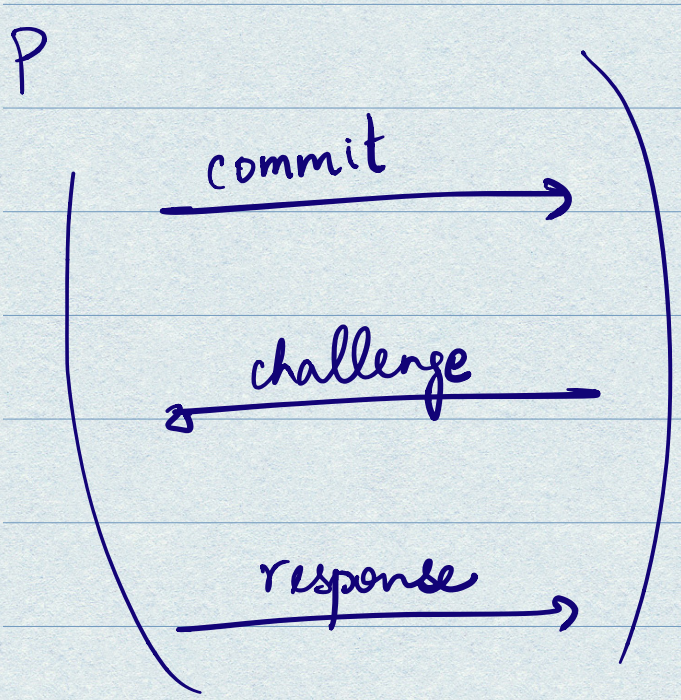
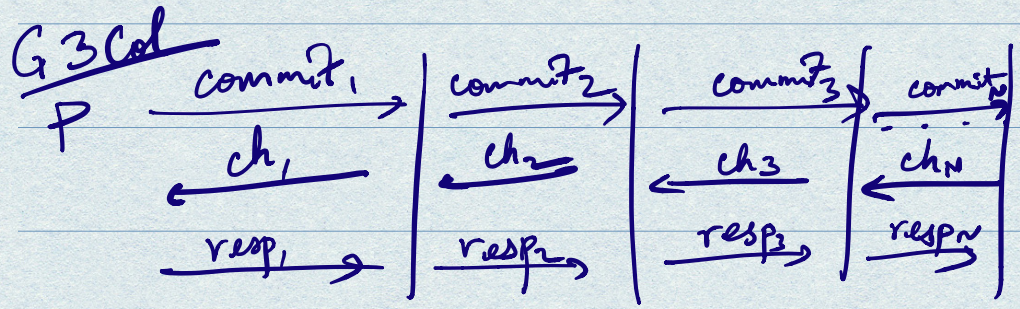
LECTURE - 17



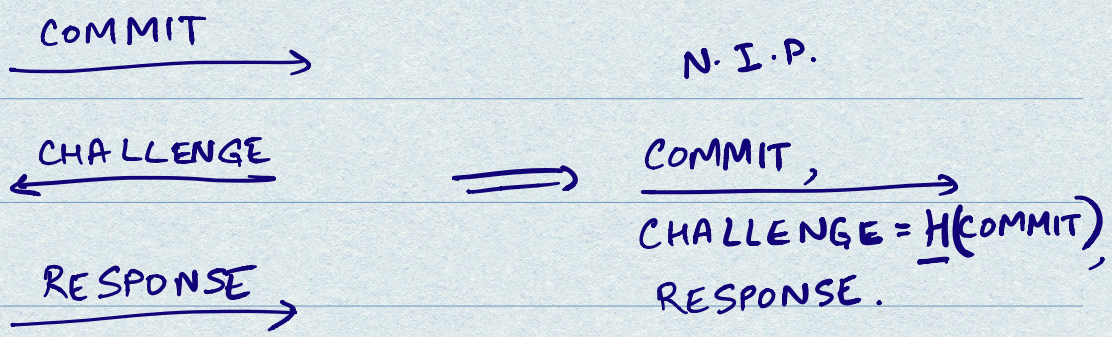
Σ - protocols

Graph 3-coloring : challenge space = # edges

Stern-like : challenge space = $\{1,2,3\}$



IN PRACTICE: Fiat-Shamir transform.



(Random Oracle): On every input, produces uniformly random output.

Assume SHA256 behaves like a Random Oracle.

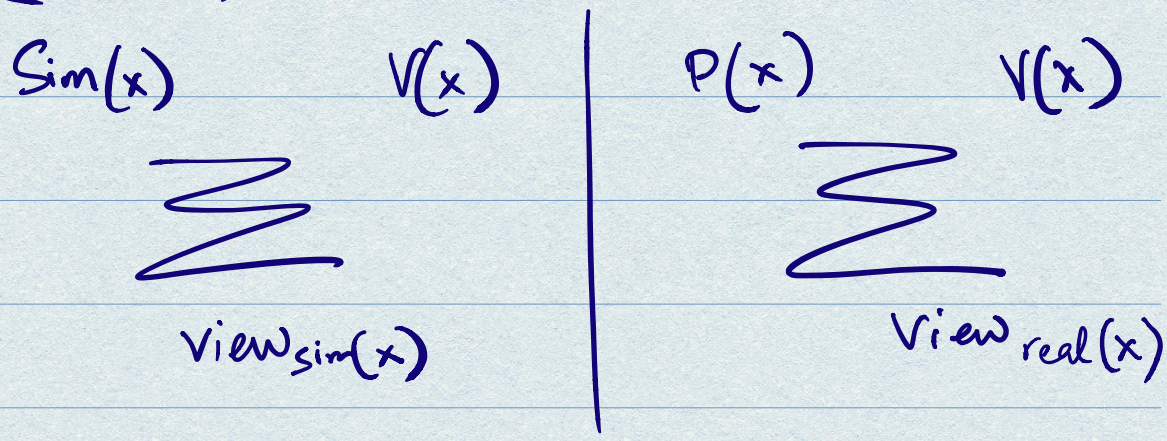
[Heuristic]

Resulting N.I.P. is simulatable (ZK) in Random Oracle Model.

In theory, there exist hash functions s.t. F-S for certain types of Σ-protocols is sound (and simulatable).

[Fiat-Shamir: From Practice to Theory]

(Lec 14)



$View_{sim} \approx View_{real}$.

$\Rightarrow View_{sim}(x)$ should be an accepting proof.

For NP-hard languages

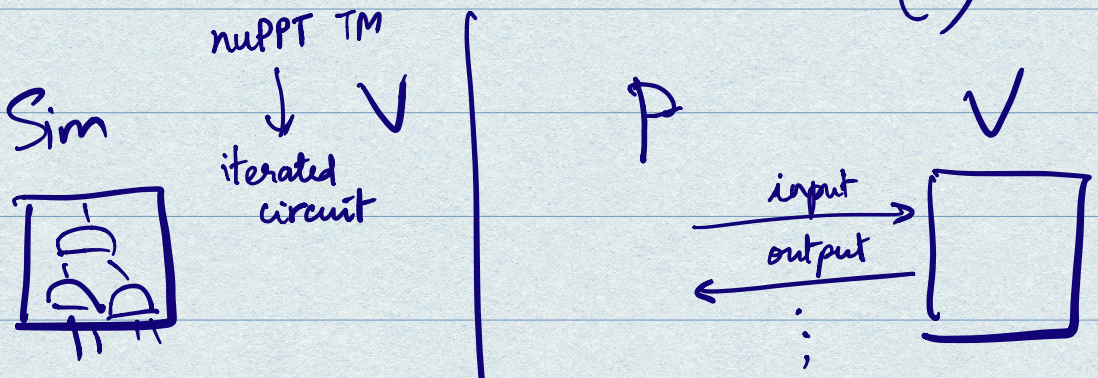
Sim(x) cannot decide whether $x \in L$.

$\Rightarrow View_{sim}(x)$ should be accepting even when $x \notin L$

"Rewinding". In ROM, Sim programs RO.

TODAY, Non-Black-Box Simulation

($\exists$ Sim s.t. $\forall V$ $Sim(V) \approx real$)

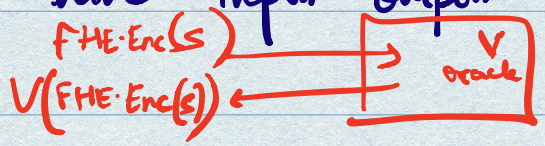


Q: Given FHE.Enc(s) and an arbitrary circuit V, is it possible to efficiently compute FHE.Enc(V(s))?

V lies in the class of circuits that

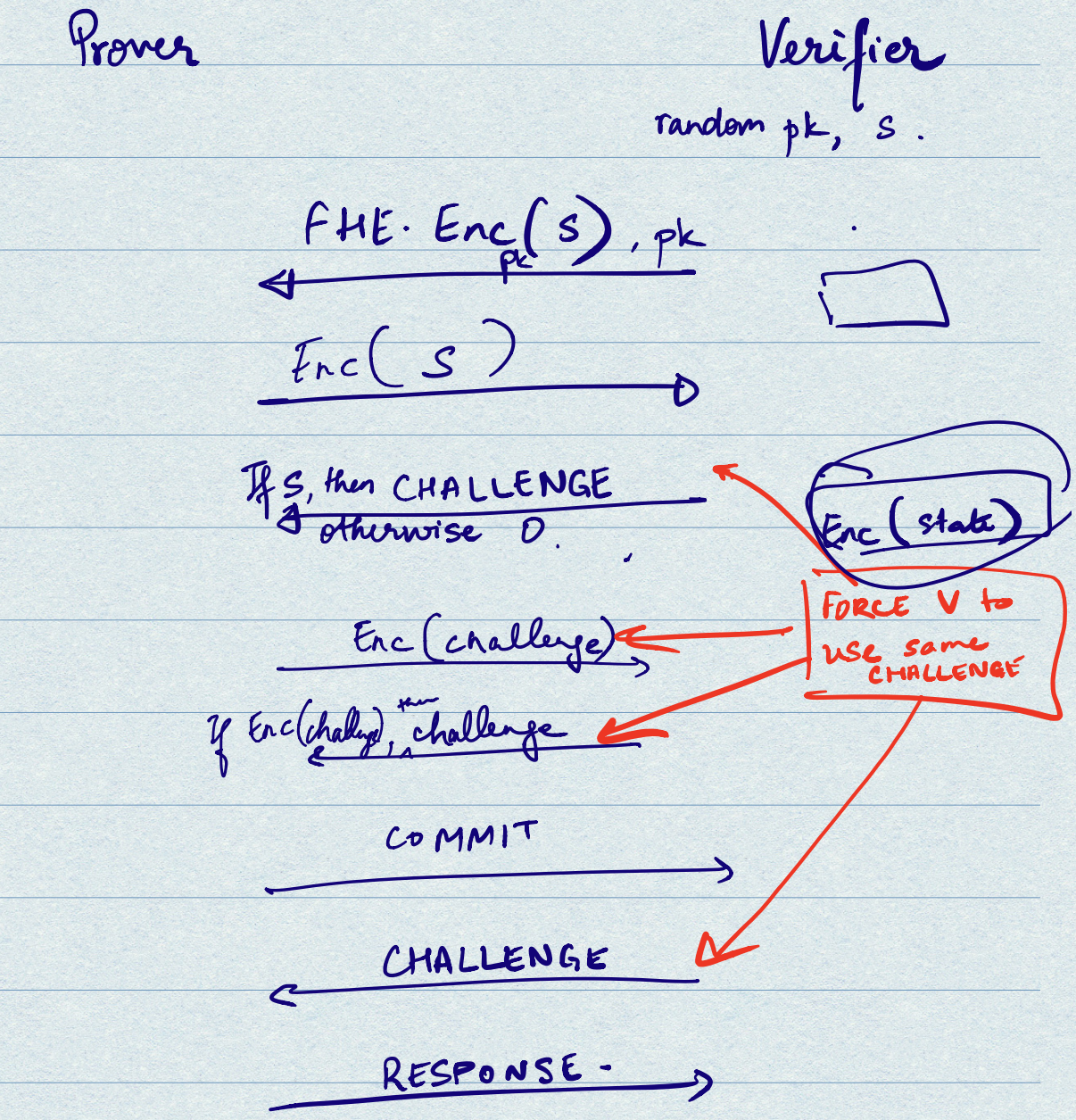
YES, assuming FHE supports

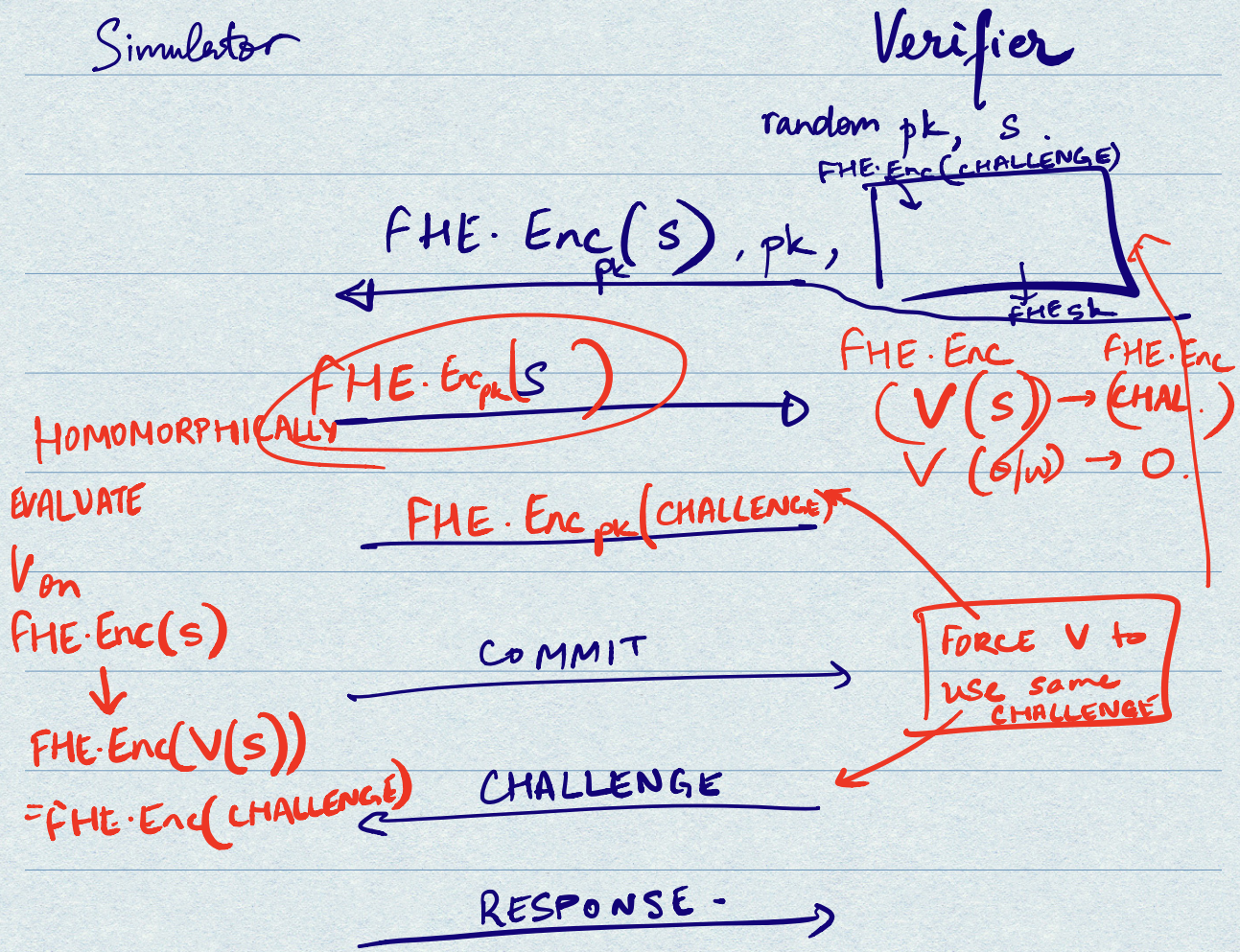
How about when you don't have circuit V, but only have input-output access to V?



Unclear.

GOAL: Design NBB ZK proof system





Sim obtained $FHE.Enc_{pk}(CHALLENGE)$.

Must now find a way to decrypt.

Selective decryption of FHE.Enc(CHALLENGE).

LOCKABLE OBFUSCATION

Obfuscation : FHE on steroids

↓ encrypted programs

↓ encrypted computation

LOCKABLE OBF. is concerned with a special class of programs.

$P_{[f, lock, msg]}$

On input x, if $f(x) = lock$, o/p msg

if $f(x) \neq lock$, o/p $\perp$.

Lockable Obfuscation :

$Obf(f, lock, msg) \longrightarrow \tilde{C}$ s.t. $\tilde{C} \equiv P_{f, lock, msg}$

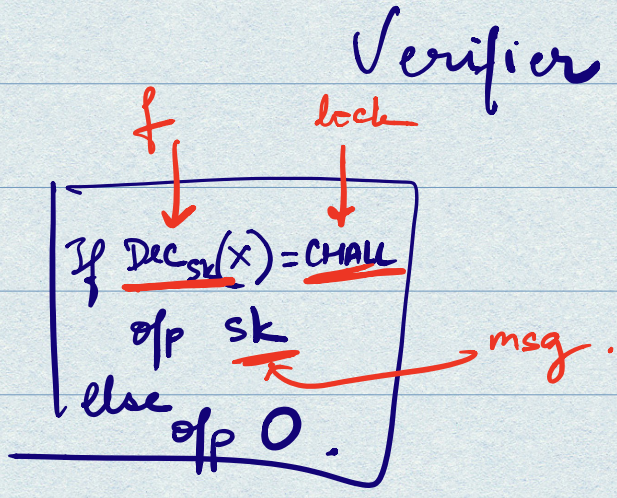
$\hat{C}(x)$: if $f(x) = lock$, return msg

else $\perp$.

SECURITY.

If $lock \leftarrow \{0,1\}^n$, $\hat{C} \approx_c Obf(f, \alpha, 0)$

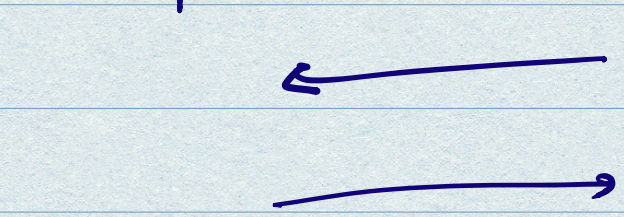
[i.e. msg is semantically hidden].

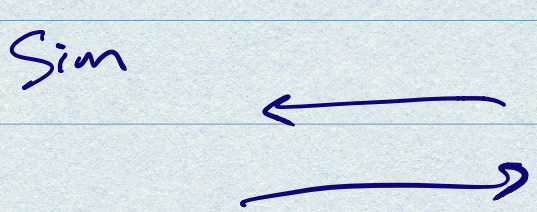


Can be obtained from LWE!

DISTINGUISHER-DEPENDENT ZK.

$\forall V, \forall \mathcal{D}, \exists$ Sim s.t. simulated-view $\approx$ real view by distinguisher $\mathcal{D}$





(Impossible via rewinding)

[Bitansky-Khurana-Paneth 19]

POST-QUANTUM ZK

[BITANSKY - SHMUELI 20].