Long-term secure signatures for the IoT

Andreas Hülsing
Hash-based Signature Schemes
[Mer89]

Long-term secure
• Only needs secure hash function
• Post-quantum
• Possibility of hash combiners

IoT compatible?
• Only needs secure hash function
Lamport-Diffie OTS [Lam79]

Message $M = b_1, \ldots, b_m$, OWF $H$  

$\ast$ = n bit
One-time signatures

• Can only be used once
• Basic building block
• Secret keys can be generated pseudorandomly

WOTS⁺ [Hue13]

• Shorter signatures
• Size-speed trade-off
Chain-based OTS
Chain-based OTS [NY89]

- Extremely fast signing via „pebbling“
- Extremely fast verification of sequential signatures
- Small keys
- Small sigs (for sequential signatures)
- Extremely useful in combination with aggregator
- Stateful

Merkle’s signature scheme

SIG = (i=2, \text{signature}, \text{message}, \text{SK})
Merkle’s signature scheme

• Fast signing via „tree traversal algorithms“
• Extremely fast verification
• Small keys
• Medium size sigs
• Stateful

Latest: XMSS-T

(Hülsing, Rijneveld, Song. Mitigating Multi-Target Attacks in Hash-based Signatures. PKC ‘16)
Multi-Tree XMSS \cite{MMM02}

Uses multiple layers of trees

\[ \Theta(2^h) \rightarrow \Theta(d \times 2^{h/d}) \]

\[ \Theta(h/2) \rightarrow \Theta(h/2d) \]
SPHINCS [BHH+15]

• Stateless Scheme
• XMSS\textsuperscript{MT} + HORST + (pseudo-)random index
• Collision-resilient
• Deterministic signing
• SPHINCS-256:
  • 128-bit post-quantum secure
  • Hundrest of signatures / sec
  • 41 kb signature
  • 1 kb keys
Performance on small devices

- STM32L100C development board: Cortex M3, 32MHz, 32-bit architecture, 256KB Flash, 16KB RAM

<table>
<thead>
<tr>
<th></th>
<th>KeyGen</th>
<th>Sign</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMSSMT</td>
<td>278.80s</td>
<td>0.61s</td>
<td>0.16s</td>
</tr>
<tr>
<td>SPHINCS</td>
<td>0.88s</td>
<td>18.41s</td>
<td>0.51s</td>
</tr>
</tbody>
</table>

- Issue: SPHINCS sigs (41KB) don’t fit single APDU
Future

• XMSS Internet Draft in IRSG poll

• At least two SPHINCS submissions for NIST
  • Faster / smaller signatures

• Several works on dedicated hash functions (Haraka, Siempira)
Thank you!
Questions?