Updates

Minor technical changes

“Single-shot” API

Lots of API clarification and editorial cleanup

Test vectors

Interop on Base/PSK between Go (Barnes) and C (Wood) implementations
### Analysis

**Assuming:**
- Gap-DH for DH
- IND-CCA2 for AEAD
- ROM for Extract and Hash
- PRF for Expand

<table>
<thead>
<tr>
<th>Mode</th>
<th>no key compromise</th>
<th>long-term key compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secrecy</td>
<td>Auth¹</td>
</tr>
<tr>
<td>Base</td>
<td>Done</td>
<td>–</td>
</tr>
<tr>
<td>PSK</td>
<td>Done</td>
<td>Done</td>
</tr>
<tr>
<td>Auth</td>
<td>Done</td>
<td>Done</td>
</tr>
<tr>
<td>AuthPSK</td>
<td>Done</td>
<td>Done</td>
</tr>
</tbody>
</table>

CryptoVerif proofs from Ben Lipp at Inria. ¹All messages are replayable. Valid for P-256 and P-521; Curve25519 and Curve448 are WIP.

**Goals:**
- IND-CCA2 Public Key Encryption
- Relevant authentication properties by mode
Status and Next Steps

Status

- Implementation and interop done on Base, PSK modes
- Interop still pending for Auth, AuthPSK modes
- Analysis in progress for key compromise cases, Curve25519 and Curve448, and more correspondence properties e.g. identity binding

Start RGLC?