

$$r, s \leftarrow \{0, 1\}^{n+1}, c \leftarrow \{0, 1\}^n$$