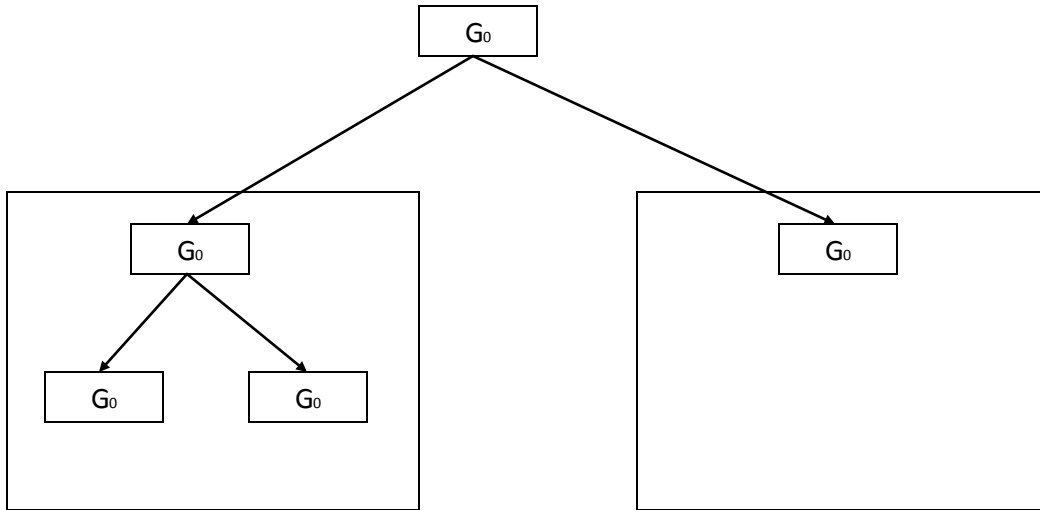


## NETWORK SECURITY, Class 5 notes

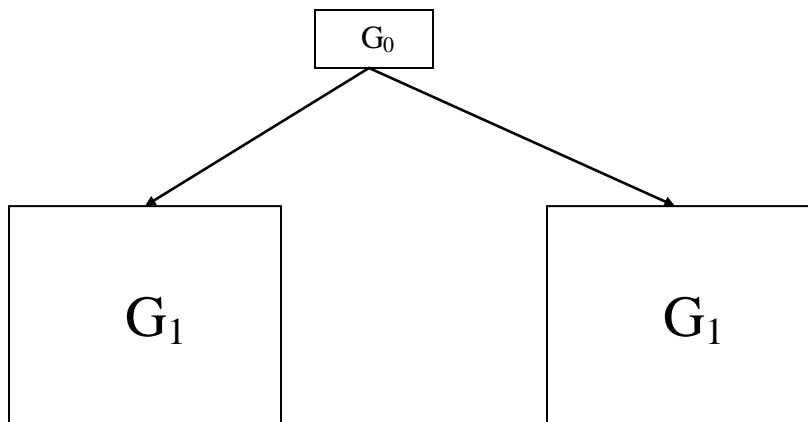
### The Goldreich-Goldwasser-Micali Pseudo Random Generator:



Suppose  $G_0: \{0, 1\} \longrightarrow \{0, 1\}^{2l}$  is a  $t, \epsilon$ -secure PRG. Then, we define:

$$G_i(X) = G_{i-1}(\text{left}(G_0(X))) \parallel G_{i-1}(\text{right}(G_0(X)))$$

Suppose  $G_i$  is  $t', \epsilon'$ -secure:



$$G_0 \circ u_1 \sim u_{2l}.$$

By DPI,

$$f(G_0 \circ u_1) \sim f(u_{21}) = G_1 \circ u_1 \parallel G_1 \circ u_1 \sim u_2^{i+2} \circ u_1$$

**THEOREM:**

Suppose  $G_0: \{0, 1\} \longrightarrow \{0, 1\}^{2^i}$  is a  $(t, \epsilon)$  secure PRG. Then,

$$G_i(X) = G_{i-1}(\text{left}(G_0(X))) \parallel G_{i-1}(\text{right}(G_0(X)))$$

Proof:

Base case :  $G_0 \circ u_1 \sim u_{21}$

Inductive step: Suppose  $G_i \circ u_1 \sim u_2^{i+1} \circ u_1$ , then by arguments on board,

$$G_{i+1} \circ u_1 \sim u_2^{i+2} \circ u_1$$

**Definition:**

Functions(X, Y) = {f: X  $\longrightarrow$  Y}

Let R be a random function from X to Y.

$$R \longleftarrow \text{Funcs}(\{0,1\}^{128}, \{0,1\}^{1024})$$

**Definition:**

F: Keys \* X  $\longrightarrow$  Y is  $(t, q, \epsilon)$  secure Pseudo Random function if for all A running in time  $\leq t$  and making at most q oracle queries,

$$\text{Adv}_A = |\Pr[A^{F_k} = 1 \mid K \longleftarrow u_{\text{keys}}] - \Pr[A^R = 1 \mid R \longleftarrow \text{Funcs}(X, Y)]| \leq \epsilon$$

where,  $A^{F_k}$ : A is given oracle access to  $F_k$ .