Saddling up cryptosystems for a quantum showdown

December 7 2023, by Kelly Izlar

Credit: Pixabay/CC0 Public Domain

A lone ranger riding off into the sunset might say something sage and vague, such as "a man is only as good as his word." But these gritty

prophets never said anything about verifying a man's—or anyone else's—word in the wild frontiers of the digital or quantum era.

Virginia Tech mathematicians are working on both of these issues as they investigate techniques to keep digital interactions secure both today and into the future. In a paper published earlier this fall for Crypto 2023, the Annual International Cryptology Conference, Jason LeGrow and a team of researchers may have found the key to locking down threats from a large-scale quantum attack in an algebraic structure known as a quadratic twist.

Digital signatures

The authenticity of a digital message is verified through something called a digital signature. This mathematical scheme is an electronic fingerprint attached to a digital document that gives the same guarantees as a real ink-on-paper signature. Digital signatures authenticate identity and preserve data integrity in online systems such as banking and health care.

"A digital signature assures that you are the only one who could have produced that signature and that you endorse the content of the document," said LeGrow, assistant professor of mathematics at the College of Science and Commonwealth Cyber Initiative Fellow.

As critical as they are, however, a regular digital signature isn't the right hat for all occasions.

Exotic signatures

Imagine being a member of a stakeholder board of a company where something unethical is afoot. By implementing an "exotic" digital

signature called a ring signature, a board member can authoritatively leak a document to appropriate authorities while preserving anonymity.

Or imagine wanting to endorse a vote in a digital election without disclosing who a person voted for. A blind signature disguises the content of a message before it is signed. The signer does not view the message content, but a third party can later verify the signature.

"Blind signatures were originally proposed for untraceable payments in digital cash," said LeGrow. These days, blind signatures are most often used in blockchain and cryptocurrency when a person wants to pay for something without being traced.

"Other applications of blind signatures include when a person doesn't want to run afoul of rules in other jurisdictions, even if their actions were perfectly legitimate in their locale, like donating to a certain refugee organization or purchasing marijuana in Canada," said LeGrow.

Quantum quickdraw

Digital signatures of all types will fall under the gun the moment a large-scale quantum computer steps onto the street. Why? Because these encryption schemes rely on how hard it is for a computer to solve a certain type of problem. A laptop, for instance, may need lifetimes to solve one. A quantum computer could do it in a few heartbeats.

"As soon as we have a large-scale quantum computer, we're going to be in bad shape," LeGrow said. "We really need to protect digital communications from the looming quantum threat that looks darker every year."

According to LeGrow, the most promising class of efficient blind signatures known to withstand quantum attacks is based on certain

mathematical protocols that are believed to be quantum-safe. LeGrow, who recently received an award from the Academy of Data Science Discovery Fund to support this line of data science-driven research, is exploring a special family of quantum-safe algebraic structures known as quadratic twists.

"A quadratic twist is simple, innocuous, even a cute little thing you can do," said LeGrow. "It turns out that knowledge of this cute little thing was extraordinarily necessary to get our protocol to work."

By adding the quadratic twist to the armory, LeGrow and his collaborators can venture into deeper territories of number theory to bring digital safeguards up to scratch for a quantum showdown.

More information: Shuichi Katsumata et al, CSI-Otter: Isogeny-Based (Partially) Blind Signatures from the Class Group Action with a Twist, *Advances in Cryptology—CRYPTO 2023* (2023). DOI: 10.1007/978-3-031-38548-3_24

Provided by Virginia Tech