DES AND SDES

MATH 195

First, some notation: $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. In general, $\mathbb{F}_q$ denotes a finite field with q elements: So $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if p is prime; in general, q needs to be of the form $q = p^n$, with p prime and $n \geq 1$. Note: $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$.

In SDES and DES, we have $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^{2k=8 \text{ or } 64}$, $k = 4$ or 32, $\mathcal{K} = \mathbb{F}_2^{10 \text{ or } 56}$, $\mathcal{S} = \mathbb{F}_2^{8 \text{ or } 48}$ (the *subkey space*), $t = 2$ or 16 (the number of rounds). In order to define

$$\begin{aligned} E : \mathcal{P} \times \mathcal{K} &\to \mathcal{P} \\ (z, K) &\mapsto E_K(z) \end{aligned}$$

and similarly D_K, we need three ingredients:

- A map $\mathcal{K} \to \mathcal{S}^t = \underbrace{\mathcal{S} \times \cdots \times \mathcal{S}}_{t}$, $K \mapsto (K_1, \dots, K_t)$;
- A *round function* $F : \mathbb{F}_2^k \times \mathcal{S} \to \mathbb{F}_2^k$;
- An initial permutation ι (of $\mathcal{P}$).

Given these three ingredients, E and D are defined as follows:

$$E_K(z) = (\iota^{-1} \circ G_t \circ s \circ \cdots \circ s \circ G_2 \circ s \circ G_1 \circ \iota)(z),$$

where $s(x, y) = (y, x)$ and $G_i(x, y) = (x + F(y, K_i), y)$ and therefore

$$D_K(z) = (\iota^{-1} \circ G_1 \circ s \circ \cdots \circ s \circ G_{t-1} \circ s \circ G_t \circ \iota)(z).$$

The initial permutation $\iota : \mathbb{F}_2^{2k} \to \mathbb{F}_2^{2k}$ permutes the $2k$ coordinates according to the following formula [see p. 53 in the text]: in SDES: $\iota(z_1, \dots, z_8) = \iota(z_2, z_6, z_3, z_1, z_4, z_8, z_5, z_7)$, and in DES [see Table 3.2(a), p. 68],

$$\iota(z_1, \dots, z_{64}) = (z_{58}, z_{50}, \dots, z_{15}, z_7).$$

As a check, we include "parity bits" in our key. We let

$$\mathcal{K} = \{(k_1, \dots, k_{64}) \in \mathbb{F}_2^{64} : \sum_{i=8j+1}^{8(j+1)} k_i = 0,\ j = 0, 1, \dots, 7\}$$

i.e. $k_1 + k_2 + \cdots + k_8 = 0$, $k_9 + k_{10} + \cdots + k_{16} = 0$, $\dots$, $k_{57} + \cdots + k_{64} = 0$. We let the least significant bit in each byte be treated as extraneous information, so we have only 56 meaningful bits.

Now the subkey generation is a map $K \mapsto (K_1, \dots, K_t)$ (for DES) where $K \in \mathbb{F}_2^{64}$, $K_i \in \mathbb{F}_2^{48}$:

$$K_i = (\tau \circ \lambda^{n_i} \circ \sigma)(K) :$$

where [Table 3.4(a), p. 72]

$$\sigma(k_1, \dots, k_{56}, \dots, k_{64}) = (k_{57}, k_{49}, k_{41}, \dots, k_{12}, k_4)$$

This is some of the material covered February 19–21, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

(recall we write the 56 bits as 64 bits, using the bits $k_8, \dots, k_{64}$ as parity bits), [Table 3.4(b), p. 72]

$$\tau(k_1, \dots, k_{56}) = (k_{14}, k_{17}, \dots, k_{29}, k_{32}) \in \mathbb{F}_2^{48},$$

and

$$\lambda(k_1, \dots, k_{28}, k_{29}, \dots, k_{56}) = (k_2, k_3, \dots, k_{28}, k_1, k_{30}, k_{31}, \dots, k_{56}, k_{29})$$

and [Table 3.4(c), p. 72] $n_1 = 1, n_2 = 2, n_3 = 4, \dots, n_{16} = 28 = 0$.

The round function $F : \mathbb{F}_2^{32} \times \mathbb{F}_2^{48} \to \mathbb{F}_2^{32}$ is equally explicit. To compute $F(x, k)$, expand

$$x = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ & \vdots & & \\ x_{29} & x_{30} & x_{31} & x_{32} \end{pmatrix}$$

to

$$\epsilon(x) = \begin{pmatrix} x_{32} & x_1 & x_2 & x_3 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_7 & x_8 & x_9 \\ & \vdots & & & & \\ x_28 & x_{29} & x_{30} & x_{31} & x_{32} & x_1 \end{pmatrix};$$

write k also as an 8×6-matrix

$$k = \begin{pmatrix} k_1 & k_2 & \dots & k_6 \\ & & \vdots & \\ k_{43} & k_{44} & \dots & k_{48} \end{pmatrix}$$

and then add them:

$$k + \epsilon(x) = \begin{pmatrix} k_1 + x_{32} & \dots & x_5 + k_6 \\ & \vdots & \\ k_{43} + x_{28} & \dots & x_1 + k_{48} \end{pmatrix}.$$

Then apply the ith S-box S_i to the ith row of that matrix, $i = 1, \dots, 8$ [p. 71]. This compresses the bits on the basis of a table-lookup. Finally, follow it by the permutation of the 32 positions [Table 3.2(d), p. 68]. That results in an 8×4 matrix, which read as a vector gives $F(x, k) \in \mathbb{F}_2^{32}$.

For a word about design criteria—diffusion and confusion, resistance against differential cryptanalysis and linear cryptanalysis, ease of use and analysis—see the text [e.g. p. 60/61].