CAREER: Lightweight and Fast Authentication for Internet of Things

Research Challenges:

(I) Resource-limited IoTs need low crypto overhead, scalability and non-repudiation, but existing methods are either unscalable or costly. How to *create lightweight digital signatures for low-end IoTs?*

(II) Delay-aware IoTs (e.g., smart-grid, autonomous driving, drones) need real-time authentication, but existing methods might be slow. *How to create fast digital signatures for delay-aware IoTs?*

(III) *How to efficiently enhance the privacy in IoTs while ensuring authentication and integrity?*

Solutions:

(I) Novel light-weight and fast digital signatures that exploit synergies among primitives as such *encodings, pre-computation, additive homomorphic and one-way functions.*

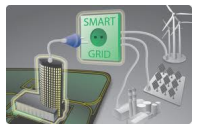
(II) New lightweight public key crypto primitives for authentication and key distribution for IoT systems, open-source frameworks.

(III) Privacy-enhancing schemes (e.g., ORAM, PEKS) with *authentication and access control.*

Project: NSF - CNS 1652389 (2017-2022)
PI: Dr. Attila A. Yavuz, **Email:** attilaayavuz@usf.edu

New Delay-Aware Signatures





100x faster signing, higher security, but larger keys

CEDA [CNS'18], Tachyon [CCS'18], ARIS [ICC'19], FAAS [FC'19]

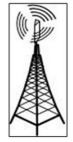
New Lightweight Signatures/Frameworks


7x-35x improved energy efficient, high compactness

Dronecrypt [Milcom'18], PKCFramework [IoT Wkps'18], ESEM [CNS'19], SEMECS [IEEE TSC'19]

New Privacy Enhancing Technologies



10x-200x lower delay, high security, and access control

S3ORAM [CCS'17], Lattices-PEKS [IEEE TDCS'18, DBSec'17], DSSE [ICC'18], POSUP [PETS'19], TrustSAS [INFOCOM'19], IM-DSSE [IEEE TSC'19], OMAT/OTREE [IEEE TCC'18], Loc-PIR [IEEE TCCN'19]

Scientific Impact:

Over 20 intellectual merits in in 2.5 years:

1. Four delay-aware signatures
2. Two lightweight PKC frameworks
3. Two signer near-optimal signature schemes
4. Two lattice-based public key searchable enc.
5. Three symmetric searchable enc. schemes
6. Two ORAM schemes
7. Two location-privacy frameworks
8. Three patents
9. Over ten open-source crypto frameworks

Broader Impact:

1. Improving the national security via enhancing the security of IoTs.
2. Broad applicability to many domains: Medical, energy delivery, transportation, cloud computing and wireless networks.
3. Educational/Outreach: (i) Portable course modules (integrating the research into four cyber-security courses). (ii) Research activities for under-represented groups via REUs (NSF Bulls-EYE, WICSE, FGLSAMP). (iii) CodeBreakHERS STEM Summer Camp for high-school female students.