


Syed Mahbub Hafiz

Homepage: homes.sice.indiana.edu/shafiz

Google scholar: goo.gl/nw73Vd

shafiz@iu.edu

(317) 767-9588

: [syedhafiz](#)

RESEARCH INTERESTS

- Applied cryptography
- Security & privacy
- Private information retrieval
- Privacy-enhancing technology

EDUCATION

- **Indiana University–Bloomington** Bloomington, IN
PhD candidate in Computer Science Aug. 2015–May 2020
(expected)
Thesis: Private Information Retrieval (PIR) in Practice.
Supervisor: Prof. Ryan Henry
- **Indiana University–Bloomington** Bloomington, IN
MS in Computer Science Aug. 2015–Dec. 2018
- **Indiana University–Purdue University Indianapolis** Indianapolis, IN
PhD student in Computer Science (transferred) Aug. 2014–Jul. 2015
- **Bangladesh University of Engineering and Technology** Dhaka, Bangladesh
BS & Engg. in Computer Science and Engineering Jun. 2007–Apr. 2012

EMPLOYMENT

- **Indiana University–Bloomington** Bloomington, IN
Instructor Aug. 2019–Dec. 2019
 - **Course:** Teaching Introduction to the Mathematics of Cybersecurity, a class of 80 students, with two TAs.
- **Research Assistant of Prof. Ryan Henry** Aug. 2015–May 2020
 - **Optimal-rate PIR:** Implemented most efficient “1-private” PIR protocols.
 - **Expressive PIR:** Developed faster expressive IT-PIR employing indexing and polynomial batch coding.
 - **Tor hidden service:** Experimentation with Tor in chutney network simulator to evaluate the performance of our proposed solution to a deanonymization attack on Tor hidden services.
- **International Computer Science Institute (affiliated with UC Berkeley)** Berkeley, CA
Research Intern of Dr. Sadia Afroz and Prof. Damon McCoy Aug. 2018–Nov. 2018
 - **Practical evaluation of proxy distribution mechanisms in the wild:** Implementation and evaluation of state-of-the-art Tor Bridge distribution methods in real-life Tor to circumvent internet censorship.
- **Indiana University–Purdue University Indianapolis** Indianapolis, IN
Teaching Assistant Aug. 2014–May 2015
 - **Courses:** Grading and tutoring recitation class of Computer Architecture (Fall 2014) and Systems Programming (Spring 2015)
- **Research Assistant of Prof. Xukai Zou** Jun. 2015–Jul. 2015
 - **Authentication:** Privacy preserving biometric authentication using Secure Two-Party Multiplication. Biometric-Capsule based privacy preserving user authentication in non-fully trusted environments. An analytic survey on user behaviour based secure authentication in mobile devices.
- **Kona International** Dhaka, Bangladesh & Seoul, South Korea
Software Engineer, R&D May 2012–Aug. 2014
 - **Public Key Infrastructure Middleware:** PKI cryptographic operations for Smart Card. Role (scrum master): analyzed, designed, and implemented RSA Laboratories PKCS#11 modules.
 - **Kona Secure Minidriver (CSP):** CryptoAPI operations in smart card using Windows Base CSP. Role (scrum team member): analysed and developed Windows Minidriver functionalities.
 - **Trusted Service Manager (TSM):** NFC eco-system of Mobile Operators, Service Providers, and users. Role (scrum team member): analysed and developed the Global Platform Standards.
- **Structural Data Systems Ltd.** Dhaka, Bangladesh
Jr. Software Engineer Dec. 2011–May 2012
 - **FreeBeePay:** A coupon management system for merchants and consumers. Role (back-end team member): implemented user commands which involve critical business logic and complex stored procedures in Database.

PUBLICATIONS

• Peer-reviewed journal paper

- **Hafiz, S.M.;** Henry, R. “*A Bit More Than a Bit Is More Than a Bit Better: Faster (essentially) optimal-rate many-server PIR.*” In Proceedings of the 19th Privacy Enhancing Technologies, PoPETS/PETS 2019.

• Peer-reviewed conference paper

- **Hafiz, S.M.;** Henry, R. “*Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR.*” In Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS'17), ACM, New York, NY, USA, 1361-1373. (Acceptance rate: $151/836 = 18.06\%$)
- **Hafiz, S.M.;** Hasan, M.N.; Islam, M.M. “*An efficient scanning based learning free algorithm for face detection.*” International Conference on Informatics, Electronics & Vision, IEEE/OSA/IAPR ICIEV, May 2012.

• Poster (abstract) presentation

- **Hafiz, S.M.;** Henry, R. “*Faster Optimal-rate Many-server Private Information Retrieval (PIR).*” Presented in IEEE S&P (Oakland) 2019 and USENIX Security 2019.

• Manuscript under preparation

- **Hafiz, S.M.;** Henry, R. “*Protecting Tor Hidden Services with Tunicate Onion Descriptors.*”
- **Hafiz, S.M.;** Afroz, S.; McCoy, D. “*Practical Evaluation of Proxy Distribution Mechanisms in Tor.*”
- Bayatbabolghani, F.; **Hafiz, S.M.;** Henry, R. “*System of Knowledge: Private Information Retrieval.*”

TALKS

- Presented “Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR” at CCS'17, Dallas, TX, USA on November 1st, 2017.

AWARDS

- Received student travel grant at IEEE S&P (Oakland) 2019.
- Outstanding student leader award 2018 at Indiana University.

EXTRA-CURRICULAR ACTIVITIES

- **Elected president** Bloomington, IN
Bangladesh Student Association at Indiana University *Jul. 2017–Jun.2018*
 - **Leadership:** Organized the cultural display of Bangladesh at Indiana University World Fare, International Mother Language Day celebration (with 120+ guests) , and Bengali New Year Celebration Night (with 250+ guests).
- **Organizer and coordinator** Dhaka, Bangladesh
Department of Computer Science and Engineering, BUET *Oct. 2011–Dec.2011*
 - **Leadership:** Organized CSE Festival (with 500+ guests) and led the finance and human resource management groups.