- Scribes?
- lecture recording

$\underline{P}(C, w)$ $\qquad\qquad$ $\underline{V}(C)$ $\qquad\qquad$ $C(w) = 1$

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

<u>Soundness:</u> If C is not satisfiable then for any PPT P^*, $\Pr[\langle P^*, V(C)\rangle = \text{accept}] \leq \text{negl.}$

<u>Knowledge extraction</u>: For any PPT P^* and any C, if

P^* convinces $V(C)$ to accept w/ prob. ε then we can extract a witness w from P^* s.t. $C(w) = 1$ w/ prob. $\varepsilon - \text{negl}$

Gennaro-Gentry-Parno-Raykova

SNARK - <u>Succinct</u> non-interactive argument of knowledge

Bilinear maps: two groups G, G_T - cyclic groups, prime order q

bilinear map $e: G \times G \to G_T$

$$\underline{e(g^a, g^b) = e(g, g)^{ab}} \quad \text{for all } a, b \in \mathbb{Z}_q$$

$g^a, g^b \Longrightarrow g^{a+b}$

Knowledge assumption

Example: Consider the following problem:

given $\boxed{g^s, \quad g^{\alpha s}}$ for uniform $\alpha, s \in \mathbb{Z}_q$

output $P, Q \in G$ s.t. $\underline{P^\alpha = Q}$

(note: can check that $\underline{e(Q, g^s) \stackrel{?}{=} e(P, g^{\alpha s})}$

can write $Q = P^\beta$ for some β

$$e(Q, g^s) = e(P, g^{\alpha s})$$

$$\Longrightarrow e(P, g)^{\beta \cdot s} = e(P, g)^{\alpha \cdot s} \Longrightarrow \beta = \alpha \ )$$

Easy to do, as follows: pick arbitrary $r \in \mathbb{Z}_q$,

output $P = (g^s)^r, \quad Q = (g^{\alpha s})^r$

Assumption: this is the only way to solve the problem

More formally: given any PPT algorithm A where $A(X, Y)$ outputs P, Q s.t. $e(Q, X) = e(P, Y)$, we can extract from A a value r s.t. $P = X^r$, $Q = Y^r$

More generally: Given $g, g^s, g^{s^2}, \ldots, g^{s^n}$ ←

$g^\alpha, g^{\alpha s}, g^{\alpha s^2}, \ldots, g^{\alpha s^n}$, ←

if an algorithm can output P, Q s.t. $P^\alpha = Q$,

then we can extract $r_0, \ldots, r_n$ s.t.

$$P = \prod (g^{s^i})^{r_i}, \quad Q = \prod (g^{\alpha s^i})^{r_i}$$

equivalently, a polynomial $r(X)$ of degree at most n
s.t. $P = g^{r(s)}$, $Q = g^{\alpha \cdot r(s)}$

QAP - quadratic arithmetic program

Given set of polynomials $\underbrace{\{v_i\}_{i=0}^{n} \{w_i\}_{i=0}^{n} \{y_i\}_{i=0}^{n}}$ and a ~~target~~ target polynomial $\underline{t}$

Say this QAP is satisfiable if there exist $a_1, \dots, a_n \in \mathbb{Z}_q$

s.t. $t(X) \mid \underline{\left(\sum a_i \cdot v_i(X)\right) \cdot \left(\sum a_i \cdot w_i(X)\right) - \sum a_i\, y_i(X)}$

<u>Claim</u>: Any arithmetic circuit over $\mathbb{Z}_q$ can be transformed into a QAP s.t. QAP is satisfiable iff circuit is satisfiable

<u>Proof</u> (sketch)

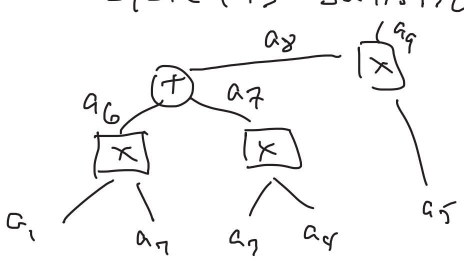
We can convert any arithmetic circuit into a set of quadratic constraints:

$$\boxed{\left(\sum a_i v_{iq}\right) \cdot \left(\sum a_i w_{iq}\right) = \sum a_i\, y_{i,q}} \qquad q = 1, \dots, N$$

$\{v_{iq}\}, \{w_{iq}\}, \{y_{iq}\}$ are public - determined by the circuit

The system is satisfiable iff $\exists\, a_1, \dots, a_n$ satisfying all equations

System is satisfiable $\iff$ circuit is satisfiable



$a_1 \cdot a_2 = a_6$

$a_3 \cdot a_4 = a_7$

$(a_6 + a_7) \cdot a_5 = a_9$

Define polynomials v_i, w_i, y_i as follows

- pick $r_1, \dots, r_N \in \mathbb{Z}_q$
- Make sure that $v_i(r_j) = v_{i,j}$ for $j = 1, \dots, N$

$$w_i(r_j) = w_{i,j}$$

$$y_i(r_j) = y_{i,j}$$

- Set $t(X) = \prod (x - r_i)$

Claim: $t(X) \mid \left(\sum a_i v_i(x)\right) \cdot \left(\sum a_i w_i(X)\right) - \sum a_i y_i(x)$

$\iff \{a_i\}$ satisfy the N equations above

Take any QAP $\{v_i\}, \{w_i\}, \{y_i\}, t$ $\qquad E(x) = g^x$

and construct a SNARK as follows:

CRS: $\{E(v_i(s))\}_{i=1}^n, \quad \{E(w_i(s))\}_{i=1}^n, \quad \{E(y_i(s))\}_{i=1}^n,$

$\{E(\alpha \cdot v_i(s))\}, \quad \{E(\alpha \cdot w_i(s))\}, \quad \{E(\alpha \cdot y_i(s))\},$

$\longrightarrow \{E(s^i)\}, \quad E(t(s))$

$\{E(\alpha \cdot s^i)\}$

Prover: Computes $h(X)$ and $\{a_i\}$ s.t.

$$h(X) \cdot t(X) = \left(\sum a_i v_i(X)\right) \cdot \left(\sum a_i w_i(X)\right) - \sum a_i y_i(X)$$

$$\left(\Rightarrow h(s) \cdot t(s) = \left(\sum a_i v_i(s)\right) \cdot \left(\sum a_i w_i(s)\right) - \sum a_i y_i(s)\right)$$

Output proof $E\left(\sum a_i v_i(s)\right), \ E\left(\sum a_i w_i(s)\right), \ E\left(\sum a_i y_i(s)\right), \ E(h(s))$

$E\left(\alpha \cdot \sum a_i v_i(s)\right), \ E\left(\alpha \cdot \sum a_i w_i(s)\right), \ E\left(\alpha \cdot \sum a_i y_i(s)\right),$

$E(\alpha \cdot h(s))$

Verify: check that each element in 2nd row is α times element in first row

Check that

$$\boxed{\underline{h(s)} \cdot \underline{t(s)} = \underline{\left(\sum a_i v_i(s)\right)} \cdot \underline{\left(\sum a_i w_i(s)\right)} - \underline{\sum a_i y_i(s)}}$$

<u>Soundness?</u>

Knowledge assumption tells us that the only way the prover could have generated $E(\sum a_i v_i(s))$, $E(\alpha \cdot \sum a_i v_i(s))$ is if it knows $\{a_i\}$ $\Rightarrow$ can extract those values