

From: [Scholl, Matthew A. \(Fed\)](#)
To: [Kuhn, D. Richard \(Fed\)](#); [Chandramouli, Ramaswamy \(Fed\)](#)
Subject: Re: Intel creates chip to control quantum computers
Date: Monday, December 9, 2019 1:59:55 PM

Yes. Jake Taylor at OSTP gave me an estimated number and it was a million GOOD qbits.

----- Original Message -----

From: "Kuhn, D. Richard (Fed)" <d.kuhn@nist.gov>
Date: Mon, December 09, 2019 1:27 PM -0500
To: Timothy Grance (b) (6), "Scholl, Matthew A. (Fed)"
<matthew.scholl@nist.gov>, "Chandramouli, Ramaswamy (Fed)"
<ramaswamy.chandramouli@nist.gov>
Subject: Re: Intel creates chip to control quantum computers

I haven't see any estimates on number of qubits, but Lily must have an idea. All the date estimates I have seen when public keys are at risk seem to still be way out though.

Rick Kuhn
National Institute of Standards & Technology
Email kuhn@nist.gov Ph +1 301-975-3337
<https://www.nist.gov/people/d-richard-kuhn>

From: Timothy Grance (b) (6)
Date: Monday, December 9, 2019 at 6:34 AM
To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Kuhn, D. Richard (Fed)"
<d.kuhn@nist.gov>, "Chandramouli, Ramaswamy (Fed)"
<ramaswamy.chandramouli@nist.gov>
Subject: Intel creates chip to control quantum computers

do we have any informed speculation, official or otherwise on how many quality qubits it would take to break public key? somewhere in the range of 1 million or so? this tells me, albeit an untutored mind on the topic, that it will be a while before we hit that threshold. we might have a real quantum computer by 2030, but not with the coherence and quality needed to break public key.

tim

Intel creates chip to control quantum computers

<https://www.reuters.com/article/us-intel-tech/intel-creates-chip-to-control-quantum-computers-idUSKBN1YD1NE?il=0>

Sent from [Flipboard](#)

Sent from my iPad