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

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

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

IARPA
1. PANTHEON: Programming Architecture iNtegrated Toolchain for compiling Homomorphic Encryption and ONline Secure Computation. PI: Rafail Ostrovsky (Stealth Software Inc.), UConn PI: Benjamin Fuller. 2019-2024, PI share: 249K.

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

Office of Naval Research
3. Adaptive Generation of Trustworthy Configurations (AGTCon). PIs: Yan Song (URI) and Benjamin Fuller, co-PI: Laurent Michel. 400K, 2019-2020, share: 25%.

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

Comcast Center for Excellence
5. Embedded System Authentication and New Authentication Techniques. PI: Marten van Dijk, co-PI: Benjamin Fuller. 100K with an additional 50K fellowship, 2017, share: 50%.

PUBLICATIONS[1]

JOURNAL PAPERS

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

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

Cryptography
3. 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
4. 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

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

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

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

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

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

ACISP
10. 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
11. 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
12. Robert Cunningham, Benjamin Fuller, and Sophia Yakoubov. *Catching MPC Cheaters: Identification and Openability.* ICITS 2017.

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

IEEE S&P
14. 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
15. Benjamin Fuller, Leonid Reyzin, and Adam Smith. *When are Fuzzy Extractors Possible?* Asiacrypt, December 2016. (pp. 277-306)

Eurocrypt
16. 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
17. Benjamin Fuller and Ariel Hamlin. *Unifying Leakage Classes: Simulatable Leakage and Pseudoentropy.* ICITS 2015. (pp. 69-86)

HOST
18. 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
19. Benjamin Fuller, Leonid Reyzin, and Xianrui Meng. *Computational Fuzzy Extractors.* Advances in Cryptology – Asiacrypt, December 2013. (pp. 174-193)

TCC
20. 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.

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 1, 2, 4, 6, 9, 11, 12, 13, 15, 16, 17, 19, and 20 are listed alphabetically. Students supervised by Dr. Fuller are underlined.

NCA 21. Benjamin Fuller, Roger Khazan, Joseph Cooley, and Galen Pickard. *ASE: Authenticated Statement Exchange.* IEEE Network Computing and Applications, 2010. (pp. 155-161) **Award:** Best Paper.

NCA 22. 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 23. 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)

Referred Workshop Papers

AMV 24. 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 25. 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 26. 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 27. Gene Itkis, Venkat Chandar, Benjamin Fuller, Joseph Campbell, Robert Cunningham. *Iris Biometric Security Challenges and Possible Solutions: For your eyes only? Using the iris as a key*. IEEE Signal Processing Magazine, 2015. (pp. 42-53)

Papers in Submission

Devon Callahan, Timothy Curry, Daniel Davidson, Heytem Zitoun, Benjamin Fuller, and Laurent Michel. *FASHION: Functional and Attack graph Secured HybrId Optimization of virtualized Networks*. 2019

Luke Demarest, Benjamin Fuller, and Alexander Russell. *Code offset in the exponent*. 2019

Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith. *Reusable Fuzzy Extractors for Low Entropy Distributions*. 2018

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

Teaching

2019, 2020 **Cybersecurity Laboratory**

UConn CSE 3140, Lab introducing students to cybersecurity issues. Supported by generous gift from Stephen and Samuel Altschuler. News coverage: UConn Today, Hartford Courant, NBC Connecticut, Hartford Business Journal WFSB

2019 **Independent Study in Computer Security**

UConn CSE 5099

2017,18 **Introduction to Discrete Mathematics**

UConn CSE 2500, Class Homepage

2018 **Modern Cryptography: Primitives and Protocols**

UConn CSE 5854, Class Homepage

2017 Introduction to Network Security

UConn CSE 4095 Co-taught and developed with Professor Bing Wang. Class Homepage

2016 Modern Cryptography: Foundations

UConn CSE 5852, Class Homepage

2016-2005 Teaching Assistant for Intro. to Network Security, Intro. to Cryptography, Computer Architecture, Calculus I, Computer Organization

STUDENTS

DOCTORAL

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

1. Devon Callahan, 2017-2020. First position as faculty at United States Military Academy

MASTERS

1. Jonathan Huang, 2016-2017, First job at Akamai.

UNDERGRADUATE

1. 2019-2020
   CHRISTOPER GEIGER 2020, McNair Scholar, privacy of machine learning models.
   DANIEL DAVIDSON 2020, estimating resources of cryptographic protocols with functional programming.
   MOHIT MALI 2020, flexible and secure configuration of networks.
   JOSHUA COHN 2020, economic and technical aspects of blockchain.
2. 2018-2019
   ANDY GUO 2019, Honors Thesis: Lattices in Cryptography.
   ETHAN HANNA 2019, cheating and detection in video games.
   JAMES STEEL 2019, statistics of iris for key derivation.
3. 2017-2018
   SAILESH SIMHADRI 2018, Honors Thesis: Reusable Authentication from the Iris.
   TREVOR PHILLIPS 2018, Honors Thesis: Security Analysis of the UConn Husky One Card.
   SHREYA VARSHNEY 2018, Honors Thesis:
   Gender and Major Differences in Privacy Views of UConn Students.
   MERLINA ESCORLA 2018 suitability of passwords for subpopulations.
4. 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

CSCML 2020
1. Cyber Security, Cryptology, and Machine Learning 2020

CNS 2019
2. IEEE Computer and Network Security 2019

TCC 2017
3. Theory of Cryptography Conference 2017

ICITS 2016, 2017
4. International Conference on Information Theoretic Security 2016, 2017

UCONN

Research Excellence Program Reviewer, 2020

Upsilon Pi Epsilon Faculty Advisor, 2019-2020

Cyber Security Club Faculty Advisor 2016-2019

NATIONAL SCIENCE FOUNDATION

Secure and Trustworthy Cyberspace, Panel Member, 2017.

EXTERNAL REVIEWER

ACNS 2015
ASIACRYPT 2018
CRYPTO 2018, 2010
CCC 2016, 2013
CCS 2015
CHES 2013, 2012
MDPI CRYPTOGRAPHY 2018
TDSC 2019, 2018, 2015
DESIGNS, CODES, AND CRYPTOGRAPHY 2020, 2017, 2016
ESORICS 2018
EUROCRYPT 2020, 2019, 2015, 2014
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
TIFS 2018, 2017, 2014
TCC 2016-B, 2015
JOURNAL OF MATHEMATICAL CRYPTOLOGY 2012
MILCOM 2010
TRANS MOBILE COMPUTING 2019
NSDI 2014
PKC 2019, 2018
ACM PRIVACY AND SECURITY 2017
RANDOM 2015
IEEE SECURITY AND PRIVACY MAGAZINE 2019
SCN 2014
SSS 2010
STOC 2019
TRANS SIGNAL PROCESSING 2019
ACM TISSEC 2015

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 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 June 23, 2020