

# CryptoCommands Test

Roy Stracovsky

March 4, 2024

$\mathcal{A}$ ,  $\mathcal{F}$ ,  $\mathcal{Q}$ . I like the group  $\mathbb{G}$  and  $R$ ,  $\mathbb{F}$ .  $\perp$  vs  $\perp \mathcal{G}$ . and a bunch of random text to make the line longer and stuff. If I were to add more text would this work even more let me check.

Enc and Dec and Vrfy of  $\text{PKE.Enc}(\text{pk}, \text{msg})$ .  $\text{ct} \xleftarrow{\$} \text{PKE.Enc}(\text{pk}, \text{msg})$  and a bunch of random text to make the line longer and stuff.

$$\mathbf{Adv}_{\text{SE}, \mathcal{A}}^{\text{OW-Pass}}(\lambda) = \Pr[\mathcal{G}_{\text{SE}, \mathcal{A}}^{\text{Ind\$-CCA}}(\lambda) \Rightarrow 1].$$

$$\mathbf{Adv}_{\text{SE}, \mathcal{A}}^{2\text{PreR}}(\lambda) = \Pr[\mathcal{G}_{\text{SE}, \mathcal{A}}^{\text{EUf-CMA}}(\lambda) \Rightarrow 1].$$

We like random oracles  $\mathcal{O}$  and also some linear algebra  $\mathbf{A}\mathbf{s} + \mathbf{e}$ . The  $\mathbb{Z}_{\geq 0}$  is less ambiguous than using naturals. We work with  $\mathbb{Z}_p^*$  quite a lot and rarely  $\mathbb{Z}_{<0}$ . Also  $\mathbb{R} \setminus \mathbb{Q}$  and  $i\mathbb{R}$  haha.

I think I realized something.  $2^{\{0,1\}}$  no longer fails right. Sample an  $i \xleftarrow{\$} \{1, \dots, q_H\}$ .  $f = \gcd(\lambda)$ . It is  $O(n^2)$ . Let  $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ .