

malickc@oregonstate.edu

CS 427, Assignment 3

Cody Malick

February 2, 2017

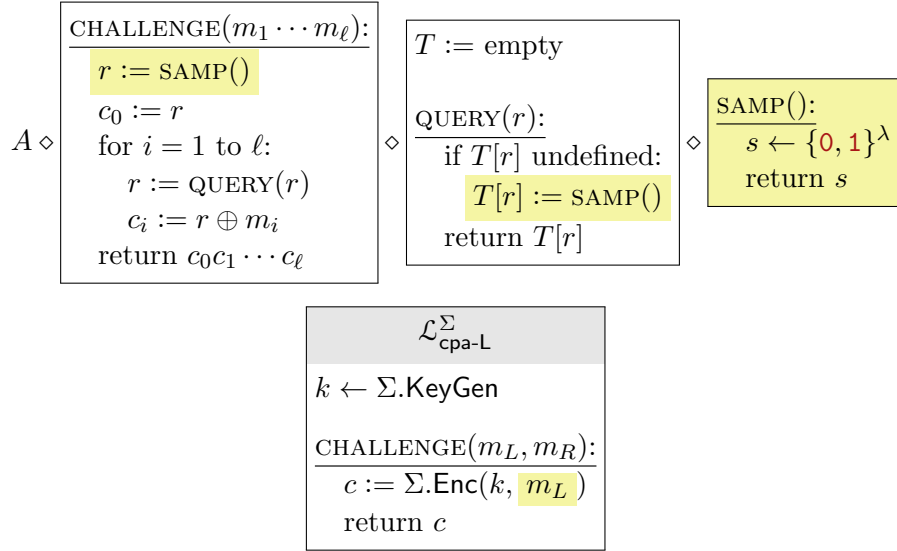
1

1.1

1.2

1.3

2



$$\mathcal{L}_{\text{left}} \equiv \mathcal{L}_{\text{right}} \Leftrightarrow \forall A : \Pr[A \diamond \mathcal{L}_{\text{left}} \text{ outputs } 1] = \Pr[A \diamond \mathcal{L}_{\text{right}} \text{ outputs } 1]$$

$$\mathcal{L}_{\text{left}} \approx \mathcal{L}_{\text{right}} \Leftrightarrow \forall \text{ poly-time } A : \Pr[A \diamond \mathcal{L}_{\text{left}} \text{ outputs } 1] \approx \Pr[A \diamond \mathcal{L}_{\text{right}} \text{ outputs } 1]$$

| | | |
|---|---|---|
| $\frac{\text{KeyGen:}}{k \leftarrow \{\mathbf{0}, \mathbf{1}\}^\lambda}$ $\text{return } k$ | $\frac{\text{Enc}(k, m):}{r \leftarrow \{\mathbf{0}, \mathbf{1}\}^\lambda}$ $x := F(k, r) \oplus m$ $\text{return } (r, x)$ | $\frac{\text{Dec}(k, (r, x)):}{m := F(k, r) \oplus x}$ $\text{return } m$ |
|---|---|---|

| |
|--|
| $\frac{H(s):}{x := G(s)}$ $y := G(x_{\text{right}})$ $\text{return } x_{\text{left}} \ y$ |
|--|