

We are looking for highly motivated, hardworking, and self-driven PhD students to work in the areas of applied cryptography and network security. We have (fully funded) multiple PhD positions, starting from Fall 2019 (August 2019) 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 lead-industrial 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 is not limited to:

- **Cryptocurrency and Blockchains**
 - 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

The qualified candidate is expected to conduct innovative research on the aforementioned areas based on his/her experience and research interests. It is also expected of the qualified candidate to have solid backgrounds in Computer Science and Mathematics. Strong programming and system building skills are also expected. It is desirable (but not necessary) if the candidate has prior publications in cyber-security domain.

The candidate should fulfill the following requirements:

- A BS degree with a high-GPA and research experience.
- Very good programming skills (e.g., C, C++), familiarity with OS/Systems.
- Good Academic Writing and Presentation Skills.
- Having prior courses on cyber-security is desirable.
- MS degree in computer science, electrical engineering or mathematics 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:

- Transcripts
- Curriculum vitae
- Three reference letters (after pre-screening done, letter writers should directly send their letters to Dr. Yavuz, for exceptions, contact with Dr. Yavuz)
- Previous publications (preferred but not required)
- Motivation letter
- Research statement
- GRE and TOEFL/IELTS scores

Informal Application Deadline: As soon as possible for evaluation.

Formal Application deadline: February 01, 2019 (apply to USF for Fall 2019)

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.