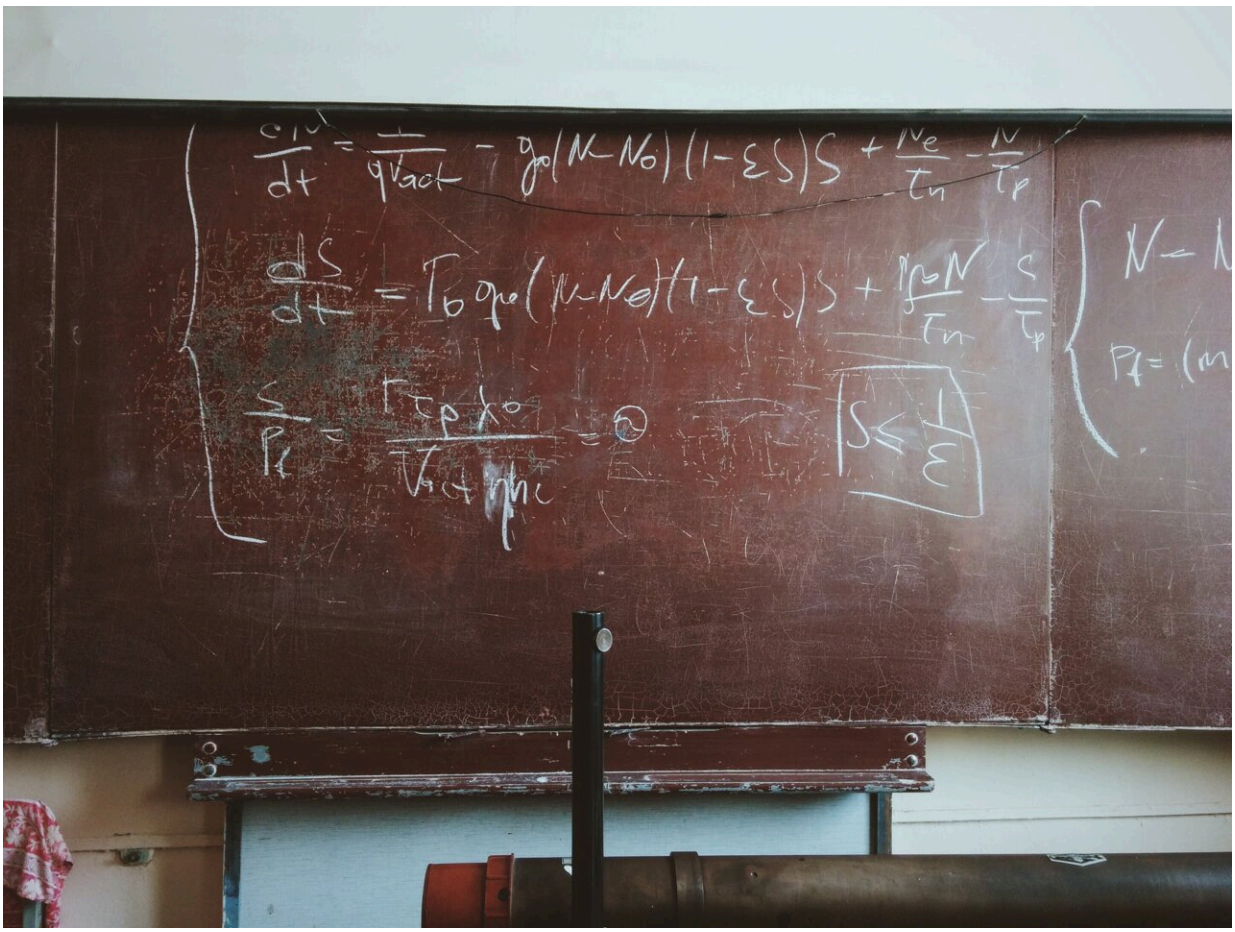
Q&A: Algorithm to serve as cryptography standard for quantum computing era

September 22 2022, by Mary Stuart



Credit: Unsplash/CC0 Public Domain

Mathematicians often toil in obscurity, and that's likely because few

people, apart from fellow mathematicians who share the same sub-specialty, understand what they do. Even when algorithms have practical applications, like helping drivers see approaching cars that the eye can't discern, it's the car manufacturer (or its software developer) that gets the credit.

This is especially true of cryptographers, the unsung heroes whose algorithms keep people's communications and data secure when they use the internet—technology known as public key cryptography.

But sometimes, pure math impacts the real world. That happened this summer when the National Institute of Standards and Technologies selected four cryptography algorithms to serve as standards for public key security in the impending era of quantum computers, which will make current encryption systems quickly obsolete.

Three of the four chosen algorithms rest on work led by a team of mathematicians at Brown: professors Jeffrey Hoffstein, Joseph Silverman and Jill Pipher (who also serves as Brown's vice president for research).

The story of the NIST-endorsed Falcon algorithm—and NTRU, the public key cryptosystem upon which Falcon is based—began in the mid-'90s, when quantum computing was still in the realm of science fiction. At the time, Hoffstein's goal was to develop an algorithm to simplify and speed up the way conventional cryptographic algorithms worked; in 1996, he co-founded NTRU Cryptosystems Inc. with Silverman and Pipher (who is also married to Hoffstein) to take it to market. Hoffstein said the history of NTRU is a "bloodcurdling saga," but the company was ultimately successful, finding a suitable purchaser in Qualcomm. Falcon, which Hoffstein co-designed with nine other cryptographers, and two out of the three other algorithms NIST selected, are built upon the original NTRU framework.

From before his doctoral study at MIT through each of the positions he's held at the Institute for Advanced Study, Cambridge University, the University of Rochester and Brown, Hoffstein has been "a numbers guy," through and through: "It never occurred to me not to be a mathematician," he said. "I promised myself that I would continue to do math until it was no longer fun. Unfortunately, it's still fun!"

On the heels of NIST's selection, Hoffstein described his transformation from a number theorist to an applied mathematician with a solution to an impending global problem of critical importance.

Q: What is public key cryptography?

When you connect to Amazon to make a purchase, how do you know that you are really connected to Amazon, and not a fake website set up to look exactly like Amazon? Then, when you send your credit card information, how do you send it without fear of it being intercepted and stolen? The first question is solved by what is known as a digital signature; the second is solved by public key encryption. Of the NIST's standardized algorithms, one is for public key encryption, and the other three, including Falcon, are for digital signatures.

At the root of these are problems of pure mathematics of a very special type. They are hard to solve (think: time until the universe ends) if you have one piece of information and they are easy to solve (takes microseconds) if you have an extra piece of secret information. The wonderful thing is that only one of the parties communicating—Amazon, in this case—needs to have the secret piece of information.

Q: What is the security challenge that quantum computers pose?

Without a sufficiently strong quantum computer, the time to solve the encryption problem is eons. With a strong quantum computer, the time to solve the problem comes down to hours or less. To put it more alarmingly, if anyone had possession of a strong quantum computer, the entire security of the internet would completely break down. And the National Security Agency and major corporations are betting that within five years there is a good chance that a quantum computer strong enough to break the internet could be built.

Q: You came up with the NTRU solution in the early to mid-90s, well in advance of anyone thinking about the cryptography needs of potential quantum computers. What was your thinking at the time?

I found the three main approaches to public key cryptography to be very clunky and unaesthetic. Just as one example, the most well-known method, RSA, involves taking numbers that are many hundreds of digits long, then raising them to powers that are hundreds of digits long, dividing by yet another number that is hundreds of digits long, and finally taking the remainder. This computation is easily doable on a computer but not very practical if you have a small, lightweight processor, like a cell phone from 1996. RSA is also very slow—okay, milliseconds, but that still counts as slow.

Our dream was to find a method for doing public key cryptography that was orders of magnitude faster than RSA and could run on low-powered devices. And we did it! People implementing it were able to run it at speeds 200 to 300 times faster than RSA. I didn't do this alone—I thought obsessively about the problem for a year and a half, but it didn't coalesce into a solution until I joined with Joe Silverman and Jill Pipher, my Brown colleagues and the co-founders of NTRU.

Q: What does NTRU stand for?

We never said—people just assumed we meant something technical and used their imaginations! But it stands for "Number Theorists R Us." This irritated Jill as she is a harmonic analyst, not a number theorist, but she eventually forgave me.

Q: You've described your start-up NTRU Cryptosystems as having about five "near death" experiences. What were some of the challenges you faced?

The gatekeepers in the field are mostly cryptographers who work for companies and in computer science departments. It is incredibly hard to get any new algorithm to be taken seriously, and it's particularly hard if you're not in the cryptography club. In our case, we rang alarm bells for two reasons. We were outsiders, for one, and we added extra structure from algebraic number theory to lattices to make things more efficient.

Whenever you do that, there is a serious risk that you have accidentally introduced weaknesses. Yes, it is wonderful to do something more efficiently. But have you lost some vital piece of security in the process? It is completely understandable that people were deeply suspicious of this extra structure, which introduced the ability to multiply as well as add. It took 10 years of intense scrutiny before people started to accept that no weaknesses had been added.

Q: This wasn't just an academic exercise. NTRU was a company that had to work with investors and potential customers. Early on, NTRU came unjustly under attack in a paper written by some household

names in cryptography (who later acknowledged their error). How did NTRU survive that?

It turned out that their paper was largely ignored, but our paper was sufficiently interesting that everybody dove into it. They tried to attack and destroy it, and it got a tremendous amount of attention. Every single surface you can imagine was beset by battering rams. The cryptography community was so resistant to mathematicians encroaching on their turf. If we hadn't been well-known mathematicians from Brown, we wouldn't have survived the controversy. In the end, that attention probably helped us.

Q: Were there any ways in which being mathematicians—outsiders, this world—was an advantage?

The thing that I'm proudest of isn't necessarily the fact that the particular algorithm ended up in the final four of the NIST picks, although every single one of the three lattice-based algorithms uses our ring structure (the multiplication feature). They all use the math that we introduced because after more than 25 years of scrutiny, not a single weakness has come up because of adding that structure. That math, which came from algebraic number theory, wasn't part of cryptography before. It is part of what I do for my other living, and I find it particularly delightful that we were able to take this completely abstract theoretical thing of apparently no use whatsoever and find a practical application. As a result, the present generation of cryptographers all have to know algebraic theory, which is kind of fun.

Q: What is it like to be married to another mathematician?

It is the most blissful thing in the universe to be married to someone who understands what it's like to be a mathematician. In math, 99.9% of the time you spend hours, weeks, months, and years thinking about something that comes to nothing. So many times, you think you have a fantastic idea, and it goes nowhere. It is wonderful to be married to someone who understands that feeling, even if we don't always understand the details of what the other is working on.

Q: She realizes when you are lost in thought?

Yes, and she probably is too.

Provided by Brown University

Citation: Q&A: Algorithm to serve as cryptography standard for quantum computing era (2022, September 22) retrieved 26 June 2024 from https://phys.org/news/2022-09-qa-algorithm-cryptography-standard-quantum.html