Zero knowledge using Garbled circuits

OR

How to prove non-algebraic stmts efficiently

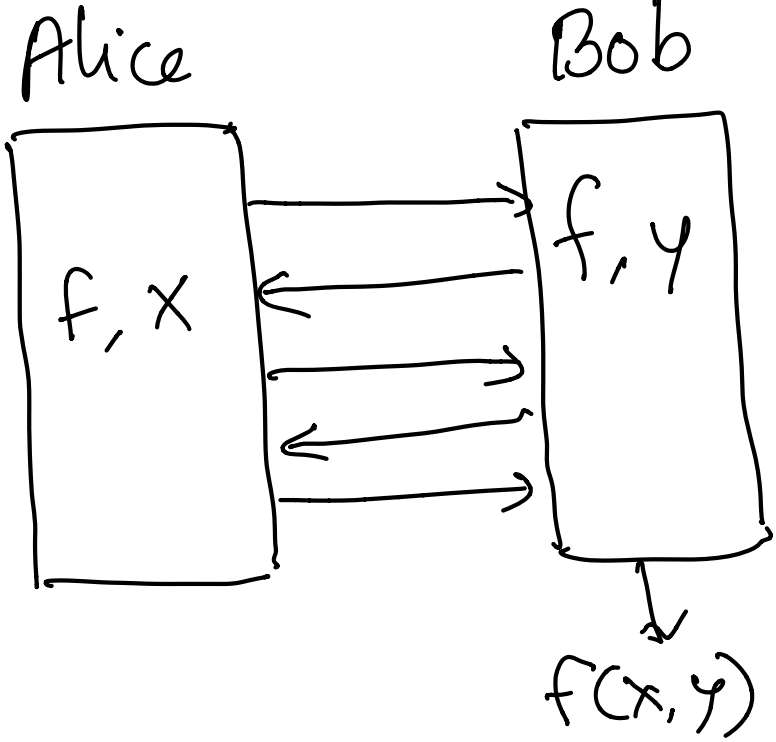
Proof : RH → Graph → 3-coloring

Non-algebraic statements : GC

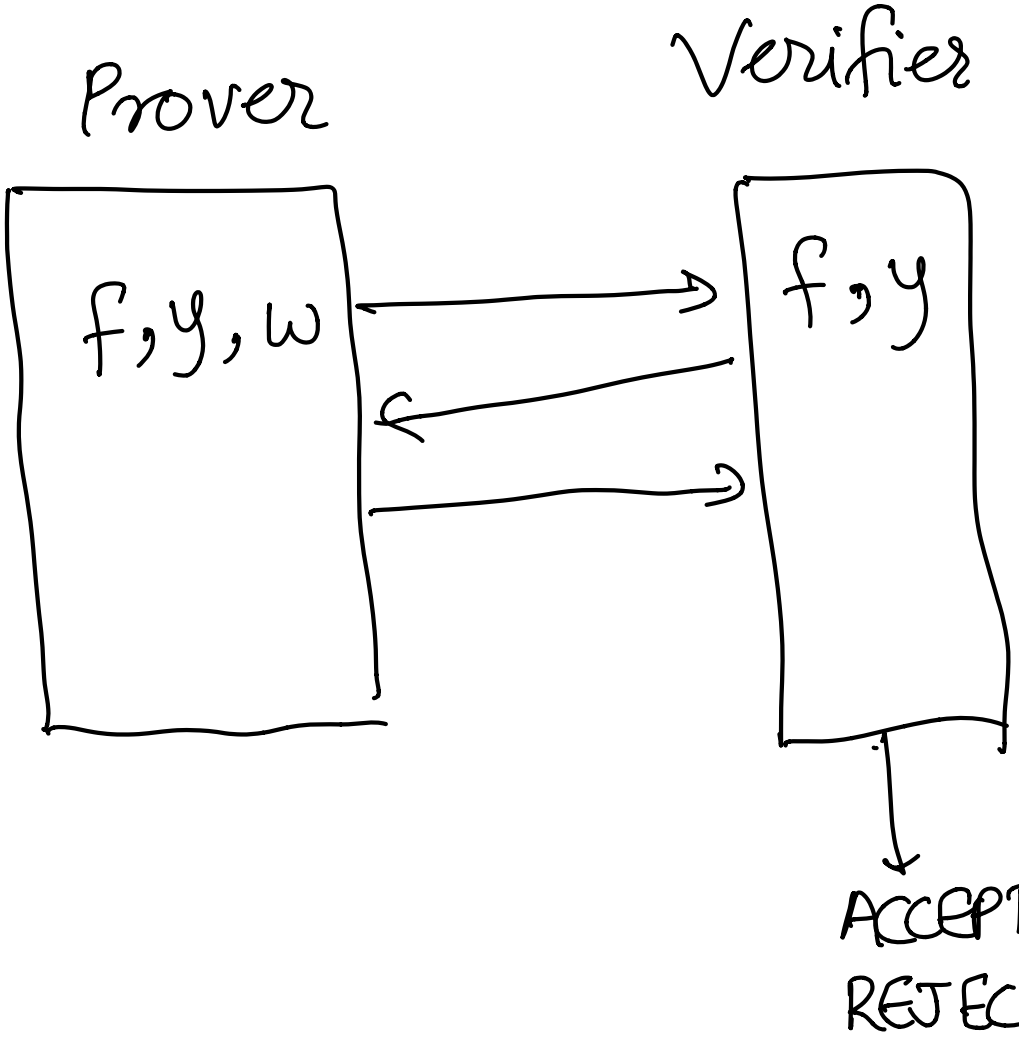
I have an x, s.t. $SHA\text{-}256(x) = y$

ZKP v/s 2PC

2PC $f(x,y)$



ZKP



Bellare's formulation of GC

1^k: security parameter

f: $\{0,1\}^n \longrightarrow \{0,1\}$

n: poly (k)

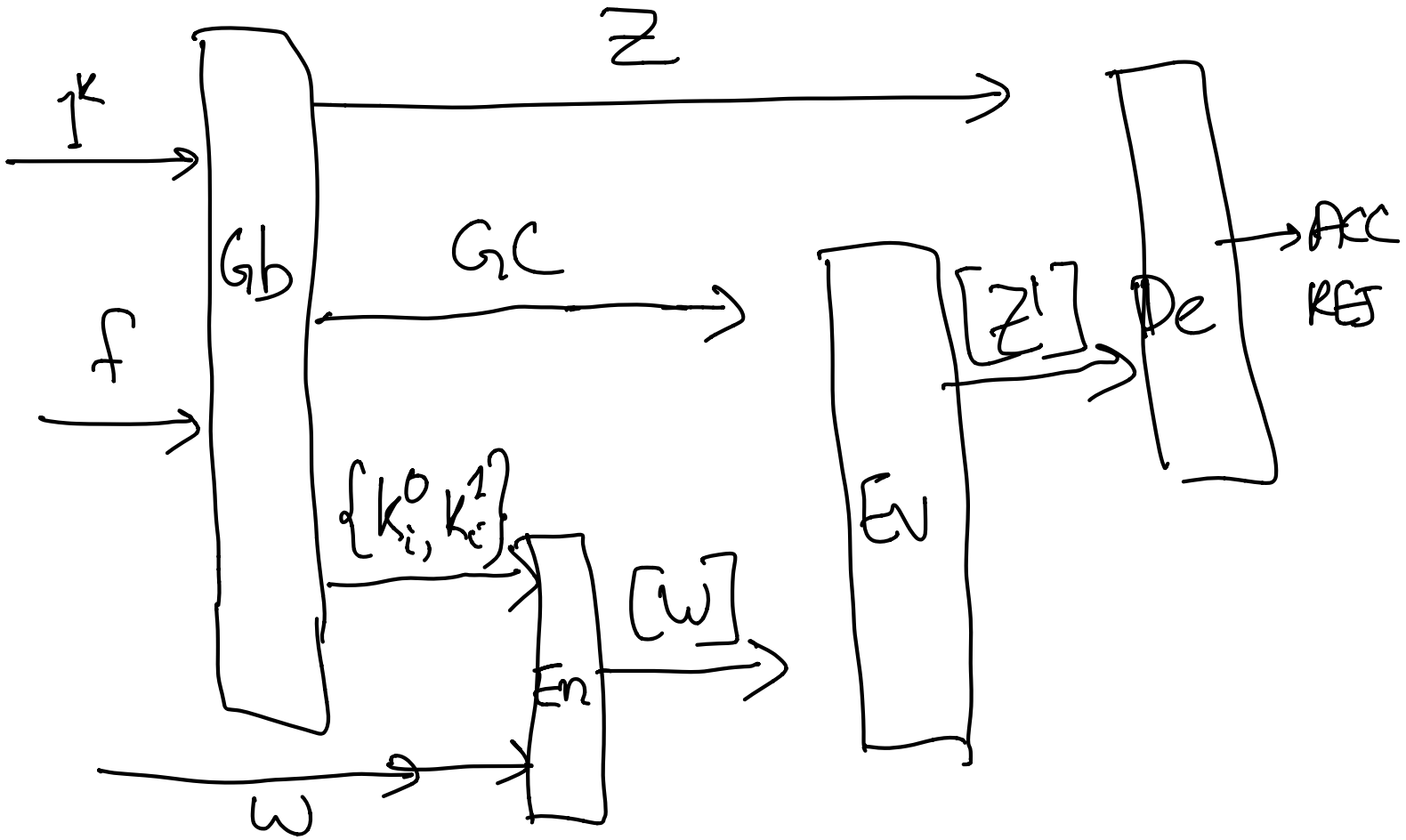
randomized

$Gb : (1^k, f) \longrightarrow (GC, \{K_i^0, K_i^1\}, [Z])$

$En : (\{k_i^0, k_i^1\}, w) \longrightarrow [W]$

$Ev : (GC, [W]) \longrightarrow [Z']$

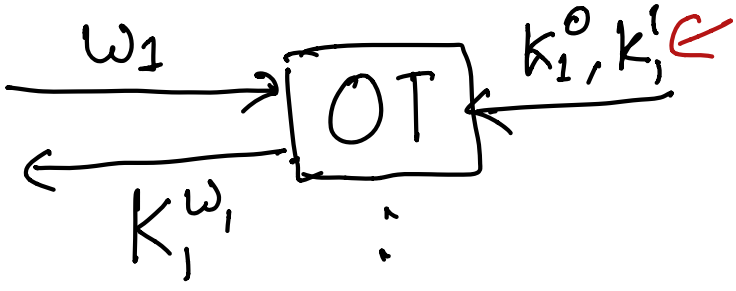
$De : ([Z'], [Z]) \longrightarrow$ ACCEPT
REJECT



Prover (w)

Verifier ( )

G, b



$[w]$

n times

$[GC]$

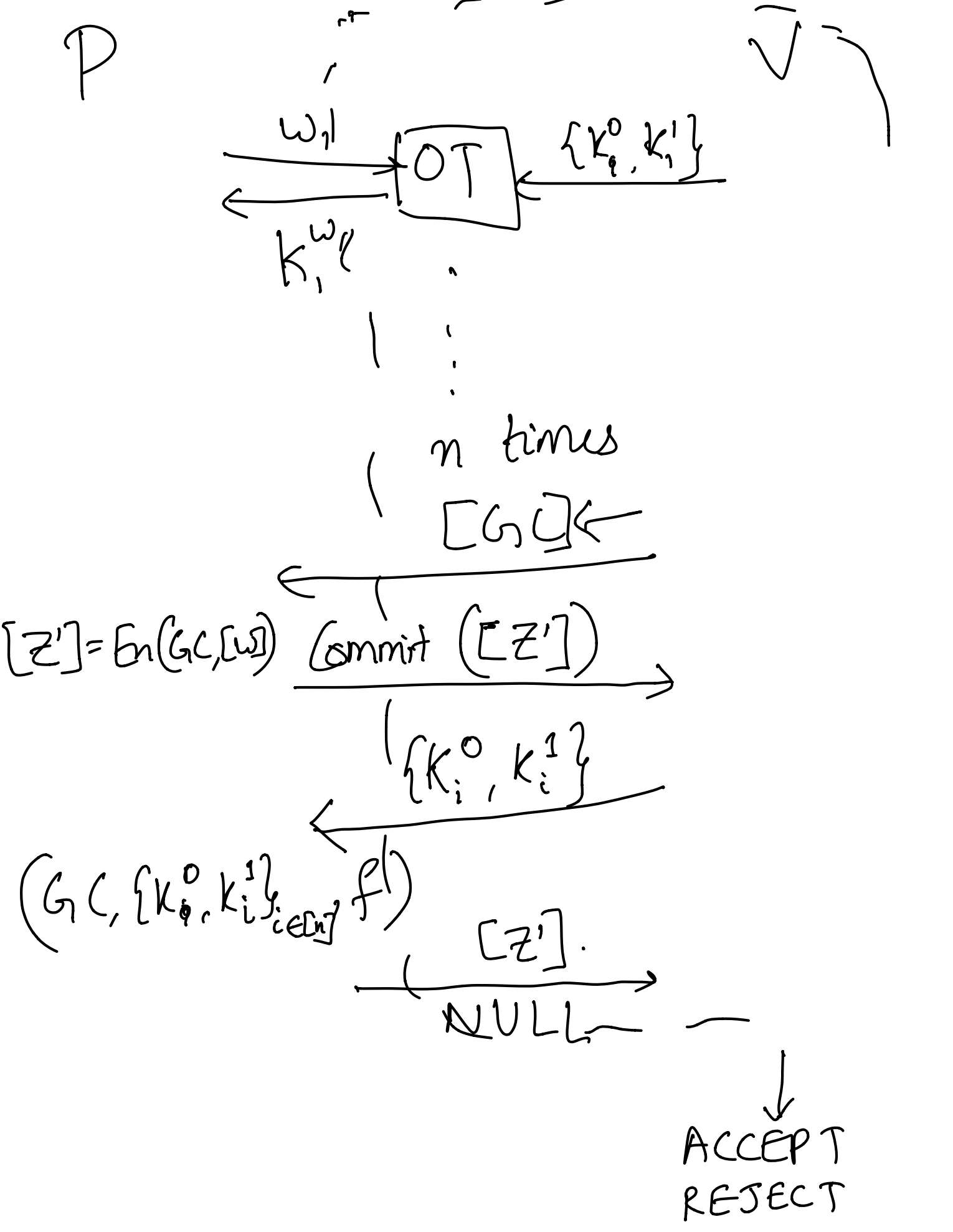
$[Z'] = En(GC, [w])$

$[Z']$

$De([Z'], [Z])$

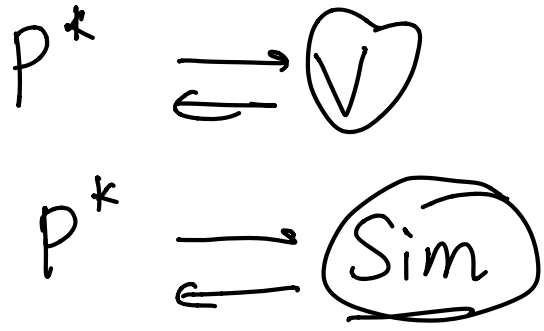
Q. Is this secure?

Q. Is this zero-knowledge?


P
V
w_1
OT
$\{k_1^0, k_1^1\}$
$k_1^{w_1}$
n times
$[G, C]$
$[z'] = Enc(GC, [w])$
Commit $([z'])$
$\{k_i^0, k_i^1\}$
$(GC, \{k_i^0, k_i^1\}_{i \in [n]}, f)$
$[z']$
NULL
ACCEPT
REJECT

Security

Malicious Prover P^*



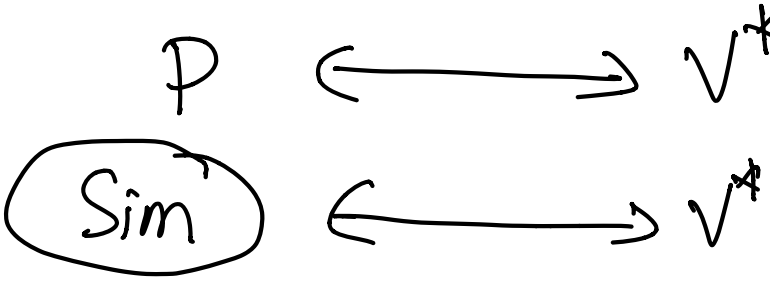
Sim knows w

$\Rightarrow$ If $f(w) = y$:

then ACCEPT

else REJECT

Malicious Verifier V^*



$$\{k_i^0, k_i^1\}_{i \in [n]}$$