CHALLENGES AND OPPORTUNITIES IN POST-QUANTUM CRYPTOGRAPHY FOR NETWORKS AND PROTOCOLS

Sofía Celi
Brave Software, Inc
The state

- NIST ran a process for selection of algorithms to standardise that are safe from quantum computers attacks
  - A first phase of the process ended this month. Announcement of “selected” algorithms for:
    - Key Exchange (KEMs)
    - Authentication (digital signatures)

See NISTs report: https://csrc.nist.gov/publications/detail/nistir/8413/final
### The tradeoffs

#### SIGNATURE ALGORITHMS

<table>
<thead>
<tr>
<th>Scheme Name</th>
<th>Problem</th>
<th>Public key size (bytes)</th>
<th>Signature size (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-2048</td>
<td>Factoring</td>
<td>272</td>
<td>256</td>
</tr>
<tr>
<td>Ed25519</td>
<td>Elliptic curve discrete logarithm</td>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td>Dilithium2</td>
<td>Lattice-based (MLWE/MSIS)</td>
<td>1312</td>
<td>2420</td>
</tr>
<tr>
<td>Falcon-512</td>
<td>Lattice-based (NTRU)</td>
<td>897</td>
<td>666</td>
</tr>
<tr>
<td>Rainbow-l-Classic</td>
<td>Multi-variate equations</td>
<td>161,600</td>
<td>66</td>
</tr>
<tr>
<td>Picnic (L1-FS)</td>
<td>Hash+Block Cipher</td>
<td>32</td>
<td>34032 (max)</td>
</tr>
<tr>
<td>XMSS</td>
<td>Hash-based</td>
<td>32</td>
<td>979</td>
</tr>
<tr>
<td>SPHINCS+ (128s)</td>
<td>Hash-based</td>
<td>32</td>
<td>8080</td>
</tr>
<tr>
<td>SQISign (6983)</td>
<td>Isogeny-based</td>
<td>64</td>
<td>204</td>
</tr>
<tr>
<td>MAYO</td>
<td>Multivariate Quadratic</td>
<td>830</td>
<td>420</td>
</tr>
</tbody>
</table>
The tradeoffs

- Bigger sizes, bigger computational times
- They don’t fit perfectly with all ‘DH-like’ actions
- Some schemes don’t have a perfect post-quantum counterpart:
  - OPRFs
  - Zero-Knowledge proofs
  - Threshold Signatures
Some focus

● Continue with experimentation
● Build designs that are generic for post-quantum but also for other ideas

● Workshop on the challenges/opportunities of putting post-quantum into networks and protocols: PQNet (https://sofiaceli.com/PQNet-Workshop/)
  ○ Next iteration in November (to coordinate with NIST)
  ○ Important notes:
    ■ https://sofiaceli.com/PQNet-Workshop/tls.html
    ■ https://sofiaceli.com/PQNet-Workshop/dnssec.html
● Let’s start discussing over: pqc@ietf.org
THANK YOU!

@claucece