REALTIME DIGITAL SIGNATURES FOR NAMED DATA NETWORKING

Charalampos Katsis
ckatsis@purdue.edu

Ankush Singla
asingla@purdue.edu

Elisa Bertino
bertino@purdue.edu
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.

Is that really YouTube?

Consumer → YouTube → Producer
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
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.
We choose the parameters $L$ and $d$ such that:

$$d \cdot L = b$$

$= 256 \text{ bits}$

- Number of bits per chunk
- Length of the hash output
- Number of chunks we divide the message hash
Let's do some crypto!

\[ y_{i,j} \leftarrow H(i||j)^u \mod n \]
Let's do some crypto!

\[ s \leftarrow \prod_{i=1}^{L} y_i \mod n \]

\[ y_i \leftarrow \Gamma[i][\text{hash}[i]] \]
**SCRA - VERIFICATION PHASE**

- **Received Data packet**
  - Wire encode
  - Wire encoded Data packet

- **SHA-256**
  - 256-bit message digest
  - L chunks

- **Received aggregated signature**

- **Verification algorithm**
  - Let's do some crypto!

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!**

- **Let's do some crypto!
- 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

<table>
<thead>
<tr>
<th></th>
<th>ECDSA-256</th>
<th>RSA-3072</th>
<th>SCRA-C-RSA [L=32]</th>
<th>SCRA-C-RSA [L=16]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public key size</td>
<td>91</td>
<td>422</td>
<td>422</td>
<td>422</td>
</tr>
<tr>
<td>Average signature size</td>
<td>71</td>
<td>384</td>
<td>5.82</td>
<td>5.82</td>
</tr>
<tr>
<td>Average signing time</td>
<td>0.059</td>
<td>1.49</td>
<td>0.22</td>
<td>0.11</td>
</tr>
<tr>
<td>Average verification</td>
<td>0.10</td>
<td>0.063</td>
<td>0.040</td>
<td>0.02</td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-to-end delay</td>
<td>0.35</td>
<td>1.85</td>
<td>0.46</td>
<td>0.30</td>
</tr>
</tbody>
</table>
## Performance evaluation

### Real-time conferencing (NDN-RTC)

<table>
<thead>
<tr>
<th></th>
<th>ECDSA-256</th>
<th>RSA-3072</th>
<th>SCRA-C-RSA [L=32]</th>
<th>SCRA-C-RSA [L=16]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public key size</td>
<td>91</td>
<td>422</td>
<td>422</td>
<td>422</td>
</tr>
<tr>
<td>Signature size</td>
<td>71</td>
<td>384</td>
<td>384</td>
<td>384</td>
</tr>
<tr>
<td>Average signing time</td>
<td>0.13</td>
<td>3.17</td>
<td>0.50</td>
<td>0.26</td>
</tr>
<tr>
<td>Total packets signed</td>
<td>7665</td>
<td>7733</td>
<td>7637</td>
<td>7686</td>
</tr>
<tr>
<td>Average verification time</td>
<td>0.30</td>
<td>0.12</td>
<td>0.16</td>
<td>0.12</td>
</tr>
<tr>
<td>Total packets verified</td>
<td>1492</td>
<td>1485</td>
<td>1488</td>
<td>1489</td>
</tr>
</tbody>
</table>
REALTIME DIGITAL SIGNATURES
FOR NAMED DATA NETWORKING

Charalampos Katsis
ckatsis@purdue.edu

Ankush Singla
asingla@purdue.edu

Elisa Bertino
bertino@purdue.edu