ACM ICN 2020 MONTRÉAL

REALTIME DIGITAL SIGNATURES FOR NAMED DATA NETWORKING

Charalampos Katsis
ckatsis@purdue.edu

Ankush Singla
asingla@purdue.edu

Elisa Bertino
bertino@purdue.edu

PURDUE UNIVERSITY | Department of Computer Science

Named Data Networking

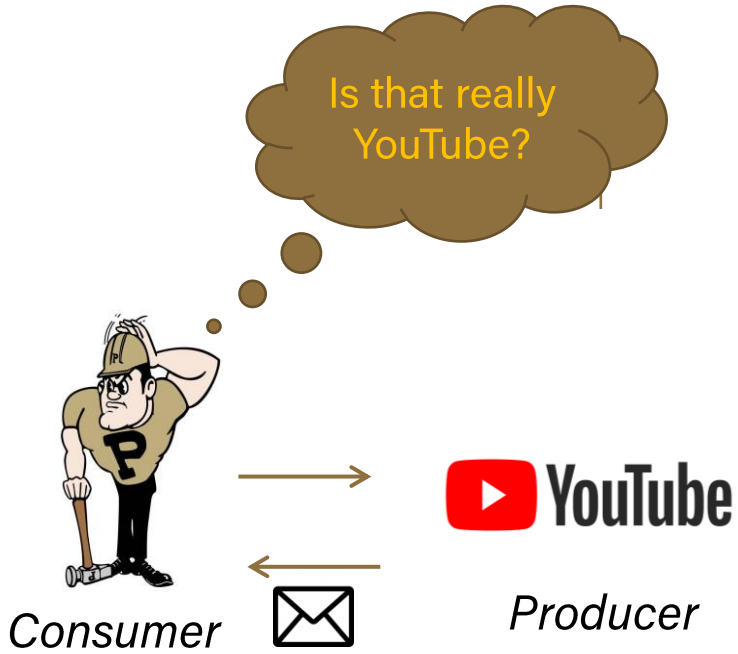
Data authenticity in NDN

- Some supported schemes:
  - Digest SHA-256
  - SHA-256 with RSA
  - SHA-256 with ECDSA
  - HMAC SHA-256

- Merely for integrity protection

- Integrity and provenance protection

- Partially supported in NDN-CXX.
- Short-lived symmetric keys.
  - Memory-based TPM.



Named Data Networking

What is the problem with the current signature schemes??

- Introduce significant computational overhead.
  - Latency in the communication.
  - Include costly mathematical operations.

- Unsuitable for time-critical applications, such as video conferencing, streaming etc.
  - Low latency requirement.

OUR GOAL

Provide secure and cost-effective authentication for NDN packets.

STRUCTURE-FREE AND COMPACT REAL-TIME AUTHENTICATION (SCRA)

A highly-parallelizable offline-online signature scheme

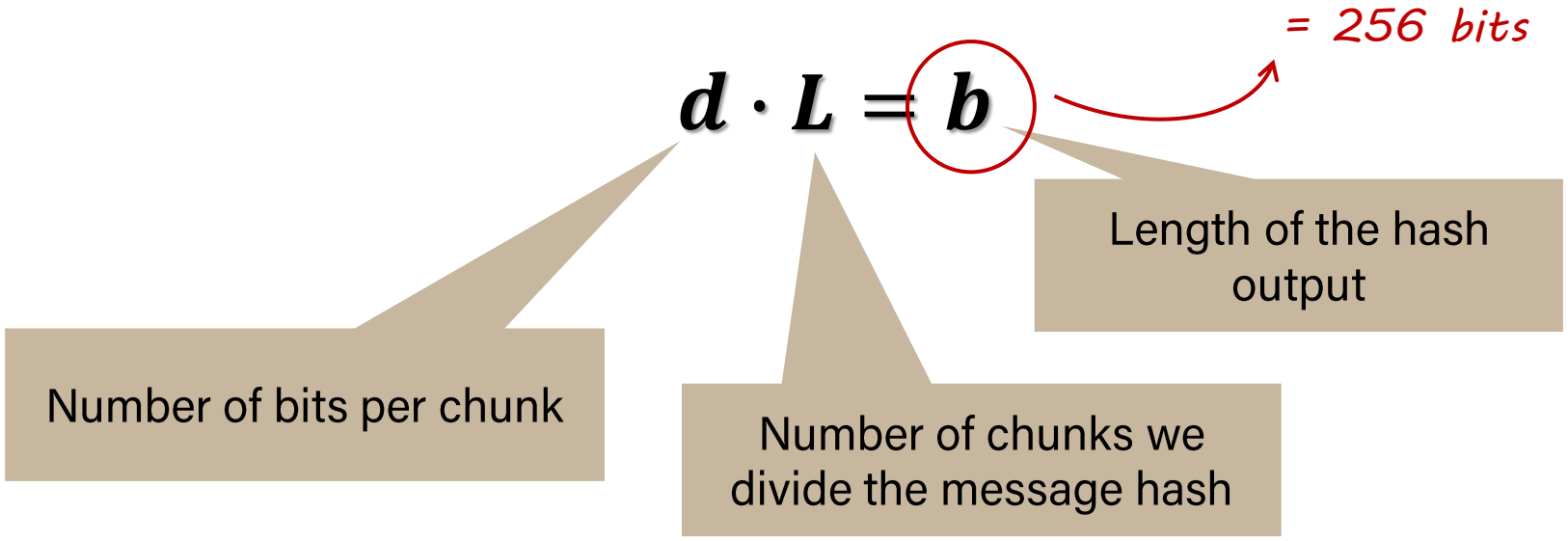
SCRA

Divide the work into offline and online phases.

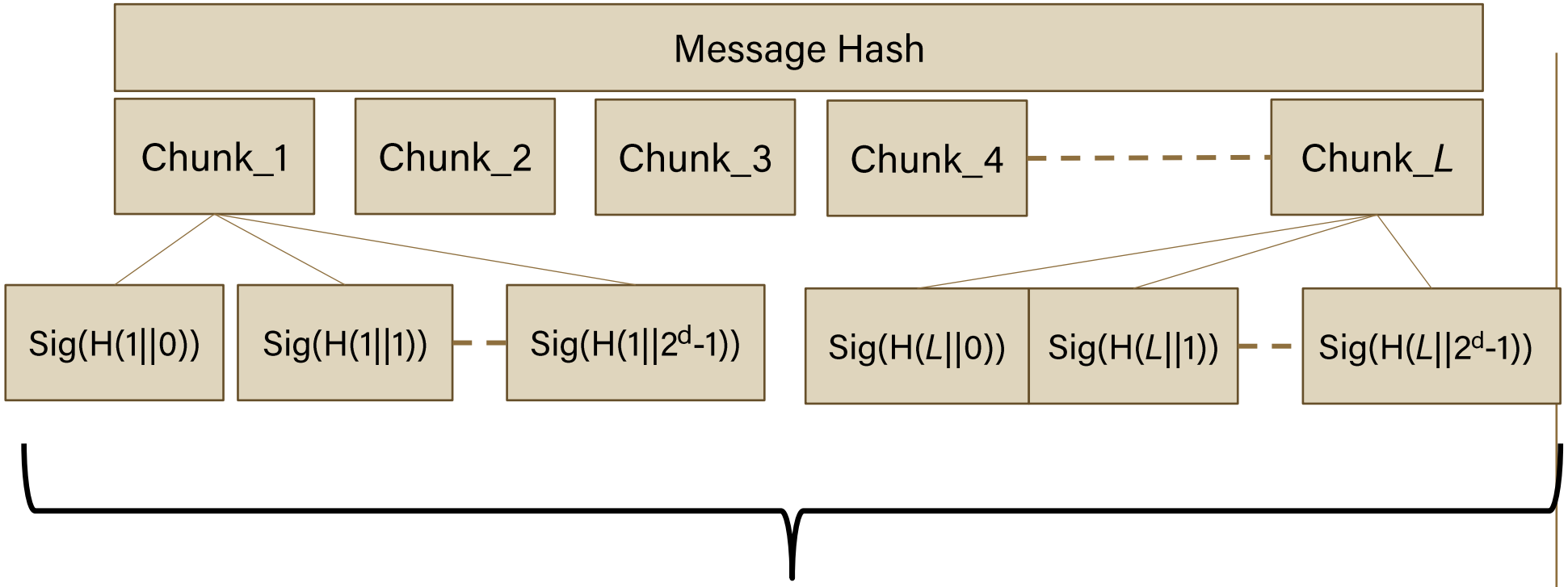
- Do most of the heavy lifting in the offline phase.
  - Calculate signature for all possibilities.
  - Store these signatures in a table.
- Do efficient operations in the online phase.
  - Use this pre-computed table to calculate the actual signature.
- SCRA-C-RSA instantiation.

SCRA – OFFLINE PHASE

- We choose the parameters L and d such that:



SCRA – OFFLINE PHASE

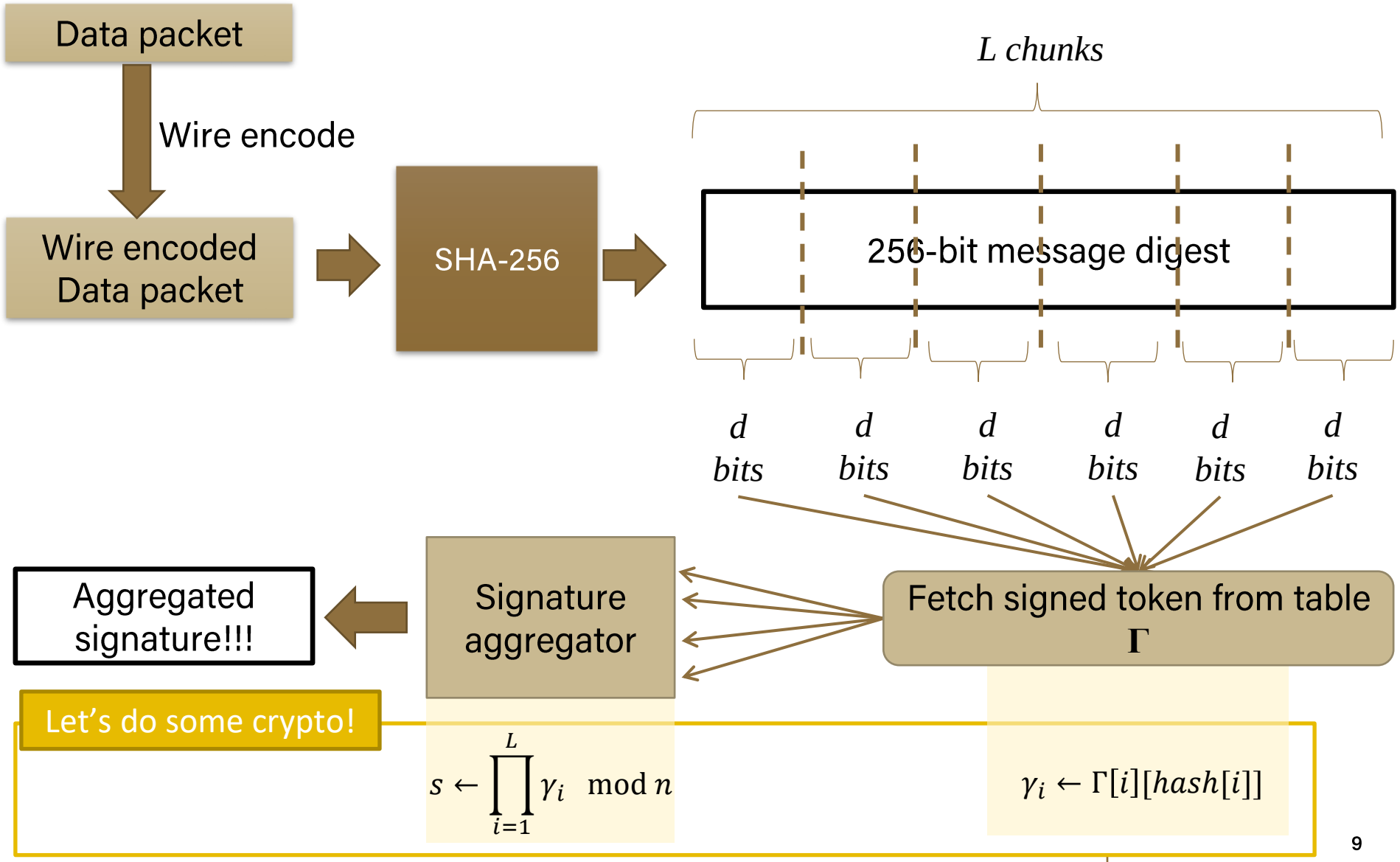


Store this table in memory

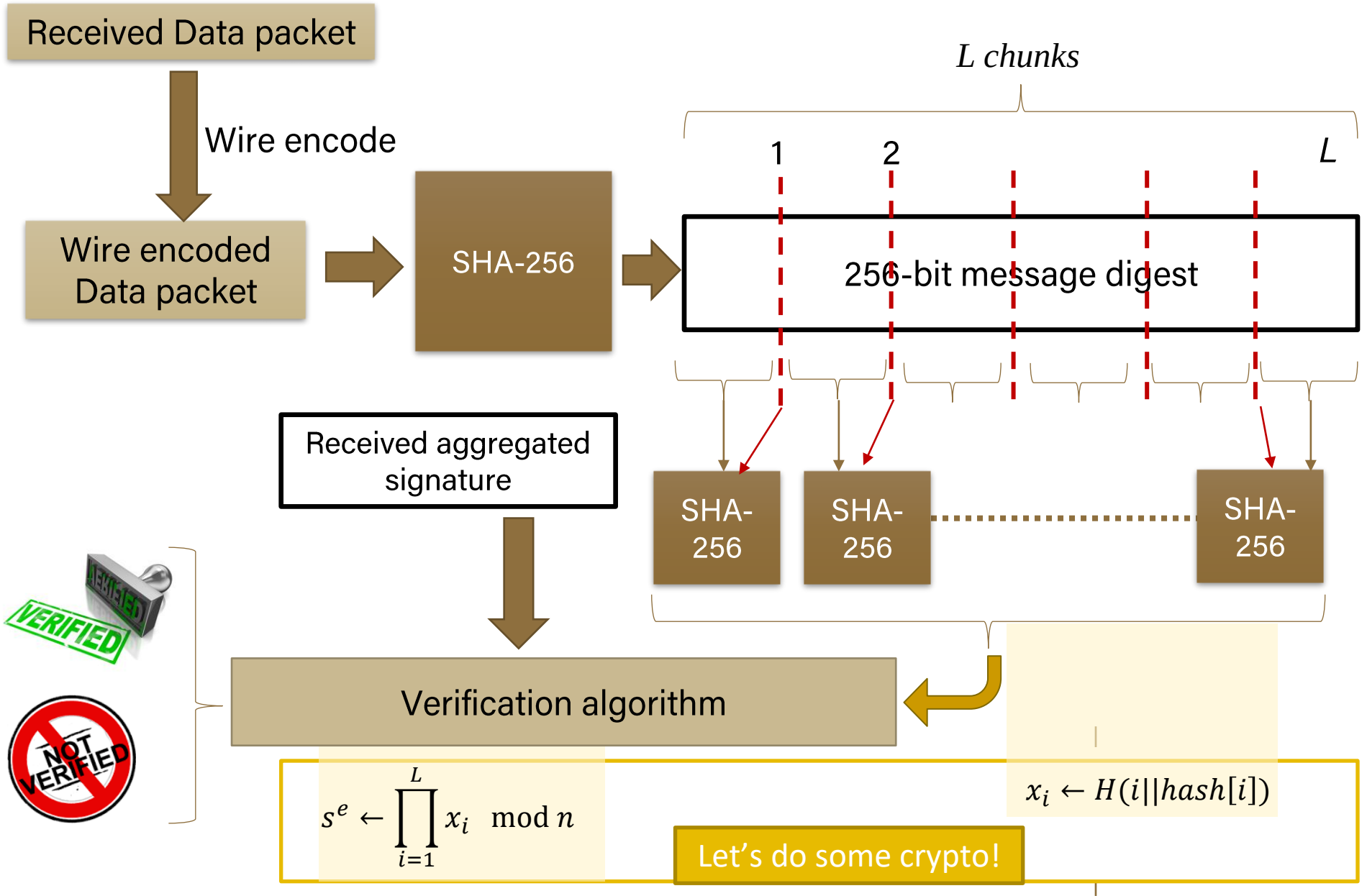
Let's do some crypto!

$$\gamma_{i,j} \leftarrow H(i||j)^u \mod n$$

SCRA – ONLINE PHASE



SCRA – VERIFICATION PHASE



Real-time Application Optimizations

- Signing a bundle of k packets:
  - This reduces the signature size by a factor of k.
  - Costly exponentiation occur one every k packets.
- Probabilistic signing.
- Different values of the parameter L.
- Inherent parallelizability of SCRA.

Performance evaluation

Message authentication with 100-packet signature aggregation

	ECDSA-256	RSA-3072	SCRA-C-RSA [L=32]	SCRA-C-RSA [L=16]
Public key size	91	422	422	422
Average signature size	71	384	**5.82**	**5.82**
Average signing time	**0.059**	1.49	**0.22**	**0.11**
Average verification time	0.10	0.063	**0.040**	**0.02**
End-to-end delay	0.35	1.85	**0.46**	**0.30**

Performance evaluation

Real-time conferencing (NDN-RTC)

	ECDSA-256	RSA-3072	SCRA-C-RSA [L=32]	SCRA-C-RSA [L=16]
Public key size	91	422	422	422
Signature size	**71**	384	384	384
Average signing time	**0.13**	3.17	**0.50**	**0.26**
Total packets signed	7665	7733	7637	7686
Average verification time	0.30	0.12	**0.16**	**0.12**
Total packets verified	1492	1485	1488	1489

ACM ICN 2020 MONTRÉAL

REALTIME DIGITAL SIGNATURES FOR NAMED DATA NETWORKING

Charalampos Katsis
ckatsis@purdue.edu

Ankush Singla
asingla@purdue.edu

Elisa Bertino
bertino@purdue.edu

PURDUE UNIVERSITY | Department of Computer Science