award: $325K, PI
SaTC: CORE: Small: Batch Techniques for Practical Private Information Retrieval
CNS-1718475
September 2017–August 2020 (estimated)

NSF SaTC-BSF, IU Award: $255K (Personal share: $255K; Total: $635K), PI
SaTC-BSF: CORE: Small: Collaborative: Making Blockchains Scale Privately and Reliably
Collaborative award with Aniket Kate (Purdue University) and Amir Herzberg (Bar Ilan University)
CNS-1718595
August 2017–July 2020 (estimated)

As Co-Principal Investigator (Co-PI)

NSF SaTC, IU Award: $1.8M (Personal share: $840K; Total: $3M), Co-PI
TWC: Large: Collaborative: Living in the Internet of Things
PI: L. Jean Camp; Co-PI: Steven Myers
Collaborative award with Tadayoshi Kohno and Shwetak Patel (University of Washington)
CNS-1565375
August 2016–July 2021 (estimated)

Teaching experience

G: Graduate course; **U**: Undergraduate course; **U/G**: Undergraduate and graduate course

School of Informatics, Computing, and Engineering; Indiana University Bloomington

	Instructor, INFO-I231/CSCI-C231: Introduction to the Mathematics of Cybersecurity (**U**)	spring 2018
	Instructor, INFO-I538/CSCI-B504: Introduction to Cryptography (**G**)	spring 2017
	Instructor, CSCI-B609: Private Information Retrieval (**G**)	spring 2017
	Co-Instructor, INFO-I500/CSCI-B649: Privacy & Security in the IoT (**G**)	fall 2016
	Instructor, INFO-I231/CSCI-C231: Introduction to the Mathematics of Cybersecurity (**U**)	spring 2016
(★)	**Instructor**, INFO-I538/CSCI-B504: Introduction to Cryptography (**G**)	fall 2015
	Instructor, INFO-I538/CSCI-B504: Introduction to Cryptography (**G**)	spring 2015

(★) Honoured with Indiana University Trustees Teaching Award, based on student evaluations

Cheriton School of Computer Science; University of Waterloo

(★★)	**Instructor**, CS458/658: Computer Security and Privacy (**U/G**)	fall 2013
	Teaching assistant, CS458/658: Computer Security and Privacy (**U/G**)	spring 2012
	Teaching assistant, CS458/658: Computer Security and Privacy (**U/G**)	spring 2011
	Teaching assistant, CS458/658: Computer Security and Privacy (**U/G**)	spring 2010
	Teaching assistant, CS115: Introduction to Computer Science I (**U**)	fall 2009

(★★) Recognized as one of the top 10 instructors in CS department, based on student evaluations

Department of Mathematics and Computer Science; Brandon University

Lab instructor, 62:261: Introduction to Set Theory and Logic (**U**) — fall 2008
Lab instructor, 62:261: Introduction to Set Theory and Logic (**U**) — fall 2007
Lab instructor, 62:172: Introduction to Statistical Inference (**U**) — fall 2006
Lab instructor, 62:261: Introduction to Set Theory and Logic (**U**) — fall 2006

Tutorial presenter on Private Information Retrieval — 11/2017
24th ACM Conference on Computer and Communications Security (CCS 2017)

Faculty supervisor of Lattice Reading Group — 04/2017–*present*
School of Informatics, Computing, and Engineering, Indiana University Bloomington

Math Centre Assistant (tutor), Mathematics & Writing Centre — 09/2006–12/2008
Faculty of Science, Brandon University

Awards & distinctions

Indiana University Trustee's Teaching Award, Indiana University, 2016	$ 2,500	
Award for Outstanding Achievement in Graduate Studies, University of Waterloo, 2014	$ —	
Vanier Canada Graduate Scholarship (Vanier CGS), NSERC, 2011–2014	$ 150,000	
Alexander Graham Bell Canada Graduate Scholarship (CGS-D3), NSERC, 2011-2014	~~$ 105,000~~	*(declined)*
Government of Ontario/Bell Emergis Scholarship (GO-Bell), University of Waterloo, 2012–2014	$ 24,000	
Ontario Graduate Scholarship (OGS), OSAP, 2011–2012	~~$ 15,000~~	*(declined)*
President's Graduate Scholarship, University of Waterloo, 2011–2012	~~$ 10,000~~	*(declined)*
Award for Outstanding Achievement in Graduate Studies, University of Waterloo, 2011	$ —	
QNX Graduate Scholarship, QNX / Research in Motion, 2011	$ 5,000	
Ontario Graduate Scholarship (OGS), OSAP, 2011	$ 15,000	
President's Graduate Scholarship, University of Waterloo, 2011	$ 10,000	
1st prize in MITACS Poster Competition, MITACS, 2010	$ 300	
Alexander Graham Bell Canada Graduate Scholarship (CGS-M), NSERC, 2010	$ 17,500	
President's Graduate Scholarship, University of Waterloo, 2010	$ 10,000	
David R. Cheriton Graduate Scholarship, University of Waterloo, 2009–2011	$ 20,000	
Graduate Experience Award, University of Waterloo, 2009–2011	$ 2,000	
Silver Medal in Mathematics, Brandon University, 2009	$ —	
Silver Medal in Computer Science, Brandon University, 2009	$ —	
Roland Kitchen Scholarship in Mathematics, Brandon University, 2008–2009	$ 3,785	
WCG Scholarship in Computer Science, Brandon University, 2008–2009	$ 1,500	
Roland Kitchen Scholarship in Mathematics, Brandon University, 2007–2008	$ 3,785	
Undergraduate Student Research Award (USRA), NSERC, 2007	$ 4,500	
Roland Kitchen Scholarship in Mathematics, Brandon University, 2006–2007	$ 3,785	
Undergraduate Student Research Award (USRA), NSERC, 2006	$ 4,500	

Supervision & mentoring

PhD committee member

Adam Shull, Indiana University (Defended: January 2018)
Thesis: *Techniques and Challenges for Cryptographic Implementation of Access Control in the Cloud*

Postdoctoral supervisor

Fattaneh Bayatbabolghani, Indiana University (PhD Notre Dame) November 2017 – October 2019

PhD supervisor

Adithya Vadapalli, Indiana University January 2018 – *present*
Andrew Holland, Indiana University August 2017 – *present*
Swaminathan Vengalathur Ramesh, Indiana University August 2016 – *present*
Syed Mahbub Hafiz, Indiana University August 2015 – *present*

Graduate mentor

Natnatee (Ko) Dokmai, Indiana University
Omkar Bhide, Indiana University
Vineeta Sangaraju, Indiana University
Rohan Pillai, Indiana University
Narendar Edunuri, Indiana University
Tulasi Ram Kambhammettu, Indiana University
Anuj Bhandar, Indiana University
William Muldoon, Indiana University

Undergraduate mentor

(⋆) Bailey Kacsmar, Brandon University
Jacob Beauchamp, Indiana University
Christopher Dillon, Indiana University
Dyson Bridges, Indiana University
Boo Hyun Kim, Indiana University
Aaron Tsay, Indiana University
Paul Hendry, University of Waterloo

(⋆) Resulted in a publication in the proceedings of the 24th Annual Conference on Selected Areas in Cryptography (SAC 2017).

Publications

Peer-reviewed journal and magazine articles

[SPSI 2018] **Ryan Henry**, Amir Herzberg, and Aniket Kate: *"Blockchain Access Privacy: Challenges and Directions"* IEEE Security and Privacy Magazine: Special Issue on the Blockchain (to appear in Jan. or Feb., 2018).

[PoPETs 2016] **Ryan Henry**: *"Polynomial Batch Codes for Efficient IT-PIR"* Proceedings on Privacy Enhancing Technologies (PoPETs), volume 2016(4):202 – 218.
https://doi.org/10.1515/popets-2016-0036

Selected peer-reviewed conference and workshop papers

[CCS 2017] Syed Mahbub Hafiz and **Ryan Henry**: *"Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR"*. Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS 2017), Dallas, TX, USA (October–November 2017). (Acceptance rate: 151/836 ≈ 18.1%.)
https://doi.org/10.1145/3133956.3134008

[SAC 2017] Bailey Kacsmar, Sarah Plosker, and **Ryan Henry**: *"Computing Low-Weight Discrete Logarithms"*. Proceedings of the 24th Annual Conference on Selected Areas in Cryptography (SAC 2017), volume 10719 of LNCS, pages 106–126, Ottawa, ON, Canada (August 2016). (Acceptance rate: 23/66 ≈ 34.8%.)
https://doi.org/10.1007/978-3-319-72565-9_6

[PETs 2016] **Ryan Henry**: *"Polynomial Batch Codes for Efficient IT-PIR"*. Proceedings of the 16th Privacy Enhancing Technologies Symposium (PETS 2016), Darmstadt, Germany (July 2016). (Acceptance rate: 26/89 ≈ 29.2%.)
https://doi.org/10.1515/popets-2016-0036

[WPES 2013] **Ryan Henry** and Ian Goldberg: *"Thinking Inside the BLAC Box: Smarter Protocols for Faster Anonymous Blacklisting"*. Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society (WPES 2013), pages 71–81, Berlin, Germany (November 2013). (Acceptance rate: 20/103 ≈ 19.0%.)
https://dx.doi.org/10.1007/978-3-642-38980-1_32

[ACNS 2013] **Ryan Henry** and Ian Goldberg: *"Batch Proofs of Partial Knowledge"*. Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS 2013), volume 7954 of LNCS, pages 102–118, Banff, AB, Canada (June 2013). (Acceptance rate: 33/150 ≈ 22.0%.)
https://dx.doi.org/10.1007/978-3-642-38980-1_7

[NDSS 2013] **Ryan Henry**, Yizhou Huang, and Ian Goldberg: *"One (Block) Size Fits All: PIR and SPIR with Variable-Length Records via Multi-Block Queries"*. Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS 2013), San Diego, CA, USA (February 2013). (Acceptance rate: 47/250 ≈ 18.8%.)
https://internetsociety.org/doc/one-block-size-fits-all-pir-and-spir-variable-length-records-multi-block-queries

[SHARCS 2012] **Ryan Henry** and Ian Goldberg: *"Solving Discrete Logarithms in Smooth-Order Groups using CUDA"*. Proceedings of the 5th Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems (SHARCS 2012), Washington, DC, USA (March 2012). (Acceptance rate: *not publicized*)
http://2012.sharcs.org/record.pdf

[CCS 2011] **Ryan Henry**, Femi Olumofin, and Ian Goldberg: *"Practical PIR for Electronic Commerce"*. Proceedings of the 18th ACM Conference on Computer Communications Security (CCS 2011), pages 677–690, Chicago, IL, USA (October 2011). (Acceptance rate: 60/429 ≈ 14.0%.)
https://doi.org/10.1145/2046707.2046784

[S&P 2011A] **Ryan Henry** and Ian Goldberg: *"Extending Nymble-like Systems"*. Proceedings of the 32nd IEEE Symposium on Security and Privacy (IEEE S&P 2011), pages 523–537, Berkeley, CA, USA (May 2011).
https://doi.org/10.1109/sp.2011.17 (Acceptance rate: 34/306 ≈ 11.1%.)

[S&P 2011B] **Ryan Henry** and Ian Goldberg: *"Formalizing Anonymous Blacklisting Systems"*. Proceedings of the 32nd IEEE Symposium on Security and Privacy (IEEE S&P 2011), pages 81–95, Berkeley, CA, USA (May 2011).
https://doi.org/10.1109/sp.2011.13 (Acceptance rate: 34/306 ≈ 11.1%.)

[PETS 2010] **Ryan Henry**, Kevin Henry, and Ian Goldberg: *"Making a Nymbler Nymble using VERBS"*. Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS 2010), volume 6205 of LNCS, pages 111–129, Berlin, Germany (July 2010). (Acceptance rate: 16/57 ≈ 28.1%.)
https://dx.doi.org/10.1007/978-3-642-14527-8_7

Peer-reviewed posters, poster abstracts, extended abstracts, and work-in-progress papers

[Can-CWIC 2017] Bailey Kacsmar, Sarah Plosker, and **Ryan Henry**: *"Computing Low-Weight Discrete Logarithms"*. Poster presented at the 2nd Annual ACM Canadian Celebration of Women in Computing (Can-CWIC 2017), Montreal, QC, Canada (November 2017).

[TRESTLE 2017] **Ryan Henry**: *"Overcoming a Mathematical Proof Techniques Bottleneck"*. Poster presented at the 2nd TRESTLE Annual Meeting and Course Transformation Institute (TRESTLE 2017), Indiana University, Bloomington, IN, USA (September 2017).

[REU 2017] Christopher Dillon, Omkar Bhide, and **Ryan Henry**: *"Bluetooth Low Energy Fingerprinting"*. Poster presented at the Indiana University School of Informatics, Computing, and Engineering 2017 REU Research Symposium, Indiana University, Bloomington, IN, USA (August 2017).

[MMC 2017] **Ryan Henry**, Bailey Kacsmar, and Sarah Plosker: *"Computing Low-Weight Discrete Logarithms"*. Extended abstract at the 1st International Workshop on Mathematical Methods for Cryptography (MMC 2017), Svolvær-Lofoten, Norway (September 2017).
http://people.uib.no/chunlei.li/workshops/lofoten/Abstract/MMC-Henry.pdf

[SaTC PI 2017] L. Jean Camp, Steven Myers, **Ryan Henry**, Tadayoshi Kohno, and Shwetal Patel: *"Give people controls they can understand and trust, for the privacy and security they want"*. Poster presented at the 3rd Biennial NSF Secure and Trustworthy CyberSpace Principal Investigators' Meeting (SaTC PI 2017), Arlington, VA, USA (January 2017).

[PMPML 2016] Tariq Elahi and **Ryan Henry**: *"Privacy-Preserving Anomaly Detection in Tor"*. Work-in-progress paper presented at the 1st NIPS Workshop on Private Multi-Party Machine Learning (PMPML 2016), Barcelona, Spain (December 2016).
https://pmpml.github.io/PMPML16/papers/PMPML16_paper_16.pdf

[S&P 2013] **Ryan Henry** and Ian Goldberg: *"Thinking Inside the BLAC Box: Smarter Protocols for Faster Anonymous Blacklisting"*. Poster presented at the 34th IEEE Symposium on Security and Privacy (IEEE S&P 2013), San Francisco, CA, USA (May 2013).
https://www.ieee-security.org/TC/SP2013/posters/Ryan_Henry.pdf

[S&P 2012a] **Ryan Henry**, Yizhou Huang, and Ian Goldberg: *"(Symmetric) PIR over Arbitrary Sized Records"*. Poster presented at the 33rd IEEE Symposium on Security and Privacy (IEEE S&P 2012), San Francisco, CA, USA (May 2012).
https://www.ieee-security.org/TC/SP2012/posters/Symmetric%20PIR.pdf

[S&P 2012b] **Ryan Henry**, Tariq Elahi, and Ian Goldberg: *"A Privacy-Preserving Protocol for Gathering Statistics About Tor Users"*. Poster presented at the 33rd IEEE Symposium on Security and Privacy (IEEE S&P 2012), San Francisco, CA, USA (May 2012).
https://www.ieee-security.org/TC/SP2012/posters/A%20Privacy-Preserving%20Protocol.pdf

[Cheriton 2011] **Ryan Henry**, Femi Olumofin, and Ian Goldberg: *"Practical PIR for Electronic Commerce"*. Poster presented at the 2011 Cheriton Research Symposium, University of Waterloo, Waterloo, ON, Canada (September 2011).

[S&P 2011] **Ryan Henry**, Femi Olumofin, and Ian Goldberg: *"Practical PIR for Electronic Commerce"*. Poster presented at the 32nd IEEE Symposium on Security and Privacy (IEEE S&P 2011), Oakland, CA, USA (May 2011).
https://www.ieee-security.org/TC/SP2011/posters/Practical_PIR_for_Electronic_Commerce.pdf

[UW 2011] **Ryan Henry**, Femi Olumofin, and Ian Goldberg: *"Pay-per-PIR and PIRACL: Symmetric Private Information Retrieval with Per-Record Pricing and Access Control Lists"*. Poster presented at the 2011 University of Waterloo Graduate Research Conference, Waterloo, ON, Canada (April 2011).

[Cheriton 2010] **Ryan Henry**, Kevin Henry, and Ian Goldberg: *"Making a Nymbler Nymble using VERBS"*. Poster presented at the 2010 Cheriton Research Symposium, University of Waterloo, Waterloo, ON, Canada (September 2010).

[MITACS 2010] **Ryan Henry**, Kevin Henry, and Ian Goldberg: *"Making a Nymbler Nymble using VERBS"*. Poster presented at the MITACS/CORS 2010 Annual Conference, Edmonton, AB, Canada (May 2010).
(🏆) Awarded 1st prize in the MITACS/CORS poster competition

[S&P 2010c] **Ryan Henry**, Kevin Henry, and Ian Goldberg: *"Making a Nymbler Nymble using VERBS"*. Poster presented at the 31st IEEE Symposium on Security and Privacy (IEEE S&P 2010), Oakland, CA, USA (May 2010).

[UW 2011] **Ryan Henry**, Kevin Henry, and Ian Goldberg: *"Making a Nymbler Nymble using VERBS"*. Poster presented at the 2010 University of Waterloo Graduate Research Conference, Waterloo, ON, Canada (April 2010).

[PNRMS 2007] **Ryan Henry** and Michael Roddy: *"A Class of Irreducible Union-closed Families"*. Poster presented at the Inaugural Meeting of the Prairie Network for Research in the Mathematical Sciences (PNRMS 2007), Regina, SK, Canada (May 2007).

Position papers and abstracts at workshops without proceedings

[NTIA 2016] L. Jean Camp, **Ryan Henry**, Steven Myers, and Gianpaolo Russo: *"Comment in response to Dept. of Commerce NTIA 'Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things'"*.
https://www.ntia.doc.gov/files/ntia/publications/camp_et_al.pdf

Theses

[Henry 2014] **Ryan Henry**: *"Efficient Zero-Knowledge Proofs and Applications"*. UWSpace: PhD thesis, University of Waterloo, Waterloo, ON, Canada (August 2014).
https://hdl.handle.net/10012/8621

[Henry 2011] **Ryan Henry**: *"Nymbler: Privacy-Enhanced Protections from Abuses of Anonymity"*. UWSpace: MMath thesis, University of Waterloo, Waterloo, ON, Canada (January 2011).
https://hdl.handle.net/10012/5699

Technical reports

[ePrint 2017a] Syed Mahbub Hafiz and **Ryan Henry**: *"Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR"*. IACR Cryptology ePrint Archive: Report 2017/825 (August 2017).
https://eprint.iacr.org/2017/825.pdf

[ePrint 2017b] Bailey Kacsmar and Sarah Plosker and **Ryan Henry**: *"Computing Low-Weight Discrete Logarithms"*. IACR Cryptology ePrint Archive: Report 2017/720 (July 2017).
https://eprint.iacr.org/2017/720.pdf

[ePrint 2016] **Ryan Henry**: *"Polynomial Batch Codes for Efficient IT-PIR"*. IACR Cryptology ePrint Archive: Report 2016/598 (June 2016).
https://eprint.iacr.org/2016/598.pdf

[CACR 2013b] **Ryan Henry** and Ian Goldberg: *"Thinking Inside the BLAC Box: Smarter Protocols for Faster Anonymous Blacklisting"*. CACR technical report 2013-26, University of Waterloo (November 2013).
http://cacr.uwaterloo.ca/techreports/2013/cacr2013-26.pdf

[CACR 2013a] **Ryan Henry** and Ian Goldberg: *"Batch Proofs of Partial Knowledge"*. CACR technical report 2013-08, University of Waterloo (March 2013).
http://cacr.uwaterloo.ca/techreports/2013/cacr2013-08.pdf

[CACR 2012b] **Ryan Henry** and Ian Goldberg: *"All-but-k Mercurial Commitments and their Applications"*. CACR technical report 2012-26, University of Waterloo (November 2012).
http://cacr.uwaterloo.ca/techreports/2012/cacr2012-26.pdf

[CACR 2012a] **Ryan Henry** and Ian Goldberg: *"Solving Discrete Logarithms in Smooth-Order Groups with CUDA"*. CACR technical report 2012-02, University of Waterloo (January 2012).
http://cacr.uwaterloo.ca/techreports/2012/cacr2012-02.pdf

[CACR 2011] **Ryan Henry** and Ian Goldberg: *"Practical PIR for Electronic Commerce"*. CACR technical report 2011-04, University of Waterloo (February 2011).
http://cacr.uwaterloo.ca/techreports/2011/cacr2011-04.pdf

[CACR 2010d] **Ryan Henry**: *"Pippenger's Multiproduct and Multiexponentiation Algorithms"*. CACR technical report 2010-26, University of Waterloo (September 2010).
http://cacr.uwaterloo.ca/techreports/2010/cacr2010-26.pdf

[CACR 2010c] **Ryan Henry** and Ian Goldberg: *"Formalizing Anonymous Blacklisting Systems"*. CACR technical report 2010-24, University of Waterloo (September 2010).
http://cacr.uwaterloo.ca/techreports/2010/cacr2010-24.pdf

[CACR 2010b] **Ryan Henry** and Ian Goldberg: *"Extending Nymble-like Systems"*. CACR technical report 2010-23, University of Waterloo (September 2010).
http://cacr.uwaterloo.ca/techreports/2010/cacr2010-23.pdf

[CACR 2010a] **Ryan Henry**, Kevin Henry, and Ian Goldberg: *"Making a Nymbler Nymble using VERBS"*. CACR technical report 2010-05, University of Waterloo (May 2010).
http://cacr.uwaterloo.ca/techreports/2010/cacr2010-05.pdf

Invited talks

Efficient, Expressive, and Private Information Retrieval from Indexes of Queries

- I-SENSE Seminar Series, Florida Atlantic University, Boca Raton, FL, USA (February 2018)
- Computing Colloquium Series, Boise State University, Boise, ID, USA (November 2017)
- ITI Seminar Series, University of Illinois, Urbana–Champaign, IL, USA (November 2017)

Batch Techniques for Efficient Private Information Retrieval

- Cyber Security Club at IU, Bloomington, IN, USA (April 2016)
- Microsoft Research Redmond, Redmond, WA, USA (April 2016)
- University of Washington at Tacoma, Tacoma, WA, USA (April 2016)
- CERIAS seminar, Purdue University, West Lafayette, IN, USA (March 2016)

Batch Techniques for Efficient Private Information Retrieval

- Research Horizons, Indiana University, Bloomington, IN, USA (September 2016)

Computing Low-Weight Discrete Logarithms

- University of Waterloo, Waterloo, ON, Canada (June 2016)

Practical PIR for Electronic Commerce

- Cornell, Ithaca, NY, USA (April 2014)
- Concordia University, Montreal, QC, Canada (March 2014)
- McMaster University, Hamilton, ON, Canada (March 2014)
- University of Calgary, Calgary, AB, Canada (February 2014)
- University of New Hampshire, Durham, NH, USA (February 2014)
- Drexel University, Philadelphia, PA, USA (February 2014)
- Indiana University, Bloomington, IN, USA (February 2014)
- Florida State University, Tallahassee, FL, USA (February 2014)
- Arizona State University, Tempe, AZ, USA (January 2014)

Practical PIR for Electronic Commerce

- University of North Carolina at Chapel Hill, Chapel Hill, NC, USA (October 2012)

Making a Nymbler Nymble using VERBS

- Brandon University, Brandon, MB, Canada (June 2010)

A Primer on Zero-Knowledge Proofs

- University of Waterloo, Waterloo, ON, Canada (March 2010)

Frankl's Conjecture: One of the most embarrassing gaps in combinatorial knowledge

- Brandon University, Brandon, MB, Canada (September 2009)

The Chinese Remainder Theorem with Applications to Cryptography

- Brandon University, Brandon, MB, Canada (March 2009)

Conference & workshop talks

"Tutorial: Private Information Retrieval"
24th ACM Conference on Computer and Communications Security (CCS 2017), Dallas, TX, USA (November 2017).

"Computing Low-Weight Discrete Logarithms"
1st International Workshop on Mathematical Methods for Cryptography (MMC 2017), Svolvær-Lofoten, Norway (September 2017).

"Trademark LitigaTor"
16th Privacy Enhancing Technologies Symposium Rump Session (PETS 2016), Darmstadt, Germany (July 2016).

"Polynomial Batch Codes for Efficient IT-PIR"
16th Privacy Enhancing Technologies Symposium (PETS 2016), Darmstadt, Germany (July 2016).

"Thinking Inside the BLAC Box: Smarter Protocols for Faster Anonymous Blacklisting" 12th ACM Workshop on Privacy in the Electronic Society (WPES 2013), Berlin, Germany (November 2013).

"Batch Proofs of Partial Knowledge"
11th International Conference on Applied Cryptography and Network Security (ACNS 2013), Banff, AB, Canada (June 2013).

"One (Block) Size Fits All: PIR and SPIR with Variable-Length Records via Multi-Block Queries"
20th Annual Network & Distributed System Security Symposium (NDSS 2013), San Diego, CA, USA (February 2013).

"Solving Discrete Logarithms in Smooth-Order Groups using CUDA"
5th Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems (SHARCS 2012), Washington, DC, USA (March 2012).

"Practical PIR for Electronic Commerce"
18th ACM Conference on Computer Communications Security (CCS 2011), Chicago, IL, USA (October 2011).

"Censorship Resistance for Offline Users"
20th USENIX Security Symposium Rump Session (USENIX Security 2016), San Francisco, CA, USA (August 2011).

"Extending Nymble-like Systems"
32nd IEEE Symposium on Security and Privacy (IEEE S&P 2011), Berkeley, CA, USA (May 2011).

"Formalizing Anonymous Blacklisting Systems"
32nd IEEE Symposium on Security and Privacy (IEEE S&P 2011), Berkeley, CA, USA (May 2011).

"Making a Nymbler Nymble using VERBS"
10th Privacy Enhancing Technologies Symposium (PETS 2010), Berlin, Germany (July 2010).

Academic service

NSF review panels

Years: 2015, 2016 (SaTC SMALL); 2018 (SaTC MEDIUM)

Editorial board

Proceedings on Privacy Enhancing Technologies (PoPETS), 2014 – *present*

Award committees

Caspar Bowden PET Award for Outstanding Research in Privacy Enhancing Technologies, 2017
PET Award for Outstanding Research in Privacy Enhancing Technologies, 2015

Organizing committee

Publications Co-Chair, 25th ACM Conference on Computer and Communications Security (CCS 2018)
General Co-Chair, Best Practices In The IoT Workshop (2017), Seattle, WA, USA
Student chair, 2nd Meeting of the Prairie Network for Research in the Mathematical Sciences (PNRMS 2008)

Session chair

Identities and Payments, Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016)
Cryptographic Methods I, 16th Privacy Enhancing Technologies Symposium (PETS 2016)
Privacy of Genomic Data and of Accesses, 12th ACM Workshop on Privacy in the Electronic Society (WPES 2013)

Program committee

2018

18th Privacy Enhancing Technologies Symposium (PETS 2018)
22nd International Conference on Financial Cryptography and Data Security (FC 2018)

2017

17th Privacy Enhancing Technologies Symposium (PETS 2017)
9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017)

2016

16th Privacy Enhancing Technologies Symposium (PETS 2016)
8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2016)

2015

14th ACM Workshop on Privacy in the Electronic Society (WPES 2015)
15th Privacy Enhancing Technologies Symposium (PETS 2015)
7th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2015)

2012

17th European Symposium on Research in Computer Security (ESORICS 2012)

Paper shepherd

18th Privacy Enhancing Technologies Symposium (PETS 2018)
16th Privacy Enhancing Technologies Symposium (PETS 2016)
22nd International Conference on Financial Cryptography and Data Security (FC 2018)

External reviewer (partial listing)

Journals

Discrete Applied Mathematics: The Journal of Combinatorial Algorithms, Informatics and Computational Sciences, 2017
IEEE Transactions on Dependable and Secure Computing (TDSC), 2017
ETRI Journal, 2016
KSII Transactions on Internet and Information Systems (TIIS), 2015
IEEE Transactions on Services Computing: Special Issue on Security and Dependability of Cloud Systems and Services, 2015
INFOCOMP Journal of Computer Science, 2014
ACM Transactions on Information and System Security (TISSEC), 2013
IEEE Systems Journal: Special Issue on Security and Privacy in Complex Systems, 2012
ACM Transactions on Information and System Security (TISSEC), 2011

Conferences and workshops

39th IEEE Symposium on Security and Privacy (IEEE S&P 2018)
36th International Cryptology Conference (CRYPTO 2016)
35th International Conference on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2015)
34th International Conference on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2014)
13th ACM Workshop on Privacy in the Electronic Society (WPES 2014)
17th International Conference on Information Security (ISC 2014)
20th ACM Conference on Computer and Communications Security (CCS 2013)
12th Privacy Enhancing Technologies Symposium (PETS 2012)
4th International Conference on Post-Quantum Cryptography (PQCRYPTO 2011)
10th ACM Workshop on Privacy in the Electronic Society (WPES 2011)
18th ACM Conference on Computer and Communications Security (CCS 2011)
11th Privacy Enhancing Technologies Symposium (PETS 2011)
17th ACM Conference on Computer and Communications Security (CCS 2010)

Memberships

Association for Computing Machinery (ACM)
Institute of Electrical and Electronics Engineers (IEEE)

Professional references

Steven A. Myers
Associate Professor &
Security Program Director
Computer Science
Indiana University
Bloomington IN 47405-7000
+1 (812) 345-4692
samyers@indiana.edu

Ian Goldberg
Professor & University
Research Chair
School of Computer Science
University of Waterloo
Waterloo ON N2L 3G1
+1 (519) 888-4567 ×36168
iang@cs.uwaterloo.ca

Douglas R. Stinson
University Professor
School of Computer Science
University of Waterloo
Waterloo ON N2L 3G1
+1 (519) 888-4567 ×35590
dstinson@uwaterloo.ca

Nicholas J. Hopper
Associate Professor
Computer Science & Engineering
University of Minnesota
Minneapolis MN 55455-0149
+1 (612) 626-1284
hopper@cs.umn.edu

Alfred Menezes
Professor
Combinatorics & Optimization
University of Waterloo
Waterloo ON N2L 3G1
+1 (519) 888-4567 ×36934
ajmeneze@uwaterloo.ca

Nikita Borisov
Associate Professor
Electrical & Computer Engineering
University of Illinois
Urbana–Champaign IL 61801-3444
+1 (217) 903-4401
nikita@illinois.edu