a pond can add to each other or cancel each other out, to factoring integer numbers into primes, the integers that cannot be further divided without a remainder.

Shor's algorithm would make a quantum computer exponentially faster than a classical one at cracking an encryption system based on large prime numbers — called Rivest–Shamir–Adleman, or RSA, after the initials of its inventors — as well as some other popular cryptography techniques, which currently protect online privacy and security. But implementing Shor's technique would require a quantum computer much larger than the prototypes that are available. The size of a quantum computer is measured in quantum bits, or qubits. Researchers say it might take one million or more qubits to crack RSA. The largest quantum machine available now — the Osprey chip, announced in November by IBM — has 433 qubits.

A fresh approach

Shijie Wei at the Beijing Academy of Quantum Information Sciences and collaborators took a different route to beat RSA, based not on Shor's technique but on Schnorr's algorithm — a process for factoring integer numbers devised by mathematician Claus Schnorr at Goethe University in Frankfurt, Germany, in the 1990s. Schnorr's algorithm was designed to run on a classical computer, but Wei's team implemented part of the process on a quantum computer, using a procedure called the quantum approximate optimization algorithm, or QAOA.

In the paper, which has not yet been peer reviewed, the authors claim that their algorithm could break strong RSA keys — numbers with more than 600 decimal digits — using just 372 qubits. In an e-mail to *Nature* on behalf of all the authors, Guilu Long, a physicist at Tsinghua University in Beijing, cautioned that having many qubits is not enough, and that current quantum machines are still too error-prone to do such a large computation successfully. "Simply increasing the qubit number without reducing the error rate does not help."

The team demonstrated the technique on a 10-qubit quantum computer, to factor the relatively manageable 15-digit number 261,980,999,226,229. (It splits into two primes, as 15,538,213 × 16,860,433.) The researchers say this is the largest number yet to have been factored with the aid of a quantum computer — although it is much smaller than the encryption keys used by modern web browsers.

Controversial paper

The trouble is, no one knows whether the QAOA makes factoring large numbers faster than just running Schnorr's classical algorithm on a laptop. "It should be pointed out that the quantum speedup of the algorithm is unclear," write the authors. In other words, although Shor's algorithm is guaranteed to break encryption efficiently when (and if) a large-enough quantum computer becomes available, the optimization-based technique could run on a much smaller machine, but it might never finish the task.

Michele Mosca, a mathematician at the University of Waterloo in Canada, also points out that the QAOA is not the first quantum algorithm known to be able to factor whole numbers using a small number of qubits. He and his collaborators described[3] one in 2017. So researchers already knew that there is nothing fundamental that requires quantum computers to be very large to factor numbers.

"Confidence in digital infrastructures would collapse."

Other researchers have complained that, although the latest paper could be correct, the caveat regarding speed comes only at the very end of it. "All told, this is one of the most misleading quantum computing papers I've seen in 25 years," blogged quantum-computing theorist Scott Aaronson at the University of Texas at Austin.

In his e-mail, Long says that he and his collaborators plan to change the paper and will move the caveat higher up. "We welcome the peer review and the communication with scientists," the statement added.

Even if the Schnorr-based technique won't break the Internet, quantum computers could eventually do so by running Shor's algorithm. Security researchers have been developing alternative 'post-quantum' or 'quantum-safe' cryptographic systems that are seen as less likely to succumb to a quantum attack. But researchers might also discover quantum algorithms that can beat these systems.

"Confidence in digital infrastructures would collapse," says Mosca. "We'd suddenly switch from managing the quantum-safe migration through technology life-cycle management to crisis management," he adds. "It won't be pretty any way you slice it."

[1] Yan, B. *et al.* Preprint at https://arxiv.org/abs/2212.12372 (2022).
[2] Shor, P. W. *Phys. Rev. A* **52**, R2493–R2496 (1995).
[3] Bernstein, D. J., Biasse, J.-F. & Mosca, M. in *Post-Quantum Cryptography* Vol. 10346 (eds Lange, T. & Takagi, T.) 330–346 (Springer, 2017).

IS CORONAVIRUS VARIANT XBB.1.5 A GLOBAL THREAT?

A new Omicron subvariant is rising, but whether it will cause a surge in hospitalizations isn't clear.

By Ewen Callaway

New year, new variant. Just as scientists were getting to grips with the alphabet soup of SARS-CoV-2 variants circulating globally — your BQ.1.1, CH.1.1 and BF.7 — one lineage seems to be rising to the top, thanks to a peculiar new mutation.

The XBB.1.5 subvariant now makes up around 28% of US COVID-19 cases, according to projections from the US Centers for Disease Control and Prevention (CDC) in Atlanta, Georgia, and its prevalence is on the rise globally. In the northeastern United States, it seems to have rapidly out-competed the menagerie of other immunity-dodging variants that were expected to circulate alongside one another this winter.

"It's almost certainly going to dominate in the world. I cannot find a single competitor now. Everything else is incomparable," says Yunlong Cao, an immunologist at Peking University in Beijing whose team is studying the properties of XBB.1.5 in the laboratory.

Scientists caution that XBB.1.5's impact, in the United States and beyond, is still far from clear. The variant might not cause a big surge in infections or hospitalizations in many countries, thanks to immunity built up from vaccinations, particularly recent boosters, and exposure during earlier waves of COVID-19.

However, even if XBB.1.5 does not cause big COVID-19 waves, it will be important to track the lineage closely, researchers say. The subvariant bears a rarely seen mutation that might enhance its infectivity — and create an opportunity for further evolutionary gains.

Great-grandchild of Omicron

As its name suggests, XBB.1.5 is an offshoot of a SARS-CoV-2 variant called XBB. That lineage is a recombinant of two descendants of the BA.2 lineage that began spiking in early 2022; BA.2 itself is an offshoot of Omicron. XBB's spike protein has a suite of mutations that boost the variant's ability to evade antibodies. This has helped XBB to become common over the past few months, particularly in Asia, where it caused a surge in cases in Singapore.

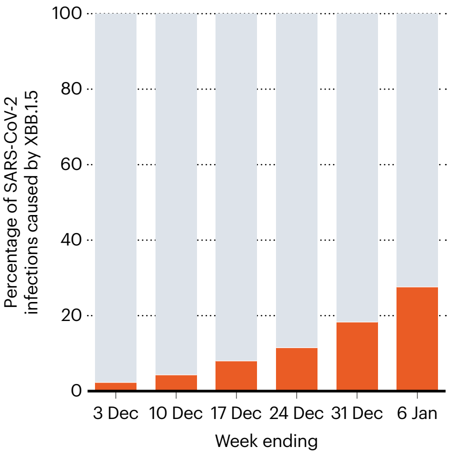
Variant-watchers noticed XBB.1.5 in late 2022, thanks to a rarely seen amino-acid change, called F486P, in the spike protein. Experiments from Cao's lab suggest that the mutation improves the variant's ability to attach to the human ACE2 receptor, which SARS-CoV-2 uses to invade cells[1]. Importantly, the mutation doesn't seem to erode XBB's prowess at eluding antibodies. The results were posted to the bioRxiv preprint server on 5 January and have not yet been peer reviewed. "XBB really sucks at ACE2 binding," says Cao, and the F486P change present in XBB.1.5 helps to surmount that shortcoming.

The relationship between a variant's ability to attach to ACE2 and its transmissibility isn't fully clear, says Jesse Bloom, an evolutionary virologist at the Fred Hutchinson Cancer Center in Seattle, Washington. But for XBB.1.5, "F486P seems to have given it another boost, which is enabling the virus to spread", he says.

The CDC estimates that XBB.1.5 is currently the second most common variant in the United States, comprising 28% of cases nationally, and upwards of 70% in the northeast (see 'New year, new variant'). Moritz Gerstung, a computational biologist at the German Cancer Research Centre in Heidelberg, estimates that cases of the variant are doubling roughly every week in the United States, and a bit more slowly in other countries where the variant has appeared. That's comparable to the rate at which the BQ.1 and BQ.1.1 variants grew in September 2022, but slower than earlier Omicron waves. "XBB.1.5's spread is still impressively fast," Gerstung says.

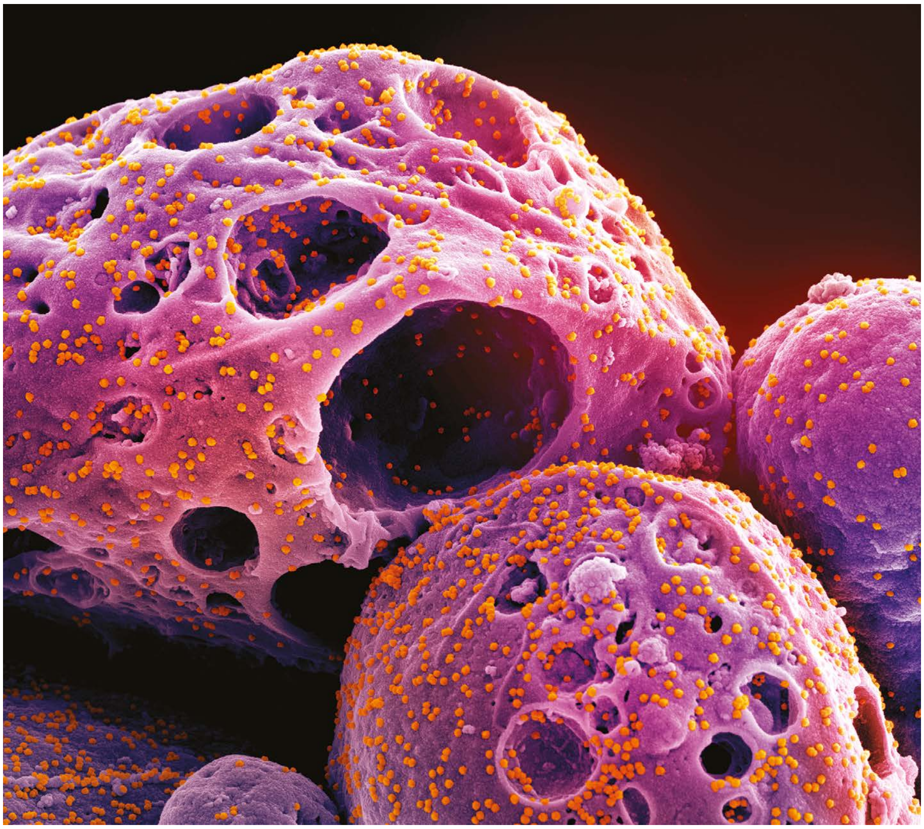
NEW YEAR, NEW VARIANT

An offshoot of Omicron called XBB.1.5 began to take hold in the United States towards the end of 2022. Modelling suggests that the share of SARS-CoV-2 infections caused by XBB.1.5 rose from 2% in early December to 28% by early January.



SOURCE: US CENTERS FOR DISEASE CONTROL AND PREVENTION

What's not clear is whether such growth will be sustained or whether the variant will drive up infections significantly, Gerstung adds. BQ.1 and BQ.1.1 looked set to drive sizeable waves, only to run out of steam in Europe and North America. If the same thing happens with XBB.1.5, the lineage could wind up silently replacing other variants in some countries without causing a big rise in cases.



A mutation helps the XBB.1.5 variant attach to cells (shown covered in SARS-CoV-2 particles).

NIAID/NIH/SPL

Big-city variant

Jennifer Surtees, a biochemist at the University at Buffalo in New York, wonders whether researchers are overestimating XBB.1.5's growth in the northeastern United States. The variant has become more common in the western New York sequences that her team handles, but she hasn't yet noticed the meteoric rise in XBB.1.5 genomes that labs in New York City are recording.

Gauging XBB.1.5's impact might not be straightforward, owing to the drop-off in testing for COVID-19, Surtees adds. "I think that we are truly flying blind right now. We have no idea how many cases are really out there."

Tulio de Oliveira, a bioinformatician at Stellenbosch University in South Africa, thinks researchers should look at hospital cases and other measures of disease severity to best measure XBB.1.5's impact. Factors such as a cold snap in the northeastern United States and holiday gatherings could partly explain the variant's apparent surge, he says. "I think that many scientists are jumping to conclusions and predictions very early and with very little data."

Evasion expert

One thing that researchers can agree on is that XBB.1.5, like its predecessor XBB, is a master of immune evasion. It carries numerous spike mutations that blunt the potency of antibodies raised by vaccination and previous infections – including infection with earlier Omicron strains. Bivalent vaccines boost levels of antibodies capable of blocking XBB infection (and probably XBB.1.5) in lab tests[2,3], but not by much, notes Cao.

Throughout 2022, researchers including Cao watched Omicron lineages pick up a succession of antibody-evading mutations in the viral spike protein that allowed new lineages to overcome immunity gained from vaccines and previous waves. XBB.1.5 is vastly more transmissible than other circulating variants thanks to the addition of the F486P mutation, so there is currently little evolutionary pressure on the lineage to change further, says Cao.

But as global immunity to the subvariant builds, XBB.1.5 won't stand still, he says. "We are going to see a lot of new mutations that we have never seen before."

1. Yue, C. *et al.* Preprint at bioRxiv https://doi.org/10.1101/2023.01.03.522427 (2023).
2. Zou, J. *et al.* Preprint at bioRxiv https://doi.org/10.1101/2022.11.17.516898 (2022).
3. Davis-Gardner, M. E. *et al. N. Engl. J. Med.* https://doi.org/10.1056/NEJMc2214293 (2022).