Ashrujit Ghoshal

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

EDUCATION

University of Washington,
Ph.D. in Computer Science — Jan 2019 – Present
Advisors: Stefano Tessaro, Rachel Lin

University of California, Santa Barbara,
Ph.D. 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

Ashrujit Ghoshal, Stefano Tessaro. On the Memory Tightness of Hashed ElGamal. Eurocrypt 2020.

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

Ashrujit Ghoshal, Sikhar Patranabis, Debdeep Mukhopadhyay (2018) Template-Based Fault Injection Analysis of Block Ciphers. In: Chattopadhyay A., Rebeiro C., Yarom Y. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2018. Lecture Notes in Computer Science, vol 11348. Springer, Cham

Ashrujit Ghoshal, Thomas De Cnudde (2017) Several Masked Implementations of the Boyar-Peralta AES S-Box. In: Patra A., Smart N. (eds) Progress in Cryptology – INDOCRYPT 2017. INDOCRYPT 2017. Lecture Notes in Computer Science, vol 10698. Springer, Cham

Rajat Sadhukhan, Sikhar Patranabis, Ashrujit Ghoshal, Vishal Saraswat, Debdeep Mukhopadhyay, Santosh Ghosh. Journal of Hardware and Systems Security (2017) 1: 203.

TEACHING ASSISTANTSHIPS

CSE526: Cryptography, University of Washington — April-Jun 2019

LONG TERM VISITS

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

Computer Security and Industrial Cryptography group, KU Leuven, Belgium. — May 2017 – Jul 2017
Visiting Scholar. Hosted by: Vincent Rijmen.

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

AWARDS & RECOGNITIONS

Regents Fellowship, Univerity of California Santa Barbara. — 2018

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 for being adjudged to be the best in extra-curricular activities in the graduating batch.

Gora Lal Syngal Memorial Scholarship, IIT Kharagpur — 2015,2016,2017
Awarded for academic excellence.

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

OTHER DETAILS

Nationality: Indian

[*CV compiled on 2020-02-04*]