zero-knowledge proof of disjunctive statements (OR proofs)

Asked 4 years, 9 months ago Modified 11 months ago Viewed 1k times

2

I know there are standard ways to prove disjunctive statements about discrete logs, e.g. OR proof. But are there similar approaches for other class of language? For example, how can one go about proving either G_1 or G_2 has a Hamiltonian path (without leaking which one)?

zero-knowledge-proofs

1

Share Improve this question Follow

asked May 26, 2017 at 11:53

qweruiop

326 1 9

1 Answer

Active Oldest Votes

4

You can use the CDS94-technique for that. Suppose you have two zero-knowledge proof systems σ_1 and σ_2, both of which consist of three messages: a commitment com, a (public-coin) challenge ch, and a response r. And suppose you want to prove the OR of both claims, meaning that you can generate a valid proof for (wlog.) σ_1 for any challenge even after generating the commitment, but in order to generate a valid proof for σ_2 you must get the challenge first and compute the commitment from there. So you have essentially one degree of freedom in the choice of (ch_1, ch_2), *i.e.*, one is fixed beforehand but you want to hide which one. The clue is to get a new challenge ch' from the verifier and guarantee that (ch_1, ch_2, ch') satisfies a suitable relation, for instance sum-to-zero. So the proof system for σ_1-OR-σ_2 looks like this:

- preprocessing by the prover: compute com_2, ch_2, rsp_2 for a random ch_2
- prover sends commitment: com_1, com_2
- verifier sends challenge: ch'
- prover computes $ch_1 \leftarrow ch' - ch_2$ and uses this to complete σ_1
- prover sends response: $(ch_1, rsp_1), (ch_2, rsp_2)$
- verifier verifies that (com_1, ch_1, rsp_1) is valid, that (com_2, ch_2, rsp_2) is valid, and that $ch_1 + ch_2 + ch' = 0$

You can use $\sum_i ch_i = ch'$ for OR-proofs consisting of any number of claims. However, in some cases you want to prove more specific facts such as "t out of these n claims are true". In this case, you want to use Shamir's secret sharing and exchange the sum-to-zero relation for a polynomial of degree $n + 1 - t$: this guarantees that all $n - t$ degrees of freedom for choosing ch_i must be used up by the false claims.

The CDS-94 technique applies to any zero-knowledge proof system that follows this three-pass public coin structure. Schnorr's protocol for proving discrete logarithm knowledge is just one particular case of that structure.

CDS94: Cramer, Ronald, Ivan Damgård, and Berry Schoenmakers. "Proofs of partial knowledge and simplified design of witness hiding protocols." CRYPTO 1994.

Share Improve this answer Follow

edited Apr 11, 2021 at 9:39
Community Bot
1

answered May 26, 2017 at 12:55
Alan
1,350 8 9

Can you give an example for the "t out of n claims" or a reference? – Jus12 Jan 8, 2019 at 18:23

The CDS'94 paper referenced above treats this case extensively. – Alan Jan 9, 2019 at 19:15