Each week Quanta Magazine explains one of the most important ideas driving modern research. This week, computer science staff writer Ben Brubaker explains how researchers harness quantum physics to develop new encryption techniques and undermine existing ones.

How Quantum Physics Is Reshaping Privacy

By BEN BRUBAKER

People have used clever codes to protect secret information for millennia. In the 1970s,
cryptography researchers figured out how to do it using math. The basic idea is to build
data encryption techniques based on notoriously difficult math problems. Do this in just
the right way, and would-be code breakers can’t steal your private data — at least, not
without a revolutionary new algorithm, or procedure, for solving one of those hard
problems. The more researchers tried and failed to find such clever algorithms, the more
comfortable they felt assuming that these problems really were hard.

In the years that followed, researchers began to work out the technical details of this
“computational” approach to cryptography. Then quantum physics came along and
upended their most cherished beliefs — not just once, but twice.

The first twist came in 1984, in a groundbreaking paper by the physicist Charles Bennett
and the computer scientist Gilles Brassard. They discovered a cryptographic technique
based directly on the laws of quantum physics, formulated more than half a century
earlier to describe the behavior of atoms and molecules. At least in this one case, finding
a sufficiently insoluble math problem wasn’t essential to providing security after all.

Bennett and Brassard’s breakthrough shocked researchers, but it didn’t make traditional
computational cryptography obsolete. That’s because cryptography is a rich subject
encompassing many different techniques for protecting secret information (as I
discussed in the April 29 Fundamentals newsletter). Bennett and Brassard’s new
quantum cryptography scheme worked for one application, but cryptographers would
still need to rely on assumptions about hard math problems for others.

The second twist came 10 years later, when the applied mathematician Peter Shor
realized that with an assist from quantum physics, some of those hard problems
wouldn’t be so hard after all. He’d been wondering whether the quantum trickery that
Bennett and Brassard had used to safeguard information would also enable new ways to
process information, using a hypothetical quantum computer.

Shor’s curiosity soon paid off. He discovered an algorithm that quantum computers
could use to easily solve a famously hard problem: breaking very large numbers into
their prime factors. That factoring problem was at the root of public-key encryption, a
celebrated cryptographic technique vital to secure communication over the internet. When it came to privacy, quantum physics had turned out to be a fickle friend, doling out favors to cryptographers and code breakers alike.

**What’s New and Noteworthy**

Immediately after Shor discovered his quantum factoring algorithm, cryptographers began searching for a new foundation for public-key encryption that would stand up to attacks by future quantum computers. In the mid-2000s, they settled on some promising candidates: Problems about navigating multidimensional arrays of points, called lattices, seemed just as hard for quantum computers as for conventional ones.

But cryptographers aren’t resting easy — nobody’s discovered a fast quantum algorithm for solving lattice problems yet, but that doesn’t mean nobody ever will. Indeed, there was a close call in April, when the cryptographer Yilei Chen posted a 62-page paper about a new quantum lattice algorithm to an online preprint server. Dozens of researchers around the world put their own projects on hold to scrutinize the inner workings of Chen’s algorithm, until a subtle flaw was discovered after about a week. Lattice-based cryptography remains safe … for now.

As a practical matter, factoring-based cryptography is also safe for now, simply because nobody’s been able to build a quantum computer powerful enough to factor large numbers using Shor’s algorithm. But last summer, the pioneering lattice cryptographer Oded Regev wrote a paper describing a new and improved variant of Shor’s algorithm that could be easier to implement. Practical applications of quantum factoring remain far off, but they could become a reality a bit sooner than researchers anticipated. It’s a striking reminder that even well-studied algorithms can harbor surprises.

Meanwhile, exciting new developments have followed Bennett and Brassard’s approach, harnessing quantum theory to enhance rather than attack encryption. Two weeks ago, I reported on a string of recent papers reexamining the foundations of quantum cryptography, which discovered that many different applications of encryption could be
made secure even in a hypothetical world where all conventional cryptography is impossible.

AROUND THE WEB

Gilles Brassard wrote an engaging first-person account of his collaboration with Bennett in the early days of quantum cryptography.

The Qiskit channel on YouTube has a video interview in which Peter Shor recounts how he developed his famous algorithm.

The Veritasium channel on YouTube released a video explainer that does a nice job visualizing the inner workings of Shor’s algorithm.