

Biographical Sketch

Benjamin Fuller

Professional Preparation

Rensselaer Polytechnic Institute, Troy, New York, 12180, USA.

Mathematics and Computer Science B.S., 2006

Boston University, Boston, Massachusetts, 02215, USA.

Computer Science M.A., 2011

Boston University, Boston, Massachusetts, 02215, USA.

Computer Science Ph.D., 2015

Appointments

Assistant Professor,

Department of Computer Science and Engineering

University of Connecticut, Storrs, Connecticut (2016 – Present)

Research Scientist,

MIT Lincoln Laboratory, Lexington, Massachusetts (2007 – 2016)

Most Relevant Products

1. Benjamin Fuller, Mayank Varia, Arkady Yerukhimovich, Emily Shen, Ariel Hamlin, Vijay Gadepally, Richard Shay, John Darby Mitchell, Robert Cunningham. *SoK: Cryptographically Protected Database Search*. IEEE Security & Privacy, May 2017.
2. Benjamin Fuller, Leonid Reyzin, Adam Smith. *When are Fuzzy Extractors Possible?* Advances in Cryptology – Asiacrypt 2016. <http://eprint.iacr.org/2014/961>.
3. Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, Adam Smith. *Reusable fuzzy extractors for low-entropy distributions* Advances in Cryptology – Eurocrypt, 117-146, 2016. <http://eprint.iacr.org/2014/243>.
4. Benjamin Fuller, Leonid Reyzin, Xianrui Meng. *Computational Fuzzy Extractors*. Advances in Cryptology – Asiacrypt, 174-193, December 2013. <http://eprint.iacr.org/2013/416>.
5. Benjamin Fuller, Adam O’Neill, Leonid Reyzin. *A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy*. Journal of Cryptology. Vol. 28, No. 3, 671-717. <http://eprint.iacr.org/2012/005>.

Other Products

1. Benjamin Fuller, Ariel Hamlin. *Unifying Leakage Classes: Simulatable Leakage and Pseudoentropy*. International Conference on Information Theoretic Security, 69-86, 2015. <http://eprint.iacr.org/2015/857>.

2. Merrielle Spain, Benjamin Fuller, Kyle Ingols, Robert Cunningham. *Robust Keys from Physical Unccloneable Functions*. IEEE Symposium on Hardware Oriented Security and Trust, 88-92, 2014. Available [here](#).
3. Robert Cunningham, Benjamin Fuller, Sophia Yakoubov. *Catching MPC Cheaters: Identification and Openability*. To appear at International Conference on Information Theoretic Security 2017. <http://eprint.iacr.org/2016/611>.
4. Joseph Cooley, Roger Khazan, Benjamin Fuller, Galen Pickard. *GROK: A Practical System for Securing Group Communications*. IEEE Network Computing and Applications, 100-107, 2010. Available [here](#).
5. Jeremy Blackthorne, Benjamin Kaiser, Benjamin Fuller, Bulent Yener. *Environmental Authentication in Malware*. Latincrypt 2017. .

Synergistic Activities

1. Dr. Fuller is the advisor of Cyber Security club at the University of Connecticut. This club engages students at all levels, teaching how computers work and how to secure computing resources.
2. Program Committee Member for ICITS 2016, 2017, TCC 2017.
3. Dr. Fuller is developing cybersecurity concentration at the University of Connecticut. Dr. Fuller has developed new courses on network security and cryptography.
4. Dr. Fuller served as panel member for NSF SaTC program.