Zero knowledge proofs: validation without information

Cyber-attacks on large corporations and institutions, such as recent data breaches at some Australian universities, cost the economy hundreds of millions of dollars, writes Jan de Gier, professor of mathematics and statistics at the University of Melbourne and Director of Australia's mathematical sciences research institute MATRIX

Mathematical ideas that reduce the need for information exchange can help improve security.

Online exchanges are secure thanks to cryptographic algorithms based on properties of prime numbers and elliptic curves (solutions to the equation $y^2 = x^3 + ax + b$). The large amounts of electronically stored data however are increasingly vulnerable to security breaches.

A zero-knowledge proof is a verification method that does not rely on sharing data, such as a payment app that checks your capacity to pay without needing to know your balance nor income. Zero-knowledge proofs have become increasingly relevant due to blockchain applications.

Zero-knowledge protocols use random verifications of small pieces of information that cannot be linked. Multiple verifications accumulate evidence and the method gives up absolute certainty for overwhelming probability.

The typical example is the validation of whether a map can be coloured with three colours such that neighbouring countries have distinct colours. This may sound removed from most real world applications, but formal statements can be reformulated into the mathematics of abstract map colourability and thus the latter has universal applicability.

The zero-knowledge idea is that you can only check two neighbouring countries at a time, and that each time you check, the colours are randomly replaced by a set of labels. In this way you can verify that the map only uses three colours and that neighbouring countries have distinct colours, but you will never know the actual colour of each country.

Professor Avi Wigderson (Princeton) was one of the researchers who first developed the concept of a zero-knowledge proof in the 1980s at MIT. He won the prestigious Abel Prize in mathematics for foundational contributions to theoretical computer science and discrete mathematics, and their leading role in shaping them into central fields of modern mathematics. Professor Wigderson will present an online seminar on 7th September 2021 at the Australian mathematical research institute MATRIX.

Prof. Jan de Gier
MATRIX
https://www.matrix-inst.org.au/events-01/online-seminars/ (or other link with more info)