From: Dworkin, Morris J.
To: Chen, Lily
Cc: Moody, Dustin; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Perlner, Ray; Jordan, Stephen P; Liu, Yi-Kai; Peralta, Rene; Dworkin, Morris J.; Scholl, Matthew
Subject: Re: IPR question for PQC
Date: Friday, January 29, 2016 12:50:04 PM

Thanks, LIly.

My understanding of the SHA-3 competition, and the AES competition before it, is that the IPR rights were only waived conditionally, e.g., for the purposes of vetting, and in the event that NIST standardized the algorithm. (We also requested that submitters disclose IPR that they thought might read on *other* candidates, although I don’t think we had any way of enforcing this request.) Therefore, the question of “returning” the rights should’t arise—my intuition is that something like Option 1 should be workable even for an informal, ongoing process.

The main issue is whether we can expect to obtain acceptable algorithms under Option 1. The block cipher modes process operates under Option 2, because the possibilities for modes are more limited than for the underlying block cipher, and we don’t always know in advance what properties will be required of the mode. For example, we’re about to approve modes for format-preserving encryption that are encumbered by IPR, because we don’t have any good, royalty-free methods that achieve the same properties.

For PQC, perhaps it would be useful to examine the scope of existing patents (e.g., NTRU’s, I assume?) to help inform this decision.

Morrie

On Jan 29, 2016, at 10:43 AM, Chen, Lily <lily.chen@nist.gov> wrote:

> I include Morrie. Morrie has discussed with lawyers on IPR issues for some modes. I also include Matt since I think we need to talk with NIST general council. We need to format our question and find a right person to talk with the lawyers.
>
> Lily
>
> **From:** Moody, Dustin
> **Sent:** Friday, January 29, 2016 9:47 AM
> **To:** Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Chen, Lily; Perlner, Ray; Jordan, Stephen P; Liu, Yi-Kai; Peralta, Rene
> **Subject:** IPR question for PQC
>
> Everyone,
> We have (it seems to me) two possible ways we can approach the IPR issue in our call:
>
> 1) Require that there is no royalties, no IPR, require patent disclosures, etc.. during our process. Right will be returned to the submitters if we do not

standardize their algorithm. This is similar to what was done with SHA-3, which then returned the rights to the submitters of the algorithms that weren't selected. If we do it this way, when would we return the rights? We're describing this as kind of like the modes process, where even if we don't initially choose to standardize an algorithm, it doesn't meet that it is "out".

2) We could ask for patent disclosures, but not require algorithms be royalty-free. We would need to warn submitters that it is obviously a big advantage to submit IPR free algorithms, as it will be a big factor in our decision.

Any thoughts? Do we need to get the advice of Matt/Donna/lawyers?

Dustin