

Technology

Mathematician warns US spies may be weakening next-gen encryption

Quantum computers may soon be able to crack encryption methods in use today, so plans are already under way to replace them with new, secure algorithms. Now it seems the US National Security Agency may be undermining that process

By [Matthew Sparkes](#)

📅 10 October 2023




▲ **The US National Security Agency headquarters at Fort Meade, Maryland**


SAUL LOEB/AFP via Getty Images




A prominent cryptography expert has told New Scientist that a US spy agency could be weakening a new generation of algorithms designed to protect against hackers equipped

with quantum computers.


[Daniel Bernstein](https://cr.yp.to/djb.html)  <https://cr.yp.to/djb.html> at the University of Illinois Chicago says that the US National Institute of Standards and Technology (NIST) is deliberately obscuring the level of involvement the US National Security Agency (NSA) has in developing new encryption standards for “post-quantum cryptography” (PQC). He also believes that NIST has made errors – either accidental or deliberate – in calculations describing the security of the new standards. NIST denies the claims.

“NIST isn’t following procedures designed to stop NSA from weakening PQC,” says Bernstein. “People choosing cryptographic standards should be transparently and verifiably following clear public rules so that we don’t need to worry about their motivations. NIST promised transparency and then claimed it had shown all its work, but that claim simply isn’t true.”

The mathematical problems we use to protect data are practically impossible for even the largest supercomputers to crack today. But when quantum computers become [reliable and powerful enough](#)  [/article/2379347-which-quantum-computer-is-the-most-powerful-ever-its-complicated/](#), they will be able to break them in moments.


Although it is [unclear when such computers will emerge](#)  [/article/2370022-cryptographers-bet-cash-on-when-quantum-computers-will-beat-encryption/](#), NIST has been running a project [since 2012](#)  https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf to standardise a new generation of algorithms that resist their attacks. Bernstein, who [coined the term post-quantum cryptography](#)  <https://archive.ph/BHGOM> in 2003 to refer to these kinds of algorithms, says the NSA is actively engaged in putting secret weaknesses into new encryption standards that will allow them to be more easily cracked with the right knowledge. NIST’s standards are used globally, so flaws could have a large impact.


Bernstein alleges that NIST’s calculations for one of the upcoming PQC standards, Kyber512, are “glaringly wrong”, making it appear more secure than it really is. He says that NIST multiplied two numbers together when it would have been more correct to add them, resulting in an artificially high assessment of Kyber512’s robustness to attack.


“We disagree with his analysis,” says [Dustin Moody](#)  <https://www.nist.gov/people/dustin-moody> at NIST. “It’s a question for which there

isn't scientific certainty and intelligent people can have different views. We respect Dan's opinion, but don't agree with what he says."

Moody says that Kyber512 meets NIST's "level one" security criteria, which makes it at least as hard to break as a commonly used existing algorithm, AES-128. That said, NIST recommends that, in practice, people should use a stronger version, Kyber768, which Moody says was a suggestion from the algorithm's developers.

NIST is currently in a period of [public consultation](#)  [/article/2327054-us-chooses-encryption-tools-to-protect-us-from-quantum-computers/](#) and hopes to reveal the final standards for PQC algorithms next year so that organisations can begin to adopt them. The Kyber algorithm seems likely to make the cut as it has already progressed through several layers of selection.

Given its secretive nature, it is difficult to say for sure whether or not the NSA has influenced the PQC standards, but there have long been suggestions and rumours that the agency deliberately weakens encryption algorithms. In 2013, The New York Times reported that the agency [had a budget of \\$250 million for the task](#) 

<https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html>, and intelligence agency documents leaked by Edward Snowden in the same year contained references to the NSA deliberately placing a backdoor in a cryptography algorithm, although that algorithm was [later dropped from official standards](#) 

<https://archive.nytimes.com/bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/>.

Moody denies that NIST would ever agree to deliberately weaken a standard at the behest of the NSA and says that any secret weakness would have had to be inserted without its knowledge. He also says that in the wake of the Snowden revelations, NIST has tightened guidelines to ensure transparency and security and to rebuild confidence with cryptographic experts.

"We wouldn't have ever intentionally done anything like that," says Moody, but he acknowledges the Snowden leaks caused a backlash. "Anytime the NSA gets brought up, there's a number of cryptographers that are concerned and we've tried to be open and transparent about our interactions."

Moody says that the NSA has also – as far as a secretive intelligence agency can – tried to be more open. But the agency declined to comment when approached by *New Scientist*.

“All we can do is tell people that NIST are the ones in the room making the decisions, but if you don’t believe us, there’s no way you could verify that without being inside NIST,” says Moody.

However, Bernstein alleges that NIST hasn’t been open about the level of input by the NSA, “stonewalling” him when he has asked for information. As a result, he has made freedom of information requests and taken NIST to court, [forcing it to reveal details of the NSA’s involvement](https://blog.cr.yp.to/20231003-countcorrectly.html) <https://blog.cr.yp.to/20231003-countcorrectly.html>.

Documents released to Bernstein indicate that a group described as the “Post Quantum Cryptography Team, National Institute of Standards and Technology” included many NSA members and that NIST had met with someone from the UK’s Government Communications Headquarters (GCHQ), the UK equivalent of the NSA.

[Alan Woodward](https://en.wikipedia.org/wiki/Alan_Woodward_(computer_scientist)) [https://en.wikipedia.org/wiki/Alan_Woodward_\(computer_scientist\)](https://en.wikipedia.org/wiki/Alan_Woodward_(computer_scientist)) at the University of Surrey, UK, says there are reasons to be wary of encryption algorithms. For example, the GEA-1 code used in mobile phone networks during the 1990s and 2000s was found to have a flaw that made it [millions of times less computationally intensive than it should have been to crack](/article/2281423-flaw-in-old-mobile-phone-encryption-code-could-be-used-for-snooping/) </article/2281423-flaw-in-old-mobile-phone-encryption-code-could-be-used-for-snooping/> – although a culprit who put it there has never been identified.

But Woodward says that the current PQC candidates have been heavily scrutinised by academics and industry and haven’t yet been found lacking, while other algorithms that featured in earlier stages of the competition have been [demonstrated to be flawed and were eliminated](/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/). </article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/>

“Intelligence agencies have a history of weakening encryption, but there’s been such a lot of security analysis done on these candidates that I would be surprised if Kyber were somehow booby-trapped,” he says.