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/integrity? How to efficiently address functionality versus privacy conundrum?*

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.*

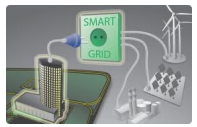
(II) New lightweight public key crypto primitives for authentication and key distribution for IoT systems, open-source frameworks.

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

Project: NSF - CNS 1917627 (2017-2023)
PI: Dr. Attila A. Yavuz, **Email:** attilaayavuz@usf.edu

New Delay-Aware Signatures





100x faster signing, higher security, but larger keys

SCRA [IEEE TIFS'17], CEDA [CNS'18], Tachyon [CCS'18], ARIS [ICC'19], FAAS [FC'19] Schnorr-HIBS-P [AsiaCCS'21], Sch-IBE [ISC'21]

New Lightweight Signatures/Frameworks


7x-35x improved energy efficient, compactness, quantum-safety, distributed verification

Dronecrypt [Milcom'18], PKCFramework [IoT Wkps'18], IoD-Crypt [ArXiv'19], ESEM [CNS'19], SEMECS [IEEE TSC'20], CORE [IEEE CNS'20], PoUR [Secrpyt'20], Lattice-PoW [CBT '21], ANT [ACSAC'21]

New Privacy Enhancing Technologies




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

S3ORAM [CCS'17], Lattices-PEKS [IEEE TDCS'18, DBSec'17], FS-DSSE [ICC'18], POSUP [PETS'19], TrustSAS [INFOCOM'19], IM-DSSE [IEEE TSC'19], OMAT/OTREE [IEEE TCC'18], Loc-PIR [IEEE TCCN'19], S3ORAM' [ACM TOPS'20], TrustSAS' [IEEE ACCESS '20], MOSE [ACM CODASPY'20], MACAO [NDSS'20], Titanium [NDSS'22],

Scientific Impact:

Over 62 intellectual merits (32 publication and 6 patents):

1. Six delay-aware signatures
2. Four lightweight PKC frameworks
3. Four signer near-optimal signature schemes
4. Two proof of works schemes
5. Two lattice-based public key searchable enc.
6. Six symmetric searchable enc. schemes
7. Two distributed ORAM schemes
8. Three ORAM/AC schemes
9. Three location-privacy frameworks
10. Six patents
11. Twenty-four 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. (iv) 3 Ph.D. students and 4 MS students graduated