Shannon’s Idea of Confusion and Diffusion

The DES, AES and many block ciphers are designed using Shannon’s idea of confusion and diffusion. The objectives of this document is to introduce

- linear and nonlinear functions; and

- Shannon’s confusion and diffusion.

Linear Functions

Notation: Let $\mathbf{F}_2$ denote the set $\{0, 1\}$ and let

$$\mathbf{F}_2^n = \{(x_1, x_2, \cdots, x_n) | x_i \in \mathbf{F}_2\}.$$

Here $\mathbf{F}_2^n$ is associated with the bitwise exclusive-or operation, denoted $+$.

Linear functions: Let f be a function from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$, where n and m are integers. f is called **linear** if

$$f(x + y) = f(x) + f(y)$$

for all $x, y \in \mathbf{F}_2^n$.

Example: Let $f(x) = x_1 + x_2 + \cdots + x_n$, where

$$x = (x_1, \cdots, x_n) \in \mathbf{F}_2^n.$$

Then f is a linear function from $\mathbf{F}_2^n$ to $\mathbf{F}_2$. Note that $+$ denotes the modulo-2 addition.

Examples of Linear Functions

Linear permutations: Let P be a permutation of the set $\{1, \cdots, n\}$. Define a function L_P from $\mathbf{F}_2^n$ to itself by

$$L_P((x_1, x_2, \cdots, x_n)) = (x_{P(1)}, x_{P(2)}, \cdots, x_{P(n)})$$

for any $x = (x_1, x_2, \cdots, x_n) \in \mathbf{F}_n$.

Lemma: L_P is linear with respect to the bitwise exclusive-or.

Conclusion: Such a linear function is used in both DES and AES.

Examples of Linear Functions

Linear function by circular shift: Let i be any positive integer. Define a function LS_i from $\mathbf{F}_2^n$ to $\mathbf{F}_2^n$ by

$$\begin{aligned} & LS_i((x_0, x_1, \cdots, x_{n-1})) \\ = \; & (x_{(0-i) \bmod n}, x_{(1-i) \bmod n}, \cdots, x_{(n-1-i) \bmod n}) \end{aligned}$$

for any $x = (x_0, x_1, \cdots, x_{n-1}) \in \mathbf{F}_n$.

Conclusion: LS_i is linear with respect to the bitwise exclusive-or.

$\boxed{\text{Nonlinear Functions}}$

Definition Let f be a function from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$, where n and m are positive integers. f is called **nonlinear** if

$$f(x+y) \neq f(x) + f(y)$$

for at least one pair of $x, y \in \mathbf{F}_2^n$.

Example: Let $f(x) = x_1x_2 + x_2 + \cdots + x_n$, where

$$x = (x_1, \cdots, x_n) \in \mathbf{F}_2^n.$$

Note that $+$ denotes the modulo-2 addition.

Nonlinearity of S-Boxes

The S-box in AES: A function from GF(2^8) to GF(2^8) defined by

$$S(x) = x^{2^8-2}$$

The nonlinearity is measured by

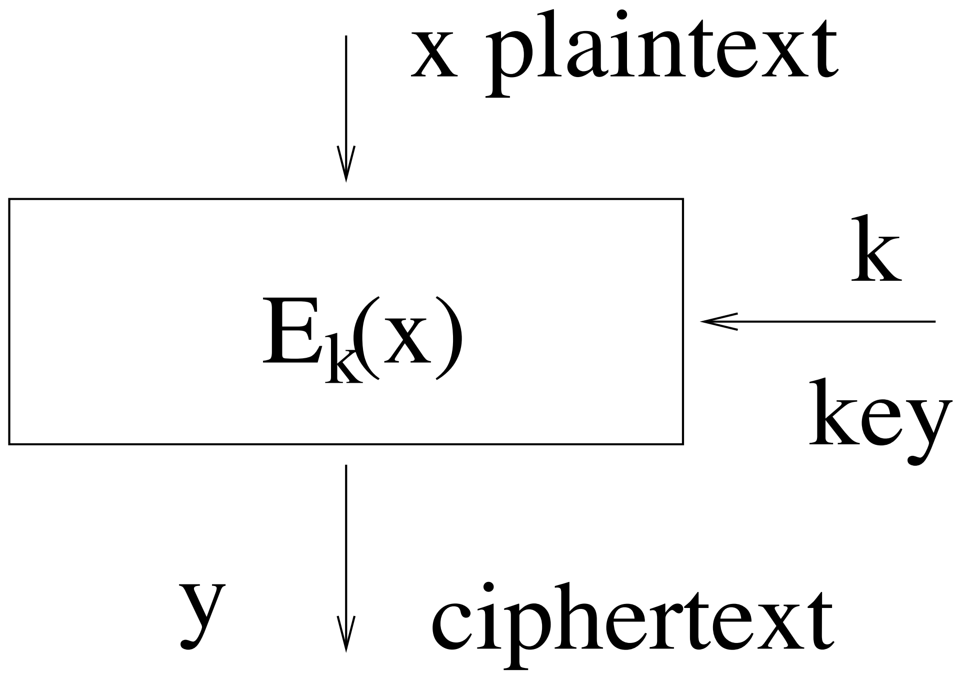
$$P_S = \max_{\substack{0 \neq a \in GF(2^8), \\ b \in GF(2^8)}} |\{x \in GF(2^8) : S(x+a) - S(x) = b\}|$$

Comment: The smaller the P_S, the higher the nonlinearity of S.

Remark: S is highly nonlinear.

Diffusion Requirement

Diffusion: Each plaintext block bit or key bit affects many bits of the ciphertext block.



Remark: Linear functions are responsible for confusion.

Diffusion Requirement

Diffusion: Each plaintext block bit or key bit affects many bits of the ciphertext block.

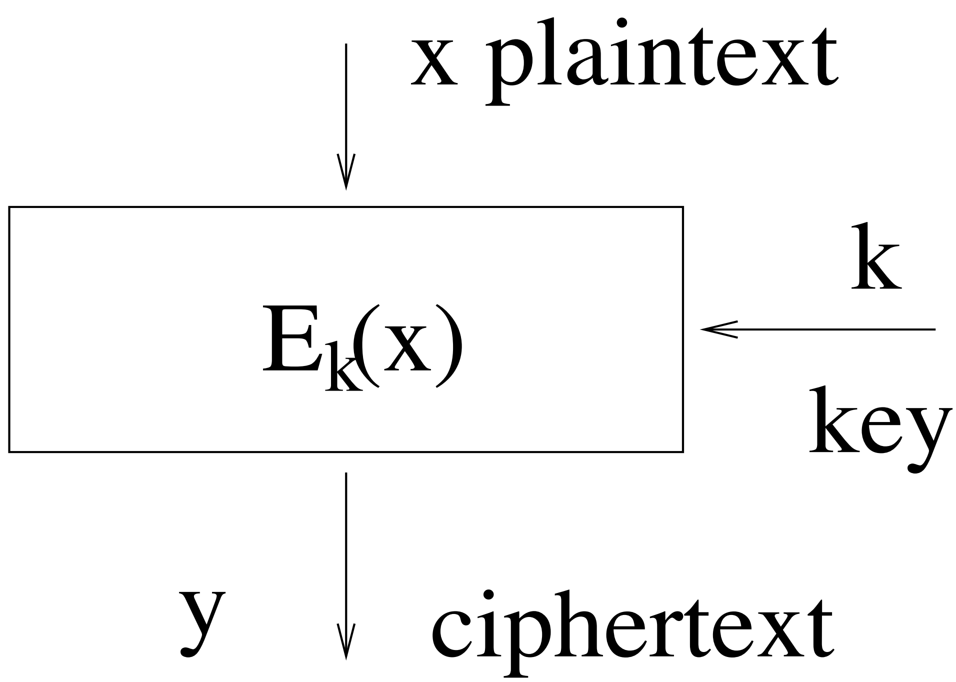
Example: Suppose that x, y and k all have 8 bits. If

$$
\begin{aligned}
y_1 &= x_1 + x_2 + x_3 + x_4 + k_1 + k_2 + k_3 + k_4 \\
y_2 &= x_2 + x_3 + x_4 + x_5 + k_2 + k_3 + k_4 + k_5 \\
y_3 &= x_3 + x_4 + x_5 + x_6 + k_3 + k_4 + k_5 + k_6 \\
y_4 &= x_4 + x_5 + x_6 + x_7 + k_4 + k_5 + k_6 + k_7 \\
y_5 &= x_5 + x_6 + x_7 + x_8 + k_5 + k_6 + k_7 + k_8 \\
y_6 &= x_6 + x_7 + x_8 + x_1 + k_6 + k_7 + k_8 + k_1 \\
y_7 &= x_7 + x_8 + x_1 + x_2 + k_7 + k_8 + k_1 + k_2 \\
y_8 &= x_8 + x_1 + x_2 + x_3 + k_8 + k_1 + k_2 + k_3
\end{aligned}
$$

then it has very **good** diffusion, because each plaintext bit or key bit affects half of the bits in the output block y.

Confusion Requirement

Confusion: Each bit of the ciphertext block has highly nonlinear relations with the plaintext block bits and the key bits.



Remark: Nonlinear functions are responsible for confusion.

Confusion Requirement

Confusion: Each bit of the ciphertext block has highly nonlinear relations with the plaintext block bits and the key bits.

Example: Suppose that x, y and k all have 8 bits. If

$$\begin{aligned}
y_1 &= x_1 + x_2 + x_3 + x_4 + k_1 + k_2 + k_3 + k_4 \\
y_2 &= x_2 + x_3 + x_4 + x_5 + k_2 + k_3 + k_4 + k_5 \\
y_3 &= x_3 + x_4 + x_5 + x_6 + k_3 + k_4 + k_5 + k_6 \\
y_4 &= x_4 + x_5 + x_6 + x_7 + k_4 + k_5 + k_6 + k_7 \\
y_5 &= x_5 + x_6 + x_7 + x_8 + k_5 + k_6 + k_7 + k_8 \\
y_6 &= x_6 + x_7 + x_8 + x_1 + k_6 + k_7 + k_8 + k_1 \\
y_7 &= x_7 + x_8 + x_1 + x_2 + k_7 + k_8 + k_1 + k_2 \\
y_8 &= x_8 + x_1 + x_2 + x_3 + k_8 + k_1 + k_2 + k_3
\end{aligned}$$

then it has **bad** confusion, as they are linear relations.

Shannon's Suggestion

The encryption and decryption functions of a cipher should have both good confusion and diffusion of the message block bits and secret key bits.