Mathematical theorem used to crack US government encryption algorithm

November 23 2022, by Catarina Chagas

Credit: CC0 Public Domain

In the digital era and moving towards quantum computing, protecting data against hack attacks is one of our biggest challenges—and one that experts, governments, and industries worldwide work hard to address. While this is an effort to build a more connected and safe future, it can certainly learn from the past.

In July, the US National Institute of Standards and Technology (NIST) selected four encryption algorithms and posed some challenge problems to test their security, offering a $50,000 reward for whomever managed to break them. It happened in less than an hour: one of the promising algorithm candidates, named SIKE, was hacked with a single personal computer. The attack did not rely on a powerful machine, but on powerful mathematics based on a theorem developed by a Queen's professor decades ago.

Ernst Kani has been researching and teaching since the late 1970s—first at the University of Heidelberg, in Germany, and then at Queen's, where he joined the Department of Mathematics and Statistics in 1986. His main research focus is arithmetic geometry, an area of mathematics that uses the techniques of algebraic geometry to solve problems in number theory.

The problems Dr. Kani works to solve stretch back to ancient times. His specific field of research was pioneered by Diophantus of Alexandria around 1,800 years ago and is a set of problems known as Diophantine questions. One of the most famous questions in the field is Fermat's Last Theorem, posed by Pierre Fermat in 1637 and which took the math community 350 years to prove—an accomplishment by Princeton professor Andrew Wiles in 1994. Wiles received many prizes and honors for this work, including an honorary doctorate from Queen's in 1997.

Neither Diophantus nor Fermat dreamt of quantum computers, but Dr. Kani's work on Diophantine questions resurfaced during the NIST round of tests. The successful hackers—Wouter Castryck and Thomas Decru, both researchers at the Katholieke Universiteit Leuven, in Belgium—based their work on the "glue and split" theorem developed by the Queen's mathematician in 1997.

As a matter of fact, Dr. Kani was not concerned about cryptographic

algorithms when he developed the theorem. That work kicked-off in the 1980s, in collaboration with another German mathematician, Gerhard Frey—whose work was crucial in solving Fermat's last theorem. Drs. Kani and Frey wanted to advance research on elliptic curves, a particular kind of equation that would later be used for cryptographic purposes.

Both researchers' goals at that time were purely theoretical. They were interested in manipulating mathematical objects to learn more about their own properties. "Doing pure mathematics is an end by itself, so we don't think of real-world applications," Dr. Kani explains. "But, later, many of those studies are useful for different purposes. When Fermat proposed his theorem hundreds of years ago, his intent was to be able to factor certain large numbers. The application to cryptography came only much later in 1978. Basically, all the methods we use today for data encryption are based on mathematics."

Doughnuts and curves

Mathematicians often refer to mathematics as a beautiful thing. For those who don't work in the field, it might be challenging to see this beauty, or even to have a high-level understanding of what these research projects are all about—it requires some imagination.

Imagine an object shaped like a doughnut, with a hole in the middle: that's a visual model of an elliptic curve, also known as a genus one curve. Drs. Kani and Frey wanted to combine two genus one curves to form a new object—a genus two curve, something we can imagine like two doughnuts stuck solidly together side by side. They aimed to use some properties of the constructed genus two curve to deduce certain properties of the two original genus one curves, which were "glued" together.

In his 1997 paper, Dr. Kani generalized the original construction by

gluing together an arbitrary pair of elliptic curves. But in that case the construction sometimes fails—it might construct an object in which the two doughnuts only touch each other in a single point. The paper analyzes the precise conditions for when this happens (i.e., when the construction fails or "splits"). Castryck and Decru used this characterization of the failure in their method of attacking the proposed encryption scheme SIKE.

"Our problem had nothing to do with cryptography, which is why I was surprised when I heard of the algorithm attack. It was quite ingenious, what they did there!" says Dr. Kani. "One of the co-authors of the SIKE algorithm expressed surprise in the fact that genus two curves could be used to gain information about elliptic curves. But this was precisely our original strategy in the 1980's and 1990's (and afterwards)."

Although cryptographers and computing engineers are not always well-versed in all the high-powered techniques of mathematics, many different skills and forms of knowledge can be combined to advance the way we store and transmit data.

"Cryptography uses a lot of sophisticated mathematics, especially arithmetic geometry. Computing experts and math experts have to work together to advance this field," says Dr. Kani, who continues to teach undergraduate and graduate courses and to work in arithmetic geometry—particularly on problems involving genus two curves and elliptic curves.

More information: Original paper: The Number of Curves of Genus Two with Elliptic Differentials

Provided by Queen's University