A <u>function family</u> is a map $F: K \times D \to R$. Here K is the set of keys of F and D is the domain of F and R is the range of F. For any key $k \in K$ we define the map $F_k: D \to R$ by $F_k(X) = F(k, X)$. We call the function F_k an instance of function family F. Usually $K = \{0,1\}^k$ for some integer k, the <u>key length</u>, $D = \{0,1\}^l$ for some integer l called the <u>input length</u>, and $R = \{0,1\}^L$ for some integer L called the output length. There is some probability distribution on the set of keys K. Usually we assume uniform probability distribution U_K on K.

A map $\pi: D \to D$ is a permutation if for every $y \in D$ there is exactly one $x \in D$ such that $\pi(x) = y$. We say that F is a family of permutations if $Dom(F) = Range(F)$ and each F_k is a permutation on this common set.

<u>Example 1</u>: A block cipher is a family of permutations. In particular DES is a family of permutations $DES: K \times D \to R$ with $K = \{0,1\}^{56}$, $D = \{0,1\}^{64}$, $R = \{0,1\}^{64}$. Similarly AES is a family of permutations $AES: K \times D \to R$ with $K = \{0,1\}^{128}$, $D = \{0,1\}^{128}$, $R = \{0,1\}^{128}$.

<u>Random Functions and Permutations</u>: Let $D, R \subseteq \{0,1\}^*$ be finite non-empty sets and let $l, L \geq 1$ be integers. $Func(D,R)$ is the family of all functions of D to R. $Perm(D)$ is the family of all permutations on D. We let $Func(l, L)$, $Func(l)$, and $Perm(l)$ denote

Func(D, R), Func(D, D), and Perm(D), respectively, where $D = \{0,1\}^l$ and $R = \{0,1\}^L$. A randomly chosen instance of Func(D, R) will be a random function from D to R, and a randomly chosen instance of Perm(D) will be a random permutation on D.

Random Functions: The set of instances of Func(D, R) is the set of all functions mapping D to R. The key describing any particular instance function is simply a description of this instance function in some canonical notation. For example, order the domain D lexicographically as $X_1, X_2, \ldots$, and then let the key for a function f be the list of values $(f(X_1), f(X_2), \ldots)$. The key-space of Func(D, R) is simply the set of all these keys, under the uniform distribution.

Consider Func(l, L). The key for a function in this family is simply a list of all the output values of the function as its input ranges over $\{0,1\}^l$.

$\text{Keys}(\text{Func}(l,L)) = \{(Y_1, \ldots, Y_{2^l}) : Y_1, \ldots, Y_{2^l} \in \{0,1\}^L\}$ is the set of all sequences of length 2^l in which each entry of a sequence is an L-bit string. For any $X \in \{0,1\}^l$ we interpret X as an integer in the range $\{1, \ldots, 2^l\}$ and set $\text{Func}(l,L)((Y_1, \ldots, Y_{2^l}), X) = Y_X$.

Example 2: Consider $f \in \text{Func}(3,2)$ defined by:

x	000	001	010	011	100	101	110	111
$f(x)$	10	11	01	11	10	00	00	10

The key corresponding to f is:

$$(10, 11, 01, 11, 10, 00, 00, 10).$$

Example 3: Consider Func (l, L).

① Fix $X \in \{0,1\}^l$ and $Y \in \{0,1\}^L$. Then
$\Pr[f(X) = Y] = 2^{-L}$.

② Fix $X_1, X_2 \in \{0,1\}^l$ and $Y_1, Y_2 \in \{0,1\}^L$, and assume $X_1 \neq X_2$. Then $\Pr[f(X_1) = Y_1 \mid f(X_2) = Y_2] = 2^{-L}$.

③ Fix $X_1, X_2 \in \{0,1\}^l$ and $Y \in \{0,1\}^L$. Then

$$\Pr[f(X_1) = Y \text{ and } f(X_2) = Y] = \begin{cases} 2^{-2L} & \text{if } X_1 \neq X_2 \\ 2^{-L} & \text{if } X_1 = X_2 \end{cases}$$

④ Fix $X_1, X_2 \in \{0,1\}^l$ and $Y \in \{0,1\}^L$. Then

$$\Pr[f(X_1) \oplus f(X_2) = Y] = \begin{cases} 2^{-L} & \text{if } X_1 \neq X_2 \\ 0 & \text{if } X_1 = X_2 \text{ and } Y \neq 0^L \\ 1 & \text{if } X_1 = X_2 \text{ and } Y = 0^L \end{cases}$$

⑤ Suppose $l \leq L$ and let $\tau : \{0,1\}^L \to \{0,1\}^l$ denote the function that on input $Y \in \{0,1\}^L$, returns the first l bits of Y. Fix distinct $X_1, X_2 \in \{0,1\}^l$, $Y_1 \in \{0,1\}^L$, and $Z_2 \in \{0,1\}^l$. Then

$$\Pr[\tau(f(X_2)) = Z_2 \mid f(X_1) = Y_1] = 2^{-l}$$

Random Permutations: The set of instances of Perm (D) is the set of all permutations on D. The key describing a particular instance is some description of the function. Consider Perm (l). We have

$$\text{Keys}(\text{Perm}(l)) = \{(Y_1, \ldots, Y_{2^l}) : Y_1, \ldots, Y_{2^l} \in \{0,1\}^l \text{ and } Y_1, \ldots, Y_{2^l} \text{ are all distinct}\}.$$

For any $X \in \{0,1\}^\ell$ we interpret X as an integer in the range $\{1, \dots, 2^\ell\}$ and set $\mathrm{Perm}(\ell)((Y_1, \dots, Y_{2^\ell}), x) = Y_x$.

Example 4: An example of $\pi \in \mathrm{Perm}(3)$ is:

x	000	001	010	011	100	101	110	111
$\pi(x)$	010	111	101	011	110	100	000	001

The key corresponding to π is:

(010, 111, 101, 011, 110, 100, 000, 001).

Example 5: Consider $\mathrm{Perm}(\ell)$.

① Fix $X, Y \in \{0,1\}^\ell$. Then $\Pr[\pi(X) = Y] = 2^{-\ell}$.

② Fix $X_1, X_2 \in \{0,1\}^\ell$ and $Y_1, Y_2 \in \{0,1\}^2$, and assume $X_1 \neq X_2$. Then

$$\Pr[\pi(X_1) = Y_1 \mid \pi(X_2) = Y_2] = \begin{cases} \frac{1}{2^\ell - 1} & \text{if } Y_1 \neq Y_2 \\ 0 & \text{if } Y_1 = Y_2 \end{cases}$$

③ Fix $X_1, X_2 \in \{0,1\}^\ell$ and $Y \in \{0,1\}^\ell$. Then

$$\Pr[\pi(X_1) = Y \text{ and } \pi(X_2) = Y] = \begin{cases} 0 & \text{if } X_1 \neq X_2 \\ 2^{-\ell} & \text{if } X_1 = X_2 \end{cases}$$

④ Fix $X_1, X_2 \in \{0,1\}^\ell$ and $Y \in \{0,1\}^\ell$. Then

$$\Pr[\pi(X_1) \oplus \pi(X_2) = Y] = \begin{cases} \frac{1}{2^\ell - 1} & \text{if } X_1 \neq X_2 \text{ and } Y \neq 0^\ell \\ 0 & \text{if } X_1 \neq X_2 \text{ and } Y = 0^\ell \\ 0 & \text{if } X_1 = X_2 \text{ and } Y \neq 0^\ell \\ 1 & \text{if } X_1 = X_2 \text{ and } Y = 0^\ell \end{cases}$$

In the case $X_1 \neq X_2$ and $Y \neq 0^l$ the probability is computed as follows:

$Pr[\pi(X_1) \oplus \pi(X_2) = Y]$

$$= \sum_{Y_1} Pr[\pi(X_2) = Y_1 \oplus Y \mid \pi(X_1) = Y_1] \cdot Pr[\pi(X_1) = Y_1]$$

$$= \sum_{Y_1} \frac{1}{2^l - 1} \cdot \frac{1}{2^l} = 2^l \cdot \frac{1}{2^l - 1} \cdot \frac{1}{2^l} = \frac{1}{2^l - 1}.$$

(5) Suppose $l \leq L$ and let $\tau : \{0,1\}^L \to \{0,1\}^l$ denote the function that on input $Y \in \{0,1\}^l$ returns the first l bits of Y. Fix distinct $X_1, X_2 \in \{0,1\}^l$, $Y_1 \in \{0,1\}^L$ and $Z_2 \in \{0,1\}^l$. Then

$$Pr[\tau(\pi(X_2)) = Z_2 \mid \pi(X_1) = Y_1] = \begin{cases} \dfrac{2^{L-l}}{2^L - 1} & \text{if } Z_2 \neq Y_1[1 \cdots l] \\[2ex] \dfrac{2^{L-l} - 1}{2^L - 1} & \text{if } Z_2 = Y_1[1 \cdots l] \end{cases}$$

We compute the probability as follows:

Let $S = \{ Y_2 \in \{0,1\}^L : Y_2[1 \cdots l] = Z_2 \text{ and } Y_2 \neq Y_1 \}$.

We note that $|S| = 2^{L-l}$ if $Y_1[1 \cdots l] \neq Z_2$ and $|S| = 2^{L-l} - 1$ if $Y_1[1 \cdots l] = Z_2$. Then

$$Pr[\tau(\pi(X_2)) = Z_2 \mid \pi(X_1) = Y_1] = \sum_{Y_2 \in S} Pr[\pi(X_2) = Y_2 \mid \pi(X_1) = Y_1]$$

$$= \frac{|S|}{2^L - 1} = \begin{cases} \dfrac{2^{L-l}}{2^L - 1} & \text{if } Z_2 \neq Y_1[1 \cdots l] \\[2ex] \dfrac{2^{L-l} - 1}{2^L - 1} & \text{if } Z_2 = Y_1[1 \cdots l] \end{cases}$$