From PRG to PRF

Wednesday, September 8, 2021 3:57 PM

From PRG to PRF

Defn: A collection of functions

$$\{f_\lambda\} : \{K_\lambda\} \times \{D_\lambda\} \to \{C_\lambda\}$$

is PRF if:

Real

E_1: $k \xleftarrow{\$} K$

Query(x):

return $f(k,x)$

Rand

E_2 Dict := $\emptyset$

Query(x):

if x hasn't been queried,

$y \xleftarrow{\$} C$,

store (x,y) in dict

return y s.t. $(x,y) \in$ Dict

adv. can choose

$RF_{D,C}$ = set of all functions $\{g : D \to C\}$

E_2' $g \xleftarrow{\$} RF_{D,C}$

Query(x):

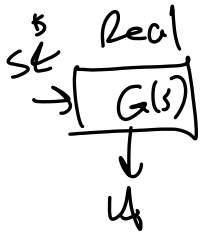
return $g(x)$

Q: $|RF_{D,C}|$ in terms of $|D|, |C|$?

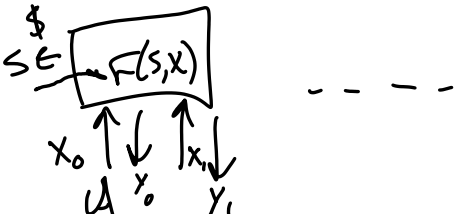
$|C|^{|D|}$? $|D|^{|C|}$?

Illustrate PRG vs PRF

PRG

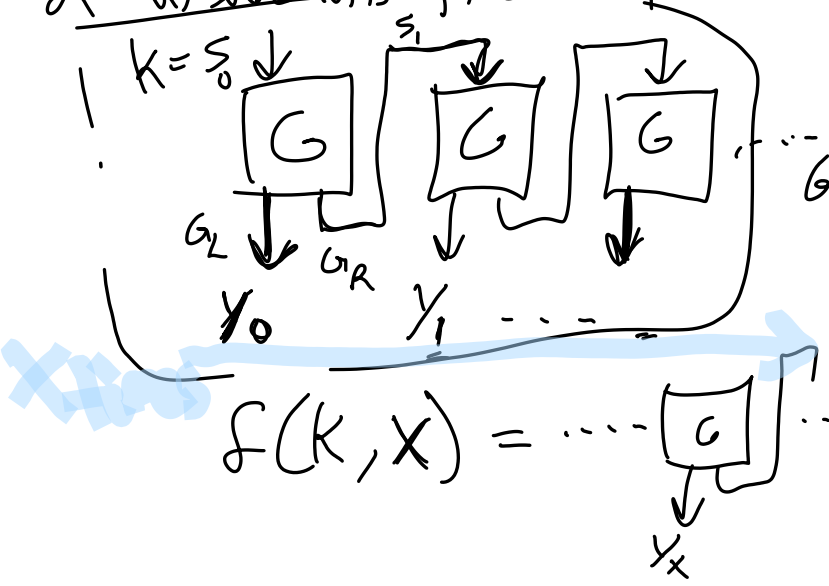


PRF



2 Constructions PRG => PRF

for length-Doubling PRGs



$G_L(s) \| G_R(s) = G(s)$

$= G_L(G_R \cdots (G_R(k)) \cdots)$

$= G_L(G_R^x(k))$

Tree Construct