

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 Spring 2021 (January 2021) or Fall 2021 (August 2021) at University of South Florida (USF). USF is a Rank-1 Research University (rank 31 of CS departments at US public universities per according Academic Analytics on Scholarly Research Index, top 8th for invention disclosures in the USA) 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**
 - Use of blockchain infrastructure to enhance cyber-security
 - Cryptographic protocols to enhance the trust and privacy on blockchains
 - Post-quantum secure blockchains

- **Secure and Reliable Internet of Things and Systems (IoTs)**
 - Light-weight cryptography for IoT
 - Cryptographic protocols for vehicular and UAV networks
 - Post-quantum secure IoTs

- **Privacy-Enhancing Technologies**
 - Secure Multi-party Computation, ORAM
 - Distributed cloud security
 - Breach-Resilient Infrastructures (Protection of Genetic/Medical Data)
 - Trusted hardware-based searchable encryption and ORAM

- **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 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.

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 a plus but not required.

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

1. Transcripts
2. Curriculum vitae
3. Three reference letters (will be sent by referees during interview process)
4. Motivation letter
5. Research statement
6. Previous publications, if any

Preferred Application Deadline): ASAP for evaluation.

Formal Application Deadline: Please see below.

<https://www.usf.edu/admissions/graduate/admission-information/requirements-deadlines.aspx>

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.