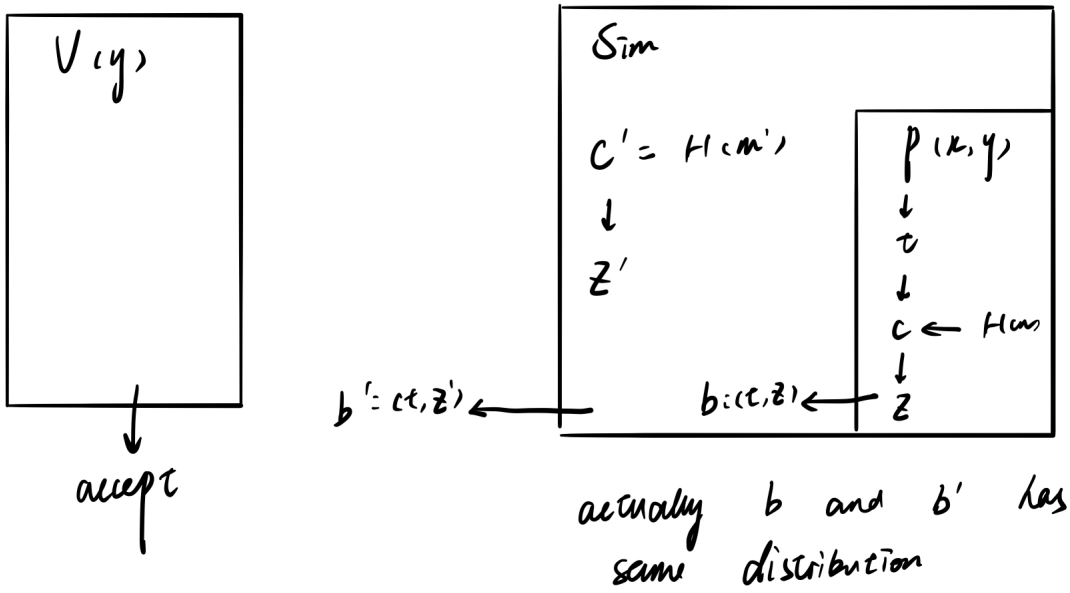
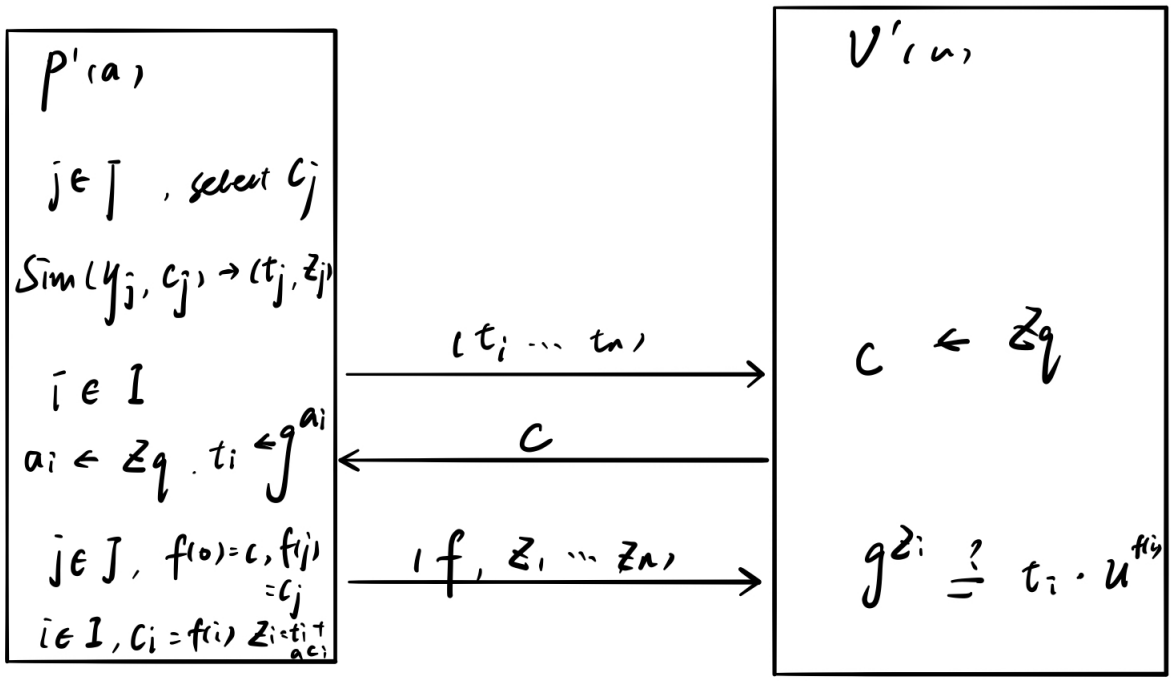
1: The First Problem



2: The Second Problem



3: The Third Problem

GQ is more efficient than RSA-FDH because it can reduce interaction rounds and credential holder cost.

GQ:

$\text{keyGen}()$: $x \leftarrow \mathbb{Z}_N^*$, $X \xleftarrow{N} x^e$

Sign:

$sk \leftarrow x$

$r_t \leftarrow \mathbb{Z}_n^*$, $y_t \leftarrow r_t^e$

$c \leftarrow H(m, y_t)$

$r_z \leftarrow r_t \cdot x^c$

$\sigma = (y_t, r_z)$ →

Verify:

$pk = y$

$c' \leftarrow H(m, y_t)$

accept:

$r_z^e = y_t \cdot y^{c'}$

RSA - FDH:

$\text{keyGen}()$: $pk \leftarrow (N, e)$, $sk \leftarrow (N, d)$

Sign (sk, m):

$\sigma \xleftarrow{N} [H(m)]^d$ →

Verify (pk, m, σ)

$b \leftarrow (\sigma^e \overset{N}{=} H(m))$