LECTURE - 18

ZERO - KNOWLEDGE FAQ.

Proofs of Knowledge

GGM, AGM. : Generic Group / Algebraic Group Models.

Zero - Knowledge

* Rewinding - based
* NI Proofs in ROM
* FHE - based / NBB Zero - Knowledge

WHAT IS ZK USEFUL FOR?

SECURE COMPUTATION.

Alice f Bob

a b

(pk, sk)

pk FHE.Enc$_{pk}(a)$

y FHE.Enc$_{pk}(f(a,b))$

z FHE.Dec$_{sk}(y)$

$f(a,b)$ $f(a,b)$

$\exists (r, sk)$ s.t. $\text{FHE.Dec}_{sk}(y) = z$

AND $\text{KeyGen}(1^\lambda, r) \to sk, pk$

ZK compiles honest-but-curious to malicious protocols.

HONEST - BUT - CURIOUS / SEMI - HONEST SECURE COMPUTATION.

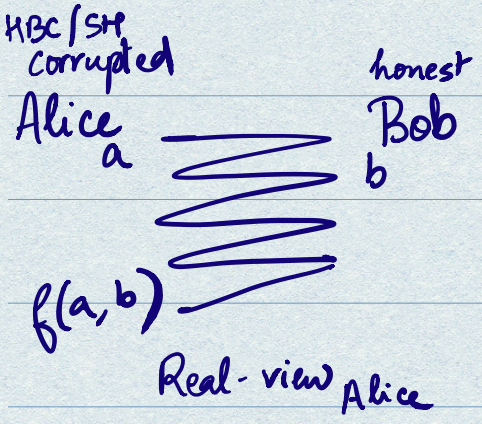
A protocol π is a HBC/SH secure comp. protocol if:

Correctness:

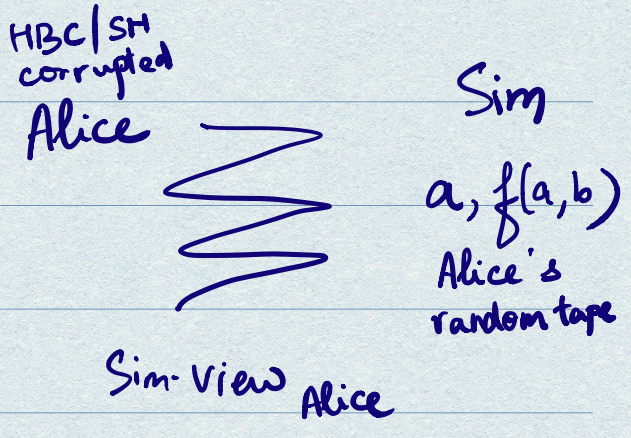
$$\forall a, b, f, \; out_{\pi}(Alice(a), Bob(b)) = f(a, b)$$

Security:

REAL



SIMULATED.

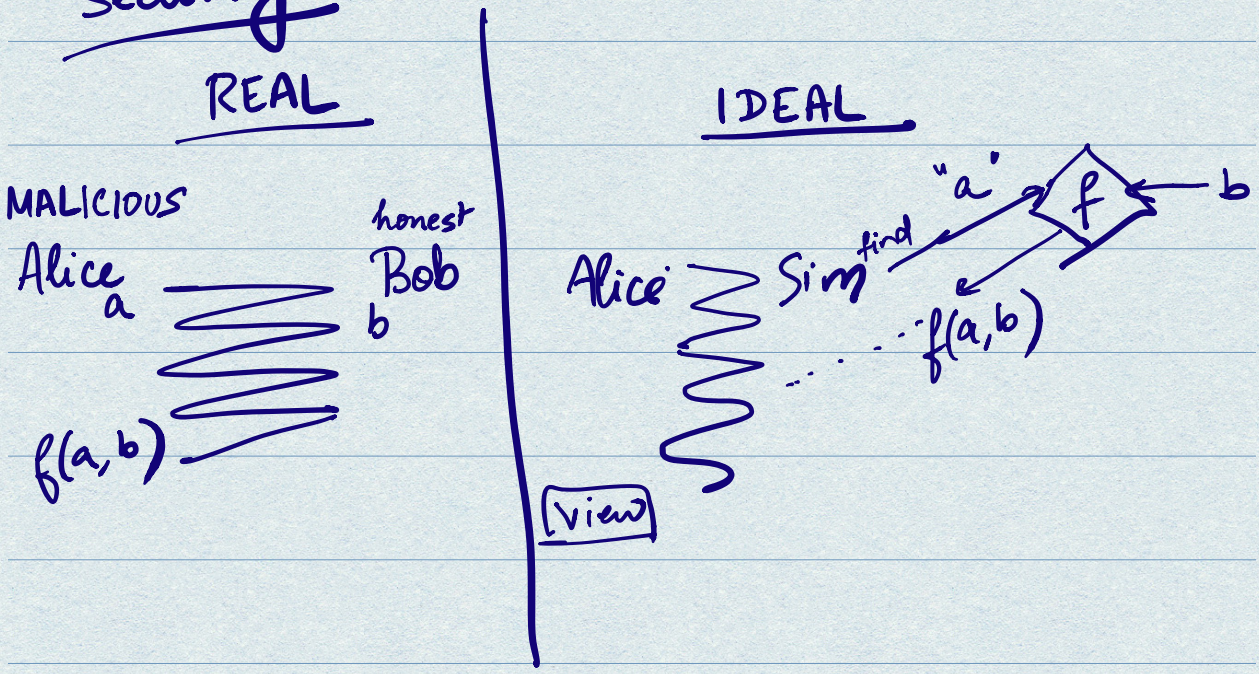


$$Real\text{-}view_{Alice} \approx Sim\text{-}view_{Alice}$$

MALICIOUSLY SECURE COMPUTATION

Correctness: Same as before.

Security:

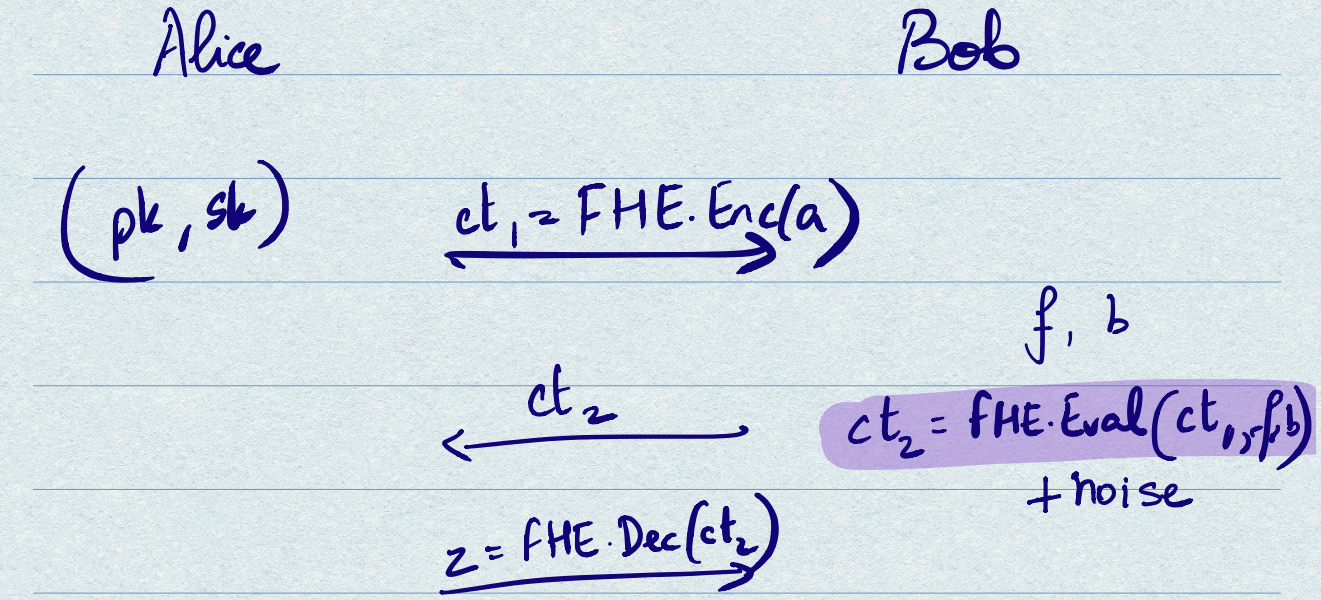


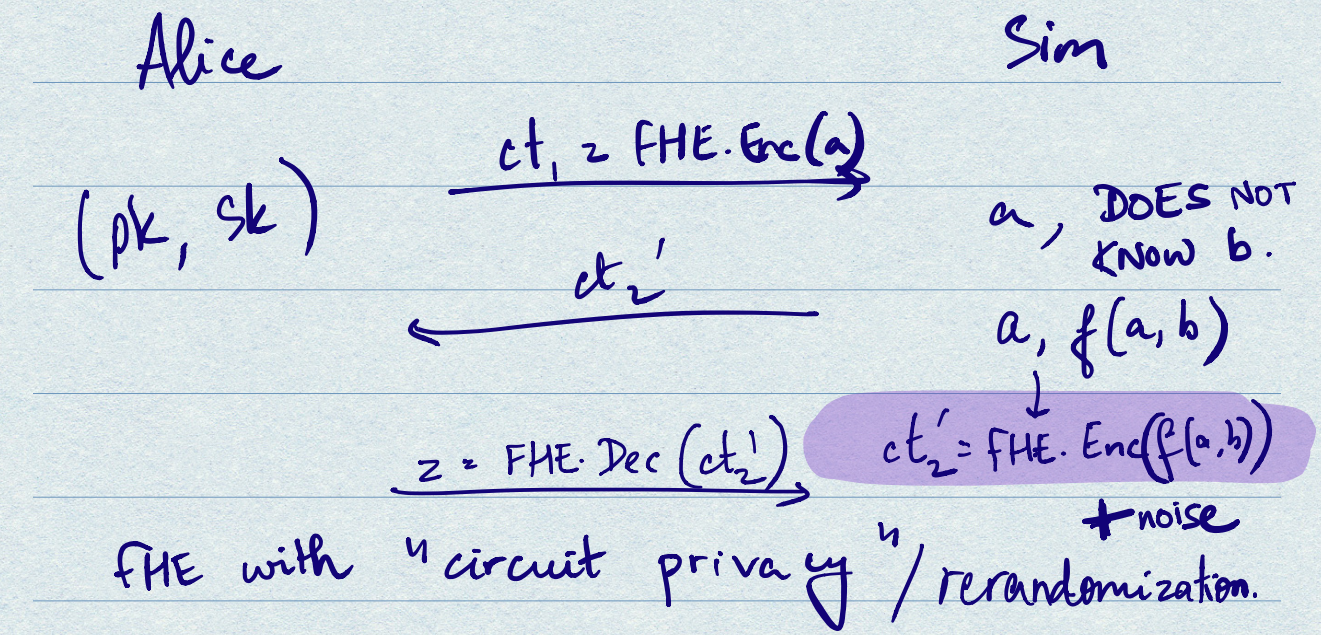
Real-view$_{Alice}$ $\approx$ Sim-view$_{Alice}$

(Anybody can run Sim on themselves)

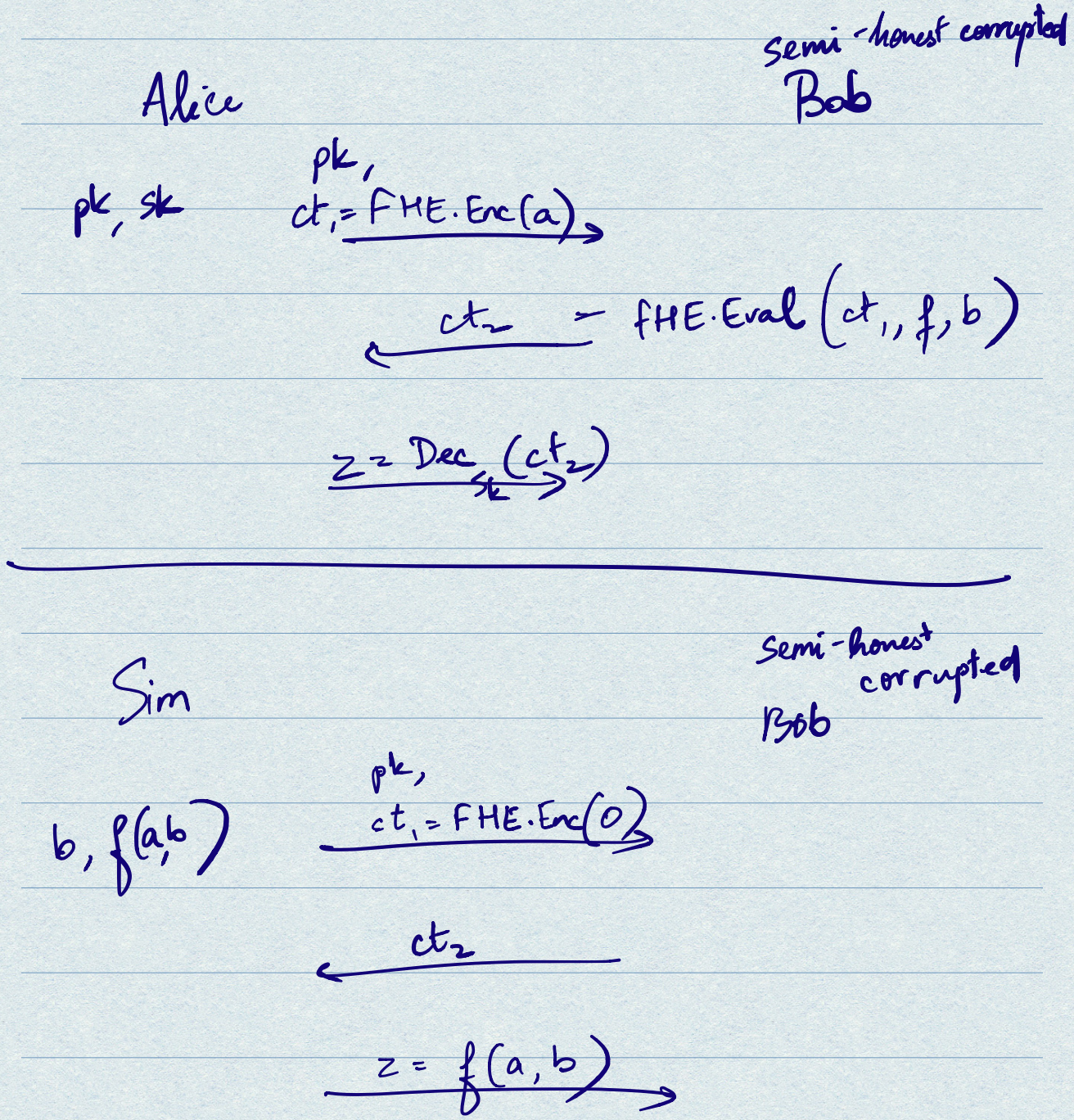
$f_1(a,b)$, $f_2(f_1(a,b), a, b \ldots)$

SEMI-HONEST SECURITY OF FHE-BASED PROTOCOL.

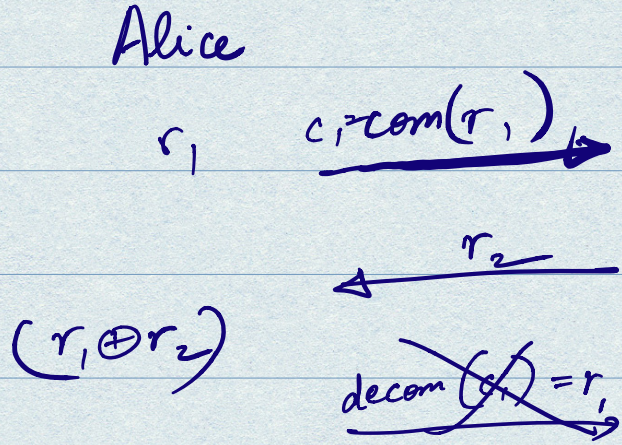




FHE with "circuit privacy" / rerandomization.


Alice
semi-honest corrupted
Bob
pk, sk
pk,
ct₁ = FHE.Enc(a)
ct₂ = fHE.Eval(ct₁, f, b)
z = Dec_sk(ct₂)
Sim
b, f(a,b)
semi-honest corrupted
Bob
pk,
ct₁ = FHE.Enc(0)
ct₂
z = f(a, b)

COIN-TOSSING



MALICIOUSLY SECURE FHE.

[GMW Compiler]