CryptoCommands Test

Roy Stracovsky

June 3, 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 $\mathsf{PKE.Enc}(\mathsf{pk}, \mathsf{msg})$. $\mathsf{ct} \xleftarrow{\$} \mathsf{PKE.Enc}(\mathsf{pk}, \mathsf{msg})$ and a bunch of random text to make the line longer and stuff.

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

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

We like random oracles O and also some linear algebra $\mathbf{As} + \mathbf{e}$. 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 $i \xleftarrow{\$} \{1, \ldots, q_H\}$. $f = \gcd(\lambda)$. It is $O(n^2)$. Let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$.

Here are some notes I have. Here are some other notes. Here are some final notes.