IDEA - International Data Encryption Standard

Janez Žibert

16. junij 1999

1 Uvod

IDEA je simetrični bločni enkripcijski algoritem. Prvič sta ga objavila X. Lai in J.L. Massey leta 1990 z imenom PES (Proposed Encryption Standard) [7]. Kasneje pa sta ga z nekaj izboljšavami preimenovala v IPES (Improved Proposed Encryption Standard). Leta 1992 je dobil postopek dokončno ime IDEA (International Data Encryption Algorithm).

IDEA spada v isti razred enkripcijskih algoritmov kot DES, ki je bolj znan in razširjen algoritem. Bistvena razlika med IDEO in DES-om je dolžina ključa, ki ga uporabljata algoritma. Razlike so še v samem postopku, kjer se pri IDEI izognemo uporabi "pastem", kot so S-škatle pri DES-u. Postopek enkripcije in dekripcije z IDEO je ob učinkoviti izvedbi algoritma praviloma nekajkrat hitrejši od DES-a. To pa so tudi bistvene lastnosti algoritma, ki mu zagotavljajo v prihodnjih letih prednost pred DES-om, če se bo le izkazalo, da je varnejši v primerjavi s podobnimi simetričnimi enkripcijskimi algoritmi.

2 Opis postopka IDEE

2.1 Osnovni opis

IDEA je simetrični bločni enkripcijski algoritem. Enkripcija se izvaja nad 64-bitnimi bloki, ki jih v osnovnem postopku razdelimo na 16-bitne podbloke. Pri postopku enkripcije in dekripcije se uporablja isti algoritem, ki uporablja 128-bitni ključ, le vrstni red podključev, tvorjenih iz osnovnega ključa, je spremenjen. Rezultat enkripcije so prav tako 64-bitni bloki tajnopisa.

Osnovna ideja postopka je uporaba treh različnih algebraičnih operacij iz različnih grup. Operacije, ki se prepletajo na vsakem koraku postopka, so:

- $\oplus$: XOR,
- $\boxplus$: seštevanje po modulu 2^{16},
- $\odot$: množenje po modulu $2^{16}+1$, pri tem definiramo število $0\ldots0 = 2^{16}$.

Vse operacije v osnovnem postopku se izvajajo nad 16-bitnimi podbloki. Lahko se uporabljajo tudi operacije nad podbloki dolžine 4 ali 8 bitov. V takih primerih se izvaja postopek nad 16- ali 32-bitnimi bloki čistopisa. Posplošitev na večje podbloke (dolžine 32-bitov in s tem skupnega bloka dolžine 128-bitov) ni možna zaradi dejstva, da število $2^{32}+1$ ni praštevilo, s tem pa

nimamo zagotovljenih inverznih elementov za operacijo množenja po modulu $\odot$, ki so pomembni pri postopku dekripcije. V prej opisanih primerih so števila za množenje po modulu praštevila.

IDEA je iterativen postopek, kar pomeni, da je sestavljena iz posameznih krogov. Vsi takšni algoritmi slonijo na dejstvu, da združjemo kriptografsko "šibke" funkcije (to pomeni, da jih znamo z razmeroma malo čistopisa in ustreznega tajnopisa razbiti) iz posameznega kroga v več krogov, dokler ne dobimo "močnejših" funkcij.

2.2 Opis algoritma enkripcije in dekripcije

Osnovni algoritem enkripcije (in dekripcije) je dolg osem krogov. Na začetku naprej razdelimo 64-bitni blok na štiri podbloke X_1, X_2, X_3 in X_4 dolžine 16 bitov. V vsakem krogu se med temi podbloki skupaj s šestimi 16-bitnimi podključi izvedejo vse tri operacije: XOR ter seštevanje in množenje po modulu. Med prehodom iz enega na drugi krog postopka se zamenjata drugi in tretji blok, razen v zadnjem (osmem) krogu. Na koncu po osmih krogih dobljene štiri podbloke še transformiramo z dodatnimi štirimi ključi tako, da dobimo končni tajnopis.

V vsakem krogu (vzemimo r-ti krog) se izvedejo v zaporedju naslednji koraki (kjer podključ $Z_j^{(r)}$ predstavlja j-ti ključ v r-tem krogu):

(1) Pomnožimo X_1 s prvim podključem $Z_1^{(r)}$.

(2) Seštejemo X_2 in drugi podključ $Z_2^{(r)}$.

(3) Seštejemo X_3 in tretji podključ $Z_3^{(r)}$.

(4) Pomnožimo X_4 s četrtim podključem $Z_4^{(r)}$.

(5) Izvedemo XOR med rezultatoma iz (1) in (3).

(6) Izvedemo XOR med rezultatoma iz (2) in (4).

(7) Pomnožimo rezultat iz (5) s petim podključem $Z_5^{(r)}$.

(8) Seštejemo rezultata iz (6) in (7).

(9) Pomnožimo rezultat iz (8) s šestim podključem $Z_6^{(r)}$.

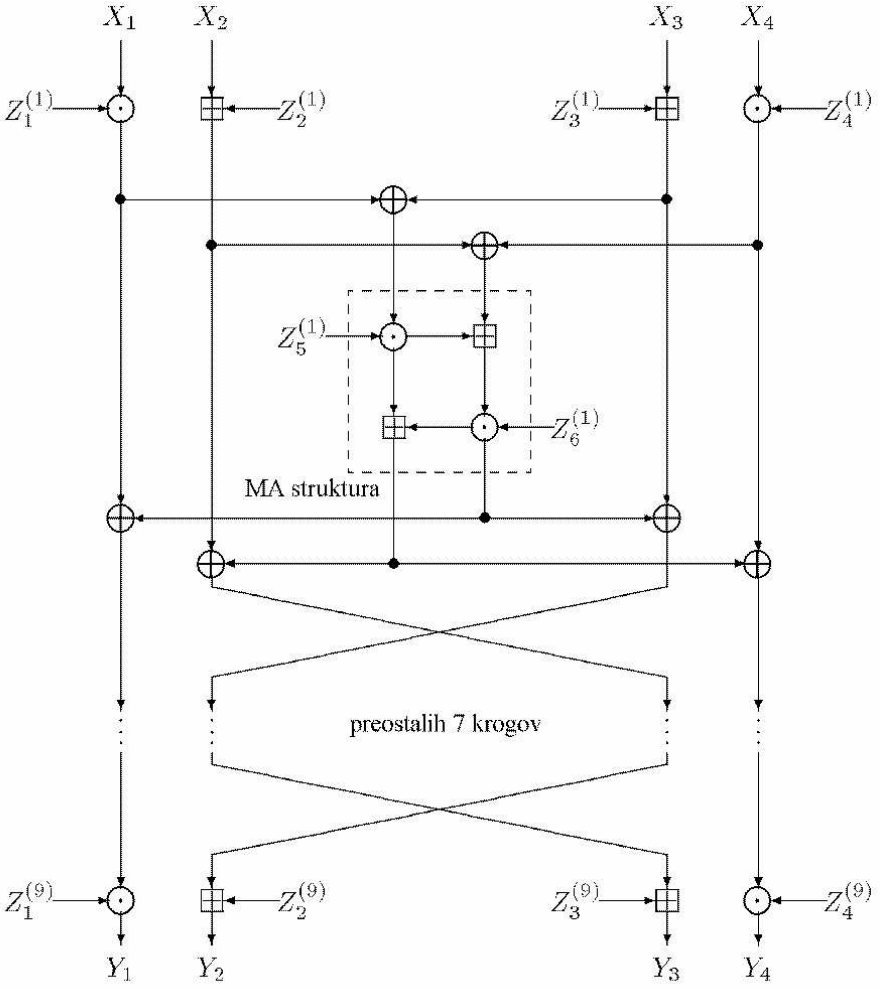
(10) Seštejemo rezultata iz (7) in (9).

(11) Izvedemo XOR med rezultatoma iz (1) in (9).

(12) Izvedemo XOR med rezultatoma iz (3) in (9).

(13) Izvedemo XOR med rezultatoma iz (2) in (10).

(14) Izvedemo XOR med rezultatoma iz (4) in (10).



Slika 1: Shema enkripcije postopka IDEE. X_i so 16-bitni podbloki čistopisa, Y_i so 16-bitni podbloki tajnopisa, $Z_i^{(r)}$ so 16-bitni podključi. $\oplus$: XOR, $\boxplus$: seštevanje po modulu 2^{16}, $\odot$: množenje po modulu $2^{16}+1$, pri tem je $0\ldots0 = 2^{16}$.

Rezultat enega kroga so podbloki iz korakov (11), (12), (13) in (14). Ti predstavljajo vhodne podbloke za naslednji krog postopka, pri čemer samo še zamenjamo podbloka iz (12) in (13). To naredimo na vsakem koraku razen na zadnjem. Zaporedje operacij izvedenih v korakih (7), (8), (9) in (10) predstavlja t.i. MA (multiplication-addition) strukturo. Slika 1 prikazuje celoten potek algoritma IDEE.

Po končani osmem krogu izvedemo še naslednjo transformacijo:

(1) Pomnožimo X_1 iz osmega kroga s prvim podključem $Z_1^{(9)}$.

(2) Seštejemo X_2 iz osmega kroga in drugi podključ $Z_2^{(9)}$.

(3) Seštejemo X_3 iz osmega kroga in tretji podključ $Z_3^{(9)}$.

(4) Pomnožimo X_4 iz osmega kroga s četrtim podključem $Z_4^{(9)}$.

Rezultat zadnje transformacije je končni tajnopis.

Kot smo že omenili se za dekripcijo uporablja isti postopek, različno je le zaporedje ključev.

Tako opisanemu postopku, ki ga sestavlja osem krogov in zadnja transformacija, pravimo osnovni postopek dolžine 8.5 krogov. Postopek IDEE pa lahko tudi reduciramo, se pravi, da zmanjšamo število krogov postopka. Potem govorimo o reduciranih postopkih štirih (štirih in pol, če je še zadnja transformacija) krogov, šestih (šestih in pol) krogov itd. Reducirani postopki IDEE so seveda zaradi tega hitrejši in hkrati manj varni.

2.3 Ključi

Iz postopka je razvidno, da uporabimo za vseh osem in pol krogov algoritma 52 podključev, in sicer šest za vsak krog ter dodatne štiri za končno transformacijo. Osnovni ključ, ki je uporabljen pri IDEI, ima dolžino 128 bitov. Ta ključ najprej razdelimo na osem 16-bitnih podključev. Tako dobimo prvih osem podključev za algoritem (šest jih uporabimo za prvi krog, preostala dva pa še za prva dva drugega kroga), preostale pa zgeneriramo po naslednjem postopku: osnovni ključ zarotiramo za 25 bitov v levo in ga zopet razdelimo na osem podključev. Prve štiri uporabimo še v drugem krogu, preostale štiri pa v tretjem. Postopek nadaljujemo tako, da zopet zarotiramo osnovni ključ za 25 bitov v levo in ga razdelimo na osem podključev. Te zopet uporabimo v nadaljnjih krogih postopka in tako ponavljamo, dokler ne dobimo vseh 52 podključev.

Pri dekripciji se uporabljajo isti že zgenerirani podključi, le da jemljemo inverzne elemente podključev za operaciji seštevanja in množenja po modulu v obratnem vrstnem redu. Ob dejstvu, da je $2^{16}+1$ praštevilo, je izpolnjen pogoj, da za vsako število med 1 in 2^{16} obstaja inverzni element za množenje po modulu $2^{16}+1$. To pa pomeni, da postopek IDEE ne moremo posplošiti na 32-bitne bloke, saj število $2^{32}+1$ ni praštevilo, zato tudi za vsa števila ne obstajajo inverzni elementi za množenje po modulu, tako da z istim postopkom ne moremo izvesti dekripcije.

V tabeli 1 so predstavljeni podključi za enkripcijo po posameznih krogih in ustrezni podključi dekripcije.

krog	podključi enkripcije	podključi dekripcije
1.	$Z_1^{(1)}\,Z_2^{(1)}\,Z_3^{(1)}\,Z_4^{(1)}\,Z_5^{(1)}\,Z_6^{(1)}$	$Z_1^{(9)-1}\;-Z_2^{(9)}\;-Z_3^{(9)}\,Z_4^{(9)-1}\,Z_5^{(8)}\,Z_6^{(8)}$
2.	$Z_1^{(2)}\,Z_2^{(2)}\,Z_3^{(2)}\,Z_4^{(2)}\,Z_5^{(2)}\,Z_6^{(2)}$	$Z_1^{(8)-1}\;-Z_2^{(8)}\;-Z_3^{(8)}\,Z_4^{(8)-1}\,Z_5^{(7)}\,Z_6^{(7)}$
3.	$Z_1^{(3)}\,Z_2^{(3)}\,Z_3^{(3)}\,Z_4^{(3)}\,Z_5^{(3)}\,Z_6^{(3)}$	$Z_1^{(7)-1}\;-Z_2^{(7)}\;-Z_3^{(7)}\,Z_4^{(7)-1}\,Z_5^{(6)}\,Z_6^{(6)}$
4.	$Z_1^{(4)}\,Z_2^{(4)}\,Z_3^{(4)}\,Z_4^{(4)}\,Z_5^{(4)}\,Z_6^{(4)}$	$Z_1^{(6)-1}\;-Z_2^{(6)}\;-Z_3^{(6)}\,Z_4^{(6)-1}\,Z_5^{(5)}\,Z_6^{(5)}$
5.	$Z_1^{(5)}\,Z_2^{(5)}\,Z_3^{(5)}\,Z_4^{(5)}\,Z_5^{(5)}\,Z_6^{(5)}$	$Z_1^{(5)-1}\;-Z_2^{(5)}\;-Z_3^{(5)}\,Z_4^{(5)-1}\,Z_5^{(4)}\,Z_6^{(4)}$
6.	$Z_1^{(6)}\,Z_2^{(6)}\,Z_3^{(6)}\,Z_4^{(6)}\,Z_5^{(6)}\,Z_6^{(6)}$	$Z_1^{(4)-1}\;-Z_2^{(4)}\;-Z_3^{(4)}\,Z_4^{(4)-1}\,Z_5^{(3)}\,Z_6^{(3)}$
7.	$Z_1^{(7)}\,Z_2^{(7)}\,Z_3^{(7)}\,Z_4^{(7)}\,Z_5^{(7)}\,Z_6^{(7)}$	$Z_1^{(3)-1}\;-Z_2^{(3)}\;-Z_3^{(3)}\,Z_4^{(3)-1}\,Z_5^{(2)}\,Z_6^{(2)}$
8.	$Z_1^{(8)}\,Z_2^{(8)}\,Z_3^{(8)}\,Z_4^{(8)}\,Z_5^{(8)}\,Z_6^{(8)}$	$Z_1^{(2)-1}\;-Z_2^{(2)}\;-Z_3^{(2)}\,Z_4^{(2)-1}\,Z_5^{(1)}\,Z_6^{(1)}$
z.t.	$Z_1^{(9)}\,Z_2^{(9)}\,Z_3^{(9)}\,Z_4^{(9)}$	$Z_1^{(1)-1}\;-Z_2^{(1)}\;-Z_3^{(1)}\,Z_4^{(1)-1}$

Tabela 1: Podključi enkripcije in dekripcije pri IDEA-i.

Iz sheme postopka na sliki 1 je razvidno, da z dekripcijo iz tajnopisa ob

uporabi takšnega vrstnega reda podključev dobimo prvoten čistopis.

2.4 Hitrost algoritma enkripcije (dekripcije)

Bistvena lastnost bločnih algoritmov je poleg varnosti tudi hitrost izvajanja enkripcije in dekripcije, saj take algoritme uporabljamo za zaščito večjih količin besedila.

Algoritem IDEE je zelo primeren za računalniško implementacijo, ker se v postopku uporabljajo 16-bitne operacije. Hitrost postopka je odvisna od implementacije samega algoritma, bodisi programske ali stojne. Strojne izvedbe postopka so praviloma hitrejše in učinkovitejše. V primerjavi z DES-om je postopek enkripcije/dekripcije pri IDEI več kot dvakrat hitrejši; implementacija algoritma IDEE z motorolinim čipom DSP 56166 v ECB načinu izvaja enkripcijo (dekripcijo) celo 3.6-krat hitrejše kot algoritem DES-a, [9].

Programske implementacije algoritma so nekoliko počasnejše. V tabeli 2 je zbranih nekaj primerjav hitrosti enkripcije (dekripcije) na različnih računalniških sistemih. Podatki so povzeti po [4] in se razlikujejo od podatkov v [11], vendar so istega vellikostnega reda.

računalnik	hitrost enkripcije
VAX 8650	430 kbits/s
486DX2-66	1.700 kbits/s
Pentium, 90 MHz	4.600 kbits/s
PentiumPro, 180 MHz	16.000 kbits/s

Tabela 2: Hitrost enkripcije/dekripcije algoritma IDEA-e na posameznih računalnikih.

Za primerjavo: na računalniku PentiumPro, 180 MHz je hitrost algoritma DES 5.500 kbits/s.

3 Napadi na IDEO

3.1 Kriptoanaliza IDEE

IDEA je zaradi dolžine ključa (128 bitov) in kombinacije treh operacij v različnih grupah v primerjavi z DES-om varnejši enkripcijski algoritem.

Sama dolžina ključa zagotavlja popolno varnost algoritma pred požrešnim napadom, saj bi s takim napadom potrebovali 2^{128} (10^{38}) enkripcij (dekripcij), da bi poiskali pravi ključ. Če bi na primer skonstruirali čip, ki bi pregledal 10^9 ključev na sekundo, bi še vedno potrebovali 10^{13} let, da bi pregledali vse ključe, kar pa je več, kot je staro naše vesolje. Če bi vzporedno uporabljali 10^{24} takih čipov, bi našli pravi ključ v enem dnevu, vendar takega stroja ni mogoče izdelati, saj ni toliko silicijevih atomov v vesolju. Zato uporabljamo druge tehnike napadov.

Ker IDEO kot simetrični bločni enkripcijski algoritem vedno primerjamo z DES-om, se podobno kot pri DES-u tudi tu uporabljajo podobne tehnike kriptoanalize: diferenčna in linearna kriptoanaliza ter napadi, ki uporabljajo metode obeh, s skupnim imenom diferenčno - linearna kriptoanaliza. Skupna

značilnost metod je, da so statistične, kar pomeni, da napadalec zbira večje količine čistopisov in ustreznih tajnopisov, ki so bili zgenerirani z istim ključem, da dobi potrebno informacijo za določitev iskanega ključa.

Diferenčno kriptoanalizo sta prva predstavila Eli Biham in Adi Shamir [1]. Bistvo napada s to tehniko je v tem, da skozi celoten postopek algoritma spremljamo, kako se tvorijo razlike (diference) parov tajnopisov pri točno izbranih razlikah parov čistopisov. Dejansko analiziramo, kaj se v enkripcijskem postopku dogaja z razliko (diferenco, ki jo dobimo z operacijo $\oplus$) dveh čistopisov. Na podlagi te informacije, potem iščemo ključ enkripcije. Natančneje izbiramo takšne diference tajnopisov in čistopisov, da je verjetnost, da za poljubno diferenco čistopisa dobimo izbrano diferenco tajnopisa, največja. Pri tem predpostavljamo, da so ključi po posameznih krogih neodvisno izbrani in enakomerno porazdeljeni. Na podlagi tako izbranih diferenc, ki jim pravimo karakteristike, dobimo ob večjih količinah čistopisa dovolj informacije za izračun posameznih ključev (ključa zadnjega kroga). Bistveni del tega napada z izbranim čistopisom je poiskati karkateristike, se pravi pare diferenc čistopisa in tajnopisa z največjo verjetnostjo. Če dan enkripcijski algoritem ustreza Markovovim tajnopisom [8] in je pripadajoča matrika verjetnosti prehodov simetrična, lahko zelo hitro najdemo takšne pare diferenc z največjo verjetnostjo. Tako so učinkovito razbili DES. Podobne lastnosti je imel tudi PES, zato so ga popravili (in preimenovali v IPES) in sicer tako, da matrika verjetnosti prehodov ni bila več simetrična [8]. Popravljena IDEA je tako imuna na takšne vrste napadov.

Druga tehnika napada je t.i. linearni napad, ki ge je leta 1993 prvi predstavil Matsui [10]. Linearni napad je prav tako statistični napad, vendar napad s poznanim čistopisom. Tu z linearnimi relacijami aproksimiramo nelinearne komponente, operacije v postopku, kot so npr. S-škatle pri DES-u ali pa množenja pri IDEI. Uporabiti moramo takšne linearne aproksimacije, da z največjo verjetnostjo opisujejo akcije, ki smo jih aproksimirali. V bistvu gre za to, da poskušamo z zaporedjem operacij, ki jih uporablja postopek enkripcije, glede na sam potek postopka, določiti zvezo med enim samim bitom (ali nekaj biti) ključa enkripcije na eni strani in biti čistopisa in pripadajočega tajnopisa na drugi strani. V splošnem je verjetnost $\frac{1}{2}$, da je ena stran linearne relacije enaka drugi strani. V samem postopku poskušamo dobiti takšno linearno zvezo, da je ta verjetnost različna od $\frac{1}{2}$. In prav to odstopanje verjetnosti od pričakovane izkoristimo za izračun bitov ključa enkripcije ob predpostavki, da imamo večje količine čistopisa in pripadajočih tajnopisov. Poudariti velja še, da čim več podatkov čistopisa in tajnopisa imamo, bolj zanesljivo uganemo ključ, oziroma čim večje je odstopanje od verjetnosti od $\frac{1}{2}$ (čim širši je pas te verjetnosti), tem bolj zanesljivo lahko uganemo ključ ob enaki količini podatkov čistopisa in tajnopisa. DES je bil razbit tudi s to tehniko napada, [10]. V naslednjih poglavjih si bomo ogledali, kako lahko uporabimo to tehniko napada pri postopku IDEE.

Pri kriptoanalizi IDEE se uporablja še ena tehnika napadov, linearno - diferenčni napadi, ki združujejo obe predhodni tehniki. Tu iščemo linearne zveze med posameznimi biti ključa in biti diferenc tajnopisa in čistopisa. Takšni napadi so bili uspešni za reducirane postopke IDEE dveh, treh in treh in pol krogov [2], vendar posplošitve takšnih napadov na osnovni postopek niso možne.

Omeniti velja še tako imenovane razrede slabih ključev pri IDEI. To pomeni, če uporabljamo take ključe, lahko z določeno tehniko znanih napadov (linerani, diferenčni napadi) razbijemo postopek IDEE. J. Daemen [3] je za 8.5 krogov IDEE našel dva razreda slabih ključev. V prvem razredu je s tehniko linearne

kriptoanalize našel razred 2^{23} slabih ključev, v drugem razredu pa se dá poiskati 2^{51} ključev, ki zadoščajo z verjetnostjo ena določeni diferenčni aproksimaciji, [3]. P. Hawkes [6] je poskal še večji razred ključev (2^{63} ključev) z uporabo diferenčno - linearnih tehnik napada. Tako je dokazal, da je v povprečju za IDEO 8.5 krogov slab eden izmed 2^{65} ključev. To pa pomeni, da kljub tem razredom slabih ključev, postopek še vedno varen, tudi če naključno izbiramo ključe enkripcije. Poleg tega pa se da postopek z nekaj modifikacijami popraviti tako, da se izognemo slabim ključem.

3.2 Linearni napad

3.2.1 Postopek napada

Kot je bilo že omenjeno, pri linearnem napadu za poljuben postopek iščemo "učinkovite" linearne aproksimacije oblike

$$P[i_1, i_2, \ldots, i_a] \oplus C[j_1, j_2, \ldots j_b] = K[k_1, k_2, \ldots, k_c], \tag{1}$$

kjer predstavljajo $i_1, i_2, \ldots, i_a, j_1, j_2, \ldots j_b$ in $k_1, k_2, \ldots, k_c$ posamezne bite čistopisa P, tajnopisa C in ključa K. Operacija $\oplus$ uporabljena v (1) je XOR. Linearna zveza (1) mora biti takšna, da je leva stran enaka desni z verjetnostjo $p \neq \frac{1}{2}$ za naključno izbran P in pripadajoči C. Odstopanje $\left|p - \frac{1}{2}\right|$ predstavlja učinkovitost linearne aproksimacije (1); večje je, boljša je aproksimacija.

Ko enkrat imamo takšno linearno zvezo, določimo bit (bite) ključa z naslednjim algoritmom. Naj predstavlja N število poznanega čistopisa. Algoritem A je:

(1) Štejemo tisti čistopis, za katerega je leva stran enačbe (1) enaka 0. Naj bo T število čistopisa, za katerega to velja.

(2) Če je $T > \frac{N}{2}$,
potem je

$$K[k_1, k_2, \ldots, k_c] = \begin{cases} 0, & \text{če } p > 1/2 \\ 1, & \text{če } p < 1/2 \end{cases},$$

sicer je

$$K[k_1, k_2, \ldots, k_c] = \begin{cases} 1, & \text{če } p > 1/2 \\ 0, & \text{če } p < 1/2 \end{cases}.$$

Problema, ki se tu pojavljata sta:

- poiskati najbolj učinkovito (optimalno) aproksimacijo (odvisno od postopka) in
- določiti stopnjo zanesljivosti linearne aproksimacije v odvisnosti od števila N in odstopanja $\left|p - \frac{1}{2}\right|$.

Linearni napad lahko še izboljšamo z uporabo t.i. kR metod. Pri $1R$ metodi uporabljamo linearno zvezo

$$P[i_1, i_2, \ldots, i_a] \oplus C[j_1, j_2, \ldots j_b] \oplus F_n(C_n, K_n)[l_1, l_2, \ldots l_d] = K[k_1, k_2, \ldots, k_c], \tag{2}$$

kjer je $F_n(C_n, K_n)$ enkripcijska funkcija zadnjega n-tega kroga postopka in C_n izhod $n-1$-vega kroga postopka ter K_n ključ v zadnjem krogu postopka. kR

metode so posplošitve $1R$ metode, tako da uporabljamo kombinacije enkripcijskih funkcij od zunaj navznoter (se pravi pri $2R$ metodi uporabimo še F_1 itd.). S tako obliko aproksimacije (2) dobimo linearne zveze za $n-1$ krogov postopka, hkrati pa povečamo število števcev, ki jih potrebujemo v algoritmu.

Algoritem B za $1R$ metodo je naslednji:

(1) Naj bo T_i število čistopisa, pri katerem je leva stran enačbe (2) enaka 0, za vsak kandidat $K_n^{(i)}$ $(i = 1, 2, \ldots)$ ključa K_n.

(2) Naj bo T_{max} maksimalno in T_{min} minimalno število izmed T_i-jev:

- Če je $|T_{max} - N/2| > |T_{min} - N/2|$, potem vzamemo tisti ključ, ki pripada T_{max} in postavimo $K[k_1, k_2, \ldots, k_c] = 0$ (če je $p > 1/2$) ali 1 (če je $p < 1/2$).
- Če je $|T_{max} - N/2| < |T_{min} - N/2|$, potem vzamemo tisti ključ, ki pripada T_{min} in postavimo $K[k_1, k_2, \ldots, k_c] = 1$ (če je $p > 1/2$) ali 0 (če je $p < 1/2$).

Pri kR metodah v bistvu zmanjšujemo število krogov postopka in s tem povečujemo učinkovitost napada, saj zmanjšamo količino čistopisa potrebnega za linearni napad. Po drugi strani pa potrebujemo več dela (več števcev) za iskanje ključev iz leve strani enačbe (2). Pri DES-u z osmimi krogi je bila za razbitje uporabljena $1R$ metoda, [10].

3.2.2 Matsuijevi lemi

Pogledali si bomo nekaj ocen in zvez, ki so bistvene za linearni napad. Obravnavali bomo primer algoritma A, torej brez uporabe kR metod.

Oceno zanesljivosti relacij v algoritmu nam poda naslednja lema:

Lema 3.1 *Naj bo N število poznanega čistopisa in p verjetnost, da linearna relacija (1) velja. Ob predpostavki, da je odstopanje $\left|p - \frac{1}{2}\right|$ dovolj majhno, lahko ocenimo zanesljivost algoritma z*

$$\int_{2\sqrt{N}\left|p-\frac{1}{2}\right|}^{\infty} \frac{1}{2\sqrt{\pi}} e^{-x^2/2} dx. \tag{3}$$

V tabeli 3 so podane zanesljivosti linearnih aproksimacij v odvisnosti od količine besedila N in odstopanja $\left|p - \frac{1}{2}\right|$.

N	$\frac{1}{4}\left\|p-\frac{1}{2}\right\|^{-2}$	$\frac{1}{2}\left\|p-\frac{1}{2}\right\|^{-2}$	$\left\|p-\frac{1}{2}\right\|^{-2}$	$2\left\|p-\frac{1}{2}\right\|^{-2}$
zanesljivost	84.1%	92.1%	97.7%	99.8%

Tabela 3: Zanesljivosti linearnih aproksimacij v odvisnosti od količine besedila N in odstopanja $\left|p - \frac{1}{2}\right|$.

Določitev učinkovitih aproksimacij (tako, da je odstopanje največje) je odvisno od samega postopka. Pri DES-u aproksimiramo S-škatle, pri IDEI, množenja. Ko enkrat določimo linearne aproksimacije za vsak krog postopka, jih združujemo skupaj. Za izračun verjetnosti združenih linearnih aproksimacij v eno samo skupno linearno zvezo uporabimo drugo Matsuijevo lemo:

Lema 3.2 *(Pilling-Up lema) Naj bodo X_i, $(1 \leq i \leq n)$, neodvisne slučajne spremenljivke, za katere velja, da je $P(X_i = 0) = p_i$ in $P(X_i = 1) = 1 - p_i$. Potem je verjetnost, da je $X_1 \oplus X_2 \oplus \ \ldots \ \oplus X_n = 0$, enaka*

$$\frac{1}{2} - 2^{n-1} \prod_{i=1}^{n} \left(p_i - \frac{1}{2} \right). \tag{4}$$

Dokaz: Dokazovali bomo s popolno indukcijo.
Za $n = 2$ je $X_1 \oplus X_2 = 0$ le, če sta $X_1 = 0$, $X_2 = 0$ ali $X_1 = 1$, $X_2 = 1$. Torej je verjetnost $P(X_1 \oplus X_2 = 0) = p_1 p_2 + (1 - p_1)(1 - p_2) = 1 - p_1 - p_2 + 2p_1 p_2$. Iz (4) pri $n = 2$ dobimo enako $\frac{1}{2} + 2\left(p_1 - \frac{1}{2}\right)\left(p_2 - \frac{1}{2}\right) = 1 - p_1 - p_2 + 2p_1 p_2$.
Predpostavimo, da (4) velja za $n - 1$. Verjetnost $P(X_1 \oplus \ldots \oplus X_n = 0) = P(X_n = 0)\, P(X_1 \oplus \ldots \oplus X_{n-1} = 0) + P(X_n = 1)\, P(X_1 \oplus \ldots \oplus X_{n-1} = 1)$, ker so spremenljivke X_i neodvisne. Tako potem dobimo

$$\begin{aligned}
& P(X_1 \oplus \ldots \oplus X_n = 0) \\
= \ & P(X_n = 0)\, P(X_1 \oplus \ldots \oplus X_{n-1} = 0) + P(X_n = 1)\, P(X_1 \oplus \ldots \oplus X_{n-1} = 1) = \\
= \ & p_n \left(\frac{1}{2} + 2^{n-2} \prod_{i=1}^{n-1} \left(p_i - \frac{1}{2} \right) \right) + (1 - p_n) \left(\frac{1}{2} - 2^{n-2} \prod_{i=1}^{n-1} \left(p_i - \frac{1}{2} \right) \right) = \\
= \ & \frac{1}{2} - 2^{n-2} \prod_{i=1}^{n-1} \left(p_i - \frac{1}{2} \right) + \left(p_n - \frac{1}{2} + \frac{1}{2} \right) 2^{n-1} \prod_{i=1}^{n-1} \left(p_i - \frac{1}{2} \right) = \\
= \ & \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \left(p_i - \frac{1}{2} \right).
\end{aligned}$$

S tem pa je dokaz končan. ■

Spremenljivke X_i iz druge leme si moramo predstavljati kot linearne aproksimacije za posamezen krog postopka. Tako lahko ob predpostavki, da so te aproksimacije med seboj neodvisne, uporabimo zgornjo lemo za izračun odstopanja verjetnosti linearne zveze od $\frac{1}{2}$.

Poglejmo si še primer linearnega napada na DES dolžine 3 krogov.

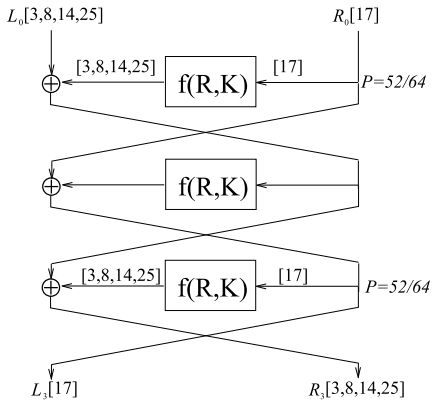
Primer 3.1 *Škatla S_5 pri DES-u je najbolj občutljiva točka pri linearnem napadu, saj je za več linearnih aproksimacij odstopanje od $\frac{1}{2}$ največje, [10]. Vzemimo linearno aproksimacijo za i-ti krog*

$$K_i[26] = 1 \oplus R_{i-1}[17] \oplus L_{i-1}[3, 8, 14, 25] \oplus R_i[3, 8, 14, 25].$$

Verjetnost takšne relacije je $p = \frac{52}{64}$ in izhaja iz nelinearnosti S_5-škatle. S-škatle so tudi edine nelinearne zveze pri postopku DES-a. Ker zgornja linearna aproksimacija velja za vsak krog postopka, tako združimo aproksimaciji iz prvega in tretjega kroga v skupno linearno zvezo

$$K_1[26] \oplus K_3[26] = R_0[17] \oplus L_3[17] \oplus L_0[3, 8, 14, 25] \oplus R_3[3, 8, 14, 25].$$

Potek postopka in združevanja je prikazan na sliki 2.
Verjetnost linearne zveze izračunamo (lahko iz Pilling-Up leme ali pa direktno) in je $\left(\frac{52}{64}\right)^2 + \left(\frac{12}{64}\right)^2 \approx 0.695$. Na koncu moramo še preveriti ali je desna stran linearne zveze enaka ena za več kot $\frac{N}{2}$ čistopisa ali ne. Če je, potem postavimo $K_1[26] \oplus K_3[26] = 1$, sicer pa je $K_1[26] \oplus K_3[26] = 0$.
Za 98% zanesljivost linearne aproksimacije, potrebujemo v našem primeru treh krogov DES-a 26 poznanega čistopisa.



Slika 2: Primer linearnega napada na DES dolžine treh krogov.

3.3 Linearni napad na IDEO

3.3.1 Uvod

V naslednjih poglavjih si bomo pogledali, kako lahko uporabimo linearne tehnike napadov pri IDEI dolžine R krogov. Tu se ne bomo omejili samo na 16-bitne podbloke, ampak bomo problem zastavili splošneje, in sicer bomo uporabljali operacije množenja po modulu $2^m + 1$ in seštevanja po modulu 2^m za ustrezne dolžine podblokov, kjer je $m \in \{4, 8, 16\}$. Tako se ob enkratni uporabi postopka IDEE zakodira $n = 4m$ (16, 32 ali 64) bitov čistopisa.

Izvedba linearnega napada na IDEO je težja kot pri DES-u zaradi naslednjih razlogov:

- nelinearne operacije, ki jih želimo aproksimirati so odvisne od izbire ključev (pri DES-u ni tako),
- tudi podključe, ki jih uporabljamo v postopku, generiramo z nelinearnimi operacijami (rotacije za 25 bitov v levo),
- rezultat aproksimirane operacije je hkrati vhod druge operacije, ki jo aproksimiramo v istem krogu, tako da ne moremo brez dodatnih privzetkov uporabljati Pilling-Up leme, ki bi nam zagotovila izračun odstopanja verjetnosti od $\frac{1}{2}$.

Bistvo našega napada bo čimboljša aproksimacija operacij množenja po modulu, saj je seštevanje že linearna operacija. Poiskali bomo takšne linearne operacije, s katerimi bomo aproksimirali operacije množenja z veliko verjetnostjo, operacije seštevanja pa z verjetnostjo ena. Tako bomo sestavili linearno aproksimacijo med čistopisom in tajnopisom, ki bo optimalna, ko bomo uporabili minimalno število aproksimacij za množenje. Najprej bomo izračunali, koliko operacij množenja moramo aproksimirati pri R krogih postopka. Nadalje pa bomo določili najbolj optimalne aproksimacije in pokazali učinkovitost linearnega napada.

3.3.2 Linearne aproksimacije

Predpostavimo, da je R število vseh krogov IDEE, kjer $R+1$ -vi krog označuje zadnjo transformacijo postopka. Označimo še delne tajnopise na začetku r-tega

kroga postopka s $C^{(r)} = C_1^{(r)}C_2^{(r)}C_3^{(r)}C_4^{(r)}$, kjer $C_i^{(r)}$ predstavljajo podbloke dolžine m. Tako je čistopis enak $X = C^{(1)}$, tajnopis pa $Y = C^{(R+2)}$. Za osnovni postopek IDEE, kjer je $R = 8$, velja $X = C^{(1)}$ in $Y = C^{(10)}$.

V r-tem krogu bomo predstavili linearne aproksimacije oblike

$$\alpha^{(r)} \cdot C^{(r)} + \alpha^{(r+1)} \cdot C^{(r+1)} = 0, \tag{5}$$

kjer je $\alpha^{(r)} = \alpha_1^{(r)}\alpha_2^{(r)}\alpha_3^{(r)}\alpha_4^{(r)}$ za $1 \leq r \leq R+1$, $\alpha^{(r)}, \alpha^{(r+1)} \in \mathbb{Z}_2^n$ in je $\alpha_i^{(r)} \cdot C_i^{(r)} = \sum_{j=0}^{m} \alpha_i^{(r)}[j]\, C_i^{(r)}[j] \pmod 2$ skalarni produkt po bitih ustreznih podblokov. Koeficiente $\alpha^{(r)}$ lahko obravnavamo kot bitne maske. Operacija seštevanja v linearni aproksimaciji (5) je po modulu 2. Omenimo še, da ta linearna aproksimacija vsebuje ključ(-e) iz r-tega kroga v $C^{(r+1)}$.

Definirajmo še linearne relacije po posameznih krogih postopka in linearne zveze tvorjene iz teh relacij.

Definicija 3.1 *Linearno relacijo (round association) $RA_{u,v}^{(r)}$ v r-tem krogu postopka definiramo kot*

$$RA_{u,v}^{(r)} = \left(a_1^{(r)}, a_2^{(r)}, a_3^{(r)}, a_4^{(r)}\right) \overset{M_r, A_r}{\longrightarrow} \left(b_1^{(r)}, b_2^{(r)}, b_3^{(r)}, b_4^{(r)}\right), \tag{6}$$

kjer je $a_i^{(r)}, b_i^{(r)} \in \{0,1\}$ in $u = \sum_{i=1}^{4} a_i^{(r)} \cdot 2^{4-i}$, $v = \sum_{i=1}^{4} b_i^{(r)} \cdot 2^{4-i}$. Bitno število $a_i^{(r)}$ ($b_i^{(r)}$) predstavlja i-ti vhodni (izhodni) blok posameznega kroga, ki smo ga uporabili v linearni relaciji, kjer smo uporabili M_r aproksimacij operacije $\odot$ in A_r aproksimacij operacije $\boxplus$.

Tako predstavlja npr. linearna relacija $RA_{10,12}^{(r)} = (1,0,1,0) \overset{1,1}{\longrightarrow} (1,1,0,0)$ aproksimacijo med prvim in tretjim vhodnim blokom r-tega kroga in prvim in drugim izhodnim blokom, kjer smo uporabili eno operacijo množenja in eno operacijo seštevanja po modulu.

V tabeli 4 so predstavljene vse možne linearne relacije po posameznem krogu, ki vsebujejo samo eno aproksimacijo množenja.

Linearne relacije so enake za vsak krog. Razlika je le v zadnji transformaciji. Linearno relacijo za aproksimacijo zadnje transformacije označimo s $TA_{u,v}^{(R+1)}$, predstavlja pa zvezo $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \overset{M_{R+1}, A_{R+1}}{\longrightarrow} (\alpha_1, \alpha_3, \alpha_2, \alpha_4)$.

Zaporedje linearnih relacij po posameznih krogih skupaj z linearno relacijo iz zadnje transformacije združimo v eno samo linearno aproksimacijo, ki predstavlja linearno zvezo med čistopisom in tajnopisom. V ta namen definiramo združljivost dveh linearnih relacij.

Definicija 3.2 *Linearni relaciji RA_{u_1,v_1} in RA_{u_2,v_2} sta združljivi (kompatibilni), če velja $v_1 = u_2$. To zapišemo simbolno kot $RA_{u_1,v_1} \longrightarrow RA_{u_2,v_2}$.*

Združene linearne relacije, ki so med seboj kompatibilne, predstavljajo linearno aproksimacijo za celoten postopek in jim pravimo linearne zveze.

Definicija 3.3 *Za IDEO z R krogi definiramo simbolno linearno zvezo kot $LA_{u,v} = (a_1, a_2, a_3, a_4) \overset{M,A}{\longrightarrow} (b_1, b_2, b_3, b_4)$. Zveza predstavlja množico R lineranih relacij $\left\{RA_{u_r,v_r}^{(r)} \mid 1 \leq r \leq R\right\}$ in aproksimacijo zadnje transformacije $TA_{u_{R+1},v_{R+1}}^{(R+1)}$, za katere velja*

$$RA_{u,v_1}^{(1)} \longrightarrow RA_{v_1,v_2}^{(2)} \longrightarrow \ \ldots \ \longrightarrow RA_{v_{R-1},v_R}^{(R)} \longrightarrow TA_{v_R,v}^{(R+1)}, \tag{7}$$

kjer je $u = u_1$, $v = v_{R+1}$ *in* $M = \sum_{r=1}^{R} M_r$, $A = \sum_{r=1}^{R} A_r$. *Linearna zveza za* R *krogov postopka IDEE je optimalna, ko je* M *najmanjši.*

ena aproksimacija $\odot$ za posamezen krog		pogoji
$RA_{4,1}$	$(0,1,0,0) \xrightarrow{1,3} (0,0,0,1)$	
$RA_{4,3}$	$(0,1,0,0) \xrightarrow{1,3} (0,0,1,1)$	$\alpha_3^{(r+1)} \neq \alpha_4^{(r+1)}$
$RA_{5,3}$	$(0,1,0,1) \xrightarrow{1,1} (0,0,1,1)$	$\alpha_3^{(r+1)} = \alpha_4^{(r+1)}$
$RA_{6,5}$	$(0,1,1,0) \xrightarrow{1,4} (0,1,0,1)$	
$RA_{6,7}$	$(0,1,1,0) \xrightarrow{1,4} (0,1,1,1)$	$\alpha_3^{(r+1)} \neq \alpha_4^{(r+1)}$
$RA_{6,10}$	$(0,1,1,0) \xrightarrow{1,3} (1,0,1,0)$	
$RA_{6,14}$	$(0,1,1,0) \xrightarrow{1,3} (1,1,1,0)$	$\alpha_1^{(r+1)} \neq \alpha_2^{(r+1)}$
$RA_{10,12}$	$(1,0,1,0) \xrightarrow{1,1} (1,1,0,0)$	$\alpha_1^{(r+1)} = \alpha_2^{(r+1)}$
dve aproksimaciji $\odot$ za posamezen krog		
$RA_{3,6}$	$(0,0,1,1) \xrightarrow{2,3} (0,1,1,0)$	
$RA_{7,5}$	$(0,1,1,1) \xrightarrow{2,4} (0,1,0,1)$	
$RA_{7,6}$	$(0,1,1,1) \xrightarrow{2,4} (0,1,1,0)$	ni pogojev
$RA_{12,6}$	$(1,1,0,0) \xrightarrow{2,2} (0,1,1,0)$	
$RA_{14,6}$	$(1,1,1,0) \xrightarrow{2,3} (0,1,1,0)$	
$RA_{14,10}$	$(1,1,1,0) \xrightarrow{2,3} (1,0,1,0)$	

Tabela 4: Prva skupina RA-jev predstavlja eno aproksimacijo operacije množenja na vsak krog. Druga skupina RA-jev so vsi taki, ki so kompatibilni s prvo skupino, in sicer tako, da velja $RA_{u_1,v_1} \longrightarrow RA_{u_2,v_2} \longrightarrow RA_{u_3,v_3}$, kjer sta RA_{u_1,v_1} in RA_{u_3,v_3} iz prve skupine, RA_{u_2,v_2} pa iz druge.

Kot primer vzemimo linerano zvezo $LA_{6,10} = (0,1,1,0) \overset{11,17}{\longmapsto} (1,0,1,0)$, ki pove, da obstaja linearna aproksimacija med drugimi in tretjimi podbloki čistopisa in prvimi in tretjimi podbloki tajnopisa, za katero potrebujemo 11 aproksimacij operacije množenja $\odot$ in 17 aproksimacij operacije seštevanja $\boxplus$ po modulu.

Iz tabele 4 je razvidno, da v posameznem krogu postopka ne moremo dobiti tri združljive linearne relacije, ki bi ustrezale pogoju, da z vsako aproksimiramo samo eno množenje. To pomeni, da v treh krogih postopka ne moremo aproksimirati na vsakem krogu samo eno operacijo množenja (torej skupaj tri), ampak moramo v treh krogih aproksimirati vsaj štiri množenja. Tako velja naslednji izrek.

Izrek 3.1 *Za* R *krogov postopka IDEE potrebujemo za linearne aproksimacije oblike* $\alpha \cdot X + \beta \cdot Y + \gamma \cdot Z = 0$, *kjer so* X *čistopis,* Y *tajnopis in* Z *ključi, vsaj* $R + \lfloor \frac{R}{3} \rfloor + [R \neq 0 \mod 3]$ *linearnih aproksimacij množenja po modulu, kjer predstavlja* [.] *logično spremenljivko vrednosti* 0 *ali* 1.

Dokaz: (skica dokaza) V treh krogih postopka IDEE potrebujemo v lineranih relacijah vsaj 4 aproksimacije množenj po modulu. Če je število R deljivo s

tri, potem ne potrebujemo še dodatne aproksimacije množenja za zadnjo transformacijo. ■

Po izreku tako za IDEO dolžine 8 krogov potrebujemo vsaj 11 aproksimacij množenja po modulu. Linearnim zvezam, pri katerih potrebujemo natanko 11 aproksimacij množenja, pravimo optimalne. Koliko takšnih optimalnih linearnih zvez lahko dobimo iz lineranih relacij iz posameznih krogov, pove naslednja lema:

Lema 3.3 *Število linearnih aproksimacij (zvez) za postopek IDEE dolžne R krogov je*

$$\lambda(R) = \begin{cases} 2^{\lfloor \frac{R}{3} \rfloor}, & \text{če } R \equiv 0 \bmod 3 \\ 8 \cdot 2^{\lfloor \frac{R}{3} \rfloor}, & \text{če } R \equiv 1 \bmod 3 \\ 9 \cdot 2^{\lfloor \frac{R}{3} \rfloor}, & \text{če } R \equiv 2 \bmod 3 \end{cases}$$

V tabeli 5 je prikazano nekaj optimalnih linearnih zvez $LA_{u,v}$ za 8 krogov IDEE. Podane so izbrane linearne zveze oblike kot v (7) z $R+2$ -terico $(u, v_1, v_2, \ldots, v_{R-1}, v_R, v)$.

$LA_{5,6}$	$(0,1,0,1) \overset{11,18}{\longmapsto} (0,1,1,0)$	$(5,3,6,10,12,6,10,12,6,6)$
$LA_{6,4}$	$(0,1,1,0) \overset{11,20}{\longmapsto} (0,1,0,1)$	$(6,10,12,6,10,12,6,5,2,4)$
$LA_{6,5}$	$(0,1,1,0) \overset{11,18}{\longmapsto} (0,1,0,1)$	$(6,10,12,6,10,12,6,5,3,5)$
$LA_{6,6}$	$(0,1,1,0) \overset{11,20}{\longmapsto} (0,1,1,0)$	$(6,14,6,10,12,6,10,12,6,6)$
$LA_{6,10}$	$(0,1,1,0) \overset{11,17}{\longmapsto} (1,0,1,0)$	$(6,10,12,6,10,12,6,10,12,10)$
$LA_{10,6}$	$(1,0,1,0) \overset{11,17}{\longmapsto} (0,1,1,0)$	$(10,12,6,10,12,6,10,12,6,6)$

Tabela 5: Nekaj izbranih optimalnih linearnih zvez za 8 krogov IDEE.

Osnovni linearni napad na IDEO lahko razširimo na aproksimacije oblike

$$\alpha \cdot X + \beta \cdot Y + \delta_1 \cdot F(Z_1) + \delta_R \cdot F(Z_R) + \gamma \cdot Z = 0, \tag{8}$$

kjer predstavljaja $F(Z_1)$ funkcijo ključev na izhodu prvega kroga in $F(Z_R)$ funkcijo ključev na izhodu zadnjega kroga pred zadnjo transformacijo. V primeru, ko je eden izmed δ_1 ali δ_R različen od nič, govorimo o $1R$-metodi, ko pa sta oba različna od nič pa o $2R$-metodi. Osnovni linearni napad lahko še razširmo na kR-napade z namenom zmanjšati število aproksimacij za posamezen krog postopka, vendar se hkrati poveča delo za požrešno iskanje podključev iz posameznih krogov. O številu aproksimacij za kR-metodo govori naslednja posledica:

Posledica 3.1 *Za R krogov postopka IDEE potrebujemo za vsako linearno aproksimacijo, kjer uporabljamo kR-metodo, vsaj $(R-k) + \lfloor \frac{R-k}{3} \rfloor$ aproksimacij množenj po modulu.*

Toda za iskanje podključev, ki nastopajo v kR-napadu, potrebujemo dodatnih 2^{16k} števcev. Zato si izbiramo manjše k-je ($k = 1$ ali $k = 2$).

3.3.3 LSB aproksimacije

Za uspešno izvedbo linearnega napada potrebujemo učinkovite linearne aproksimacije. To so takšne aproksimacije, da je odstopanje $\left|p - \frac{1}{2}\right|$ največje. Pri IDEI pa moramo upoštevati še dejstvo, da linearne relacije niso nujno neodvisne med seboj. Zato si je potrebno, če hočemo za izračun odstopanja uporabiti Pilling-Up lemo, izbrati takšne linearne aproksimacije, ki bodo zadostile zahtevam linearnega napada.

Primer takšnih aproksimacij so *LSB (least significant bit) aproksimacije* operacije $\odot$ oblike

$$1 \cdot X + 1 \cdot (X \odot Z) = 0, \tag{9}$$

kjer je X število pred operacijo in $X \odot Z$ število po izvedbi operacije $\odot$. Število 1 je bitna maska in pomeni, da vzamemo zadnji bit (least significant bit) obeh števil iz (9) ter ju seštejemo z operacijo + po modulu 2. V našem primeru predstavlja X blok delnega tajnopisa, ki ga množimo z operacijo množenja po modulu $\odot$ s podključem Z iz posameznega kroga postopka.

LSB aproksimacije, s katerimi aproksimiramo seštevanja in množenja po modulu pri IDEI, so optimalne linearne aproksimacije, ker aproksimirajo množenja z največjo verjetnostjo, seštevanja pa z verjetnostjo ena, [5]. Zaradi te lastnosti lahko uporabimo tudi Pilling-Up lemo za izračun odstopanja, saj dobimo ob privzetku, da so ključi neodvisni in enakomerno porazdeljeni, neodvisne linearne relacije. To pa zato, ker aproksimacije operacije seštevanja veljajo z verjetnostjo ena in zato ne povzročijo soodvisnosti aproksimacij.

Po [5] lahko izračunamo povprečno odstopanje LSB aproksimacije za množenje pri IDEI.

Lema 3.4 *(po [5]) Povprečno odstopanje verjetnosti LSB aproksimacije za množenje pri IDEI, definirano kot*

$$p_n^* = \sum_{Z \in \mathbb{Z}_2^m} \left| \left(2^{-m} \cdot \sum_{X \in \mathbb{Z}_2^m} [1 \cdot X + 1 \cdot (X \odot Z)] \right) - \frac{1}{2} \right|,$$

pri čemer je $n = 4m$, *je za* $n = 16, 32, 64$ *enako* $p_{16}^* = 2^{-3}$, $p_{32}^* = 2^{-5.73}$ *in* $p_{64}^* = 2^{-11.48}$.

Ker lahko uporabimo Pilling-Up lemo, izračunamo povprečno odstopanje (4) linearne zveze (7) , ki jo dobimo iz LSB aproksimacij, po naslednjem izrazu

$$2^{T-1} \prod_{i=1}^{T} (p_i - 1), \tag{10}$$

kjer je $p_i = p_n^*$ za vsak i in $T = R + \left\lfloor \frac{R}{3} \right\rfloor + [R \neq 0 \mod 3]$ število aproksimacij množenja po izreku 3.1. Tako je za 8 krogov IDEE ob privzetku, da so ključi neodvisni in enakomerno porazdeljeni, povprečno odstopanje optimalnih linearnih aproksimacij oblike $\alpha \cdot P + \beta \cdot C + \gamma \cdot Z = 0$ za $n = 16, 32, 64$ zaporedoma enako 2^{-23}, $2^{-53.1}$ in $2^{-116.3}$.

Iz tabele 3 lahko ugotovimo, da potrebujemo za zanesljivost aproksimacij približno $\left|p - \frac{1}{2}\right|^{-2}$ čistopisa, kar v našem primeru pomeni, da linearni napad za osnovni postopek IDEE ni učinkovit, saj potrebujemo celo več čistopisa, kot bi ga, če bi hoteli razbiti postopek s požrešnim napadom, kar je lepo razvidno iz tabele 6.

št. krogov R	2	3	4	5	6	7	8
št. aproksimacij T	3	4	6	7	8	10	11
odstopanje $\left\|p-\frac{1}{2}\right\|$	$2^{-32.4}$	$2^{-42.9}$	$2^{-63.9}$	$2^{-74.4}$	$2^{-84.8}$	$2^{-105.8}$	$2^{-116.3}$
št. podatkov $\left\|p-\frac{1}{2}\right\|^{-2}$	$2^{64.8}$	$2^{85.8}$	$2^{127.8}$	$2^{148.8}$	$2^{169.6}$	$2^{211.6}$	$2^{232.6}$

Tabela 6: Število čistopisa potrebnega za razbitje IDEE z linearnim napadom za $n = 64$. Linerani napad z LSB aprokimacijami ni učinkovit že za $R > 4$.

3.3.4 Možnost razbitja IDEE z linearnim napadom

Kljub temu da linearni napad z LSB aproksimacijami za osnoven postopek IDEE v splošnem ni učinkovit, lahko uporabimo rezultate, da poiščemo deleže ključev, za katere lahko uspešno izvedemo tak napad. Poiskali bomo delež ključev za osnovni postopek IDEE z osmimi krogi za $n = 16, 32, 64$, kjer bomo uporabili 11 LSB aproksimacij za množenje.

V ta namen bomo uporabili generativne funkcije, ki so za aproksimacije $\alpha \cdot X + \beta \cdot (X \odot Z) = 0$, oblike

$$F_{\alpha,\beta,n}(x) = \left(\sum_{Z \in \mathbb{Z}_2^n} \frac{1}{2^m} x^{\log_2(p(\alpha,\beta,Z))} \right)^{11} = \left(\sum_{0<q<\frac{1}{2}} a_q x^{\log_2(q)} \right)^{11}, \qquad (11)$$

kjer je $p(\alpha,\beta,Z) = \left| P(\alpha \cdot X + \beta \cdot (X \odot Z) = 0) - \frac{1}{2} \right|$. Koeficienti a_q predstavljajo deleže ključev Z, za katere velja $p(\alpha,\beta,Z) = q$. Ko zapišemo vsoto iz (11) v obliki polinoma, dobimo člene oblike fx^q, kjer predstavljajo koeficienti f deleže ključev, za katere velja

$$\sum_{i=1}^{11} \log_2 p(\alpha,\beta,Z_i) = q, \qquad (12)$$

kjer je Z_i podključ, ki smo ga uporabili v i-ti aproksimaciji.

Z uporabo Pilling-Up leme in ocene iz tabele 3 lahko ugotovimo, da linearen napad ni učinkovit, če velja

$$\left| p - \frac{1}{2} \right|^{-2} = \left| 2^{10} \cdot \prod_{i=1}^{11} p(\alpha,\beta,Z_i) \right|^{-2} \geq 2^n \iff \sum_{i=1}^{11} \log_2 p(\alpha,\beta,Z_i) \leq -\frac{n}{2} - 10. \qquad (13)$$

Tako dobimo delež ključev, za katere lahko uporabimo linearen napad z LSB aproksimacijami, tako da seštejemo koeficiente f v členih fx^q generativne funkcije $F_{1,1,n}$, za katere velja $q \geq -\frac{n}{2} - 10$.

Polinomom generativnih funkcij $F_{\alpha,\beta,n}$, katerim odvzamemo člene s potencami $q < -\frac{n}{2} - 10$, pravimo reducirani polinomi in jih označimo z $F^*_{\alpha,\beta,n}$. Tako lahko npr. z generativno funkcijo $F^*_{1,1,n}(1)$ izračunamo uspeh linearnega napada z LSB aproksimacijami $1 \cdot X + 1 \cdot (X \odot Z) = 0$ za osem korgov IDEE.

V primeru, ko je $n = 16$, dobimo po [5] za osem krogov IDEE generativno funkcijo oblike

$$F_{1,1,16}(x) = \left(\frac{1}{2} x^{-3} + \frac{1}{8} x^{-1} \right)^{11}.$$

Ob upoštevanju pogoja $q \geq -18$, je reducirani polinom naslednje oblike

$$F^*_{1,1,16}(x) = \frac{1.164}{10^{10}}x^{-12} + \frac{5.122}{10^9}x^{-14} + \frac{1.024}{10^7}x^{-16} + \frac{1.229}{10^6}x^{-18}.$$

Delež ključev, za katere je linearen napad uspešen, je $F^*_{1,1,16}(1) = 1.337 \cdot 10^{-6} = 2^{-19.5}$. To pomeni, da je možnost približno ena proti milijon, da z linearnim napadom razbijemo postopek IDEE osmih krogov za $n = 16$. Podobno lahko izračunamo polinome $F_{1,1,32}$ in $F_{1,1,64}$, tako da lahko pokažemo naslednjo lemo:

Lema 3.5 *Linearni napad z LSB aproksimacijami za osem krogov IDEE ob predpostavki, da so ključi nedovisni in enakomerno porazdeljeni, je uspešen pri* $n = 16, 32, 64$ *zaporedoma za naslednje deleže ključev* $2^{-19.2}$, $2^{-45.9}$, $2^{-100.8}$.

Ob dejstvu, da so LSB aproksimacije zaradi svojih lastnosti ene izmed boljših aproksimacij za linearen napad, lahko ugotovimo, da je ta tehnika sorazmerno neučinkovita za osnoven (8.5 krogov) postopek IDEE. Lahko pa jo uporabimo za reducirane postopke in postopke z manjšimi dolžinami osnovnih blokov, kjer uporabimo kombinacije linearno - diferenčnih napadov. Na žalost pa so ti napadi zelo specifični, tako da jih je praktično nemogoče razširiti na osnoven postopek.

4 Sklep

Enkripcijski algoritem IDEE je eden izmed najobetavnejših bločnih algoritmov. Prepletanje treh operacij iz različnih grup v vsakem krogu postopka zagotavlja večjo varnost in enostavno izvedbo postopka. Poleg varnosti pa je ravno zaradi svojih lastnosti hitrost enkripcije in dekripcije v primerjavi s sorodnimi postopki večja. Kljub temu, da je postopek mlajši in manj razširjen od primerljivih sistemov (DES), je sorazmerno varen pred znanimi tehnikami napadov.

Vse te lastnosti pa zagotavljajo IDEI vodilno mesto med simetričnimi bločnimi enkripcijskimi algoritmi.

Literatura

[1] E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[2] J. Borst, L. R. Knudsen, V. Rijmen, *Two Attacks on Reduced IDEA (Extended Abstract)*, Proc. Eurocrypt '97, LNCS 1233, W. Fummy, Ed., Springer-Verlag, 1997, pp. 1 -13.

[3] J. Daemen, R. Govaerts, J. Vandewalle, Weak Keys of IDEA, v Advances in Cryptology, Proc. Crypto '93, LNCS 773, D.R. Stinson, Ed., Springer-Verlag, 1994, pp. 224-231.

[4] Entrust Technologies Europe, URL:*http://www.r3.ch/products/idea/index.html*

[5] P. Hawkes, L. O'Connor, *On Applying Linear Cryptanalysis to IDEA*, v Advances in Cryptology, Proc. AsiaCrypt '96, LNCS 1163, K. Kim, T. Matsumoto, Ed., Springer-Verlag, 1996, pp. 105-115.

[6] P. Hawkes, *Differential - Linear Weak Key Classes of IDEA*, Proc. Eurocrypt '98, LNCS 1403, K. Nyberg, Ed., Springer-Verlag, 1998, pp. 112-126.

[7] X. Lai, J. L. Massey, *A Proposal for a New Block Encryption Standard*, Advances in Cryptology, Proc. Eurocrypt '90, pp. 389-404.

[8] X. Lai, J. L. Massey, S. Murphy, *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology, Proc. Eurocrypt '91, D. W. Davies, Ed. Springer-Verlag, 1991, pp. 17-38.

[9] T. R. Madhusudan Sastry, T. Ganesan, B. Madhukar, N. Srinivasa, *Time is right for a good, secure 'Idea'*, Electronic Engineering Times, October 1995.

[10] M. Matsui, *Linear Cryptanlysis Method for DES Cipher*, v Advances in Cryptology, Proc. Eurocrypt '93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1993, pp. 386-397.

[11] B. Schneier, *Applied Cryptography*, second edition, John Wiley & Sons, 1996, pp. 319-325.