БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

Роберт Йорданов Ценков

ИЗСЛЕДВАНЕ НА УСЛОВИЯТА ЗА ЛИНЕЕН КРИПТОАНАЛИЗ В МРЕЖИ НА ФАЙСТЕЛ

А В Т О Р Е Ф Е Р А Т

на дисертация за присъждане на
образователната и научната степен „Доктор“

Научна специалност:
01.01.12 Информатика
Професионално направление:
4.6 Информатика и компютърни науки

На самостоятелна подготовка

Научни консултанти:
проф. дмн Петър Бойваленков
доц. д-р Юри Борисов

София, 2016 г.

Дисертационната работа е обсъдена и насочена за защита от обединено научно звено от хабилитирани специалисти на ИМИ-БАН, НБУ и ФМИ - Софийски университет, на 17 октомври 2016 г. (дата на вътрешна защита).

Изследванията по дисертацията са извършвани в Института по математика и информатика при БАН.

Дисертационната работа е с общ обем от 143 страници и съдържа 25 таблици и 1 фигура. Литературата обхваща 131 заглавия. Има 4 приложения.

Защитата на дисертацията ще се състои на ..... г. от ..... ч. в зала ..... на .....

Материалите по защитата са на разположение в библиотеката на Института по математика и информатика, ул. „Акад. Г. Бончев“, бл. 8, София.

Автор: Роберт Йорданов Ценков

Заглавие: Изследване на условията за линеен криптоанализ в мрежи на Файстел

Научни консултанти: проф. дмн Петър Бойваленков, доц. д-р Юри Борисов

Увод

Актуалност на темата

Задачата за осигуряването на информацията в различните нейни аспекти е изключително сложен и комплексен проблем в настоящето високотехнологично общество и огромните информационни потоци. От гледна точка на защита на информацията, представена във формализиран запис, криптографията има водеща и в много случаи и решаваща роля. Надпреварата в осигуряване на сигурни средства за криптографска защита и усилията за тяхното преодоляване с цел нерегламентиран достъп се изразява в стремежа за използване на възможно най-модерни технологии и влагане на огромни финансови ресурси. Би могло да се каже, че като наука криптографията е сравнително консервативна, тъй като понякога от нея се очакват решения, които да бъдат актуални десетки години напред, независимо от развитието на познанието и технологиите. Показателен пример за това е стандартът за криптиране на данни Data Encryption Standard (DES), публикуван от американският Национален институт по стандарти и технологии (National Institute of Standards and Technology – NIST) през 1977 г. [35] и официално оттеглен едва през 2005 г., като неговата модифицирана версия Triple Data Encryption Algorithm (TDEA) [38], известна като Triple-DES (3DES), продължава да е стандарт за криптиране на данни и към настоящия момент [40]. Въпреки тази си „консервативност“, поради непрестанно растящите скорости и обеми на комуникация, а едновременно с това развитието на технологии, работещи с все по-малки ресурси, криптографската наука е принудена непрекъснато да търси нови решения, както и да развива и разширява наличните. Нуждите от съвместимост и икономичност правят гъвкавостта на решенията изключително важна.

Криптоалгоритъмът в DES е от тип мрежа на Файстел (Feistel Network – FN), на името на един от авторите на стандарта. Публикуването на самия стандарт дава голям тласък на публичните проучвания в областта на криптографията и криптоанализа. Важен аспект от тези проучвания е приложението на теорията на информацията, търсейки различни модели за конструкция и анализ, използвайки различни форми на ентропия и подходи за събиране на емпирични данни. Изключителен принос в теоретическите анализи има основополагащата работа на Люби и Ракоф [27], в която те формализират строго понятията за сигурност на блокови шифри в термините на псевдослучайните функции и пермутации, разглеждайки модел със случаен оракул, като доказват сигурността на Файстел-схемите в този модел. Като резултат моделът затвърждава възловото си място в криптографската теория и бива интензивно изучаван. Едновременно с това Файстел-мрежите, заедно със заместително-разместителните мрежи (Substitution-Permutation Networks – SPN), остават и до настоящия момент два-

та най-използвани модела за конструкция на симетрични блокови шифри (виж, напр. [56, 5, 1]). Допълнително предимство на схемите на Файстел е, че те предлагат сравнително икономична реализация на алгоритъма (виж, напр. [23, стр. 16]). Освен това, такива структури имат значителен потенциал за търсене на гъвкави решения. Доказателство за тяхното признание и популярност е фактът, че в структурата на три от петте криптоалгоритъма, избрани за финалисти в конкурса за наследник на DES – Advanced Encryption Standard (AES) [37], се използват мрежи на Файстел – Twofish [52], RC6 [50] и MARS [7]. Също така, аналогът на DES в бившия Съветски Съюз, стандартът ГОСТ 28147-89 [17], има структура на Файстел, а настоящият криптографски стандарт на Русия GOST R 34.12-2015 [14] използва такава структура в алгоритъма си за развитие на криптографския ключ и генериране на рундови ключове.

Изтъкнатото дотук показва, че мрежите на Файстел продължават да бъдат основен и много интересен обект на изследване в криптографската наука и всеки нов резултат за техните свойства би допринесъл за още по-рационалното им разбиране и приложение.

Мотивация на изследването. В началото на 90-те години на миналия век в публичното пространство се появяват две основни техники за атака на модерните симетрични блокови шифри: така наречените диференциален и линеен криптоанализ [3, 28]. И двете се прилагат към действащия към момента стандарт за криптиране на данни Data Encryption Standard (DES) [35] и показват, че при съответните сценарии на атака стандартът е „разбиваем“ с по-малка степен на трудност отколкото при атака с изчерпващо търсене на ключа. Въпреки, че главната цел на тези техники за криптоанализ е бил DES, впоследствие тяхната приложимост към голям брой други блокови шифри остава извън съмнение. Дори и днес, един от първите въпроси, отговорът на които бива очакван от криптографската общност при всяко ново предложение за блоков криптографски алгоритъм, е дали той е устойчив на тези видове атаки [39, 18].

Общо казано, идеята на линейния криптоанализ на блокови шифри е да използва линейни стохастични апроксимации на шифъра от следния тип:

$$\mathbf{P}[\chi_P] + \mathbf{C}[\chi_C] = \mathbf{K}[\chi_K],$$

където с $\mathbf{P}, \mathbf{C}$ и $\mathbf{K}$ са означени явният текст, съответният шифров текст и тайният ключ, съответно, докато $\mathbf{B}[\chi_B] = B_{b_1} \oplus B_{b_2} \oplus \cdots \oplus B_{b_m}$ за подмножеството (или маска) $\chi_B = \{b_1, b_2, \ldots, b_m\}$ от битови индекси в $\mathbf{B}$. Измежду тези релации (наричани още характеристики), най-ценните за криптоанализа са тези, които са изпълнени с вероятност, значително различаваща се от идеалната стойност $1/2$. За итерационни шифри, базирани на използването на заместителни таблици (S-кутии), каквито са и DES, и настоящия стандарт за криптиране на

данни AES, основен начин за получаване на линейни характеристики е чрез първоначални апроксимации на отделните заместителни таблици и последващо комбиниране на тези апроксимации в рамките на един или повече рундове.

В настоящия дисертационен труд се разглежда ефектът от наличие на допълнителни линейни връзки в един криптографски алгоритъм по отношение на устойчивостта му на линеен криптоанализ. Всеобщо схващане е, че наличието на такива зависимости би следвало да засили уязвимостта към подобен тип атаки. Това е основната хипотеза, от която ние изхождаме и подлагаме на проверка, като получените резултати дават ясен отговор, подкрепен от значителен обем аналитични и експериментални резултати, в рамките на разглеждания в експеримента контекст. Моделът, който реализираме, е въвеждане на допълнителна линейност чрез вграждане на контролен бит по четност в изходите на заместителните таблици на криптографския алгоритъм. Базов за експеримента е алгоритъмът от DES [35], върху който за първи път са демонстрирани успешно техниките за линеен криптоанализ [29] и за който има натрупано голямо количество емпирични данни и изследвания, даващи много добра възможност за извършване на сравнителния анализ, цел на настоящата работа.

DES е първият блоков симетричен криптографски алгоритъм за публично приложение, който е одобрен като стандарт на САЩ, и към сегашния момент продължаващ съществуването си под формата на 3DES. Добре известно е, че силата на DES се основава главно на неговата единствена нелинейна част – S-кутиите (S-boxes). Оказва се, че още при дизайна на алгоритъма е заложен критерий, относим към разработения много по-късно метод, известен като „линеен криптоанализ“ (вж. [10]).

Една краен частен случай на споменатия по-горе критерий е следната:

Сумата по модул 2 на четирите изходни бита на всяка от заместителните таблици не трябва да бъде константа.

Е, какво би се случило тогава, ако това ограничение бъде нарушено (изкуствено)? Например, като по един бит от всяка оригинална S-кутия бъде подменен с бит за контрол по четност на останалите три изходни бита, чиито стойности се запазят. Какво може да бъде казано на пръв поглед за заместителни таблици, получени по такъв начин?

В нашия конкретен случай S-кутиите практически се трансформират в подходящо конструиран код с четно (или, съответно, нечетно) тегло и дължина 4. Тези таблици са инструмента за въвеждане на нелинейност в криптографската трансформация, така че допълнителна линейност в тях, разбира се, по принцип влошава качествата им в този аспект (и в термините на дефиницията, дадена за пръв път в [41]). От друга страна обаче, така конструирани S-кутии притежават способност за откриване на единична грешка и затова са имунни (в определена степен) срещу атаки чрез въвеждане на грешки по време на изпълнение на

алгоритъма. В допълнение, такава S-кутия удовлетворява автоматично критерия относно спектъра на разстоянията по Хеминг между изходните стойности, имащ отношение в случая на диференциален криптоанализ (виж, за детайли [10] или като обобщение [24, стр. 301]).

Съществува и още един аспект в общата криптографската теория и практика, от който може да бъде разгледан поставеният експеримент. Това е от гледна точка на т.н. „trade-off“ в криптографията, или казано с други думи – техниката за замяна на едни ресурси с други при оценката и реализацията на криптографските алгоритми (напр., в [21]) или на атаките срещу тях (в резюме, в [23, стр. 96]). Най-често основните ресурси, които могат да бъдат взаимно заменяни или съпоставяни, са времето за изпълнение и необходимата компютърна памет (пространство), като неотменен придружаващ компонент на всяка практическа оценка са и съответните финансови измерения. Допълнителна мярка за съпоставка, разбира се, е и нивото на сигурност, което се постига с криптографската трансформация, когато в съответния модел е допустимо сигурността да бъде разглеждана като параметър в определени граници. От тази гледна точка оценката на ефекта от подмяната на един от изходните битове на една S-кутия с контролен бит може да бъде разглеждана като замяна на реализация на алгоритъма (в тази му част) с четири нелинейни булеви функции чрез три такива функции плюс проста линейна комбинация на техните изходи. Второто решение по принцип предполага по-малка „цена“ за реализация. Съотнесено към целия алгоритъм (с 8 S-кутии), отношението между двете решения би било вариант с 32 независими булеви функции срещу вариант само с 24 такива в една итерация. С по-малко нелинейни функции обаче нивото на сигурност по принцип намалява в рамките на една итерация, което пък може да бъде компенсирано чрез изпълнение на повече итерации (за сходна съпоставка виж, напр. [57]). Така всъщност стигаме до разглеждане на „trade-off“ между цената за реализация на алгоритъма и времето за неговото изпълнение. Типична ситуация за възникване на необходимост от вземане на решение за „trade-off“ между различни типове ресурси е при проектиране на скалируеми шифри, където трябва да се осигури механизъм за работа с различни стойности на параметрите на алгоритъма.

Поради значителната сложност на съвременните криптографски алгоритми, оценката при една задача от формулирания по-горе тип не е така ясна и очевидна на пръв поглед и за да бъде даден аргументиран отговор са необходими задълбочени и обстойни изследвания. Криптоалгоритъмът от DES е от тип Файстел-мрежа, което носи своите особености при конструкцията на линейни характеристики и анализа на техните свойства. Въпреки това по-голямата част от прилаганите техники и формулираните изводи биха били относими към много по-широк кръг от шифри на Файстел, а някои от тях и изобщо за симетрични

блокови алгоритми.

Цели и задачи на дисертационния труд

Целта на настоящата дисертация е да се изследва влиянието на определен вид модификации на симетрични итерационни шифри върху податливостта на тези шифри на линеен криптоанализ. Разглежданите шифри са от тип класическа мрежа на Файстел, а модификацията се състои във въвеждането на контрол по четност в изходите на използваните в криптографския алгоритъм заместителни таблици (S-кутии).

Конкретните задачи за постигането на тази цел са:

1. Да се разгледа и анализира отражението на разглеждания тип трансформации върху свойствата и вида на линейно апроксимиращите таблици за S-кутиите на криптоалгоритъма.
2. Да се анализират свойствата на най-добрите линейни характеристики за малък брой рундове на модифицирания криптоалгоритъм.
3. Да се анализират аспектите от конструкцията на многорундови характеристики, в които разглеждания тип трансформации влияят, и механизмите на това влияние.
4. Да се разработи алгоритъм за търсене на многорундови линейни характеристики за разглеждания тип шифри, който да позволява адаптация и прилагане и за семейството модифицирани алгоритми.
5. Да се сравнят двата основни подхода при конструкция на многорундови характеристики – чрез използване на най-много една активна заместителна таблица на рунд и чрез използване на двурундови итеративни характеристики.
6. Да се направи сравнение на резултатите, получени за модифицирания шифър, с аналогичните резултати за оригиналния шифър.
7. Да се обобщят резултатите от експеримента и се направят изводи за релацията между разглеждания тип допълнителни зависимости и условията за прилагане на линеен криптоанализ към мрежи на Файстел.

Като базов алгоритъм за експеримента се използва Data Encryption Standard, върху който за пръв път Мацуи [28, 29] демонстрира успешно техниките на линейния криптоанализ и който дава много добри възможности за извършване на сравнителен анализ, каквато е нашата цел. Изводите, които могат да се направят от този анализ значително надхвърлят рамките на конкретно използвания базов алгоритъм и могат да бъдат обобщени както за целия клас алгоритми,

на който той принадлежи, така и изобщо по отношение на оценката на условията, благоприятстващи ефективното прилагане на линеен криптоанализ към симетрични блокови шифри.

Методология на изследването

Методологията на изследването се състои основно в намиране на най-добрите линейни характеристики и сравнение на тяхната ефективност. Тъй като сложността на една линейна атака е пропорционална на ефективността на използваните апроксимиращи изрази, сравнението на ефективностите дава оценка и за отношението между ресурсите, необходими за съответни линейни атаки. В някои от сравняваните апроксимации се разглежда и броят на активните S-кутии и ефективните битове, което дава допълнителна информация при оценките.

Проследява се отражението на допълнителни връзки между битове в честотното поведение на линейните комбинации, отразени в апроксимиращите таблици. На тази база се прави оценка на възможността за прогнозируем ефект чрез контролиран избор на модификация.

При конструкцията на многорундови линейни характеристики вниманието е насочено в три направления на влияние на разглежданата трансформация:

1. Влияние върху сумите на изходни битове.
2. Влияние върху сумите от входни битове.
3. Влияние върху възможностите за междурундово съгласуване на еднорундови характеристики.

Констатациите от горните наблюдения се използват в реализацията на алгоритми за конструкция и търсене, резултатите от които се използват за сравнителен анализ. При сравнителния анализ се сравняват резултати в две направления:

1. Резултати, получени чрез различни подходи.
2. Резултати за модифицирания шифър спрямо резултати за базовия шифър.

Като краен резултат от сравнителния анализ се правят изводи относно влиянието на наличието на зависимости от разглеждания тип върху условията за прилагане на линеен криптоанализ.

Съдържание на дисертацията

Настоящата дисертация се състои от увод, пет глави, заключение, списък на цитираната литература и четири приложения. Общият обем е 143 страници, има 25 таблици и 1 фигура. Литературата включва 131 заглавия на 13 страници.

Номерацията на структурата и елементите в този автореферат съответства на номерацията в дисертацията.

Глава 1. Криптография и криптоанализ

В първа глава се дава общ преглед на съвременните концепции в криптографията и криптоанализа, с акцент върху линейния криптоанализ и по-голямо внимание върху шифрите със структура от тип Файстел, каквито са основните обекти на проучване в дисертацията.

Науката за криптирането.

Криптографията и криптоанализът, в своята неразривна връзка, дават съвременния облик на науката за „скриване“ на съдържанието на съобщенията чрез тяхното преобразуване в „нечитаем“ вид – криптологията. Формулираният още през 1883 г. *принципът на Кирхоф* [31, стр. 14], че сигурността на една криптографска трансформация трябва да бъде съсредоточена единствено в тайно избрания криптографски ключ, предполагайки самият алгоритъм за общодостъпен, намира израз в настоящите публични стандарти за криптиране.

Симетрична и асиметрична криптография.

Съвременните криптографски схеми се делят да две глобални, принципно различни групи. Когато ключовете за криптиране и декриптиране съвпадат или лесно (изчислително) се получават един от друг, то те, както и самата схема, се наричат *симетрични*. В противен случай ключовете и схемата се наричат *асиметрични*. Симетричните схеми задължително предполагат и еднаквост или голяма близост като математически операции и изчислителна сложност на алгоритмите за криптиране и декриптиране, което не е така при асиметричните схеми. Предимствата и недостатъците на двата типа техники водят до съвместната им употреба в т.н. *хибридни* схеми.

Криптографски механизми.

Модерната концепция за *осигуряване* на информацията включва голям брой *услуги за сигурност* на базата на различни *криптографски механизми* и протоколи. Защита на информацията се извършва в различни нейни аспекти (свойства), основните от които са *поверителност*, *цялост (интегритет)*, *автентичност* и *неотказваемост*. Използват се предимствата и на двата вида криптография, заедно с различни типове математически преобразувания без ключ.

Структура на симетричните криптографски алгоритми.

Фундаментален принцип при конструкция на симетричните криптографски алгоритми си остава *принципът на Шенон* [55] за *„конфузията“ (разбъркване, confusion)* и *дифузията (diffusion)*, често изразявани като слоеве в конструкцията на алгоритмите. Допълнителни аспекти при проектирането на съвременните шифри са също тяхната глобална структура, броят на рундовете и схемата за генериране на рундови ключове [48].

Двете най-използвани глобални структури в криптографските алгоритми са мрежите на Файстел (Feistel Networks, FN), каквато е структурата на стандарта DES [35] и заместително-разместителните мрежи (Substitution-Permutation Networks, SPN), каквато структура има стандартът AES [39]. Характерно за мрежите на Файстел е, че част от блока в една итерация се запазва и се използва за модифицирането на останалата част от блока, след което различните части се пермутират. Това обуславя тяхната по-голяма икономичност на реализацията, което обаче е за сметка на броя рундове, необходими за постигане на желаните качества.

За постигане на нелинейност на трансформацията най-използваният инструмент са т.н. *заместителни таблици* (*S-кутии*, *S-boxes*), а за дифузия често се използват MDS кодовете, както в настоящият стандарт AES. Чрез S-кутиите също се осигурява и определена степен на дифузия.

Желано свойство на криптографските примитиви от гледна точка на по-голяма гъвкавост на решенията е свойството *скалируемост*. Един алгоритъм се нарича *скалируем*, ако по дизайн негови базови параметри могат да приемат алтернативни стойности. Препоръки за гъвкавост на алгоритмите има изрично заложени от Националния институт за стандарти и технологии на САЩ (NIST) в обявения конкурс за AES, като задължително условие е скалируемост по отношение дължината на ключа [36]. В резултат, част от кандидатите предлагат и скалируемост по отношение дължината на блока (напр. RC6 [50] и Rijndael [12]). При подобни задачи специфичната структура на Файстел-мрежите дава големи възможности за вариативност при проектирането и съответно за търсене на оптимизация. Сходна на концепцията за скалируемост е техниката на *еластичните шифри* [9], идеята за които произхожда от желанието да се избегне изкуственото допълване (padding) на последния блок за криптиране, водещо до увеличаване на дължината на съобщението и създаване на потенциални уязвимости.

Информация и ентропия в криптологията.

В криптологията централен обект за манипулиране е информацията. В основополагащата си работа [53, 54] по теория на информацията Шенон дефинира *ентропията* на един източник на съобщения като мярка за количеството информация, което този източник съдържа. Различните форми на ентропия –

съвместна, *условна*, *относителна*, *крос-ентропия* и т.н., са мощен инструмент в анализите и доказателствата за сигурност в криптологията. В съвременните изследвания се използват и различни други типове ентропия, освен дефинираната от Шенон, като *ентропия на Рени*, *мин-ентропия*, *HILL-ентропия*, *ентропия на Яо* и др. [8, 49]. Модерният криптоанализ разглежда различни модели на достъп до информация с цел използването ѝ за атака.

Доказуема сигурност.

Теоретическата сигурност на криптосистемите е предмет на разглеждане още в работата [55] на Шенон от 1949 г. В нея той развива концепциите за *перфектна сигурност* и *практическа сигурност* на криптографски системи в рамките на идеализиран модел. Работата на Голдвасер и Микали [16] полага основата за развитие на формален апарат за доказателство чрез идеята за *доказуема сигурност*. През 1988 г. Люби и Ракоф [27] доказват сигурността на идеализирана Файстел-схема в модела за неразличимост със случаен оракул. Развитието на този модел продължава и до днес [45, 13, 19, 32]. Идея за осигуряване на доказуема сигурност предлага *теорията за декорелацията* на Водене [58, 59]. При нея в основния алгоритъм се вграждат т.н. *декорелиращи модули*, които са математически примитиви на малко разстояние от перфектно случайната функция/пермутация. В зависимост от типа налични данни, основните класове атаки в модела за доказуема сигурност са [15]: с известен явен текст (KPA); с избран явен текст (CPA); с избран шифров текст (CCA); с избран явен-шифров текст (CPCA); с адаптивно избран явен текст (ACPA); с адаптивно избран шифров текст (ACCA); с адаптивно избран явен-шифров текст (ACPCA). Използваните мерки за разстояние до перфектно случайната функция/пермутация са различни и се дефинират в зависимост от типа атака.

Видове криптоанализ.

Публикуването на де факто първият криптографски стандарт DES [35] дава силен тласък за развитие на криптоанализа. Първият реално успешен опит за атака на DES е чрез *диференциалния криптоанализ*, изобретен от Бихам и Шамир [2, 3] Той е от класа CPA (атаки с избираем явен текст). При него се разглеждат релациите от типа

$$\triangle c = \mathcal{E}(m \oplus \triangle m) \oplus \mathcal{E}(m),$$

където $\triangle m$ и $\triangle c$ са фиксирани разлики в стойностите съответно на входа и изхода на криптографската трансформация $\mathcal{E}$. Горното уравнение има вероятностен характер, когато входът m се разглежда като случайна величина. Диференциалният криптоанализ цели да използва онези стойности на $\triangle m$ и $\triangle c$, при които отклонението на вероятността за изпълнение на релацията от идеалната стойност $1/2$ е най-голямо. Двойката $(\triangle m, \triangle c)$ се нарича *диференциал* или *диференциална характеристика*. За последващото разкриване на тайния

ключ или части от него се използва статистическият метод на максималното правдоподобие.

В резултат на последващите проучвания възникват понятията *шифър на Марков* [25] и *диференциална равномерност* [42].

С възникването си [28, 29] *линейният криптоанализ* става вторият успешен метод за атака на DES. Негов автор е японският криптограф Мицуро Мацуи. За разлика от диференциалния анализ, този тип атака спада към класа KPA, т.е. атаки с известен явен текст. Техниката се състои в използване на линейна апроксимация на шифъра от вида

$$m_{j_1} \oplus m_{j_2} \oplus \ldots \oplus m_{j_s} \oplus c_{l_1} \oplus c_{l_2} \oplus \ldots \oplus c_{l_t} = k_{i_1} \oplus k_{i_2} \oplus \ldots k_{i_r},$$

където с m_{j_u}, c_{l_u} и k_{i_u} са означени битове съответно от входа, изхода и ключа. Двойката множества от битове на входа и изхода, участващи в апроксимацията, се нарича *линейна характеристика*. Аналогично на диференциалния анализ, тук също се търсят характеристики с най-голямо отклонение на вероятността за изпълнение на уравнението, благоприятстващи прилагането на статистически анализ. Веднага след появяването си линейният криптоанализ става предмет да обстойни изследвания за доказуема сигурност срещу него [43, 44], а алгоритъмът на Мацуи за търсене на най-добри характеристики бива адаптиран и оптимизиран и за други шифри.

Диференциалният и линейният криптоанализ остават и до днес най-мощните техники за атака на симетрични блокови шифри. Към момента съществуват вече много и различни техни обобщения. Само част от тях по отношение на линейния криптоанализ са *използването и на нелинейни апроксимации* [22], използване на *многокомпонентни линейни апроксимации* [4], *би-линеен криптоанализ* [11], криптоанализ *с нулева корелация* [6], комбинация с диференциален анализ под името *диференциално-линеен криптоанализ* [26].

Мрежи на Файстел.

Мрежите на Файстел (шифри на Файстел, FN) получават голяма популярност с въвеждането през 1977 г. на стандарта DES [35], базиран на точно такава структура. Името им се свързва с един от разработчиците му – Хорст Файстел (Horst Feistel). Ключовата работа на Люби и Ракоф [27], в която те доказват сигурността на Файстел-схемите в термините на псевдослучайните функции и пермутации при модел със случаен оракул, дава основание тези шифри понякога се наричат и *схеми на Люби-Ракоф*, а моделът на Люби и Ракоф – *случаен Файстел-шифър*. Изследванията в този модел продължават да се развиват интензивно и до сега ([45, 46, 47]).

Класическият шифър на Файстел е итерационен блоков шифър съпоставящ на $2b$-битов явен текст (L_0,R_0), с b-битови блокове L_0 и R_0, шифров текст (R_n,L_n), чрез n-рундов процес, където $n \geq 1$. За $1 \leq j \leq n$, рунд j съпоставя

$(L_{j-1}, R_{j-1}) \stackrel{K_j}{\to} (L_j, R_j)$ както следва:

$$\begin{aligned} L_j &= R_{j-1}, \\ R_j &= L_{j-1} \oplus f(R_{j-1}, K_j), \end{aligned}$$

като всеки подключ K_j се извлича от ключа на шифъра K, а f е зададена трансформираща функция. След изпълнение на последния рунд блоковете отново се разменят. Характерно е, че структурата на самата схема позволява функцията f да не е обратима.

При класическата схема на Файстел трансформациите при криптиране и декриптиране, $\mathcal{E}$ и $\mathcal{D}$, са еднакви, с единствената разлика, че подключовете за итерациите трябва да се вземат в обратен ред. При симетрично използване на ключа трансформацията става инволюция, т.е. $\mathcal{E} = \mathcal{E}^{-1} = \mathcal{D}$. Други характерни свойства, произтичащи от структурата, са:

$$\begin{aligned} \triangle L_j &= \triangle R_{j-1}, \\ R_j &= R_{j-2} \oplus f(R_{j-1}, K_j), \end{aligned}$$

където с $\triangle$ сме означили разликата в стойностите. Тези свойства съществено се използват в криптоанализа и оценката за сигурност на такъв тип алгоритми.

След публикуването на DES систематичното изучаване на класическата структура на Файстел води до голям брой нейни модификация, известни под общото име *обобщени мрежи на Файстел* (Generalized FN). Едни от популярните модели са т.н. схеми на Файстел от *Тип 1*, *Тип 2* и *Тип 3*, въведени в [61] от Зенг, Мацумото и Имаи и наричани също понякога и *разширени мрежи на Файстел* (Extended FN) [20, 60]. В [34] Накахара, Вандервал и Пранел формализират описанието на *процеса на дифузия* при Файстел-мрежи чрез понятието за *пълнота на функция*. Една функция (шифър) се нарича *пълна* (от гледна точка на дифузията), ако всеки неин изходен бит зависи от всичките ѝ входни битове. В [51] Шнайер и Келси разглеждат формално структурата и въвеждат *небалансираните мрежи на Файстел* (UFN) на базата на строга теория и дефиниция на понятия като *балансираност*, *хомогенност*, *пълнота* (от структурна гледна точка), *съгласуваност*, *обобщени UFN*, *цикъл*, *ротация*, *ниво на конфузия* и *ниво на дифузия*. Нивата на конфузия и дифузия са тясно свързани с оценките за устойчивост на линеен и диференциален криптоанализ.

Многообразието на този тип шифри идва от вариативността при избора на: общ тип структура; разделяне на подблокове; трансформиращи функции и тяхното комбиниране; финална пермутация; алгебрични структури, в които се извършват операциите. Една частична и много обща класификация на най-използваните типове мрежи на Файстел е: класическа, небалансирана, небалансирана целочислена, алтерниращa, алтерниращa целочислена, Тип 1, Тип 2,

Тип 3 [19, 33]. Гъвкавостта на структурата обуславя изключително широко приложение на Файстел-мрежите в съвременната криптография. Примери за това, без да са изчерпващи, са: като част от други типове структури; конструкции на оптимално допълване при асиметрична криптография (OAEP); за генериране на пермутации в малки домейни с размер, който не е степен на двойката; механизми за автентификация; хеш-функции; олекотени шифри; криптиране със запазване на форма́та и т.н.

Глава 2. Необходими понятия

Във втора глава се въвеждат основни понятия и означения, необходими за по-нататъшното изложение. Въпреки, че част от тях са валидни и в по-общи рамки, основният контекст на разглеждане е линеен криптоанализ на Файстел-мрежи, предимно в терминологията и класическия подход на Мацуи [28, 29] и използвайки като базов алгоритъма на DES.

2.1 Означения

Разглеждаме фамилия от криптографски алгоритми от тип класическа схема на Файстел и въвеждаме следните означения: S_k — k-та заместителна таблица (S-кутия) на шифъра; L_j, R_j — ляв и десен подблок на входния блок за j-тия рунд; K, K_j — секретния, входен за шифъра, ключ и съответния подключ за j-я рунд; X_j, F_j — входен и съответен изходен блок данни от трансформиращата функция в j-я рунд; $f_j(X_j, K_j)$ — трансформираща функция в j-я рунд; $I_X(j)$, $I_F(j)$ — множества от индексите на всички битове на X_j и F_j, участващи в линейната характеристика за j-я рунд; $\oplus$ — двоичен XOR-оператор; $\circ$ — двоичен AND-оператор; & — побитов AND-оператор между двоични вектори; $A[i]$ — i-ти бит на вектора A; $A[i, j, \ldots, k] = A[i] \oplus \cdots \oplus A[k]$; $B_1 + B_2$ — обединение $B_1 \cup B_2$ на множествата B_1 и B_2, когато $B_1 \cap B_2 = \phi$.

2.2 DES алгоритъм

При DES алгоритъма [35] схемата е пълна, балансирана, хомогенна мрежа на Файстел от класически тип, с 16 рунда,64-битов блок и 56-битов ключ. Има осем заместителни таблици $S_k : \mathbb{F}_2^6 \to \mathbb{F}_2^4$, $k = 1, \ldots, 8$. Тези S-кутии са единственият нелинеен компонент на цялата трансформация. Рундовите подключове K_j са състоят от по 48-битови. Схемата е хомогенна, като трансформиращата функция f има вида $f_j(R_{j-1}, K_j) = RP(S(E(R_{j-1}) \oplus K_j))$, където с E е означена разширяваща функция от 32 до 48 бита, S е съвместно прилагане на осемте S-кутии, а RP е рундова пермутация, обща за всички рундове. Разширяването E става, като половината от входните битове се дублират. При това дублиране

във входовете на всеки две съседни кутии (включително S_8 и S_1) участват по два общи бита. Цялата схема за криптиране започва с начална пермутация IP на битовете на входния блок и завършва с крайна пермутация IP^{-1}, обратна на началната. Рундовата пермутация RP е такава, че четирите изходни бита от коя да е S-кутия се разпределят във входовете на четири различни S-кутии за следващия рунд.

За по-лесно сравнение на резултатите, използваме конвенциите на Мацуи за индексиране на битовете и S-кутиите [28, 29] в DES алгоритъма. Всяка S-кутия се представя като едномерен масив с входа на S-кутията като индекс. Началната и крайната пермутации се пропускат, тъй като те не оказват влияние върху изводите в този случай. Това се дължи на типа атака, а именно – атака с известен явен текст (KPA), която работи със случайни стойности на явния текст [29].

2.3 Линейни характеристики

Първата цел на линейния криптоанализ е намирането на линеен апроксимиращ израз от вида $P[i_1, \ldots, i_p] \oplus C[j_1, \ldots, j_q] = K[k_1, \ldots, k_r]$, изпълнен с вероятност $p \neq 1/2$ за случайно избран явен текст P, съответния шифров текст C и фиксиран шифров ключ K. Величината $p - 1/2$ се нарича *отклонение*, а нейната големина $|p - 1/2|$ се нарича *ефективност* на апроксимиращия израз.

Конструирането на апроксимиращи изрази става чрез използване на линейни характеристики, които се дефинират с маски на вектори или с множества от индекси.

Дефиниция 2.3.3. 1-рундова линейна характеристика *за рунд j на Файстел-шифър е двойка $(I_X(j), I_F(j))$ множества от индекси на битове от входа и изхода на този рунд, съответно.* n-рундова линейна характеристика *за рундовете $1, \ldots, n$, $n \geq 3$, е n-торка $((I_X(1), I_F(1)), \ldots, (I_X(n), I_F(n)))$ от 1-рундови линейни характеристики със свойството*

$$I_F(j+1) = (I_F(j-1) \cup I_X(j)) \backslash (I_F(j-1) \cap I_X(j))$$

за всички $2 \leq j \leq n-1$ (т.е. ако $I_F(j+1)$ е симетричната разлика на $I_F(j-1)$ и $I_X(j)$).

Сумирането на всички битове, определени от една линейна характеристика, дава краен израз от необходимия вид, с който тя се асоциира. Съвместното сбъдване на всички 1-рундови апроксимации, определени от характеристиката, водят до изпълнение и на крайния апроксимиращ израз. Апроксимиращият израз с най-голяма ефективност се нарича *най-добър израз*, неговата вероятност – *най-добра вероятност*, а линейна характеристика, от която е получен – *най-добра характеристика.*

От гледна точка на линейния криптоанализ, стохастичните апроксимиращи изрази, които се различават само с адитивна константа, се разглеждат като еквивалентни, тъй като адитивна константа би променила (евентуално) само знака на отклонението, но всички използвани при криптоанализа параметри на уравнението, в това число и неговата ефективност, се запазват (виж, напр [23, Гл. 8.2]).

Линейната линейна характеристика (апроксимация), дефинирана с множествата индекси (I_X, I_F), се нарича *тривиална нула–към–нула* характеристика (апроксимация), ако $I_X = \phi$ и $I_F = \phi$. S-кутията S се нарича *активна* за линейната характеристика l, ако в l участва приближение на S, което не е тривиалната нула–към–нула апроксимация. Един рунд се нарича *активен* за линейната характеристика l, ако в l има активна S-кутия от този рунд.

Детерминистичен се нарича линеен апроксимиращ израз, който е изпълнен с вероятност 1 или 0. Детерминистичните изрази нямат особен самостоятелен смисъл за приложение в линейния криптоанализ, освен като съставна част на по-сложни характеристики.

Характерно за итерационните шифри със симетрична структура, какъвто е DES, е че линейните характеристики за тях или са със симетрична структура (разгледана спрямо първия и последния рунд), или могат да бъдат групирани по двойки несиметрични, но симетрични една на друга характеристики [28].

2.4 Вероятности на линейните характеристики

За намиране на линейна апроксимация на целия шифър компонентите, които е важно да бъдат линейно апроксимирани, са нелинейните елементи от трансформацията. Това става с т.н. линейно апроксимиращи таблици. В DES алгоритъма S-кутиите са единствения нелинеен елемент, поради което с тяхна апроксимация започва изграждането на каквито и да е линейни приближения.

Дефиниция 2.4.1. *За дадена S-кутия S_k с a-битов вход и c-битов изход и дадени числа α и β такива, че $0 \leq \alpha \leq 2^a - 1$ и $0 \leq \beta \leq 2^c - 1$, дефинираме $NS_k(\alpha, \beta)$ като броя пъти от общо 2^a възможни входни стойности на S_k, такива, че XOR-сумата на входните битове, маскирани чрез α, съвпада с XOR-сумата на изходните битове, маскирани чрез β. С други думи*

$$NS_k(\alpha, \beta) = \#\{x | 0 \leq x \leq 2^a - 1 \ и \ \oplus_s (x[s] \circ \alpha[s]) = \oplus_t (S_k(x)[t] \circ \beta[t])\}.$$

Таблицата, в която вертикалата и хоризонталата изразяват α and β съответно, и всеки елемент съдържа стойността $NS_k^*(\alpha, \beta) = NS_k(\alpha, \beta) - 2^{a-1}$, се нарича линейно апроксимираща таблица *(*ЛАТ*) за S_k.*

За DES има 8 ЛАТ с по 64 реда и 16 колони. Случаите, когато $\alpha = 0$ или $\beta = 0$, за DES не са информативни и затова не биват разглеждани.

Основните свойства на ЛАТ за DES Мацуи формулира в [28] като лема.

Лема 2.4.1. (i) $NS_k(\alpha, \beta)$ *е четно.*
(ii) *Ако* $\alpha = 1, 32$ *или* 33, *то* $NS_k(\alpha, \beta) = 32$ *за всички* S_k *и* β.

Ефективността на една линейна апроксимация на S-кутия се смята директно от ЛАТ. За изчисление на ефективността на комбинация от повече от една апроксимации на S-кутии, в един или повече рундове, се използва т.н. „Пилинг-ъп"-лема (Piling-up Lemma, [28]).

2.5 Подходи за конструиране на ефективни характеристики

Двата основни подхода за конструкция на добри многорундови линейни характеристики са – чрез не повече от една активна S-кутия на рунд („Тип I") и чрез двурундови итеративни характеристики, изградени от една нетривиална 1-рундова апроксимация с нулева входна маска и ненулева ефективност и една тривиална нула–към–нула апроксимация („Тип II") [30]. И двата подхода са израз на една и съща стратегия – минимизиране на броя активни S-кутии с цел повишаване на ефективността (имайки предвид „Пилинг-ъп" лемата). Мацуи показва, че Тип I подходът дава по-добри резултати при DES, но при някои негови модификации характеристиките от Тип II са по-добри.

2.6 Уравнения за битовете на ключа

При конструкцията на линейни апроксимиращи изрази чрез една характеристика може да се използва както директно сумата от всички битове в характеристиката, така и по-сложни релации [28, 29]. Ако n е броят на рундовете в алгоритъма, чрез характеристика за първите $(n-1)$ рунда и вътрешните релации във Файстел-схемата за последния рунд се получава нов тип апроксимация. Ако характеристиката е за рундове от 2 до $(n-1)$ и се използват структурните релации от двата крайни рунда, се получава трети тип апроксимация.

Битовете от текста (явен и шифров) и от ключа, чиито стойности влияят върху стойностите в апроксимиращите изрази, се наричат *ефективни битове*. S-кутиите, изходни битове от които участват в тези изрази, се наричат *активни S-кутии* за съответните уравнения. Ефективните битове от текста се разглеждат като известни, тъй като те се заместват по време на криптоанализа с налични данни, докато ефективните ключови битове се разглеждат като част от неизвестните, спрямо които се решава уравнението, определено от линейната апроксимация.

2.7 Конструкция на линейни атаки

Общата конструкция на атака при линейния криптоанализ включва: намиране на най-добрите линейни апроксимиращи изрази; определяне на ефективните битове; намиране чрез метода на максималното правдоподобие на стойностите на ефективните ключови битове и на още един бит на ключа под формата на сума от битове; намиране на останалите (неизвестни) битове на ключа чрез изчерпващо търсене [29]. При наличие на повече от една използваема характеристика, те се комбинират подходящо, в зависимост от конкретните условия.

По-обобщен модел на техниката може да бъде описана като: *фаза на дестилация*; *фаза на анализ*; *фаза на търсене* [4].

2.8 Сложност на линейните атаки

В своята основополагаща работа Мацуи [28, 29] е анализирал линейно апроксимиращите таблици, намерил е най-добрите линейни характеристики за брой рундове от 3 до 20 и е изследвал различни техники за конструкция на атаки на различен брой рундове на DES алгоритъма. Първата, изобщо, експериментална криптоатака на DES, демонстрирана от него [29], се базира на апроксимации, базирани на най-добрите 14-рундови характеристики. Мацуи доказва, че сложността на линейна атака, основана на разглеждания тип апроксимации, зависи практически само от ефективността e на апроксимацията и участващите в нея изходни битове от трансформациите в крайните рундове. Броят двойки явен текст/шифров текст, необходими за успешна атака с висока вероятност, е пропорционална на e^{-2}.

Глава 3. Модифицирано семейство от алгоритми

В трета глава се разглежда базовата концепция за вграждане на контрол по четност в изходите на заместителните таблици на един шифър. Представени са основните техники, използвани за търсене и анализ на най-добри линейни характеристики, и резултатите от тяхното прилагане при еднакви позиции на контролните битове.

3.1 Общо описание на подхода

Първата фаза на нашия експеримент се състои от следните стъпки:

- вграждане на бит за контрол по четност на една и съща позиция в изходите на всички S-кутии на DES алгоритъма;
- анализ на свойствата на новите линейно апроксимиращи таблици (ЛАТ);

- за четирите различни възможни избора на позиции на контролните битове, намиране на най-добрите характеристики от Тип I за брой рундове от 3 до 20 и на най-добрите двурундови итерационни характеристики (Тип II);
- сравнение на получените резултати с тези за оригиналния шифър;
- сравнение на характеристиките от Тип I и Тип II за модифицирания шифър;
- изследване на нов тип 1-рундови характеристики, дължащи съществуването си на въведената модификация и позволяващи конструкция на двурундови итеративни характеристики;
- сравнение на двата типа двурундови итеративни характеристики за модифицирания шифър.

Без ограничение на общността, вграждаме контрол по четност с нечетна сума на битовете (контрол по нечетност). Стойност 0 на маската на контролния бит се асоциира с S-кутия на оригиналния алгоритъм. С $S_{k(\pi)}$ означаваме S-кутията, получена от S_k на DES при маска π на контролния бит, а с $NS_k^*(\pi;\alpha,\beta)$ – стойностите в ЛАТ за $S_{k(\pi)}$.

3.2 Свойства на ЛАТ

3.2.1 Частта от ЛАТ с ненулеви входна и изходна маски

В случая на ненулеви входна и изходна маски е в сила следната теорема:

Теорема 3.2.1. *Нека S_k е S-кутия на DES. Нека $\pi \neq 0$ е маска на контролния бит по четност в изхода на S_k. Тогава:*

(i) $NS_k^*(\pi;\alpha,15) = 0$ *за всички* α*;*

(ii) $NS_k^*(\pi;\alpha,\beta) = NS_k^*(\alpha,\beta)$ *за всички* α *и* β *такива, че* $\beta\&\pi = 0$*;*

(iii) $NS_k^*(\pi;\alpha,\beta) = -NS_k^*(\alpha,15-\beta)$ *за всички* α *и* $\beta < 15$ *такива, че* $\beta\&\pi \neq 0$.

Непосредствени изводи от горната теорема са, че „новите“ ЛАТ са „обратно“ симетрични, както и че единственият глобален екстремум в ЛАТ на DES, $NS_5^*(16,15) = -20$, бива заменен в резултат на модификацията на S_5 с 0, независимо от позицията на контролния бит.

Пълните ЛАТ за модифицираната S_1 са дадени в Приложение А.

3.2.2 Частта от ЛАТ, съдържаща нулеви маски

Твърдение 3.2.1. *За всяка S-кутия S_k на DES и контрол по четност с нечетна контролна сума, приложен към нейния изход с маска $\pi \neq 0$, имаме, че е изпълнено:*

(i) $NS_k^*(\pi; 0, \beta) = 0$ *за всички* $\beta : 15 > \beta > 0$*;*
(ii) $NS_k^*(\pi; 0, 15) = -32$*, докато* $NS_k^*(\pi; 0, 0) = 32$*;*
(iii) $NS_k^*(\pi; \alpha, 0) = 0$ *за всички* $\alpha \neq 0$*.*

Твърдението ни дава основания в по-нататъшните разсъждения да разглеждаме като нетривиални само линейните приближения на S-кутии с ненулеви входна и изходна маски, като Мацуи при оригиналния DES.

3.3 Стратегия с не повече от една активна заместителна таблица на рунд

Настоящият раздел е посветен на характеристиките от Тип I, чрез които Мацуи ([29]) реализира първия в историята успешен експериментален криптоанализ на стандарта за криптиране DES.

3.3.1 Възможности за използване на частта от ЛАТ, съдържаща нулеви маски

Ограничената употреба на частта от ЛАТ, съдържаща нулеви маски, е предмет на следващото твърдение.

Твърдение 3.3.1. *Нека разгледаме произволна многорундова линейна характеристика на модифициран DES алгоритъм с вграден контрол по четност, базирана на най-много една активна S-кутия на рунд. Ако в нейната структура има поне една 1-рундова характеристика, която не е тривиална (нула-към-нула) характеристика и съществува последователност от три 1-рундови характеристики, две от които са тривиални, то тогава тази многорундова характеристика определя линеен апроксимиращ израз, който е детерминистичен.*

3.3.2 Намаляващата ефективност на линейните характеристики за малък брой рундове

Използвайки особеностите на Файстел-структурите и вече доказаното, имаме възможност да формулираме следващата теорема, която съдържа един от основните резултати в тази глава.

Теорема 3.3.1. *Всяко вграждане на контрол по четност в изходите на S-кутиите на DES води до редуциране на най-високата ефективност на едно-рундовите и 3-рундовите линейни характеристики, получени в рамките на линеен криптоанализ на базата на най-много една активна заместителна таблица на рунд.*

3.3.3 Базов алгоритъм за търсене (БАТ) на най-добрите многорундови характеристики

Основната цел на Базовия алгоритъм за търсене е конструкция на всички n-рундови ($n \geq 3$) линейни характеристики с ненулево отклонение. Алгоритъмът

включва две главни фази: 1) Инициализация и 2) Междурундово съгласуване (round chaining) с финализация в последния рунд.

Инициализация. Напълно се конструират извадките от входни и изходни битове за първия рунд и изходни битове за втория рунд. Частично се конструира входната извадка за втория рунд.
Междурундово съгласуване (една стъпка; изпълнява се последователно за $j = 2, 3, \ldots, n-1$). Довършва се конструкцията на входната извадка за j-тия рунд и се конструира напълно изходната извадка за рунд $(j+1)$. Ако $(j+1)$-ят рунд не е последен, входната извадка за него се конструира частично, в противен случай – напълно.

От извършения до момента анализ се извеждат редица вътрешни релации в многорундовите характеристики, които се използват ефективно за оптимизация в БАТ.

3.3.4 Описание на БАТ

Използваното в БАТ описание на характеристики е чрез множества от битови индекси. За удобство се въвеждат и две допълнителни дефиниции – за *съвместимост* и за *обратна съвместимост* между две S-кутии от два съседни рунда. БАТ може да бъде използван при много общи условия за широка фамилия от шифри, които са наречени „Обобщен шифър“.

Обобщен шифър. Обобщеният шифър е фамилия шифри на Файстел с дължина на блока $2b$ и рундова функция в j-я рунд

$$f_j(X_j, K_j) = Prm(Sub(Exp(X_j) \oplus K_j)),$$

където: Exp е разширяваща функция от b бита до e бита; Sub е заместителна функция; $Sub(X) = S_1(X) \| S_2(X) \| \ldots \| S_m(X)$, като S_k е S-кутия от (e/m) бита към (b/m) бита, $1 \leq k \leq m$, и $\|$ е конкатенация на двоични вектори; Prm е пермутация на b бита.

Обобщеният шифър има логическа структура, обобщаваща тази на DES. Това е основна принципна структура при конструкция на криптографски алгоритми, която често служи като база за модификации и усложнения.

3.3.5 Приложение на БАТ за DES

Логиката на Базовия алгоритъм за търсене дава възможност при софтуерната му реализация да бъдат използвани ефективно характерни особености на DES, дължащи се на конкретните математически примитиви в него.

За намиране на най-добрите линейни характеристики са необходими две допълнителни модификации на БАТ. Първо, изборът на входна извадка за първия и последния рунд трябва да се оптимизира чрез селектиране само на конфигурации с максимална ефективност. Второ, трябва да се поддържа и опреснява информация за най-добрата, намерена до момента, характеристика.

За целите на експеримента е направена реализация на БАТ на езика C++.

3.3.6 Адаптация на БАТ при вграден контрол по четност

Общото условие за междурундова съгласуваност при линейни характеристики за Файстел-шифри е при хипотеза за независимост между изходните битове от един рунд. Наличието на контрол по четност позволява отслабване (разширение) на изискванията при съгласуване, което трябва да бъде отразено в алгоритъма за конструкция на характеристики. В същото време симетричността на ЛАТ за модифицирания шифър дава възможност за инициализиране на БАТ само с половината от възможните комбинации, тъй като останалата половина само дублират резултатите.

Допълнително, търсенето на характеристики е ограничено само до първите намерени оптимални входни извадки за първия и последния рунд, при вече фиксирани изходни извадки за тях. Това е така, защото активните S-кутии остават същите, а това е достатъчно за нашата основна цел – сравнение на стойностите на най-добрите вероятности и структурата на най-добрите характеристики в различните случаи.

3.3.7 Ефекти от вграждането на контрол по четност

Вграждането на контрол по четност влияе върху линейните характеристики в два основни аспекта – тяхната структура и техните вероятности. Някои ненулеви отклонения се нулират и съответните 1-рундови апроксимации не могат вече да участват в конструкция на многорундови. Някои нулеви отклонения пък стават ненулеви и дават възможност за нови конструкции. Част от ненулевите отклонения остават ненулеви, но се променят по абсолютна стойност, което води до промяна на техния принос в отклонението на многорундовите характеристики. Наличието на „паритет“ между определени битове пък увеличава вътрешните варианти за междурундово съгласуване на 1-рундови характеристики и дава възможност за получаване на повече многорундови апроксимации с ненулево отклонение.

Допълнителна информация за сложността на търсене чрез БАТ за оригиналния и за модифицирания алгоритъм са дадени в Приложение Г.

3.3.8 Най-добри вероятности

Вероятностните отклонения на най-добрите характеристики, получени чрез реализирания алгоритъм за търсене, са дадени в Таблица 3.3. От нея може да се заключи, че въпреки намаляването на ефективността на най-добрите 1-рундови характеристики, ефективността на най-добрите многорундови характеристики може както да расте спрямо оригиналния шифър, така и да намалява, в зависимост от позицията на контролния бит.

3.3.9 Най-добри характеристики: брой и тип

Използването на повече характеристики при криптоанализа дава възможност за определяне чрез тях на стойностите на повече битове на ключа, което упростява фазата на изчерпващо търсене при атаката.

Броят и структурата на най-добрите характеристики, намерени чрез БАТ, са дадени в Таблица 3.4. Ясно се вижда, че те силно зависят от наличието и мястото на контролния бит. В почти всички случаи в нашия експеримент броят на най-добрите характеристики за модифицирания шифър е поне колкото този в оригиналния шифър. Въпреки това, и тук има „изключения“ и в другата посока.

В Приложение Б е описана подробно структурата на всички най-добри характеристики, заедно с участващите в 1-рундовите апроксимации битове.

3.3.10 Сравнение на най-добри многорундови апроксимиращи изрази

В Таблица 3.5 са обобщени някои детайли, свързани с 16-рундовите и 19-рундовите апроксимиращи изрази, използващи съответно 14-рундовите и 17-рундовите най-добри линейни характеристики за оригиналния и модифицирания шифър. Таблицата включва означение на апроксимациите, тяхната ефективност и броя на активните S-кутии за всяка апроксимация.

Таблицата показва, че няма еднозначно правило за зависимост на сложността на потенциална атака от наличието на контрол по четност между изходните битове. При вграден такъв контрол има случаи на по-ниска и по-висока ефективност, комбинирана с повече или по-малко на брой активни S-кутии, в сравнение с оригиналния шифър.

Още детайли и коментари относно 16-рундовите апроксимиращи изрази са дадени в Приложение В.

3.3.11 Заключение

При вграждане на битове за контрол по четност на едни и същи позиции в изходите на всички S-кутии на DES, резултатите в раздел 3.3 доказват, че ефективността на най-добрите 1-рундови и 3-рундови характеристики от Тип I за модифицирания алгоритъм винаги се редуцира. Това не е вярно обаче за характеристики за по-голям брой рундове, където анализите сочат, че модификация от разглеждания тип не означава еднозначно намаление или увеличение на най-високата ефективност. Освен това, броят на най-добрите характеристики също варира в зависимост от избора на позиция на контролния бит, като това се отнася и за броя активни S-кутии в крайните линейни уравнения и съответно броя ефективни битове на текста и на ключа в тях.

3.4 Стратегия с двурундови итеративни характеристики

В този раздел се разглеждат линейните характеристики от Тип II за модифицирания шифър. Тъй като те изцяло се определят от използваните двурундови итерационни характеристики, които от своя страна пък напълно се дефинират чрез участващата в тях единствена нетривиална 1-рундова характеристика, разглежданията са съсредоточени основно върху 1-рундовите характеристики от необходимия тип. В разглежданията се включват и новия тип 1-рундови характеристики, позволяващи итериране и възникнали благодарение на типа на модификацията.

3.4.1 Еднорундови характеристики с нулева входна маска

Когато се разглеждат едновременно апроксимации на две или повече S-кутии на DES алгоритъма, могат да бъдат намерени 1-рундови характеристики с нулева входна маска и ненулева изходна маска, имащи ефективност в отворения интервал (0,1/2), т.е. не са детерминирани. Възможност за това дава специалният вид на разширение на входния текст за всяка итерация, при което от 32 бита се получават 48 бита чрез дублиране на 16 от входните битове. При вграден контрол по четност същият тип характеристики продължават да съществуват.

Чрез целево разработен софтуер на C++ е извършено изчерпващо търсене за комбинации от апроксимации на S-кутии, даващи най-добри еднорундови характеристики с нулева входна маска и ненулева изходна маска и ненулево отклонение. Резултатите от него са представени в Таблица 3.6 чрез съответните стойности в ЛАТ. Те сочат, че най-добрите характеристики от Тип II и в четирите случая с наличен контролен бит имат по-лоша ефективност в сравнение с тези за оригиналния шифър.

3.4.2 Еднорундови характеристики с входна маска, поддържаща паритета

Оказва се, че, благодарение на вграждането на контролен бит, възниква още един, нов, тип 1-рундови характеристики, базирани на комбинации от апроксимации на повече от една S-кутия, които могат да бъдат използвани за конструкция на 2-рундови итеративни характеристики.

Дефиниция 3.4.1. *Множеството от всички изходни битове на една S-кутия ще наричаме* паритетно множество битове, *а тяхната XOR-сума –* паритетна сума. *Входна маска, определяща непразно множество от входни битове, което е обединение на подмножества, всяко от които е паритетно, получено в предходния рунд, наричаме* входна маска, поддържаща паритета.

Сумата на входните битове, определени от такъв тип входни маски, е константна и, тъй като в линейния криптоанализ адитивните константи биват игнорирани в апроксимиращите изрази, 1-рундовите характеристика с входна маска,

поддържаща паритета, могат да бъдат използвана по същия начин, както характеристиките с нулева входна маска, за конструкция на 2-рундови итеративни характеристики. Необходимо е да се има предвид, че, поради разширението на входния текст чрез размножаване на половината битове от него, една и съща като съдържание комбинация от входни битове може да бъде селектирана чрез различни комбинации на входни маски на S-кутии. При това обаче участващите в апроксимацията битове на ключа ще бъдат различни.

3.4.3 Еднорундови характеристики с входна маска, определяща константа

Двата типа входни маски, позволяващи конструкция на двурундови итеративни характеристики за модифицирания алгоритъм, обединяваме чрез следната дефиниция.

Дефиниция 3.4.3. *Входна маска, определяща множество от входни битове, XOR-сумата на които е тъждествено равна на константа, наричаме* входна маска, определяща константа.

Отчитайки характерните особености на конкретните математически примитиви в DES, може да бъде получена оценка за ефективността на еднорундовите характеристики с такава входна маска. Следващата теорема съдържаща основния извод в раздел 3.4.

Теорема 3.4.1. *При модифициран алгоритъм с еднакви позиции на контролните битове максималната ефективност, която може да има еднорундова характеристика с входна маска, определяща константа, е* $9 \cdot 2^{-8}$ *и тя е по-малка от максималната ефективност на еднорундова характеристика с нулева входна маска при оригиналния алгоритъм.*

3.4.4 Заключение

В този раздел показахме, че при вграждане на битове за контрол по четност на едни и същи позиции в изходите на всички S-кутии на DES ефективността на най-добрите характеристики от Тип II за модифицирания алгоритъм винаги намалява в сравнение с оригиналния алгоритъм. Доказахме също, че максималната ефективност, която може да се постигне чрез възникналия нов тип 1-рундови характеристики, позволяващи итериране, е по-ниска от ефективността на характеристиките от Тип II.

3.5 Сравнение на резултатите при различните стратегии

В Таблица 3.9 се прави сравнение на резултатите от двата подхода (Тип I и Тип II) за модифицирания алгоритъм. На базата на резултатите при маска на контролния бит $\pi = 0010$ се демонстрира, че е в сила извод, аналогичен на направения от Мацуи в [30], т.е. че, за разлика от DES, в някои случаи

за модифицирания алгоритъм най-добрите характеристики от Тип II имат по-високи ефективности от тези от Тип I.

Глава 4. Независим избор на позиции на контролните битове

В четвърта глава въвеждането на контрол по четност се разглежда в много по-широк кръг от трансформации, предполагащи независим избор на позиции за контролните битове за различните S-кутии. Търсят се границите на вариация на ефективността на най-добрите характеристики при различен брой рундове и удобни и приложими критерии за предварителна оценка и/или контрол на ефекта от прилагане на модификация.

4.1 Свойства на ЛАТ

Проведените наблюдения показват, че определен тип елементи на ЛАТ могат да имат важна роля в задачата за оптимизация.

Дефиниция 4.1.1. *Елементът* $NS_k^*(\alpha, \beta)$, $1 \leq \alpha \leq 63$, $1 \leq \beta \leq 14$, *на ЛАТ за* S_k *на DES се нарича* инвариантен при прилагане на контрол по четност *(или просто* инвариантен*) ако*

$$|NS_k^*(\alpha, \beta)| = |NS_k^*(\pi; \alpha, \beta)|$$

за всяка маска π *на контролния бит.*

Нека I е множеството от всички инвариантни елементи на всички ЛАТ и $M_I := \max_{\mathcal{L} \in I} |\mathcal{L}|$. Следващото твърдение разкрива смисъла на дефиницията за инвариантност.

Твърдение 4.1.1. *Нека* π_k *е маската на контролния бит на* S_k *на DES,* $1 \leq k \leq 8$. *Тогава*

$$\max_{k,\alpha,\beta} \left\{ |NS_k^*(\pi_k; \alpha, \beta)| \right\} \geq M_I,$$

където максимумът е по всички $1 \leq k \leq 8$, $1 \leq \alpha \leq 63$ *и* $1 \leq \beta \leq 14$.

4.2 Стратегия с не повече от една активна заместителна таблица на рунд

4.2.1 Оптимални характеристики за малък брой рундове

За малък брой рундове е в сила следната теорема.

Теорема 4.2.1. *Нека π_7 е маската на контролния бит на S_7. В сила са следните твърдения:*
(i) Необходимото и достатъчно условие за запазване максимално възможна ефективността на най-добрата еднорундова характеристика е $\pi_7 \neq 4$. Максималната големина на елемент в ЛАТ в този случай е 18.
(ii) Необходимото и достатъчно условие за минимизиране на ефективността на най-добрата еднорундова характеристика, базирана на една S-кутия, е $\pi_7 = 4$. Максималната големина на елемент в ЛАТ в този случай е 16.
(iii) Условията в подточки (i) и (ii) са необходими и достатъчни и за получаване на оптимални 3-рундови характеристики. Техните ефективности са $2(18/64)^2 \approx 0.1582$ и $2(16/64)^2 = 0.1250$, съответно.

4.2.2 Оптимални характеристики по отношение на условията за атака при много рундове

Търсене на оптимални конфигурации от маски в този случай означава търсене на

$$\max_{\overline{\pi}} \max_{l} \{eff\},$$

където l е линейна характеристика за съответния брой рундове, eff е нейната ефективност и $\overline{\pi}$ е комбинация от осемте маски на контролните битове.

Резултатите от проведеното изчерпващо търсене за брой рундове от 3 до 20 са дадени в Таблица 4.1. Може да се види, че опитно установеният брой на оптималните конфигурации при три рунда съответства на доказаното в Теорема 4.2.1, подточка (i). Този брой е точно $49152 = 4^8 - 4^7$. Същото важи и за установената ефективност.

Съществуването на стойности на ефективност, които не могат да бъдат постигнати с еднаква позиция на контролните битове показва, че *при независим избор на позиции на контролните битове за различните S-кутии могат да бъдат създадени по-благоприятни условия за атака, отколкото при еднакви позиции на контролните битове.*

Малкият брой стойности, по-голяма от тази при оригиналния шифър, потвърждава общата тенденция за намаляване на ефективността на най-добрите характеристики, въпреки че, в зависимост от позициите на контролните битове, тя може и да расте. Тази тенденция се потвърждава и от факта, че има един единствен случай, за 5 рунда, при който независим избор на позиции може да доведе до по-голяма ефективност отколкото при DES, която не може да бъде достигната с еднакви позиции на контролни битове.

4.2.3 Оптимални характеристики по отношение на устойчивостта на атака при много рундове

В този случай търсенето ще има вида

$$\min_{\overline{\pi}} \max_{l} \{eff\}.$$

Съответно, Таблица 4.2 съдържа резултатите от изчерпващото търсене.

И тук опитно установеният брой на оптималните конфигурации при три рунда съответства на доказаното в подточка (ii) на Теорема 4.2.1. Той е точно $16384 = 4^7$. Същото важи и за установената ефективност.

Съществуването на стойности, които не могат да бъдат постигнати с еднаква позиция на контролните битове показва, че *чрез независим избор на позиции може да се осигури по-висока устойчивост на линейни атаки, отколкото при еднакви позиции на контролните битове.*

4.3 Стратегия с двурундови итеративни характеристики

4.3.1 Оптимални характеристики от Тип II по отношение на условията за атака

Задачата за оптимизация в този случай е същата, както при най-много една активна S-кутия на рунд, но измежду различен тип характеристики. Резултатите от изчерпващото търсене, представени в Таблица 4.3, показват че в този случай независимият избор на позиции за контролните битове не може да доведе до по-висока ефективност. Причината за това е дадена в следващото твърдение.

Твърдение 4.2.1. *Нека π_8 е маската на контролния бит в изхода на заместителната таблица S_8. Тогава $\pi_8 = 2$ е необходимо и достатъчно условие за максимизиране на ефективността на най-добрата еднорундова характеристика с нулева входна маска.*

4.3.2 Оптимални характеристики от Тип II по отношение на устойчивостта на атака

Резултатите от изчерпващото търсене са дадени в Таблица 4.4. Те показват, че чрез независим избор на позиции може да се постигне по-висока устойчивост в сравнение със случая на еднакви позиции на контролните битове.

4.4 Анализ на резултатите

4.4.1 Характеристики с най-много една активна S-кутия на рунд

В Таблица 4.5 са дадени границите на вариация на ефективността на най-добрите характеристики с не повече от една активна S-кутия на рунд за модифицирания алгоритъм. В общия случай тази ефективност, разгледана спрямо порядъка на ефективността при оригиналния алгоритъм, се влошава средно в граници приблизително половината от този порядък.

4.4.2 Характеристики с входна маска, определяща константа

За този тип характеристики е в сила следващата теорема.

Теорема 4.4.1. *При независим избор на позиции на контролните битове, по отношение на максималната ефективност на 1-рундови характеристики*

с входна маска, определяща константа, са в сила следните твърдения:
(i) Максимално постижимата ефективност е по-малка от максималната ефективност на характеристики с нулева входна маска при оригиналния алгоритъм.
(ii) Стойността на максималната ефективност на такива характеристики е $9 \cdot 2^{-8}$*. Тя може да бъде достигната само за характеристики с нулева входна маска, като необходимото и достатъчно условие за съществуването на такава характеристика е маската на контролния бит в изхода на заместителната таблица* S_8 *да е* 2*. Такава ефективност не може да бъде достигната при характеристики с входна маска, поддържаща паритета.*

Забележка 4.4.1. При използване на DES за базов алгоритъма се получава, че характеристиките с входна маска, поддържаща паритета, дават по-малка максимална ефективност, отколкото характеристиките с нулева входна маска. Този извод обаче не може да бъде механично пренесен за произволен алгоритъм, тъй като резултатът съществено зависи от механизмите за конструкция на характеристиките и компонентите на алгоритъма, като например съдържанието на S-кутиите, начина за генериране на рундовия ключ и т.н.

Глава 5. Контрол по четност като част от афинна трансформация на изходите на заместителните таблици

В тази глава кръгът от изследвани модификации се разширява още повече, като контролът по четност се разглежда в рамките на обща афинна трансформация на изходите на S-кутиите.

5.1 Обща постановка

Да означим с $b^{(k)} = b_3^{(k)} b_2^{(k)} b_1^{(k)} b_0^{(k)}$, $1 \leq k \leq 8$, изхода в битове на S_k на DES. Разглеждаме модификация, при която към изхода на всяка S_k е приложена допълнителна афинна трансформация $\Theta_k : \mathbb{F}_2^4 \to \mathbb{F}_2^4, \mathbb{F}_2 = \mathbf{GF}(2)$, имаща вида:

$$d_i^{(k)} = a_{i3}^{(k)} \circ b_3^{(k)} \oplus a_{i2}^{(k)} \circ b_2^{(k)} \oplus a_{i1}^{(k)} \circ b_1^{(k)} \oplus a_{i0}^{(k)} \circ b_0^{(k)} \oplus c_i^{(k)},$$

където $a_i^{(k)} = a_{i3}^{(k)} a_{i2}^{(k)} a_{i1}^{(k)} a_{i0}^{(k)}$ е двоичен вектор, $i = 0, 1, 2, 3$. Изходът от модифицираната S_k означаваме с $d^{(k)} = d_3^{(k)} d_2^{(k)} d_1^{(k)} d_0^{(k)}$. Трансформация Θ_k разглеждаме като модификация на самата S-кутия, получена чрез поелементно прилагане на трансформацията. Елементите на ЛАТ за модифицираната S-кутия означаваме с $NS^*_{\Theta_k}(\alpha, \beta)$.

Маските на изходите на S-кутиите разглеждаме като елементи от четиримерното линейно векторно пространство $\{0, 1\}^4$, в което събирането на елементи

е дефинирано като побитово сумиране по модул 2, означавано със символа &. В термините на това пространство използваме понятията за *линейна комбинация*, *линейна независимост*, *линейна обвивка* и *линейно подпространство*. Линейната обвивка на маските $\mu^{(1)}, \ldots, \mu^{(m)}$ означаваме с $l(\mu^{(1)}, \ldots, \mu^{(m)})$, а нейната размерност – с $dim(\mu^{(1)}, \ldots, \mu^{(m)})$. За всяка изходна маска $\beta, 0 \leq \beta \leq 15$, маската $\overline{\beta} = 15 - \beta$ наричаме нейна *симетрична*.

5.2 Свойства на ЛАТ

Твърдение 5.2.1. *Нека $\mu_i = 2^i$, $i = 0, 1, 2, 3$. Тогава за елементите на ЛАТ за модифицираната S_k са в сила следните свойства:*
(i) $NS^*_{\Theta_k}(\alpha, \mu_i) = (-1)^{c_i^{(k)}} NS^*_k(\alpha, a_i^{(k)})$ *за всяко* i *и всяко* α.
(ii) За всяко α *и всяко* β *имаме* $NS^*_{\Theta_k}(\alpha, \beta) = (-1)^{c(\alpha,\beta)} NS^*_k(\alpha, \mu(\alpha, \beta))$, *за някаква константа* $c = c(\alpha, \beta) \in \{0, 1\}$ *и маска* $\mu = \mu(\alpha, \beta) \in l(a_0^{(k)}, a_1^{(k)}, a_2^{(k)}, a_3^{(k)})$.

Непосредствени следствия от това твърдение са, че винаги можем да запазим поне четири от оригиналните колони за ненулеви маски чрез подходящ избор на трансформация, както и че от оригиналната ЛАТ се запазват само колоните за маски от $l(a_0^{(k)}, a_1^{(k)}, a_2^{(k)}, a_3^{(k)})$.

5.3 Контрол по четност като част от афинна трансформация

Вграждането на контрол по четност при прилагане на афинна трансформация към изхода на S_k се изразява в допълнителното тъждество

$$d_3^{(k)} \oplus d_2^{(k)} \oplus d_1^{(k)} \oplus d_0^{(k)} = c^{(k)},$$

където константата $c^{(k)}$ е 0 или 1. От криптографска гледна точка най-съществен е случаят с максимално висока сложност на зависимостите, затова разглеждаме само трансформации, при които $dim(a_0^{(k)}, a_1^{(k)}, a_2^{(k)}, a_3^{(k)}) = 3$.

Твърдение 5.3.1. *Нека означим за краткост $l(a) = l(a_0^{(k)}, a_1^{(k)}, a_2^{(k)}, a_3^{(k)})$. Тогава за произволна маска β на изхода на S_k, $1 \leq \beta \leq 14$, са в сила твърденията:*
(i) Ако $15 \in l(a)$, *то* $\beta \in l(a)$ *тогава и само тогава, когато* $\overline{\beta} \in l(a)$.
(ii) Ако $15 \notin l(a)$, *то* $\beta \in l(a)$ *тогава и само тогава, когато* $\overline{\beta} \notin l(a)$.

5.4 Оптимални линейни характеристики за малък брой рундове при най-много една активна S-кутия на рунд

Теорема 5.4.1. *По отношение на ефективността на линейните характеристики за малък брой рундове на модифицирания алгоритъм е изпълнено:*
(i) При подходящи афинни трансформации максималната ефективност на

най-добрата еднорундова характеристика, базирана на една S-кутия, се запазва такава, каквато е за оригиналния алгоритъм, т.е. максимално възможна. Най-голямата абсолютна стойност на елемент на ЛАТ в този случай е 20. Необходимо и достатъчно условие за това е $15 \in l(a_0^{(5)}, a_1^{(5)}, a_2^{(5)}, a_3^{(5)})$.
(ii) Минималната възможна ефективност на най-добрата еднорундова характеристика, базирана на една S-кутия, съответства на абсолютна стойност на елемент в ЛАТ, равна на 16. Необходимо и достатъчно условие за постигане на такава ефективност е едновременно да имаме $15 \notin l(a_0^{(5)}, a_1^{(5)}, a_2^{(5)}, a_3^{(5)})$, $15 \notin l(a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, a_3^{(1)})$ *и* $4 \notin l(a_0^{(7)}, a_1^{(7)}, a_2^{(7)}, a_3^{(7)})$.
(iii) Условията в подточки (i) и (ii) са необходими и достатъчни и за получаване на оптимални 3-рундови характеристики, базирани на не повече от една активна S-кутия на рунд.

5.5 Оптимални двурундови итеративни характеристики

Теорема 5.5.1. *При афинна трансформация с контрол по четност, ефективността на най-добрите еднорундови характеристики с входна маска, определяща константа, за модифицирания алгоритъм:*
(i) винаги е не по-голяма от тази при оригиналния алгоритъм;
(ii) може да бъде запазена равна на тази при оригиналния алгоритъм чрез подходящ избор на афинна трансформация и това се постига само за характеристики с нулева входна маска.

5.6 Заключение

В тази глава доказахме, че, за разлика от случая на модификация на изходите на S-кутиите чрез проста подмяна на един от битовете с контролен бит по четност, при общи афинни трансформации с контрол по четност максималната ефективност на линейните характеристики от Тип I за малък брой рундове може да бъде запазена както при оригиналния алгоритъм. Същото важи и за най-добрите характеристики от Тип II.

Допълнително установихме, че при общ вид афинни трансформации с контрол по четност устойчивостта на атаки чрез характеристики от Тип II (измерена чрез максимална ефективност на такива характеристики) не може да бъде подобрена в сравнение с трансформациите само с вграждане на контролни битове.

Заключение

В дисертацията се изследва влиянието на определен вид модификации на симетрични итерационни шифри върху податливостта на тези шифри на ли-

нейни атаки. Разглежданите шифри са от тип класическа мрежа на Файстел, като за базов е взет алгоритъмът от Data Encryption Standard (DES). Основната модификация се състои във въвеждане на контрол по четност в изходите на S-кутиите на алгоритъма. Като мярка за уязвимостта главно се разглежда ефективността на най-добрите линейни характеристики. Анализират се резултатите от два основни подхода за конструкция на добри характеристики, използвани резултатно и за базовия алгоритъм още докато е действащ стандарт – чрез най-много една активна S-кутия на рунд (характеристики от Тип I) и чрез двурундови итеративни характеристики с тривиална апроксимация за втория рунд (характеристики от Тип II). Установен е и е включен в разглежданията и нов тип двурундови итеративни характеристики, съществуващ благодарение на допълнителните зависимости между битове в модифицирания шифър. Използван е подход с постепенно обобщение на модифициращата трансформация с цел възможност за по-детайлно изследване на ефекта от нея. Извършен е сравнителен анализ на резултатите както от използване на двата подхода за конструкция на характеристики, така и за модифицирания алгоритъм спрямо базовия. В заключение могат да се направят следните изводи:

1). Резултатите от изследванията опровергават интуитивното очакване за неизбежно влошаване на устойчивостта на шифъра срещу линейни атаки при наличие на повече линейни зависимости в неговата структура. Това означава, че в общия случай при оценка в процес на проектиране на алгоритъм не винаги би било необходимо прилагане на техника на „trade-off“ за компенсиране на послабата устойчивост на шифъра с повече на брой рундове и съответно по-дълго време за изпълнение на операциите. При разглеждания от нас експеримент в някои случаи условията за атака наистина се подобряват, но общата тенденция е към понижаване на ефективността на най-добрите линейни характеристики. Оказва се, че ефектът от модификацията съществено зависи от мястото на въвеждане на допълнителни зависимости и конкретните компоненти на шифъра.

2). При разглеждания тип трансформация ефективността на най-добрите линейни характеристики за малък брой рундове може (евентуално) да се запази, но не може да надхвърли тази при оригиналния шифър.

3). Допълнителните линейни зависимости водят до промени на много места в конструкцията на линейни характеристики, включително и до възможност за построяване на нов тип двурундови итеративни характеристики с тривиална апроксимация за втория рунд. В нашия експеримент тези характеристики имат по-ниска ефективност от двурундовите итеративни характеристики на базата на 1-рундови апроксимации с нулева входна маска, но това не може да бъде обобщено за произволен шифър, тъй като съществено зависи от характера на използваните зависимости и конкретните компоненти на шифъра.

4). Допълнителни линейни зависимости в S-кутиите водят до нови свойства

на техните линейно апроксимиращите таблици, които могат да бъдат използвани за оценка на границите на вариация на ефективността при разглеждания тип трансформации за малък брой рундове без помощта на компютър.

5). Резултатите в настоящата дисертация внасят допълнителна яснота относно механизмите на влияние на допълнителни линейни зависимости в един алгоритъм върху неговата устойчивост на линеен криптоанализ. Все пак, преди финални препоръки за практически приложения, разглежданият тип шифри и модификации следва да бъдат подложени и на други достъпни форми на анализ, използващ линейните зависимости в тях.

Авторска справка

Приносите на дисертационния труд са свързани главно с оценката на влиянието на допълнителни линейни зависимости в един криптоалгоритъм върху условията за линеен криптоанализ срещу него. По мнение на автора, основните от тях са:

1. Изследван е механизмът на влияние на допълнителни линейни зависимости в изходите на S-кутиите на един криптоалгоритъм върху свойствата на техните линейно апроксимиращи таблици (ЛАТ).

2. Чрез използване на новите свойства на ЛАТ е доказано неповишаването на ефективността на най-добрите линейни характеристики, базирани на не повече от една S-кутия, за малък брой рундове.

3. Изследвано е влиянието на допълнителни линейни зависимости в криптоалгоритъма върху механизмите за конструкция на многорундови линейни характеристики за него. Това е отразено в разработен на C++ алгоритъм за търсене на линейни характеристики за Файстел-шифри, чрез който са намерени най-добри характеристики за модифицирания алгоритъм. Чрез техния анализ е показано, че наличието на допълнителни линейни връзки не обуславя задължително по-добри условия за линеен криптоанализ.

4. За модифицирания алгоритъм са намерени най-добри двурундови итерационни характеристики. Показано е че, въпреки по-малката им ефективност спрямо тези за базовия алгоритъм, този тип характеристики може да води до по-добри многорундови приближения в сравнение с подхода чрез най-много една активна S-кутия на рунд.

5. Изследван е механизмът на влияние на допълнителните линейни зависимости за възникване на нов вид двурундови итерационни характеристики.

В резултат на това са въведени понятията „входна маска, поддържаща паритета“ и „входна маска, определяща константа“. Доказано е, че ефективността, която може да се достигне чрез тези характеристики, е по ниска от тази, достижима чрез нулеви входни маски. Това е валидно за DES, но силно зависи от математическите примитиви в алгоритъма и не може да бъде обобщено.

6. Изследвано е как наличието на допълнителни линейни връзки прави важни определен тип елементи в ЛАТ, наречени „инвариантни“ (по отношение на прилаганата трансформация), и е демонстрирано как в някои случаи те дават възможност за бързи и точни изводи и оценки без помощта на компютърни изчисления.

7. Голяма част от изводите в дисертацията могат да се обобщат за по-широк кръг от алгоритми и трансформации от разглежданите. В частност, те са приложими и в контекста на конструиране на криптографски алгоритми, когато, например, е необходимо да бъде оценена нуждата от използване на повече рундове за сметка на по-малко нелинейни булеви функции.

Апробация на резултатите

Резултатите в дисертацията са докладвани на:

- Национален семинар по Теория на кодирането „Стефан Додунеков“, Велико Търново, 2014;
- 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques „Advances in Cryptology – EUROCRYPT 2015“, София, България, 2015;
- Second Annual International Conference on Cryptography and Information Security „BalkanCryptSec 2015“, Копер, Словения, 2015;
- Fifteenth International Workshop on „Algebraic and Combinatorial Coding Theory“ (ACCT 2016), КК „Албена“, България, 2016.

Списък на публикациите по дисертацията

Основните резултати по дисертацията са включени в следните публикации:

1. Y. Borissov, P. Boyvalenkov, R. Tsenkov. Linear cryptanalysis and modified DES with parity check in the S-boxes. *Second Conference on Cryptography*

and Information Security in the Balkans, *LNCS* 9540, Springer-Verlag, 2016, pp. 60–78.

2. R. Tsenkov, Y. Borissov. Narrow sense linear cryptanalysis of a family of modified DES ciphers with even weight S-boxes. *Proceedings of Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory*, 2016, pp. 284–289.

3. Y. Borissov, P. Boyvalenkov, R. Tsenkov. On a Linear Cryptanalysis of a Family of Modified DES Ciphers with Even Weight S-boxes. *Cybernetics and Information Technologies*, 16(4), IICT-BAS, 2016, предстои да излезе.

Изданието *Lecture Notes in Computer Sciences*, където е публикувана първата статия, има SJR-ранг 0.252 за 2015 г., а *Cybernetics and Information Technologies*, където е публикувана третатата статия, за 2015 г. има SJR-ранг 0.170.

Благодарности

Работата ми над тази дисертация е свързана с много труд и моменти на силни емоции, голямата част от които прекрасни. Срещнах много и различни предизвикателства, с някои от които едва ли щях да се справя сам. Вложените усилия ме обогатиха значително не само в областта на науката, но и в чисто човешки аспект.

Първо, искам да благодаря на научните си консултанти професор Петър Бойваленков и доцент Юри Борисов за това, че в критичните за мене моменти ми оказваха необходимата и достатъчна подкрепа, за да извървя целия път и да изпитам удовлетвореност от натрупаните знания и умения и постигнатите резултати.

Искам да благодаря и на прекрасния колектив на секция „Математически основи на информатиката“ към Института по математика и информатика на БАН, който ми позволи да се почувствам като негов член и част от една голяма задружна общност с високи цели.

Решаващо значение за успеха на работата ми има и подкрепата от моите колеги от организацията, в която работя. Благодаря за тяхната съпричастност и съдействие.

Накрая, благодаря и на моята съпруга Силвия, че прие с разбиране за едно не малко време да принадлежа изключително на науката и много по-малко на нея и семейството.

Работата ми беше частично подкрепена по договор I01/0003 с Националния Фонд „Научни Изследвания“, за което също изказвам благодарности.

Литература

[1] M. Bellare, P. Rogaway, T. Spies. The FFX mode of operation for format preserving encryption. Submission to NIST, available from http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html, 2010.

[2] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology* 4(1), Springer-Verlag, 1991, pp. 3–72.

[3] E. Biham, A. Shamir. Differential cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993, ISBN: 978-1-4613-9316-0.

[4] A. Biryukov, C.D Cannière, M. Quisquater. On Multiple Linear Approximations. *Advances in Cryptology – CRYPTO 2004*, *LNCS* 3152, Springer-Verlag, 2004, pp. 1–22.

[5] A. Biryukov, G. Leurent, L. Perrin. Cryptanalysis of Feistel Networks with Secret Round Functions. IACR Cryptology ePrint Archive, 2015:723.

[6] A. Bogdanov, V. Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Designs, Codes and Cryptography*, 70(3), Springer-Verlag, 2014, pp. 369–383.

[7] C. Burwick, D. Coppersmith, E. D. Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford, N. Zunic. MARS – a candidate cipher for AES. Submitted as candidate for AES, available from http://citeseerx.ist.psu.edu, 1997.

[8] C. Cachin. Entropy Measures and Unconditional Security in Cryptography. PhD Thesis, ETH Zurich, 1997, *ETH Series in Information Security and Cryptography*, 1, Hartung-Gorre Verlag, Konstanz, 1997,ISBN: 3-89649-185-7.

[9] D. L. Cook. Elastic Block Ciphers. PhD Thesis, Columbia University, 2006.

[10] D. Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38(3), 1994, pp. 243–250.

[11] N. T. Courtois. Feistel schemes and bi-linear cryptanalysis. *Advances in Cryptology – CRYPTO 2004*, *LNCS* 3152, Springer-Verlag, 2004, pp. 23–40.

[12] J. Daemen and V. Rijmen. AES proposal: Rijndael, Version 2.0. 1999, available from http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

[13] Y. Dodis, K. Pietrzak. Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks. *Advances in Cryptology – CRYPTO 2010*, *LNCS* 6223, Springer-Verlag, 2010, pp. 21–40.

[14] Federal Agency on Technical Regulating and Metrology, Information technology. Cryptographic data security. Block ciphers, GOST R 34.12-2015, 2015.

[15] L. Fibikova. Provable Secure Scalable Block Ciphers. Dissertation, University of Duisburg-Essen, 2003, pp. 1–139.

[16] S. Goldwasser, S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2), 1984, pp. 270—299.

[17] Government Committee of the USSR for Standards, Cryptographic Protection for Data Processing System, Gosudarstvennyi Standard of USSR, GOST 28147-89, 1989.

[18] H. M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia* 26, 2002, pp. 189–221.

[19] V. T. Hoang, P. Rogaway. On Generalized Feistel Networks. IACR Cryptology ePrint Archive, 2010:301.

[20] S. Ibrahim, M. A. Maarof. Diffusion Analysis of a Scalable Fiestel Network. *WEC* (5), 2005, pp. 98–101.

[21] S. Ibrahim, M. A. Maarof, M. S. Ngadiman. Practical Security against Differential Cryptanalysis for Extended Feistel Network. Universiti Teknologi Malaysia, 2007.

[22] L. R. Knudsen, M. J. B. Robshaw. Non-Linear Approximations in Linear Cryptanalysis. *Advances in Cryptology – EUROCRYPT '96*, *LNCS* 1070, Springer-Verlag, 1996, pp. 224–236.

[23] L. R. Knudsen, M. J. B. Robshaw. The Block Cipher Companion. Springer-Verlag, 2011. ISBN: 978-3-642-17341-7.

[24] A.G. Konheim. Computer Security and Cryptography. John Wiley & Sons Inc., New Jersey, 2007, ISBN: 978-0-471-94783-7.

[25] Xuejia Lai, James L. Massey, S. Murphy. Markov Ciphers and Differential Cryptanalysis. *Advances in Cryptology – EUROCRYPT '91*, *LNCS* 547, Springer-Verlag, 1991, pp. 17–38.

[26] S. K. Langford, M. E. Hellman. Differential-linear cryptanalysis. *Advances in Cryptology – CRYPTO '94*, *LNCS* 839, Springer-Verlag, 1994, pp. 17—25.

[27] M. Luby, C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal of Computing*, 17(2), 1988, pp. 373–386.

[28] M. Matsui. Linear cryptanalysis method of DES cipher. *Advances in Cryptology – EUROCRYPT '93*, *LNCS* 765, Springer-Verlag, 1993, pp. 386–397.

[29] M. Matsui. The first experimental cryptanalysis of the Data Encryption Standard. *Advances in Cryptology – CRYPTO '94*, *LNCS* 839, Springer-Verlag, 1994, pp. 1–11.

[30] M. Matsui. On correlation between the order of S-boxes and the strength of DES. *Advances in Cryptology – EUROCRYPT '94*, *LNCS* 950, Springer-Verlag, 1995, pp. 366–375.

[31] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997, ISBN: 0-8493-8523-7.

[32] V. Nachef. Generic attacks on Alternating Unbalanced Feistel Schemes. IACR Cryptology ePrint Archive 2009:287.

[33] V. Nachef, E. Volte1, J. Patarin. Differential Attacks on Generalized Feistel Schemes. IACR Cryptology ePrint Archive, 2011:705.

[34] J. Nakahara Jr, J. Vandewalle, B. Praneel. Diffusion Analysis of Feistel Networks. *20th Symposium on Information Theory in the Benelux*, 1999, pp. 101–108.

[35] National Institute of Standards and Technology. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46, U.S. Department of Commerce, Washington D.C., January 1977.

[36] National Institute of Standards and Technology. Announcing request for candidate algorithm nominations for the Advanced Encryption Standard (AES). U.S. Department of Commerce, available from http://csrc.nist.gov/archive/aes/pre-round1/aes_9709.htm, September 1997.

[37] National Institute of Standards and Technology. AES press release 990809: NIST Announces Encryption Standard Finalists. Available from http://csrc.nist.gov/archive/aes/round2/AESpressrelease-990809.pdf, August 1999.

[38] National Institute of Standards and Technology. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46-3, U.S. Department of Commerce, Washington D.C., October 1999.

[39] National Institute of Standards and Technology. Advanced encryption standard. Federal Information Processing Standard (FIPS), Publication 197, U.S. Department of Commerce, Washington D.C., November 2001.

[40] National Institute of Standards and Technology. Recommendation for the triple data encryption algorithm (TDEA) block cipher. Special Publication 800-67, Revision 1, January 2012.

[41] K. Nyberg. On the construction of highly nonlinear permutation. *Advances in Cryptology – EUROCRYPT '92*, *LNCS* 658, Springer-Verlag, 1993, pp. 92–98.

[42] K. Nyberg. Differentially uniform mappings for cryptography. *Advances in Cryptology – EUROCRYPT '93*, *LNCS* 765, Springer-Verlag, 1994, pp. 55–64.

[43] K. Nyberg. Linear approximation of block ciphers. *Advances in Cryptology – EUROCRYPT '94*, *LNCS* 950, Springer-Verlag, 1994, pp. 439–444.

[44] L. O'Connor. Properties of linear approximation tables. *Fast Software Encryption '94*, *LNCS* 1008, Springer-Verlag, 1995, pp. 131–136.

[45] J. Patarin. Luby-Rackoff: 7 Rounds Are Enough for $2^{n(1-\varepsilon)}$ Security. *Advances in Cryptology – CRYPTO 2003*, *LNCS* 2729, 2003, pp. 513-–529.

[46] J. Patarin, V. Nachef, C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. *Advances in Cryptology – ASIACRYPT 2006*, *LNCS* 4284, Springer-Verlag, 2006, pp. 396–411.

[47] J. Patarin, V. Nachef, C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. *Advances in Cryptology – ASIACRYPT 2007*, *LNCS* 4833, Springer-Verlag, 2007, pp. 325–341.

[48] B. Preneel, V. Rijmen, A. Bosselaers. Recent developments in the design of conventional cryptographic algorithms. Course on Computer Security and Industrial Cryptography, *State of the Art in Applied Cryptography*, LNCS 1528, Springer-Verlag, 1998, pp. 105–130.

[49] L. Reyzin. Some Notions of Entropy for Cryptography. *Information Theoretic Security - 5th International Conference (ICITS) 2011*, *LNCS* 6673, Springer-Verlag, 2011, pp. 138–142.

[50] R. L. Rivest, M. J. B. Robshaw, R. Sidney, Y. L. Yin. The RC6 block cipher. Submitted as candidate for AES, available from http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf, 1998.

[51] B. Schneier, J. Kelsey. Unbalanced Feistel Network and Block-Cipher Design. *Fast Software Encryption '96*, *LNCS* 1039, Springer-Verlag, 1996, pp. 121–144.

[52] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson. Twofish: A 128-bit block cipher. Submitted as candidate for AES, available from whttps://www.schneier.com/academic/twofish/, 1998.

[53] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27(3), July 1948, pp. 379–423.

[54] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27, October 1948, pp. 623–656, Continued from July 1948.

[55] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4), October 1949 pp. 656–715.

[56] K. Shibutani , A. Bogdanov. Towards the optimality of Feistel ciphers with substitution-permutation functions. *Designs, Codes and Cryptography*, 73(2), Springer-Verlag, 2014, pp. 667–682.

[57] T. Shirai, K. Shibutani. On Feistel Structures Using a Diffusion Switching Mechanism. *Fast Software Encryption 2006*, *LNCS* 4047, Springer-Verlag, 2006, pp. 41–56.

[58] S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. *15th Annual Symposium on Theoretical Aspects of Computer Science 1998*, *LNCS* 1373, Springer-Verlag, 1998, pp. 249–275.

[59] S. Vaudenay. Decorrelation: A Theory for Block Cipher Security. *Journal of Cryptology*, 16(4), Springer-Verlag, 2003, pp. 249-–286.

[60] H. Yap. Differential Cryptanalysis and Impossible Differential Characteristics of Extended Feistel Networks. *International Journal of u-and e-Service*, Science and Technology, 2009, 1(1), pp. 1–8.

[61] Y. Zheng, T. Matsumoto, H. Imai. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. *Advances in Cryptology – CRYPTO '89*, *LNCS* 435, Springer-Verlag, 1990, pp. 461–480.