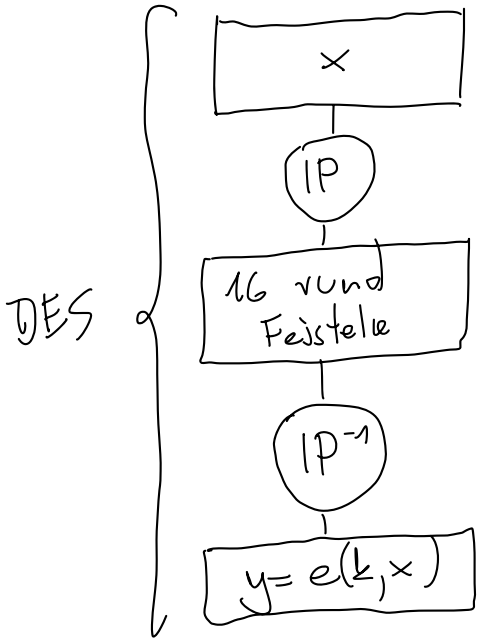
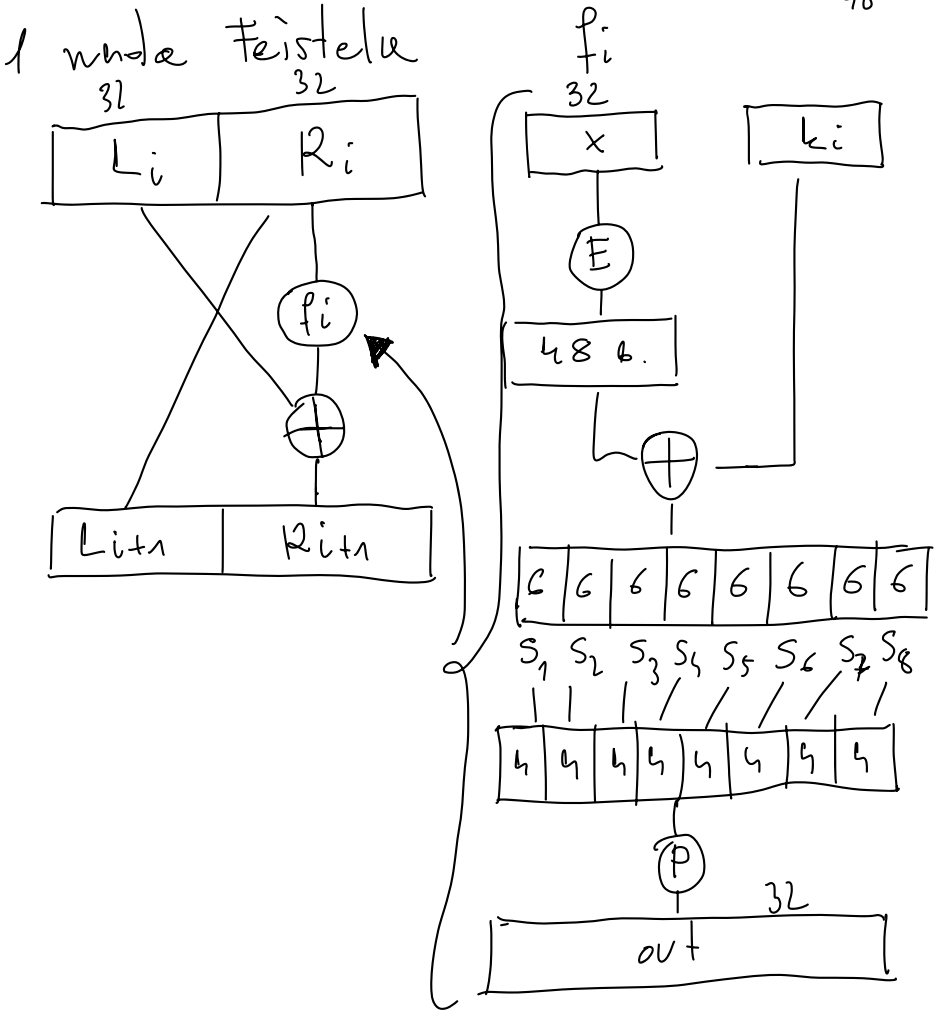
DES 16-rundowa sieć Feistela 64-bity $k \to k_1, \dots, k_{16}$ (56 → 48)





Kryptoanaliza DES

- Jak długi jest klucz? 56-bitów
- Brute-force 2^{56}

1977	1 dzień	\$20 mln.
1993	1,5 dnia	\$100 tys. Wiener
1998	2 dni	\$250 tys.
2006	1 dzień	\$10 tys. 120 FPGA

1989 Biham, Shamir — Kryptoanaliza różnicowa

2^{47} (chosen plaintext)

Zmiana w IBM w latach 70

1994 Matsui Kryptoanaliza liniowa

$2^{56} \rightsquigarrow 2^{43}$ (x, y)

40 dni → 10 dni

(x, y) k

3DES $e^{3DES} : \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{P} \to C$

$\mathcal{K}$: 56 56 56

$e^{3DES}(k_1, k_2, k_3, x) = e^D(k_1, d^D(k_2, e^D(k_3, x)))$

$e^{3DES}(k_1, k_1, k_1, x) = e^D(k_1, x)$

168 b. 2^{168}

Dlaczego nie 2DES?

$e^{2DES}(k_1, k_2, x) = e^D(k_1, e^D(k_2, x))$

56 56

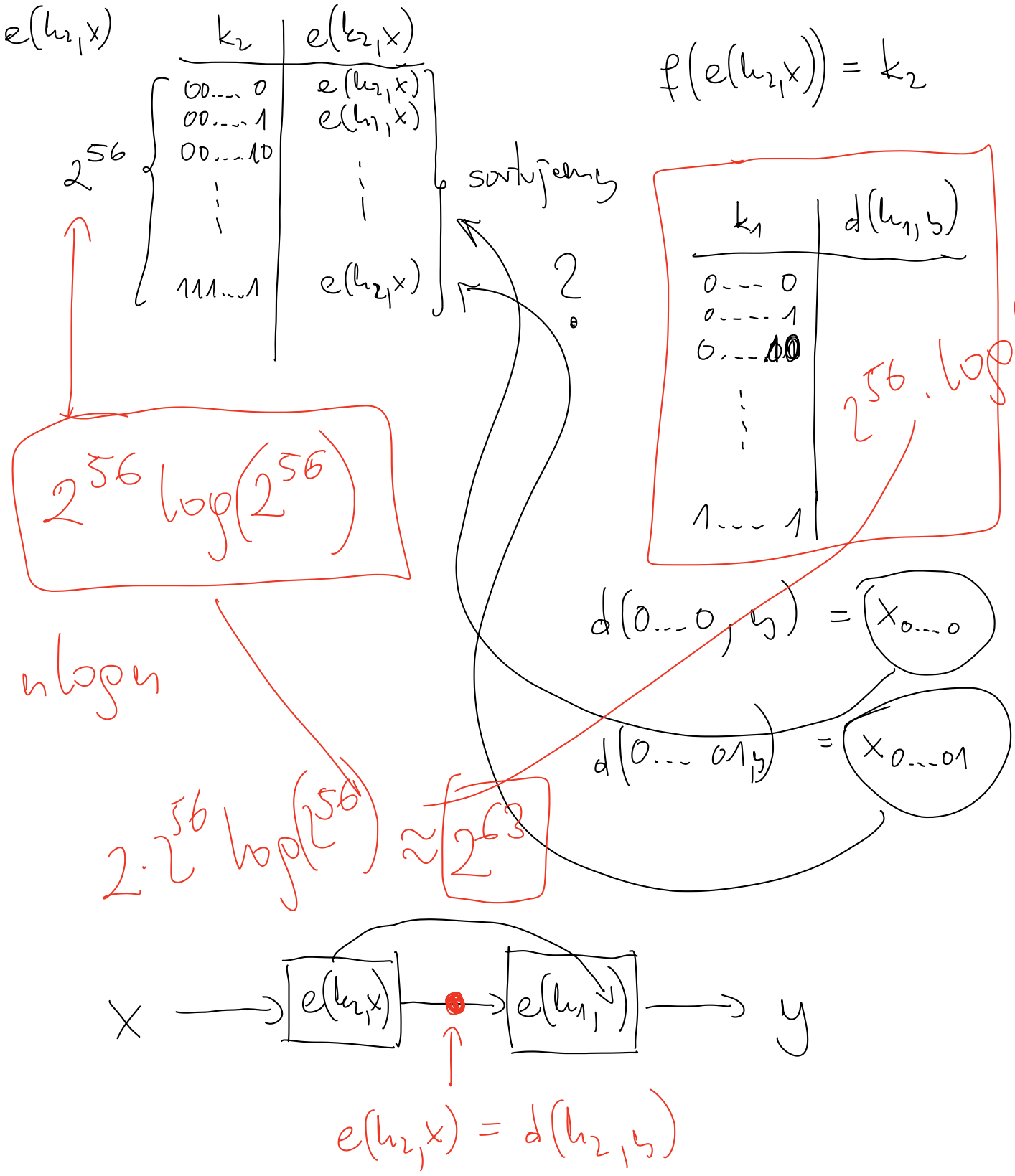
2^{112}

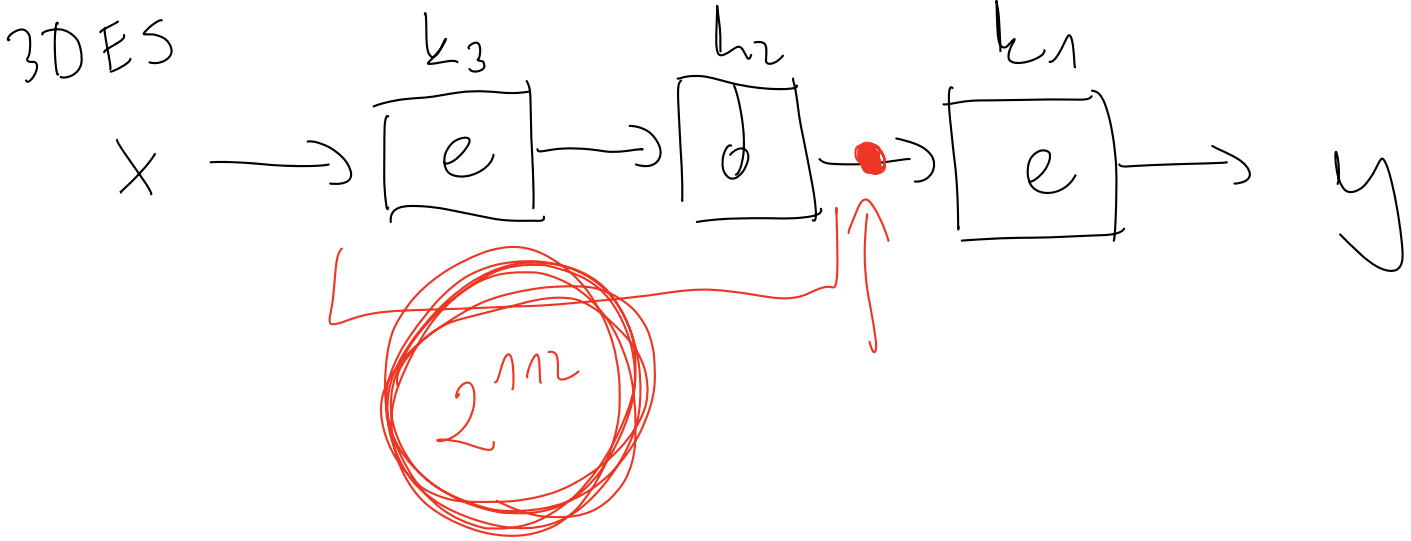
$x \to e(k_1, e(k_2, x)) = y$ $d(k_1, \cdot)$

$d(k_1, e(k_1, e(k_2, x))) = d(k_1, y)$

$e(k_2, x) = d(k_1, y)$

Meet-in-the-middle (time-memory trade-off)




3DES
k_3
k_2
k_1
X
e
d
e
y
2^{112}