MI-PB-5

Diferenciální kryptoanalýza, analýza S-boxů, diferenciální aproximační funkce, extrakce bitů klíče.

Diferenciální kryptoanalýza: Využívá vysokou pravděpodobnost určitých výskytů rozdílů OT a rozdílů v poslední rundě šifry

Pokud $[X_1X_2...X_n]$ jsou vstupy a $[Y_1Y_2...Y_n]$ výstupy kryptosystému, máme dva vstupy X', X'' a dva odpovídající výstupy Y', Y'':
Vstupní rozdíl je $\Delta X = X' \oplus X'' = [\Delta X_1 \Delta X_2 ... \Delta X_n]$, kde $\Delta X_i = X'_i \oplus X''_i$.
Výstupní rozdíl je $\Delta Y = Y' \oplus Y'' = [\Delta Y_1 \Delta Y_2 ... \Delta Y_n]$, kde $\Delta Y_i = Y'_i \oplus Y''_i$

Ideální případ náhodné šifry: pravděpodobnost výskytu rozdílů ΔY daných ΔX je právě $\frac{1}{2^n}$, kde n je délka X
DK hledá využití možnosti výskytu jednotliých ΔY daných ΔX s velmi vysokou pravděpodobností $p_D > \frac{1}{2^n}$

Rozdíl (diferenciál): dvojice $(\Delta X, \Delta Y)$

Diferenciální charakteristiky: Sekvence vstupních a výstupních rozdílů v rundách t.ž. výstupní rozdíly jedné rundy jsou vstupní rozdíly druhé rundy
Vysoce pravděpodobná diferenciální charakteristika: využití informace přocházející do poslední rundy k odvození bitů poslední vrstvy klíče

Průběh DK

Analýza SBOXů

- **Tvorba diferenční distribuční tabulky:** s jakou pravděpodobností se ΔY vyskytuje pro dané ΔX
  - Ideální SBOX: 1 výskyt každého páru $(\Delta X, \Delta Y)$
- **Klíčovaný SBOX:** *(maskování)* Klíč naxorován na vstup každého SBOXu
  - Při DK žádný vliv:

Pokud $\Delta W = [W'_1 \oplus W''_1, ..., W'_n \oplus W''_n]$ diference vstupu do SBOXu,
$\Delta W_i = W'_i \oplus W''_i = (X'_i \oplus K_i) \oplus (X''_i \oplus K_i) = X'_i \oplus X''_i = \Delta X_i$

- Klíčovaný SBOX má stejnou diferenční distribuční tabulku jako neklíčovaný

- **Tvorba diferenciální charakteristiky** pro $R - 1$ rund
  - Volba aktivních SBOXů a jejich vstupních a výstupních rozdílů (cíl: vysoká pravděpodobnost)
  - Z nich počítána **celková pravděpodobnost diference šifry** jako $\prod_{i=1}^{k} p_i$, kde p_i je pravděpodobnost výskytu zvolené výstupní diference pro zvolenou vstupní diferenci (z tabulky)

Extrakce bitů klíče:

- Pro každý **pravý pár OT** (pár, kde ΔOT sedí na zvolenou diferenci do první rundy):
  - **Pro každý možný podklíč** (zajímavou část -- kde jsou aktivní SBOXy poslední rundy):
    - Porovnat **rozdíly na vstupu poslední rundy** získané z OT s **rozdíly hodnot získaných zpětným chodem** od ŠT
      Zpětný chod: $\mathrm{SBOX}^{-1}(\mathrm{ŠT} \oplus \mathrm{podklíč})$
    - Pokud shoda, inkrementovat čítač u podklíče
- **Pravděpodobnost podklíčů** pro N pravých dvojic: $\mathrm{prob} = \frac{\mathrm{count}}{N}$
- Zvolit podklíč s **nejvyšší pravděpodobností**