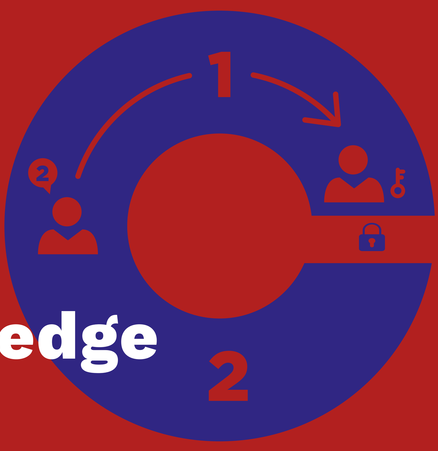


Zero-Knowledge Proofs

Showing that a problem has a solution without revealing it

Is it possible to demonstrate that we know how to prove a theorem, but without disclosing the proof? Surprisingly, the answer turns out to be “yes.” This result, discovered in the 80’s, had a profound impact on our understanding of privacy, and opened the floodgates of a myriad of applications in cryptography and computer security.

THE ORIGIN

1985
Goldwasser, Micali, and Rackoff introduced the notion of zero-knowledge proofs: proofs that yield no information beyond the validity of the statement.

1986
Goldreich, Micali, and Wigderson, showed the wide applicability of this concept: they demonstrated that, under widely believed assumptions, any theorem whose proof can be verified efficiently also admits a zero-knowledge proof.

AN EXAMPLE

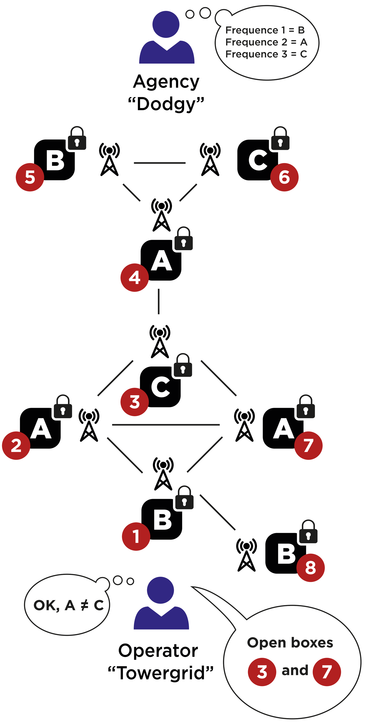
Imagine a network of radio towers that can emit at three different frequencies. To avoid interference, we want that two nearby towers always emit at a different frequency. In general, determining whether this task can be achieved is a hard combinatorial problem. Dodgy is an agency that claims to have a solution (a setting of the frequencies), wishes to sell it to an operator and will only reveal its frequency setting after it has been paid. The operator, Towergrid, is suspicious and wants to be convinced that Dodgy really knows a solution before paying.

The paper of Goldreich, Micali, and Wigderson gives a nice solution to the above conundrum.

1 - Dodgy chooses random names for the frequencies, e.g., A,B, and C.
2 - Dodgy puts the name of the chosen frequency for each tower in a “cryptographic box”.
3 - Towergrid then asks Dodgy to open two randomly chosen boxes for nearby towers.
4 - Towergrid checks whether the letters are indeed different.

After enough repetitions of steps 1 to 4, any cheater is guaranteed to be caught (with whatever probability of error Towergrid likes to achieve), but the solution is never revealed.

This radio-tower problem described above is well-known to be “NP-complete”. In essence, this means that by finding a zero-knowledge proof for this problem, Goldreich, Micali, and Wigderson have in fact found a zero-knowledge proof for all problems with efficiently-verifiable proofs!



Impact

37 years laters, zero-knowledge proofs have revolutionised cryptography.

They enable powerful authentication and verification mechanisms: any user can demonstrate possession of an appropriate credential, or execution of an appropriate procedure, without revealing any of the private information (personal data, passwords, cryptographic keys) used in the process.

They are a core component in blockchain or in electronic voting, and are routinely used by banks and companies in the finance sector.