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 $C: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}$ be the circuit

1. Let $s$ be the number of wires in the circuit. Index them topologically.
2. Let $t_1, ..., t_s \in \{0,1\}$ be the value of the wires in $C(x,w)$
3. Prover commits to each wire by constructing a BGN ciphertext:
   - Sample $r_i \in \mathbb{Z}_N$ 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 $c_1, ..., c_s$, NIZK proofs for each NAND gate and the openings for the statement $(r_1, ..., r_n)$ and for the output $r_s$.

To verify, check NIZK proofs all verify and that

$$c_i = g^{r_i} h^{r_i} \text{ for all } i \in \{n\} \text{ and } c_s = g^{r_s}$$
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 $t$)?

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

\[
e(c, cg^{-1}) = e(g^t h^r, g^{t-1} h^r) = e(g^t, h^r) \cdot e(h^r, g^{t-1}) \cdot e(h^r, h^r) \\
\text{vanishes for } e(h^r, g^{t-1}) = e(h^r, (g^{2t-1} h^r)^r)
\]

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

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

\[
e(c, cg^{-1}) = e(g^t h^r, g^{t-1} h^r) = e(g^t, h^r) \cdot e(h^r, g^{t-1}) \cdot e(h^r, h^r) \\
\text{mod-} \mathbb{G} \text{ subgroup of } \mathbb{G}_t
\]

$t(t-1) \neq 0$ 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

$e(c, cg^{-1}) = e(h, u)$.

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

Prover picks $\alpha \in \mathbb{Z}_N^*$. 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

$$e(c, cg^{-1}) = e(\Pi_1, \Pi_2) = e(h^\alpha, u^{\alpha^{-1}}) = e(h, u).$$

Also give out $\Pi_3 = g^\alpha$ and have verifier check that

$$e(g, \Pi_1) = e(\Pi_3, h) \quad \text{[necessary for soundness]}$$

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:

$$g^{t_1}h_1^{r_1}, g^{t_2}h_2^{r_2}, g^{t_3}h_3^{r_3}$$

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:

$$c_1 = g^{t_1}h_1^{r_1}, c_2 = g^{t_2}h_2^{r_2}, c_3 = g^{t_3}h_3^{r_3} \implies c_1 \cdot c_2 \cdot c_3^2 \cdot g^2 = g^{t_1 + t_2 - 2t_3 + 2}h^{r_1 + r_2 - 2r_3 + 2}$$

prove this is commitment to old value.