UNIVERSITAT DE BARCELONA

Treball final del grau de matemàtiques

Facultat de Matemàtiques i Informàtica

UN ESTUDI DE LA CRIPTOANÀLISI DIFERENCIAL I DE LA CRIPTOANÀLISI LINEAL

Eric Santiño Cervera

Dirigit per: Artur Travesa Grau

Departament de Matemàtiques i Informàtica

Barcelona, gener de 2018

Abstract

To analyze the security of block ciphers, several methods are used, including primarily linear and differential cryptanalysis. The goal in this dissertation is to study and understand how these cryptographic attacks work, as well as understanding how they can be used for the practical testing of security in this kind of cryptosystems.

Resum

Per a analitzar la seguretat dels criptosistemes de xifrat en bloc, es fan servir diferents mètodes, entre els quals hi ha primordialment la criptoanàlisi lineal i la criptoanàlisi diferencial. L'objectiu d'aquest treball és estudiar i entendre el funcionament teòric d'aquests atacs criptogràfics, així com també comprendre'n bé la seva utilitat per a la comprovació pràctica de la seguretat d'aquests criptosistemes.

Agraïments

Aquest treball no hauria estat possible sense l'ajuda de diverses persones.

En primer lloc m'agradaria agrair al meu tutor, Artur Travesa, per la seva paciència i dedicació durant el procés de creació i revisió del treball, així com per guiar-me quan m'ha fet falta.

Vull agrair també a la meva germana, pel seu suport quan estava estressat pel treball, a més del seu consell en innumerables qüestions.

Finalment, vull agrair al doctor Howard Heys, atès que sense el seu tutorial sobre la criptoanàlisi diferencial i sobre la criptoanàlisi lineal amb m'hauria estat molt més difícil entendre aquests conceptes i dur a bon terme el treball.

Contingut

Introducció

"La criptografia canvia el balanç de poder entre el monopoli de la violència i aquells que comprenen les matemàtiques i el disseny de la seguretat." – Jacob Appelbaum (informàtic teòric)

Des dels temps de l'antiga Mesopotàmia, la criptografia ha estat una de les eines més rellevants per a salvaguardar la confidencialitat de la informació, una necessitat que ha estat rellevant al llarg de la història i que avui dia, en un món completament interconnectat i digitalitzat, ho és més que mai.

La necessitat de salvaguardar informació privada o de caràcter secret és tant important com fràgil: cal tenir molta cura que el mètode emprat no es pugui vulnerar, o en cas contrari ens arrisquem que aquesta informació que volem guardar en secret deixi d'ésser segura. L'estudi de la seguretat criptogràfica és la força motriu que impulsa aquest treball, en el qual estudiarem dos dels atacs criptogràfics més coneguts: la criptoanàlisi diferencial, i la criptoanàlisi lineal. Aquests atacs són d'especial interès ja que van ésser dissenyats per a trencar els criptosistemes de xifrat en bloc, un tipus de criptosistema molt rellevant perquè molts estàndards internacionals de seguretat han estat xifrats en bloc.

El treball s'estructura de la manera següent: comença amb una exposició bàsica de què és un criptosistema i com es classifiquen, per a donar pas a l'introducció dels xifrats en bloc com a resultat de diferents idees que han proliferat al llarg de la història de la criptografia. Acabada aquesta introducció de conceptes bàsics, el treball explica en profunditat els atacs diferencial i lineal, on efectua a més a més una anàlisi de la seguretat que pot tenir un criptosistema donat contra aquests atacs. Finalment, es conclou el treball amb un exemple d'aplicació pràctica d'un d'aquests atacs contra un criptosistema real.

1 Criptografia i criptoanàlisi

1.1 Criptosistemes

Definició 1.1.1. *Sigui $\mathcal{A}$ un conjunt finit totalment ordenat que denominarem* ***l'alfabet****. Definim un* ***xifratge criptogràfic*** *en un alfabet $\mathcal{A}$ com:*

$$\begin{aligned} e\colon \mathcal{A}^m &\to \mathcal{A}^n \quad \text{per a certs } m,n \in \mathbb{N} \text{ on } n \geq m \\ P &\mapsto C \end{aligned}$$

tal que la funció e és injectiva, és a dir:

$$\exists d\colon \mathcal{A}^n \to \mathcal{A}^m \mid d\big(e(P)\big) = P, \ \forall P \in \mathcal{A}^m$$

La funció d és un ***desxifratge criptogràfic*** [4]. Aquest parell de funcions ens permeten passar d'un missatge inicial P (anomenat el *missatge pla*) a un altre missatge C (anomenat el *missatge xifrat*) i a l'inrevés. En la gran majoria de casos, ambdós missatges són de la mateixa mida: $m = n$. No obstant, existeixen casos on aquest fet no es compleix [18].

Definició 2.1.2. *Donat un alfabet $\mathcal{A}$, un* ***criptosistema*** *en aquest alfabet és una 5-tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ on:*

1. *$\mathcal{P}$ és el conjunt de possibles missatges plans (en l'alfabet triat).*
2. *$\mathcal{C}$ és el conjunt de possibles missatges xifrats (en l'alfabet triat).*
3. *$\mathcal{K}$ és el conjunt de possibles claus.*
4. *$\mathcal{E}$ és la família de possibles xifratges: $\{ e_K\colon \mathcal{P} \to \mathcal{C} \}_{K \in \mathcal{K}}$.*
5. *$\mathcal{D}$ és la família de possibles desxifratges: $\{ d_K\colon \mathcal{C} \to \mathcal{P} \}_{K \in \mathcal{K}}$.*

En un criptosistema, a més, s'ha de complir la següent propietat:

$$\forall K \in \mathcal{K}, \quad d_K\big(e_K(P)\big) = P, \ \forall P \in \mathcal{P}$$

Cal notar que tot criptosistema determina un únic xifratge e_K i desxifratge d_K donada una clau $K \in \mathcal{K}$. No obstant, això no significa que $\#\mathcal{E} = \#\mathcal{K}$, perquè pot passar que per a $K_1, K_2 \in \mathcal{K}$ amb $K_1 \neq K_2$ es compleixi que $e_{K_1} = e_{K_2}$.

A l'hora de treballar amb els missatges, usualment no es treballa directament amb els elements de l'alfabet $\mathcal{A}$. En tot cas, es considera una aplicació bijectiva $\mathcal{A} \to \mathbb{Z}/t\mathbb{Z}$ i es treballa amb els elements de l'anell $\mathbb{Z}/t\mathbb{Z}$ amb les operacions usuals de suma i producte, on es té que $t = \#\mathcal{A}$. Aquest procés es coneix com a ***codificació*** de l'alfabet, i ens dóna una forma de treballar numèricament amb les cadenes de caràcters de $\mathcal{A}^m$, $\forall m \in \mathbb{N}$ usant la bijecció $\mathcal{A}^m \to (\mathbb{Z}/t\mathbb{Z})^m$.

En el cas del món digital, l'aplicació amb què treballarem serà $\mathcal{A} \to F_2$, on F_2 és el cos finit $\mathbb{Z}/2\mathbb{Z}$. Als elements d'aquest cos se'ls anomena ***bits***, dels quals agafarem per convenció el conjunt de representants $\{0, 1\}$. Per a treballar amb cadenes de bits, es fa de la manera següent: es considera la funció $f: F_2^r \to F_{2^r}$ on $f\big((a_0, \dots, a_{r-1}) \in F_2^r\big) = a_0 + a_1 x + \cdots + a_{r-1} x^{r-1}$, i la representació del cos finit F_{2^r} donada per l'isomorfisme que té aquest cos amb l'anell $F_2[X] \,/\, m(x)$, on $m(x)$ és un polinomi irreductible de grau r en F_2. En conseqüència, la suma de cadenes de bits es fa component a component, mentre que la multiplicació cal d'efectuar el producte dels polinomis corresponents mòdul $m(x)$.

Normalment escriurem les cadenes de bits com a nombres naturals, utilitzant la representació donada per $f\big((a_0, \dots, a_{r-1})\big)(2) = a_0 + a_1 2 + \cdots + a_{r-1} 2^{r-1}$, ja sigui en notació decimal o hexadecimal.

És important notar que com en $(F_2, +)$ cada element és el seu propis oposat, la suma en F_{2^r} és equivalent a la porta lògica XOR, i per aquesta raó denotarem la suma en aquest cos amb el símbol $\oplus$ utilitzat usualment en lògica [4].

1.2 Consideracions de seguretat

Per tal que un criptosistema sigui computacionalment segur, ha de complir els següents dos casos:

1. El temps necessari per a trobar la clau $K \in \mathcal{K}$ donat el *missatge xifrat* C és computacionalment intractable (amb la potència de càlcul de què es disposa avui dia, es tardarien milers d'anys o més).

2. En cas que una part de la clau sigui informació pública, aleshores cal que el temps necessari per a calcular la part restant donat el *missatge xifrat* C sigui computacionalment intractable. Generalment això passa si el càlcul depèn de la dificultat de resolució d'un problema *NP,* com podria ser-ho el càlcul del logaritme discret o el logaritme el·líptic. El temps de càlcul necessari en problemes NP és no polinòmic en tota màquina de Turing determinista com pot ser-ho un ordinador.

Així doncs, la fortalesa del criptosistema radica o bé en la dificultat d'invertir el procés de xifratge tot i tenint accés a una part de la clau K emprada, o bé en la dificultat d'endevinar per complert la clau que s'ha utilitzat en el xifratge donat el *missatge xifrat* C. En aquest últim cas la seguretat del criptosistema es resumeix en un problema de cerca en $\mathcal{K}$. Si no existeix cap mètode més eficient que una cerca exhaustiva, aleshores la seguretat del criptosistema dependrà del temps necessari per completar un ***atac per força bruta***.

1.3 Classificació de criptosistemes

Els criptosistemes es poden dividir en dues gran àrees [18]:

- La **criptografia simètrica**, que està conformada pels criptosistemes on la clau és completament privada. La criptografia simètrica és el focus del nostre treball.

- La **criptografia asimètrica**, que està conformada pels criptosistemes on part de la clau es coneix de forma pública. En aquests criptosistemes, es considera a efectes pràctics que existeixen dues claus: una de privada i una de pública.

  Aquests criptosistemes, anomenats criptosistemes de clau pública, es basen en problemes matemàtics on es difícil trobar el dual o invers d'un element donat sense tenir que executar un càlcul computacionalment molt costós. Un exemple seria el problema del logaritme discret en alguns grups cíclics: trobar l'exponent x donat $y = g^x$ i un generador g del grup no és trivial, ja que no es coneix encara cap algorisme que pugui calcular $x = \log_g(y)$ en temps polinomial.

1.4 Criptografia simètrica

La criptografia simètrica engloba tots els criptosistemes on s'utilitza una única clau privada K tant per a xifrar com per a desxifrar. Aquesta clau representa un secret compartit entre dues o més persones amb la qual poden comunicar-se de manera segura [4].

La seguretat, com ja hem vist, dependrà del grau de dificultat per a aconseguir la clau a nivell computacional. En tot cas, cal també ser curosos que la clau no sigui fàcil d'obtenir físicament d'una de les persones que estan involucrades en les comunicacions (ja sigui per coerció, traïció, robatori, compra o qualssevol altra possible raó). En conseqüència, la clau s'ha d'intercanviar sempre per canals segurs i no s'ha de reutilitzar mai, o en el seu defecte, ha de canviar-se periòdicament per a evitar comprometre les noves comunicacions en el cas que una persona no autoritzada l'obtingui [18].

El principal desavantatge dels criptosistemes de clau privada radica, així doncs, en la protecció de la clau K. Un segon desavantatge es dóna quan un usuari té una clau K_i diferent per a comunicar-se amb diferents persones $p_1, p_2, \dots, p_n$. Tot i que aquesta mesura de seguretat garanteix que la pèrdua o robatori d'una clau K_i no posa en risc la integritat dels missatges enviats a altres destinataris $p_{j \neq i}$, cal guardar-les totes de manera segura i recordar quina clau correspon a cada persona: es necessita d'una política de maneig de claus [4].

En tot cas, la criptografia simètrica presenta molts avantatges. Per començar, tant el *xifrat de Vernam* (l'únic criptosistema per al qual s'ha provat que té seguretat incondicional) com l'AES (actual estàndard criptogràfic internacional) són criptosistemes de clau privada. A més a més, els criptosistemes simètrics o de clau privada també són bastant més ràpids en el seus càlculs que els seus homòlegs asimètrics, doncs no depenen de problemes matemàtics amb càlculs complexos. Aquesta rapidesa els fa idonis per a xifrar fluxos constants de dades, els coneguts com *xifrats de flux*. Finalment, els criptosistemes simètrics o de clau privada també han demostrat una relativa resistència vers els atacs efectuats per ordinadors quàntics [2]. Aquest últim fet és degut al problema de cerca exhaustiva en què estan basats, que requereix d'un temps computacional de l'ordre de $\mathcal{O}(s)$, on s és al cardinal de l'espai de claus $\mathcal{K}$. Tot i que en els ordinadors quàntics aquest ordre de complexitat es pot reduir a $\mathcal{O}(\sqrt{s})$, existeix una fàcil solució a aquesta vulnerabilitat: considerar un espai de claus $\mathcal{K}$ amb cardinal $s' = s^2 \Longrightarrow \mathcal{O}(\sqrt{s'}) = \mathcal{O}(s)$.

En els criptosistemes simètrics, considerarem que $\mathcal{P} = \mathcal{A}^m$, $\mathcal{C} = \mathcal{A}^n$, $\mathcal{K} = \mathcal{A}^k$ per a certs nombres $m, n, k \in \mathbb{N}$ donat un alfabet $\mathcal{A}$.

1.5 Criptosistemes de substitució

Els criptosistemes de substitució són criptosistemes de clau privada on grups de n caràcters consecutius del *missatge pla* P, anomenats n-grames, es xifren de manera que el *missatge xifrat* C cada n-grama ha estat substituït per un altre. En el cas més senzill, el criptosistema treballa amb unigrames, obtenim:

$$C_i = P_i * K_i \ , \ \ \forall i$$

per a una operació binària donada $*$, normalment la suma.

Definició 1.5.1. *Un* ***xifrat alfabètic*** *és un criptosistema de substitució on la funció de xifratge actua de la següent forma, donada una clau* $K \in \mathcal{A}^k$*:*

$$\begin{aligned} e_K\colon\ \mathcal{A}^n &\to \mathcal{A}^n \\ (P_1, \dots, P_n) &\mapsto \left(P_1 + K_{1\ (mod\ k)}, \dots, P_n + K_{n\ (mod\ k)}\right). \end{aligned}$$

Si $k = 1$*, el xifrat s'anomena* ***monoalfabètic****.*
Si $k > 1$*, el xifrat s'anomena* ***polialfabètic****.*

Un dels primers criptosistemes del que es té referència és el *xifrat de Cèsar*, que deu el seu nom a Julius Cèsar, la figura històrica que el va utilitzar en la seva correspondència privada, així com en missatges enviats a les tropes romanes. És un criptosistema molt bàsic, però tot i així és rellevant ja que tot xifrat monoalfabètic és una adaptació del *xifrat de Cèsar*.

El *xifrat de Cèsar* és un criptosistema molt pobre en termes de seguretat, però: l'espai de cerca té només $\#\mathcal{A}$ opcions. Una millora significativa de la seva idea bàsica la donà Giovan Battista en inventar el *xifrat de Vigènere* (a qui es va atribuir la seva invenció erròniament), que podem veure com $k > 1$ xifrats de Cèsar aplicats de manera periòdica sobre el *missatge pla*. Tot xifrat poli-alfabètic és una adaptació del *xifrat de Vigènere*. En particular, si $\mathcal{K} = \mathcal{P} = \mathcal{C}$ aleshores tenim un *xifrat de Vernam*.

Els xifrats alfabètics són simples d'aplicar i d'entendre, però es poden trencar fàcilment utilitzant una tècnica de criptoanàlisi coneguda com el ***test de Kasiski*** [18]: com que el procés xifratge és periòdic, se cerquen repeticions de cadenes caràcters al *missatge* C, i calculem les distàncies d_i que les separen, que han de ser múltiples de la longitud k de la clau emprada. Per tant, $k \mid d_i$ obtenint $k \mid mcd(d_1, \dots, d_r)$. Cal tenir cura, ja que és possible que existeixin repeticions que siguin simples coincidències. Caldrà calcular diferents possibles valors de k i veure quin és el més probable. Si el valor de k es prou baix, es pot trobar la clau amb un *atac per força bruta* en poc temps. En altre cas, podem trobar quina és la clau més probable que s'ha utilitzat mitjançant una *anàlisi de freqüències* per a cada xifrat monoalfabètic, és a dir, comparar les freqüències dels caràcters corresponents amb les esperades del missatge.

No tots els criptosistemes de substitució utilitzen unigrames com en el cas dels xifrats alfabètics, no obstant. Un exemple seria el xifrat de Playfair [18], en el qual les lletres de la clau s'escriuen un únic cop en l'ordre que apareixen (sense repetir-ne cap) en una matriu 5×5. La resta d'espais s'emplenen amb les lletres restants per ordre alfabètic, i on a més s'identifica la lletra J amb la I (per a representar tots els caràcters de l'alfabet clàssic $\mathcal{A} = \{A, B, C, \dots, X, Y, Z\}$ en una matriu quadrada). La transformació aplicada a cada bigrama del text P es basa en la posició dels caràcters individuals que conformen els bigrames a la matriu, convertint el xifratge e en una permutació a l'espai de bigrames $\mathcal{A}^2$.

Existeixen molts més criptosistemes de substitució amb trigrames i fins i tot amb n-grames de longitud superior. Tot i així, l'anàlisi de freqüències es pot ampliar per a atacar també aquests criptosistemes utilitzant el que avui dia es coneix com a processament del llenguatge natural: donat un *corpus* de textos recopilats en l'idioma que ens interessa, només ens cal deixar que un algoritme recompti tots els n-grames i les seves freqüències relatives per a analitzar els resultats del criptosistema.

Com més grans siguin $\#\mathcal{A}$ i la longitud dels n-grames considerats, més difícil es torna aquesta tasca, però al mateix temps més complexa es torna l'el·lecció d'una funció de xifratge e que no resulti en una permutació trivial de $\mathcal{A}^n$ (on n és la longitud dels n-grames considerats). Addicionalment, l'ús de permutacions que depenguin de la clau K pot resultar complicat: s'ha d'evitar la possibilitat que resulti en permutacions poc segures.

1.6 Criptosistemes de transposició

Els criptosistemes de transposició o permutació són un tipus de criptosistemes de clau privada on els caràcters del text no es canvien per d'altres, si no que es canvia la seva posició. D'igual manera que passa amb els criptosistemes de substitució, la transposició es pot fer directament sobre caràcters individuals o agrupant-los en n-grames. El *missatge xifrat* $C = e_K(P)$ resultant d'aplicar un xifrat de transposició és un anagrama del *missatge pla* P, és a dir, constitueix un reordenament dels caràcters del mateix. És possible que C presenti caràcters addicionals respecte al text original P si cal afegir-n'hi per tal que la mida del text sigui divisible pel nombre de caràcters de cada n-grama (aquesta tècnica es coneix com a *farciment*).

Els criptosistemes de transposició són completament vulnerables a una anàlisi de freqüències, essent el reordenament dels seus caràcters l'únic problema. Tot i així, el problema del reordenament es pot expressar com un problema d'optimització respecte a la diferència o proporció amb les freqüències esperades dels bigrames, trigrames i tetragrames del text. Per tant, la clau K que determina quin és el procés de xifratge e_K emprat es pot trobar usant algorismes genètics [14].

Al llarg de la història els criptosistemes de transposició han estat populars en bona part degut a la seva relativa facilitat d'ús, així com a la dificultat per trencar-los a mà. Alguns dels exemples més rellevants inclouen l'escítala (un dels primers usos registrats de la criptografia, usada pels espartans), així com el mètode de transposició per rails i la transposició per columnes.

ATAQUEUALVESPREPELFLANCSUDXX → AUPFUTEASRLLSDAULEEEACXQVPNX

A						U						P						F						U			
	T				E		A				S		R				L		L				S		D		
		A		U				L		E				E		E				A		C				X	
			Q						V						P						N						X

Figura 1: Exemple del mètode de xifratge de transposició per rails.

1.7 Xifrats en bloc

Un tipus de criptosistema més modern són els criptosistemes híbrids, també coneguts com a criptosistemes producte, terminologia popularitzada per Claude Shannon. Els criptosistemes producte combinen les dues idees que s'han vist fins ara: substitució i transposició (també conegudes com confusió i difusió, respectivament [22]). La família més importants de criptosistemes producte són, sense cap mena de dubte, els xifrats en bloc.

Definició 1.7.1. *Els* ***xifrats en bloc*** *són criptosistemes on el missatge pla* P *es divideix en blocs de* b *caràcters, degudament farcit si cal. A cada bloc s'hi aplica una funció* $R_{K_i} = \mathcal{A}^b \to \mathcal{A}^b$ *anomenada* ***funció de ronda****,* $\forall i \in \{1, \dots, r\}$.

El nombre r *representa la quantitat de rondes del xifrat. A les claus* K_i *se les anomena* ***claus de ronda****.*

Sovint, el procés de xifratge e d'un xifrat en bloc consta de r rondes principals, on a cada ronda la funció R_{K_i} efectua un procés de substitució S_{K_i} i un altre de permutació P_{K_i}, i d'una ronda inicial i una ronda final si cal. El criptosistema a servir una clau global K de la qual s'extreuen les claus de ronda necessàries $K_1, \dots, K_r$ mitjançant una política de programació de claus.

Dintre dels xifrats en bloc n'hi ha dos tipus especialment importants: les xarxes de substitució-permutació, i les xarxes de Feistel. En ambdós casos, l'alfabet que es considera habitualment és el binari, és a dir, $\mathcal{A} = F_2$.

Xarxes de substitució-permutació

Definició 1.7.2. *Una permutació no lineal* S: $F_{2^k} \to F_{2^k}$ *amb* $k \in \mathbb{N}$ *emprada en un criptosistema de xifrat de bloc és una* ***caixa de tipus S****.*

Definició 1.7.3. *Una permutació lineal* P: $F_{2^b} \to F_{2^b}$ *amb* $b \in \mathbb{N}$ *emprada en un criptosistema de xifrat de bloc és una* ***caixa de tipus P****.*

Definició 1.7.4. *Les* ***xarxes de substitució-permutació*** *són criptosistemes de xifrat en bloc on cada bloc de* b *caràcters es divideix en* s *sub-blocs de mida* 2^k *,* $k \in \mathbb{N}$ *fix, on es té que* $s\, 2^k = b$.

En cada ronda $i \in \{1, \dots, r\}$*, la funció de ronda* R_{K_i} *consisteix en el XOR de cada bloc amb la clau de ronda pertinent* K_i*, així com en l'aplicació de* s *caixes de tipus S en cada sub-bloc i de l'aplicació d'una caixa de tipus P a tot el bloc.*

Per abreujar, sovint s'acostuma a denominar a les *caixes de tipus S* com a caixes-S, i a les *caixes de tipus P* com a caixes-P.

La característica de no linealitat de les *caixes de tipus S* ens assegura que, en general, no es pot reconstruir la sortida en base a sortides parcials d'una mateixa entrada. És a dir, si $x = x_1 \oplus x_2$ es té que $S(x_1) \oplus S(x_2) \neq S(x_1 \oplus x_2)$. La propietat de no linealitat també és a la vegada una mesura de complexitat de la funció S comparada amb altres permutacions més senzilles que es poden modelitzar amb expressions lineals o afins del tipus $a \cdot x \oplus b$. Una caixa-S on una aproximació donada per una expressió lineal o afí no la permet distingir-se d'una funció aleatòria uniforme en F_{2^k} se l'anomena *perfecte* [17].

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figura 2: Exemple d'una *caixa de tipus S* usant blocs de 2 bytes, en notació hexadecimal (extreta de les especificacions del criptosistema AES [6]).

La no linealitat es pot mesurar amb la següent fórmula:

$$NL(f) = \min_{a,\, b \in F_{2^k}} \left\{ \min_{x \in F_{2^k}} \left\{ d_{Hamming}\ (S(x),\ \ a \cdot x \oplus b) \right\} \right\},$$

on la *distància de Hamming* mesura la quantitat de bits diferents entre els valors donats, en notació vectorial (recordem que tenim una bijecció entre F_{2^k} i l'espai vectorial F_2^k donada per l'aplicació $f(a) = a_0 + a_1 x + \cdots + a_{r-1} x^{r-1}$).

Les permutacions de tot el bloc les efectuen les *caixes de tipus P*, i és una part essencial del disseny de la xarxa, ja que difonen els canvis efectuats en una ronda a diferents sub-blocs de la següent. Dintre de les *caixes de tipus P* en podem diferenciar dos tipus: les rectes (*straight* en anglès), i les expansives.

Les caixes rectes són simples transposicions de bits, de manera que canviïn de posició en el bloc. El resultat és una permutació lineal, on si denotem per x un dels blocs de b bits amb els que treballem, s'obté $P(x_1) \oplus P(x_2) = P(x_1 \oplus x_2)$. Tot i que són una aplicació directa del concepte vist en els criptosistemes de transposició, les caixes rectes no difonen necessàriament els canvis efectuats en un sub-bloc a més d'un sub-bloc de la ronda següent. Per a que això passi, la xarxa ha d'usar caixes-P expansives, que són molt més complexes i difícils de dissenyar perquè la idea es que un sol bit de x es pot copiar en diferents posicions de $P(x)$, expandint els seus canvis en un *efecte allau*. Les còpies, però, han de respectar la composició de x, de manera que si $x = x_1 \oplus x_2$ aleshores s'ha de tenir que $P(x_1) \oplus P(x_2) = P(x_1 \oplus x_2)$.

Un exemple visual de la diferència entre ambdós tipus de caixes-P:

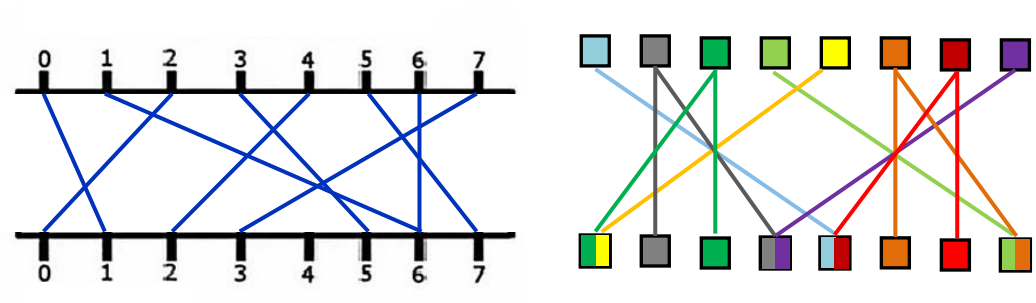


Figura 3: A l'esquerra, un exemple de caixa-P recta (transposició de bits). A la dreta, un exemple de caixa-P expansiva on cada bit té colors diferents.

Els bits compostos d'una caixa expansiva s'han de combinar predictiblement, com pot ser l'operació usual XOR. Així doncs, el resultat és una permutació $P: \mathcal{A}^b \to \mathcal{A}^b$ que manté la propietat de linealitat [12].

Està clar que el disseny de bones *caixes de tipus S* és difícil, perquè $NL(S)$ ha d'ésser al més petit possible, fet que no resulta gens fàcil d'aconseguir si les funcions $S_{i1}(K_i, x), \ldots, S_{is}(K_i, x)$ d'una ronda $i \in \{1, \ldots, r\}$ depenen de les claus de ronda K_i. Anàlogament, les *caixes de tipus P* expansives també resulten molt difícils de dissenyar: ens interessa que difonguin al màxim possible els canvis d'una caixa-S en una ronda entre les *caixes de tipus S* de la ronda següent. Això implica que si les funcions $P_1(K_1, x), \ldots, P_r(K_r, x)$ depenen de les claus de ronda K_i, pot haver-hi problemes per a certes claus si s'utilitza una política d'el·lecció de *caixes de tipus S* i *P* subòptima per a la xarxa.

Tot i que existeixen xarxes de substitució-permutació on caixes-S i caixes-P canvien en base a la clau emprada (per exemple, el criptosistema Twofish [19]), en la gran majoria de casos s'utilitzen funcions $S_{i1}, \ldots S_{is}$ constants per a cada ronda, així com permutacions $P_1, \ldots, P_r$ fixades. El pas de sumar les claus de ronda amb els blocs mitjançant l'operació XOR evita que el missatge C sigui trivialment desxifrable, degut al fet que les funcions S_{ij}, P_i són ara trivialment invertibles per ésser constants i bijectives. Conseqüentment, calen rondes addicionals al principi i final del procés de xifratge on s'apliqui una clau addicional, si aquest no era el primer o l'últim pas de la *funció de ronda*.

L'actual estàndard de seguretat en el camp de la criptografia simètrica és el AES (Advanced Encryption Standard), una xarxa de substitució-permutació que opera amb blocs de 128 bits, i on els bytes es representen segons el cos $F_{2^8} \cong F_2[X] \,/\, (x^8 + x^4 + x^3 + x + 1)$ [6]. Fou dissenyat entre 1997 i 1998 pels criptòlegs belgues Rijmen i Daemen amb el nom conjunt de RIJNDAEL, i acceptat com a estàndard internacional l'any 2001, succeint a l'anterior estàndard, el DES (Data Encryption Standard).

Xarxes de Feistel

Les xarxes de Feistel són un tipus d'estructura criptogràfica de xifrat en bloc que va gaudir de gran popularitat durant els anys 70 i 80 degut a la senzillesa del seu disseny.

Definició 1.7.4. *Les **xarxes de Feistel** són criptosistemes de xifrat en bloc. El seu funcionament és el següent* [12,21]:

- *Cada bloc es divideix en dues parts en cada ronda:* L_i, R_i. *Si la mida de les dues parts no és igual, aleshores és una xarxa no balancejada.*
- $\forall i \in \{1, \dots, r\}, \quad \begin{cases} L_{i+1} = R_i \,, \\ R_{i+1} = L_i \oplus F(K_i \oplus R_i) \,. \end{cases}$
- *El missatge xifrat* C *ve donat per la parella* (L_{r+1}, R_{r+1}).

L'avantatge de les xarxes de Feistel és el fet que el procés de xifratge e i el de desxifratge d són simètrics, per tant no cal que l'aplicació F utilitzada en la funció de ronda R_{K_i} es pugui invertir. Això permet un major grau de llibertat en dissenyar cada criptosistema, ja que en les xarxes de substitució-permutació les funcions han de ser invertibles.

En concret, es pot utilitzar com a F una ronda completa d'una xarxa de substitució-permutació. De fet, és una decisió popular en diferents xarxes de Feistel. L'anterior criptosistema que fou estàndard internacional, el Data Encryption Standard (escurçat DES), utilitza precisament *caixes de tipus S* no invertibles i una permutació dels bits resultants com a funció F [7].

Ja que cada part es transforma cada 2 rondes, calen com a mínim el doble de rondes per a tenir el mateix nivell de seguretat que l'equivalent d'una xarxa de substitució-permutació.

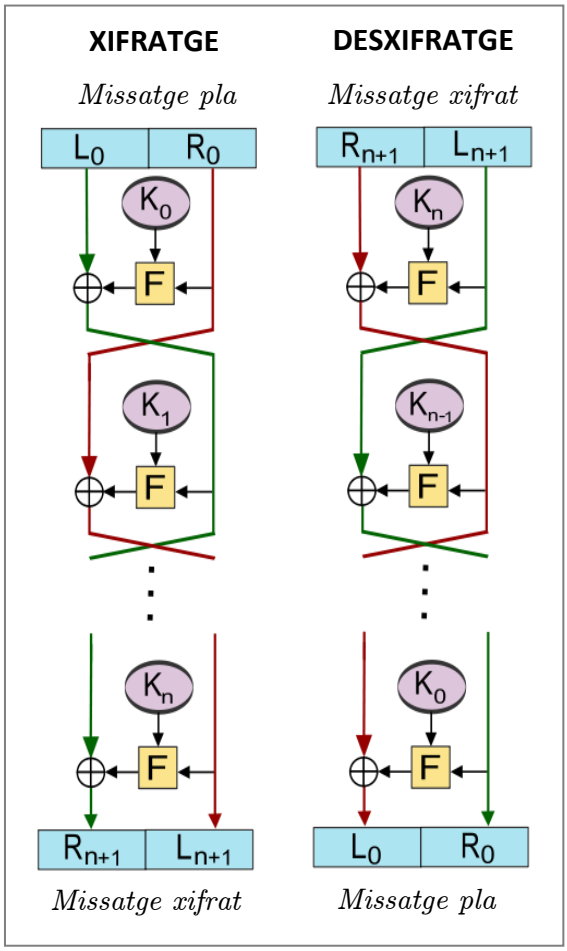


Figura 4: Esquema del funcionament d'una xarxa de Feistel (extret de [26]).

1.8 Principis de criptoanàlisi

La criptoanàlisi és la disciplina que s'encarrega de l'estudi dels criptosistemes i de la seva seguretat, mitjançant l'ús d'algorismes que puguin recuperar les dades originals d'un missatge xifrat. Així doncs, tant la criptografia com la criptoanàlisi són camps àmpliament interrelacionats, podent millorar els nous criptosistemes així com els ja existents degut als nous atacs descoberts. Tot i que existeixen multitud d'atacs criptogràfics, començant pels més bàsics com el *test de Kasiski* i l'anàlisi de freqüències (que ja hem vist), en aquest treball ens centrarem només en dos atacs criptogràfics concrets: la criptoanàlisi diferencial i la criptoanàlisi lineal, usualment utilitzats contra els xifrats en bloc.

En 1883 Auguste Kerchkoffs (lingüista i criptògraf holandès) enuncià una sèrie de principis per al disseny de criptosistemes segurs [11]. Tot i que molts dels seus principis han quedat antiquats, els dos primers encara són de vital interès:

1. Si el sistema no es teòricament segur, ha de ser-ho a la pràctica.
2. L'efectivitat del criptosistema no ha d'estar basada en el seu secretisme.

Per antonomàsia, al segon principi se l'anomena habitualment com a *Principi de Kerchkoff*, o fins i tot com a *màxima de Shannon,* degut al seu important treball en el camp de la criptografia i al seu rol a popularitzar el principi de no secretisme [3]. Basant-nos en la premissa que coneixem el funcionament intern del criptosistema que pretenem atacar, però desconeixem la clau K, tot atac criptogràfic que no es basi en el comportament del maquinari on s'ha implementat el criptosistema segueix un dels següents models d'atac [18].

- ***Atac de missatge xifrat:*** s'inspeccionen missatges xifrats qualssevol que s'hagin pogut interceptar o aconseguir.
- ***Atac de missatge xifrat conegut:*** s'inspeccionen missatges xifrats dels quals es coneix el missatge original $P = d_K(C)$ corresponent.
- ***Atac de missatge xifrat escollit:*** s'inspeccionen missatges xifrats escollits per l'atacant on es coneix el missatge original corresponent. Es pot considerar la variant *adaptativa*, on el mètode d'escollir pot variar amb el temps segons el coneixement guanyat al llarg de l'atac.
- ***Atac de missatge pla escollit:*** tenim accés a la màquina de xifratge, i podem xifrar els missatges que vulguem i analitzar-los. Similarment al cas anterior, es pot considerar la variant *adaptativa*.
- ***Atac de claus relacionades:*** tenim accés a la màquina de xifratge, i en aquest cas podem escollir la clau a utilitzar. Analitzem les parelles de missatges (P, C) resultants d'usar claus diferents.

2 La criptoanàlisi diferencial

2.1 Resum de l'atac

En 1990, els criptòlegs Eli Biham i Adi Shamir (coinventor del RSA) van donar a conèixer al públic un nou atac criptogràfic: la ***criptoanàlisi diferencial*** [3]. L'atac era conegut tant per IBM com per la NSA amb el nom de T-attack abans de la seva publicació, i el Data Encryption Standard fou dissenyat per a ésser resistent contra aquest atac criptogràfic, des de l'elecció de les caixes de tipus S, fins al nombre de rondes del criptosistema [5]. Tot i que la criptoanàlisi diferencial es va dissenyar com un atac als xifrats en bloc, es pot emprar també contra altres criptosistemes simètrics de substitució, transposició o híbrids (tot i que usualment existeixen atacs més eficients en aquest casos, com l'anàlisi de freqüències) [23]. Per una qüestió d'espai i de simplicitat, exposarem tan sols el funcionament de la criptoanàlisi diferencial amb xarxes SPN.

L'atac depèn de conèixer el funcionament intern del criptosistema (màxima de seguretat de Shannon), en concret de la composició de les caixes de tipus S i P que utilitza [18,21].

Definició 2.1.1. *Denotem l'entrada d'una caixa-S del criptosistema com a* X*, i la modelitzarem com a una variable aleatòria. Anàlogament, notarem la sortida d'una caixa-S com a* $Y = S(X)$*, que serà també una variable aleatòria.*

Definició 2.1.2. *Donada la funció* ***diferència*** Δ: $(A,\ B) \to A \oplus B$*, considerem dues entrades* X, X' *a una caixa-S qualsevol, i les sortides* $Y = S(X)$, $Y' = S(X')$ *corresponents.*

El resultat $\Delta(X, X')$ *és una variable aleatòria que anomenarem la diferència de* X, X'*. Anàlogament definim* $\Delta(Y, Y')$ *una variable aleatòria que anomenarem la diferència de* Y, Y'*. Per abús de notació, usualment es denoten com a* $\Delta X,\ \Delta Y$.

L'atac és basa en la premissa següent: donada una diferència $\Delta X \neq 0$ en dues entrades qualssevol X, X' d'una caixa-S, volem determinar si existeix $\Delta Y \neq 0$ de manera que $| P(\Delta Y \mid \Delta X) - 2^{-k} |$ sigui un biaix estadístic significatiu. Això és degut al fet que si cada caixa-S fos completament aleatòria (fet que resulta impossible perquè el procés de xifratge e_K deixaria de ser reversible), aleshores es compliria que $P(\Delta Y \mid \Delta X) \approx 2^{-k}$. Com més gran sigui la desviació del valor esperat 2^{-k}, més vulnerable és el criptosistema [8].

Definició 2.1.3. *El parell* $(\Delta X,\ \Delta Y)$ *escollit en una caixa-S* (*on* $\Delta X, \Delta Y \neq 0$) *és* ***el diferencial***, *amb probabilitat associada* $P(\Delta Y \mid \Delta X)$ [8,12,21].

Donat un procés de xifratge de r rondes, considerem les diferències ΔY_S de les sortides de cada caixa-S en la ronda i-èsima. El vector de diferències resultant el denotarem per ΔY_i, on $1 \leq i \leq r$. Les diferències ΔY_i són invariants pel XOR amb les claus de ronda K_i, atès que: $X_{i+1} \oplus X'_{i+1} = (Y_i \oplus K_i) \oplus (Y_i \oplus K_i) = Y_i \oplus Y'_i$. Per tant, es té que les diferències de les sortides de les caixes-S en una ronda coincideixen amb les entrades en la ronda següent.

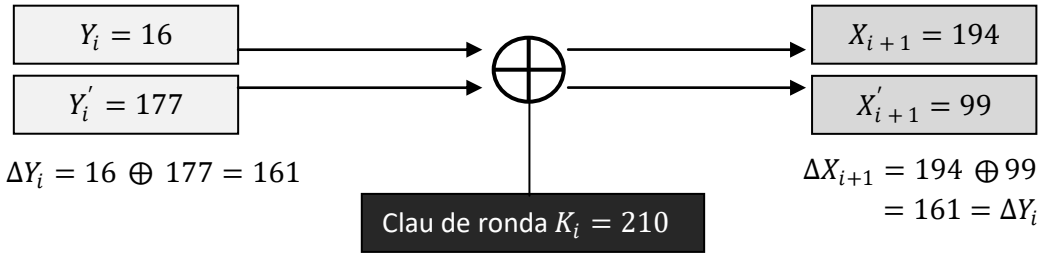


Figura 5: Exemple d'invariància de les diferències, on $\Delta X_{i+1} = \Delta Y_i$.

Aquest mateix argument ens diu que, donats dos *missatges plans* P, P', llavors es té que $\Delta P = \Delta X_1$ siguin quin siguin els valors de les variables aleatòries P, P', atès que el diferencial ΔP és invariant pel XOR amb la clau de ronda K_1.

Definició 3.1.3. *Una successió de diferencials* $\{(\Delta X_i, \Delta Y_i)\}_{1 \leq i \leq r-1}$ *es coneix com una* ***característica diferencial*** [8,12,21].

Proposició 3.1.4. *Donada una característica diferencial, aquesta determina un nou diferencial* $(\Delta P, \Delta Y_{r-1})$ *que comprèn totes les rondes del criptosistema, i que anomenarem com a* ***diferencial global***.

És important notar que el *diferencial global* es pot obtenir d'altres successions de *diferencials* $\{(\Delta X_i, \Delta Y_i)\}$, sempre i quan les diferències ΔX_1, ΔY_{r-1} siguin les mateixes. Per tant, no hi ha una *característica* única que el determini [8,21].

Donat el *diferencial* $(\Delta P, \Delta Y_{r-1})$ amb probabilitat d'ocórrer $p = P(\Delta Y_{r-1} \mid \Delta P)$, ens caldria una quantitat de parelles de *missatges plans* proporcional al valor de p per a trobar alguna parella que tingués el *diferencial* $(\Delta P, \Delta Y_{r-1})$. Per tant, l'atac necessita una quantitat de parelles de missatges N que vindrà donada per $N \approx p^{-1}$ [8]. És a dir, calen de l'ordre de $1/p$ parelles de missatges per a poder muntar un atac diferencial exitós.

Usualment, per a trobar el valor d'una de les claus de ronda K_i emprades en el procés de xifratge, ens caldria provar $\mathcal{O}(2^b)$ candidats en un atac per força bruta, on b és la quantitat de bits de la clau de ronda K_i. Amb l'atac diferencial podem reduir considerablement aquests càlculs.

Utilitzant les *característiques diferencials* del criptosistema, podem recuperar un total de d *bits* de l'última clau de ronda mitjançant el següent algorisme.

Algorisme de l'atac diferencial

(1) Trobar una característica diferencial C_d amb probabilitat d'ocórrer $Pr(C_d)$, tal que $2^d \cdot Pr(C_d)^{-1} \leq 2^b$.

(2) Generar $Pr(C_d)^{-1}$ missatges aleatoris P, P' amb $\Delta P_{\in C_d} \neq 0$.

(3) Computar $C = e_K(P)$, $C' = e_K(P')$.

(4) Crear una taula de comptadors, inicialitzats a 0, de tots els possibles valors dels bits H de K_{r+1} que coincideixen amb les caixes-S amb $\Delta X_r \neq 0$.

(5) Computar X_r desxifrant parcialment l'última ronda usant H.

(6) Si ΔX_r coincideix amb el diferencial ΔY_{r-1} donat per la característica C_d, augmentem el comptador de H.

(7) Finalment escollim el candidat H amb comptador més alt.

En la seva formulació típica, la criptoanàlisi diferencial és un *atac de missatge pla escollit*: l'atacant pot escollir missatges P, P' amb diferència ΔP fixada, i xifrar-los per a obtenir els missatges C, C' corresponents. Si l'atacant pot trobar una *característica diferencial* amb una probabilitat d'ocórrer $Pr(C_d)$ tal que $\mathcal{O}\left(2^d \cdot Pr(C_d)^{-1}\right) \leq \mathcal{O}(2^b)$, llavors pot recuperar d *bits* de l'última clau de ronda K_{r+1} en un temps raonable, facilitant la cerca dels *bits* restants [5,8,21].

En alguns criptosistemes, és possible determinar el valor de la clau general K a partir de l'última clau de ronda K_{r+1}, com és el cas DES [6]. En cas contrari, sempre podem tornar a intentar un atac diferencial sobre la pròxima clau de ronda, i així successivament fins a obtenir totes les claus de ronda. En el cas del criptosistema DES, per exemple, cada clau de ronda K_i està composta per 48 bits de la clau K general després de l'aplicació de l'*el·lecció permutada* PC-1. Conegut el valor de qualsevol clau de ronda K_i, podem trobar fàcilment el valor de la clau general K, considerant els 8 *bits* restants (són 2^8 opcions), i aplicant que $d_K\left(e_K(P)\right) = P$ es complirà per a tot *missatge pla* P només per a la clau K correcta.

Considerarem que un criptosistema és segur contra la criptoanàlisi diferencial si la complexitat de l'algorisme anterior és major a la d'un atac per força bruta. Això només es complirà si $\max\{Pr(C_d) - 2^{d-b},\ 0\} = 0$, per a tot valor de d i per a tota *característica* C_d, donat un valor prou elevat de r (el nombre de rondes en el procés de xifratge).

2.2 Diferencial d'una caixa-S

Considerem ara una xarxa de substitució-permutació on les *caixes de tipus P* i *de tipus S* ens són conegudes. Per simplicitat, considerarem també que les caixes són constants i que no depenen de les claus de ronda del criptosistema (un estudi sobre com es podria atacar un criptosistema amb caixes variables en funció de les claus de ronda, com és el cas del criptosistema *Twofish*, es pot veure en [19]). Al llarg d'aquesta secció ens centrarem en l'estudi de les caixes de tipus S, i en els seus diferencials $(\Delta X_S,\ \Delta Y_S)$.

Definició 2.2.1. *Donada S una caixa de tipus S d'una xarxa de substitució-permutació, llavors $(\Delta X_S = X \oplus X',\ \Delta Y_S = Y \oplus Y')$ és una parella de diferències si X, X' són variables aleatòries uniformes on $Y = S(X)$, $Y' = S(X')$.*

Definició 2.2.2. *La probabilitat associada a una parella $(\Delta X_S,\ \Delta Y_S)$ ve donada per la fórmula* [13,15]:

$$Pr(\Delta Y_S \mid \Delta X_S) = \frac{\#\{X \in F_{2^k} \mid \Delta Y_S = S(X) \oplus S(X \oplus \Delta X_S)\}}{2^k}.$$

Sigui una xarxa de substitució-permutació genèrica amb r rondes de xifratge, on el missatge es parteix en blocs de b bits i on s'apliquen s caixes-S en cada ronda que denotarem com a S_{ij} respectivament, on $i \in \{1, \dots, r\},\ \ j \in \{1, \dots, s\}$, i amb r caixes-P que denotarem com a σ_i.

Les *caixes de tipus S* són funcions bijectives $S_{ij} : F_{2^k} \to F_{2^k}$ on $k \in \mathbb{N},\ 2^k\, s = b$. Donada una caixa $S \in \{S_{ij}\}$ qualsevol, la diferència ΔX_S és el XOR de dues entrades X, X' qualssevol, i anàlogament ΔY_S és el XOR de les corresponents sortida. Per a una ronda i de la xarxa, denotarem $\Delta X_i = \left(\Delta X_{S_{i\,1}}, \dots, \Delta X_{S_{i\,s}}\right)$, i anàlogament per a $\Delta Y_i = \left(\Delta Y_{S_{i\,1}}, \dots, \Delta Y_{S_{i\,s}}\right)$.

En tota xarxa de substitució-permutació, els únics elements que no són lineals (i que per tant no mantenen les diferències $\Delta X, \Delta Y$) són les caixes-S [7,21]. El XOR de les difèrencies amb les claus de ronda K_i manté les diferències $\Delta X_{i+1} = \Delta Y_i$, com ja hem vist a la secció anterior. Pel que respecta a les permutacions de bloc σ_i, tot i que no mantenen estrictament les diferències, al ésser cada σ_i coneguda, constant i lineal, sabem en tot moment com passar de la diferència ΔY_{i-1} d'una ronda a la diferència $\Delta X_i = \sigma_i(\Delta Y_{i-1})$ de la ronda següent, ja que la propietat de linealitat s'aplica precisament a la composició mitjançant el XOR de diferents entrades. Per tant, els elements que ens caldrà estudiar per a veure el comportament dels diferencials són les caixes-S.

Sigui l'exemple de *caixa de tipus S* que podem veure a continuació, denotant els elements de F_{2^4} com nombres naturals (veure fórmula en la pàgina 3):

$S: F_{2^4} \rightarrow F_{2^4}$	
0 --> 3	8 --> 8
1 --> 14	9 --> 11
2 --> 1	10 --> 15
3 --> 10	11 --> 2
4 --> 4	12 --> 13
5 --> 9	13 --> 12
6 --> 5	14 --> 0
7 --> 6	15 --> 7

Cada entrada X de la caixa-S es transformarà en un única sortida $Y = S(X)$, però la caixa no actuarà de forma bijectiva sobre les diferències $\Delta X = X \oplus X'$ ja que poden venir donades per diferents entrades. Per exemple:

$$X_a = (0,1,0,1) = 5, \quad X'_a = (0,0,0,1) = 1\,,$$
$$\Delta X_a = X_a \oplus X'_a = 5 \oplus 1 = 4\,,$$
$$\Delta Y_a = S(X_a) \oplus S(X'_a) = 9 \oplus 14 = 7.$$

$$X_b = (0,1,1,1) = 7, \quad X'_b = (0,0,1,1) = 3\,,$$
$$\Delta X_b = X_b \oplus X'_b = 7 \oplus 3 = 4\,,$$
$$\Delta Y_b = S(X_b) \oplus S(X'_b) = 6 \oplus 10 = 12 \neq 7 = \Delta Y_a\,.$$

Per tant, cada ΔX es transformarà en diferències ΔY diferents. Si considerem tots els possibles parells de les variables aleatòries X, X', podem calcular una taula d'incidències on $S(\Delta X_S) = \Delta Y_S$, denominada la ***taula de distribució de diferències*** de la caixa S [8,12]. Les normes $\Delta X_S \rightarrow \Delta Y_S$ (equivalentment $S(\Delta X_S) = \Delta Y_S$) amb un major nombre d'incidències seran les candidates a ser el *diferencial* de la caixa, degut a que s'allunyen més del valor esperat 2^{-k}.

La *taula de distribució de diferències* compleix una sèrie de propietats bàsiques.

- Tots els valors de la taula són parells, perquè les diferències $\Delta(X, X')$ no canvien segons l'ordre dels seus arguments perquè $\oplus$ és commutativa.
- La suma dels valors en tota fila o columna dóna 2^k, on $k \in \mathbb{N}$ és el valor donat per $S: F_{2^k} \rightarrow F_{2^k}$. En conseqüència, podem dividir els valors de cada cel·la per 2^k per obtenir les probabilitats de cada norma.
- $\Delta Y_S = 0 \Leftrightarrow \Delta X_S = 0$, atès que S és injectiva. En conseqüència, la norma $\Delta X_S = 0 \rightarrow \Delta Y_S = 0$ és compleix amb probabilitat 1. Com aquesta norma no ens dóna cap informació de la caixa S en particular, no ens és útil.

- Si S fos la identitat, aleshores tota norma $\Delta X_S \to \Delta X_S$ es compliria amb probabilitat 1, i l'atac diferencial obtindria K_{r+1} molt fàcilment. De fet, tota caixa de tipus S amb una norma que es compleixi amb probabilitat 1 i on $\Delta X_S \neq 0$, representa una debilitat catastròfica del criptosistema [8]. En veurem un exemple al capítol final d'aquest treball.

ΔX_S \ ΔY_S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	4	0	0	0	2	0	0	0	2	0	6	0	0
2	0	2	2	0	2	0	0	2	0	2	0	2	0	2	0	2
3	0	0	2	0	2	0	0	0	0	2	4	0	4	0	0	2
4	0	0	0	0	2	4	0	6	0	0	0	0	2	0	0	2
5	0	0	2	0	2	0	2	2	2	0	4	0	0	0	0	2
6	0	0	2	2	0	2	2	0	4	0	0	0	2	0	2	0
7	0	0	0	2	0	2	0	0	2	0	0	4	0	0	2	4
8	0	2	0	0	0	6	0	0	2	2	0	2	0	0	2	0
9	0	0	2	2	2	2	4	0	4	0	0	0	0	0	0	0
A	0	2	0	0	2	0	0	0	2	2	2	0	4	0	2	0
B	0	4	2	2	0	0	0	0	0	4	2	2	0	0	0	0
C	0	2	4	0	2	0	0	0	0	0	2	0	2	2	2	0
D	0	2	0	2	0	0	2	2	0	2	2	0	0	0	0	4
E	0	0	0	2	0	0	2	0	0	2	0	4	2	4	0	0
F	0	0	0	0	2	0	4	2	0	0	0	0	0	2	6	0

Figura 6: *Taula de distribució de diferències* de S usant notació hexadecimal.

Examinant la taula anterior, trobem quatre possibles *diferencials* amb major nombre d'incidències per a la caixa-S proposada: $(1, D)$, $(4, 7)$, $(8, 5)$ i (F, E). Totes aquestes parelles tenen màxima probabilitat d'ocórrer d'entre totes les possibles *parelles de diferencies*, i per tant representen el màxim biaix possible respecte de 2^{-k} en la caixa S donada [8].Tot i que no és obligatori que el *diferencial* escollit tingui probabilitat maximal d'entre totes les opcions possibles, certament és preferible.

Definició 2.2.3. *La màxima probabilitat que pot assolir una parella* $(\Delta X_S,\ \Delta Y_S)$ *en una caixa* S *ve donada per la fórmula*

$$PM_S = \max_{(\Delta X_S \neq 0,\ \Delta Y_S)} \{ Pr(\Delta Y_S \mid \Delta X_S) \}.$$

La probabilitat maximal PM_S d'entre els possibles *diferencials* d'una caixa jugarà un paper important en l'anàlisi de la seguretat contra l'atac diferencial.

2.3 Construcció de característiques diferencials

Considerem un altre cop una xarxa de substitució-permutació amb r rondes de xifratge, s caixes de tipus S i P en cada ronda, i blocs de b bits (on $b = s \cdot 2^k$, amb $k \in \mathbb{N}$ donat per les caixes $S: F_{2^k} \to F_{2^k}$). Podem expressar el funcionament de qualsevol xarxa amb aquestes característiques mitjançant l'esquema següent:

$$
\begin{aligned}
&\textit{Missatge pla:} && P_{[0\,\ldots\,b]} = Y_0\,, \\
&\text{Ronda 1:} && X_1 = \sigma_1(Y_0) \oplus K_1 \quad \longrightarrow\ Y_1 = \big(S_{11}(X_1), \ldots, S_{1\,s}(X_1)\big)\,, \\
&\text{Ronda 2:} && X_2 = \sigma_2(Y_1) \oplus K_2 \quad \longrightarrow\ Y_2 = \big(S_{21}(X_2), \ldots, S_{2\,s}(X_2)\big)\,, \\
&\ \vdots \\
&\text{Ronda } r\text{:} && X_r = \sigma_r(Y_{r-1}) \oplus K_r \quad \longrightarrow\ Y_r = \big(S_{r1}(X_r), \ldots, S_{r\,s}(X_r)\big)\,, \\
&\textit{Missatge xifrat:} && C_{[0\,\ldots\,b]} = Y_r \oplus K_{r+1}\,.
\end{aligned}
$$

Conegudes les caixes S_{11} , … , S_{1s} , … , S_{r1} , … , S_{rs} del criptosistema i els seus possibles *diferencials*, podem seguir el camí dels *bits* no nuls de les diferències en cada ronda. L'objectiu és trobar una possible *característica diferencial* C_d amb alta probabilitat d'ocórrer per tal d'atacar el criptosistema [8,12,21]. És important notar que el camí resseguit en la *característica* C_d pot involucrar (i usualment involucra) més d'una caixa de tipus S en cada ronda.

Per exemple: sigui una xarxa de substitució-permutació tal que $b = 16$, $r = 4$, $s = 4$, $k = 4$ i amb permutacions $\sigma_{ik} = \sigma_{jk}\ \ \forall i, j \in \{2, \ldots, r\}$, $k \in \{1, \ldots, s\}$. Podem veure a continuació un esquema representatiu d'aquesta xarxa:

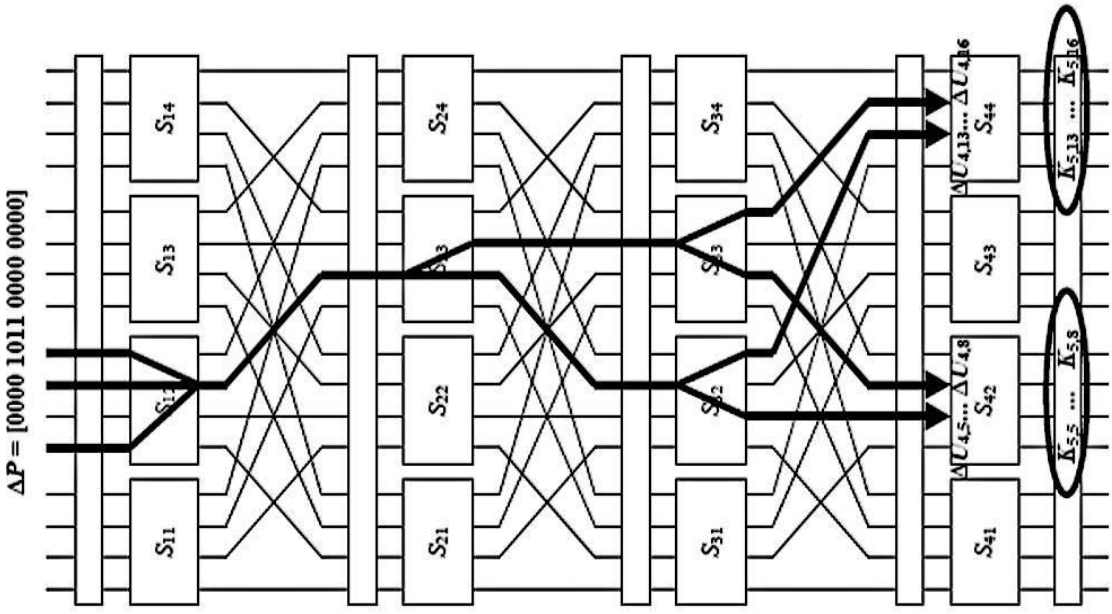


Figura 7: Una possible *característica diferencial* de la xarxa de substitució-permutació exemple (imatge original per Howard Heys, extreta de [8]).

En la figura de la pàgina anterior es pot veure el recorregut en la xarxa d'una *característica diferencial* C_d començant en $\Delta P = \Delta X_1 = (0, 11, 0, 0)$.

El camí resseguit és:

Ronda 1
Considerem en S_{12} el *diferencial* $\left(\Delta X_{S_{12}} = 11,\ \Delta Y_{S_{12}} = 2\right)$.
La permutació σ_2 transforma $\Delta Y_1 = (0, 2, 0, 0)$ en $\Delta X_2 = (0, 0, 4, 0)$.

$$Pr\left(\Delta Y_{S_{12}} \mid \Delta X_{S_{12}}\right) = 8/16\,,$$

Ronda 2
Considerem en S_{23} el *diferencial* $\left(\Delta X_{S_{23}} = 4,\ \Delta Y_{S_{23}} = 6\right)$.
La permutació σ_3 transforma $\Delta Y_2 = (0, 0, 6, 0)$ en $\Delta X_3 = (0, 2, 2, 0)$.

$$Pr\left(\Delta Y_{S_{23}} \mid \Delta X_{S_{23}}\right) = 6/16\,,$$

Ronda 3
Ara ens cal considerar dues caixes-S: S_{32} amb *diferencial* $\left(\Delta X_{S_{32}} = 2,\ \Delta Y_{S_{32}} = 5\right)$ i S_{33} amb *diferencial* $\left(\Delta X_{S_{33}} = 2,\ \Delta Y_{S_{33}} = 5\right)$. La permutació σ_4 transforma ΔY_3 en $\Delta X_4 = (0, 6, 0, 6)$.

$$Pr\left(\Delta Y_{S_{32}} \mid \Delta X_{S_{32}}\right) = 6/16\,,$$
$$Pr\left(\Delta Y_{S_{33}} \mid \Delta X_{S_{33}}\right) = 6/16\,.$$

Normalment, les *característiques diferencials* es construeixen des l'última ronda considerada $(r-1)$ a la primera: així podem fixar el nombre de bits d que es consideren en l'algorisme. Hem exposat el recorregut a l'inversa per claredat. Suposant que les probabilitats dels *diferencials* són independents (fet que no és necessàriament cert, però que resulta una hipòtesi raonable per a simplificar els càlculs [8,21]), la *característica* que hem escollit té una probabilitat associada:

$$Pr(C_d) = \frac{8}{16} \cdot \left(\frac{6}{16}\right)^3 = \frac{27}{1024}.$$

La *característica* C_d té bits no nuls en ΔY_r en dues caixes-S, per tant $d = 8$. Com que es compleix que $2^d \cdot Pr(C_d)^{-1} < 2^b$, ja que $9.709{,}037 < 2^{16}$, llavors es té que C_d es pot utilitzar per atacar amb èxit la xarxa d'exemple considerada.

És important remarcar que els *diferencials* que considerem en cada caixa-S no necessàriament han de tenir probabilitat maximal PM_S, ja que probablement això és impossible. Aquesta afirmació resulta evident si ens fixem en l'exemple donat: el *diferencial* escollit en S_{21} no té perquè ser la parella de diferències amb major probabilitat d'ocórrer, atès que la diferència $\Delta Y_{S_{21}}$ ens ve fixada pel vector de diferències ΔY_2.

En qualsevol cas, podem escollir el *diferencial* de S_{21} per tal que tingui probabilitat maximal amb $\Delta Y_{S_{21}}$ fixada. En l'exemple anterior:

$$PM_{S \mid \Delta Y_S = (0,0,6,0)} = \max_{\Delta X_S} \{ Pr(\Delta Y_S = (0,0,6,0) \mid \Delta X_S) \} \leq PM_S .$$

Així, hem d'escollir una *característica* C_d escollint les diferències en cada ronda de manera que maximitzin $Pr(C_d)$ en les rondes anteriors. Això dependrà tant dels valors $PM_{S \mid \Delta Y_S \neq 0}$ com de la quantitat de *caixes de tipus S* que considerem a la característica: quantes més caixes considerem, menor serà $Pr(C_d)$.

Definició 2.3.2. *A les caixes de tipus S amb diferència d'entrada* ΔX_S *no nul·la se les denomina* ***caixes-S diferencialment actives*** [8,9,19].

Definició 2.3.3. *Definim* $n(C_d)$ *com la quantitat de caixes-S diferencialment actives en una característica diferencial* C_d. *El seu valor ve donat per* [9]

$$n(C_d) = \# \left\{ \Delta X_{S_{ij}} \neq 0 \;\middle|\; \left(\Delta X_i = \left(\Delta X_{S_{i1}}, \ldots, \Delta X_{S_{is}}\right),\ \Delta Y_i\right) \in C_d \right\}.$$

Per a poder muntar un atac exitós, ens interessa que la nostra *característica* tingui el mínim nombre de caixes-S *diferencialment actives* possible; és a dir, volem minimitzar $n(C_d)$.

Pel contrari, un criptosistema serà més segur contra la criptoanàlisi diferencial com major sigui el nombre $n(C_d)$ de caixes *diferencialment actives.* Aleshores, queda palès que $n(C_d)$ jugarà un paper important en l'anàlisi de la seguretat d'un criptosistema vers la criptoanàlisi diferencial.

2.4 Obtenció de l'última clau de ronda

Un cop tenim una *característica diferencial* C_d amb d *bits* a considerar en ΔY_{r-1} i probabilitat $Pr(C_d)$ tal que $2^d \cdot Pr(C_d)^{-1} < 2^b$, és possible trobar quina és l'última clau de ronda emprada usant l'algorisme descrit en la secció 2.1 d'aquest capítol, més una cerca exhaustiva dels $b - d$ *bits* restants.

L'algorisme es basa en el següent raonament: si el candidat H és el correcte, aleshores per a un nombre parell de *missatges plans* P, P' proporcional al valor $Pr(\Delta Y_{r-1} \mid \Delta P)^{-1}$ és té que $\Delta X_r = \Delta Y_{r-1}$. Anomenarem a aquests parells com a ***parells correctes*** [8,19,21]. Per a qualsevol altre candidat H el nombre de parells de missatges on $\Delta X_r = \Delta Y_{r-1}$ serà usualment menor, ja que el desxiframent parcial resultarà en prediccions pseudo-aleatòries de X_r. Pot ocórrer que un candidat H erroni tingui un comptador més alt del que no s'esperaria d'una variable aleatòria amb distribució uniforme, però segons Biham i Shamir l'algorisme aconsegueix extreure la clau correcte en un $99'9\%$ dels casos [13].

També aconsegueix exposar en el DES una vulnerabilitat de seguretat si es redueix el nombre de rondes a menys de setze [3,13,21]. La quantitat de parelles de *missatges plans* necessàries per a l'algorisme és de l'ordre de $Pr(\Delta Y_{r-1} \mid \Delta P)^{-1}$ [8].

És important notar que si la clau de ronda K_{r+1} no existís, no s'efectuaria cap XOR després de la ronda r-ésima, i llavors el criptosistema tindria, a efectes pràctics, només $r-1$ rondes de xifratge. Això és perquè els resultats de l'última ronda es tornarien trivialment invertibles (en ésser tota caixa de tipus P ó S bijectives, constants i conegudes). De manera similar, l'acció d'una permutació de bloc σ_i ó una caixa-S abans de l'aplicació al *missatge pla* P de la clau de ronda K_1 no aporta cap seguretat al criptosistema, exactament per les mateixes raons. Per tant, en tota xarxa de substitució-permutació, l'ús d'una permutació inicial σ_1 és innecessària a nivell de l'anàlisi de la seguretat. Un exemple és el cas del DES, que efectua tant una permutació inicial IP com una permutació final $FP = IP^{-1}$ [7]. Això planteja una estructura simplificada per a tota xarxa, donada per la proposició següent:

Proposició 2.4.1. *Tota xarxa de substitució-permutació amb* r *rondes es pot simplificar en una estructura* $(P \to XOR \to S)^r \to XOR$, amb $\sigma_1 = Id$, *sense cap pèrdua de generalitat en l'anàlisi de la seguretat de la mateixa.*

2.5 Anàlisi de la seguretat contra l'atac

Considerem totes les possibles parelles de diferències $(\Delta X, \Delta Y)$ d'una caixa S donada, on $S = S_{ij}$ per a alguns $i \in \{1, \dots, r\}$, $j \in \{1, \dots, s\}$. Si considerem totes les *caixes de tipus* S que hi ha en una xarxa de substitució-permutació, aleshores podem definir:

$$PM_{S_i} = \max_{\substack{1 \le j \le s \\ 1 \le i \le r}} \left\{ PM_{S_{ij}} \right\} = \max_{\substack{1 \le j \le s \\ 1 \le i \le r}} \left\{ \max_{(\Delta Y_{S_{ij}},\ \Delta X_{S_{ij}} \neq 0)} \left\{ Pr\left(\Delta Y_{S_{ij}} \mid \Delta X_{S_{ij}} \right) \right\} \right\}.$$

Definició 2.5.1. *Donada una cadena de caràcters* $a \in \mathcal{A}^n$, *on* $a = (a_1, \dots, a_n)$ *per a un alfabet donat* $\mathcal{A}$, *el pes de Hamming* $Hw(a)$ *és el nombre de caràcters no nuls de en la cadena* [9]*:*

$$Hw(a) = \#\{i \mid a_i \neq 0,\ a_i \in \mathcal{A} \quad i \in \{1, \dots, n\}\}$$

Donat l'alfabet $\mathcal{A} = F_{2^k}$, considerarem els vectors de diferències ΔX_i, ΔY_i com a cadenes de s caràcters en aquest alfabet. És important notar que amb aquesta convenció, els caràcters venen donats per les diferències individuals $\Delta X_{S_{ij}}$, $\Delta Y_{S_{ij}}$. Aquesta consideració és important, perquè el *pes de Hamming* de les diferències ΔX_i, ΔY_i ens donarà el nombre de caixes-S *diferencialment actives* a la ronda i.

Segons la proposició 2.4.1, qualsevol xarxa de substitució-permutació es pot simplificar a un esquema estructural com el següent:

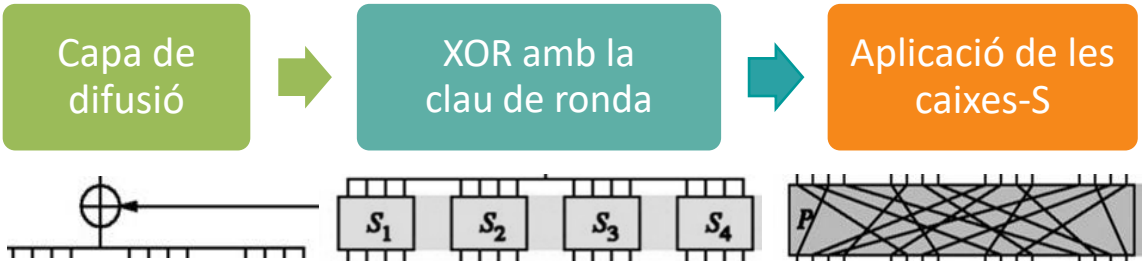


Figura 8: Esquema simplificat del funcionament d'una ronda en una xarxa de substitució-permutació qualsevol.

Per a cada ronda $i \in \{1, \dots, r\}$, anomenarem ***capa de difusió*** a la permutació del bloc sencer donada per σ_i. La seguretat de la xarxa depèn del nombre $n(C_d)$ de caixes de tipus S *diferencialment actives* que pot arribar a tenir una *característica diferencial* C_d qualsevol [8,9]. No obstant, el nombre $n(C_d)$ dependrà de la composició de les *capes de difusió* σ_i que formen la xarxa.

Definició 2.5.2. *Considerem una xarxa SPN qualsevol. Donada* $\sigma_{i \in \{2 \dots r-1\}}$ *una de les seves permutacions de bloc, definim el seu* ***nombre de ramificació diferencial*** *com*

$$NRD(\sigma_i) = \min_{\Delta Y_{i-1} \neq 0} \left\{ Hw(\Delta Y_{i-1}) + Hw\left(\sigma_i(\Delta Y_{i-1})\right) \right\}.$$

És clar que per a tota permutació σ, com que el mínim $Hw(\Delta Y_{i-1})$ és 1, llavors s'ha de complir que $2 \leq NRD(\sigma) \leq s + 1$ [9,20].

Definició 2.5.3. *Una capa de difusió* σ_i *és* ***maximal*** *o* ***òptima*** *si i només si* $NRD(\sigma_i) = s + 1$.

Com que les aplicacions σ_i són lineals, tenim que $\sigma_i(X \oplus X') = \sigma_i(X) \oplus \sigma_i(X')$. Si podem representar-les com a matrius, com per a qualsevol matriu M se satisfà que $M(x \oplus x') = M(x) \oplus M(x')\ \forall x, x' \in F_{2^k}^s$, aleshores es té que l'acció de cada permutació σ_i és igual a l'acció d'una matriu $M_i = (m_{i\ jk})$ de dimensió $s \times s$, de tal manera que $m_{i\ jk} \in F_{2^k}$ i on $M_i\, x = \sigma_i(x)$.

$$M_i = \begin{pmatrix} m_{i\ 11} & \dots & \dots & m_{i\ 1s} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ m_{i\ s1} & \dots & \dots & m_{i\ ss} \end{pmatrix} = \begin{pmatrix} \sigma_i(1, \dots, 0) \\ \vdots \\ \vdots \\ \sigma_i(0, \dots, 1) \end{pmatrix}.$$

Podem reescriure el *nombre de ramificació diferencial* com [9]:

$$NRD(\sigma_i) = \min_{\Delta Y_{i-1} \neq 0} \{ Hw(\Delta Y_{i-1}) + Hw(M_i \cdot \Delta Y_{i-1}) \}$$

A partir d'ara, obviarem les claus de ronda ja que no afecten a les diferències.

Proposició 2.5.4. *Sigui $M_i \in M_{s\times s}$ una matriu que representi la capa de difusió σ_i, amb $2 \leq i \leq s$. La capa de difusió σ_i és maximal si i només si la matriu M_i no té cap submatriu $M_{l\times l}$ singular, $\forall l \in \{1, \dots, s\}$.*

DEMOSTRACIÓ. [$\Longrightarrow$] Suposem que existeix $l \leq s$ tal que la submatriu $M_{l\times l}$ té determinant nul. Aleshores $\exists \Delta Y_{i-1} \neq 0$ tal que

$$\begin{pmatrix} m_{i\ 11} & \dots & \dots & m_{i\ 1l} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ m_{i\ l1} & \dots & \dots & m_{i\ ll} \end{pmatrix} \begin{pmatrix} \Delta Y_{S_{i-1}\ 1} \\ \vdots \\ \vdots \\ \Delta Y_{S_{i-1}\ k} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}.$$

Ampliant fins a $M = M_{s\times s}$ i considerant $\Delta Y_{i-1} = \left(\Delta Y_{S_{i-1}\ 1}, \dots, \Delta Y_{S_{i-1}\ l}, 0, \dots, 0\right)^T$, obtenim que

$$\begin{pmatrix} m_{i\ 11} & \dots & \dots & m_{i\ 1l} & \dots & \dots & \dots & m_{i\ 1s} \\ \vdots & & & \vdots & & & & \vdots \\ \vdots & & & \vdots & & & & \vdots \\ m_{i\ l1} & \dots & \dots & m_{i\ ll} & \dots & \dots & \dots & m_{i\ ks} \\ \vdots & & & \vdots & & & & \vdots \\ \vdots & & & \vdots & & & & \vdots \\ \vdots & & & \vdots & & & & \vdots \\ m_{i\ s1} & \dots & \dots & m_{i\ sk} & \dots & \dots & \dots & m_{i\ ss} \end{pmatrix} \begin{pmatrix} \Delta Y_{S_{i-1}\ 1} \\ \vdots \\ \vdots \\ \Delta Y_{S_{i-1}\ l} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \\ \delta_{k+1} \\ \vdots \\ \delta_s \end{pmatrix}.$$

Aquí $\delta_j \in F_{2^k}$, $\forall j \in \{l+1, \dots, s\}$. Aleshores és cert que $Hw(M \cdot \Delta Y_{i-1}) \leq s - l$, i la *capa de difusió* σ_i no pot ser maximal, atès que

$$NRD(\sigma_i) \leq Hw(\Delta Y_{i-1}) + Hw(M_i \cdot \Delta Y_{i-1}) \leq l + (s - l) = s < s + 1\,.$$

[$\Longleftarrow$] Suposem ara que $NR(\sigma_i) < s + 1$. Aleshores existeix una diferència ΔY_{i-1} tal que $NRD(\sigma_i) \leq Hw(\Delta Y_{i-1}) + Hw(M_i \cdot \Delta Y_{i-1}) \leq s$. Suposem que en ΔY_{i-1} hi ha l elements no nuls, de manera que $\Delta Y_{S_{i-1}\ j} = 0$ per a $j \in \{l+1, \dots, s\}$. Llavors el *pes de Hamming* seria $Hw(\Delta Y_{i-1}) = l$, i obtenim que $Hw(M_i \cdot \Delta Y_{i-1}) \leq s - l$.

Per tant, M_i té una submatriu $M_{l\times l}$ formada pels índexs $i_1, \dots, i_l$ dels elements nuls de $M_i \cdot \Delta Y_{i-1}$, tals que $M_{l\times l} \cdot \Delta Y_{i-1} = 0 \Longrightarrow M_{l\times l}$ és singular. ■

Proposició 2.5.5. *Donada una xarxa de substitució-permutació, considerem una característica diferencial* C_d *amb probabilitat associada* $Pr(C_d)$*. Suposant que els diferencials de* C_d *tenen probabilitats independents, aleshores*

$$Pr(C_d) \leq \max_{S_{ij}} \left\{ Pr\left(\Delta Y_{S_{ij}} \,\middle|\, \Delta X_{S_{ij}} \right) \right\}^{\sum_{i \text{ parell}}^{r-1} NRD(\sigma_i) + r - 1 \,(mod\, 2)}.$$

DEMOSTRACIÓ. Considerem la col·lecció d'índexs $J(i)$ definida de la següent manera:

$$J(i) = \left\{ j \in \{1, \dots, s\} \mid \exists x \in C_d,\ \left(\Delta X_{S_{ij}} \neq 0,\ \Delta Y_{S_{ij}} \right) \in x \right\}.$$

Aquest conjunt ens dóna les caixes-S *diferencialment actives* a cada ronda, i en conseqüència tenim que $\sum_i \#J(i) = n(C_d)$. Sota la hipòtesi d'independència dels *diferencials,* obtenim que

$$Pr(C_d) = \prod_{i=1}^{r-1} Pr(\Delta Y_i \mid \Delta X_i) = \prod_{i=1}^{r-1} \prod_{j \in J(i)} Pr\left(\Delta Y_{S_{ij}} \mid \Delta X_{S_{ij}} \right) \leq$$

$$\leq \prod_{i=1}^{r-1} \prod_{j \in J(i)} PM_{S_i} \leq \prod_{i=1}^{r-1} \prod_{j \in J(i)} \max_{1 \leq i \leq s} \left\{ PM_{S_i} \right\} \leq \max_{1 \leq i \leq s} \left\{ PM_{S_i} \right\}^{n(C_d)}.$$

Per tant,

$$Pr(C_d) \leq \max_{S_{ij}} \left\{ Pr\left(\Delta Y_{S_{ij}} \,\middle|\, \Delta X_{S_{ij}} \right) \right\}^{n(C_d)}.$$

Una cota inferior de $n(C_d)$ vindrà donada pel mínim nombre de caixes de tipus S *diferencialment actives* que pot haver-hi en cada ronda*:*

$$Pr(C_d) \leq \max_{S_{ij}} \left\{ Pr\left(\Delta Y_{S_{ij}} \,\middle|\, \Delta X_{S_{ij}} \right) \right\}^{\sum_{i \text{ parell}}^{r-1} NRD(\sigma_i) \,+ \left(r - 1 \,(mod\, 2)\right)}.$$

Com que $NRD(\sigma_i)$ compta la quantitat de caixes-S amb entrada o sortida no nul·la en les rondes $i-1$, és necessari sumar per parells. Finalment, si ens falta cap ronda sense considerar, hi haurà com a mínim una caixa-S *diferencialment activa.* ■

Proposició 2.5.6. *Sigui el diferencial global* $(\Delta P,\ \Delta Y_{r-1})$ *donat per l'elecció d'una característica diferencial qualsevol en el nostre criptosistema. Aleshores, poden existir diverses característiques* C_d *on* $(\Delta X_1 = \Delta P,\ \cdot), (\cdot,\ \Delta Y_{r-1}) \in C_d$*, i per tant la probabilitat del diferencial global és*

$$Pr(\Delta Y_{r-1} \mid \Delta \mathrm{P}) = \sum_{\substack{C_d \\ (\Delta P,\ \cdot)\,(\cdot,\ \Delta Y_{r-1}) \in C_d}} Pr(C_d)$$

Conclusions

És important destacar que el valor que cal considerar a l'hora de considerar la seguretat del criptosistema vers la criptoanàlisi diferencial és $p = Pr(\Delta Y_r \mid \Delta P)$, ja que és el valor que influeix en l'ordre de complexitat de l'atac. No obstant, generalment no ens resulta possible calcular aquest valor, i per tant usarem l'aproximació donada per la probabilitat $Pr(C_d)$. La cota superior de $Pr(C_d)$ determina les propietats que ha tenir una xarxa de substitució-permutació per a considerar-se segura contra un atac diferencial [8,13,21].

1. Cap caixa de tipus S no pot tenir cap parella de diferències amb probabilitat d'ocórrer gaire alta, minimitzant $\max_{1 \le i \le s} \{ PM_{S_i} \}$.
2. Les caixes de tipus P han de tenir un *nombre de ramificació* alt, per a maximitzar el valor de $\sum_{i \text{ parell}}^{r-1} NRD(\sigma_i)$. Això implica utilitzar caixes-P expansives.

Si es compleixen aquestes propietats, aleshores $\max\{Pr(C_d) - 2^{d-b},\ 0\} = 0,\ \forall d,$ donat un valor de r suficientment gran, i podem considerar que queda provat que el criptosistema és segur contra un possible atac diferencial. Cal ser curosos en tot cas, recordant que [8]:

i. El càlcul està basat en la suposició que els *diferencials* de cada ronda en C_d són independents, que tot i ésser una relaxació raonable de les condicions per a efectuar el càlcul, pot no ésser certa.

ii. La probabilitat $Pr(C_d)$ de la *característica* és menor a la probabilitat del *diferencial global* $p = P(\Delta Y_r \mid \Delta P)$, i per tant la complexitat real de l'atac és lleugerament menor.

Així doncs, és important ser generosos amb els marges de seguretat que donem, optimitzant al màxim les caixes de tipus S i P de la xarxa, i augmentant si cal el nombre de rondes del criptosistema.

3 La criptoanàlisi lineal

3.1 Resum de l'atac

La criptoanàlisi lineal és un atac criptogràfic descobert en 1993 pel criptòleg nipó Mitsuru Matsui [15], basat en l'ús d'aproximacions lineals i afins de l'acció del criptosistema. Matsui muntà el primer atac experimental un any després sobre el Data Encryption Standard (DES) [16]. Avui dia, s'espera que tot nou criptosistema de xifrat en bloc sigui resistent contra la criptoanàlisi lineal [23]. Similarment al capítol anterior, exposarem el funcionament de l'atac lineal tan sols en el cas de les xarxes de substitució-permutació.

La criptoanàlisi lineal, com la criptoanàlisi diferencial, es basa en l'assumpció del coneixement del funcionament del criptosistema (màxima de seguretat de Shannon). En aquest treball, exposarem només el funcionament de l'anomenat Algorisme 2 que exposa Matsui en el seu article, ja que és el més utilitzat.

Definició 3.1.1. *Denotem l'entrada d'una caixa-S del criptosistema com a X, i la modelitzarem com a una variable aleatòria. Anàlogament, denotarem amb Y a la sortida d'una caixa-S, on $Y = S(X)$ també és una variable aleatòria.*

Definició 3.1.2. *Donats dos vectors X, Y d'entrada i sortida (d'una caixa de tipus S, o d'una ronda sencera), qualsevol expressió $E(X,Y)$ del tipus següent*:

$$\bigoplus_{j=1}^{k} \alpha_j X_j \bigoplus_{j=1}^{k} \beta_j Y_j = c \qquad \alpha, \beta, X, Y \in F_{2^k}\,,\ c \in F_2\,,\ \forall j \in \{1, \dots, k\}\,.$$

*és una **expressió lineal** si $c = 0$, o una **expressió afí** si $c = 1$. Els valors $\alpha_j, \beta_j \in \{0,1\}$ són els coeficients d'aquesta expressió $E(X,Y)$, que és un polinomi de primer grau en les variables X_j, Y_j.*

Proposició 3.1.3. *Si les variables X, Y tinguessin distribució uniforme, llavors es tindria que per a tota expressió $E(X,Y)$ es compleix que* [8]:

$$Pr(E(X,Y) = 0) = Pr(E(X,Y) = 1) = 1/2\,.$$

DEMOSTRACIÓ. Trivial. ■

Definició 3.1.4. *Per a tota expressió lineal $E(X,Y)$, definim el seu **biaix lineal** com $\varepsilon = Pr(E(X,Y) = 0) - 1/2$. Per a tota expressió afí $E(X,Y)$, definim el seu biaix com l'oposat del biaix de l'expressió complementària $E(X,Y) \oplus 1$.*

L'objectiu de l'atac es basa en trobar una expressió involucrant els bits del *missatge pla* P amb un alt biaix en valor absolut $|\varepsilon| = |\, Pr(E(P, \cdot) - 1/2\,|$. Com més alt sigui aquest biaix, més s'allunya el criptosistema del comportament aleatori que s'espera, i per tant més vulnerable resulta, atès que tindrà una pobre capacitat d'ofuscació. Les *expressions lineals* o *afins* amb un alt biaix es poden utilitzar per a vulnerar la seguretat del criptosistema mitjançant tècniques similars a les usades en la criptoanàlisi diferencial.

Definició 3.1.5. *Una expressió* $E(X,Y)$ *escollida d'una caixa de tipus* S *on els vectors de coeficients* $\alpha = (\alpha_1, \dots, \alpha_k), b = (\beta_1, \dots, \beta_k)$ *tenen algun element* $\neq 0$ *s'anomena* ***aproximació lineal*** *de la caixa* S [8,16].

Tindrà un biaix associat de $\varepsilon_S = Pr(E_S(X,Y) = 0) - 1/2$, *on* $\varepsilon_S \in \left[-\frac{1}{2}, +\frac{1}{2}\right]$.

Podem generalitzar el concepte d'*aproximació lineal* al cas on X, Y són vectors d'entrada i sortida en rondes. Considerant *aproximacions lineals* de diferents caixes S_{ij} d'una mateixa ronda, aleshores l'*aproximació lineal* de tota la ronda vindrà donada pel vector següent:

$$E(X_i, Y_i) = \left(E_{S_{i\,1}}(X_{S_{i\,1}},\, Y_{S_{i\,1}}), \dots, E_{S_{i\,s}}\left(X_{S_{i\,s}},\, Y_{S_{i\,s\,i}}\right)\right).$$

X, Y són els vectors d'entrada i sortida de tot el bloc a la ronda i-èsima, amb $i \in \{1, \dots, r\}$. Es a dir: $X_i = \left(X_{S_{i\,1}}, \dots, X_{S_{i\,s}}\right),\ Y_i = \left(Y_{S_{i\,1}}, \dots, Y_{S_{i\,s}}\right)$.

Utilitzant aproximacions adequades de cada ronda, de manera que els bits de Y_i considerats en l'*aproximació lineal* $E(X_i, Y_i)$ d'una ronda i es corresponguin amb el bits de X_{i+1} de la ronda següent, podem trobar *expressions lineals* amb entrada en una ronda i sortida en l'altra. Per exemple,

$$X_{i1} \oplus X_{i3} \oplus X_{i5} \oplus X_{i7} \oplus Y_{i+1,3} \oplus Y_{i+1,6} \oplus K_{i+1,3} \oplus K_{i+1,6} = 0\,.$$

Fixem-nos que, com que les claus de ronda K_i no varien en base al *missatge pla* que estem xifrant, la suma $\Sigma\, K_{ij}$ dels bits de la clau de ronda és un valor fix. Podem considerar la mateixa expressió sense aquests bits [8,16,17], quedant

$$E(X_i, Y_{i+1}):\ X_{i1} \oplus X_{i3} \oplus X_{i5} \oplus X_{i7} \oplus Y_{i+1,3} \oplus Y_{i+1,6} = 0\,.$$

Així, els bits de la clau de ronda queden implícits en aquesta *expressió lineal*, ja que si $\Sigma\, K_{ij} = 0$ aleshores $E(X_i, Y_{i+1})$ tindrà biaix ε, i si $\Sigma\, K_{ij} = 1$ serà $-\varepsilon$.

Definició 3.1.6. *Donada una successió* $\{E(X_i, Y_i)\}_{1 \le i \le r-1}$ *d' aproximacions lineals de cada una de les rondes excepte l'última, aquesta s'anomena el* ***camí lineal*** (*a vegades també anomenada característica lineal*). *La notarem com* $\mathcal{CL}$.

Cada camí lineal determina una nova expressió $E(P, Y_{r-1})$ que és la ***coberta lineal*** $\mathcal{L}$. La seva probabilitat i biaix són molt difícils de calcular, ja que una mateixa *coberta lineal* pot venir donada per diferents *característiques lineals*, anàlogament al cas del *diferencial global* i les *característiques diferencials*.

És important remarcar que ni el *camí lineal* ni la *coberta lineal* són úniques, ja que depenen de les *expressions lineals* $E(X_i, Y_i)$ escollides per a aproximar cada ronda. Denotarem per $\varepsilon_{\mathcal{L}}$ el biaix de la *coberta lineal*. Matsui enuncia que són necessaris $N \approx \varepsilon_{\mathcal{L}}^{-2}$ missatges plans per a muntar l'atac [16], com ja veurem.

Algorisme de l'atac lineal

(1) Trobar un camí / característica lineal $\mathcal{CL}$ amb biaix $\varepsilon_{\mathcal{CL}}$, tal que $2^d \cdot \varepsilon_{\mathcal{L}}{}^{-2} \leq 2^b$.

(2) Generar un missatge aleatori P, i computar $C = e_K(P)$.

(3) Crear una taula de comptadors, inicialitzats a 0, de tots els possibles valors dels bits H de K_{r+1} que coincideixen amb les caixes-S amb bits d'entrada considerats en $\mathcal{CL}$.

(4) Computar Y_{r-1} desxifrant parcialment l'última ronda amb H.

(5) Avaluem $\mathcal{L}$. Si l'expressió és correcta, augmentem en 1 el comptador de H.

(6) Finalment, després d'analitzar N missatges generats aleatòriament, escollim el candidat H amb comptador al més allunyat del valor esperat de $N/2$.

En la seva formulació típica, la criptoanàlisi lineal és un *atac de missatge pla conegut*: l'atacant pot escollir *missatges plans* P i xifrar-los per a obtenir els *missatges xifrats* C corresponents tantes vegades com vulgui. Si l'atacant pot trobar una *aproximació lineal* amb biaix $\varepsilon_{\mathcal{L}}$ tal que $\mathcal{O}\left(2^d \cdot \varepsilon_{\mathcal{CL}}^{-2}\right) \leq \mathcal{O}(2^b)$, llavors pot recuperar d *bits* de l'última clau de ronda K_{r+1}. Per a trobar la resta dels bits, pot tornar a aplicar l'atac, o fer una cerca exhaustiva [5, 21].

Com ja vàrem comentar en el capítol anterior, hi ha alguns criptosistemes on és possible determinar el valor de la clau general K si obtenim alguna clau de ronda, com és el cas del Data Encryption Standard.

Considerarem que un criptosistema és segur contra la criptoanàlisi lineal si la complexitat de l'algorisme anterior és major a la d'un atac per força bruta (per això comparem la complexitat d'execució amb 2^b, que són els càlculs necessaris per a trobar K_{r+1} en un atac per força bruta, essent b la mida dels blocs). Aquesta condició només es complirà si $\max\{\varepsilon_{\mathcal{CL}}^2 - 2^{d-b},\ 0\} = 0$, per a tot valor de d i per a tot *camí lineal* $\mathcal{L}$ del criptosistema.

Com en el cas de la criptoanàlisi diferencial, aquesta seguretat vindrà influïda pel nombre de rondes r que tingui el procés de xifratge, les *capes de difusió* del criptosistema, i els biaixos ε_S de les *expressions lineal* o *afins* de les caixes-S.

3.2 Aproximació lineal d'una caixa-S

Proposició 3.2.1. *Sigui una xarxa de substitució-permutació funcionant sobre blocs de* b *bits, amb* r *rondes de xifratge,* s *caixes de tipus P i S que denotarem* $\sigma_{ij}, S_{ij}, \forall i \in \{1,\dots,r\}, j \in \{1,\dots,s\}$ *respectivament i on* $2^k s = b$ i $S_{ij}: F_{2^k} \to F_{2^k}$. *Suposarem també que les caixes són constants i conegudes.*

Donada una caixa $S: F_{2^k} \to F_{2^k}$ *d'aquesta xarxa, existeixen* $\tilde{\alpha} = (\tilde{\alpha}_1,\dots,\tilde{\alpha}_k) \neq 0$, $\tilde{\beta} = (\tilde{\beta}_1,\dots,\tilde{\beta}_k) \neq 0$ *tals que:*

$$\left| Pr(\alpha \cdot X \oplus \beta \cdot Y) - \frac{1}{2} \right| \leq \left| Pr(\tilde{\alpha} \cdot X \oplus \tilde{\beta} \cdot Y) - \frac{1}{2} \right|, \quad \forall \alpha, \beta, X, Y \in F_2^k,$$

$$\mathrm{M}\varepsilon_S = \left| Pr(\tilde{\alpha} \cdot X \oplus \tilde{\beta} \cdot Y) - 1/2 \right|.$$

DEMOSTRACIÓ. Considerar tots els possibles valors de $\alpha, \beta \in F_2^k$ equival a l'el·lecció de quins bits considerar en X i Y, siguin quin siguin els seus valors. Com n'hi ha un total de 2^{2k} possibilitats, que és un nombre finit, existeix una elecció $\tilde{\alpha}, \tilde{\beta}$ amb biaix maximal. ■

Per tant, sigui quina sigui l'expressió $E_S(X,Y)$ que triem d'una *caixa de tipus S* de la xarxa, com més pròxim sigui el seu biaix maximal $\mathrm{M}\varepsilon_S$ a zero, més segura serà la xarxa i menys pràctic serà l'atac. Anem a centrar-nos ara a trobar una expressió adient d'una *caixa de tipus S,* a ser possible una amb biaix maximal. Sigui la permutació no lineal següent:

S: $F_{2^4} \to F_{2^4}$

0 --> 2	8 --> 7
1 --> 3	9 --> 0
2 --> 9	10 --> 5
3 --> 12	11 --> 10
4 --> 11	12 --> 8
5 --> 4	13 --> 13
6 --> 15	14 --> 6
7 --> 1	15 --> 14

Proposem diferents expressions que podríem fer servir per a aproximar S:

$$X_2 = Y_1 \oplus Y_2, \qquad X_1 \oplus X_3 = Y_1 \oplus Y_2,$$
$$X_3 \oplus X_4 = Y_2 \oplus Y_4, \qquad X_1 = Y_1 \oplus Y_2.$$

Tenint en compte que cada nombre d'entrada X es descompon en la seva expressió binària (X_1, X_2, X_3, X_4), i anàlogament per a la sortida Y, tenim que:

$$Pr(X_2 = Y_1 \oplus Y_2) = Pr(X_2 \oplus Y_1 \oplus Y_2 = 0) = 12/16 \implies \varepsilon = +1/4\,,$$

$S(0)$	$S(1)$	$S(2)$	$S(3)$	$S(4)$	$S(5)$	$S(6)$	$S(7)$
$S(8)$	$S(9)$	$S(10)$	$S(11)$	$S(12)$	$S(13)$	$S(14)$	$S(15)$

Per tant, $X_2 \oplus Y_1 \oplus Y_2 = 0$ resulta una *aproximació lineal* de la caixa S bastant encertada. En la taula podem veure en verd els casos on l'expressió és certa, i en gris els casos on no ho és, que són: $0 \to 2,\ 3 \to 12,\ 6 \to 15$ i $13 \to 13$.

$$Pr(X_1 \oplus X_3 \oplus Y_1 \oplus Y_2 = 0\,) = 4/16 \implies \varepsilon = -1/4\,,$$

$S(0)$	$S(1)$	$S(2)$	$S(3)$	$S(4)$	$S(5)$	$S(6)$	$S(7)$
$S(8)$	$S(9)$	$S(10)$	$S(11)$	$S(12)$	$S(13)$	$S(14)$	$S(15)$

En aquest cas, el biaix és el mateix que l'anterior en valor absolut, i per això tant *l'expressió lineal* $X_2 \oplus Y_1 \oplus Y_2 = 0$ com *l'expressió* $X_1 \oplus X_3 \oplus Y_1 \oplus Y_2 = 0$ són igual de bones. Per acabar:

$$Pr(X_3 \oplus X_4 \oplus Y_2 \oplus Y_4 = 0\,) = 2/16 \implies \varepsilon = -3/8\,,$$

$S(0)$	$S(1)$	$S(2)$	$S(3)$	$S(4)$	$S(5)$	$S(6)$	$S(7)$
$S(8)$	$S(9)$	$S(10)$	$S(11)$	$S(12)$	$S(13)$	$S(14)$	$S(15)$

$$Pr(X_1 \oplus Y_1 \oplus Y_2 = 0\,) = 8/16 \implies \varepsilon = 0\,.$$

$S(0)$	$S(1)$	$S(2)$	$S(3)$	$S(4)$	$S(5)$	$S(6)$	$S(7)$
$S(8)$	$S(9)$	$S(10)$	$S(11)$	$S(12)$	$S(13)$	$S(14)$	$S(15)$

Podem crear una taula T que contingui la quantitat d'encerts/èxits de cada una de les expressions possibles menys 2^{k-1}, de manera que en dividir per 2^k obtinguem el biaix ε de cada expressió $E_S(X, Y)$ considerada. En concret:

$$|\mathrm{M}\varepsilon_S| = \frac{\max_{i,j} |T_{ij}|}{2^k}\,.$$

Aquesta taula es coneix com a ***taula d'aproximació lineal*** [8], i ens serveix per a fer-nos una idea de les bones propietats d'aleatorietat i ofuscació que té cada una de les caixes-S de la xarxa.

Proposició 3.2.2. *Totes les entrades de la taula d'aproximació lineal de S són nombres parells.*

DEMOSTRACIÓ. Considerem una expressió $E_S(X,Y)$ qualsevol d'entre les 2^{2k} possibles. Agruparem tots els sumands X_i com un únic valor BX, i anàlogament agruparem tots els sumands Y_i com un únic valor BY. Està clar que BX, BY són valors binaris, i per tant tindran un valor fixat 0 ó 1 en la meitat dels casos a considerar, que són 2^{k-1} (recordem que 2^k és la mida de la caixa S). Podem representar les possibles combinacions dels estats de BX, BY i en quants casos s'hi compleixen aquestes combinacions de la forma següent:

BX	BY		
1	1	$\leftarrow x$	(desconegut)
1	0	$\leftarrow 2^{k-1} - x$	($BX = 1$ en la meitat dels casos)
0	1	$\leftarrow 2^{k-1} - x$	($BY = 1$ en la meitat dels casos)
0	0	$\leftarrow 2^{k-1} - (2^{k-1} - x)$	($BX = 0$ en la meitat dels casos)

Així doncs, $E_S(X,Y) = BX \oplus BY = 0$ es complirà en $2x$ casos, que és un nombre parell, on $0 \leq x \leq 2^{k-1}$. Restar un nombre parell a un altre no canvia la seva paritat, per tant tot element de la taula és parell. ■

Les *taules d'aproximació lineal* són eines molt útils per a determinar quina és la *expressió lineal* o *afí* d'una caixa-S donada que millor l'aproxima.

		b en hexadecimal															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
a en hexadecimal	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	-2	-2	0	0	+2	+2	0	0	+2	-2	-4	-4	+2	-2	0
	2	0	0	0	+4	+2	+2	-2	+2	+2	+2	-2	+2	0	0	0	-4
	3	0	+2	-2	0	+2	0	0	-2	-2	-4	0	-2	0	+2	+2	-4
	4	0	0	0	0	+2	+2	-2	-2	+2	-2	-2	+2	0	+4	0	+4
	5	0	-2	+2	-4	-2	0	0	-2	+2	0	0	+2	0	+2	-2	-4
	6	0	0	-4	0	0	0	+4	0	+4	0	0	0	+4	0	0	0
	7	0	+2	-2	0	-4	+2	-2	-4	0	+2	-2	0	0	-2	+2	0
	8	0	-2	0	+2	+2	-4	-2	-4	0	+2	0	-2	+2	0	-2	0
	9	0	0	-2	-2	+2	+2	0	0	-4	+4	+2	+2	+2	+2	0	0
	A	0	+2	-4	-2	0	-2	-4	+2	+2	0	+2	0	-2	0	-2	0
	B	0	0	+2	-2	0	0	-2	+2	+2	+2	0	-4	+2	+2	+4	0
	C	0	+2	0	-2	0	-2	0	+2	-2	0	-6	0	+2	0	-2	0
	D	0	+4	+2	-2	+4	0	+2	-2	+2	+2	0	0	-2	-2	0	0
	E	0	-2	0	-2	+2	+4	-2	0	0	-2	0	-2	+2	-4	-2	0
	F	0	+4	+2	+2	-2	+2	0	0	0	0	+2	-2	+2	+2	-4	0

A l'hora de triar la millor expressió utilitzant la taula, cal obviar les primeres fila i columna, perquè representen expressions del tipus $X_j = 0$ i $Y_j = 0$, que tindran sempre 2^{k-1} encerts, i no ens donen per tant cap nova informació.

3.3 Lema de l'apilament

Ara que ja sabem escollir la millor *aproximació lineal* d'una caixa de tipus S, ens cal un eina que ens permeti combinar diferents *aproximacions lineals* i els seus biaixos, per tal de calcular el biaix del *camí lineal* [8,16].

Lema 3.3.1. (Lema de l'apilament)
Siguin $B_1, \dots, B_n$ *variables aleatòries binàries independents, on* $n \in \mathbb{N}$ *qualsevol. Definim* $p_i = Pr(B_i = 0)$ *així com* $\varepsilon_i = p_i - 1/2$, *per a cada* $1 \le i \le n$.
Aleshores:

$$Pr(B_1 \oplus \dots \oplus B_n = 0) = \frac{1}{2} + \varepsilon_{1\dots n}\,, \quad \text{on } \varepsilon_{1\dots n} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i\,.$$

DEMOSTRACIÓ. Demostrarem el Lema de l'apilament per inducció sobre n:

És trivial veure que si $n = 1$ es compleix la igualtat, ja que $Pr(B_1) = 1/2 + \varepsilon_1$, per definició del biaix ε_1.

Sigui ara certa aquesta propietat fins a un cert nombre $t \in \mathbb{N}$; anem a veure que la igualtat també és certa en el cas $t + 1$. Considerem $T = B_1 \oplus \dots \oplus B_t$,

$$Pr(B_1 \oplus \dots \oplus B_{t+1} = 0) = Pr(T \oplus B_{t+1})\,,$$
$$Pr(T \oplus B_{t+1} = 0) = Pr(T = 0 \cap B_{t+1} = 0) + Pr(T = 1 \cap B_{t+1} = 1)\,.$$

Per hipòtesi, les variables $B_1, \dots, B_{t+1}$ són independents. Obtenim que

$$Pr(T \oplus B_{t+1} = 0) = Pr(T = 0) \cdot Pr(B_{t+1} = 0) + Pr(T = 1) \cdot Pr(B_{t+1} = 1).$$

Denotant la probabilitat $Pr(T = 0)$ per p_T, i aplicant la hipòtesi d'inducció:

$$Pr(T \oplus B_{t+1} = 0) = p_T \cdot p_{t+1} + (1 - p_T) \cdot (1 - p_{t+1})\,,$$
$$Pr(T \oplus B_{t+1} = 0) = 2p_T p_{t+1} - p_T - p_{t+1} + 1\,,$$
$$Pr(T \oplus B_{t+1} = 0) = 2\left(\tfrac{1}{2} + \varepsilon_T\right)\left(\tfrac{1}{2} + \varepsilon_{t+1}\right) - \left(\tfrac{1}{2} + \varepsilon_T\right) - \left(\tfrac{1}{2} + \varepsilon_{t+1}\right) + 1\,,$$
$$Pr(T \oplus B_{t+1} = 0) = \tfrac{1}{2} + 2\varepsilon_T \varepsilon_{t+1}\,,$$
$$Pr(T \oplus B_{t+1} = 0) = \tfrac{1}{2} + 2\,\varepsilon_{1\dots t}\,\varepsilon_{t+1}\,,$$

$$Pr(B_1 \oplus \dots \oplus B_{t+1} = 0) = \frac{1}{2} + 2^{t-1} \prod_{i=1}^{t} \varepsilon_i\,\varepsilon_{t+1} = \frac{1}{2} + 2^t \prod_{i=1}^{t+1} \varepsilon_i\,. \qquad \blacksquare$$

3.4 Construcció d'aproximacions lineals completes

Considerem un altre cop una xarxa de substitució-permutació amb r rondes en el procés de xifratge, s caixes de tipus S en cada ronda, blocs de b bits, i on $b = s \cdot 2^k$ amb $k \in \mathbb{N}$ donat per les caixes $S: F_{2^k} \to F_{2^k}$ de la xarxa. Expressem de manera resumida el funcionament de la xarxa amb aquest esquema:

$$
\begin{aligned}
&\textit{Missatge pla:} && P_{[0\,\ldots\,b]} = Y_0, \\
&\text{Ronda 1:} && X_1 = \sigma_1(Y_0) \oplus K_1 \quad \longrightarrow\ Y_1 = \big(S_{11}(X_1), \ldots, S_{1\,s}(X_1)\big), \\
&\text{Ronda 2:} && X_2 = \sigma_2(Y_1) \oplus K_2 \quad \longrightarrow\ Y_2 = \big(S_{21}(X_2), \ldots, S_{2\,s}(X_2)\big), \\
&\ \vdots \\
&\text{Ronda } r\text{:} && X_r = \sigma_r(Y_{r-1}) \oplus K_r \quad \longrightarrow\ Y_r = \big(S_{r1}(X_r), \ldots, S_{r\,s}(X_r)\big), \\
&\textit{Missatge xifrat:} && C_{[0\,\ldots\,b]} = Y_r \oplus K_{r+1}.
\end{aligned}
$$

Recordem que σ_1 no ofereix cap seguretat addicional a la xarxa, i que per la proposició 2.4.1, podem considerar que $\sigma_1 = Id$.

Ara que ja sabem quines són les possibles expressions de cada caixa de tipus S, i la seva eficàcia, ens preguntem com muntem el *camí o característica lineal* $\mathcal{CL}$ de manera que el seu biaix $\varepsilon_{\mathcal{CL}}$ tingui un valor absolut al més gran possible [7,13,21]. Com ja hem vist a l'anterior capítol, això dependrà de les *capes de difusió* o permutacions σ_i entre les rondes.

Per exemple: sigui una xarxa de substitució-permutació tal que $b = 16$, $r = 4$, $s = 4$, $k = 4$ i amb permutacions $\sigma_{ik} = \sigma_{jk}\ \ \forall i, j \in \{2, \ldots, r\}$, $k \in \{1, \ldots, s\}$. Podem veure a continuació un esquema representatiu d'aquesta xarxa:

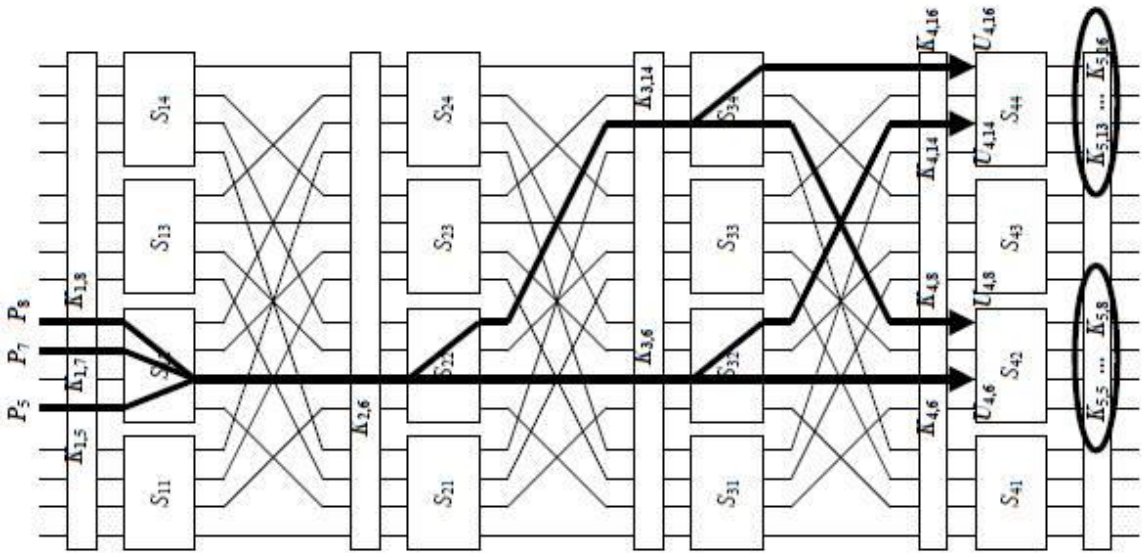


Figura 9: Un possible *camí lineal* en la xarxa de substitució-permutació exemple (imatge original per Howard Heys, extreta de [8]).

En la figura 9, es pot veure el recorregut en la xarxa d'un *camí lineal que* comença amb els bits P_5, P_7, P_8. El camí resseguit és:

Ronda 1
En la primera caixa-S, que és S_{12}, considerem l'*aproximació lineal* donada per:

$$E_{S_{12}}(X_1, Y_1): \; X_{1,5} \oplus X_{1,7} \oplus X_{1,8} \oplus Y_{1,6} = 0\,,$$

La seva probabilitat és $14/16$, i per tant el seu biaix és $\varepsilon_{S_{12}} = +3/8$.

Ronda 2
En la primera caixa-S, que és S_{22}, considerem l'*aproximació lineal* donada per:

$$E_{S_{22}}(X_2, Y_2): \; X_{2,6} \oplus Y_{2,6} \oplus Y_{2,8} = 0\,,$$

La seva probabilitat és $4/16$, i per tant el seu biaix és $\varepsilon_{S_{22}} = -1/4$.

Ronda 3
Les caixes a considerar ara són S_{32} i S_{34}, amb *aproximacions lineals*:

$$E_{S_{32}}(X_3, Y_3): \; X_{3,6} \oplus Y_{3,6} \oplus Y_{3,8} = 0\,,$$
$$E_{S_{34}}(X_3, Y_3): \; X_{3,14} \oplus Y_{3,14} \oplus Y_{3,16} = 0\,.$$

Les probabilitats i biaixos són els mateixos: $\varepsilon_{S_{32}} = \varepsilon_{S_{34}} = +3/8$.

Similarment a les *característiques diferencials,* que es construeixen des l'última ronda considerada $(r-1)$ a la primera, es fa el mateix per als *camins lineals.* D'aquesta manera podem fixar d, els bits actius en l'algorisme. Utilitzant el fet que les caixes de tipus P d'aquesta xarxa són permutacions de bits (és a dir, són caixes rectes), tenim que: $Y_{1,6} = X_{2,6}$, $Y_{2,6} = X_{3,6}$, $Y_{2,8} = X_{3,14}$, etcètera. En aquest cas, la *coberta lineal* $\mathcal{L}$ és

$$X_{1,6} \oplus X_{1,7} \oplus X_{1,8} \oplus Y_{3,6} \oplus Y_{3,8} \oplus Y_{3,14} \oplus Y_{3,16} = 0\,.$$

Com que calcular el biaix de $\varepsilon_{\mathcal{L}}$ és molt complicat, utilitzarem usualment $\varepsilon_{\mathcal{CL}}$ com a aproximació (anàlogament al cas de les *característiques* i el *diferencial global).* Per a calcular $\varepsilon_{\mathcal{CL}}$ utilitzarem el **Lema de l'apilament**, suposant que els bits involucrats en el camí $\mathcal{CL}$ són independents (una hipòtesi raonable per a poder efectuar els càlculs, que tot i que pot no ésser certa, ens dóna bones aproximacions en molts criptosistemes [8,17,21]). Obtenim el resultat

$$\varepsilon_{\mathcal{CL}} = 2^3\, \varepsilon_{12}\, \varepsilon_{22}\, \varepsilon_{32}\, \varepsilon_{34} = -27/256\,.$$

La *coberta lineal* té bits no nuls en Y_{r-1} que es corresponen a dues caixes de tipus S diferents, per tant $d = 8$.

Com que és cert que $2^d \cdot \varepsilon_{\mathcal{CL}}^{-2} < 2^b$ per complir-se $23.014{,}013 < 2^{16}$, tenim que l'*aproximació* donada per $\mathcal{L}$ es pot utilitzar amb èxit per tal d'atacar la xarxa d'exemple considerada.

És important remarcar que les *expressions* que considerem en cada caixa per tal d'aproximar-la no necessàriament han de tenir biaix maximal $M\varepsilon_S$, ja que probablement això és impossible. Aquesta afirmació resulta evident si ens fixem en l'exemple donat: l'*aproximació* $E_{S_{22}}(X_2, Y_2)$ escollida en S_{22} no té perquè ser l'*expressió lineal* o *afí* amb major biaix possible, perquè els bits $Y_{2,6}$, $Y_{2,8}$ han d'estar considerats en l'expressió obligatòriament. En tot cas, podem escollir $E_{S_{22}}(X_2, Y_2)$ per tal que tingui biaix maximal amb les condicions que se'ns demanen.

Definició 3.4.1. *A les caixes de tipus S que aproximem linealment amb una expressió* $E_S(X, Y)$ *donada per vectors* $\alpha, \beta \in F_2^k$ *amb* $\alpha, \beta \neq 0$ *les denominem* ***caixes-S linealment actives*** [8,9,13]. *Als vectors* α, β *de* l'*expressió emprada els anomenarem* ***màscares de bits*** [13,16].

En concret, les màscares de bits $\alpha_1 = (\alpha_{S_{11}}, \dots, \alpha_{S_{1s}})$, $\beta_{r-1} = (\beta_{S_{r-1\ 1}}, \dots, \beta_{S_{r-1\ s}})$ són les màscares utilitzades en la *coberta lineal* $\mathcal{L}$, per a tot *camí lineal* que tingui aquestes màscares en la seva aproximació inicial i final.

Definició 3.4.2. D*efinim* $n(\mathcal{CL})$ *com la quantitat de caixes-S linealment actives en un camí lineal* $\mathcal{CL}$*, donada per la fórmula següent*:

$$n(\mathcal{CL}) = \#\left\{ \alpha_{S_{ij}}\ ,\ \beta_{S_{ij}} \neq 0 \;\middle|\; \alpha_{S_{ij}},\ \beta_{S_{ij}} \in E_{S_{ij}}\left(X_{S_{ij}}, Y_{S_{ij}}\right) \subseteq \mathcal{CL} \right\}.$$

Per a poder muntar un atac exitós, ens interessa que la nostra *aproximació lineal* donada pel *camí lineal* $\mathcal{CL}$ tingui el mínim nombre de caixes-S *linealment actives* possible; és a dir, volem minimitzar $n(\mathcal{L})$.

Per contra, un criptosistema serà més segur contra la criptoanàlisi lineal com més *caixes-S linealment actives* tingui, ja que el biaix serà menor.

3.5 Obtenció de l'última clau de ronda

Un cop tenim un *camí lineal* $\mathcal{CL}$ amb d *bits* a considerar i amb probabilitat biaix $\varepsilon_{\mathcal{CL}}$ tal que $2^d \cdot \varepsilon_{\mathcal{CL}}^{-2} < 2^b$, és possible trobar quina és la última clau de ronda utilitzant l'algorisme descrit en la secció 3.1 d'aquest capítol, més una cerca exhaustiva dels $b - d$ *bits* restants.

L'algorisme es basa en el raonament següent: si el candidat H és el correcte, aleshores per a un nombre de *missatges plans* proporcional a $(1/2 + \varepsilon_{\mathcal{L}})$ és té que és certa l'expressió $E(P, Y_{r-1})$ donada per les *màscares de bits* en P i Y_{r-1}. Per a qualsevol altre candidat H el nombre de missatges on l'expressió sigui certa serà usualment menor, ja que $\sigma_r^{-1}\left(S_r^{-1}(C \oplus H)\right)$ resultarà en prediccions pseudo-aleatòries de X_r .

Segons Mitsuru Matsui, aquest algorisme aconsegueix un llistat que contingui els candidats amb comptador més alt on estigui la clau de ronda K_{r+1} un $97'72\%$ dels casos si $N \approx \varepsilon_{\mathcal{L}}^{-2}$ [16]. L'argument que utilitza és el següent:

Proposició 3.5.1. *Sigui T la quantitat de missatges on es compleix la coberta lineal $\mathcal{L}$. Aleshores $Pr(T > N/2) \geq 0{,}9772$ si es té que $N \approx \varepsilon_{\mathcal{L}}^{-2}$.*

DEMOSTRACIÓ. Si $p = P(E(P, Y_{r-1}) = 0) > 1/2$, aleshores $T > N/2$. Com la variable aleatòria T segueix una distribució binomial amb esperança $E[T] = Np$ i variància $Var[T] = p(1-p)$, podem aproximar-la per una normal estàndard:

$$Pr\left(T > \frac{N}{2}\right) = 1 - Pr\left(T \leq \frac{N}{2}\right) \approx 1 - \phi\left(\frac{\frac{N}{2} - Np}{\sqrt{N}\sqrt{p(1-p)}}\right) =$$

$$= 1 - \phi\left(\frac{-\sqrt{N}\left(p - \frac{1}{2}\right)}{\sqrt{p(1-p)}}\right) \geq 1 - \phi\left(-2\sqrt{N}\left(p - \frac{1}{2}\right)\right) \approx \phi\left(2\sqrt{N}\left(p - \frac{1}{2}\right)\right).$$

Per tant, si $N = (p - 1/2)^{-2} = \varepsilon_{\mathcal{L}}^{-2}$ es té que $Pr(T > N/2) = \phi(2) \geq 0{,}9772$. ■

Aquest càlcul serveix també per a justificar que és necessari $N \approx \varepsilon_{\mathcal{L}}^{-2}$ per tal de muntar un atac lineal exitós. No obstant, cal notar que amb aquest algorisme cal provar molts més candidats que en l'algorisme de l'atac diferencial.

3.6 Seguretat contra l'atac lineal

Considerem totes les possibles *aproximacions lineals* d'una caixa S donada, que són les *expressions lineals* i *afins* amb totes les possibles *màscares* $\alpha_S, \beta_S \neq 0$. Siguin S_{ij} , $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$ totes les *caixes de tipus S* que hi ha en una xarxa de substitució-permutació, definim:

$$M\varepsilon = \max_{1 \leq j \leq s} \left\{ \max_{1 \leq i \leq r} \left\{ M\varepsilon_{S_{ij}} \right\} \right\}.$$

El valor $M\varepsilon$ representa el màxim biaix trobat entre totes les caixes-S que hi ha a la xarxa. Sigui Hw la funció *pes de Hamming* que vàrem definir anteriorment en 2.5.1., aleshores donat $\mathcal{A} = F_{2^k}$ considerarem els vectors X_i, Y_i com a

paraules en aquest alfabet, on els caràcters venen donats per les entrades i les sortides de cada caixa-S a la ronda i-èsima: les diferències individuals $X_{S_{ij}}$, $Y_{S_{ij}}$. Així, el *pes de Hamming* ens donarà el nombre de caixes-S *linealment actives* a la ronda i.

Anàlogament a com passava en la criptoanàlisi diferencial, la seguretat de la xarxa dependrà del nombre $n(\mathcal{CL})$ de *caixes de tipus S linealment actives* que pot arribar a tenir un *camí lineal* qualsevol [8,9]. Aquest nombre dependrà, a la seva vegada, de les caixes-P o *capes de difusió* σ_i de la xarxa.

Definició 3.6.1. *Donada una xarxa de substitució-permutació qualsevol i sigui* $\sigma_{i \in \{2 \dots r-1\}}$ *una de les seves capes de difusió, definim el seu* ***nombre de ramificació lineal*** $NRL(\sigma_i)$ *com*

$$NRL(\sigma_i) = \min_{\beta_{i-1} \neq 0} \{ Hw(\beta_{i-1}) + Hw(\sigma_i(\beta_{i-1})) \}.$$

...on β_{i-1} *és la màscara de bits de la sortida* Y_{i-1}*. Per convenció,* $Y_0 = P$*.*

Igual que ocorre amb el *nombre de ramificació diferencial* $NRD(\sigma_i)$, com per a tota permutació σ el mínim $Hw(Y_{i-1})$ és 1, es té que: $2 \leq NRL(\sigma) \leq s+1$ [9]. Això implica que tan sols les caixes-P expansives tenen bones propietats de difusió pel que respecta a l'anàlisi de la seguretat d'un criptosistema vers la criptoanàlisi lineal.

Definició 3.6.2. *Una capa de difusió* σ_i *de la xarxa és* ***maximal*** *o* ***òptima*** *si i només si es compleix que* $NRL(\sigma_i) = s+1$.

Altre cop, suposarem que podem identificar cada permutació σ_i amb una matriu $M_i = (m_{i\ jk}) \in \mathcal{M}_{b \times b}(F_{2^k})$, amb $m_{i\ jk} \in F_{2^k}$, i on $M_i \cdot x = \sigma_i(x)$.

$$M_i = \begin{pmatrix} m_{i\ 11} & \dots & \dots & m_{i\ 1s} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ m_{i\ s1} & \dots & \dots & m_{i\ ss} \end{pmatrix} = \begin{pmatrix} \sigma_i(1,\dots,0) \\ \vdots \\ \vdots \\ \sigma_i(0,\dots,1) \end{pmatrix}.$$

Podem reescriure el *nombre de ramificació lineal* com [9]

$$NRL(\sigma_i) = \min_{\beta_{i-1} \neq 0} \{ Hw(\beta_{i-1}) + Hw(M_i^T \cdot \beta_{i-1}) \}.$$

La caracterització de les propietats de la matriu per a ésser una *capa de difusió maximal* ve donada per la proposició 2.5.4., adaptada al cas lineal.

Proposició 3.6.3. *Donada una xarxa de substitució-permutació, considerem un camí lineal $\mathcal{CL}$ amb biaix associat $\varepsilon_{\mathcal{CL}}$. Suposant que les aproximacions lineals que determinen $\mathcal{CL}$ tenen probabilitats independents, aleshores:*

$$\varepsilon_{\mathcal{CL}} \leq \frac{1}{2}\,(2\,M\varepsilon)^{\sum_{i\ \text{parell}}^{r-1} NRL(\sigma_i) + (r-1\ (mod\ 2))}.$$

DEMOSTRACIÓ. Aplicant el **Lema de l'Apilament** usant la hipòtesi que les aproximacions són independents, obtenim que

$$\varepsilon_{\mathcal{CL}} = 2^{n(\mathcal{CL})-1} \prod_{i=1}^{n(\mathcal{CL})} \varepsilon_i\,.$$

Considerem la col·lecció d'índexs $J(i)$ definida de la següent manera:

$$J(i) = \left\{ j \in \{1,\dots,s\} \mid \exists E_{S_{ij}} \left(X_{S_{ij}}, Y_{S_{ij}}\right) \in \mathcal{CL}\,, \quad \alpha_{S_{ij}}, \beta_{S_{ij}} \neq 0 \right\}.$$

Aquest conjunt ens dóna les caixes-S *linealment actives* a cada ronda, i en conseqüència tenim que $\sum_i \#J(i) = n(\mathcal{CL})$. Sota la hipòtesi d'independència de les *aproximacions lineals* donades per les expressions $E_{S_{ij}}(X_{S_{ij}}, Y_{S_{ij}})$ del *camí* $\mathcal{CL}$, obtenim que

$$\varepsilon_{\mathcal{CL}} = 2^{n(\mathcal{CL})-1} \prod_{i=1}^{r-1} \prod_{j \in J(i)} \varepsilon_{S_{ij}} \leq 2^{n(\mathcal{CL})-1} \cdot M\varepsilon^{n(\mathcal{CL})} = \frac{1}{2}(2M\varepsilon)^{n(\mathcal{CL})}.$$

Una cota inferior de $n(\mathcal{CL})$ vindrà donat pel mínim nombre de caixes de tipus S *linealment actives* que pot haver-hi en cada ronda*:*

$$\varepsilon_{\mathcal{CL}} \leq \frac{1}{2}\,(2\,M\varepsilon)^{\sum_{i\ \text{parell}}^{r-1} NRL(\sigma_i) + r - 1\ (mod\ 2)}. \qquad \blacksquare$$

Proposició 3.6.4. *Considerem la coberta lineal $\mathcal{L} = E(P, Y_{r-1})$ donada per la característica o camí lineal escollit. Llavors, poden existir diversos camins $\mathcal{CL}$ amb probabilitats diferents on $E(X_1, \cdot), E(\cdot, Y_{r-1}) \in \mathcal{CL}$.*

La probabilitat associada a la coberta lineal $\mathcal{L}$ és:

$$Pr(\mathcal{L}) = \sum_{\substack{\mathcal{CL} \\ E(X_1,\ \cdot),\ E(\cdot\ ,Y_{r-1}) \in \mathcal{CL}}} Pr(\mathcal{CL})$$

Conclusions

És important destacar que el valor que cal considerar a l'hora de considerar la seguretat del criptosistema vers la criptoanàlisi diferencial és $\varepsilon_{\mathcal{L}} = Corr(\mathcal{L})/2$, perquè és el valor que influeix en l'ordre de complexitat de l'atac. No obstant, generalment no ens resulta possible calcular aquest valor, fet pel qual usarem l'aproximació donada per $\varepsilon_{\mathcal{CL}}$. La cota superior de $\varepsilon_{\mathcal{CL}}$ determina les propietats que ha tenir una xarxa de substitució-permutació per a considerar-se segura contra un atac lineal [8,10,16,21]:

1. Cap caixa de tipus S no pot tenir una *expressió lineal* o *afí* amb una probabilitat d'ocórrer que s'allunyi gaire de $1/2$, per a minimitzar el valor de $M\varepsilon$.
2. Les caixes de tipus P han de tenir un *nombre de ramificació* alt, per a maximitzar $\sum_{i\ \text{parell}}^{r-1} NRL(\sigma_i)$. Això implica usar caixes expansives.

Com es pot veure, l'anàlisi de la seguretat contra la criptoanàlisi lineal té molts paral·lelismes amb el de la criptoanàlisi diferencial. Si es compleixen aquestes propietats, aleshores $\max\{\varepsilon_{\mathcal{L}}^2 - 2^{d-b},\ 0\} = 0,\ \forall d$ per a algun valor de r gran (el nombre de rondes de la xarxa), i podem considerar que queda provat que el criptosistema és segur contra la criptoanàlisi lineal. Com en el cas diferencial, no obstant, cal ser molt curosos recordant que:

i. El càlcul està basat en la suposició que els biaixos de cada caixa en $\mathcal{CL}$ són independents, que tot i ésser una relaxació raonable de les condicions per a efectuar el càlcul, pot no ésser certa.

ii. El biaix $\varepsilon_{\mathcal{L}}$ de la *coberta lineal* és probablement diferent al biaix $\varepsilon_{\mathcal{CL}}$ calculat, i per tant la complexitat real pot ser menor a la cota usada per a calcular $\varepsilon_{\mathcal{CL}}$. Normalment, però, si un *camí lineal* té un biaix elevat, aleshores sol dominar la *coberta lineal* [8].

Altre cop, així doncs, és important ser generosos amb els marges de seguretat que donem. Cal optimitzar al màxim les caixes-S i caixes-P de la xarxa, i augmentar el nombre rondes si cal.

4 Aplicació a un cas real: FEAL-4

En aquest capítol aplicarem de manera pràctica un dels atacs exposats al llarg d'aquest treball. El criptosistema objectiu que hem escollit per a intentar trencar és el FEAL-4 (*Fast data Encipherment ALgorithm*), on el procés de xifratge està compost per una ronda inicial, 4 rondes principals i una ronda final. La família de criptosistemes FEAL és notòria entre els criptòlegs degut a la seva vulnerabilitat contra pràcticament tots els atacs criptogràfics coneguts, fet pel qual resulta un candidat perfecte per a practicar els atacs estudiats en aquest treball. En concret, el criptosistema FEAL és una xarxa de Feistel, fet que ens permet aplicar els coneixements apresos fins ara en altres casos que no siguin xarxes de substitució-permutació.

En aquest capítol explicarem el seu funcionament, així com també com atacar-lo utilitzant la criptoanàlisi diferencial per a obtenir totes les claus de ronda del criptosistema. El codi en què està escrit tant el FEAL-4 com l'atac diferencial es pot trobar en el fitxer `diff_cryptanalysis.c` adjunt a la memòria, que es troba en el llenguatge de programació C respectant l'estàndard C99.

Descripció del criptosistema

El FEAL-4 és un xifrat en bloc que opera sobre blocs de 64 bits. L'estructura de Feistel parteix cada bloc en dos sub-blocs de 32 bits cadascun, anomenats L i R, als que aplicarem un XOR amb dues claus de ronda K_L, K_R respectives abans de començar el propi procés de xifratge. Les claus de ronda usades en cada ronda principal són K_1, K_2, K_3, K_4.

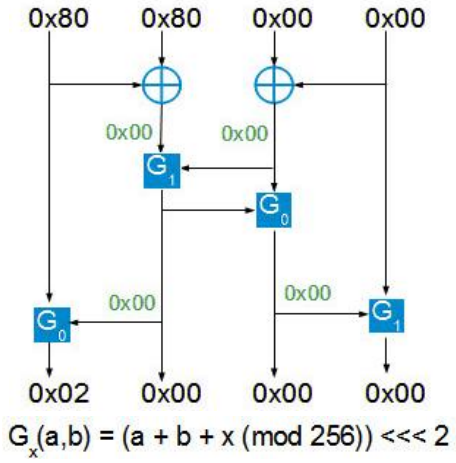
En cada ronda, aplicarem una funció f a cada bloc de 32 bits (que agruparem en 4 bytes x_0, x_1, x_2, x_3 d'entrada i 4 bytes y_0, y_1, y_2, y_3 de sortida). Es té que

$$y_0 = x_0 + y_1 \ \ mod\ 256 \lll 2\,, \qquad y_1 = x_1 \oplus x_2 + x_3 + 1\ mod\ 256 \lll 2\,,$$
$$y_2 = x_2 \oplus x_3 + y_1 \ \ mod\ 256 \lll 2\,, \qquad y_3 = x_3 + y_2 + 1\ mod\ 256 \lll 2\,,$$

on l'operació $x \lll 2$ representa circular de manera cíclica dues posicions els bits de x cap a l'esquerra. Per a un byte qualsevol, es té que: $x = x \lll 8k,\ \forall k \in \mathbb{N}$.

Descripció de l'atac diferencial

Aquesta funció f té una vulnerabilitat crítica: el diferencial donat per $(\Delta X = 0\text{x}80800000, \Delta Y = 0\text{x}02000000)$ es dóna amb probabilitat 1. En conseqüència, la diferència $\Delta P = 0\text{x}8080000080800000$ ens permet muntar un atac diferencial exitós fins a la tercera ronda, on es té que $\Delta Y_3 = \Delta X_4 = 0\text{x}02000000********$.



Això ens permet obtenir l'última clau de ronda (K_4) emprant un nombre mínim de parells de missatges.

Repetint el mateix procediment amb noves característiques diferencials, totes tals que la diferència considerada en la penúltima ronda a atacar és 0x02000000********, podem obtenir totes les claus de ronda del criptosistema en $4 \cdot 2^{32}$ operacions com a màxim, ja que cada clau té 32 bits.

L'esquema següent representa l'atac criptogràfic per a obtenir la clau K_4, amb cada diferència de la característica remarcada amb un color diferent:

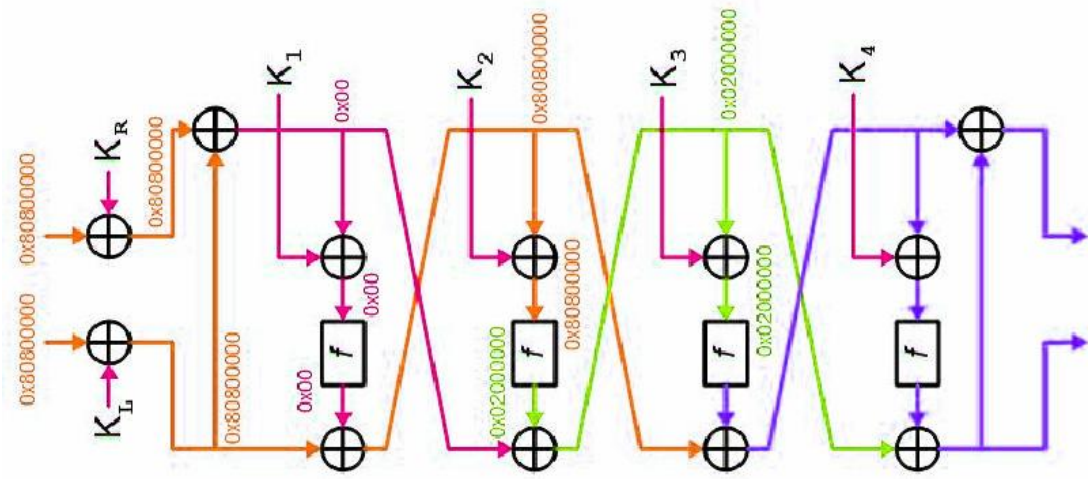


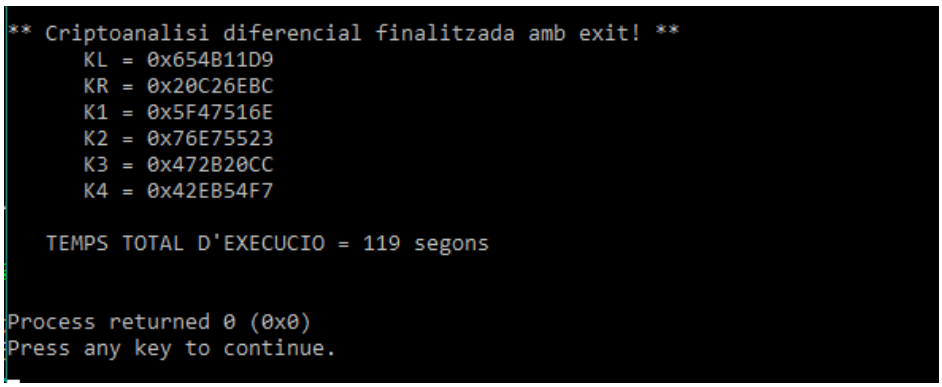
Figura 10: Esquema de l'atac diferencial del FEAL-4 (extreta de [25]), així com del seu funcionament general.

Cal tenir en compte que el mètode emprat per a trencar el FEAL-4 presenta algunes variacions respecte a l'algorisme bàsic de l'atac diferencial exposat en el capítol 2, aprofitant el fet que la característica diferencial es compleix amb probabilitat 1: per exemple, no cal tenir comptadors per a cada candidat, ja que el valor correcte de la clau de ronda K_i sempre determinarà de manera correcta la diferència $\Delta Y_{i-1} = \Delta X_i$ per a cada parell de missatges. Per tant, tan sols ens cal un candidat que funcioni per a tots els parells que generem.

Per a trencar les claus de ronda K_1, K_L, K_R en l'últim pas s'executa un atac molt similar. La cerca només s'efectua sobre K_1 no obstant, perquè els valors de K_L, K_R es poden extreure de les diferències $P \oplus X_1$ dels parells de missatges.

Resultats de l'experiment

L'ordinador amb què s'han dut a terme els càlculs d'aquest experiment té un processador AMD FX-8350 amb 8 nuclis. El temps d'execució de l'atac varia en funció de les claus de ronda escollides a l'atzar, però sol rondar entre el minut i mig i els cinc minuts.



Tot i que els càlculs s'han efectuat utilitzant un únic nucli, cal notar que els algorismes dels atacs diferencial i lineal són fàcilment paral·lelitzables, podent reduir així el temps de càlcul.

L'atac diferencial al FEAL-4 aconsegueix obtenir totes les claus de ronda del criptosistema $K_L, K_R, K_1, K_2, K_3, K_4$ (que són 192 bits en total) en un total de 2^{34} operacions, comparat amb les 2^{192} operacions que caldrien si féssim una cerca exhaustiva. L'atac s'ha dut a terme amb 8 parells de missatges, que és un petit múltiple del valor $N \approx p^{-1} = 1$, ja que s'ha trobat experimentalment que era el nombre més petit amb el que l'atac trobava totes les claus de ronda en un màxim de 20 execucions.

Cal remarcar que l'atac dut a terme contra el FEAL-4 és un cas excepcional. La majoria de criptosistemes que es poden atacar requereixen de moltíssims més parells de missatges, així com d'una quantitat de càlculs major.

Conclusions

Els atacs exposats en aquest treball representen atacs majoritàriament teòrics, degut al gran volum de missatges coneguts que calen per a dur-los a terme, així com a l'elevada quantitat de càlculs necessaris. Tot i que requereixen menys càlculs que un atac per força bruta, romanen en molts casos suficientment grans com per resultar impossibles fins i tot amb els millors superordinadors d'avui dia: en el cas del AES, el millor atac conegut requereix de 2^{126} operacions, que comparat amb una potència de càlcul de $\sim 1{,}15 \cdot 10^{18}$ operacions per segon del superordinador més potent conegut avui dia (Sunway TaihuLight), equival a uns 2.000.000.000.000 anys de càlculs. La quantitat de missatges plans necessaris per a muntar els atacs sol ser, a més a més, impràctica i poc realista.

Tanmateix, en el món de la criptografia, establir la màxima seguretat possible en la manera de salvaguardar les nostres dades és primordial, i és precisament en aquest context on tant la criptoanàlisi diferencial com la criptoanàlisi lineal representen possibles atacs que cal evitar: el risc d'un futur atac que sigui pràctic es ben real. S'espera de tot nou criptosistema de xifrat en bloc que, com a mínim, sigui resistent contra la criptoanàlisi diferencial i la criptoanàlisi lineal. Cal destacar també que han resultat eines d'anàlisi molt rellevants i sobre les quals hi ha hagut una gran activitat d'investigació per part dels criptòlegs. De fet, existeixen diverses variants més complexes dels dos atacs amb una millora significativa en l'aplicabilitat i utilitat dels atacs bàsics [8, 23].

En aquest treball exposem les criptoanàlisis diferencial i lineal bàsiques, i fem una anàlisi de la seguretat dels criptosistemes de xifrats en bloc en base a les seves característiques, donant una cota del mínim cost computacional teòric que podria arribar a tenir cada atac. En destaca especialment el paper de les *caixes de tipus P*, on es pot apreciar que les caixes expansives que siguin maximals augmenten de manera exponencial la seguretat del xifrat, a causa del *nombre de ramificació* present a l'exponent de les cotes de seguretat. Una gran majoria de criptosistemes moderns de xifrat en bloc (AES, Anubis, Camellia, Hierocrypt, KHAZAD, SHARK, Twofish, etcètera) utilitzen *caixes de tipus P* expansives i maximals precisament per aquesta raó.

Bibliografia

[1] Barker, Elaine et al: Recommendation for Key Management; *National Institute of Standards and Technology* (2013).

[2] Bernstein, Daniel J.; Buchmann, Johannes; Dahmen, Erik: *Post-Quantum Cryptography*; Springer Science and Business Media, University of Illinois, Chicago, 2009.

[3] Biham, Eli; Shamir, Adi: Differential Cryptanalysis of DES like cryptosystems; *Weizmann Instute of Science - Technical Report* CS90-16, Israel (1990).

[4] Buchmann, Johannes: *Introduction to Cryptography*, Springer Science and Business Media, Luxemburg, 2004.

[5] Coppersmith, Don: The Data Encryption Standard and its strength against attacks; *IBM Journal of Research and Development*, Nova York (1994).

[6] Daemen, Joan; Rijmen, Vincent: AES Proposal – Rijndael; *National Instute of Standards and Technology* (1999).

[7] Data Encryption Standard; *National Instute of Standards and Technology FIPS PUB* 46 (1977).

[8] Heys, Howard: A Tutorial on Linear and Differential Cryptanalysis*; Memorial University Publications*, Canadà (2002).

[9] Hong, Seokhie; Lee, Sangjin; Lin, Jongin; Sung, Jaechul; et al: Provable Security against Differential and Linear Cryptanalysis for the SPN Structure; CIST Publications, Seül (2000).

[10] Janson, Christian: Boolean functions; *Brëmen University thesis repository*, Alemanya (2012).

[11] Kerchkoffs, Auguste: La cryptographie militaire; *Journal des sciencies militaires* vol. IX (1883).

[12] Kraschewski, Daniel: Symmetrische Blockchiffren; *Kharlruher Instutut für Technologie*, Alemanya (2013).

[13] Kruppa, Hannes; Uamir, Syed; Shah, Ahmed: Differential and Linear Cryptanalysis of AES Candidate Algorithms; Alemanya, 1998.

[14] Matthews, Robert A. J.: The use of genetic algorithms in cryptanalysis; *Cryptologia* vol. 17, Anglaterra (1993).

[15] M. Matsui; A. Yamagishi: A new method for known plaintext attack of FEAL cipher*;* EUROCRYPT '92 (*Lecture notes in Computer Science* vol. 658), Springer-Verlag.

[16] M. Matsui: Linear Cryptanalysis Method for DES Cipher; EUROCRYPT '93 (*Lecture notes in Computer Science* vol. 765), Springer-Verlag.

[17] K. Nyberg: Linear Approximations of Block Ciphers*;* EUROCRYPT '94 *(Lecture notes in Computer Science* vol. 950), Springer-Verlag.

[18] Pastor Franco, José; Sarasa López, Miguel Ángel; Salazar Riaño, José Luís*: Criptografía digital: Fundamentos y aplicaciones* (segona edició), Prensas universitarias de Zaragoza, Saragossa, 2001.

[19] Robshaw, Matt; Murphy, Sean: *Differential Cryptanalysis, Key dependent S-boxes, and Twofish*; Springer Science and Business Media, Països Baixos, 2000.

[20] Sarkar, Sumanta; Syed, Habeeb: Bounds on the Differential Branch Number of Permutations; *TCS Innovation Labs,* India (2017).

[21] Schneier, Bruce: *Applied Cryptography: Protocols, Algorithms and source code in C* (segona edició), John Wiley; Sons, Nova York, 1996.

[22] Shannon, Claude E.: Communication Theory of Secrecy Systems; *Bell System Technical Journal*, Nova Jersey (1949).

[23] Velichkov, Vesselin: *Recent methods for Cryptanalysis of symmetric key cryptographic algorithms*; Arenberg Doctoral School, Bèlgica, 2012.

[24] https://www.random.org/randomness/

[25] http://theamazingking.com/crypto-feal.php

[26] https://en.wikipedia.org/wiki/Feistel_cipher