# Kryptografia

## z elementami kryptografii kwantowej

**Ryszard Tanaś**

http://zon8.physd.amu.edu.pl/~tanas

**Wykład 12**

# Spis treści

# 18 Kryptoanaliza

## 18.1 Podstawowe rodzaje ataku

- Atak typu ciphertext-only — znane są tylko kryptogramy — chcemy znaleźć klucz lub tekst jawny
- Atak typu known plaintext — znane są pewne pary kryptogram-tekst jawny — szukamy klucza
- Atak typu chosen plaintext — znane są kryptogramy dla dowolnie wybranego tekstu jawnego
- Atak typu chosen ciphertext — atakujący ma możliwość uzyskania tekstu jawnego dla dowolnie wybranego tekstu tajnego

# 18 Kryptoanaliza

## 18.1 Podstawowe rodzaje ataku

- Atak typu ciphertext-only — znane są tylko kryptogramy — chcemy znaleźć klucz lub tekst jawny
- Atak typu known plaintext — znane są pewne pary kryptogram-tekst jawny — szukamy klucza
- Atak typu chosen plaintext — znane są kryptogramy dla dowolnie wybranego tekstu jawnego
- Atak typu chosen ciphertext — atakujący ma możliwość uzyskania tekstu jawnego dla dowolnie wybranego tekstu tajnego

# 18 Kryptoanaliza

## 18.1 Podstawowe rodzaje ataku

- Atak typu ciphertext-only — znane są tylko kryptogramy — chcemy znaleźć klucz lub tekst jawny
- Atak typu known plaintext — znane są pewne pary kryptogram-tekst jawny — szukamy klucza
- Atak typu chosen plaintext — znane są kryptogramy dla dowolnie wybranego tekstu jawnego
- Atak typu chosen ciphertext — atakujący ma możliwość uzyskania tekstu jawnego dla dowolnie wybranego tekstu tajnego

# 18 Kryptoanaliza

## 18.1 Podstawowe rodzaje ataku

- Atak typu ciphertext-only — znane są tylko kryptogramy — chcemy znaleźć klucz lub tekst jawny
- Atak typu known plaintext — znane są pewne pary kryptogram-tekst jawny — szukamy klucza
- Atak typu chosen plaintext — znane są kryptogramy dla dowolnie wybranego tekstu jawnego
- Atak typu chosen ciphertext — atakujący ma możliwość uzyskania tekstu jawnego dla dowolnie wybranego tekstu tajnego

# 18 Kryptoanaliza

## 18.1 Podstawowe rodzaje ataku

- Atak typu ciphertext-only — znane są tylko kryptogramy — chcemy znaleźć klucz lub tekst jawny
- Atak typu known plaintext — znane są pewne pary kryptogram-tekst jawny — szukamy klucza
- Atak typu chosen plaintext — znane są kryptogramy dla dowolnie wybranego tekstu jawnego
- Atak typu chosen ciphertext — atakujący ma możliwość uzyskania tekstu jawnego dla dowolnie wybranego tekstu tajnego

- Atak typu adaptive chosen plaintext — atakujący ma możliwość wielokrotnego szyfrowania tekstu jawnego, który jest modyfikowany w zależności od uzyskanych wcześniej wyników

## 18.2 Kryptoanaliza różnicowa

- Eli Biham i Adi Shamir w 1990 r. znaleźli metodę ataku na DES przy wybranym tekście jawnym, która okazała się bardziej efektywna niż przeszukiwanie wszystkich możliwości (atak brutalny).
- W kryptoanalizie różnicowej porównuje się pary kryptogramów, które powstały w wyniku zaszyfrowania par tekstów jawnych o ustalonych różnicach.

## 18.2 Kryptoanaliza różnicowa

- Eli Biham i Adi Shamir w 1990 r. znaleźli metodę ataku na DES przy wybranym tekście jawnym, która okazała się bardziej efektywna niż przeszukiwanie wszystkich możliwości (atak brutalny).
- W kryptoanalizie różnicowej porównuje się pary kryptogramów, które powstały w wyniku zaszyfrowania par tekstów jawnych o ustalonych różnicach.

## 18.2 Kryptoanaliza różnicowa

- Eli Biham i Adi Shamir w 1990 r. znaleźli metodę ataku na DES przy wybranym tekście jawnym, która okazała się bardziej efektywna niż przeszukiwanie wszystkich możliwości (atak brutalny).
- W kryptoanalizie różnicowej porównuje się pary kryptogramów, które powstały w wyniku zaszyfrowania par tekstów jawnych o ustalonych różnicach.

- Przypuśćmy, że mamy dwa bloki o równej długości $X$ i $X'$ i obliczymy różnicę obu bloków $\Delta X = X \oplus X'$, tzn. dodajemy modulo $2$ odpowiadające sobie bity obu bloków (operacja xor). W wyniku dostajemy jedynki na tych miejscach gdzie ciągi bitów się różnią.

- Rozważmy parę wejściową $X$ i $X'$ tekstów jawnych i uwzględniając fakt, że operacje liniowe nie zmieniają różnicy $\Delta X$, dokonajmy operacji xor z kluczem $K_i$, która daje:

  $$Y = X \oplus K_i \qquad Y' = X' \oplus K_i$$

  $$\Delta Y = (X \oplus K_i) \oplus (X' \oplus K_i) = X \oplus X' = \Delta X$$

  a więc przed wejściem do S-boksa różnice się zachowują i nie zależą od wartości klucza.

- Przypuśćmy, że mamy dwa bloki o równej długości $X$ i $X'$ i obliczymy różnicę obu bloków $\Delta X = X \oplus X'$, tzn. dodajemy modulo $2$ odpowiadające sobie bity obu bloków (operacja xor). W wyniku dostajemy jedynki na tych miejscach gdzie ciągi bitów się różnią.

- Rozważmy parę wejściową $X$ i $X'$ tekstów jawnych i uwzględniając fakt, że operacje liniowe nie zmieniają różnicy $\Delta X$, dokonajmy operacji xor z kluczem $K_i$, która daje:

  $$Y = X \oplus K_i \qquad Y' = X' \oplus K_i$$

  $$\Delta Y = (X \oplus K_i) \oplus (X' \oplus K_i) = X \oplus X' = \Delta X$$

  a więc przed wejściem do S-boksa różnice się zachowują i nie zależą od wartości klucza.

- Przypuśćmy, że mamy dwa bloki o równej długości $X$ i $X'$ i obliczymy różnicę obu bloków $\Delta X = X \oplus X'$, tzn. dodajemy modulo $2$ odpowiadające sobie bity obu bloków (operacja xor). W wyniku dostajemy jedynki na tych miejscach gdzie ciągi bitów się różnią.

- Rozważmy parę wejściową $X$ i $X'$ tekstów jawnych i uwzględniając fakt, że operacje liniowe nie zmieniają różnicy $\Delta X$, dokonajmy operacji xor z kluczem $K_i$, która daje:

  $$Y = X \oplus K_i \qquad Y' = X' \oplus K_i$$

  $$\Delta Y = (X \oplus K_i) \oplus (X' \oplus K_i) = X \oplus X' = \Delta X$$

  a więc przed wejściem do S-boksa różnice się zachowują i nie zależą od wartości klucza.

- Przypuśćmy, że mamy dwa bloki o równej długości $X$ i $X'$ i obliczymy różnicę obu bloków $\Delta X = X \oplus X'$, tzn. dodajemy modulo $2$ odpowiadające sobie bity obu bloków (operacja xor). W wyniku dostajemy jedynki na tych miejscach gdzie ciągi bitów się różnią.

- Rozważmy parę wejściową $X$ i $X'$ tekstów jawnych i uwzględniając fakt, że operacje liniowe nie zmieniają różnicy $\Delta X$, dokonajmy operacji xor z kluczem $K_i$, która daje:

  $$Y = X \oplus K_i \qquad Y' = X' \oplus K_i$$

  $$\Delta Y = (X \oplus K_i) \oplus (X' \oplus K_i) = X \oplus X' = \Delta X$$

  a więc przed wejściem do S-boksa różnice się zachowują i nie zależą od wartości klucza.

- Przypuśćmy, że mamy dwa bloki o równej długości $X$ i $X'$ i obliczymy różnicę obu bloków $\Delta X = X \oplus X'$, tzn. dodajemy modulo $2$ odpowiadające sobie bity obu bloków (operacja xor). W wyniku dostajemy jedynki na tych miejscach gdzie ciągi bitów się różnią.

- Rozważmy parę wejściową $X$ i $X'$ tekstów jawnych i uwzględniając fakt, że operacje liniowe nie zmieniają różnicy $\Delta X$, dokonajmy operacji xor z kluczem $K_i$, która daje:

$$Y = X \oplus K_i \qquad Y' = X' \oplus K_i$$

$$\Delta Y = (X \oplus K_i) \oplus (X' \oplus K_i) = X \oplus X' = \Delta X$$

a więc przed wejściem do S-boksa różnice się zachowują i nie zależą od wartości klucza.

- Nieliniowym elementem DES'a są $S$-boksy i różnica $\Delta Y$ zostanie przez $S$-boks na ogół zmieniona. Jeśli wynikiem działania $S$-boksu będzie $Z = S(Y)$, to różnica $\Delta Z = S(Y) \oplus S(Y')$ będzie zależała od klucza $K_i$ i okazuje się, że tylko niektóre wartości dla $\Delta Z$ są możliwe, a to oznacza, że możliwe jest uzyskanie informacji o kluczu $K_i$.
- W tablicy podane są liczby możliwych $\Delta Z$ dla danej różnicy $\Delta X$ (różnice $\Delta X$ i $\Delta Z$ podane są układzie szestnastkowym o czym przypomina wskaźnik $x$). Liczba znajdująca się w tablicy podzielona przez $64$ określa prawdopodobieństwo wystąpienia danej różnicy $\Delta Z$.

- Nieliniowym elementem DES'a są $S$-boksy i różnica $\Delta Y$ zostanie przez $S$-boks na ogół zmieniona. Jeśli wynikiem działania $S$-boksu będzie $Z = S(Y)$, to różnica $\Delta Z = S(Y) \oplus S(Y')$ będzie zależała od klucza $K_i$ i okazuje się, że tylko niektóre wartości dla $\Delta Z$ są możliwe, a to oznacza, że możliwe jest uzyskanie informacji o kluczu $K_i$.

- W tablicy podane są liczby możliwych $\Delta Z$ dla danej różnicy $\Delta X$ (różnice $\Delta X$ i $\Delta Z$ podane są układzie szestnastkowym o czym przypomina wskaźnik $x$). Liczba znajdująca się w tablicy podzielona przez $64$ określa prawdopodobieństwo wystąpienia danej różnicy $\Delta Z$.

| $\Delta X$ | $\Delta Z$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $0_x$ | $1_x$ | $2_x$ | $3_x$ | $4_x$ | $5_x$ | $6_x$ | $7_x$ | $8_x$ | $9_x$ | $A_x$ | $B_x$ | $C_x$ | $D_x$ | $E_x$ | $F_x$ |
| $0_x$ | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $1_x$ | 0 | 0 | 0 | 6 | 0 | 2 | 4 | 4 | 0 | 10 | 12 | 4 | 10 | 6 | 2 | 4 |
| $2_x$ | 0 | 0 | 0 | 8 | 0 | 4 | 4 | 4 | 0 | 6 | 8 | 6 | 12 | 6 | 4 | 2 |
| $3_x$ | 14 | 4 | 2 | 2 | 10 | 6 | 4 | 2 | 6 | 4 | 4 | 0 | 2 | 2 | 2 | 0 |
| $4_x$ | 0 | 0 | 0 | 6 | 0 | 10 | 10 | 6 | 0 | 4 | 6 | 4 | 2 | 8 | 6 | 2 |
| $5_x$ | 4 | 8 | 6 | 2 | 2 | 4 | 4 | 2 | 0 | 4 | 4 | 0 | 12 | 2 | 4 | 6 |
| $6_x$ | 0 | 4 | 2 | 4 | 8 | 2 | 6 | 2 | 8 | 4 | 4 | 2 | 4 | 2 | 0 | 12 |
| $7_x$ | 2 | 4 | 10 | 4 | 0 | 4 | 8 | 4 | 2 | 4 | 8 | 2 | 2 | 2 | 4 | 4 |
| $8_x$ | 0 | 0 | 0 | 12 | 0 | 8 | 8 | 4 | 0 | 6 | 2 | 8 | 8 | 2 | 2 | 4 |
| $9_x$ | 10 | 2 | 4 | 0 | 2 | 4 | 6 | 0 | 2 | 2 | 8 | 0 | 10 | 0 | 2 | 12 |
| $A_x$ | 0 | 8 | 6 | 2 | 2 | 8 | 6 | 0 | 6 | 4 | 6 | 0 | 4 | 0 | 2 | 10 |
| $B_x$ | 2 | 4 | 0 | 10 | 2 | 2 | 4 | 0 | 2 | 6 | 2 | 6 | 6 | 4 | 2 | 12 |
| $C_x$ | 0 | 0 | 0 | 8 | 0 | 6 | 6 | 0 | 0 | 6 | 6 | 4 | 6 | 6 | 14 | 2 |
| $D_x$ | 6 | 6 | 4 | 8 | 4 | 8 | 2 | 6 | 0 | 6 | 4 | 6 | 0 | 2 | 0 | 2 |
| $E_x$ | 0 | 4 | 8 | 8 | 6 | 6 | 4 | 0 | 6 | 6 | 4 | 0 | 0 | 4 | 0 | 8 |
| $F_x$ | 2 | 0 | 2 | 4 | 4 | 6 | 4 | 2 | 4 | 8 | 2 | 2 | 2 | 6 | 8 | 8 |
| $10_x$ | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 14 | 0 | 6 | 6 | 12 | 4 | 6 | 8 | 6 |
| $11_x$ | 6 | 8 | 2 | 4 | 6 | 4 | 8 | 6 | 4 | 0 | 6 | 6 | 0 | 4 | 0 | 0 |
| $12_x$ | 0 | 8 | 4 | 2 | 6 | 6 | 4 | 6 | 6 | 4 | 2 | 6 | 6 | 0 | 4 | 0 |
| $13_x$ | 2 | 4 | 4 | 6 | 2 | 0 | 4 | 6 | 2 | 0 | 6 | 8 | 4 | 6 | 4 | 6 |
| $14_x$ | 0 | 8 | 8 | 0 | 10 | 0 | 4 | 2 | 8 | 2 | 2 | 4 | 4 | 8 | 4 | 0 |
| $15_x$ | 0 | 4 | 6 | 4 | 2 | 2 | 4 | 10 | 6 | 2 | 0 | 10 | 0 | 4 | 6 | 4 |
| $16_x$ | 0 | 8 | 10 | 8 | 0 | 2 | 2 | 6 | 10 | 2 | 0 | 2 | 0 | 6 | 2 | 6 |
| $17_x$ | 4 | 4 | 6 | 0 | 10 | 6 | 0 | 2 | 4 | 4 | 4 | 6 | 6 | 6 | 2 | 0 |
| $18_x$ | 0 | 6 | 6 | 0 | 8 | 4 | 2 | 2 | 2 | 4 | 6 | 8 | 6 | 6 | 2 | 2 |
| $19_x$ | 2 | 6 | 2 | 4 | 0 | 8 | 4 | 6 | 10 | 4 | 0 | 4 | 2 | 8 | 4 | 0 |
| $1A_x$ | 0 | 6 | 4 | 0 | 4 | 6 | 6 | 6 | 6 | 2 | 2 | 0 | 4 | 4 | 6 | 8 |
| $1B_x$ | 4 | 4 | 2 | 4 | 10 | 6 | 6 | 4 | 6 | 2 | 2 | 4 | 2 | 2 | 4 | 2 |
| $1C_x$ | 0 | 10 | 10 | 6 | 6 | 0 | 0 | 12 | 6 | 4 | 0 | 0 | 2 | 4 | 4 | 0 |
| $1D_x$ | 4 | 2 | 4 | 0 | 8 | 0 | 0 | 2 | 10 | 0 | 2 | 6 | 6 | 6 | 14 | 0 |
| $1E_x$ | 0 | 2 | 6 | 0 | 14 | 2 | 0 | 0 | 6 | 4 | 10 | 8 | 2 | 2 | 6 | 2 |
| $1F_x$ | 2 | 4 | 10 | 6 | 2 | 2 | 2 | 8 | 6 | 8 | 0 | 0 | 0 | 4 | 6 | 4 |

| $\Delta X$ | $\Delta Z$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $0_x$ | $1_x$ | $2_x$ | $3_x$ | $4_x$ | $5_x$ | $6_x$ | $7_x$ | $8_x$ | $9_x$ | $A_x$ | $B_x$ | $C_x$ | $D_x$ | $E_x$ | $F_x$ |
| $20_x$ | 0 | 0 | 0 | 10 | 0 | 12 | 8 | 2 | 0 | 6 | 4 | 4 | 4 | 2 | 0 | 12 |
| $21_x$ | 0 | 4 | 2 | 4 | 4 | 8 | 10 | 0 | 4 | 4 | 10 | 0 | 4 | 0 | 2 | 8 |
| $22_x$ | 10 | 4 | 6 | 2 | 2 | 8 | 2 | 2 | 2 | 2 | 6 | 0 | 4 | 0 | 4 | 10 |
| $23_x$ | 0 | 4 | 4 | 8 | 0 | 2 | 6 | 0 | 6 | 6 | 2 | 10 | 2 | 4 | 0 | 10 |
| $24_x$ | 12 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 14 | 14 | 2 | 0 | 2 | 6 | 2 | 4 |
| $25_x$ | 6 | 4 | 4 | 12 | 4 | 4 | 4 | 10 | 2 | 2 | 2 | 0 | 4 | 2 | 2 | 2 |
| $26_x$ | 0 | 0 | 4 | 10 | 10 | 10 | 2 | 4 | 0 | 4 | 6 | 4 | 4 | 4 | 2 | 0 |
| $27_x$ | 10 | 4 | 2 | 0 | 2 | 4 | 2 | 0 | 4 | 8 | 0 | 4 | 8 | 8 | 4 | 4 |
| $28_x$ | 12 | 2 | 2 | 8 | 2 | 6 | 12 | 0 | 0 | 2 | 6 | 0 | 4 | 0 | 6 | 2 |
| $29_x$ | 4 | 2 | 2 | 10 | 0 | 2 | 4 | 0 | 0 | 14 | 10 | 2 | 4 | 6 | 0 | 4 |
| $2A_x$ | 4 | 2 | 4 | 6 | 0 | 2 | 8 | 2 | 2 | 14 | 2 | 6 | 2 | 6 | 2 | 2 |
| $2B_x$ | 12 | 2 | 2 | 2 | 4 | 6 | 6 | 2 | 0 | 2 | 6 | 2 | 6 | 0 | 8 | 4 |
| $2C_x$ | 4 | 2 | 2 | 4 | 0 | 2 | 10 | 4 | 2 | 2 | 4 | 8 | 8 | 4 | 2 | 6 |
| $2D_x$ | 6 | 2 | 6 | 2 | 8 | 4 | 4 | 4 | 2 | 4 | 6 | 0 | 8 | 2 | 0 | 6 |
| $2E_x$ | 6 | 6 | 2 | 2 | 0 | 2 | 4 | 6 | 4 | 0 | 6 | 2 | 12 | 2 | 6 | 4 |
| $2F_x$ | 2 | 2 | 2 | 2 | 2 | 6 | 8 | 8 | 2 | 4 | 4 | 6 | 8 | 2 | 4 | 2 |
| $30_x$ | 0 | 4 | 6 | 0 | 12 | 6 | 2 | 2 | 8 | 2 | 4 | 4 | 6 | 2 | 2 | 4 |
| $31_x$ | 4 | 8 | 2 | 10 | 2 | 2 | 2 | 2 | 6 | 0 | 0 | 2 | 2 | 4 | 10 | 8 |
| $32_x$ | 4 | 2 | 6 | 4 | 4 | 2 | 2 | 4 | 6 | 6 | 4 | 8 | 2 | 2 | 8 | 0 |
| $33_x$ | 4 | 4 | 6 | 2 | 10 | 8 | 4 | 2 | 4 | 0 | 2 | 2 | 4 | 6 | 2 | 4 |
| $34_x$ | 0 | 8 | 16 | 6 | 2 | 0 | 0 | 12 | 6 | 0 | 0 | 0 | 0 | 8 | 0 | 6 |
| $35_x$ | 2 | 2 | 4 | 0 | 8 | 0 | 0 | 0 | 14 | 4 | 6 | 8 | 0 | 2 | 14 | 0 |
| $36_x$ | 2 | 6 | 2 | 2 | 8 | 0 | 2 | 2 | 4 | 2 | 6 | 8 | 6 | 4 | 10 | 0 |
| $37_x$ | 2 | 2 | 12 | 4 | 2 | 4 | 4 | 10 | 4 | 4 | 2 | 6 | 0 | 2 | 2 | 4 |
| $38_x$ | 0 | 6 | 2 | 2 | 2 | 0 | 2 | 2 | 4 | 6 | 4 | 4 | 4 | 6 | 10 | 10 |
| $39_x$ | 6 | 2 | 2 | 4 | 12 | 6 | 4 | 8 | 4 | 0 | 2 | 4 | 2 | 4 | 4 | 0 |
| $3A_x$ | 6 | 4 | 6 | 4 | 6 | 8 | 0 | 6 | 2 | 2 | 6 | 2 | 2 | 6 | 4 | 0 |
| $3B_x$ | 2 | 6 | 4 | 0 | 0 | 2 | 4 | 6 | 4 | 6 | 8 | 6 | 4 | 4 | 6 | 2 |
| $3C_x$ | 0 | 10 | 4 | 0 | 12 | 0 | 4 | 2 | 6 | 0 | 4 | 12 | 4 | 4 | 2 | 0 |
| $3D_x$ | 0 | 8 | 6 | 2 | 2 | 6 | 0 | 8 | 4 | 4 | 0 | 4 | 0 | 12 | 4 | 4 |
| $3E_x$ | 4 | 8 | 2 | 2 | 2 | 4 | 4 | 14 | 4 | 2 | 0 | 2 | 0 | 8 | 4 | 4 |
| $3F_x$ | 4 | 8 | 4 | 2 | 4 | 0 | 2 | 4 | 4 | 2 | 4 | 8 | 8 | 6 | 2 | 2 |

- W tabeli znajdujemy wiele zer, a to oznacza, że takie różnice nie mogą wystąpić. Prawdopodobieństwa wystąpienia poszczególnych różnic znacznie się różnią i ten fakt jest wykorzystywany w kryptoanalizie różnicowej.

  Np. dla $\Delta X = 1_x$ istnieją tylko cztery pary które dają różnicę $\Delta Z = F_x$.

  Takie pary można wcześniej wyznaczyć i w tym przypadku są to pary:
  $\{1E_x, 1F_x\}$, $\{1F_x, 1E_x\}$, $\{2A_x, 2B_x\}$, $\{2B_x, 2A_x\}$.

- W tabeli znajdujemy wiele zer, a to oznacza, że takie różnice nie mogą wystąpić. Prawdopodobieństwa wystąpienia poszczególnych różnic znacznie się różnią i ten fakt jest wykorzystywany w kryptoanalizie różnicowej.

  Np. dla $\Delta X = 1_x$ istnieją tylko cztery pary które dają różnicę $\Delta Z = F_x$.

  Takie pary można wcześniej wyznaczyć i w tym przypadku są to pary:
  $\{1E_x, 1F_x\}$, $\{1F_x, 1E_x\}$, $\{2A_x, 2B_x\}$, $\{2B_x, 2A_x\}$.

- W tabeli znajdujemy wiele zer, a to oznacza, że takie różnice nie mogą wystąpić. Prawdopodobieństwa wystąpienia poszczególnych różnic znacznie się różnią i ten fakt jest wykorzystywany w kryptoanalizie różnicowej.

  Np. dla $\Delta X = 1_x$ istnieją tylko cztery pary które dają różnicę $\Delta Z = F_x$.

  Takie pary można wcześniej wyznaczyć i w tym przypadku są to pary:
  $\{1E_x, 1F_x\}$, $\{1F_x, 1E_x\}$, $\{2A_x, 2B_x\}$, $\{2B_x, 2A_x\}$.

- Znajomość takich par oraz prawdopodobieństw ich wystąpienia pozwala przy wykorzystaniu ataku typu chosen plaintext uzyskać informację o bitach klucza. Można w ten sposób znacznie ograniczyć przestrzeń możliwych kluczy.
- Prawdopodobnie twórcy DES'a zdawali sobie sprawę z możliwości kryptoanalizy różnicowej, chociaż pojawiła się ona później niż sam DES. Liczba rund DES'a została wybrana w taki sposób, że nawet korzystanie z kryptoanalizy różnicowej wymaga dużych nakładów (mocy obliczeniowych) dla złamania szyfru.

- Znajomość takich par oraz prawdopodobieństw ich wystąpienia pozwala przy wykorzystaniu ataku typu chosen plaintext uzyskać informację o bitach klucza. Można w ten sposób znacznie ograniczyć przestrzeń możliwych kluczy.
- Prawdopodobnie twórcy DES'a zdawali sobie sprawę z możliwości kryptoanalizy różnicowej, chociaż pojawiła się ona później niż sam DES. Liczba rund DES'a została wybrana w taki sposób, że nawet korzystanie z kryptoanalizy różnicowej wymaga dużych nakładów (mocy obliczeniowych) dla złamania szyfru.

## 18.3 Kryptoanaliza liniowa

- Inną metodą kryptoanalizy jest kryptoanaliza liniowa zaproponowana przez Mitsuru Matsui w 1993 r.
- Idea kryptoanalizy liniowej polega na opisie działania urządzenia szyfrującego poprzez aproksymację liniową.
- Mimo, że $S$-boksy DES'a są elementami nieliniowymi, to mogą być one aproksymowane formułami liniowymi. Oznacza to, że zależności liniowe aproksymujące działanie $S$-boksu są spełnione z prawdopodobieństwem różnym niż $1/2$.

## 18.3 Kryptoanaliza liniowa

- Inną metodą kryptoanalizy jest kryptoanaliza liniowa zaproponowana przez Mitsuru Matsui w 1993 r.
- Idea kryptoanalizy liniowej polega na opisie działania urządzenia szyfrującego poprzez aproksymację liniową.
- Mimo, że $S$-boksy DES'a są elementami nieliniowymi, to mogą być one aproksymowane formułami liniowymi. Oznacza to, że zależności liniowe aproksymujące działanie $S$-boksu są spełnione z prawdopodobieństwem różnym niż $1/2$.

## 18.3 Kryptoanaliza liniowa

- Inną metodą kryptoanalizy jest kryptoanaliza liniowa zaproponowana przez Mitsuru Matsui w 1993 r.
- Idea kryptoanalizy liniowej polega na opisie działania urządzenia szyfrującego poprzez aproksymację liniową.
- Mimo, że $S$-boksy DES'a są elementami nieliniowymi, to mogą być one aproksymowane formułami liniowymi. Oznacza to, że zależności liniowe aproksymujące działanie $S$-boksu są spełnione z prawdopodobieństwem różnym niż $1/2$.

## 18.3 Kryptoanaliza liniowa

- Inną metodą kryptoanalizy jest kryptoanaliza liniowa zaproponowana przez Mitsuru Matsui w 1993 r.
- Idea kryptoanalizy liniowej polega na opisie działania urządzenia szyfrującego poprzez aproksymację liniową.
- Mimo, że $S$-boksy DES'a są elementami nieliniowymi, to mogą być one aproksymowane formułami liniowymi. Oznacza to, że zależności liniowe aproksymujące działanie $S$-boksu są spełnione z prawdopodobieństwem różnym niż $1/2$.

- Jeśli np. wiemy, że pomiędzy bitami klucza $k_i$, tekstu jawnego $m_i$ oraz kryptogramu $c_i$ zachodzą z prawdopodobieństwem $90\%$ zależności

  $$m_{15} \oplus k_2 \oplus m_7 \oplus k_6 = c_2 \oplus m_5 \oplus c_7$$
  $$m_8 \oplus k_2 \oplus k_6 = c_5 \oplus c_6,$$

  to znając $m_i$ i $c_i$ możemy z takim samym prawdopodobieństwem wyznaczyć $k_2 \oplus k_6$. Oczywiście tego typu zależności należy najpierw znaleźć.

- Dla DES'a przy ataku typu known plaintext kryptoanaliza liniowa wymaga średnio $2^{43}$ par tekst jawny-kryptogram do znalezienia klucza. Matsui w 1994 r. potrzebował $50$ dni aby na $12$ komputerach HP 9735 obliczyć klucz DES'a!

- Jeśli np. wiemy, że pomiędzy bitami klucza $k_i$, tekstu jawnego $m_i$ oraz kryptogramu $c_i$ zachodzą z prawdopodobieństwem $90\%$ zależności

  $$m_{15} \oplus k_2 \oplus m_7 \oplus k_6 = c_2 \oplus m_5 \oplus c_7$$
  $$m_8 \oplus k_2 \oplus k_6 = c_5 \oplus c_6,$$

  to znając $m_i$ i $c_i$ możemy z takim samym prawdopodobieństwem wyznaczyć $k_2 \oplus k_6$. Oczywiście tego typu zależności należy najpierw znaleźć.

- Dla DES'a przy ataku typu known plaintext kryptoanaliza liniowa wymaga średnio $2^{43}$ par tekst jawny-kryptogram do znalezienia klucza. Matsui w 1994 r. potrzebował $50$ dni aby na $12$ komputerach HP 9735 obliczyć klucz DES'a!

- Jeśli np. wiemy, że pomiędzy bitami klucza $k_i$, tekstu jawnego $m_i$ oraz kryptogramu $c_i$ zachodzą z prawdopodobieństwem $90\%$ zależności

  $$m_{15} \oplus k_2 \oplus m_7 \oplus k_6 = c_2 \oplus m_5 \oplus c_7$$
  $$m_8 \oplus k_2 \oplus k_6 = c_5 \oplus c_6,$$

  to znając $m_i$ i $c_i$ możemy z takim samym prawdopodobieństwem wyznaczyć $k_2 \oplus k_6$. Oczywiście tego typu zależności należy najpierw znaleźć.

- Dla DES'a przy ataku typu known plaintext kryptoanaliza liniowa wymaga średnio $2^{43}$ par tekst jawny-kryptogram do znalezienia klucza. Matsui w 1994 r. potrzebował $50$ dni aby na $12$ komputerach HP 9735 obliczyć klucz DES'a!

- Jeśli np. wiemy, że pomiędzy bitami klucza $k_i$, tekstu jawnego $m_i$ oraz kryptogramu $c_i$ zachodzą z prawdopodobieństwem $90\%$ zależności

  $$m_{15} \oplus k_2 \oplus m_7 \oplus k_6 = c_2 \oplus m_5 \oplus c_7$$
  $$m_8 \oplus k_2 \oplus k_6 = c_5 \oplus c_6,$$

  to znając $m_i$ i $c_i$ możemy z takim samym prawdopodobieństwem wyznaczyć $k_2 \oplus k_6$. Oczywiście tego typu zależności należy najpierw znaleźć.

- Dla DES'a przy ataku typu known plaintext kryptoanaliza liniowa wymaga średnio $2^{43}$ par tekst jawny-kryptogram do znalezienia klucza. Matsui w 1994 r. potrzebował $50$ dni aby na $12$ komputerach HP 9735 obliczyć klucz DES'a!