Circuit-extension handshakes for Tor
achieving forward secrecy in a quantum world

John M. Schanck$^{1,2}$    William Whyte$^1$    Zhenfei Zhang$^1$

Security Innovation, Wilmington, MA 01887, USA

Institute for Quantum Computing, University of Waterloo, Waterloo N2H 3G1, Canada

July 20, 2016
Mechanical calculator, circa 1932

source: computerhistory.org
Quantum mechanical calculator, circa 2014

Quantum mechanical calculator, circa 2014

Quantum computers are a real threat

- Currently used public key crypto will be broken.
- We need to take steps now to mitigate risk.
- We should start deploying post-quantum cryptography.
  - Alongside currently used crypto.
Hybrid ciphersuites

Using ECDH now? Switch to ECDH+PostQuantumKEX

Why?
- Low confidence
  - in the security of new primitives and
  - in the reliability of new implementations.
- Regulations (FIPS-140, etc)
Hybrid ciphersuites

Using ECDH now? Switch to ECDH+PostQuantumKEX

Why?
▶ Low confidence
  ▶ in the security of new primitives and
  ▶ in the reliability of new implementations.
▶ Regulations (FIPS-140, etc)
Pre-quantum, transitional, and post-quantum security

Three notions of security for channel establishment protocols

- Secure in a pre-quantum setting
  \[\Leftrightarrow\] pre-quantum auth and pre-quantum confidentiality.

- Secure in a transitional setting
  \[\Leftrightarrow\] pre-quantum auth and post-quantum confidentiality.

- Secure in a post-quantum setting
  \[\Leftrightarrow\] post-quantum auth and post-quantum confidentiality.
Pre-quantum, transitional, and post-quantum security

Three notions of security for channel establishment protocols

- Secure in a pre-quantum setting
  \[ \Leftrightarrow \text{pre-quantum auth and pre-quantum confidentiality.} \]

- Secure in a transitional setting
  \[ \Leftrightarrow \text{pre-quantum auth and post-quantum confidentiality.} \]

- Secure in a post-quantum setting
  \[ \Leftrightarrow \text{post-quantum auth and post-quantum confidentiality.} \]
Transitional security for Tor

Why?

▷ Full take of ciphertexts at an entry node leads to loss of anonymity and secrecy in the future.
▷ Tor users might be targetted by patient, well-funded, adversaries.

How?

▷ Add a post-quantum key encapsulation mechanism to the current circuit-extension handshake, ntor.
One-way authenticated key exchange
Published in 2013

Engineering specification Tor Proposal #216
Deployed since Tor 0.2.4.8-alpha
Anonymous client

\[(x, X) = \text{DHGen}(1^\lambda)\]

Server with long-term DH key \((a, A)\) and identity digest \(\hat{P}\)

\[(y, Y) = \text{DHGen}(1^\lambda)\]

\[\text{pms} = X^y || X^a\]

\[T_1 = \hat{P} || A || X || Y || \text{proto}_id\]

\[T_2 = \hat{P} || A || Y || X || \text{proto}_id || \text{Server}\]

\[vk = \text{HMAC}(t\_verify, \text{pms} || T_1)\]

\[\text{auth} = \text{HMAC}(t\_mac, vk || T_2)\]

\[\text{prk} = \text{HMAC}(t\_key, \text{pms} || T_1)\]

\[K = \text{HMAC}^*(\text{prk}, \text{m\_expand})\]
Anonymous client

\[(x, X) = \text{DHGen}(1^\lambda)\]

Server with long-term DH key \((a, A)\)
and identity digest \(\hat{P}\)

\[(y, Y) = \text{DHGen}(1^\lambda)\]

\[pms = X^y || X^a\]

\[T_1 = \hat{P} || A || X || Y || \text{proto_id} \]

\[T_2 = \hat{P} || A || Y || X || \text{proto_id} || \text{Server} \]

\[vk = \text{HMAC}(t_{\text{verify}}, pms || T_1)\]

\[\text{ensure } \text{auth} = \text{HMAC}(t_{\text{mac}}, vk || T_2)\]

\[\text{prk} = \text{HMAC}(t_{\text{key}}, pms || T_1)\]

\[K = \text{HMAC}^*(\text{prk}, \text{m_expand})\]
Anonymous client

\[(x, X) = \text{DHGen}(1^\lambda)\]

\[\Rightarrow X\]

\[(y, Y) = \text{DHGen}(1^\lambda)\]

\[pms = X^y || X^a\]

\[T_1 = \widehat{P} || A || X || Y || \text{proto}_\text{id}\]

\[T_2 = \widehat{P} || A || Y || X || \text{proto}_\text{id} || \text{Server}\]

\[vk = \text{HMAC}(t_{\text{verify}}, pms || T_1)\]

\[\text{ensure } auth = \text{HMAC}(t_{\text{mac}}, vk || T_2)\]

\[prk = \text{HMAC}(t_{\text{key}}, pms || T_1)\]

\[K = \text{HMAC}^*(prk, m_{\text{expand}})\]

Server with long-term DH key \((a, A)\) and identity digest \(\widehat{P}\)

\[\text{auth} \leftarrow Y, auth\]
Anonymous client

\[(x, X) = \text{DHGen}(1^\lambda)\]

\[X \rightarrow (y, Y) = \text{DHGen}(1^\lambda)\]

Server with long-term DH key \((a, A)\) and identity digest \(\hat{P}\)

\[pms = X^y || X^a\]

\[T_1 = \hat{P} || A || X || Y || \text{proto_id} \]

\[T_2 = \hat{P} || A || Y || X || \text{proto_id} || \text{Server} \]

\[vk = \text{HMAC(t\_verify, pms || T_1)} \]

\[auth = \text{HMAC(t\_mac, vk || T_2)} \]

\[\text{ensure } auth = \text{HMAC(t\_mac, vk || T_2)}\]

\[prk = \text{HMAC(t\_key, pms || T_1)} \]

\[K = \text{HMAC}^*(prk, m\_expand) \]

\[Y, auth \leftarrow pms = Y^x || A^x\]

\[T_1 = \hat{P} || A || X || Y || \text{proto_id} \]

\[T_2 = \hat{P} || A || Y || X || \text{proto_id} || \text{Server} \]

\[vk = \text{HMAC(t\_verify, pms || T_1)} \]

\[auth = \text{HMAC(t\_mac, vk || T_2)} \]

\[prk = \text{HMAC(t\_key, pms || T_1)} \]

\[K = \text{HMAC}^*(prk, m\_expand) \]
Variant of ntor with a proof of security in the pre-quantum Authenticated and Confidential Channel Establishment model (pre-quantum ACCE).
Changes to pre-master secret

- ntor:
  \[ pms = Y^x \parallel A^x \]

- hybrid-null:
  \[ pms = H(A^x) \parallel Y^x \]
Changes to auth tag

- ntor:

\[ T_1 = \hat{P} || A || X || Y || \text{proto}_id \]
\[ T_2 = \hat{P} || A || Y || X || \text{proto}_id || \text{Server} \]
\[ \text{vk} = \text{HMAC-SHA256}(\text{proto}_id: \text{verify}, pms || T_1) \]
\[ \text{auth} = \text{HMAC-SHA256}(\text{proto}_id: \text{mac}, \text{vk} || T_2) \]

- hybrid-null:

\[ T = \hat{P} || A || X || Y \]
\[ \text{prk} = \text{HMAC-SHA256}(T, pms) \]
\[ \text{auth} = \text{HMAC-SHA256}^*(\text{prk}, \text{proto}_id: \text{auth}) \]
Changes to key derivation

- **ntor:**

  \[
  prk = \text{HMAC-SHA256}(\text{proto_id:key_extract}, pms||T_1)
  \]

  \[
  K = \text{HMAC-SHA256}^*(prk, \text{proto_id:key\_expand})
  \]

- **hybrid-null:**

  \[
  prk = \text{HMAC-SHA256}(T, pms)
  \]

  \[
  K = \text{HMAC-SHA256}^*(prk, \text{proto_id:key}).
  \]
Anonymous client

\[(x, X) = DHGen(1^\lambda)\]

Server with long-term DH key \((a, A)\) and identity digest \(\hat{P}\)

\[(y, Y) = DHGen(1^\lambda)\]

\[s_0 = H(X^a)\]
\[s_1 = X^y\]
\[pms = s_0 || s_1\]
\[T = \hat{P} || A || X || Y\]
\[prk = Xtr(T, pms)\]
\[auth = Prf^*(prk, t_{auth})\]

\[pms = H(A^x) || Y^x\]
\[T = \hat{P} || A || X || Y\]
\[prk = Xtr(T, pms)\]
\[auth = Prf^*(prk, t_{auth})\]
\[K = Prf^*(prk, t_{key})\]
Anonymous client

$$(x, X) = \text{DHGen}(1^\lambda)$$

Server with long-term DH key $(a, A)$ and identity digest $\hat{P}$

$$(y, Y) = \text{DHGen}(1^\lambda)$$

$s_0 = H(X^a)$

$s_1 = X^y$

$pms = s_0 || s_1$

$T = \hat{P} || A || X || Y$

$prk = \text{Xtr}(T, pms)$

$auth = \text{Prf}^*(prk, t_{auth})$

$pms = H(A^x) || Y^x$

$T = \hat{P} || A || X || Y$

$prk = \text{Xtr}(T, pms)$

ensure $auth = \text{Prf}^*(prk, t_{auth})$

$K = \text{Prf}^*(prk, t_{key})$

$K = \text{Prf}^*(prk, t_{key})$
Anonymous client

\[(x, X) = \text{DHGen}(1^\lambda)\]
\[(esk, epk) = \text{KeyGen}(1^\lambda)\]

Server with long-term DH key \((a, A)\)
and identity digest \(\hat{P}\)

\[X, epk \rightarrow (y, Y) = \text{DHGen}(1^\lambda)\]
\[s_0 = H(X^x)\]
\[s_1 = X^y\]
\[s_2 \leftarrow \text{M}\]
\[ct = \text{Encaps}(s_2, epk)\]
\[pms = s_0||s_1||s_2\]
\[T = \hat{P}||A||X||Y||epk||ct\]
\[prk = \text{Xtr}(T, pms)\]
\[auth = \text{Prf}^*(prk, t_auth)\]

\[\downarrow Y, ct, auth\]
\[pms = H(A^x) || Y^x \ || \ \text{Decaps}(ct, esk)\]
\[T = \hat{P}||A||X||Y||epk||ct\]
\[prk = \text{Xtr}(T, pms)\]
\[\text{ensure auth = Prf}^*(prk, t_auth)\]
\[K = \text{Prf}^*(prk, t_key)\]
Performance

hybrid instantiated with ntru-ees443ep1.

<table>
<thead>
<tr>
<th></th>
<th>tap</th>
<th>ntor</th>
<th>hybrid</th>
<th>Ghosh-Kate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bytes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client → server</td>
<td>186</td>
<td>84</td>
<td>693</td>
<td>1312</td>
</tr>
<tr>
<td>server → client</td>
<td>148</td>
<td>64</td>
<td>673</td>
<td>1376</td>
</tr>
<tr>
<td><strong>computation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client init</td>
<td>258μs</td>
<td>84μs</td>
<td>661μs</td>
<td>150μs*</td>
</tr>
<tr>
<td>server response</td>
<td>682μs</td>
<td>263μs</td>
<td>306μs</td>
<td>150μs*</td>
</tr>
<tr>
<td>client finish</td>
<td>233μs</td>
<td>180μs</td>
<td>218μs</td>
<td>150μs*</td>
</tr>
<tr>
<td>total</td>
<td>1173μs</td>
<td>527μs</td>
<td>1185μs</td>
<td>450μs*</td>
</tr>
<tr>
<td>% client</td>
<td>42%</td>
<td>50%</td>
<td>74%</td>
<td>67%</td>
</tr>
</tbody>
</table>
Other considerations

1. Tor only allows 505 bytes in CREATE cells
2. Post-quantum keys and ciphertexts are huge

\[
\begin{array}{lcl}
\text{client} & \rightarrow & \text{server} \\
\text{server} & \rightarrow & \text{client}
\end{array}
\]

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Client Size</th>
<th>Server Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIDH $2^{372}3^{239} - 1$</td>
<td>564</td>
<td>564</td>
</tr>
<tr>
<td>NTRU EES443EP1</td>
<td>615</td>
<td>610</td>
</tr>
<tr>
<td>NTRU EES743EP1</td>
<td>1026</td>
<td>1021</td>
</tr>
<tr>
<td>RLWE NEWHOPE</td>
<td>1824</td>
<td>2048</td>
</tr>
</tbody>
</table>

3. Tor Proposal #249 would allow longer handshakes
Other considerations

1. Multi-ciphersuite security.
   ▶ OK to re-use \((a, A)\) between hybrid-null and hybrid-xyz?

2. One-way Anonymity

3. Post-quantum ACCE
   ▶ Active quantum attackers?

4. Symmetric crypto
   ▶ Cipher currently used by Tor doesn’t meet criteria for our proof of security
   ▶ Tor Proposals \#202, \#261 start to address this
Thanks!