From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Paper claims to break RSA-2048 with only 372 physical quibits
Date: Tuesday, January 03, 2023 06:57:58 PM ET

By now many in this forum would have likely read this paper that is being widely discussed.
https://arxiv.org/pdf/2212.12372.pdf

Factoring integers with sublinear resources on a superconducting quantum processor

We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm.

Questions for this forum:

1) How feasible is this approach for RSA-2048 and above?

2) Some companies have informed they will release 1000 qubit+ processors as early as 2025. If claims in the paper holds true for higher qubits, shouldn't the industry move faster to adopt PQC (such as for CNSA suite 2.0 timelines)

3) Can this approach be modified to break elliptic curve cryptography?

4) With some updates, Can the approach in the paper be used against any currently known PQC ?

From: Paulo Barreto <pbarreto@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] Paper claims to break RSA-2048 with only 372 physical quibits
Date: Tuesday, January 03, 2023 09:04:56 PM ET

I presume this claim should not be unduly hard to check, what with IBM's recent announcement of a 433-qubit Osprey processor and accompanying Qiskit. Anybody from IBM out there willing to have a look into this?

On Tue, Jan 3, 2023 at 3:57 PM Doge Protocol <dogeprotocol1@gmail.com> wrote:

> By now many in this forum would have likely read this paper that is being widely discussed.
> https://arxiv.org/pdf/2212.12372.pdf
>
> *Factoring integers with sublinear resources on a superconducting quantum processor*
>
> *We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm.*
>
> Questions for this forum:
>
> 1) How feasible is this approach for RSA-2048 and above?
>
> 2) Some companies have informed they will release 1000 qubit+ processors as early as 2025. If claims in the paper holds true for higher qubits, shouldn't the industry move faster to adopt PQC (such as for CNSA suite 2.0 timelines)
>
> 3) Can this approach be modified to break elliptic curve cryptography?
>
> 4) With some updates, Can the approach in the paper be used against any currently known PQC ?
>
> --
> 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/327d2e43-fe98-4238-b05f-9ecf65081cf3n%40list.nist.gov.

--

From: Markku-Juhani O. Saarinen <mjos.crypto@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: pbar...@gmail.com <pbarreto@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, dogepr...@gmail.com <dogeprotocol1@gmail.com>
Subject: Re: [pqc-forum] Paper claims to break RSA-2048 with only 372 physical quibits
Date: Wednesday, January 04, 2023 02:22:07 AM ET

Hi,

It should be noted that the paper does not claim that the proposed method is faster than classical factoring methods. When the paper talks about "resources," it omits "running time"; what is merely claimed is that the quantum circuit is very small.

The "sublinearity" means that it can be smaller in qubits than the number being factored. This is a hybrid classical+quantum method; the number N must be held on a classical computer. Based on very rough heuristics, it appears to have an exponential running time in this setting.

The proposed method is not in any way related to Shor's factoring algorithm (which actually runs in polynomial time.) It is instead based on classical Schnorr’s algorithm [29, 30], which is (putting it politely) controversial. Certainly, the experimental analysis in "This destroys the RSA cryptosystem" paper [30] is deeply flawed, and researchers have been unable to find support for its claims. Léo Ducas has a nice set of notes about claims of factoring by methods of this type at: https://github.com/lducas/SchnorrGate

As for the impact on actual PQC algorithms, there is no indication of an asymptotic (exponential) speed-up for CVP, which would potentially impact lattice-based systems. Perhaps something like the "Babai optimizer" can shave off some bits from the concrete security analysis. However, this would be merely a constant-factor improvement.

Best Regards,

- markku

On Wednesday, January 4, 2023 at 2:04:50 AM UTC pbar...@gmail.com wrote:

> I presume this claim should not be unduly hard to check, what with IBM's recent announcement of a 433-qubit Osprey processor and accompanying Qiskit. Anybody from IBM out there willing to have a look into this?

> On Tue, Jan 3, 2023 at 3:57 PM Doge Protocol <dogepr...@gmail.com> wrote:
>
>> By now many in this forum would have likely read this paper that is being widely discussed.
>> https://arxiv.org/pdf/2212.12372.pdf
>>
>> *Factoring integers with sublinear resources on a superconducting quantum processor*
>>
>> *We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm.*
>>
>> Questions for this forum:
>>
>> 1) How feasible is this approach for RSA-2048 and above?
>>
>> 2) Some companies have informed they will release 1000 qubit+ processors as early as 2025. If claims in the paper holds true for higher qubits, shouldn't the industry move faster to adopt PQC (such as for CNSA suite 2.0 timelines)
>>
>> 3) Can this approach be modified to break elliptic curve cryptography?
>>
>> 4) With some updates, Can the approach in the paper be used against any currently known PQC ?
>
>> --
>> 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+...@list.nist.gov.
>> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/327d2e43-fe98-4238-b05f-9ecf65081cf3n%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/be43a270-4dbf-4d63-b023-5f25c6be6140n%40list.nist.gov.