From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Distributed Shor's algorithm
Date: Friday, July 15, 2022 04:30:30 PM ET

Came across this new paper released this week and wanted to share with the group.

https://arxiv.org/abs/2207.05976
Compared with the traditional Shor's algorithm that uses multiple controlling qubits, this algorithm reduces nearly L/2 qubits and reduces the circuit depth of each computer.

--

From: Dan Collins <dcollinsn@gmail.com> via pqc-forum@list.nist.gov
To: Doge Protocol <dogeprotocol1@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Distributed Shor's algorithm
Date: Saturday, July 16, 2022 09:58:23 PM ET

There have been many other improvements to Shor's algorithm in the decades since it was discovered. Does this represent an improvement to the state of the art? I have a note that factoring a large integer is estimated to require 2N+3 ideal qubits, where N is the bitlength of the integer, see for example https://arxiv.org/pdf/quant-ph/0205095.pdf . That 2003 result appears to already be a superior result to the 5L/2 (plus some constant terms) described in the paper which you have linked.

Regards,

Dan

On Fri, Jul 15, 2022 at 4:30 PM Doge Protocol <dogeprotocol1@gmail.com> wrote:

> Came across this new paper released this week and wanted to share with the group.
>
> https://arxiv.org/abs/2207.05976
> Compared with the traditional Shor's algorithm that uses multiple controlling qubits, this algorithm reduces nearly L/2 qubits and reduces the circuit depth of each computer.
>
> --
> 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/db315a1b-c21a-4030-864f-3d81e7fcb0c3n%40list.nist.gov.

--
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/CA%2Btt54%2BH%3DFDvQVE9V4mX4C446VzzKur-Ygb87aeHCYKP%3D9giag%40mail.gmail.com.