Lecture 14

BGG+ ABE

Zero Knowledge

BGG+ ABE

KeyGen $\longrightarrow$ MPK $= (A, A_1, \ldots A_\ell, v)$, $MSK = T_A$

$Enc(mpk, x, m; r) \longrightarrow$ Dual-Regev type ciphertext

$$s^T \left[A \,||\, A_1 - x_1 G \,||\, A_2 - x_2 G \,||\, \ldots\ldots \,||\, A_\ell - x_\ell G \right] + \text{noise},$$

$$s^T v + \text{noise} + \mu \lfloor \tfrac{q}{2} \rfloor$$

$SKGen(msk, f) \longrightarrow$ "short, nicely distributed" r

such that $[A \,||\, A_f - G] \cdot r = v$

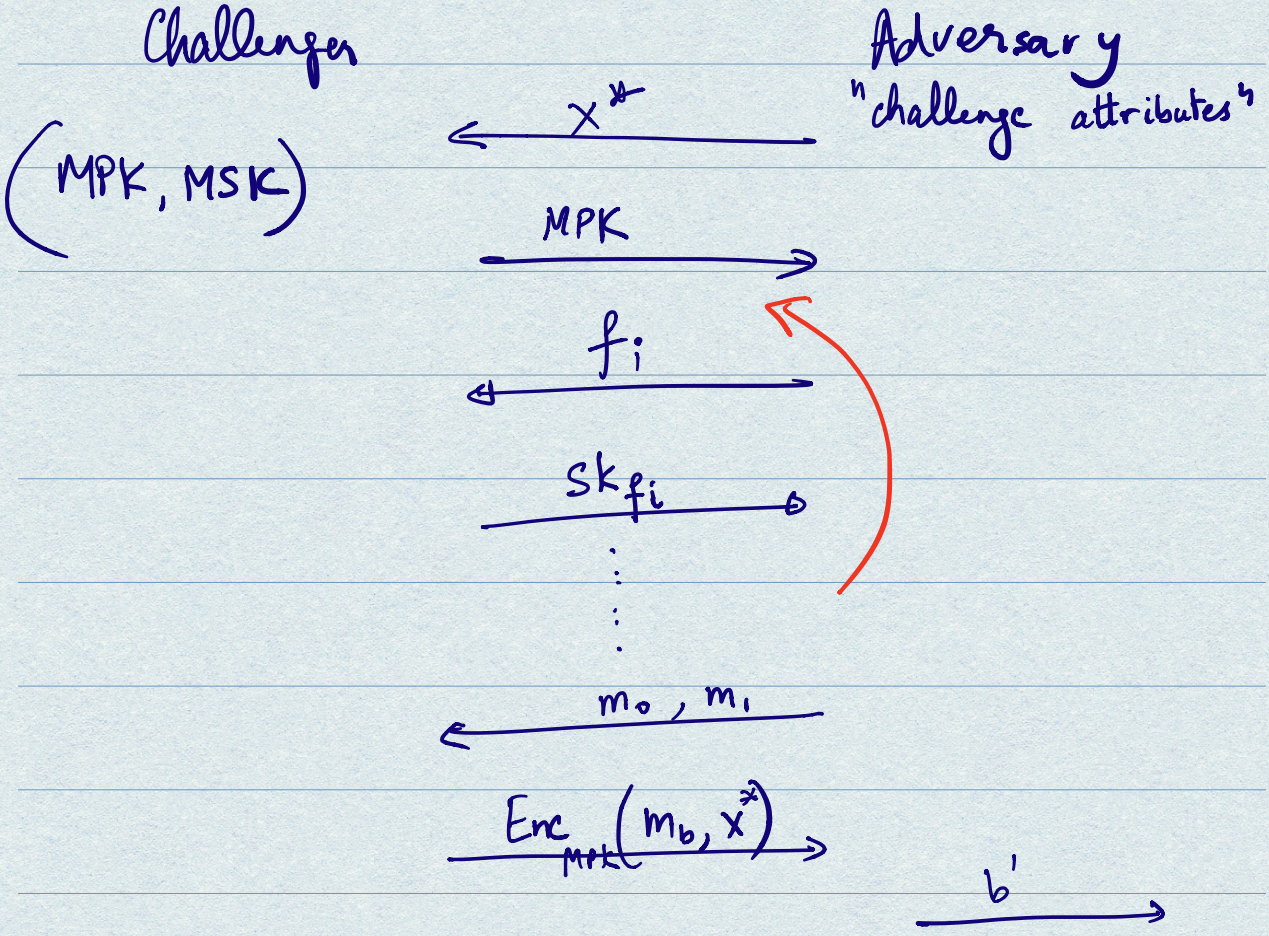
$Dec(sk_f, ct) \longrightarrow$ Parse $ct := (ct_1, ct_2)$

Perform homomorphisms on $ct_1 \longrightarrow s^T [A \,||\, A_f - f(x)G] + \text{noise}$

$s^T [A \,||\, A_f - f(x)G] \cdot r \approx s^T v$

Use this, and r, to recover μ from ct_2.

ABE SECURITY (selective)



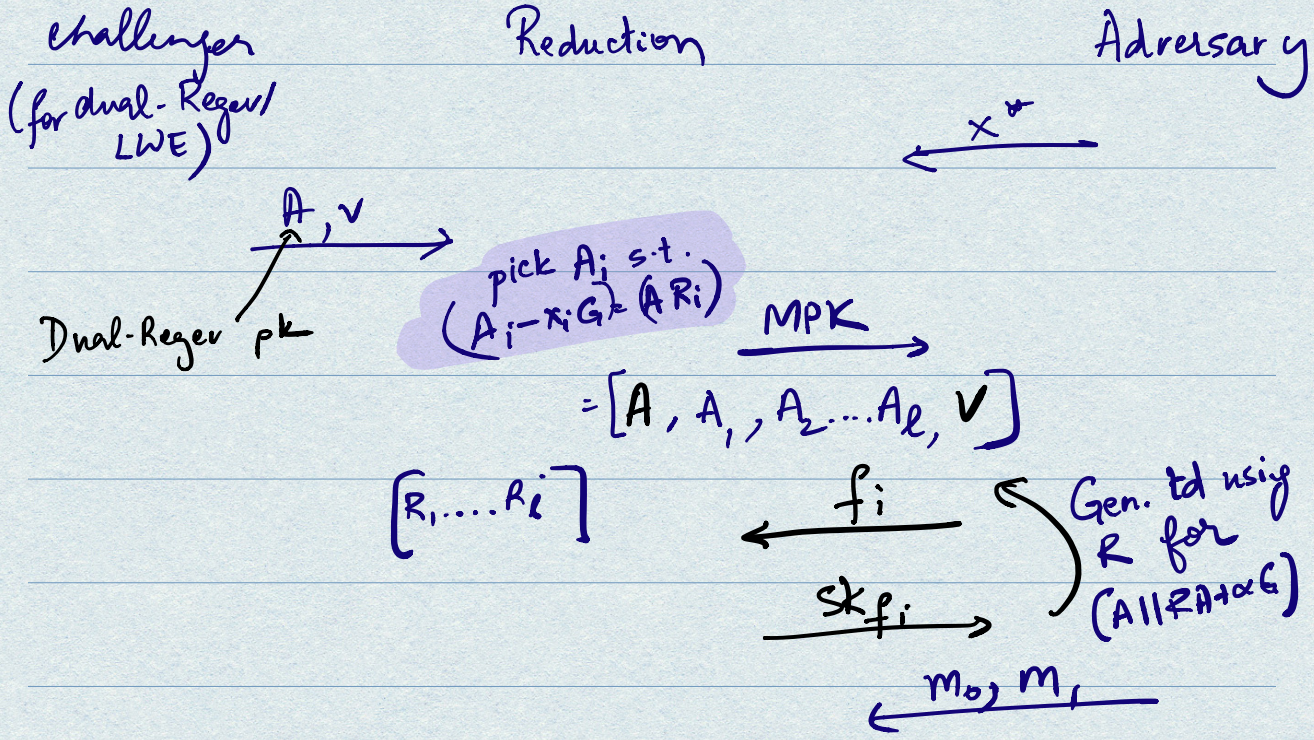
Adv "wins" if $(b' = b)$ AND $(\forall i, f_i(x^*) = 0)$,

↑ challenge attributes do not satisfy any function

We will say that ABE is secure

$$Pr[Adv \text{ wins}] \leq \frac{1}{2} + negl(\lambda)$$

Proof.



QUESTION:

$$(s^T A + \text{noise}) R \longrightarrow s^T A R + \text{noise} R$$

Suppose $(A_1 - x_1^* G) = AR$

Then $(s^T A + \text{noise}) R = s^T (A_1 - x_1^* G) + R \cdot \text{noise}$

On input f,

sk_f needs to be a short r

s.t. $\left(A \| A_f - G\right) r = v.$

But Reduction doesn't have access to T_A.

H.W. Given (B, R) where $B_2 \left[A \| RA + \alpha G \right]$ where $\alpha \neq 0$

One can find type-1 trapdoor for B.

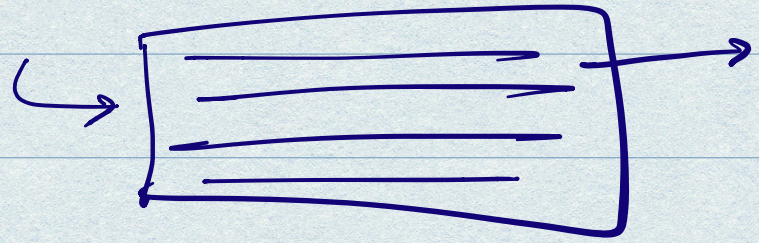
PART-2. **PROTOCOLS**

ZERO-KNOWLEDGE PROOF.

BLIND / SECURE COMPUTATION.

Prover

Verifier



Acc / Reject.

P V

q_1

a_1

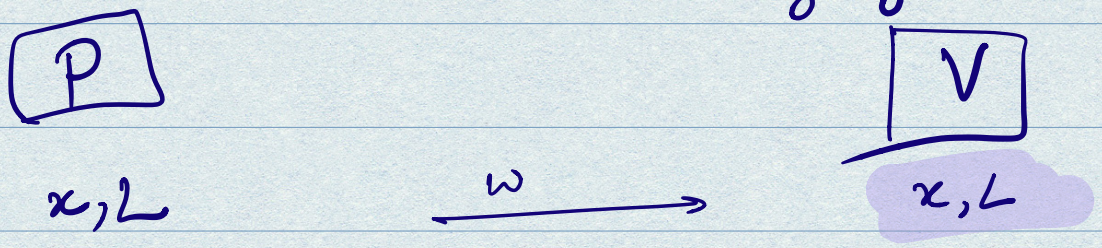
q_2

a_2

:

$Pr[V \text{ accepts} \mid P\text{'s claim false}] = negl(k)$

L is an NP language



Claim: $x \in L$

output acc $\iff R_L(x, w) = 1$.

Soundness: $\Pr[V \text{ accepts} \mid x \notin L] = \text{negl}(\lambda)$

Efficiency: V is a PPT machine.

No efficiency requirements on the prover.

Completeness: $\Pr[V \text{ accepts} \mid x \in L \text{ \& } P(x) \text{ followed instructions}] = 1 - \text{negl}(\lambda)$

APPLICATION

$pk, \text{Enc}_{pk}(m; r)$ ⟶ "x"

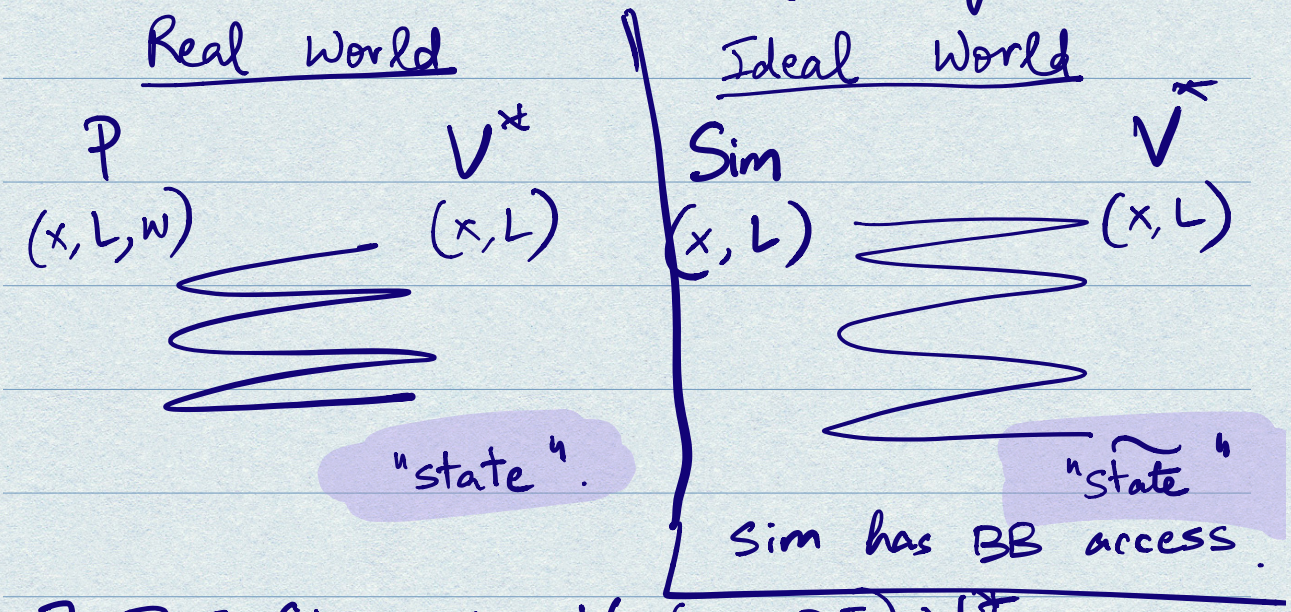
"w" = (m, r)

prove: $m < 100$.

"x", "L" defined as:

$$"L" = \{(pk, c) : \exists (m, r) \text{ s.t. } c = \text{Enc}_{pk}(m; r) \text{ and } m < 100\}$$

ZERO-KNOWLEDGE (Privacy):



$\exists$ PPT Sim s.t. $\forall$ (nu-PPT) V^*,

$\forall$ nu-PPT D (unbounded D)

$$\left| \Pr[D(\text{state}) = 1] - \Pr[D(\widetilde{\text{state}}) = 1] \right| = \text{negl}(\lambda)$$

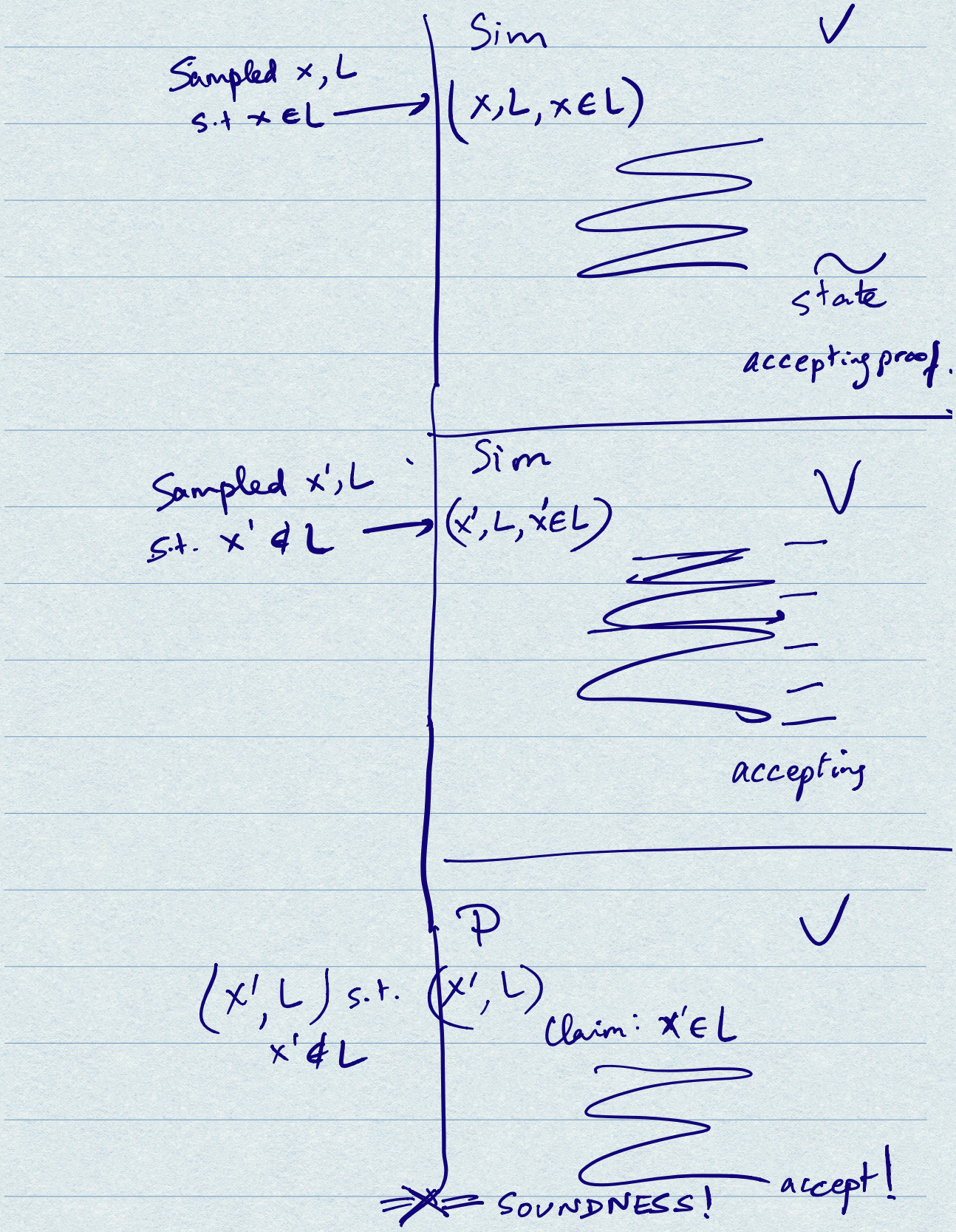
"Statistical zero-knowledge / SZK":

bounded V,

unbounded D.

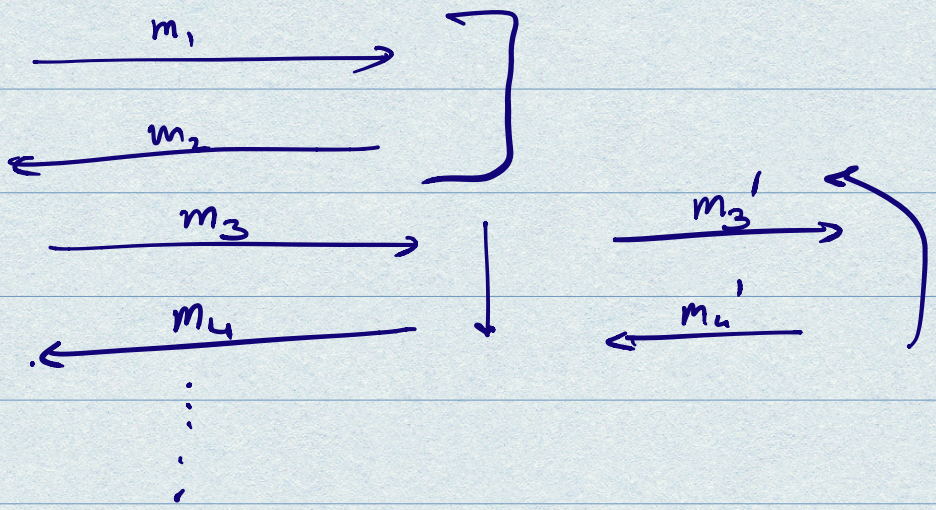
Black-box Simulation.

universal.


Sim
V
Sampled x, L
s.t. x ∈ L
(x, L, x ∈ L)
≈ state
accepting proof.
Sim
V
Sampled x', L
s.t. x' ∉ L
(x', L, x' ∈ L)
accepting
P
V
(x', L) s.t.
x' ∉ L
(x', L)
Claim: x' ∈ L
accept!
SOUNDNESS!

Black-box Simulation:

Sim has "oracle" access to V^* but can "rewind".



(Note: Prover cannot rewind)

Non-Black-Box Simulation:

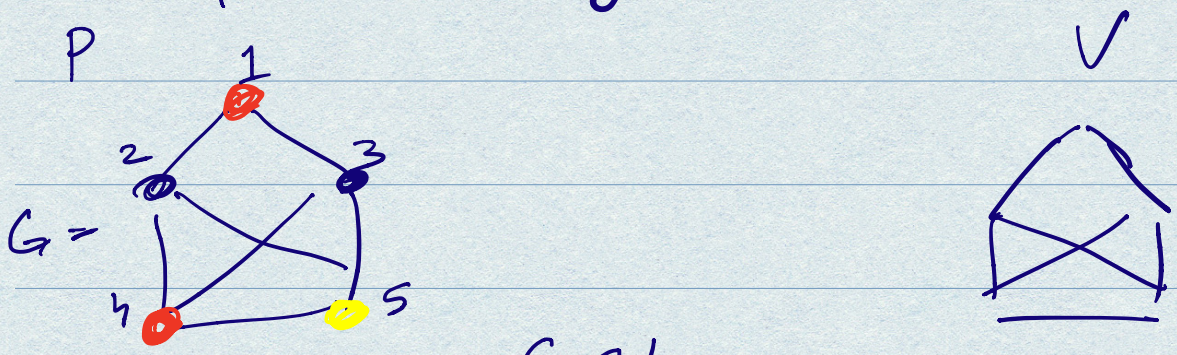
Sim has access to the description of the T.M. of V^*.

$Sim(V^*) \rightarrow$ state

EXAMPLE :

$L = \{ G : G \text{ is 3-colorable} \}$

Graph 3-coloring.



$G \in L$ ⟶

$w = (1, \bullet)$,

$(2, \bullet) \ldots$

$pk, enc(1, \bullet)$, ⟶ (2nd time)

⟵ $enc(2, \bullet)$

$\vdots$

$enc(5, \bullet)$

⟵ $v_1, v_2 \in V \times V$, s.t. v_1, v_2 connected by edge

"open" enc for v_1, v_2 ⟶

i.e., reveal colors & randomness used to build those encryptions