Open Discussion

John Kelsey (Moderator)

LWC: Who needs it?

What applications should we be targeting?

- IoT? Hardware? ***Anything without an AES instruction?***

- For a target application, we need to think about:
  - Typical message sizes
  - Available space for nonces and tags
  - Associated data
  - Hardware/software capabilities (few gates, low RAM, etc.)

- Unusual applications we should consider?
  - Special constraints in any dimension?

What else should we be asking for?

- Is (AEAD + hashing) enough to cover symmetric LWC needs?

- Should we be looking at other symmetric primitives?
  - DRBGs?
  - Fixed permutations?
  - Tweakable block ciphers?
  - Something else?

Invidious comparisons

- Security comparisons:
  - How well can we compare
    {leakage, side-channel, fault-attack}
    resistance between candidates?
  - Evaluating quality of analysis?
    - Counting is easy, but misses depth of analysis
- Performance comparisons:
  - Some candidates provide optimized implementations
  - Some candidates do hardware or constrained-device implementations
  - Not obvious how to fairly compare with others that don’t.

A quantum leap?

- Should post-quantum security influence the selection process?

- Which models should be considered?

What are we getting wrong?

- Is the standardization process going well?
- Comments regarding the timeline, evaluation criteria, selection process, next steps?
- What are we missing? What should we be doing differently?

Open discussion

- What else should we be talking about right now?