Computation ⇒ Circuit → QAPs (QSPs) ⇒ SNARKs

zkSNARK

[GGPR13] @ Eurocrypt'13

In 2013, Gennaro et al. defined an useful translation of computations into polynomials called a Quadratic Arithmetic Program (QAP) and Quadratic Span Program (QSP)

for arithmetic circuit   for Boolean circuit

QAP has become the basis for zkSNARK construction.

Def 1. An arithmetic circuit consists of wires that carry values from $\mathbb{Z}_p^*$ (a field $\mathbb{F}$) and connect to addition and multiplication gates.

Boolean circuits operate over bits, with bitwise gates for AND, OR, XOR, etc.

Def 2. (Quadratic Arithmetic Program).

A QAP Q over field $\mathbb{F}$ contains three sets of $m+1$ polynomials

left input - $\mathcal{V} = \{v_k(x)\}$ for $k \in \{0, \cdots, m\}$

right input - $\mathcal{W} = \{w_k(x)\}$

output - $\mathcal{Y} = \{y_k(x)\}$

and a target polynomial $t(x)$.

Suppose F is a function that takes as input n elements of $\mathbb{F}$ and outputs n' elements.

let $N = n+n'$.

Then, we say that Q computes F if:

$(c_1, c_2, \cdots, c_N) \in \mathbb{F}^N$ is a valid assignment

iff there exists $(c_{N+1}, \cdots, c_m)$ s.t. $\underline{t(x) \text{ divides } p(x)}$ $\exists\, h(x)$ s.t. $p(x) = h(x) \cdot t(x)$

$$\text{where } p(x) = \left(v_0(x) + \sum_{k=1}^{m} c_k \cdot v_k(x)\right)\left(w_0(x) + \sum_{k=1}^{m} c_k \cdot w_k(x)\right) - \left(y_0(x) + \sum_{k=1}^{m} c_k \cdot y_k(x)\right).$$

Goal 주어진 입/출력에 대한 연산의 중간 과정을 압축하여 증명.

함수 F에 대하여 입력값을 넣으면 출력값이 나오고 그렇게 나오게 하는 중간값도 알고 있다.