zk-SNARK

A zk-SNARK is a cryptographic construction that allows you to provide a proof of knowledge (Argument of Knowledge) of secret inputs satisfying a public mathematical statement, without leaking any information on the inputs (Zero Knowledge).

In addition, verifying a proof is a computational operation which is at worst logarithmic in the size of the mathematical statement (Succinct), and the procedure of proving and verifying a proof requires no interaction between the prover and the verifier, except passing the proof to the verifier (non-interactive).

If we don't considerSuccinctness , and if we slightly modify the notion ofZero knowledge toHonest Verifier Zero Knowledge (which is weaker than theZero Knowledge property), examples of (HV)ZK-NARK are digital signatures algorithms ECDSA and EDDSA, which are in fact applications of the Schnorr Identification Protocol. It is essentially an argument of knowledge to prove knowledge of the discrete log of a point in a group where the discrete log is hard. Verifying such signatures is not computationally costly, but does not verify theSuccinctness property as it was previously defined.

The signature schemes are specific mathematical statements, orcircuits .

Withgnark , you can write any circuit using thegnark API . An instance of such a circuit ish a s h (x) = y hash(x)=y ha s h (x)

= y , wherey y y is public andx x x secret.

A valid proof of such a statement ensures that the creator of the proof knowsx x x such thath a s h (x) = y hash(x)=y ha s h (x)

= y , without revealingx x x . It is worth noting that ify y y is not specified, there are an infinity of couples(x , y) (x,y) (x ,

y) verifyingh a s h (x) = y hash(x)=y ha s h (x)

= y . But ify y y is specified, only onex x x verifies this relation.

Public and secret inputs

Given a mathematical statement, a zk-SNARK separates the inputs asp u b l i c public p u b l i c ands e c r e t secret secre t . Typically, thep u b l i c public p u b l i c inputs are known to everyone, and there is a uniques e c r e t secret secre t input such thats e c r e t + p u b l i c secret + public secre t

+ p u b l i c inputs satisfy the statement. It's exactly like a signature; given a valid signature, there is one unique secret key that leads to the signature. However there is an infinity of valid couples (signature, secret key).

zk-SNARK activity

zk-SNARK is an active area of academic research with improvements and new protocols announced weekly. For example, according to

"A Cambrian Explosion of Crypto Proofs" overview article on Nakamoto.com

we saw the following new zk-SNARK protocols in 2019: Libra, Sonic, SuperSonic, PlonK, SLONK, Halo, Marlin, Fractal, Spartan, Succinct Aurora, RedShift, AirAssembly.

tip There are many good expositions of zk-SNARKs. Recommended ones are:

- "What are zk-SNARKs?" article
- Matter Labs curated list of references
- . *[zk-SNARK]: Zero-Knowledge Succinct Non-Interactive Argument of KnowledgeEdit this page Last updatedonMar 2, 2023 byaybehrouz Previous Concepts Next Circuits and constraint systems
- Public and secret inputs
- zk-SNARK activity