Patents and post-quantum crypto

Paul Hoffman and Sofia Celi

PQUIP WG, IETF 116, Yokohama
March 2023

This is not legal advice

- You get legal advice from lawyers or legal experts with whom you have a contract or agreement
- We are not lawyers or legal experts, and you do not have a contract or agreement with us to give you advice
- This presentation is meant to give factual information to enable discussion of the topic of “patents and post-quantum crypto”

Why we are discussing this

- In 2022, NIST chose CRYSTALS-KYBER as the KEM it intends to standardize
- On NIST's PQC mailing list, there was an active discussion about patents that some people say apply to CRYSTALS-KYBER
- NIST indicates that there are two patent portfolios that relate to CRYSTALS-KYBER

NIST PQC License Summary and Excerpts

- NIST published a detailed description of what it believes are the patents on CRYSTALS-KYBER, and what it is doing about licensing those patents
- “NIST has entered into two patent license agreements to facilitate adoption of NIST’s announced selection...”
- That document may be of interest to you if you intend to implement CRYSTALS-KYBER

What these patents may mean to you

- We don’t know because we are not you
- The NIST license for CRYSTALS-KYBER may or may not apply to you, depending on what you implement
- Some people have said in public that they are not worried about the patents for their implementations
- Some people have said in private that they are very worried about the patents and may not be able to implement CRYSTALS-KYBER

Patents, cryptography, and the IETF

- The IETF has a long history (literally more than 25 years) of dealing with patents and cryptography
- The IETF has rules about intellectual property rights (IPR) and IETF standards, detailed in BCP 79 / RFC 8179
- As of 2023-03-31, the IETF's IPR disclosure page says "No IPR disclosures with the word(s) "kyber" in the Patent Information have been submitted." Searching by WG also didn't turn up any IPR statements relating to Kyber.

More about patents and cryptography

- There may or may not be more patent claims on Kyber, or patent claims on other PQC algorithms
- When someone claims that a particular patent applies to a particular cryptographic implementation, that claim is almost always open to debate
- Different countries have different patent laws and different ways of applying those laws

The mic line (1)

- In previous IETF discussions of patents and cryptography, many comments could be summarized as legal advice (“you should...”, “we shouldn’t...”, and so on)
- Generalized legal advice is not valuable here, even if you have looked heavily into the specifics of the CRYSTALS-KYBER protocol and the patents that NIST has listed

The mic line (2)

- Please don't
- Anything important you were going to say at the mic right now would be much more useful on the PQUIP WG mailing list so that what you say can be thoughtfully discussed, and reasonable discussion threads can form
- Having said that, if anything in this presentation is not factually correct, by all means please call it out at the mic