1 Addition gate

$P$ has $x_1, r_1, x_2, r_2, x_3, r_3$. Verifier has $c_i = g^{x_i} h^{r_i}$

$P$ wants to prove $x_1 + x_2 = x_3$. Or $x_3 - x_1 - x_2 = 0$

Prover proves that he knows $\log_h \frac{c_3}{c_1 c_2}$

1. $P$ picks $r \leftarrow \mathbb{Z}_p$. Sends $\alpha = h^r$ to $V$
2. $V$ sends a random $\beta$ to $P$
3. $P$ computes $\gamma = r + \beta(r_3 - r_1 - r_2)$ to $V$

$V$ checks that $h^\gamma = \alpha \cdot (c_3/(c_1 c_2))^\beta$
1.1 Special soundness

We have $\alpha, \beta, \beta', \gamma, \gamma'$ that the verification condition holds. Denote $C = \log_g h$. Take the logarithm to the base of $g$ of the verification condition

\[ C\gamma = \log_g \alpha + (x_3 + Cr_3 - x_2 - Cr_2 - x_1 - Cr_1)\beta \]
\[ C\gamma' = \log_g \alpha + (x_3 + Cr_3 - x_2 - Cr_2 - x_1 - Cr_1)\beta' \]

\[(x_3 + Cr_3 - x_2 - Cr_2 - x_1 - Cr_1)\beta - C\gamma = (x_3 + Cr_3 - x_2 - Cr_2 - x_1 - Cr_1)\beta' - C\gamma' \]

\[ C = \frac{-x_3\beta + x_2\beta + x_1\beta + x_3\beta' - x_2\beta' - x_1\beta'}{r_3\beta - r_2\beta - r_1\beta - \gamma - r_3\beta' + r_2\beta' + r_1\beta' + \gamma'} \]

\[ C = \frac{(x_3 - x_1 - x_2)(\beta' - \beta)}{(r_3 - r_1 - r_2)(\beta' - \beta) + \gamma' - \gamma} \]
2 Multiplication gate

$P$ has $x_1, r_1, x_2, r_2, x_3, r_3$. Verifier has $c_i = g^{x_i} h^{r_i}$

$P$ wants to prove $x_1 \cdot x_2 = x_3$.

\[
\begin{align*}
    c_1 &= g^{x_1} h^{r_1} \\
    c_2 &= g^{x_2} h^{r_2} \\
    c_3 &= g^{x_3} h^{r_3}
\end{align*}
\]

1. Prover generates random $s$ and gives $c_4 = c_1^{x_2} h^s$ to the verifier. Prover proves to the verifier that he knows $r'_2, s'$, such that

\[
(g, c_1, c_2/h^{r'_2}, c_4/h^{s'})
\]

is a DH tuple. I.e. $(g, h, c_1, c_2, c_4)$ belongs to the relation

\[
\{(g_1, g_2, g_3, h_1, h_2, h_3) \mid h_i = \prod_j g_j^{z_{ij}}\},
\]

where $z_{13} = z_{23} = z_{31} = 0$ and $z_{21} = z_{33}$. Prover knows that $c_4 = g^{x_1 x_2} h^{r_1 x_2 + s}$

2. Prover proves to the verifier that he knows the DL of $c_3/c_4$ to the base of $h$
3 Proving a disjunction

1st proof: \((x_1, w_1)\), protocol: \(\alpha_1, \beta_1, \gamma_1\)
2nd proof: \((x_2, w_2)\), protocol: \(\alpha_2, \beta_2, \gamma_2\)
\(\beta_1, \beta \in \mathbb{Z}_p\)
Prover can only do the \(j\)-th proof

1. Prover simulates \(\alpha_{3-j}, \beta_{3-j}, \gamma_{3-j}\)
2. Prover generates \(\alpha_j\) normally
3. Prover sends \(\alpha_1, \alpha_2\) to verifier
4. Verifier responds with \(\beta \in \mathbb{Z}_p\)
   - In soundness proof, there’s also \(\beta'\)
5. Prover takes \(\beta_j = \beta - \beta_{3-j}\)
   - In soundness proof, there’s also \(\beta'_j\). Actually, \(\beta'_{3-j} = \beta_{3-j}\)
6. Prover computes \(\gamma_j\), based on \(\alpha_j, \beta_j, x_j, w_j\)
   - In soundness proof, there’s also \(\gamma'_j\). And \(\gamma'_{3-j} = \gamma_{3-j}\)
7. Prover sends $\gamma_1, \gamma_2, \beta_1, \beta_2$ to verifier
   - In soundness proof, sends $\gamma'_1, \gamma'_2, \beta'_1, \beta'_2$ second time

8. Verifier verifies both $(x_1, \alpha_1, \beta_1, \gamma_1)$ and $(x_2, \alpha_2, \beta_2, \gamma_2)$
   - In soundness proof, there’s also $(x_1, \alpha_1, \beta'_1, \gamma'_1)$ and $(x_2, \alpha_2, \beta'_2, \gamma'_2)$

9. Verifier checks that $\beta_1 + \beta_2 = \beta$
$W, X, Y, Z \in \mathbb{Z}_q$. $\mathbf{R}$ computes $sW + tY, sX + tZ$.
Consider just two random elements: $A$ and $B$. If we put $A = sW + tY$ and $B = sX + tZ$, then can we find $s, t$?