

Kryptoanaliza DES

Wyk ad 14 marca 2005

Literatura uzupełniająca

- E. Biham, A. Shamir „Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag 1993.
- Materiały na stronie: <http://www.cs.technion.ac.il/~biham/>
- HAC (patrz informacje na stronie wykładu)

Potencjalne s abo ci algorytmu DES

Czy wzgl dnie krótki klucz (56 bitów) umo liwia przeszukanie przestrzeni kluczy?

- W latach siedemdziesi tych, oceniano, e specjalnie zbudowany, za cen kilkudziesi ciu milionów dolarów, komputer znajdzie klucz w ci gu jednego dnia (Diffie, Hellman).
- W 1990 oceniano, e przeszukanie 2^{55} kluczy zajmie 100 lat, przy u yciu jednego, zrobionego z GaAs procesora DES firmy DEC.
- W tym samym czasie Wiener proponuje zbudowanie za 1000 000 dolarów specjalnego komputera, który znajdzie klucz w nieca e 4 godziny.
- W czerwcu 1997 przy u yciu Internetu i 14 000 do 78 000 komputerów w sieci znaleziono klucz w 90 dni.
- W styczniu 1998 przy pomocy Internetu znaleziono klucz w 39 dni.
- W lipcu 1998 maszyna „deep crack” zbudowana za 210 000 dolarów znalaz a klucz w 56 godzin.

Znane s abo ci DES

- Niejawne kryteria projektowania algorytmu
- Istnienie czterech „s abych” kluczy K , takich e dla dowolnego X : $E(K, E(K, X)) = X$; czyli $E(K, \cdot) = D(K, \cdot)$.
- Istnienie dwunastu (sze ciu par) p ó -s abych kluczy κ_1, κ_2 , takich e dla dowolnego X : $E(\kappa_1, E(\kappa_2, X)) = X$; czyli: $E(\kappa_1, \cdot) = D(\kappa_2, \cdot)$.
- Komplementarno DES: je li $C = E(K, P)$, to $\underline{C} = E(\underline{K}, \underline{P})$, gdzie operacja $(\underline{\cdot})$ oznacza odwrócenie bitów. Na przyk ad: $(\underline{0,1,1,1,0,0,1,0}) = (1,0,0,0,1,1,0,1)$.

Komplementarno DES

Ta w a ciwo DES umo liwia atak dwukrotnie szybszy ni pe ne przeszukanie przestrzeni kluczy:

3. Wybierz tekst jawny P i komplementarny do niego tekst \underline{P}

4. Uzyskaj zaszyfrowane tajnym kluczem K dwa szyfrogramy:
 $C_0 = E(K, P)$, $C_1 = E(K, \underline{P})$.

5. Sprawdź dla wszystkich 2^{55} kluczy κ , których najbardziej znaczący bit jest zerem, czy $E(\kappa, P) \in \{C_0, \underline{C_1}\}$.

6. Je li $E(\kappa, P) = C_0$, to prawdopodobnie $K = \kappa$.

7. Je li $E(\kappa, P) = \underline{C_1}$, to prawdopodobnie $K = \underline{\kappa}$.

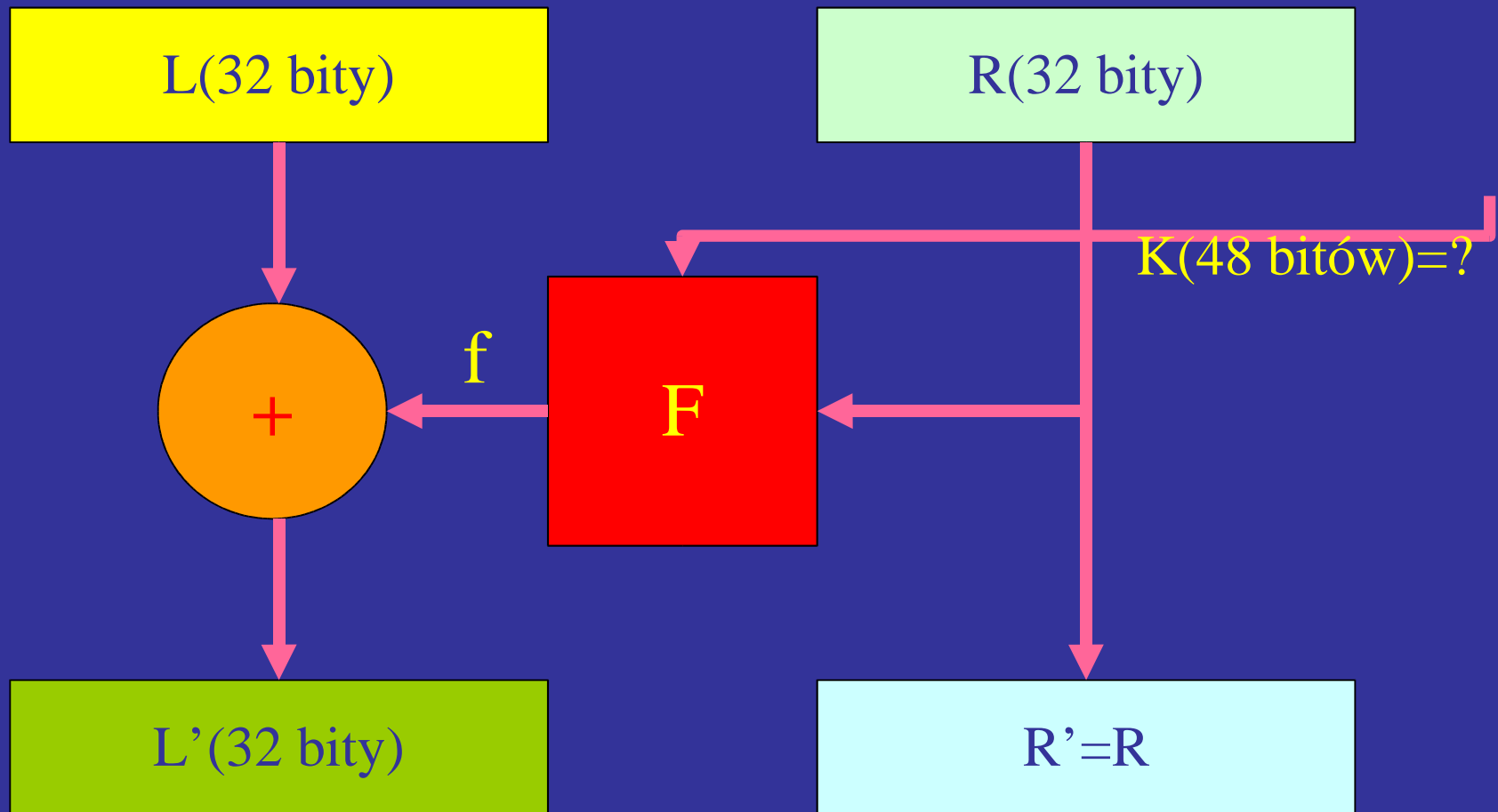
8. Je li nie zachodzi (5) lub (6), to ani κ , ani $\underline{\kappa}$ nie jest K .

Poniewa porównywanie na komputerze jest znacznie szybsz operacj ni szyfrowanie, ten atak jest dwukrotnie szybszy ni przeszukiwanie ca ej przestrzeni kluczy.

Atak na DES (1 runda) ze znanym tekstem jawnym:

Znamy P (LR) i $DES_1(K,P) = (L'R')$; szukamy K .

Po usunięciu IP i IP^{-1} , które pomijamy pozostaje:



Przykład, atak na 1 rundę DES, Tablica P^{-1}

$L \oplus f = L'$, a więc:

$L \oplus L' = f$

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2

Niech f : xxxxxxxx1 xxxxxxxx1 xxxxxx1 xxxxxxxx1x

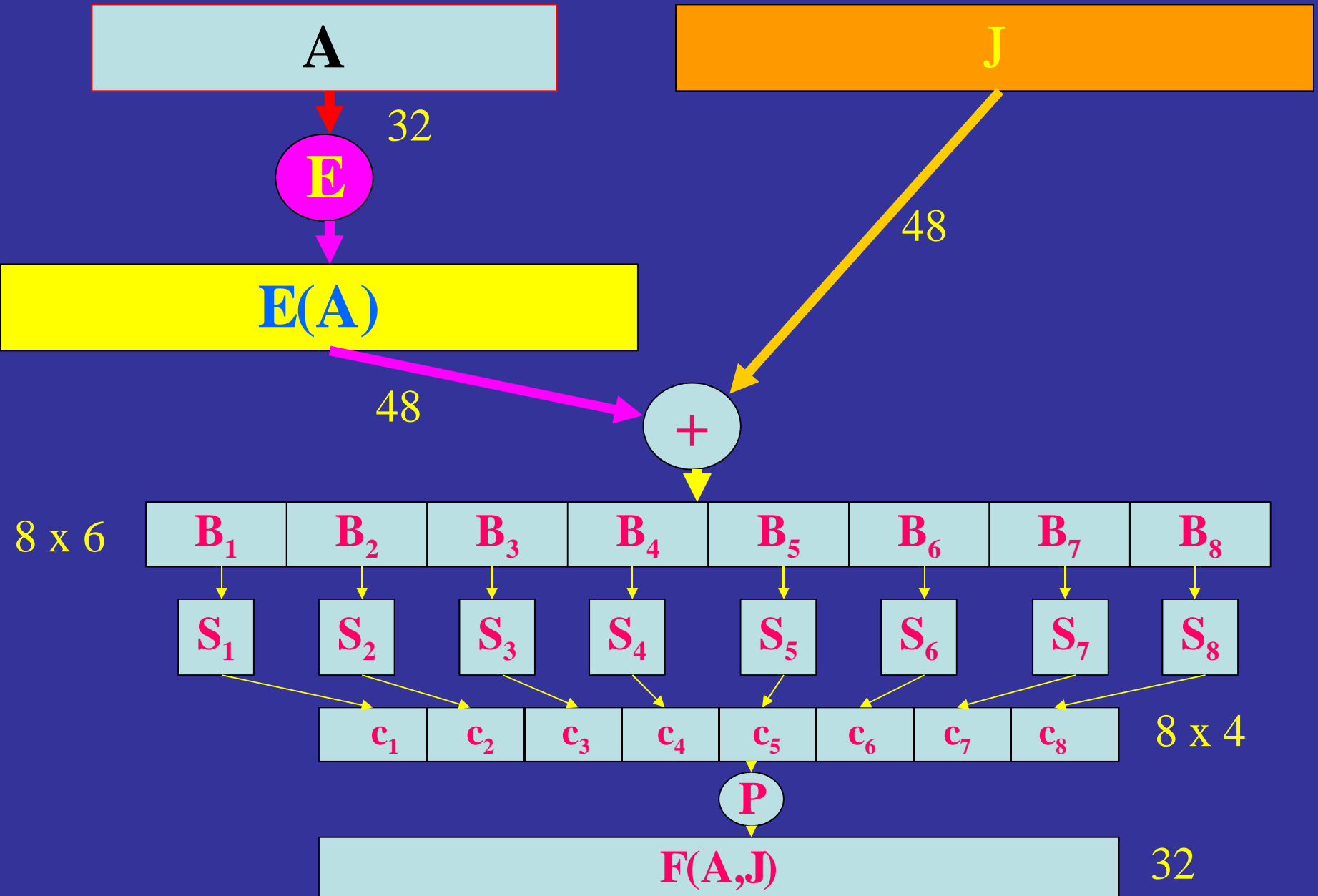
Po odwróceniu transformacji P :

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

16 7 20 21 29 12 28 17 1 15 23 26 5 18 31 10 2 8 24 14 32 27 3 9 19 13 30 6 22 11 4 25

Otrzymujemy cztery pierwsze bity f : $c_1 = (1, 1, 1, 1)$

DES, Funkcja F



DES w asno ci s-boxów

- aden s-box $S_i(X)$ nie jest liniow albo afiniczn funkcj X .
- Zmiana jednego bitu X zmienia co najmniej dwa bity $S_i(X)$.
- $S(X)$ i $S(X \oplus 001100)$ musz ró ni si przynajmniej w dwóch bitach.
- $S(X) \neq S(X \oplus 11ab00)$ dla dowolnych ab .
- S-boxy zosta y dobrane aby zminimalizowa ró nic w liczbie 0 i 1 wyniku, gdy dowolny bit argumentu jest ustalony.

DES s-box 1

S1

Wiersz	Kolumna															
Nr	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Input: $z = (z_0, z_1, z_2, z_3, z_4, z_5)$,

$(z_0, z_5) = \{0, 1, 2, 3\}$ – reprezentacja dwójkowa numeru wiersza

$(z_1, z_2, z_3, z_4) = \{0..15\}$ – reprezentacja dwójkowa numeru kolumny

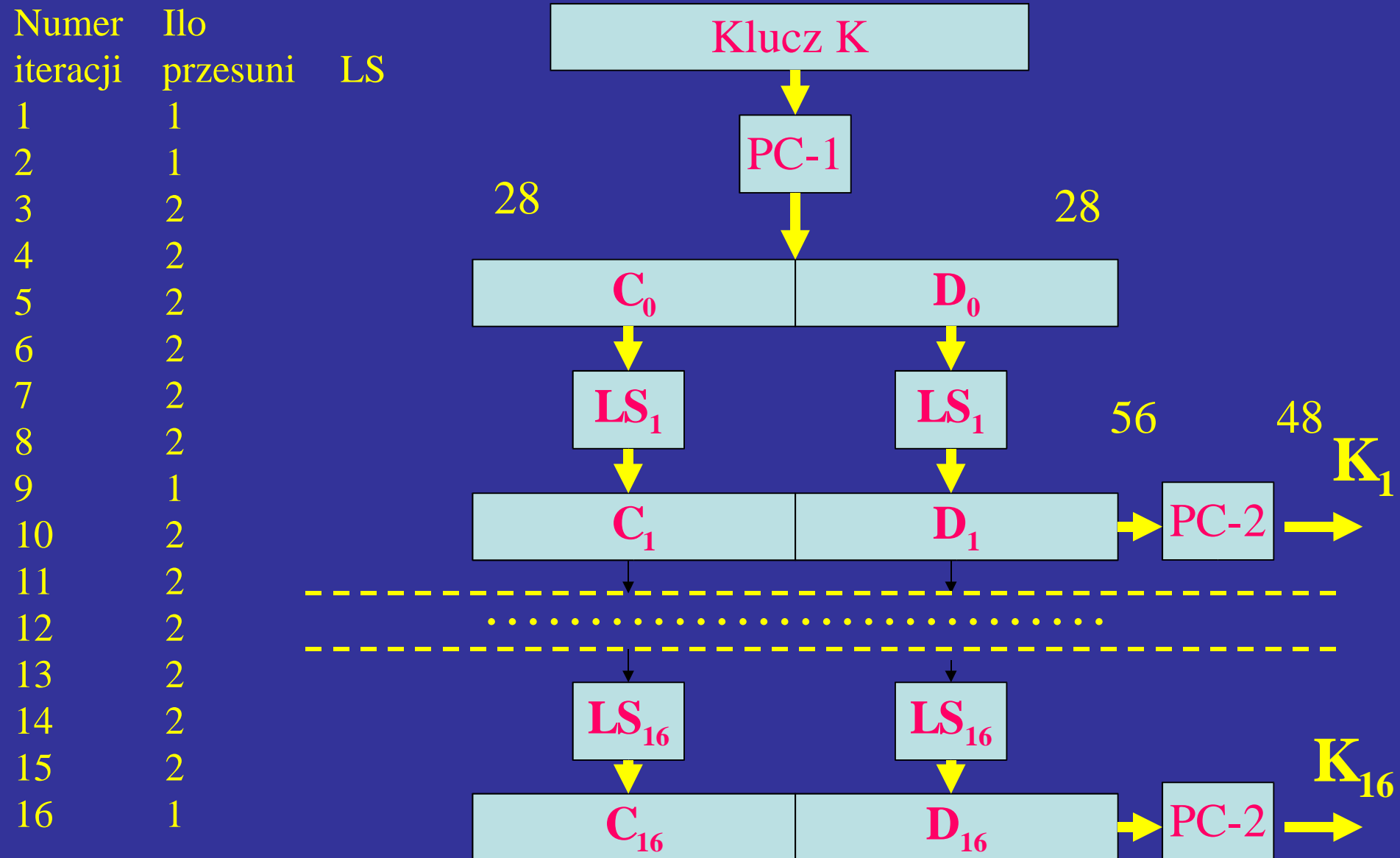
Przyk ad: $c_1 = 15$ (1,1,1,1) – mo liwe z: (1,0,0,0,0,1); (0,0,0,0,1,1); (0,0,1,0,1,0); (1,1,0,0,0,0)

Przykład, atak na 1 rundę DES B_1

B_1
(1,0,0,0,0,1
)
(0,0,0,0,1,1
)
(0,0,1,0,1,0
)
(1,1,0,0,0,0
)

E
32 1 2 3 4 5
4 5 6 7 8 9
8 9 10 11 12 13
12 13 14 15 16 17
16 17 18 19 20 21
20 21 22 23 24 25
24 25 26 27 28 29
28 29 30 31 32 1

DES : przygotowanie kluczy

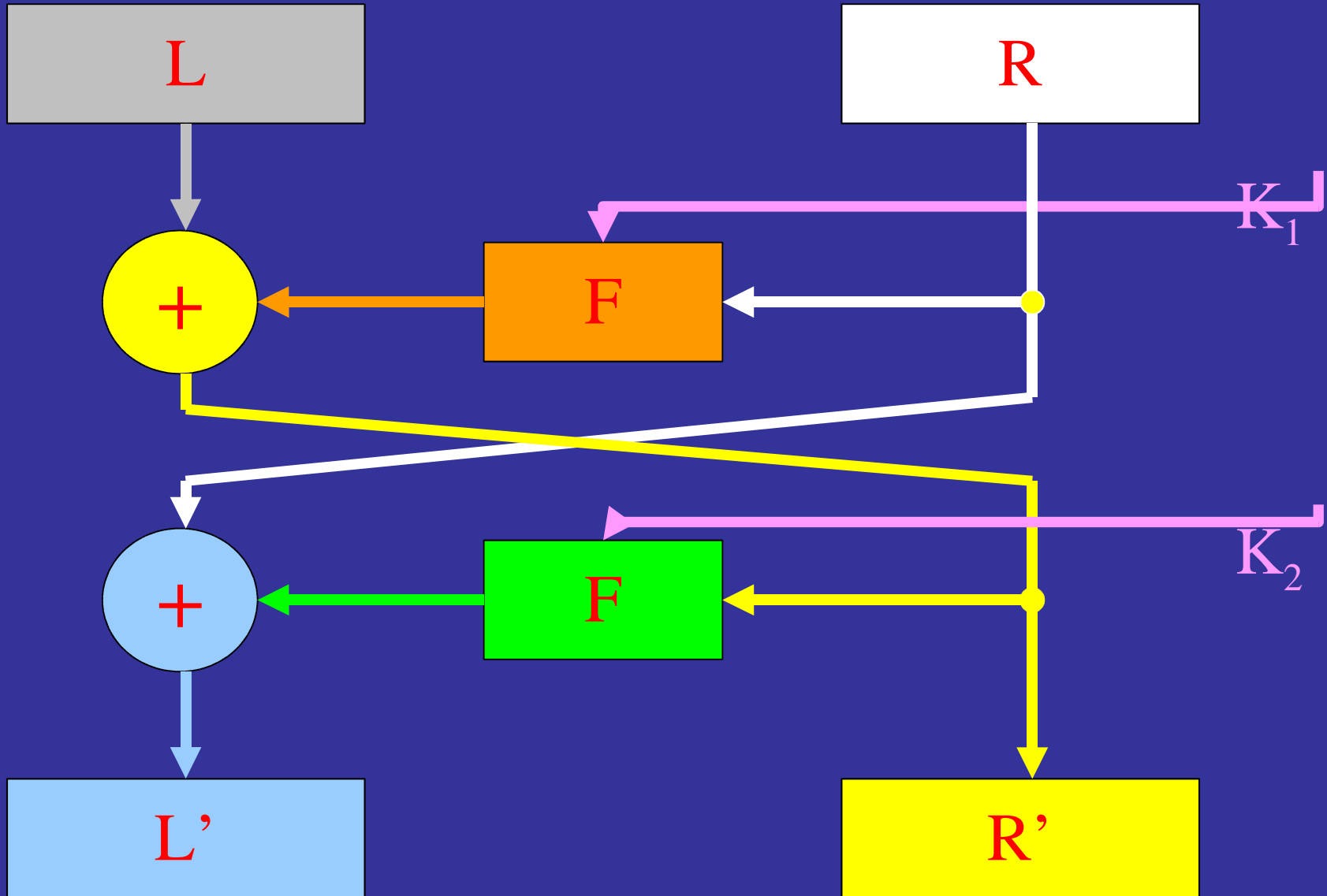


Kryptoanaliza DES 1 runda c.d.

$$(B_1 \dots B_6) = K_1 \oplus E(R)$$

Znajdź R i wszystkie możliwe kombinacje $\{B_i\}$,
możemy znaleźć 48 bitów klucza. Ponieważ w
każdym z ośmiu s-boxów każda liczba od 0 do
15 występuje cztery razy, to do zbadania mamy
 4^8 czyli 2^{16} możliwych kluczy

Kryptoanaliza DES 2 rundy



Kryptoanaliza DES 2 rundy c.d.

$$F(R, K_1) = L \oplus R'$$

$$F(R', K_2) = L' \oplus R$$

Podobnie jak w ataku na jedną rundę, pierwsza relacja redukuje liczbę kluczy K_1 do 2^{16} . Takie druga relacja redukuje ilość możliwych kombinacji K_2 do 2^{16} . Ponieważ K_1 i K_2 mają 40 bitów, które są wspólne, w praktyce liczba kluczy, które spełniają obie relacje jest bardzo mała.

Współczesne ataki na DES

- Kryptoanaliza różnicowa (E. Biham, A. Szamir 1990-1991),
zob. [1] 2^{47} tekstów jawnych
- Kryptoanaliza liniowa (M. Matsui, 1993-1994), [2] 2^{43} .
- Zmodyfikowany atak Davies'a (E. Biham, A. Biryukov, 1994)
[3] 2^{50} .
- Kryptoanaliza statystyczna (S. Vaudenay 1996), [4] $2^{42.9}$.

Kryptoanaliza różnicowa 1

Obserwacje:

- Z wyjątkiem operacji w s-boxach, wszystkie operacje elementarne DES to operacje liniowe.
- Przez dodawanie kluczy w kolejnych rundach DES uniemożliwia znalezienie argumentów s-boxów, a zatem i obliczonych wartości.

Problem:

Jak odzyskać informacje ukryte przez dodawanie kluczy w kolejnych rundach?

Kryptoanaliza różnicowa II

Modyfikacja jednego bitu

Tekst jawny

DES

klucz

Szyfrogram



Efekt lawinowy – średnio połowa bitów ulega zmianie
już po czterech rundach

Kryptoanaliza różnicowa III

Zasadnicza idea:

Badamy różnice w szyfrogramach w zależności od różnic w tekstach jawnych:

- Szyfrujemy losowy tekst P aby otrzymać C
- Modyfikujemy P przy pomocy ustalonego wzoru P' : $P^* = P \oplus P'$
- Szyfrujemy P^* , aby otrzymać $C^* = \text{DES}(K, P^*)$
- Badamy relacje pomiędzy $P' = P \oplus P^*$ i $C' = C \oplus C^*$

Będziemy się posługiwać następującą notacją: dla dowolnej wielkości X w czasie szyfrowania P i odpowiadającej jej wielkości X^* przy szyfrowaniu P^* różnic X' będziemy oznaczać:

$$X' = X \oplus X^*$$

Kryptoanaliza różnicowa IV

Zalety: łatwo obliczyć różnicę wyników operacji liniowych z jedną różnicą argumentów.

- Operacje jednoargumentowe (transformacje tablic E, P, IP):

$$(P(X))' = P(X) \oplus P(X^*) = P(X')$$

- Operacje dwuargumentowe ($X \oplus R$):

$$(X \oplus Y)' = (X \oplus Y) \oplus (X^* \oplus Y^*) = X' \oplus Y'$$

- Dodawanie klucza:

$$(X \oplus K)' = (X \oplus K) \oplus (X^* \oplus K) = X'$$

Wniosek: różnice są liniowe przy operacjach liniowych.

Nie zależą od klucza (przy operacjach liniowych!).

Kryptoanaliza różnicowa IV

Jak wybrać P' ?

- Modyfikacje P' bitów tekstu jawnego powinny w „interesujący sposób” zaburzać szyfrogram
- To zachowanie nie powinno zależeć od wyboru klucza
- To zaburzenie powinno występować z dużym prawdopodobieństwem

Kryptoanaliza różnicowa V

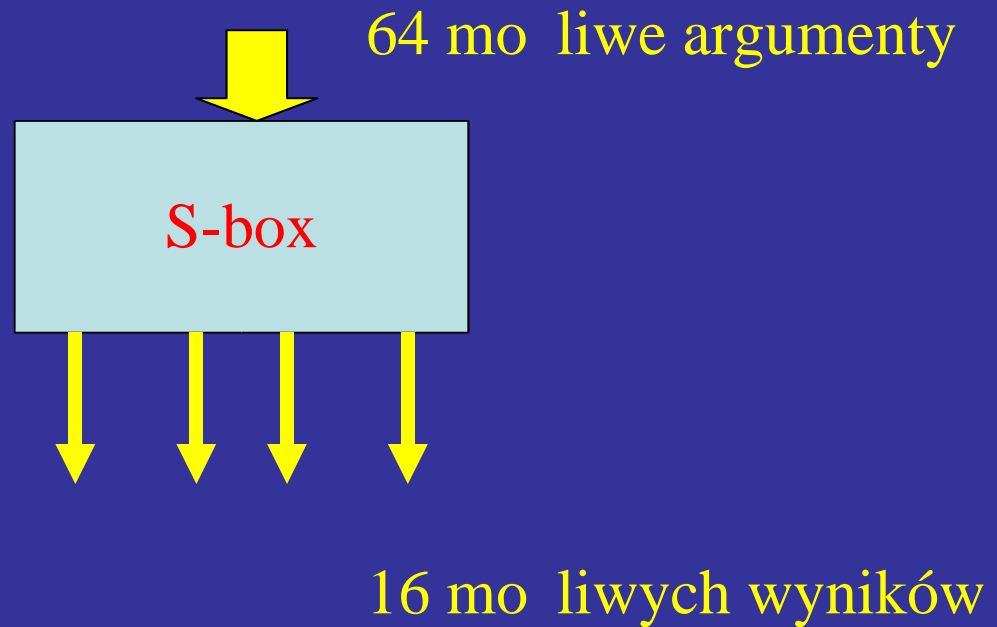
różnice i S-boxy

Mamy dwa argumenty s-boxu S : X i X^* .
Znamy tylko ich różnicę X' . Oznaczmy
 $Y = S(X)$. Co możemy powiedzieć o Y' ?
Jeśli $X' = 0$: $S(X) = S(X^*)$ dla każdego X i
 $Y' = 0$.

Jeśli $X' \neq 0$: nie znamy różnicy Y' .

Możemy jednak utworzyć tablicę rozkładu par
 (X', Y') dla wszystkich możliwych X .

Konstrukcja tablicy



S $64 \times 64 = 4096 = 2^{12}$ mo liwe pary argumentów ka dego s-boxu
Uszeregowane w 64 wierszach o takiej samej warto ci \oplus
Te 64 pary w ka dym wierszu maj 64 mo liwe warto ci, od 0 do 16
(cztery bity).

Przykład: Tablica rozkładu różnic s-boxu S1

XOR	0x	1x	2x	3x	4x	5x	6x	7x	8x	9x	Ax	Bx	Cx	Dx	Ex	Fx
0x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
Ax	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
Bx	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
Cx	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
Dx	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
Ex	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
Fx	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10x	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
...																
3Dx	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
3Ex	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
3Fx	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Przykład: Tablica rozkładu różnic s-boxu S1 c.d.

XOR	0x	1x	2x	3x	4x	5x	6x	7x	8x	9x	Ax	Bx	Cx	Dx	Ex	Fx
0x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
...
34x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
...

średnia wartość w każdym wierszu wynosi 4, a suma 64.

Wszystkie wartości są parzyste w zakresie 0-16.

Wartość **16** oznacza, że dla 1/4 par z różnic argumentów 34x $Y' = 2x$

Wartość 0 oznacza, że nie ma żadnej pary o różnicy argumentów X' i odpowiadającej jej wartości Y' .

S-boxy i różnice

Powiemy, że dla S-boxu S_i X' powoduje Y' gdy wartość pozycji (X', Y') w tablicy rozkładu różnic jest większa niż 0. Będziemy to oznaczać $X' \rightarrow Y'$.

Prawdopodobieństwo $X' \rightarrow Y'$ jest to prawdopodobieństwo, że dla pary z różnic argumentów X' różnicowa wartość spośród wszystkich możliwych par wynosi Y' . W DES to prawdopodobieństwo odpowiada wartości w odpowiednim wyrazie tabeli rozkładu, podzielonej przez 64.

Analogicznie definiujemy $X' \rightarrow Y'$ dla funkcji F , a prawdopodobieństwo obliczamy jako iloczyn prawdopodobieństw dla o i m S-boxów.

S-boxy i różnice c.d.

Na przykład, dla S-boxu 1 prawdopodobieństwo:
 $34x \rightarrow 2x = 0.25$ (16/64).

Kryptoanaliza różnicowa wykorzystuje pozycje w tablicy, które mają duże prawdopodobieństwo:
 $0x \rightarrow 0x$ i pozycje o wartości 16.

Charakterystyki

Definicja opisowa: Z każdą parą szyfrogramów związany jest XOR ich tekstów jawnych, XOR szyfrogramów, XOR argumentów do każdej kolejnej rundy obliczania obu szyfrogramów i XOR wyników każdej rundy obu obliczeń. Te wartości XOR tworzą *charakterystykę n-rund*.

Charakterystyka cechuje określone prawdopodobieństwo, którym jest wielkie prawdopodobieństwo, że losowa para o wybranym XOR tekstów jawnych ma XOR szyfrogramów i obliczeń po rundach taki jak określony w charakterystyce. Oznaczmy XOR tekstów jawnych charakterystyki przez Ω_p , a XOR szyfrogramów przez Ω_c .

Charakterystyki c.d.

Definicja formalna: charakterystyk n -rund jest uporządkowana trójka $(\Omega_P, \Omega_\Lambda, \Omega_C)$, gdzie Ω_P i Ω_C są liczbami m -bitowymi, a Ω_Λ jest list n elementów: $\Omega_\Lambda = (\Lambda_1, \Lambda_2, \dots, \Lambda_n)$, z których każdy jest par o postaci $\Lambda_i = (\lambda_I^i, \lambda_O^i)$, gdzie λ_I^i i λ_O^i są liczbami o długości $m/2$ bitów, a m jest rozmiarem bloku szyfru (w DES $m = 64$). Charakterystyka spełnia następujące warunki:

$$\lambda_I^1 = \text{prawa połowa } \Omega_P$$

$$\lambda_I^2 = \text{lewa połowa } \Omega_P \oplus \lambda_O^1$$

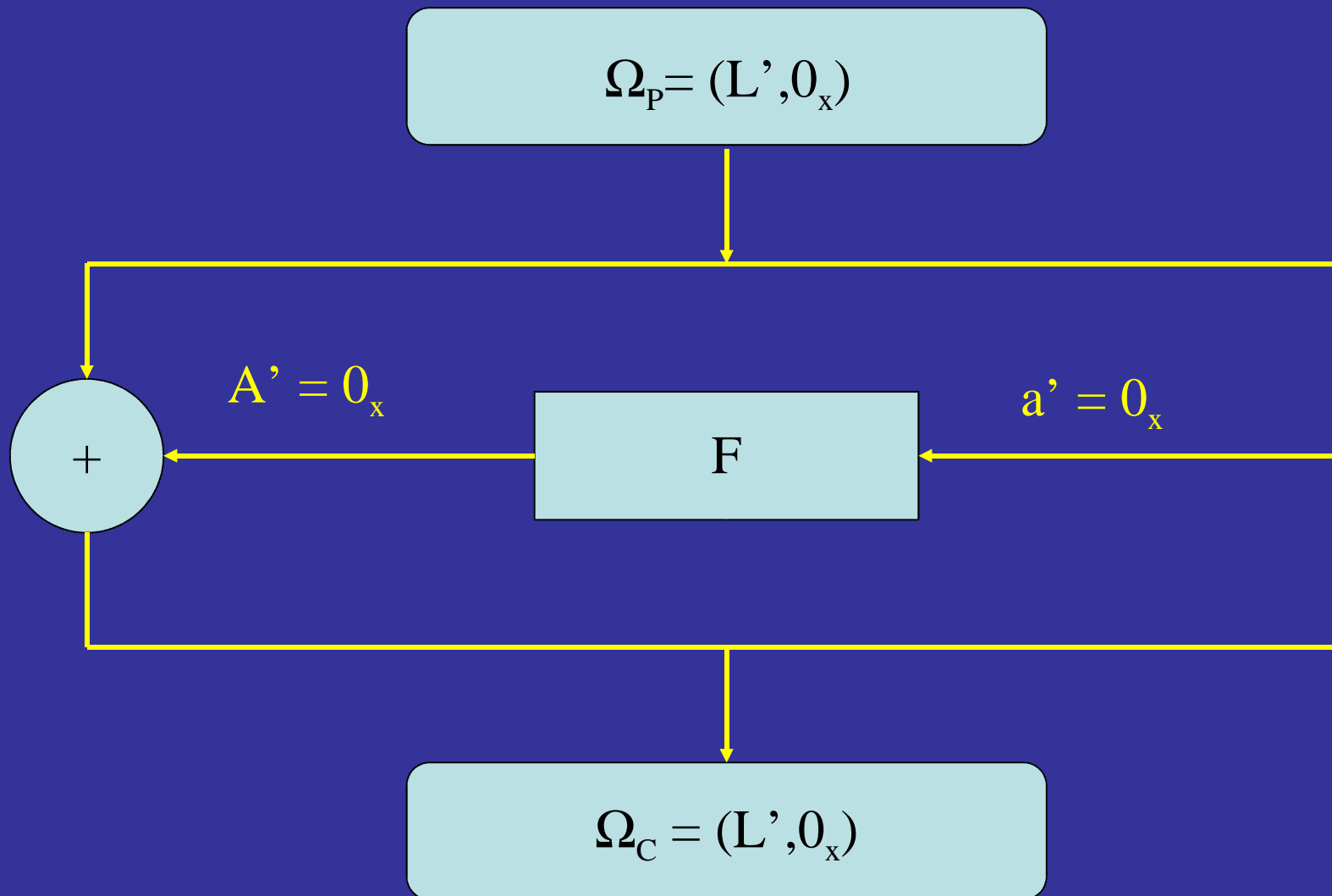
$$\lambda_I^n = \text{prawa połowa } \Omega_C$$

$$\lambda_I^{n-1} = \text{lewa połowa } \Omega_C \oplus \lambda_O^n$$

oraz dla każdego i : $2 \leq i \leq n-1$:

$$\lambda_O^i = \lambda_O^{i-1} \oplus \lambda_O^{i+1}.$$

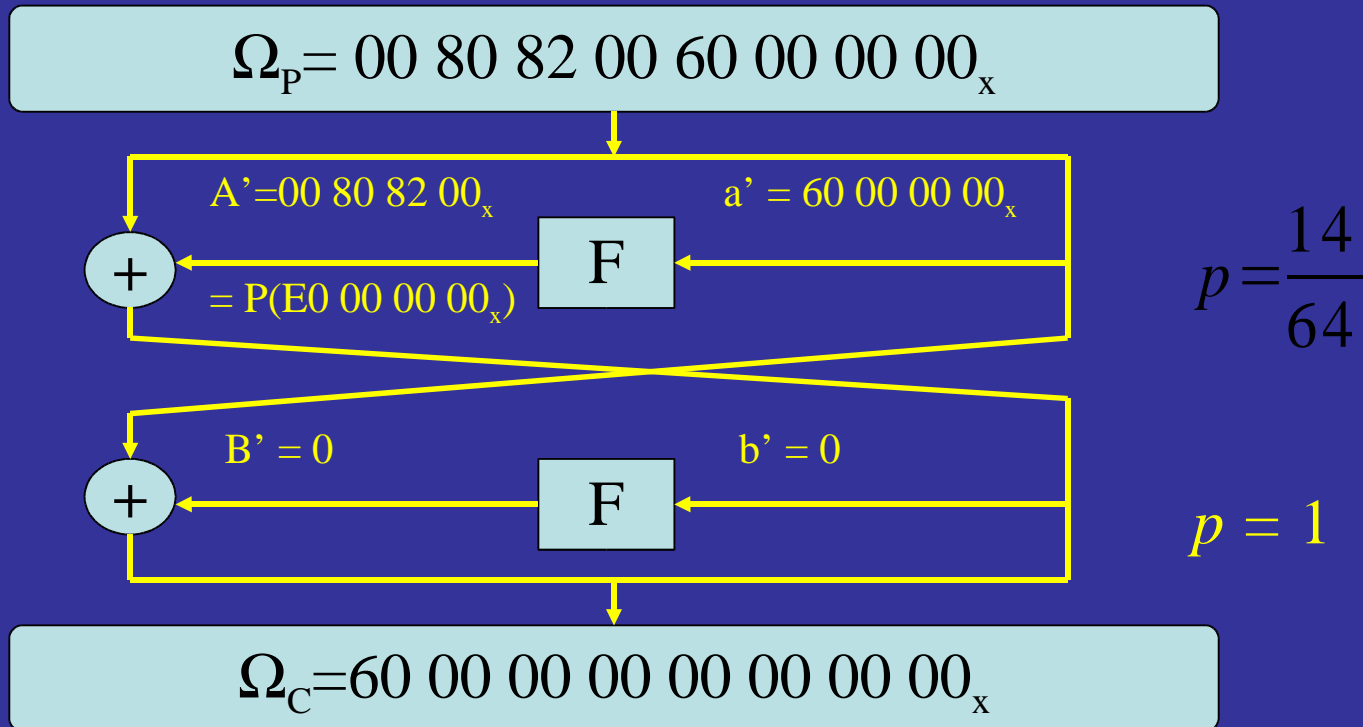
Przykład charakterystyki, $p=1$



Charakterystyki

Interesuj nas informacje statystyczne o różnicach występujących w poprzednich rundach obliczeń, dla danej różnicy dwóch tekstów jawnych.

Przykład charakterystyki dwóch rund z prawdopodobieństwem $14/64$ (W S-boxie S1 $0C_x \rightarrow E_x$ z prawdopodobieństwem $14/64$):



c.d.

Przykład kryptoanalizy różnicowej 3 rund DES
na ćwiczeniach