From: Liu, Yi-Kai (Fed)
To: Alperin-Sheriff, Jacob (Fed); Chen, Lily (Fed)
Cc: Moody, Dustin (Fed)
Subject: Re: Talking to Outside Parties and Stakeholders
Date: Tuesday, August 16, 2016 11:49:09 AM

Hi Jacob,

Lily and Dustin can probably tell you more, but I think the simplest strategy is the following: you should talk with other people from your perspective as an independent researcher, NOT claiming to represent NIST's position.

So, you can say that you think having more Ring-LWE challenges would benefit the whole PQC research community, which includes NIST. But write it in a way that indicates it is your personal opinion, not an official statement from NIST.

I hope this helps!

--Yi-Kai

_____

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, August 16, 2016 10:12 AM
To: Chen, Lily (Fed)
Cc: Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: Talking to Outside Parties and Stakeholders

Okay, so I need some specific and general guidance.

The specific case: Chris Peikert (and one of his students) is in the process of issuing Ring-LWE challenges. https://groups.google.com/forum/?utm_medium=email&utm_source=footer#!msg/cryptanalytic-algorithms/z9NnZwFRdA0/9qNA9OvwAgAJ.

The challenges are limited to instances over cyclotomic rings only, and I think it would be very useful for the PQC standardization project if they were to also issue some challenges over (the ring of integers of) some non-cyclotomic number fields as well. In particular, I would like to see it over examples of number fields that Dan Bernstein has been advocating for a while as superior to cyclotomic rings (namely over those (of degree n) whose Galois group is the entire symmetric group on n letters (S_n), and for moduli such that Z_q[x]/<f(x)> is a field, which is never the case for any modulus q when f(x) is a cyclotomic polynomial of index 2^k (where k>1), and in particular f(x)=x^p-x-1), so we can see if any algorithms that come out of it perform (significantly) better in one case or the other.

These challenges are also only for the search version of ring-LWE, whereas the security of cryptosystems is generally based on the decision version of the problem, making it less optimal for estimating real security using this results.
Search-to-decision reductions do exist for the problem over cyclotomic fields, they are not super tight and as published, are limited to certain moduli (although I believe they can be extended to all moduli via “modulus switching,” this comes at an additional cost in the relative magnitude of the error, and as far as I know such a reduction has not been published it). Moreover, for number fields of the type proposed by Bernstein, I don’t know that any such search-to-decision reductions exist at all.

Can I ask them about this?

More generally:

What can my interactions be with various stakeholders in the PQC standardization process, both (in cases like this)

as a representative of NIST and also (e.g. In outside research not directly related to PQC standardization or other NIST initiatives) in general.

And do I have to ask you first each time or can I just use my best judgement?
Thanks.

—Jacob Alperin-Sheriff