Abida Haque

804 W. Morgan St – Raleigh, NC 27603

+1 (919)-946-3299 • ahaque3@ncsu.edu

Education

- **North Carolina State University** — **Raleigh, North Carolina**
  PhD in Computer Science, advised by Dr. Alessandra Scafuro — *2017–2023*
  Interests: Cryptography, with a focus on privacy and anonymity
- **Georgia Institute of Technology** — **Atlanta, GA**
  M.S. Computer Science, GPA: 4.0 — *2015–2017*
- **Carnegie Mellon University** — **Pittsburgh, PA**
  B.S. Mathematical Sciences, GPA: 3.18 — *2006–2010*

Relevant Coursework

Cryptography, Graph Theory, Data Structures and Algorithms

Research Projects

- **Compact Traceable Ring Signatures** [Aug 2021 - May 2023]
  Constructed the first traceable ring signature scheme in the plain model. Advisor: Alessandra Scafuro
- **Stacked Garbling** [Jun 2020-Jun 2022, Eurocrypt 2022]
  Parameterized the trade-off between communication and computation in garbled circuits. Advisors: Steve Lu, Rafael Ostrovsky, Vlad Kolesnikov
- **Anonymous device authorization for cellular networks** [Jan 2020-Jun 2021, WiSec 2021]
  Analyzed the 5G authentication network for cryptographic issues. Wrote a protocol to make the PEI identifier on mobile devices private. Advisors: Alessandra Scafuro, Bradley Reaves
- **Mutual Accountability Layer: Accountable Anonymity within Accountable Trust** [Nov 2019- Jun 2022, CSCML 2022]
  Improve the group signature setting to account for adversarial managers, thus removing a single point of failure. Advisor: Alessandra Scafuro, Vanesa Daza
- **Threshold Ring Signatures: New Definitions and Post-Quantum Security** [Jan 2018-Feb 2020, PKC 2020]
  Wrote the first threshold ring signature scheme with explicit proofs of post-quantum security using the Unruh transformation. Wrote new active security definitions for threshold ring signatures. Advisor: Alessandra Scafuro
- **Logarithmic-Size (Linkable) Threshold Ring Signatures in the Plain Model** [May 2019-Jun 2022, PKC 2022]
  Introduced the first sub-linear (linkable) thring signature scheme, and prove it secure in the plain model. Mentors: Daniel Slamanig, Stephan Krenn, Christoph Striecks
- **Budget-Aware Computation: Affordable Precision on Mini-Apps** [May 2018 - Aug 2018]

Used multiple levels of floating point precision for mini-apps, showing the benefits of single and half precision. Focused on the mini-app TYCHO2 to solve a key kernel in radiation transport. Mentors: Laura Monroe, Kris Garrett, Bob Robey

- **Machine Learning Solutions to Syslog Anomalies in High Performance Computing** [May 2016 - Aug 2016, Workshop on HPC User Support Tools]

  Used Markov chain modeling on large data to guide sysadmins to find errors. Mentor: Lissa Baseman

Teaching

- **NC State** **Raleigh, NC**
  Instructor *Jan 2023–May 2023*
  Taught CSC116 - Introduction to Computer Science in Java. Instruction includes partially flipped classroom and student-written questions.
- **Navy Nuclear Power Training School** **Goose Creek, SC**
  Nuclear Instructor *Sep 2010–Jul 2014*
  Taught enlisted mathematics (Algebra I) and specialized instruction (electrical and mechanical theory) to enlisted Electronics Technicians and Electrician's Mates.

Internships

- **Facebook/Meta** **remote/Seattle, WA**
  Intern *June 2021–Aug 2021, May 2022–Sep 2022*
  Constructed and proved a private set intersection protocol for use in privacy-aware advertisement.
- **Stealth** **remote**
  Intern *June 2020–Aug 2020*
  Constructed and proved a stacked garbling scheme that allows the generator to lower communication costs while raising the computation cost for the evaluator.
- **Austrian Institute of Technology** **Vienna, Austria**
  Intern *May 2019–Aug 2019*
  Constructed and proved a logarithmic-size threshold ring signature scheme.
- **Los Alamos National Laboratory** **Los Alamos, NM**
  Research Intern *May 2018–Aug 2018*
  Investigated the outcomes of multi-level floating point precision on physics applications, notably TYCHO2. Investigated the outcomes of replacing double, single, and half precisions in terms of time, energy, and accuracy of the final solutions. Mentored undergraduate student in the high performance summer school.
- **Los Alamos National Laboratory** **Los Alamos, NM**
  Research Intern *Mar 2017–Aug 2017*
  Analyzed syslogs from HPC (High Performance Computing) systems with use of Markov chain modeling to find errors. Mentored student.

Work

- **Infor** **Boston, MA**
  Science Analyst *Feb 2016–Mar 2017*
  Created data visualizations from business clients using ggplot2 and RShiny for customer resource management project. Improved pricing margins for product distributors (using SQL, R, and Python).

- **Project X** **Detroit, MI**
  Data Scientist *2015*
  Found insights in the relationships between users via usage of Python scripts, along with Cypher (Neo4j).

Publications

- **Abida Haque**, Vanesa Daza, Alessandra Scafuro, Alexandros Zacharakis, Arantxa Zapico. "Mutual Accountability Layer: Accountable Anonymity within Accountable Trust" . International Symposium on Cyber Security, Cryptology, and Machine Learning. `https://eprint.iacr.org/2021/596`
- **Abida Haque**, Stephan Krenn, Daniel Slamanig, Christoph Striecks. "Logarithmic-Size (Linkable) Threshold Ring Signatures in the Plain Model." IACR International Workshop on Public Key Cryptography. Springer, Cham, 2022. `https://eprint.iacr.org/2020/683`
- **Abida Haque**, David Heath, Vladimir Kolesnikov, Rafail Ostrovsky, Akash Shah "Garbled Circuits With Sublinear Evaluator", Eurocrypt 2022. `https://eprint.iacr.org/2022/797`
- **Abida Haque**, Varun Madathil, Bradley Reaves, Alessandra Scafuro. "Anonymous Device Authorization for Cellular Networks". WiSeC 2021.
- **Abida Haque**, Alessandra Scafuro. "Threshold Ring Signatures: New Definitions and Post-Quantum Security." IACR International Workshop on Public Key Cryptography. Springer, Cham, 2020. `https://eprint.iacr.org/2020/135`
- **Abida Haque**, Alexandra DeLucia, and Elisabeth Baseman. 2017. "Markov Chain Modeling for Anomaly Detection in High Performance Computing System Logs." In Proceedings of the Fourth International Workshop on HPC User Support Tools (HUST'17). ACM, New York, NY, USA. DOI: `https://doi.org/10.1145/3152493.3152559`

Service

- Sub-reviewer for:
  - EUROCRYPT 2020
  - International Colloquium on Automata, Languages and Programming (ICALP) 2019
  - Public Key Crypto (PKC) 2019 and 2020
  - CRYPTO 2018
- Ph.D Recruitment Volunteer: March 2018, March 2019, February 2020, March 2021
- Secretary for Computer Science Graduate Student Alliance: Aug 2018 – May 2019

Further Information

- **Programming Languages:**
  - Proficient in: Python (numpy, scikit-learn, pandas, scipy), R, Git
  - Also past experience with: JAVA, C++
- **Citizenship:**
  - United States