Groth-Ostrovsky-Sahai (GOS) construction:

1. "Commit" to all of the wire values in the circuit
2. Prove that each output wire is the NAND of the input wires.
3. Open the output wire to a 1 (and the input wires associated with the statement)

How to commit? Use a BGN encryption scheme!

Formally, let $C: \{0,1\}^n \times \{0,1\}^h \to \{0,1\}$ be the circuit

1. Let s be the number of wires in the circuit, Index them topologically.
2. Let $t_1, \ldots, t_s \in \{0,1\}$ be the value of the wires in $C(x, w)$
3. Prover commits to each wire by constructing a BGN ciphertext:
   - Sample $r_i \xleftarrow{R} \mathbb{Z}_N$ and set $c_i = g^{t_i} h^{r_i}$
   - For each NAND gate in the circuit (with wires i, j, k), construct a NIZK proof that $t_k = \text{NAND}(t_i, t_j)$ with respect to c_i, c_j, c_k and $t_i, t_j, t_k \in \{0,1\}$.

Proof consists of commitments $c_1, \ldots, c_s$, NIZK proofs for each NAND gate and the openings for the statement $(r_1, \ldots, r_n)$ and for the output r_s.

To verify, check NIZK proofs all verify and that

$$c_i = g^{x_i} h^{r_i} \text{ for all } i \in [n] \text{ and } c_s = g h^{r_s}$$

Suffices to construct NIZK proof that $t_k = \text{NAND}(t_i, t_j)$ and $t_i, t_j, t_k \in \{0,1\}$

Suppose $c = g^t h^r$. How to prove in zero-knowledge that $t \in \{0,1\}$ (i.e., without revealing t)?

<u>Idea</u>: $t \in \{0,1\}$ if and only if $t(t-1) = 0$. Use pairing to compute $g^{t(t-1)}$.

$$e(c, cg^{-1}) = e(g^t h^r, g^{t-1} h^r)$$
$$= \underbrace{e(g,g)^{t(t-1)}}_{\text{vanishes}} \cdot \underbrace{e(g^t, h^r) \cdot e(h^r, g^{t-1}) \cdot e(h^r, h^r)}_{e(h, (g^{2t-1} h^r)^r)}$$

Proof is $u = (g^{2t-1} h^r)^r$.

<u>Soundness</u>. Suppose $c \neq g^t h^r$ for some $t \in \{0,1\}$ and $r \in \mathbb{Z}_N$. Then,

$$e(c, cg^{-1}) = e(g^t h^r, g^{t-1} h^r)$$
$$= \underbrace{e(g,g)^{t(t-1)}}_{} \cdot \underbrace{e(g^t, h^r) \cdot e(g^{t-1}, h^r) \cdot e(h^r, h^r)}_{\text{mod-}q \text{ subgroup of } \mathbb{G}_T}$$

$t(t-1) \neq 0$ so this component is non-zero in the mod-p subgroup of $\mathbb{G}_T$

Thus, there does not exist $u \in \mathbb{G}$ such that
$$e(c, cg^{-1}) = \underbrace{e(h, u)}_{\text{zero in mod-}p \text{ subgroup}}.$$

Zero-knowledge: Proof is deterministic. To prove zero-knowledge, need to randomize (to hide values of t and r).

Prover picks $\alpha \xleftarrow{R} \mathbb{Z}_N^*$ Then,

$$e(h, u) = e(h^{\alpha}, u^{\alpha^{-1}})$$

Instead of giving out u, give out $\pi_1 = h^{\alpha}$ and $\pi_2 = u^{\alpha^{-1}}$.
Check that

$$e(c, cg^{-1}) \stackrel{?}{=} e(\pi_1, \pi_2) = e(h^{\alpha}, u^{\alpha^{-1}}) = e(h, u).$$

Also give out $\pi_3 = g^{\alpha}$ and have verifier check that

$$e(g, \pi_1) \stackrel{?}{=} e(\pi_3, h) \quad \text{[necessary for soundness]}$$

Correctness: $e(g, \pi_1) = e(g, h^{\alpha}) = e(g^{\alpha}, h) = e(\pi_3, h)$.

Randomization is sufficient to prove zero-knowledge.

Proving NAND relation: $\quad g^{t_1}h^{r_1} \quad g^{t_2}h^{r_2} \quad g^{t_3}h^{r_3}$

We can show that $t_1, t_2, t_3 \in \{0,1\}$. Suffices to now show that

$$t_3 = \text{NAND}(t_1, t_2).$$

When $t_1, t_2, t_3 \in \{0,1\}$, this holds if and only if

$$t_1 + t_2 - 2t_3 + 2 \in \{0,1\}$$

[Can just check 8 possibilities for t_1, t_2, t_3]

Can now use homomorphisms of BGN to prove this:

$$\begin{aligned} c_1 &= g^{t_1}h^{r_1} \\ c_2 &= g^{t_2}h^{r_2} \\ c_3 &= g^{t_3}h^{r_3} \end{aligned} \implies c_1 \cdot c_2 \cdot c_3^{-2} \cdot g^2 = \underbrace{g^{t_1+t_2-2t_3+2}\, h^{r_1+r_2-2r_3+2}}_{\text{prove this is commitment to } 0/1 \text{ value}}$$