Zero-Knowledge Proofs
Showing that a problem has a solution without revealing it

The Origin

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

1986
Goldreich, Micali, and Rivest 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 are set at three different frequencies. To avoid interference, we want that two nearby towers always emit at a different frequency. In general, determining whether this basis can be achieved by a hard combination of towers, Dodgy is an agency that claims to have a solution (a setting of the frequencies) that works for it. Is Dodgy an operable and will only reveal the setting it claims has no interference? To verify this, Dodgy is asked and wants to be convinced that Dodgy really knows a solution before telling.

The paper of Goldreich, Micali, and Rivest gives a nice solution to the above constitution:

1. Dodgy chooses random names for the frequencies, A, B, and C.
2. Dodgy asks the name of the chosen frequency for each tower in a cryptographic box.
3. Towergrid reveals the name of the randomly chosen boxes for nearby towers.
4. Towergrid checks whether the boxes are indeed different.

After enough repetitions of steps 1 to 4, any observer is guaranteed to be fooled with whatever probability if error forgiveness here is achieved, but the solution is even more secure.

This radio tower problem described above is well known to be "incomplete" in essence, this means that by finding a zero-knowledge proof for this problem, Goldreich, Micali, and Rivest have in fact found a zero-knowledge proof for all problems with efficiently-verifiable proofs.

Impact

37 years later, zero-knowledge proofs have revolutionized cryptography. They enable powerful authentication and verification mechanisms and are now demonstrated in the possession of an appropriate credential, or execution of an appropriate procedure, without revealing any of the private information (personal data, passwords, cryptographic keys) kept used in the process.

They are a core component of identification in electronic voting, and are mostly used by banks and companies in the financial sector.