

We are looking for highly motivated, hardworking, and self-driven PhD students to conduct research in the areas of applied cryptography and network security. We have **(fully-funded) multiple PhD positions**, starting from Fall 2020 (August 2020) or Spring 2020 (January 2020) at University of South Florida (USF).

USF is a Rank-1 Research University and offers a competitive salary with an excellent working environment, all within a close proximity of high-tech industry and beautiful beaches of sunny Florida. Tampa/Orlando area is in Florida High Technology Corridor, and harbors major tech and research companies. The qualified candidate will have opportunities for research internship and joint-projects with high-tech companies. The candidate will work on the design, analysis and deployment of new cryptographic schemes and protocols in various practical application domains. Research topics include but are not limited to:

- **Trustworthy and Scalable Blockchains in the Post-Quantum Era**
 - Use of blockchain infrastructure to enhance cyber-security
 - Post-quantum secure blockchains
- **Secure and Reliable Internet of Things and Systems (IoTs)**
 - Post-Quantum Public Key Infrastructure for IoT
 - Secure Voting
 - Light-weight cryptography for implantable medical devices
 - Delay-aware authentication in smart-grid systems
- **Secure and Trustworthy Cloud Computing**
 - New searchable encryption and Oblivious RAM (ORAM) schemes
 - Distributed cloud security
 - Distributed ORAM
 - Applied Multi-Party Computation
- **Breach-Resilient Infrastructures (Protection of Genetic/Medical Data)**
 - Trusted hardware-based searchable encryption and ORAM
- **Trustworthy Unmanned Aerial Systems (Aerial Drones)**
 - Cryptographic frameworks to protect aerial drones
 - Secure aerial drones for post-quantum era
- **Trustworthy Machine Learning (TML)**
 - Privacy-Preserving Machine Learning
 - Adversarial Machine Learning
- **Practical Aspects of Quantum-Safe Cryptography**
 - A joint position with USF Mathematics Department

The qualified candidate is expected to conduct innovative research on the aforementioned areas based on their experience and research interests. It is also expected that the qualified candidate has a good background in Computer Science and Math (i.e., algorithm, data structure, number theory and algebra). Solid programming skills are also expected. It is

desirable (but not necessary) if the candidate has prior publications in the cyber-security domain.

The candidate should fulfill the following requirements:

- A BS degree in ECE/CS with a high-GPA and research experience.
- Very good programming skills (e.g., C, C++), familiarity with Linux.
- Having prior courses on cyber-security is desirable.
- MS degree in ECE/CS/Math is a big plus (high-GPA, courses on cryptography and/or network security).
- Publications in security and privacy will be regarded as additional merits.

To apply please send (by e-mail) the following documents:

1. Transcripts
2. Curriculum vitae
3. Three reference letters
4. Motivation letter
5. Research statement
6. GRE and TOEFL/IELTS scores
7. Previous publications, if any

Informal Application Deadline (preferred): As soon as possible for evaluation.

Formal Application Deadline: End of January 2020 (apply to USF for Fall 2020) and October 2019 (apply to USF for Spring 2020)

Contact: Dr. Attila A. Yavuz

E-mail: attilaayavuz@usf.edu

Webpage: <http://www.csee.usf.edu/~attilaayavuz/>

After pre-screening is done, if selected, you will be contacted for an online interview process.