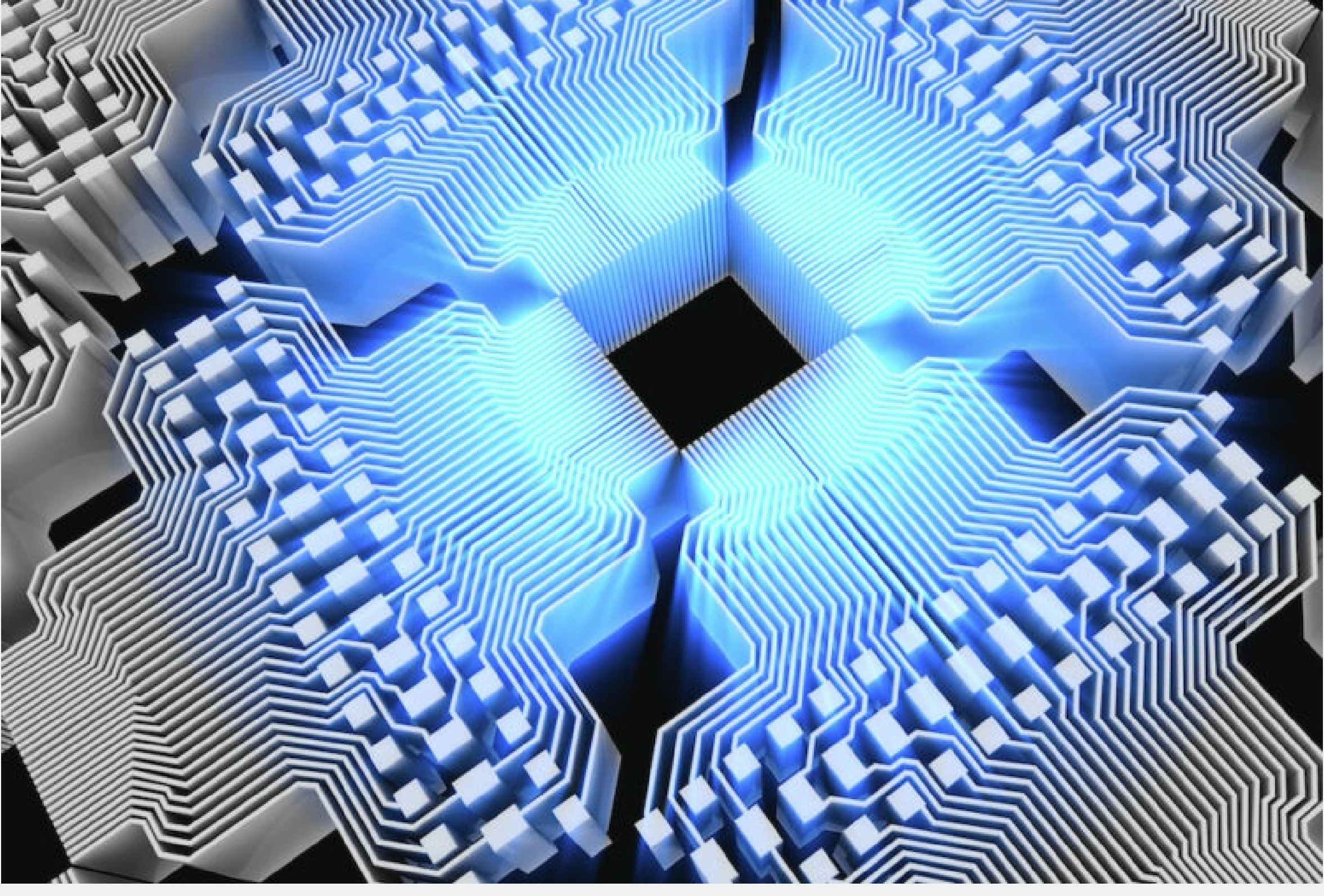





Post-quantum encryption contender is taken out by single-core PC and 1 hour

Leave it to mathematicians to muck up what looked like an impressive new algorithm.

DAN GOODIN - 8/2/2022, 12:31 PM

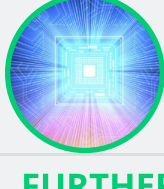


Get **enlarge**



In the US government's ongoing campaign to protect data in the age of quantum computers, a new and powerful attack that used a single traditional computer to completely break a fourth-round candidate highlights the risks involved in standardizing the next generation of encryption algorithms.

Last month, the US Department of Commerce's National Institute of Standards and Technology, or NIST, selected **four post-quantum computing encryption algorithms** to replace algorithms like RSA, Diffie-Hellman, and elliptic curve Diffie-Hellman, which are unable to withstand attacks from a quantum computer.



FURTHER READING
The cryptocalypse is nigh! NIST rolls out new encryption standards to prepare

In the same move, NIST advanced four additional algorithms as potential replacements pending further testing in hopes one or more of them may also be suitable encryption alternatives in a post-quantum world. The new attack breaks SIKE, which is one of the latter four additional algorithms. The attack has no impact on the four PQC algorithms selected by NIST as approved standards, all of which rely on completely different mathematical techniques than SIKE.

Getting totally SIKEd

SIKE—short for **Supersingular Isogeny Key Encapsulation**—is now likely out of the running thanks to research that was published over the weekend by researchers from the **Computer Security and Industrial Cryptography** group at KU Leuven. The paper, titled **An Efficient Key Recovery Attack on SIDH (Preliminary Version)**, described a technique that uses complex mathematics and a single traditional PC to recover the encryption keys protecting the SIKE-protected transactions. The entire process requires only about an hour's time. The feat makes the researchers, Wouter Castryck and Thomas Decru eligible for a \$50,000 reward from NIST.

“The newly uncovered weakness is clearly a major blow to SIKE,” David Jao, a professor at the University of Waterloo and co-inventor of SIKE, wrote in an email. “The attack is really unexpected.”

The advent of public key encryption in the 1970s was a major breakthrough because it allowed parties who had never met to securely trade encrypted material that couldn't be broken by an adversary. Public key encryption relies on asymmetric keys, with one private key used to decrypt messages and a separate public key for encrypting. Users make their public key widely available. As long as their private key remains secret, the scheme remains secure.

Advertisement

In practice, public key cryptography can often be unwieldy, so many systems rely on key encapsulation mechanisms, which allow parties who have never met before to jointly agree on a symmetric key over a public medium such as the Internet. In contrast to symmetric-key algorithms, key encapsulation mechanisms in use today are easily broken by quantum computers. SIKE, before the new attack, was thought to avoid such vulnerabilities by using a complex mathematical construction known as a supersingular isogeny graph.

The cornerstone of SIKE is a protocol called SIDH, short for Supersingular Isogeny Diffie-Hellman. The research paper published over the weekend shows how SIDH is vulnerable to a theorem known as “glue-and-split” developed by mathematician Ernst Kani in 1997, as well as tools devised by fellow mathematicians Everett W. Howe, Franck Leprévost, and Bjorn Poonen in 2000. The new technique builds on what's known as the “GPST adaptive attack,” described in a **2016 paper**. The math behind the latest attack is guaranteed to be impenetrable to most non-mathematicians. Here's about as close as you're going to get:

“The attack exploits the fact that SIDH has auxiliary points and that the degree of the secret isogeny is known,” **Steven Galbraith**, a University of Auckland mathematics professor and the “G” in the GPST adaptive attack, explained in a **short writeup** on the new attack. “The auxiliary points in SIDH have always been an annoyance and a potential weakness, and they have been exploited for fault attacks, the GPST adaptive attack, torsion point attacks, etc.

He continued:

“

Let E_0 be the base curve and let $P_0, Q_0 \in E_0$ have order 2^n . Let E, P, Q be given such that there exists an isogeny ϕ of degree 3^t with $\phi : E_0 \rightarrow E$, $\phi(P_0) = P$, and $\phi(Q_0) = Q$.

A key aspect of SIDH is that one does not compute ϕ directly, but as a composition of isogenies of degree 3. In other words, there is a sequence of curves $E_0 \rightarrow E_1 \rightarrow E_2 \rightarrow \dots \rightarrow E$ connected by 3-isogenies.

Essentially, like in GPST, the attack determines the intermediate curves E_i and hence eventually determines the private key. At step i the attack does a brute-force search of all possible $E_i \rightarrow E_{i+1}$, and the magic ingredient is a gadget that shows which one is correct.

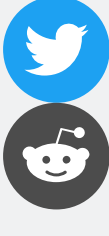
(The above is over-simplified, the isogenies $E_i \rightarrow E_{i+1}$ in the attack are not of degree 3 but of degree a small power of 3.)

”

More important than understanding the math, Jonathan Katz, an IEEE Member and professor in the department of computer science at the University of Maryland, wrote in an email: “the attack is entirely classical, and does not require quantum computers at all.”

READER COMMENTS

120
SHARE THIS STORY



DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com / **TWITTER** [@dangoodin001](https://twitter.com/dangoodin001)

Advertisement

Related Stories

Today on Ars

- STORE
- SUBSCRIBE
- ABOUT US
- RSS FEEDS
- VIEW MOBILE SITE
- CONTACT US
- STAFF
- ADVERTISE WITH US
- REPRINTS
- NEWSLETTER SIGNUP



Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

SIGN ME UP →