Quantum Computers Pose a Security Threat That We're Still Totally Unprepared For (technologyreview.com)

Posted by BeauHD on Wednesday December 05, 2018 @10:30PM from the depressing-but-probably-accurate dept.

An anonymous reader quotes a report from MIT Technology Review: *The world relies on encryption to protect everything from credit card transactions to databases holding health records and other sensitive information. A new report from the U.S. National Academies of Sciences, Engineering, and Medicine says we need to speed up preparations for the time when super-powerful quantum computers can crack conventional cryptographic defenses. The experts who produced the report, which was released today, say widespread adoption of quantum-resistant cryptography "will be a long and difficult process" that "probably cannot be completed in less than 20 years." It's possible that highly capable quantum machines will appear before then, and if hackers get their hands on them, the result could be a security and privacy nightmare.*

Today's cyberdefenses rely heavily on the fact that it would take even the most powerful classical supercomputers almost unimaginable amounts of time to unravel the cryptographic algorithms that protect our data, computer networks, and other digital systems. But computers that harness quantum bits, or qubits, promise to deliver exponential leaps in processing power that could break today's best encryption. The report cites an example of encryption that protects the process of swapping identical digital keys between two parties, who use them to decrypt secure messages sent to one another. A powerful quantum computer could crack RSA-1024, a popular algorithmic defense for this process, in less than a day. The U.S., Israel and others are working to develop standards for quantum-proof cryptographic algorithms, but they may not be ready or widely adopted by the time quantum computers arrive.

"[I]t will take at least a couple of decades to get quantum-safe cryptography broadly in place," the report says in closing. "If that holds, we're going to have to hope it somehow takes even longer before a powerful quantum computer ends up in a malicious hacker's hands."

hardware security software

→
FCC Chairman Admits Russia Meddled In Net Neutrality Debate
Recruiters Are Still Complaining About No-Shows At Interviews
Should Developers Abandon Agile?
Hackers Who Attended Black Hat and DefCon Conferences Say Hotel Security Personnel Demanded Access To Their Rooms
'Kernel Memory Leaking' Intel Processor Design Flaw Forces Linux, Windows Redesign
China Infiltrated Apple, Amazon and Other US Companies Using Spy Chips on Servers, According To Bloomberg; Apple, and Amazon, Among Others Refute the Report
Submission: Quantum Computers Pose a Security Threat That We're Still Totally Unprepared For
Australia Passes Anti-Encryption Laws [Update]

Quantum Computers Pose a Security Threat That We're Still Totally Unprepared For 1 More | Reply Login
Quantum Computers Pose a Security Threat That We're Still Totally Unprepared For
Post Load All Comments
Search 41 Comments Log In/Create an Account
Comments Filter:
- All
- Score:
- 5 Insightful
- 4 Informative
- 3 Interesting
- 2 Funny

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

- **Re: (Score:2)**
by ShanghaiBill (739463)
Most sites actually care use either 4096-bit RSA or have switched to EC at a comparable bit-strength.
What about the sites that don't care, but should?

- **Re: (Score:2)**
by gweihir (88907)
Meanwhile, the NSA has buried a lot of backdoors in ECC curves and is now running scared they could leak...

- **Don't worry, we're prepared (Score:1)**
by covfefe (4978779)
I was prepared for the 3D printing revolution! Then came the private space colonies! Then came the AI revolution! I'm ready!
- 3 hidden comments

- **Re: (Score:2)**
by ShanghaiBill (739463)
Don't forget hydrogen fuel cells! Remember those?
You should not ridicule hydrogen fuel cells. They turned out to not be the best solution, but when facing a critical need the best approach is a Flooding Algorithm [wikipedia.org], where you research every plausible solution. It is important to not only identify what works, but also what doesn't work. The cost of the research failures is negligible compared to the benefit of finding the best alternative transportation technology.

- **Good thing quantum computers don't work (Score:4, Interesting)**
by goombah99 (560566) on Wednesday December 05, 2018 @11:25PM (#57757288)
A few days ago one of the slashdot articles explained why quantum computers of a significant size will never be possible.
Which is right?
Reply to This Parent Share
twitter facebook linkedin
Flag as Inappropriate
- 2 hidden comments
- **Re: (Score:2)**
by MrMr (219533)
In a few years we can claim we knew it all along. At least for one of the stories.
- **Re: (Score:2)**
by angel'o'sphere (80593)
Well, the other stories fold into ... nothing ...
- **Re: (Score:1)**
by michelcolman (1208008)
Until you open the box.
- **Re: (Score:2)**
by angel'o'sphere (80593)
That is obvious: /. is right!!
- **Re: (Score:2)**
by arglebargle_xiv (2212710)
The one that says it's not possible. However, "post-quantum" is a really hot buzzword, possibly even hotter than "blockchain" now that one's burning out, so there's a lot of academic kudos and, once someone figures out how to commercialise it, money to be made peddling quantum crypto anything. The hype cycle tends to be 3-5 years before disillusionment, so we've got awhile to go yet.
For my part, I predict we'll have fusion reactors and Mars colonies before we have quantum cryptanalysis, so there's pl

- **Malicious hacker? (Score:3)**
by Anubis IV (1279820) on Wednesday December 05, 2018 @10:41PM (#57757104)
You mean like every hostile or competing nation state?
Reply to This Share
twitter facebook linkedin
Flag as Inappropriate
- 1 hidden comment

- **hope (Score:1)**
by Ryan adiputra (5490498)
"it will take at least a couple of decades to get quantum-safe cryptography broadly in place", I hope this will happen soon
- 2 hidden comments
- **Re: (Score:2)**
by jpaine619 (4874633)
It's no big deal really, the resources to do much with it are so insane that only a few people have it - and so intel agencies will watch - and if they use it for cracking, off goes their internet nationally. Fuck China lol.
Guess you haven't been keeping up with what quantum computing is all about.. Gonna be hard to spy on anyone when they are using quantum networking.. Observe a single bit and the sender/receiver know they're being watched..
- 3 hidden comments
- **Re: (Score:2)**
by gweihir (88907)
Funny story: All these systems have been broken so far. Turns out that the perfect theory does not translate to a perfect implementation.
- **Re: (Score:2)**
by jpaine619 (4874633)
One time pads.. Totally safe against quantum computers.. There are ways of distributing those safely when your adversary is online.
- 1 hidden comment
- **Re: (Score:2)**
by gtall (79522)
Yep, this is the answer. We'll install SneakerNet along side our Electron Challenged Networks to distribute the one-time pads. Oh, and no sneaky allowing your one-time pads escape into the wild, keep them close to your body.

Re: **(Score:2)**
by gweihir (88907)
I hope this will happen never. There is not need for it and changing things without need is just incredibly bad engineering because it always causes problems.

Re: **(Score:2)**
by jpaine619 (4874633)
No.. no.. I believe there are a couple of quantum computers out there.. They're only going to get better/smaller.. Things don't tend to get larger/worse...
1 hidden comment

Re: **(Score:2)**
by gweihir (88907)
Indeed. Some people just cannot let go of a bad idea, possibly because they have no other skills...

Pure bullshit on a level with ... **(Score:5, Insightful)**
by CaptainDork (3678879) on Wednesday December 05, 2018 @11:09PM (#57757228)
... scary AI.
I swim in the quantum theory waters and it's goddam near impossible to rake the jiggle out of one qubit. The temperature has to be at near-absolute zero and Heisenberg's Uncertainty Principle plus all of the laws of thermodynamics and the properties of quantum vacuum are working against us.
As the qubit count increases, the randomness multiplies at an exponential rate. It's a nice dream, as is the ***theory*** of AI killing us all, but the hurdles are too great.
In the spirit of, "never say never," a practical quantum computer is at least 100 years away.
And here's the 411 on the encryption fear, anyway: A quantum computer that could instantly break today's encryption could just as quickly create encryption that is impossible to break.
Reply to This Share
twitter facebook linkedin
Flag as Inappropriate
6 hidden comments

Re: **(Score:1)**
by gravewax (4772409)
no, their was a retard on here claiming it is only 3 or 4 years away.
3 hidden comments

Re: **(Score:2)**
by gravewax (4772409)
Yep but their are quite a few clueless individuals that look at X number of Qubits that have been successfully tested and think that somehow translates into the ability to turn this into an operational quantum computer (i.e. one that can operate for any length of time that would make such encryption breaking calculations possible). They don't seem to grasp the massive gulf between what we have now and where we need to get too.

Re: **(Score:1)**
by Anonymous Coward
Don't call people retards when you don't know the difference between there and their.
1 hidden comment

Re: **(Score:3)**
by Actually, I do RTFA (1058596)
And here's the 411 on the encryption fear, anyway: A quantum computer that could instantly break today's encryption could just as quickly create encryption that is impossible to break.
The difference is the NSA, and other government agencies (in various countries) will be the only ones able to afford quantum computers.

Re: **(Score:3)**
by CaptainDork (3678879)
Your point is well taken. Cost is a factor (ignoring the fact that QC can'y get that big). As the qubit count rises, the structure necessary to combat the three evils I listed gets to be enormous. We're talking LHC large, at least.
"Nil Tl Son, do you see the large cold thing? Take it out."
4 hidden comments

Re: **(Score:2)**
by jabuzz (182671)
And no more MRI scans and ... There is a reason that scientist worry about fritting away a limited and precious resource on party balloons when you could use a hydrogen/nitrogen mix that is no more dangerous than a Christmas cracker.

Re: **(Score:1)**
by mermeid007 (5624172)
Just you wait. and you wait. and you wait. No christmas presents after christmas? Jokes on you.

Re: **(Score:3)**
by angel'o'sphere (80593)
plus all of the laws of thermodynamics ... are working against us.
Actually: **no!**
Thermodynamics has nothing to do with quantum computers **n**or *Heisenberg's Uncertainty Principle* have anything to do with it ..
1 hidden comment

Re: **(Score:1)**
by Anonymous Coward
In the spirit of, "never say never," a practical quantum computer is at least 100 years away.
I wouldn't even go that far. I'm not convinced that a useful quantum computer will ever be constructed. For example, here is an interesting quote from another recent article, ***The Case Against Quantum Computing*** [ieee.org]:
"Experts estimate that the number of qubits needed for a useful quantum computer, one that could compete with your laptop in solving certain kinds of interesting problems, is between 1,000 and 100,000. So the number of continuous parameters describing the state of such a useful quantum computer at

Re: **(Score:2)**
by gweihir (88907)
And that is just the thing: Mass-hype and mass-panic that completely ignore practical aspects. Here is news for these people: Practical aspects are what makes or breaks a technology.
Incidentally, general AI has even less substance than QCs have, because there is not even a credible theory how they could work. In the few fields where we actually have theories (like automated deduction), the effort is so great that smart human beings can do things a universe-size computer could not. QCs seem to at least work

Re: **(Score:2)**
by gtall (79522)
You are ignoring another Uncertainty Principle, that is the amount of money that can be squeezed out of funding agencies by getting their bloomers in a twist over quantum: Big Bad Quantum is coming, be very afraid, very scared, and very willing to allow us to save you for a small sum, although it might seem vast from your point of view....we here at Quantum Uncertainty Enterprises assure you it is not.

Re: **(Score:1)**
by mermeid007 (5624172)
You are right. What nice people have to deal with.

Wrong, Quantum encryption. **(Score:2)**
by wolfheart111 (2496796)
Once the Bits are tampered with (observed) they change.
1 hidden comment

quantum computing **(Score:1)**
by Hrrrq (565259)
I'm of the opinion that practical quantum computing is impossible (see link below for the argument). Start believing this too, and you will have one fewer things to be worried about!
https://spectrum.ieee.org/comp... [ieee.org]

Re: **(Score:2)**
by gweihir (88907)
I agree. The whole thing is both useful idiots and "scientists" without ethics that want to profit from the hype a bit longer.
The best supporting evidence for your citation is that QCs have almost not scaled at all in now something like 40 years of research.

Isn't elliptical curve good enough? **(Score:3)**
by Actually, I do RTFA (1058596) on Wednesday December 05, 2018 @11:43PM (#57757358)
I thought elliptical curve cryptography was good enough?
Also, it occurs to me they're concerned about a "20 year" timespan to get it widely deployed. Maybe a truly excellent algorithm just got patented, and they have to wait until it's unencumbered for it to spread?
Reply to This Share
twitter facebook linkedin
Flag as Inappropriate
3 hidden comments

- **Yet... (Score:1)**
  by AndyKron (937105)
  The world relies on encryption to protect everything from credit card transactions to databases yet they keep getting hacked repeatedly so what's the point?
  - **Re: (Score:2)**
    by ClickOnThis (137803)
    The world relies on encryption to protect everything from credit card transactions to databases yet they keep getting hacked repeatedly so what's the point?
    The point is to keep making it harder for the bad guys to succeed. It's an arms race.
    Of course, the good guys can turn into the bad guys, so be vigilant.
  - **Re: (Score:2)**
    by angel'o'sphere (80593)
    Getting hacked has usually nothing to do with encryption but with stupidity.
    E.g. if I call you and ask for your credit card number, would you encrypt it somehow over the phone call?
    Would you give it to me?
  - **Re: (Score:2)**
    by gravewax (4772409)
    and? the encryption hasn't been hacked yet. just because many companies are incompetent doesn't make encryption broken. Just like if a house collapses it isn't the hammers fault.
  - **Re: (Score:2)**
    by AHuxley (892839)
    The NSA and GCHQ have the math that finds the users computer. From then its just waiting for the user to enter their pw as gov/mil pushed software collects everything.
    No easy connected network? Then MI6/CIA start to look at the workers on site.

    The magic was a PRISM like front door into the OS, telcos.
    The mathematical flaw was people had to trusted their OS crypto junk/used a telco network.

    Quantum will be a cover story for more PRISM, more police ready crypto designed into products.

    Quantum will
- **We already have quantum safe cryptography (Score:2)**
  by jpaine619 (4874633)
  It's called the OTP (one time pad). It's immune to quantum based attacks and, if your adversary is online only, you can distribute them physically..
  - 2 hidden comments
- **Can we _please_ stop with this nonsense? (Score:2)**
  by gweihir (88907)
  There are no QCs of sufficient size to even break amateur-crypto. Scaling is proving difficult enough that it is unclear whether it works at all. There is no threat here. No, really not.
  - 1 hidden comment
- **On breaking encryption for good ends. (Score:2)**
  by 3seas (184403)
  There's a lot of cryptocurrency mining hardware being dumped & can be repurposed to solve Wikileaks Insurance Files encryptons. Pursuing this direction & not knowing when solves will happen will motivate govs & banks to correct themselves. And that is a Good Thing to do.
- **meh (Score:2)**
  by sad_ (7868)
  who cares, encryption will be broken by the time viable quantum computers are a reality anyway.
  australia is just the first domino to fall, soon other nations will follow and all encryption must be breakable by law.

Related Links Top of the: **day**, **week**, **month**.
- 477 comments Recruiters Are Still Complaining About No-Shows At Interviews
- 445 comments Should Developers Abandon Agile?
- 441 comments Hackers Who Attended Black Hat and DefCon Conferences Say Hotel Security Personnel Demanded Access To Their Rooms
- 416 comments 'Kernel Memory Leaking' Intel Processor Design Flaw Forces Linux, Windows Redesign
- 369 comments China Infiltrated Apple, Amazon and Other US Companies Using Spy Chips on Servers, According To Bloomberg; Apple, and Amazon, Among Others Refute the Report

next

Australia Passes Anti-Encryption Laws [Update]
95 comments

previous

FCC Chairman Admits Russia Meddled In Net Neutrality Debate
106 comments

Slashdot

Post

Get 1 More Comment

98 of 98 loaded

Submit Story

FAQ
Story Archive
Hall of Fame
Advertising
Terms
Privacy Statement
Privacy Choices
Opt-out Choices
About
Feedback
Mobile View
Blog

Close

Slashdot

Working...