Ashrujit Ghoshal

ashrujit@cs.washington.edu ▫ https://homes.cs.washington.edu/~ashrujit

EDUCATION

University of Washington
Ph.D. student in Computer Science and Engineering — Jan 2019 – Present
Research interest: Cryptography
Advisors: Stefano Tessaro, Rachel Lin

University of California, Santa Barbara
Ph.D. student in Computer Science — Sep 2018 – Dec 2018
Advisors: Stefano Tessaro, Rachel Lin

Indian Institute of Technology, Kharagpur
Bachelor of Technology in Computer Science and Engineering — Jul 2014 – Jul 2018
Thesis: *Implementation Attacks on Block Ciphers: New Approaches and Countermeasures*
Advisor: Debdeep Mukhopadhyay

PUBLICATIONS AND PREPRINTS

Cody Freitag, Ashrujit Ghoshal, Ilan Komargodski.
Time-Space Tradeoffs for Sponge Hashing: Attacks and Limitations for Short Collisions In *Advances in Cryptology- CRYPTO 2022*.

Ashrujit Ghoshal, Ilan Komargodski.
On Time-Space Tradeoffs for Bounded-Length Collisions in Merkle-Damgård Hashing In *Advances in Cryptology- CRYPTO 2022*.

Ashrujit Ghoshal, Riddhi Ghosal, Joseph Jaeger, Stefano Tessaro.
Hiding in Plain Sight: Memory-tight proofs via Randomness Programming. In *Advances in Cryptology- EUROCRYPT 2022*.

Ashrujit Ghoshal, Stefano Tessaro.
Tight State-Restoration Soundness in the Algebraic Group Model. In *Advances in Cryptology- CRYPTO 2021*.

Ashrujit Ghoshal, Joseph Jaeger, Stefano Tessaro.
The Memory Tightness of Authenticated Encryption. In *Advances in Cryptology- CRYPTO 2020*.

Ashrujit Ghoshal, Stefano Tessaro.
On the Memory Tightness of Hashed ElGamal. In *Advances in Cryptology- EUROCRYPT 2020*.

Ashrujit Ghoshal, Rajat Sadhukhan, Sikhar Patranabis, Nilanjan Datta, Stjepan Picek, Debdeep Mukhopadhyay.
Lightweight and Side-channel Secure 4 × 4 S-Boxes from Cellular Automata Rules. In *IACR Transactions on Symmetric Cryptology*, 2018(3), 311-334.

Ashrujit Ghoshal, Sikhar Patranabis, Debdeep Mukhopadhyay.
Template-Based Fault Injection Analysis of Block Ciphers. In *Security, Privacy, and Applied Cryptography Engineering- SPACE 2018*, LNCS, vol 11348, pp 21-36, 2018.

Ashrujit Ghoshal, Thomas De Cnudde.

Several Masked Implementations of the Boyar-Peralta AES S-Box. In *Progress in Cryptology – INDOCRYPT 2017*, LNCS, vol 10698, pp 384-402, 2017

Rajat Sadhukhan, Sikhar Patranabis, Ashrujit Ghoshal, Vishal Saraswat, Debdeep Mukhopadhyay, Santosh Ghosh.
An Evaluation of Lightweight Block Ciphers for Resource-Constrained Applications: Area, Performance and Security. In *Journal of Hardware and Systems Security*, vol 1, 203-218, 2017.

TALKS

Hiding in Plain Sight: Memory-tight Proofs via Randomness Programming. EUROCRYPT 2022.

Tight State-Restoration Soundness in the Algebraic Group Model. CRYPTO 2021.

The Memory-Tightness of Authenticated Encryption. CRYPTO 2020.

On the Memory-Tightness of Hashed ElGamal. EUROCRYPT 2020.

Several Masked Implementations of the Boyar-Peralta AES S-Box. INDOCRYPT 2017.

AWARDS & RECOGNITIONS

Regents Fellowship in Computer Science. University of California, Santa Barbara. 2018
Awarded to outstanding incoming PhD students.

Best Project Award. Department of CSE, IIT Kharagpur. 2018
Awarded for best B.Tech project and thesis among all undergraduate students.

Meduri Bhanumurthy Memorial Award. IIT Kharagpur. 2018
Awarded to the best student in extra-curricular activities in the graduating batch.

Gora Lal Syngal Memorial Scholarship. IIT Kharagpur. 2015-17
Awarded for academic excellence.

Kirrtan B Behera Memorial Award. IIT Kharagpur. 2016
Awarded for being the best all-rounder in the year.

TEACHING ASSISTANTSHIPS

CSE526: Cryptography, University of Washington. Spring 2019, Spring 2020
Graduate level class in Cryptography.

LONG TERM VISITS

NTT Research, Sunnyvale, CA, USA Jun – Dec 2021, Jun – Sep 2022
Research Intern. Mentor: Ilan Komargodski.

Simons Institute for the Theory of Computing, UC Berkeley. Feb – Mar 2020
Visiting Graduate Student in the program *Lattices: Algorithms, Complexity, and Cryptography*.

COSIC, KU Leuven, Belgium. May – Jul 2017
Visiting Scholar. Hosted by: Vincent Rijmen.

Indian Statistical Institute, Kolkata. May – Jul 2016
Visiting Student. Hosted by: Mridul Nandi.

SERVICE

Subreviewer for SODA 2021, CRYPTO 2021, TCC 2021, CRYPTO 2022

Member of the 2021 PhD admissions committee at University of Washington
Student area chair for Cryptography.