IETF is Quantum-Fragile

PQUIP IETF 122 Bangkok

Deirdre Connolly, SandboxAQ

The Quantum Threat is **Now**

- Store Now, Decrypt Later attacks are in play for current traditional key agreement and secure session establishment
  - Trust Now, Forge Later in play for long-deployed auth roots of trust
- International migration deadlines are on now on the order of years, not decades
- 5 years for US, Germany, etc
- It takes in average 5 years for CFRG to bring a document to RFC
- Many OUTSIDE parties will not use a specification from the IETF unless it is an RFC
- It doesn't matter if we tell them “it's fixed, it's static”, they don't know what that means! RFC == Real Thing

Case: Hybrid KEMs at CFRG

- draft-ounsworth-cfrg-kem-combiners proposed in March 2023
- Not adopted, no call for adoption
  - ‘We’re full, we cannot take on more documents’ (!!!)
- Work already started in LAMPS in 2019 continues
- X-Wing proposed March 2024
- Implemented in multiple places, lots of CFRG support
- Not adopted, no call for adoption
- CFRG Hybrid KEMs
- Design team assembled March-July 2024
- First draft presented March 2025

TWO YEARS

Hybrid KEMs

- Object lesson on need for alacrity and agility
- The whole point of hybrid key establishment is need to move NOW to a quantum-resistant posture, while the PQ primitives, implementations are new, therefore hybridize with trusted traditional key agreement (mostly well know and deployed elliptic curves)
- Everyone is comfortable deploying hybrid key establishment NOW
- Less comfortable deploying pure PQ NOW
- The only org in IETF that has made it POSSIBLE in a standardized manner is TLSWG
    - It does help that TLS 1.3 makes the solution easy and performant, but not that much!
    - Hybrid KEMs are cryptographically boring! It's the existing incompatibilities that have made it complicated

CFRG takes too damned long

- In the last five years, the CFRG published 10 RFCs, median time from I-D to RFC: 62 months (5+ years)
- Mean is over 5 years
- Even ‘solved’ schemes invited to ‘just write it up’ in CRFG take over five years (FROST)
- The time in CFRG is quite long not even including the time /after/ Last Call
- Documents from CFRG/IETF are used outside of the org and they do not distinguish between a CFRG-produced document, Independent Stream, or whatever - it's an RFC and it solves a problem, technical /and/ social
- For many orgs, a draft document, adopted or not, is not enough to start investment into implementation or integration (eg hardware)

As everyone here keeps reminding, an RFC is not an Internet Standard, nor is there an RFC Police

CFRG != CFWG

- Despite what the rest of IETF thinks, CFRG is a research group, not a working group!
- Despite CFRG consensus, chairs will not necessarily bring up popular documents for adoption
- Despite CFRG consensus, will favor a research item instead, which takes longer to finalize
- Despite this, the rest of the IETF assumes CFRG will behave like a working group in both procedure and alacrity
- Other WGs lack confidence in cryptography and defer to the only group in I*TF that claims expertise in cryptography to give them answers/solutions
- Chicken and egg! 🥚🍳🐥

CFRG != CFWG

- “CFRG was supposed to evaluate / handle crypto for us”
- If so, the charter does not reflect that and does not do that in practice
- The charter incentivizes blocking popular, well regarded solutions in favor of CFRG’s home grown ‘research’
    - Except when it decides it likes something and invites them to just specify in CRFG
- This takes far too long and doesn't serve the needs of the IETF in this major cryptographic phase change
- Even when operating according to its charter it doesn't have enough capacity according to the chairs

Case: PQUIP

- Charter is discussion, guidance, informational
- Several documents done/almost done (hybrid signatures, pqc for engineers, etc)
- Non-normative
- Defers to CFRG, NIST, to “validate and develop” PQC mechanisms

Case: Independent Stream

- No cryptography expertise
- Basically defers to CFRG
- Venue of last resort?

Case: SAAG

- draft-paulwh-crypto-components

draft-paulwh-crypto-components

draft-paulwh-crypto-components

- WGs should be able to do whatever wirh their IANA codepoints, including Recommended, MTI, Deprecated whatever
- Just let them adopt and proceed documents towards RFC if there is WG consensus

NOT ‘get a codepoint, wait a few years, discuss again’

NOT ‘avoid RFCs for all crypto where possible’

ADs classify ‘new primitives’ as the only ‘new cryptography’

- Nope.
- Changes to protocols (IKEv2 in IPSEC, CMS, CMP to allow KEMs, generic hybrid key agreement in TLS 1.3) are seemingly not subject to this disuassion
- Why? They are all doing cryptography
- ‘New cryptography’ is not just new primitives that get registered in IAN
- The sizes and API differences in these PQ changes means the protocols will keep changing
- Drawing a line where protocol changes go to RFC but other cryptographic things don't is harmful to successful deployment

Industry is showing signs of fragmentation

- If we don't move quicker, an explosion of non-standardized non- interop PQ solutions are more likely to be deployed to meet PQ needs:

“We're going to see more non standard crypto being deployed at this rate”

“I'm already forced to do that on quite a few cases for PQC”

This is not 2010.

The IETF needs to wake up

- CFRG is not the working group everyone wants it to be
- It takes far too long to standardize the things it does do, and doesn't adopt things people want, adopts things less important
- ADs are proposing to slow down /further/ crypto documents by years
- The only WG that is close to meeting the moment is TLSWG
- LAMPS is coming close (tried to do composite KEMs while CFRG was doing nothing)
- The IETF is trending the wrong direction to support the post-quantum migration in the face of the present threat of store now decrypt later (this applies in less regard to authentication etc)

We’ve never seen a technological shift like this before.

- it's really difficult to get done what the consensus in many groups wants done
- the org solutions set up years ago are not prepared for this epochal change in cryptography in both kind and speed
- This is not Y2K - if things break we won't know it! The adversary will be gathering our plaintext in silence.
- We must be able to move and move now, not in five to ten years
- IETF made a bunch of decisions during a time and paradigm that no longer exists
- We need to stop acting like it does, and not double down on it

‘So what?’

- Let WGs adopt and proceed crypto stuff to RFC, do not dissuade them - let them be like TLSWG
- Consider changing CFRG charter - everyone in IETF expects it to be a WG anyway
- If not that, create a new crypto WG, let CFRG keep doing research, whatever that is; Crypto Engineering Working Group?
- What about an Internet Cryptography Task Force?

Stop getting in the way of consensus.

Time to be crypto agile, not fragile.

IETF is Quantum-Fragile

PQUIP IETF 122 Bangkok

Deirdre Connolly, SandboxAQ