BENJAMIN W. FULLER

PERSONAL INFORMATION

email	benjamin.w.fuller@gmail.com
email	benjamin.fuller@uconn.edu
website	http://www.benjamin-fuller.uconn.edu
phone	(O) +1 (860) 486 2122
address	371 Fairfield Way, Unit 4155, Storrs, CT 06269

GOAL

Advance security and cryptography research using techniques from information theory and complexity. Emphasize practical schemes that can be transitioned to use. Educate scientists and responsible citizens in computer science and engineering.

APPOINTMENT

2020–Present Associate Director, Connecticut Advanced Computing Center, University of Connecticut

2022–Present Associate Professor, Computer Science and Engineering, University of Connecticut

2016–2022 Assistant Professor, Computer Science and Engineering, University of Connecticut

Current research thrusts include authentication and cryptographically protected database search. Developing cybersecurity concentration at the University of Connecticut.

EDUCATION

2012-2015 Ph.D. Computer Science, Boston University

Dissertation: Strong Key Derivation from Noisy Sources
Awards: Computer Science Research Excellence Award

2009-2011 M.A. Computer Science, Boston University

Thesis: *Computational Entropy and Information Leakage*

2003-2006 B.S. Mathematics/Computer Science, Rensselaer Polytechnic Institute

Awards: Rensselaer Medal Winner · Computer Science Scholar's Award

RESEARCH SUPPORT

NSF CICI
1. CICI:UCSS: ARMOR: Secure Querying of Massive Scientific Datasets. Joint with August University, Augusta PI: Hoda Maleki. UConn portion of funds 175K, 2023-2025.

NSF CAREER
2. CAREER: Cryptographic Authentication from Biometrics. 506K, 2022-2027.

State of Connecticut
3. Certification and Acceptance Testing of Electronic Voting Equipment Required for Use by the Federal Help America Vote Act of 2002. PI: Alexander Russell.
   a) 2021-2022, 523K, share 33%.
   b) 2020-2021, 478K, share 10%.

DARPA
4. TARTUFFE: Towards Attenuated Randomness Tracking and Universal Fuzzy Extraction. UConn PI: Benjamin Fuller. 200K, 2021-2022.

Office of Naval Research
5. Adaptive Access Control for Zero Trust Architectures. PI: Benjamin Fuller. 168K, 2021-2022, share 55%.

IARPA
6. PANTHEON: Programming Architecture iNtegrated Toolchain for compiling Homomorphic Encryption and ONline Secure Computation. PI: Rafail Ostrovsky (Stealth Software Inc.), UConn PI: Benjamin Fuller. Planned Program: 2019-2024, the entire program was canceled in July 2020. Planned PI share: 249K, received funds, 50K.

NSF CRII
7. SaTC: Searchable Encryption for Biometric Databases. PI: Benjamin Fuller. 175K, 2019-2021, share: 100%.

Office of Naval Research
8. Adaptive Generation of Trustworthy Configurations (AGTCon). PIs: Yan Song (URI) and Benjamin Fuller, co-PI: Laurent Michel. 400K, 2019-2021, share: 25%.

Synchrony Financial
9. Cybersecurity Research and Development: 2018-2019 Initiatives. PI: Benjamin Fuller, co-PI: Fei Miao. 200K with four additional Ph.D. fellowships, 2018-2019, share: 66%. Two projects:
   a) Adaptive Network Defense
   b) Hardening Third-Party Authentication

Comcast
10. Embedded System Authentication and New Authentication Techniques. PI: Marten van Dijk, co-PI: Benjamin Fuller. 100K, 2017, share: 50%.

PUBLICATIONS[1]

JOURNAL PAPERS

IEEE TDSC
1. Devon Callahan, Timothy Curry, Hazel Davidson, Heytem Zitoun, Benjamin Fuller, and Laurent Michel. *FASHION: Functional and Attack graph Secured HybrId Optimization of virtualized Networks*. IEEE Transactions on Dependable and Secure Computing, 2022.

Journal of Cryptology
2. Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith. *Reusable Fuzzy Extractors for Low Entropy Distributions*. Journal of Cryptology, 34, 2 (2021).

Information and Computation
3. Benjamin Fuller, Xianrui Meng, and Leonid Reyzin. *Computational Fuzzy Extractors*. Information and Computation 2020.

Trans IT
4. Benjamin Fuller, Leonid Reyzin, and Adam Smith. *When are Fuzzy Extractors Possible?* Transactions on Information Theory 2020.

Cryptography
5. Chenglu Jin, Charles Herder, Ling Ren, Phuong Ha Nguyen, Benjamin Fuller, Srinivas Devadas and Marten van Dijk. *FPGA Implementation of a Cryptographically-Secure PUF Based on Learning Parity with Noise*. MDPI Cryptography 2018.

Journal of Cryptology
6. Benjamin Fuller, Adam O'Neil, and Leonid Reyzin. *A Unified Approach to Deterministic Encryption – New Constructions and a Connection to Computational Entropy.* Journal of Cryptology 2015. (pp. 671-717)

CONFERENCE PAPERS

Asiacrypt
7. Daniel Apon, Chloe Cachet, Peter Fenteany, Benjamin Fuller, and Feng-Hao Liu. *Nonmalleable Digital Lockers without Setup*. Asiacrypt, 2022.

IJCB
8. Sohaib Ahmad and Benjamin Fuller. *Inverting Biometric Models with Fewer Samples: Incorporating the Output of Multiple Models*. International Joint Conference on Biometrics, 2022.

Contraint Programming
9. Timothy Curry, Gabe De Pace, Yan Sun, Benjamin Fuller, and Laurent Michel. *DUELMIPs: Jointly Optimizing SDN Functionality and Security*. Constraint Programming 2022.

AsiaCCS
10. Chloe Cachet, Sohaib Ahmad, Luke Demarest, Ariel Hamlin, and Benjamin Fuller. *Proximity Searchable Encryption for the Iris Biometric*. AsiaCCS 2022.

IT Crypto
11. Luke Demarest, Benjamin Fuller, and Alexander Russell. *Code offset in the exponent*. Conference on Information-Theoretic Cryptography, 2021.

IJCB
12. Sohaib Ahmad and Benjamin Fuller. *RESIST: Reconstruction of Irises from Templates.* International Joint Conference on Biometrics, 2020.

ACNS
13. Peter Fenteany and Benjamin Fuller. *Same Point Composable and Nonmalleable Obfuscated Point Functions*. Applied Cryptography and Network Security 2020.

BTAS
14. Sohaib Ahmad and Benjamin Fuller. *ThirdEye: Triplet Based Iris Recognition without Normalization.* IEEE International Conference on Biometrics: Theory, Applications and Systems. 2019

ISC 15. Sailesh Simhadri, James Steel, and Benjamin Fuller. *Cryptographic Authentication from the Iris.* Information Security Conference, 2019

ISIT 16. Benjamin Fuller and Lowen Peng. *Continuous-Source Fuzzy Extractors: Source Uncertainty and Security*. International Symposium on Information Theory 2019.

ACISP 17. Timothy Curry, Devon Callahan, Benjamin Fuller and Laurent Michel. *DOCSDN: Dynamic and Optimal Configuration of Software-Defined Networks*. Australasian Conference on Information Security and Privacy, 2019.

AsiaCCS 18. Quentin Alamélou, Paul-Edmond Berthier, Stéphane Cauchie, Chloe Cachet, Benjamin Fuller, Philippe Gaborit, and Sailesh Simhadri. *Pseudoentropic Isometries: A New Framework for Fuzzy Extractor Reusability.* AsiaCCS 2018.

ICITS 19. Robert Cunningham, Benjamin Fuller, and Sophia Yakoubov. *Catching MPC Cheaters: Identification and Openability.* ICITS 2017.

Latincrypt 20. Jeremy Blackthorne, Benjamin Fuller, Benjamin Kaiser, and Bülent Yener. *Environmental Authentication in Malware.* Latincrypt 2017 .

IEEE S&P 21. Benjamin Fuller, Mayank Varia, Arkady Yerukhimovich, Emily Shen, Ariel Hamlin, Vijay Gadepally, Richard Shay, John Darby Mitchell, and Robert Cunningham. *SoK: Cryptographically Protected Database Search.* IEEE Security and Privacy 2017. (pp.172-192).

Asiacrypt 22. Benjamin Fuller, Leonid Reyzin, and Adam Smith. *When are Fuzzy Extractors Possible?* Asiacrypt, December 2016. (pp. 277-306)

Eurocrypt 23. Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith. *Reusable Fuzzy Extractors via Digital Lockers.* Eurocrypt 2016. (pp. 117-146) Also presented without proceedings at Allerton 2014.

ICITS 24. Benjamin Fuller and Ariel Hamlin. *Unifying Leakage Classes: Simulatable Leakage and Pseudoentropy.* ICITS 2015. (pp. 69-86)

HOST 25. Merrielle Spain, Benjamin Fuller, Kyle Ingols, and Robert Cunningham. *Robust Keys from Physical Unclonable Functions.* IEEE Symposium on Hardware Oriented Security and Trust, 2014. (pp. 88-92)

Asiacrypt 26. Benjamin Fuller, Leonid Reyzin, and Xianrui Meng. *Computational Fuzzy Extractors.* Advances in Cryptology – Asiacrypt, December 2013. (pp. 174-193)

TCC 27. Benjamin Fuller, Adam O'Neil, and Leonid Reyzin. *A Unified Approach to Deterministic Encryption – New Constructions and a Connection to Computational Entropy.* Theory of Cryptography, 2012. (pp. 582-599) Also presented without proceedings at ICITS 2012.

NCA 28. Benjamin Fuller, Roger Khazan, Joseph Cooley, Galen Pickard, and Daniil Utin. *ASE: Authenticated Statement Exchange.* IEEE Network Computing and Applications, 2010. (pp. 155-161) **Award:** Best Paper.

NCA 29. Joseph Cooley, Roger Khazan, Benjamin Fuller, and Galen Pickard. *GROK: A Practical System for Securing Group Communications.* IEEE Network Computing and Applications, 2010. (pp. 100-107) **Award:** Best Paper Nominee.

MILCOM 30. Roger Khazan, Joseph Cooley, Galen Pickard, and Benjamin Fuller. *GROK Secure Multi-User Chat at Red Flag 2007-03.* Military Communications Conference, 2008. (pp. 1-7)

PEER-REVIEWED WORKSHOP PAPERS

AMV 31. Sohaib Ahmad and Benjamin Fuller. *Unconstrained Iris Segmentation from Convolutional Neural Networks*. Advanced Machine Vision for Real-life and Industrially Relevant Applications at ACCV, 2018.

SICK 32. Galen Pickard, Roger Khazan, Benjamin Fuller, and Joseph Cooley. *DSKE: Dynamic Set Key Encryption.* LCN Workshop on Security in Communication Networks, 2012. (pp. 1006-1013)

Vizsec 33. Tamara Yu, Benjamin Fuller, John Bannick, Lee Rossey, and Robert Cunningham. *Integrated Environment Management for Information Operations Testbeds.* Workshop on Visualization for Computer Security, 2007. (pp. 67-83)

MAGAZINE ARTICLES

IEEE Signal Processing Magazine 34. Gene Itkis, Venkat Chandar, Benjamin Fuller, Joseph Campbell, Robert Cunningham. *Iris Biometric*

1 This list contains works in both the cryptographic and security communities. In the cryptographic community, authors are listed alphabetically, in the security community authors are listed by contribution. References 2, 3, 4, 6, 7, 11, 13, 16, 18, 19, 20, 22, 23, 24, 26, and 27 are listed alphabetically. Students supervised by Dr. Fuller are underlined.

Security Challenges and Possible Solutions: For your eyes only? Using the iris as a key. IEEE Signal Processing Magazine, 2015. (pp. 42-53)

PATENTS

35. John Darby Mitchell, Uri Blumenthal, Benjamin Fuller, and Robert Cunningham. *Authenticated Intention*. US Patent App: US20200026835A1, Approved May 2022.

PAPERS IN SUBMISSION

1. Benjamin Fuller, Abigail Harrison, and Alexander Russell. *Lazy Risk-Limiting Ballot Comparison Audits*. 2022.
2. Sohaib Ahmad, Christopher Geiger, and Benjamin Fuller. *RESIST: Reconstruction of Irises from Templates*. 2021.

UNPUBLISHED MANUSCRIPTS

Charles Herder, Benjamin Fuller, Marten van Dijk, and Srinivas Devadas. *Public Key Cryptosystems with Noisy Secret Keys.* 2017

Benjamin Fuller and Leonid Reyzin. *Computational Entropy and Information Leakage.* 2011

AWARDS, MEDIA, AND OUTREACH

2021 UConn AAUP Early Career Teaching Excellence Award

2020 Coverage of the UConn Altschuler Cybersecurity Laboratory: UConn Today, Hartford Courant, NBC Connecticut, Hartford Business Journal WFSB

2020 Interview on Cybersecurity Safety at Home: NBC CT Live!

TEACHING

DEVELOPED CLASSES

Modern Cryptography: Foundations UConn CSE 4702/5852, Class Homepage. First semester class in modern cryptography. Lecture based with a focus on formal definitions and proofs of security. Cryptographic tasks that consider an eavesdropper.

Modern Cryptography: Primitives and Protocols UConn CSE 5854, Class Homepage. Second-semester graduate class in modern cryptography. Partially flipped format with contact time focusing on discussion. Cryptographic tasks where some participating parties may be malicious.

Cybersecurity Laboratory UConn CSE 3140, Lab introducing students to cybersecurity issues. No lecture component focus on experiential learning. Supported by a generous gift from Stephen and Samuel Altschuler.

Introduction to Network Security UConn CSE 4402. Class Homepage. Co-taught and developed with Professor Bing Wang. Covers the basics of network security and the adversarial mindset.

Introduction to Computer Security UConn CSE 4402. First offering taught as independent study. Covers principles of computer architecture and operating system design for isolation of users and applications. Focus on safety.

OFFERED CLASSES

5854 UConn CSE 5854. Modern Cryptography II. 2018, 2020

4939/4940 UConn CSE 4939W/4940. Senior Design Laboratory. 2019, 2020

4702 UConn CSE 4702/5852. Modern Cryptography. 2016, 2022

4402 UConn CSE 4402. Introduction to Network Security. 2017

4400 UConn CSE 4400. Computer Security. 2019

3140 UConn CSE 3140. Cybersecurity Laboratory. 2019, 2020

2500 UConn CSE 2500. Introduction to Discrete Mathematics. 2017,18

Other Teaching Assistant for Intro. to Network Security, Intro. to Cryptography, Computer Architecture, Calculus I, Computer Organization. 2005-2015

STUDENTS

CURRENT DOCTORAL STUDENTS

1. Maryam Rezapour, 2020-Present
2. Timothy Curry, 2018-Present.
3. Chloe Cachet, 2018-Present.
4. Sohaib Ahmad, 2017-Present.
5. Luke Johnson, 2017-Present.

COMPLETED DOCTORAL STUDENTS

1. LTC Devon Callahan, 2017-2020. First position: Assistant Professor at United States Military Academy

MASTERS

1. Abigail Harrison, 2022-2023. Masters thesis: Efficient Risk-Limiting Audits for Connecticut
2. Samantha Bengiovanna, 2020-2022. First Position: Gartner. Masters thesis: Automatic Configuration of Software Defined Networks
3. Peter Fenteany, 2020-2021. First position: Ph.D. student at NYU in Fall 2021. Masters thesis: Same Point Composable and Nonmalleable Obfuscated Point Functions
4. Jonathan Huang, 2016-2017, First position: Akamai Technologies.

UNDERGRADUATE

1. 2022-2023

   MICHAEL GOVAERTS Implementation of lazy risk-limiting audits.

   ANIKE BRAUN Jupyter front end for lazy risk-limiting audits.

2. 2021-2022

   SERENA RIBECK Honors Thesis: Efficient Implementations of Predicate Inner product encryption.

   JULIE HA Honors Thesis. Encrypted biometric search using Bloom filters and ORAM. Supervised during 2021 REU, continued work during the academic year. Joint supervision with Mayank Varia.

   ABIGAIL HARRISON Piloting of risk-limiting audits in Connecticut.

3. 2020-2021

   CHRISTOPER GEIGER McNair Scholar, the privacy of machine learning models. Honors Thesis: RESIST: Reconstructing Irises from Templates.

   HAZEL DAVIDSON linearizable attack graph analyses.

   ETHAN LAZARO statistics of noisy sources for cryptography.

   ABIGAIL HARRISON policy implications of deploying risk limiting audits in Connecticut.

   PETER FENTEANY nonmalleable cryptography.

4. 2019-2020

   CHRISTOPER GEIGER McNair Scholar, privacy of machine learning models.

   HAZEL DAVIDSON estimating resources of cryptographic protocols with functional programming.

MOHIT MALI flexible and secure configuration of networks.
JOSHUA COHN economic and technical aspects of blockchain.

5. 2018-2019
   ANDY GUO Honors Thesis: Lattices in Cryptography.
   ETHAN HANNA cheating and detection in video games.
   KERWIN MERCADO NSF REU: automatic configuration of networks.
   ANDRE CAI Attack graph analysis.
   NICHOLAS CHAN Attack graph analysis.
   JAMES STEEL statistics of iris for key derivation.
6. 2017-2018
   SAILESH SIMHADRI Honors Thesis: Reusable Authentication from the Iris.
   TREVOR PHILLIPS Honors Thesis: Security Analysis of the UConn Husky One Card.
   SHREYA VARSHNEY Honors Thesis: Gender and Major Differences in Privacy Views of UConn Students.
   MERLINA ESCORCIA suitability of passwords for subpopulations.
7. 2016-2017
   LOWEN PENG 2017, impossibility of fuzzy extractors.

INVITED TALKS AND PRESENTATIONS

Authentication from the Iris.
NSF SaTC PI Meeting Undergraduate Track, October 2019
WPI, March 2019
Boston University, March 2018.

Cryptographically Protected Database Search.
New York Cryptoday, September 2017,
Security by the Schuylkill, Comcast, May 2017
Visa Research, May 2017
University of Maryland, College Park, April 2017
George Mason University, April 2017
MIT Security Seminar, April 2017.

Strong Key Derivation from Noisy Sources.
CHASE Conference, UConn, June 2016
Privacy Enhancing Technologies for Biometrics, Haifa, January 2015
MIT Computer and Information Security Seminar, Cambridge, November 2014.

When are Fuzzy Extractors Possible?
Brown University Crypto Reading Group, Providence, October 2014.

Key Derivation from Noisy Sources with More Errors than Entropy.
Georgetown University, Washington D.C., May 2014
MITRE, Lexington, April 2014.

A Unified Approach to Deterministic Encryption.
NYC Cryptoday, New York, March 2012.

POSTERS

Key Derivation from Noisy Sources with More Errors than Entropy.
Boston University Computer Science Research Open House, 2014.

A Unified Approach to Deterministic Encryption.
Boston University Computer Science Research Open House, 2012.

DEMOS

Chenglu Jin, Charles Herder, Lin Ren, Phuong Ha Nguyen, Benjamin Fuller, S. Devadas and Marten van Dijk, *Practical Cryptographically-Secure PUFs based on Learning Parity with Noise*. IEEE Symposium on Hardware Oriented Security and Trust, 2017.

SERVICE

PROGRAM COMMITTEES

CCS 2022
EUROCRYPT 2022, 2021
CYBER SECURITY, CRYPTOLOGY, AND MACHINE LEARNING 2022, 2020
ASIACRYPT 2021
CT RSA 2021
IEEE COMPUTER AND NETWORK SECURITY 2019
TCC 2017
INTERNATIONAL CONFERENCE ON INFORMATION THEORETIC SECURITY 2016, 2017.

UCONN

Research Excellence Program Reviewer, 2020
Upsilon Pi Epsilon Faculty Advisor, 2019-2022
Cyber Security Club Faculty Advisor 2016-2019

NATIONAL SCIENCE FOUNDATION

Secure and Trustworthy Cyberspace, Panel Member, 2021, 2017.

CT SCIENCE OLYMPIAD

Judge, Fermi Numbers 2018
Event Organizer, Codebreakers 2019

EXTERNAL REVIEWER

ACNS 2015
ANNALS OF APPLIED STATISTICS 2022
ASIACRYPT 2018
CRYPTO 2021, 2018, 2010
CCC 2016, 2013
CCS 2015, 2022
CHES 2013, 2012
COMPUTER JOURNAL 2022
DEPENDABLE AND SECURE COMPUTING 2021, 2019, 2018, 2015
DESIGNS, CODES, AND CRYPTOGRAPHY 2022, 2020, 2017, 2016
ESORICS 2018
EUROCRYPT 2020, 2019, 2015, 2014
EURO S&P 2022
FOCS 2014
HOST 2017
ICITS 2015, 2012
INFOCOM 2019, 2018

INFORMATION PROCESSING LETTERS 2015, 2014
IET INFORMATION SECURITY 2016
INDOCRYPT 2015
ICALP 2015
ISIT 2015
MATHEMATICAL CRYPTOLOGY 2012
MDPI CRYPTOGRAPHY 2018
MILCOM 2010
MOBILE COMPUTING 2019
NSDI 2014
PKC 2018, 2019
PRIVACY AND SECURITY 2017
RANDOM 2015
SECURITY AND PRIVACY MAGAZINE 2019
SCN 2014
SSS 2010
STOC 2019
SIGNAL PROCESSING 2019
TCC 2015, 2016-B
TIFS 2022, 2021, 2018, 2017, 2014
TISSEC 2015
TOPS 2022, 2021, 2017
THEORETICAL COMPUTER SCIENCE 2022, 2021

PRIOR EXPERIENCE

2015–2016 Principal Investigator, MIT Lincoln Laboratory

Security and Privacy Assurance
Contribution: Served as principal investigator leading research and software development teams, managing between 5-10 staff and 3 research companies. Primary responsibilities include project development and management, developing new cryptographic approaches, gathering and communicating requirements, specifying test procedures, integration and deployment, and evaluating user experience and technology utility. Led the adaption, integration, and pilot deployment of privacy-preserving database prototypes in a real use case.
Background: Privacy-preserving databases balance the need for individuals' privacy and the need to perform data analytics. Systems are approaching practical levels of performance for moderate-size database systems.

2007–2014 Research Scientist, MIT Lincoln Laboratory

Performed research at the intersection of theoretic cryptography and secure systems. Major projects are below.

Secure and Resilient Cloud
Contribution: Evaluated the applicability of multi-party computation to the cloud environment. Built multi-party computation techniques using a sparse communication network.
Background: Computations increasingly occur in a cloud environment. It is imprudent to assume that all cloud resources operate honestly.

Secure Cloud Authentication
Contribution: Researched image processing techniques and key derivation techniques to improve iris authentication.
Background: User's data is increasingly pushed to resources they do not control. Strong authentication is even more important in the cloud environment. The human iris is a potential authentication source.

Physical Unclonable Functions
Contribution: Developed an optical physical unclonable function, focus on algorithms for image processing

and key derivation.
Background: A strong root of trust is critical to securing hardware devices. Physical unclonable functions are one source for a root-of-trust.

Dynamic Group Key Management
Contribution: Developed and deployed new approaches for dynamic key management.
Background: Key management is a challenge in real-world cryptographic applications. Standard approaches use static keys and assume a fixed set of participants.

Large Scale User Emulation
Contribution: Developed user models and advanced visualizations, enabling repeatable, realistic, and scalable evaluations of network technology. Focused on scalable visualizations.
Background: Computer systems are vast and interconnected with many sources of nondeterminism. This complexity makes it difficult to evaluate new technologies in a repeatable and realistic environment.

2006 Intern, National Security Agency

Applied mathematical principles to real-life cryptographic problems and protocols.

2005 Intern, International Business Machines

Collected worldwide inventory aging information, and automated process to make business recommendations about assets and reserves.

Updated November 7, 2022