From: Alagic, Gorjan (Assoc)
To: Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed)
Subject: Re: fourier sampling attacks
Date: Friday, June 26, 2020 7:37:42 PM

I see, so the permutation is not well-defined unless you actually know the private code M. I guess the point is that this attack only makes sense in some setting in which the adversary has already learned M through some other means, and now wants to learn S and P to get the complete private key. Maybe that's an interesting setting and maybe it isn't, but (if memory serves) the classical support splitting attack can already finish the job from M, so a lower bound on some fancy quantum attack is not helpful.

And, on second thought, I don't see how "known M" could be interesting against, say, Classic McEliece. There it seems to me that S and P are just the operators resulting from applying the systematic form algorithm to M. So for them, M is just the private key and the systematic form of M is the public key. So then it seems like learning M is just the whole job. Is that right?

Gorjan

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Friday, June 26, 2020 3:11 PM
To: Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: RE: fourier sampling attacks

Looking up “support splitting” I found this: https://hal.inria.fr/inria-00073037/document . I don’t see any claim that this only works on specific types of codes. So I suppose the criticism should be equally valid for QC-MDPC codes.

Also notable is that searching for the permuation P isn’t a particularly exciting goal for either Goppa codes or QC-MDPC codes. Iirc, any permutation of a Goppa code is also a Goppa code, so finding the permutation is completely unnecessary (and in fact shouldn’t be possible, since every choice of the permutation is possible with an equivalent key.) For QC-MDPC codes, the public key retains the quasi-cyclic structure of the private key. I think there are only something like r^4 permutations of the code that are compatible with the underlying quasicyclic structure. Moreover, any of these permutations of the private key will also be a valid private key, so there is also nothing to learn here. I guess the permutation is well defined if you already know what the private code is supposed to be, beyond its structure, but you don’t. So, I’m not sure what relation this problem is supposed to have to breaking the cryptosystem.

Ray

From: Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>

Sent: Friday, June 26, 2020 2:11 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: fourier sampling attacks

Hi Ray and Yi-Kai,

Do you guys remember this paper about lower bounds for hidden-subgroup-style quantum attacks on Niederreiter?

[1] https://link.springer.com/content/pdf/10.1007%2F978-3-642-22792-9_43.pdf

Recently it looks like some people have tried to establish similar results but for Niederreiter with quasi-cyclic codes. I'm wondering if this has any value. If I remember right, one fundamental criticism of [1] was that, in the "known-code" model that they are working in, there are already good classical attacks (support splitting, I think they were called?) I guess the "known-code" model is where you know the code M and its scrambled version SMP but not the scrambling operators S and P, whereas in the real world I suppose you know only SMP and the whole triple (S, M, P) is private. (Now [1] of course did lots of interesting technical work, so this is just a comment about applicability to real-world security of McE etc.)

Do you guys know if this same criticism applies if one looks at quasi-cyclic codes? Are there fast classical attacks against those schemes in the known-code model?

Hope that makes sense! Thanks,
Gorjan