

# Syed Mahbub Hafiz

---

---

## Personal information

Office Luddy Hall 2030,  
700 N Woodlawn Ave,  
Bloomington, IN 47408, USA.  
Phone +1 (317) 767-9588  
Email shafiz@iu.edu  
Homepage homes.sice.indiana.edu/shafiz/

---

## Research interests

• Computer security and privacy • Applied cryptography • Privacy-enhancing technology  
• Private information retrieval • Censorship circumvention • Privacy-preserving machine learning  
• Homomorphic encryption • Secure multi-party computation

---

## Academic background

Aug. 2015 – present Indiana University, Bloomington, IN, USA.  
PhD candidate in Computer Science.  
Thesis: *Private Information Retrieval in Practice*.  
Supervisor: Prof. Ryan Henry  
Other committee members: Profs. Apu Kapadia, Funda Ergun, and David Crandall.

Aug. 2015 – Dec. 2018 Indiana University, Bloomington, IN, USA.  
MSc in Computer Science.  
CGPA: 3.77/4.0

Aug. 2014 – Jul. 2015 Indiana University–Purdue University, Indianapolis, IN, USA.  
PhD student in Computer Science (transferred.)

Jun. 2007 – Apr. 2012 Bangladesh University of Engineering and Technology, Dhaka, Bangladesh.  
BSc & Engg. (4-yr. honours) in Computer Science and Engineering.  
CGPA: 3.58/4.0; Top 30%

---

## Research experience

Aug 2015 - present Graduate research assistant,  
Dept. of computer science,  
Indiana University–Bloomington.  
PhD adviser: Prof. Ryan Henry

Aug 2018 - Nov 2018 Summer research intern,  
International Computer Science Institute, ICSI (affiliated with UC Berkeley.)  
Mentors: Dr. Sadia Afroz and Prof. Damon McCoy

Jun 2015 - Jul 2015 Graduate research assistant,  
Dept. of computer and information science,  
Indiana University–Purdue University Indianapolis.  
Adviser: Prof. Xukai Zou

Feb 2011 – Apr 2012 Undergrad research assistant,  
Bangladesh University of Engineering & Technology.  
Adviser: Prof. Md Monirul Islam

---

## Teaching experience

- Aug 2019 – Dec 2020 Instructor (primary),  
Dept. of computer science, Indiana University–Bloomington.  
CSCI-C231/INFO-I231 (*Introduction to the mathematics of cybersecurity*): Fall 2019, Spring 2020, and Fall 2020.  
Teaching a class of around 75 – 80 students and managing 3 – 5 Teaching Assistants.
- Aug 2014 – May 2015 Graduate teaching assistant,  
Dept. of computer and information science,  
Indiana University–Purdue University–Indianapolis.  
CSCI 40200 (*Computer Architecture*): Fall 2014  
CSCI 30000 (*Systems Programming*): Spring 2015  
Holding office hours, grading, and taking recitation class.

---

## Industrial experience

- May 2012 – Aug. 2014 Software engineer–research & development,  
Kona International.  
Worked both in Dhaka, Bangladesh R&D branch & Seoul, South Korea head quarter.
- Dec. 2011 – May 2012 Software engineer,  
Structural Data Systems Ltd.,  
Dhaka, Bangladesh.

---

## Grants and awards

- Dec 2019 Travel grant by Microsoft Research to attend its Private AI Bootcamp, Redmond, WA.
- May 2019 Student travel grant by IEEE S&P to attend the symposium.
- April 2018 Outstanding graduate student leader award by Indiana University–Bloomington.
- 2007-2011 Dhaka education board scholarship for excellence in the Higher Secondary Certificate exam.
- 2006 First runner up (division-wise) in the Bangladesh Math Olympiad.
- 2004-2006 Dhaka education board scholarship for excellence in the Secondary School Certificate exam.

---

## Mentorship

- Spring 2020 Zachary Zirin, Diego Rios-Rojas, and Chun Fung Lai.  
CSCI-Y390: *Undergraduate Research Opportunities in Computing*  
Dept. of computer science, Indiana University–Bloomington.  
Topic: *Employing practical private information retrieval to solve privacy problems in the wild.*
- Fall 2019 Tao Liu  
CSCI-Y390: *Undergraduate Research Opportunities in Computing*  
Dept. of computer science, Indiana University–Bloomington.  
Topic: *Practical computational private information retrieval.*

---

## Publications

Peer-reviewed journal articles:

- [PETS 2019] **Syed Mahbub Hafiz** and Ryan Henry: “A Bit More Than a Bit Is More Than a Bit Better: Faster (essentially) optimal-rate many-server PIR.” The 19th Proceedings on Privacy Enhancing Technologies. (Acceptance rate:  $67/300 = 22.33\%$ )  
[doi.org/10.2478/popets-2019-0061](https://doi.org/10.2478/popets-2019-0061)

Peer-reviewed conference papers:

- [CCS 2017] **Syed Mahbub Hafiz** and Ryan Henry: “Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR.” The 24th ACM SIGSAC Conference on Computer and Communications Security. (Acceptance rate:  $151/843 = 17.91\%$ )  
[doi.org/10.1145/3133956.3134008](https://doi.org/10.1145/3133956.3134008)

- [ICIEV 2012] **Syed Mahbub Hafiz**, Md. Najmul Hasan, and Md. Monirul Islam: “*An efficient scanning based learning free algorithm for face detection.*” The 2nd International Conference on Informatics, Electronics & Vision at Dhaka, Bangladesh.  
↗ [doi.org/10.1109/ICIEV.2012.6317390](https://doi.org/10.1109/ICIEV.2012.6317390)

Poster demos and poster abstracts:

- [SEC 2019] **Syed Mahbub Hafiz** and Ryan Henry: “*Faster Optimal-rate Many-server Private Information Retrieval (PIR).*” Poster presented at the 28th USENIX Security Symposium.  
↗ [www.usenix.org/conference/usenixsecurity19/poster-session](http://www.usenix.org/conference/usenixsecurity19/poster-session)
- [S&P 2019] **Syed Mahbub Hafiz** and Ryan Henry: “*Faster Optimal-rate Many-server Private Information Retrieval (PIR).*” Poster presented at the 40th IEEE Symposium on Security & Privacy.  
↗ [www.ieee-security.org/TC/SP2019/posters/hotcrp\\_sp19posters-final52.pdf](http://www.ieee-security.org/TC/SP2019/posters/hotcrp_sp19posters-final52.pdf)
- [Luddy Fall Research 2019] Tao Liu and **Syed Mahbub Hafiz**: “*Don’t let others know which movie you watch: An exploration to recent computational private information retrieval.*” Poster presented at the Luddy Fall Research Demo Day 2019, IU LSICE, Bloomington, IN.
- [Luddy Spring Research 2020] Zachary Zirin and **Syed Mahbub Hafiz**: “*Private content browsing.*” Poster presented at the Luddy Spring Research Demo Week 2020, IU LSICE, Bloomington, IN.
- Diego Rios-Rojas and **Syed Mahbub Hafiz**: “*Private information retrieval in IoT.*” Poster presented at the Luddy Spring Research Demo Week 2020, IU LSICE, Bloomington, IN.
- Chun Fung Lai and **Syed Mahbub Hafiz**: “*Private information retrieval.*” Poster presented at the Luddy Spring Research Demo Week 2020, IU LSICE, Bloomington, IN.

Technical reports:

- [ePrint 2017a] **Syed Mahbub Hafiz** and Ryan Henry: “*Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR.*” IACR Cryptology ePrint Archive: Report 2017/825.  
↗ [eprint.iacr.org/2017/825.pdf](http://eprint.iacr.org/2017/825.pdf)
- [arXiv preprint] Laia Amorós, **Syed Mahbub Hafiz**, Keewoo Lee, and Caner Tol: “*Gimme That Model: A Trusted ML Model Trading Protocol.*” ArXiv, abs/2003.00610.  
↗ [arxiv.org/abs/2003.00610](http://arxiv.org/abs/2003.00610)

Work-in-progress manuscripts:

- [1] **Syed Mahbub Hafiz** and Ryan Henry: “*Protecting Tor Hidden Services with Tunicate Onion Descriptors.*”
- [2] **Syed Mahbub Hafiz**, Sadia Afroz, and Damon McCoy: “*Practical Evaluation of Proxy Distribution Mechanisms in Tor.*”
- [3] Fattaneh Bayatbabolghani, **Syed Mahbub Hafiz** and Ryan Henry: “*System of Knowledge: Private Information Retrieval.*”
- [4] Laia Amorós, **Syed Mahbub Hafiz**, Keewoo Lee, and Caner Tol: “*Gimme That Model: A Trusted ML Model Trading Protocol.*”
- [5] **Syed Mahbub Hafiz**, Andrew Holland, and Ryan Henry: “*Bang the Drum All Day: PIR For Servers Who Don’t Wanna Work.*”

---

## Talks and presentations

- Jul. 2020 “Tunicate onion service descriptors for activists.”  
Rump session at the 20th Privacy Enhancing Technologies Symposium (PETS 2020).
- Feb. 2020 “Private information retrieval in practice.”  
Dept. of CS, Purdue University, West Lafayette, IN, USA.
- Dec. 2019 “Ensuring trust when trading Machine Learning models.”  
Private AI Bootcamp 2019, Microsoft Research, Redmond, WA, USA.  
↗ [youtu.be/E8PPHkTQzYc](https://youtu.be/E8PPHkTQzYc)

Nov. 2017 “Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR.”  
The 24th ACM Conference on Computer and Communications Security (CCS 2017), Dallas,  
TX, USA.  
[↗ youtu.be/YzGQVvw5vgU](https://youtu.be/YzGQVvw5vgU)

---

## Academic service

External reviewer:

SEC 2020 The 30th USENIX Security Symposium.

Sub-reviewer:

CCS 2018 The 24th ACM Conference on Computer and Communications Security.

---

## Volunteer service

Jul. 2017 – Jun. 2018 President (elected),  
Bangladesh Student Association at Indiana University–Bloomington.  
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).

Oct. 2011 – Dec. 2011 Organizer and coordinator,  
Dept. of computer science and engineering (CSE),  
Bangladesh University of Engineering and Technology.  
Leadership: organized CSE Festival (with 500+ guests) and led the finance and human  
resource management teams.

---

## Membership

Member, Association for Computing Machinery (ACM)

Member, Institute of Electrical and Electronics Engineers (IEEE)

Member, USENIX: the Advanced Computing Systems Association

---

## References

Ryan Henry, PhD  
Assistant professor,  
University of Calgary and Indiana University–Bloomington.  
Email: [ryan.henry@ucalgary.ca](mailto:ryan.henry@ucalgary.ca)  
Phone: +1 (403) 210-6307  
[↗ homes.sice.indiana.edu/henry/](https://homes.sice.indiana.edu/henry/)

Apu Kapadia, PhD  
Associate professor,  
Indiana University–Bloomington.  
Email: [kapadia@indiana.edu](mailto:kapadia@indiana.edu)  
Phone: +1 (812) 856-1465  
[↗ www.cs.indiana.edu/~kapadia/](https://www.cs.indiana.edu/~kapadia/)

Sadia Afroz, PhD  
Senior researcher,  
International Computer Science Institute, ICSI and Avast software.  
Email: [sadia@icsi.berkeley.edu](mailto:sadia@icsi.berkeley.edu)  
Phone: +1 (510) 666-2900  
[↗ www1.icsi.berkeley.edu/~sadia/](https://www1.icsi.berkeley.edu/~sadia/)