Quantum resistant Protocols for Zero-Knowledge Proofs to Strengthen Blockchain Security

Enhancing Code Based Zero-knowledge Proofs using Rank Metric


Block Chain Security

ABU DHABI, UNITED ARAB EMIRATES, September 27, 2021 / EINPresswire.com/ -- Researchers at Technology Innovation Institute (TII) in the United Arab Emirates have improved the feasibility of a new class of algorithms to protect blockchain applications against quantum computing cryptographic attacks. This builds on the considerable research already underway across the cryptographic community in developing better protocols for improving zero-knowledge proofs.

> We're in early stages of understanding & safest approach is to build the quantum-resistant scheme based on many different problems so that if one is broken, you're still hopeful that others are not."
>
> *Emanuele Bellini, Lead Cryptographer at TII*

The specialised area of cryptography has been gaining significant interest since zero-knowledge proofs are widely used in techniques like blockchain, smart contracts, and identity verification.
The most popular approaches have involved using matrix computations. However, there is some concern that future research may find new and improved ways to compromise these protocols. So, researchers are always looking for promising alternatives to provide multiple types of protection against future cryptographic attacks.

Need for alternative approaches

The various types of quantum-resistant problems and algorithms built on them are considered safe at the present time, because no one has demonstrated a credible quantum computer attack against them. Emanuele Bellini, Lead Cryptographer at TII, said: "We are in the early stages of

understanding what is quantum-resistant and what is not. The safest approach is to build the quantum-resistant scheme based on many different problems so that if one is broken, you are still hopeful that the others are not."

Technology Innovation Institute

Most of the work on quantum-resistant protocols for zero-knowledge proofs has been based on lattices. Lattices are very flexible and are one of the most malleable cryptographic mathematical structures that can be applied across the board. The TII team has focused on alternatives to lattices based on the Rank Syndrome Decoding problems, which, although promising, still need more research to make them a credible solution.

Cryptography is a bit of a cat-and-mouse game, where researchers are constantly finding enhanced solutions to break protocols and more effective ways to implement them. It is not even necessary to completely break an approach to reduce its attractiveness. Bellini said, "If someone discovers an attack to the lattice problem that just slightly improves the previous attack, it means that the lattice parameters would have to become larger, and then other approaches would become relatively more efficient."

The importance of zero-knowledge proofs

"Zero-knowledge" has recently become the most popular keyword in cryptographic papers presented at conferences. The popularity of these protocols grew in response to the enthusiasm around blockchain since this is the most common use case. In these applications, the goal is to be able to prove a statement is true without the rest of the blockchain understanding information about the exchange. The simplest implementations of zero-knowledge protocols are often used for identity verification.

A zero-knowledge-proof protocol organised the interaction between two parties in which one is the prover and the other the verifier. The two parties exchange information, and after the exchange, the prover can confirm the truthfulness of the statement, such as whether someone has enough money in a blockchain wallet for a transaction without knowing the total in the wallet. This is also done in a way that hides information from third-party observers.

Initially, the zero-knowledge-proof community focused on using classical cryptographic algorithms based on discrete logs or factorisation problems. The community has recently started exploring quantum-resistant zero-knowledge proofs.

Classical algorithms were inefficient, and the quantum-resistant implementations are even less so because they require larger keys. They also require larger parameters such as the size of the proof, the number of bits that need to be communicated between prover and verifier, and the amount of work each party must perform to build the proof. These quantum-resistant protocols might take minutes or hours to run compared to a few seconds for the protocols built on classical algorithms.

Rank Syndrome Decoding problem

TII's researchers studied the Rank Syndrome Decoding problem, an evolution of another technique called the Syndrome Decoding problem. Other popular quantum techniques have included the shortest vector problem, the NTRU problem, the isogenies problem, and the multivariate quadratic problem.

These different classes of problems organise numbers into a particular structure that is best suited for verifying a zero-knowledge proof built on top of the problem. The shortest vector and NTRU are similar and use lattices to encode the numbers to compute the problem's answer. Multivariate problems use a system of polynomials to organise the calculation. The Syndrome Decoding Problem uses a linear code. The Rank Syndrome Decoding problem is similar to the Syndrome Decoding problem but organises the linear codes more efficiently.
Emanuele Bellini, Lead Cryptographer at the TII, said: "The Rank Syndrome Decoding problem is not something we invented. However, it is a newer problem than Syndrome Decoding and the lattice problems, so it is less studied."

More efficient and adaptable

TII's researchers improved the efficiency of RSD and implemented it in a way that is more adaptable to different use cases. Their implementation is 60% smaller, and the parameters are 1% of the size compared to the state-of-the-art Syndrome Decoding implementation for a given proof. It is also considerably faster, solving one benchmark proof in 47 ms compared to 5,000 ms for Syndrome Decoding.

A key building block of this new construction is a commitment scheme that essentially requires one party to commit to a statement, such as having executed a certain amount of work, which can be verified later as part of a transaction.

TII researchers also demonstrated how this commitment scheme could be built into any kind of circuit, which is a fundamental building block for cryptographic transactions. Prior research had examined how RSD could be applied to signature schemes based on identification protocols using zero-knowledge proofs. However, the TII research is the first demonstration of how RSD could apply to any arbitrary circuit that could be used across many different applications.

An arbitrary circuit in cryptography is analogous to an electrical circuit in a computer chip in

which bits are logically combined using gates that perform logical operations such as executing AND, OR, and NOT statements. Bellini said: "if you have enough of these gates, you can build any function."

Tania Ameer
APCO Worldwide
+971 52 672 5138
tameer@apcoworldwide.com
Visit us on social media:
Facebook
Twitter
LinkedIn
