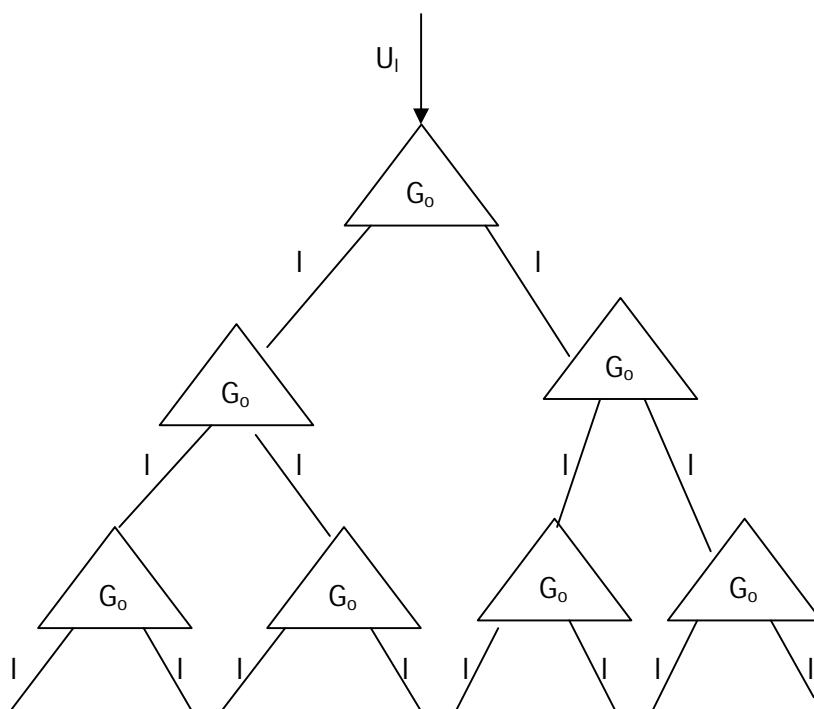


Topics Covered

- Principle of GGM Pseudo Random generator
- Proof – that GGM is a secure Pseudo Random Generator
- Problem that lead to the use of Pseudo Random Functions
- Pseudo Random Functions



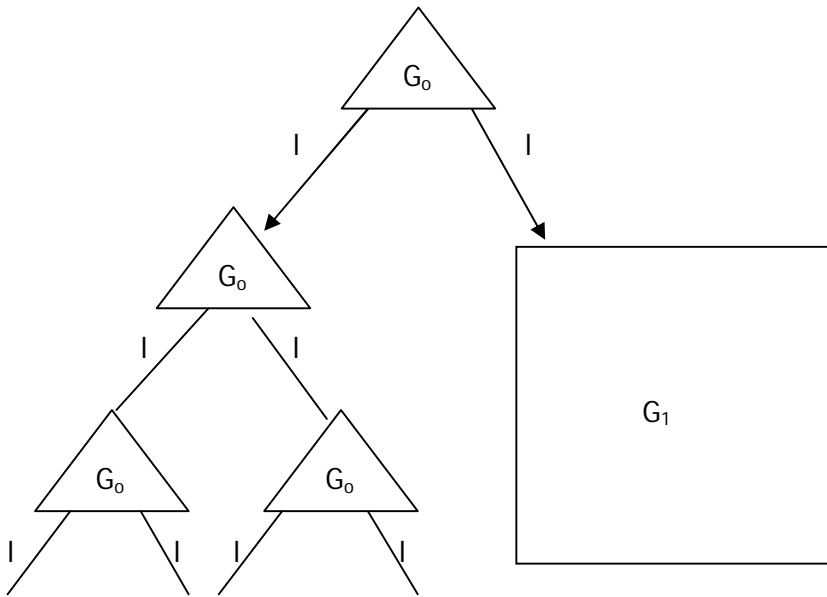
GGM Pseudo random generator

Suppose $G_0: \{0,1\}^l \rightarrow \{0,1\}^{2l}$ is a t, ϵ secure Pseudo random generator.

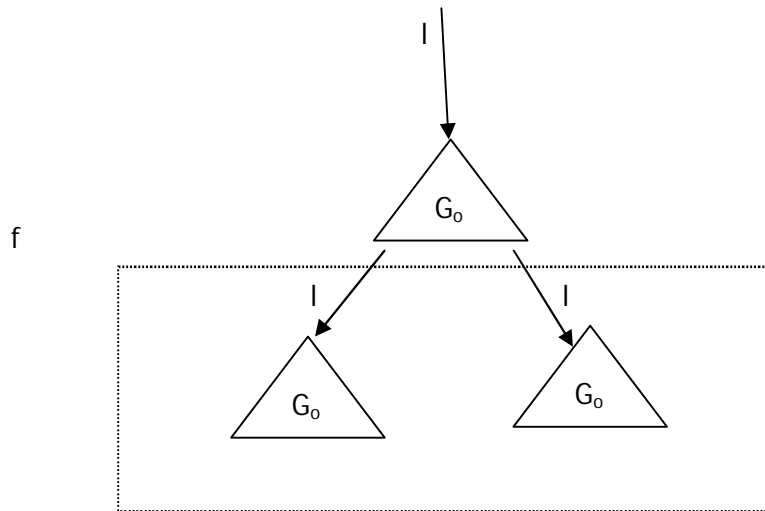
Then define

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

Note - Please see the figure in the next page

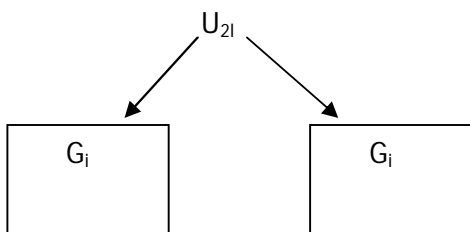


Suppose G_1 is t', ϵ' secure PRG



By Data Processing Inequality

The above is equivalent to



$$G_0 \circ U_1 \sim U_{2^1}$$

$$F(G_0 \circ U_1) \sim F(U_{2^1})$$

$$G_i \circ U_1 \sim U_{2^{i+1}} \quad (\text{By Inductive Hypothesis})$$

$$G_i \circ U_1 \parallel G_i \circ U_1 \sim U_{2^{i+1}} \parallel U_{2^{i+1}} \quad (\text{By Concatenation Theorem}).$$

$$= U_{2^{i+2}}$$

Proof

$$\text{Base case : } G_0 \circ U_1 \sim U_{2^1}$$

$$\text{Inductive step: Suppose } G_i \circ U_1 \sim U_{2^{i+1}}$$

Then by arguments on board

$$G_{i+1} \circ U_1 \sim U_{2^{i+2}}$$

Problem that lead use of Pseudo Random Functions

The criteria for security that the adversary should not be able to distinguish between elements drawn from truly random source and Pseudo Random Generator is not good enough for Encryption schemes because unlike the above scenario, we know many outputs of generator, that is, $G(x_0) G(x_1) G(x_2) \dots$ in encryption schemes involving RC4

PSEUDORANDOM FUNCTIONS

Definition.

$$\text{Functions}(x,y) = \{f: x \rightarrow y\}$$

Definition

$$R \leftarrow \text{Funcs}(X,Y)$$

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

Definition

Keys $X \rightarrow Y$ is (t, q, ϵ) secure Pseudo Random function if for every A running in time $\leq t$ and making at most q oracle queries.

$$ADV_A = |\Pr[A^{F_k} = 1 \mid K \leftarrow U_{\text{keys}}] - \Pr[A^R = 1 \mid R \leftarrow \text{Func}(X, Y)]| \leq \epsilon$$

Random Function

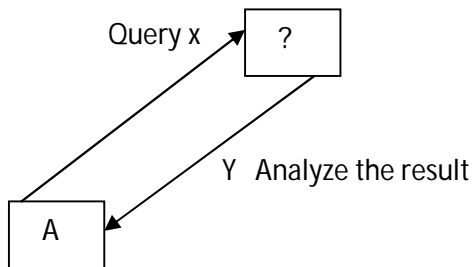
IN	OUT
1234	Some thing
2345	Something
...	...

- There are 2^{128} possible inputs, Hence there are 2^{128} rows in table representing a RANDOM FUNCTION and there are 2^{1024} choices in the output.
- Total No. of Possible Functions (2^{1024})

Notation used

- $F_k(x) = F(k, x)$

$A^{F_k} \rightarrow A$ is given oracle access to F_k



"This is F" or "This is a random function"

