Light-Weight, Delay-Aware and Scalable Authentication for Smart-Grid System

Dr. Attila A. Yavuz, Oregon State University

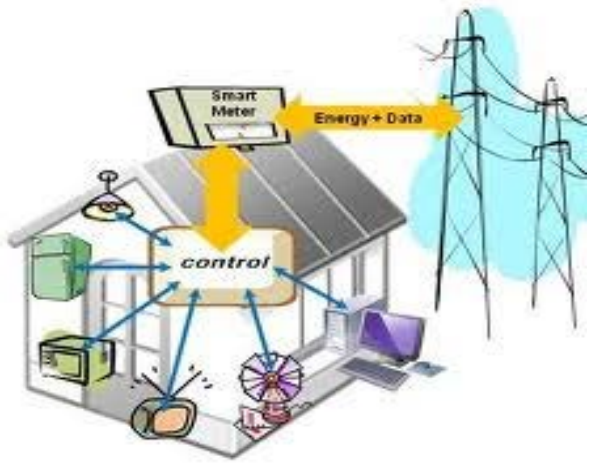
Presented by *Muslum Ozgur Ozmen*

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

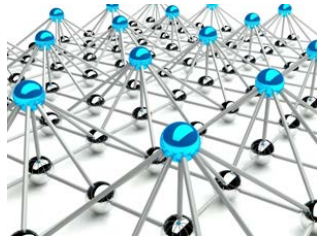
Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Research Need: Fast and Scalable Authentication

- **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



CREDC

Research Gap: Lack of Real-time Signatures

- **Symmetric crypto methods:** Unscalable for large distributed systems, lack of non-repudiation and public verifiability.

- **Traditional PKC Signatures:** (e.g., RSA [2], ECDSA [3], and Schnorr [4])
  - High computational cost, they require modular exponentiation (ExpOp) at the signer side.

- **Pre-computation:** Token-ECDSA [5] and online/offline signatures [6,7] do not require ExpOp at the signer side.
  - Linear memory overhead, K items require storing O(K) keys at the signer.

- **One-time/multiple-time Signatures:** (e.g., HORS [8])
  - They are computationally very efficient.
  - Very large signature size (2.5/5 KB) and communication overhead
  - Very large one-time public key (5 KB) for each item to be signed

Our Contribution: A new Real-Time Signature

- Structure-Free Compact Real-Time Authentication (SCRA [1])
- **Generic Design:** Transform **any** aggregate signature into a fast signing signature.
- **Ultra-Low End-to-End Delay:** SCRA schemes offer the lowest end-to-end delay among their counterparts.
  - SCRA-C-RSA: It is 7 and 19 times faster than ECDSA (pre-computed) and RSA, respectively.
- **Compact Signatures:** The signature size is almost identical to base schemes with all these improved efficiencies.
- **Limitation:** A small constant-size table stored at the signer side (highly feasible even for some embedded devices).

Main Idea: Generic SCRA from Aggregate Signatures

- **Observation:** Signature aggregation is much faster than signature generation.
- Create offline signature components to be combined (aggregated) online!
  - d-bit hash output is split into b-bit L sub-field
  - *Asig* is an aggregate digital signature scheme
  - *P* is a random padding

Pre-compute signature table **Γ** **(offline)**

Field 1 (b-bit)	Field 2 (b-bit)	.....	Field L (b-bit)
$\sigma_{1,0} = Asig_{sk}(1 \| 0 \| P)$	$\sigma_{2,0} = Asig_{sk}(2 \| 0 \| P)$		$\sigma_{L,0} = Asig_{sk}(L \| 0 \| P)$
$\vdots$	$\vdots$		$\vdots$
$\sigma_{1,2^b-1} = Asig_{sk}(1 \| 2^b - 1 \| P)$	$\sigma_{2,2^b-1} = Asig_{sk}(2 \| 2^b - 1 \| P)$		$\sigma_{L,2^b-1} = Asig_{sk}(L \| 2^b - 1 \| P)$

Sign **(online)**

(M||r), |r|= κ-bit random number $\Longrightarrow$ $(M_1^*,...,M_L^*) \leftarrow H(M \| r)$ b-bit indexes

Field 1 (b-bit)	Field 2 (b-bit)	.....	Field L (b-bit)
σ_1'	σ_2'		σ_L'

Fetch corresponding signatures from table **Γ** and aggregate them

$$s \leftarrow Asig.Agg(\sigma_1',...,\sigma_L') \Longrightarrow \sigma = (s, r)$$

Verify **(online)**

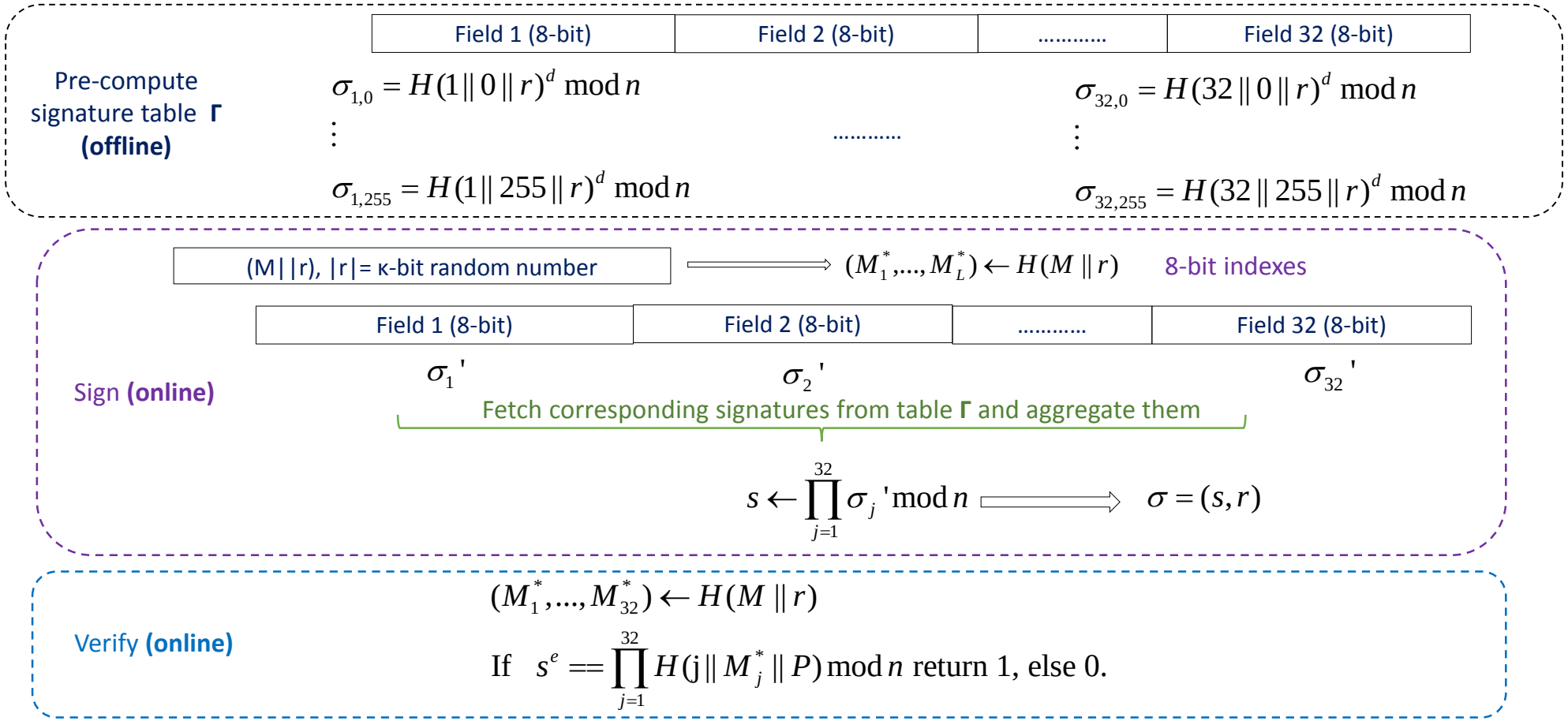
$$(M_1^*,...,M_L^*) \leftarrow H(M \| r)$$

$$\{0,1\} \leftarrow Asig.Ver(\langle 1 \| M_1^* \| P,...,L \| M_L^* \| P \rangle, s, PK)$$

CREDC

SCRA-C-RSA Instantiation

- C-RSA signature aggregation is just a modular multiplication and verification is very efficient ➔ Overall end-to-end delay is very low!



Performance Comparison (Commodity HW)

Protocol	Signing (ms)	Verification (ms)	End-to-End (ms)
ECDSA (pre-computed)	0.65	0.82	1.47
RSA	3.94	0.02	3.96
BGLS	0.46	34.00	34.46
NTRU	2.481	0.493	2.974
SCRA-C-RSA	**0.1639**	0.0513	**0.2152**
SCRA-BGLS	**0.0251**	34.21	**34.2351**
SCRA-NTRU	**0.0048**	0.507	**0.5118**

SCRA-C-RSA: Lowest end-to-end delay with mid-size table (2 MB)
SCRA-NTRU: Fastest signing with large-size table (12.33 MB)
SCRA-BGLS: The smallest table with larger delay (160 KB)

- We extended SCRA implementations to GPU setting with our collaborators!

Future Research Directions

- **Post-Quantum (PQ) Public Key Infrastructure (PKI) for Smart-Grid System**

- There are recently proposed efficient PQ key exchange schemes (e.g., New Hope [11]).

- There is a significant research gap in PQ authentication, especially for resource-limited devices.
  - We will develop new digital signature schemes, and **create a practical PQ PKI** to protect smart grids.
  - Such a PKI will have broader impact: e-commerce, Bitcoin infrastructure and IoT systems.

References

[1] **Attila A. Yavuz**, A. Mudgerikar, A. Singla, I. Papapanagiotou and E. Bertino, "Real-Time Digital Signatures for Time-Critical Networks," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2627-2639, Nov. 2017.

[2] R.L. Rivest, A. Shamir, and L.A. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21(2):120–126, 1978*

[3] American Bankers Association. ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999

[4] C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology, 4(3):161–174, 1991*

[5] D. Naccache, D. M'Raïhi, S. Vaudenay, and D. Raphaeli. Can D.S.A. be improved? Complexity trade-offs with the digital signature standard.
In *Proceedings of the 13th International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '94), pages 77–85, 1994*

[6] D. Catalano, M. D. Raimondo, D. Fiore, and R. Gennaro. Off-line/on-line signatures: Theoretical aspects and experimental results.
Public Key Cryptography (PKC), pages 101–120. Springer-Verlag, 2008

[7] A. Shamir and Y. Tauman. Improved online/offline signature schemes. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '01, pages* 355–367, London, UK, 2001

[8] L. Reyzin and N. Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. In *Proceedings of the 7th Australian Conference on Information Security and Privacy (ACIPS '02), pages 144–153. Springer-Verlag, 2002.*

[9] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. Journal of Cryptology, 14(4):297–319, 2004.

[10] L. Ducas and P. Q. Nguyen. Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In Advances in Cryptology, ASIACRYPT 2012, volume 7658 of Lecture Notes in Computer Science, pages 433–450. Springer Berlin Heidelberg, 2012.

[11] Erdem Alkim, Leo Ducas, Thomas Poppelmann, and Peter Schwabe. Post-quantum key exchange-a new hope. In USENIX Security Symposium, pages 327–343, 2016.

CREDC

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security