- Scribes?
- lecture recording

\[
P(C, w) \quad U(C) \quad C(w) = 1
\]

\[\arrowright\]

Soundness: If \( C \) is not satisfiable, then for any \( \text{PPT} \ p^* \), \( \Pr \left[ \langle p^*, U(C) \rangle = \text{accept} \right] \leq \text{negl} \).

Knowledge extraction: For any \( \text{PPT} \ p^* \) and any \( C \), if \( p^* \) convinces \( U(C) \) to accept \( w \) with \( \varepsilon \) then we can extract a witness \( w \) from \( p^* \) s.t. \( C(w) = 1 \) with prob. \( \varepsilon = \text{negl} \).

Genoa - Geneva - Paris - Ravello

SNARK - Succinct non-interactive argument of knowledge

Bilinear maps: two groups \( G, G_T \), cyclic groups, prime order \( q \).

\[ e: G \times G \rightarrow G_T \]

\[ e(g^a, g^b) = e(g, g)^{ab} \] for all \( a, b \in \mathbb{Z}_q \).
$g^a, g^b \Rightarrow g^{a+b}$

Knowledge assumption

Example: Consider the following problem:

given \begin{bmatrix} g^3, g^{\alpha s} \end{bmatrix}

For uniform $\alpha, s \in \mathbb{Z}_q$

output $P, Q \in G$ s.t. $p^\alpha = Q$

(Note: can check that $e(Q, g^3) = e(P, g^{\alpha s})$)

Can write $Q = P^\beta$ for some $\beta$

e($Q, g^3$) = e($P, g^{\alpha s}$)

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

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

output $P = (g^a)^c$, $Q = (g^{\alpha s})^c$

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 $c$ s.t. $P = X^c$, $Q = Y^c$.

More generally: Given $g, g^3, g^{3^2}, \ldots, g^{3^n}$

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

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

then we can extract $c_0, \ldots, c_n$ s.t.

$P = \Pi(g^{3^{c_i}})$, $Q = \Pi(g^{\alpha s^{c_i}})$;
equivalently, a polynomial \( r(X) \) of degree at most \( n \)
S.t. \( p = g^r(s) \), \( q = g^z \cdot r(s) \)

**QAP - quadratic arithmetic program**

Given set of polynomials \( \{ v_i \}_{i=0}^n \), \( \{ w_i \}_{i=0}^n \), \( \{ y_i \}_{i=0}^n \) and
c a target polynomial \( t \)
Say this QAP is satisfiable if there exist \( a_1, \ldots, a_n \in \mathbb{Z}_q \)
S.t. \( t(X) \mid (\sum a_i \cdot v_i(X)) \cdot (\sum a_i \cdot w_i(X)) - \sum a_i \cdot y_i(X) \)

**Claim:** Any arithmetic circuit over \( \mathbb{Z}_q \) can be transformed into a QAP s.t. QAP is satisfiable if circuit is satisfiable

**Proof (sketch)**

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

\[
(\sum a_i \cdot v_{iq}) \cdot (\sum a_i \cdot w_{iq}) = \sum a_i \cdot y_{iq} \\
q \leq 1, \ldots, N
\]

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

The system is satisfiable if \( \exists a_1, \ldots, a_n \) satisfying all equations

System is satisfiable \( \iff \) circuit is satisfiable

\[
a_1 \cdot a_2 = a_6 \\
a_3 \cdot a_7 = a_4 \\
(a_6 + a_7) \cdot a_5 = a_9
\]

Define polynomials \( v_i, w_i, y_i \) as follows
- Pick \( r_1, \ldots, r_N \in \mathbb{Z}_q \)
- Make sure that \( v_i(c_j) = v_i;_j \) for \( j = 1, \ldots, N \)
  \( w_i(c_j) = w_i;_j \)
  \( y_i(c_j) = y_i;_j \)
- Set \( \tau(X) = \prod (X - c_i) \)

**Claim:** \( \tau(X) \mid (\sum a_i v_i(X)) \cdot (\sum a_i w_i(X)) - \sum a_i y_i(X) \)

\( \iff \) \( \alpha;_i \gamma;_i \) satisfy the \( N \) equations above

---

**Take any QAP \( \{ v_i \}, \{ w_i \}, \{ y_i \}, t \),**

\[ E(X) = 0 \]

**end construct a SNARK as follows:**

**CRS:**

\[ \{ E(v_i(s)) \}_{i=1}^{n}, \{ E(w_i(s)) \}_{i=1}^{n}, \{ E(y_i(s)) \}_{i=1}^{n}, \{ E(\alpha v_i(s)) \}, \{ E(\alpha w_i(s)) \}, \{ E(\alpha y_i(s)) \}, \]

\[ \{ E(s^i) \}, \quad E(t(s)) \]

\[ \{ E(\alpha s^i) \} \]

**Proof:** Computes \( h(X) \) and \( \alpha;_i \gamma;_i \) s.t.

\[ h(X) \cdot \tau(X) = (\sum a_i v_i(X)) \cdot (\sum a_i w_i(X)) - \sum a_i y_i(X) \]

\( \iff \)

\[ h(s) \cdot \tau(s) = (\sum a_i v_i(s)) \cdot (\sum a_i w_i(s)) - \sum a_i y_i(s) \]

**Output proof:**

\[ E(\sum a_i v_i(s)), E(\sum a_i w_i(s)), E(\alpha y_i(s)) \quad E(h(s)) \]

\[ E(\alpha \sum a_i v_i(s)), E(\alpha \sum a_i w_i(s)), E(\alpha \sum a_i y_i(s)) \]

\[ E(\alpha h(s)) \]

**Verify:** Check that each element in 2nd row is \( \alpha \) times element in first row
Check that:

$$h(s) \cdot f(s) = (\sum a \cdot v_i(s)) \cdot (\sum a \cdot w_i(s)) - \sum a \cdot y_i(s)$$

Soundness?

Knowledge assumption tells us that the only way the power could have generated $E(\sum a \cdot v_i(s)), E(\sum a \cdot w_i(s))$ is if it knows $p, q \Rightarrow$ can extract those values.