OpenSSL NTRU: experiences integrating a post-quantum KEM into TLS 1.3 via an OpenSSL ENGINE

Speaker: Daniel J. Bernstein
Joint work with: Billy Bob Brumley, Ming-Shing Chen (libsntrup761 leader), Nicola Tuveri (engntru leader)

https://openssllntru.cr.yp.to
OpenSSL NTRU software architecture

Web browser (epiphany), unmodified

fast PQ KEM

TLS terminator (stunnel), unmodified

Back-end web server, unmodified

Optimized PQ software ecosystem is rapidly evolving. Decouple from OpenSSL.

Bernstein, Brumley, Chen, Tuveri openssslNTRU.cr.yp.to
OpenSSL-NTRU software architecture

- Web browser (epiphany), unmodified
- Back-end web server, unmodified
- TLS terminator (stunnel), unmodified

Fast PQ KEM

OpenSSL + reference KEM code

Optimized PQ software ecosystem is rapidly evolving.

Decouple from OpenSSL.

Bernstein, Brumley, Chen, Tuveri

opensslntru.cr.yp.to
OpenSSLNTRU software architecture

Web browser (epiphany), unmodified

OpenSSL + reference KEM code

New ENGINE engntru

TLS terminator (stunnel), unmodified

OpenSSL + reference KEM code

New ENGINE engntru

Back-end web server, unmodified

Optimized PQ software ecosystem is rapidly evolving.

Decouple from OpenSSL.

Bernstein, Brumley, Chen, Tuveri

opensslntru.cr.yp.to
OpenSSLNTRU software architecture

Web browser (epiphany), unmodified

OpenSSL + reference KEM code

New ENGINE engntru

New optimized KEM library

Fast PQ KEM

TLS terminator (stunnel), unmodified

OpenSSL + reference KEM code

New ENGINE engntru

New optimized KEM library

Back-end web server, unmodified

Optimized PQ software ecosystem is rapidly evolving.

Decouple from OpenSSL.

Bernstein, Brumley, Chen, Tuveri opensslntru.cr.yp.to
OpenSSLNTRU software architecture

Web browser (epiphany), unmodified

OpenSSL + reference KEM code

New ENGINE engntru

New optimized KEM library

fast PQ KEM

TLS terminator (stunnel), unmodified

OpenSSL + reference KEM code

New ENGINE engntru

New optimized KEM library

Back-end web server, unmodified

Optimized PQ software ecosystem is rapidly evolving. Decouple from OpenSSL.

Bernstein, Brumley, Chen, Tuveri
opensslntru.cr.yp.to
OpenSSLNTRU cryptography

OpenSSLNTRU adds the new PQ KEM to TLS 1.3. Protocol flow: similar to Google-Cloudflare CECPQ2 experiment.

**Higher performance** than post-quantum component of CECPQ2. New software for **faster key generation**. Also **higher security**.
OpenSSL NTRU cryptography

OpenSSL NTRU adds the new PQ KEM to TLS 1.3. Protocol flow: similar to Google-Cloudflare CECPQ2 experiment.

**Higher performance** than post-quantum component of CECPQ2. New software for faster key generation. Also higher security.

<table>
<thead>
<tr>
<th>NIST submission</th>
<th>ntruhrss701</th>
<th>sntrup761</th>
</tr>
</thead>
<tbody>
<tr>
<td>key+ciphertext traffic</td>
<td>2276 bytes</td>
<td>2197 bytes</td>
</tr>
<tr>
<td>keygen time</td>
<td>272028 cycles</td>
<td>166000 cycles (new)</td>
</tr>
<tr>
<td>enc time</td>
<td>26116 cycles</td>
<td>48780 cycles</td>
</tr>
<tr>
<td>dec time</td>
<td>63632 cycles</td>
<td>59120 cycles</td>
</tr>
<tr>
<td>PQ Core-SVP security</td>
<td>$2^{125}$</td>
<td>$2^{139}$</td>
</tr>
<tr>
<td>cyclotomic concerns</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>used in</td>
<td>CECPQ2</td>
<td>OpenSSLNTRU</td>
</tr>
</tbody>
</table>
OpenSSLNTRU cryptography

OpenSSLNTRU adds the new PQ KEM to TLS 1.3. Protocol flow: similar to Google-Cloudflare CECPQ2 experiment.

**Higher performance** than post-quantum component of CECPQ2. New software for **faster key generation**. Also **higher security**.

<table>
<thead>
<tr>
<th>NIST submission</th>
<th>ntruhrss701</th>
<th>sntrup761</th>
</tr>
</thead>
<tbody>
<tr>
<td>key+ciphertext traffic</td>
<td>2276 bytes</td>
<td>2197 bytes</td>
</tr>
<tr>
<td>keygen time</td>
<td>272028 cycles</td>
<td>166000 cycles (new)</td>
</tr>
<tr>
<td>enc time</td>
<td>26116 cycles</td>
<td>48780 cycles</td>
</tr>
<tr>
<td>dec time</td>
<td>63632 cycles</td>
<td>59120 cycles</td>
</tr>
<tr>
<td>PQ Core-SVP security</td>
<td>$2^{125}$</td>
<td>$2^{139}$</td>
</tr>
<tr>
<td>cyclotomic concerns</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>used in</td>
<td>CECPQ2</td>
<td>OpenSSLNTRU</td>
</tr>
</tbody>
</table>

**kyber768**: faster keygen but has cyclotomic concerns, consumes 2272 bytes, and is threatened by US patents 9094189 and 9246675.