From: BongHo Kang <bonghokang@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] LWE based PQC algorithm can be broken?
Date: Tuesday, May 03, 2022 04:02:45 AM ET

Dear PQC Forum,
Recently, I have found a paper that the LWE based PQC algorithms can be broken when applying the divide-and-conquer strategy with the help of quantum computers according to the paper.

"Quantum solvability of noisy linear problems by divide-and-conquer strategy"

http://arxiv-export-lb.library.cornell.edu/pdf/1908.06229

Could you somebody can answer whether there is a possibility of being broken regarding the lattice based algorithms such as NTRU (Ring-LWE), Kyber(LWE), and SABER (LWR)?

If there is a possibility, what would be the resolution?

Regards,

BongHo Kang.

--

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: BongHo Kang <bonghokang@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] LWE based PQC algorithm can be broken?
Date: Tuesday, May 03, 2022 07:49:38 AM ET

Hello,

On Tue, May 3, 2022 at 4:02 AM BongHo Kang <bonghokang@gmail.com> wrote:

> Dear PQC Forum,
> Recently, I have found a paper that the LWE based PQC algorithms can be broken when applying the divide-and-conquer strategy with the help of quantum computers according to the paper.

This paper does not claim anything about breaking LWE or PQC algorithms.

The problem considered in the paper is not LWE; instead, it is one where “noisy linear samples” are given in *quantum superposition* (by contrast, LWE samples are purely classical). It has been known for several years that such problems can be easy for quantum computers; see references [7,8] in the paper (and there might be even earlier results).

Sincerely yours in cryptography,

Chris

--

From: BongHo Kang <bonghokang@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: cpei...@alum.mit.edu <cpeikert@alum.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>, BongHo Kang <bonghokang@gmail.com>
Subject: Re: [pqc-forum] LWE based PQC algorithm can be broken?
Date: Tuesday, May 03, 2022 10:16:30 PM ET

Dear Professor Chris,
I really appreciate your quick response and clear explanation.

I see it is known issue and not related to LWE or PQC algorithms.

Regards,

BongHo Kang.

On Tuesday, May 3, 2022 at 8:49:33 PM UTC+9 cpei...@alum.mit.edu wrote:

> Hello,
>
> On Tue, May 3, 2022 at 4:02 AM BongHo Kang <bongh...@gmail.com> wrote:
>
> > Dear PQC Forum,
> > Recently, I have found a paper that the LWE based PQC algorithms can be broken when applying the divide-and-conquer strategy with the help of quantum computers according to the paper.
>
> This paper does not claim anything about breaking LWE or PQC algorithms.
>
> The problem considered in the paper is not LWE; instead, it is one where “noisy linear samples” are given in *quantum superposition* (by contrast, LWE samples are purely classical). It has been known for several years that such problems can be easy for quantum computers; see references [7,8] in the paper (and there might be even earlier results).
>
> Sincerely yours in cryptography,
>
> Chris

--
You received this message because you are subscribed to the Google Groups "pqc-forum"

group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/08bf9593-eda2-483d-99b5-6d8969f59eaen%40list.nist.gov.