CREDC

Lightweight, Delay-Aware, and Scalable Cryptographic Services for Smart Grid Systems

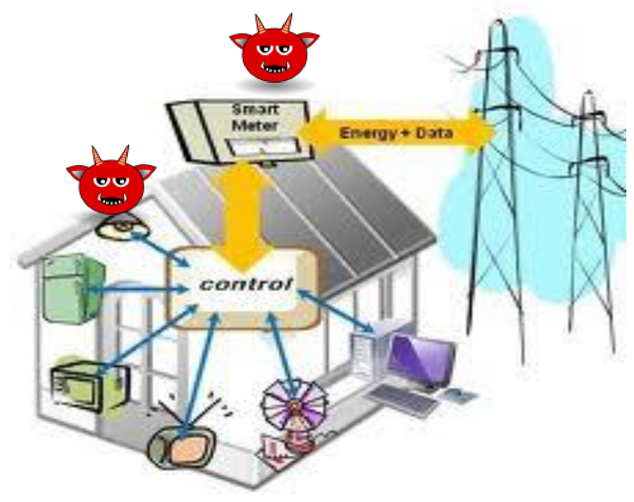
Attila A. Yavuz

GOALS

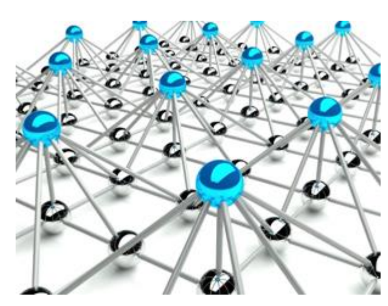
- Smart grids are vulnerable to false message injection, fake measurements, and tampering with command and control information.
  - Lack of real-time authentication and integrity is a critical problem.
  - Existing security mechanisms are either not scalable or too slow.
- **Develop novel authentication mechanisms for smart grids:**
  - Delay-aware: 60–120 messages can be authenticated per second.
  - Scalable to tens of thousands of components.
    - Broadcast authentication, compact signatures.
  - Practical test and deployment on actual smart grid infrastructure.

FUNDAMENTAL QUESTIONS/CHALLENGES

- **Critical vulnerabilities for smart grids:**
  - False data injection attacks.
  - Tampering commands.
  - Cascade failures.



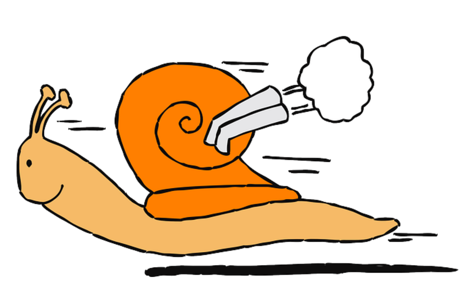
- **Authentication of commands/measurements is vital!**
  - **Real-time:** 60–120 messages per second.
  - **Scalable:** Broadcast authentication for large number of components.



- **Existing authentication methods are NOT enough.**
  - **Extremely slow:** Traditional signatures.
  - **Unscalable:** Symmetric crypto.

RESEARCH PLAN

- **Design novel delay-aware and scalable digital signatures.**



- Thrust I – Phase 1:
  - Design signer-optimal schemes with trapdoor permutations.
  - Structure-free Compact Authentication with RSA: SCRA-RSA.
    - Achieve minimum end-to-end delay.
- Thrust I – Phase 2:
  - Test SCRA-RSA on embedded devices to assess its performance.
  - Conduct experiments on actual smart grid testbeds.
- Thrust II – Phase 1:
  - Design SCRA-BGLS based on crypto pairing.
  - Design ECDLP-based message recovery (ECDLP-MR) scheme.
  - Achieve minimum signature size.
  - Produce formal proofs for given constructions.
- Thrust II – Phase 2:
  - Test SCRA-BGLS and ECDLP-MR on embedded devices.
  - Conduct experiments on actual smart grid testbeds.
- Thrust III:
  - Create an open-source crypto framework.
  - Framework tested on actual smart grid testbed.
  - Release educational course modules (e.g., portable VMs)

RESEARCH RESULTS

- **Observation:** Signature aggregation is more efficient than signing.
- Offline: Precompute signature components on hash output domain.
  - Divide & conquer strategy on hash output.
- Online: Given the hash of the message, fetch and combine precomputed signatures via signature aggregation function.

Precompute signature table (offline)

Interpret |H| output b-bit L subfields and precompute signatures on them.

Field 1 (10 bits)	Field 2 (10 bits)	…………	Field 16 (10 bits)

$\sigma_{1,0} = RSA_{sk}(1 \| 0 \| r)$ $\quad \sigma_{2,0} = RSA_{sk}(2 \| 0 \| r)$ $\quad \sigma_{10,0} = RSA_{sk}(10 \| 0 \| r)$

$\vdots \quad \vdots \quad \vdots$

$\sigma_{1,255} = RSA_{sk}(1 \| 255 \| r)$ $\quad \sigma_{2,255} = RSA_{sk}(2 \| 255 \| r)$ $\quad \sigma_{10,255} = RSA_{sk}(10 \| 255 \| r)$

Combine signatures from table based on message (online)

(Message||s), |s|=80 one-time rand. num. → HASH Function → 160 bits

Field 1 (10 bits)	Field 2 (10 bits)	…………	Field 16 (10 bits)
σ_1	σ_2		σ_{16}

$$\sigma_{1,16} = \prod_{i=1}^{16} \sigma_i \bmod n \qquad (\sigma_{1,16}, s)$$

Verify condensed (aggregate) signature (online)

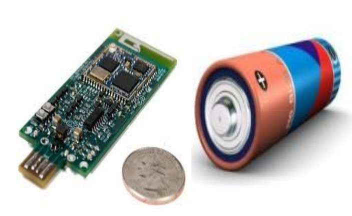
(Message||s) → HASH Function → (0||j||r), …, (16||j'||r)

$$(\sigma_{1,i})^e \bmod n = \prod_{i=1,j=1}^{16,10} H(i \| j \| r) \bmod n$$

BROADER IMPACT

- Open-source cryptographic framework.
- Publicly accessible for industry and academia.
- Broad applicability to other domains with time-critical needs.
  - Vehicular networks.

  - Wireless sensors.



  - Air drones.

FUTURE EFFORTS

- Develop formal proof for SCRA-RSA.
- Implement prototype of SCRA-RSA.
- Proceed with Thrust I – Phase 2.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY