

Forum:[Hack Forums](#)

Thread: [Discussion: Will Quantum Computers Break the Internet?](#)

techpacket - February 23, 2026, 1:45 am

If real, powerful quantum computers show up in the next 10–20 years, and we switch everything to post-quantum crypto... will that actually make the internet safe?

Or are we worrying too much about the math and not enough about how it's implemented?

Because honestly, on paper most crypto algorithms look strong. But in real life we still deal with:
Side-channel attacks (timing leaks, power analysis, cache stuff)
Cheap IoT devices with weak hardware Messy integration into TLS, VPNs, firmware updates, etc.
Downgrade attacks and simple misconfigurations

If you look back at history, most big crypto failures weren't because the math got cracked. It was usually bad implementation, bad setup, or human mistakes.

So long term, what's the bigger risk?
Quantum computers breaking the algorithms?
Or us creating new weaknesses while rushing to migrate?

Would like to hear real opinions from people who actually work in security/crypto.

R5N3T - February 23, 2026, 9:05 am

Wow, this is a heavy discussion for me, bro, hehe. I didn't think that far

5chn4pp - February 23, 2026, 9:28 am

We are not rushing to migrate to post-quantum security. OpenSSH for example has offered post-quantum key agreement (KexAlgorithms) by default since April 2022. And these are hybrid algorithms, they combine a post-quantum scheme with a classical one (ML-KEM + x25519), so even if the post-quantum math turns out to be weak, the connection is no worse off than before.

The migration doesn't have to introduce new risk.

<https://www.openssh.org/pq.html>

techpacket - February 23, 2026, 8:35 pm

(Feb 23, 2026 10:28 AM)5chn4pp Wrote: [\[CITE\]](#) We are not rushing to migrate to post-quantum security. OpenSSH for example has offered post-quantum key agreement (KexAlgorithms) by default since April 2022. And these are hybrid algorithms, they combine a post-quantum scheme with a classical one (ML-KEM + x25519), so even if the post-quantum math turns out to be weak, the connection is no worse off than before.

The migration doesn't have to introduce new risk.

<https://www.openssh.org/pq.html>

That's a fair point. Hybrid makes a lot of sense as a safety net.
I guess my concern is less about the math and more about large-scale deployment — especially outside well-maintained projects like OpenSSH. Smaller vendors and embedded systems might not

handle the transition as cleanly.

(Feb 23, 2026 10:05 AM)R5N3T Wrote: [\[CITE\]](#) Wow, this is a heavy discussion for me, bro, hehe. I didn't think that far
Soo nice of you brother for replying the post
Thanks for it. ?