Р Е Ц Е Н З И Я

на дисертационен труд
за придобиване на образователната и научна степен "Доктор"

по научната специалност 01.01.12 "Информатика"

Тема: Изследване на условията за линеен криптанализ в мрежи на Файстел

Автор: Роберт ЙордановЦенков

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

Рецензент: проф. д.м.н. Иван Николов Ланджев

Тема на дисертационния труд

Представеният дисертационен труд е посветен на група от криптографски задачи с много голяма практическа значимост, централната от които е задачата за оценката на сигурността на специален клас блокови шифри. Разглежданите въпроси са от изключителна важност поради широката приложимост на блоковите шифри. Тя се дължи на техните съществени характеристики като бързодействие, ефективност, надеждност, скалируемост и пр. Следа да се отбележи, че изследвания с подобна насоченост станаха публични едва в последните няколко десетилетия. Огромният интерес към блоковите шифри бе подхранен от създаването и публикуването на DES около 1970 г. Той е и най яркият представител на клас шифри, носещи името Файстелови мрежи. В опитите за атака срещу този шифър бяха развити редица общи методи за криптанализ, най-известните от които са линейния и деференциалния криптанализ. Устойчивостта срещу първия от тези методи е и обект на изследване в представения дисертационен труд.

Главна тема в настоящата дисертация е влиянието на "малки" модификации на симетрични шифри върху устойчивостта срещу линеен криптанализ. Тук може би е удачна аналогията с понятието "устойчивост" в динамичните системи: доколко "малки" промени в нелинейните компоненти на един шифър водят до малки промени в криптографската устойчивост срещу линеен криптанализ. Този въпрос е важен, доколкото създаването и изпитването на изцяло нов шифър е дълъг и изключително труден процес.

Изследването е концентрирано върху т.нар. мрежи на Файстел като за конкретен представител е избран добре известният Data Encryption Standard. Модификациите,

които са обект на изследване са специални промени в субституционните таблици (S-boxes), състоящи се във добавяне на допълзнителни линейни зависимости между битовете. Изненадващо. това не води до отслабване на разглеждания шифър.

Целите, които дисертантът си поставя в настоящия труд са следните:

1) Да се изследва промяната в характеристиките на линейно апроксимиращите таблици за блокови шифри от тип Файстелови мрежи.

2) Да се дефинират модификации на заместващите таблици и да се изследват линейните характеристики на модифицираните таблици при малък брой рундове.

3) Да се конструират и изследват многорундови характеристики на шифри с модифицираните заместващи таблици.

4) Да се разработи алгоритъм за конструиране на многорундови характеристики за разглежданите шифри.

5) Да се сравни устойчивостта срещу линеен криптанализ на шифрите с модифицирани заместващи таблици с тази на оригиналния DES.

Ще отбележа, че така поставените задачи са естествени. По правило ататките срещи DES започват с анализ на модифицирани варианти с малък брой рундове.

Литературен обзор

Общото ми впечатление е, че дисертантът познава много добре съвременното състояние на разглеждания проблем. Голяма част от изследванията му са върху един кръг от задачи и хипотези от криптографията, разглеждани като значими и имащи голяма важност за приложенията, по-специално в дизайна и анализа на блокови шифри. Дисертацията включва разработване на алгоритми, които се използват понататък за намиране на конструкции на ефективни характеристики при разнообразни ограничителни условия. С това дисертантът демонстрира познаване на областта си и възможности творчески да прилага знанията си. Дисертантът показва отлична информираност по голяма част от разглежданите проблеми.

Методика

Дисертантът използва основно комбинаторна аргумнтация и елементарни техники от преброителната комбинаторика. Голяма част от резултатите е получена в резултат на тежки компютърни пресмятания.

Съдържание и резултати на дисертационния труд

Дисертационният труд е в обем от 143 нестандартни машинописни страници и се състои от увод, пет глави, заключение, списък на използваната литература, включващ 131 заглавия и четири приложения.

По долу ще изложа накратко съдържанието на отделните глави от дисертационния труд.

Глава 1 е уводна. В нея се излагат основополагащи понятия дава се идея за симетрична и асиметрична криптография, описани са основните цели, които трябва дасе достигнат чрез прилагане на криптографски техники като поверителност, цялост, автентичност и неотказваемост (лош превод на non-repudiation). По-нататък се описва общата структура на симетричните криптографски алгоритми, общите изисквания към тях, както и общите ревими за използване на такива шифри. Изложена е най-общо криптографската теория на Шенон (раздел 1.5). Раздели 1.1–1.5 съдържат общоизвестни факти, изложени популярно и по мое мнение можеше да бъдат пропуснати. По-съдържателни и важни за по-нататъшното изложение са следващите три раздела. В раздел 1.6 са въведени първите съществени понятия и са изложени видовете криптографски атаки. В раздел 1.7 са представени най-популярните общи методи за криптанализ на блокови шифри – диференциален и линеен криптанализ. Раздел 1.8 съдържа прилично описание на общите мрежи на Файстел.

В глава 2 са въведени необходимите понятия и означения, които са повече или помалко стандартни. В раздел 2.2 е направено описание на DES, което от една страна е добре известно, но от друга е полезно за да не е нужна справка с други източници. Същественото тук започва в раздел 2.3, където се въвеждат линеини характеристики на блокови шифри. Дефинирано е понятието линеен апроксимиращ израз, като линейна връзка между някои битове на открития текст криптотекста и ключа, която се удовлетворява с някаква вероятност. В дисертационния труд това е някакво отклонение от средната честота. В идеалния случай (от гледна точка на криптографа) вероятността за удовлетворяване на такава връзка би била $1/2$ и всяко отклонение от тази вероятност увеличава ефективността на линейния апроксимиращ израз (при използването му в линеен криптанализ). В раздел 2.4 са изложени методи за пресмятане на вероятността за удовлетворяване на опредлени линейни характеристики, както и важната piling-up лема. В раздели 2.5 и 2.6 са описани общите подходи към конструиране на ефективни линейни характеристики и получаване на уравнения за битовете на ключа. Раздели 2.7 и 2.8 са посветени на общата конструкция на линейна атака срещу блоков шифър и оценка на сложността на такава атака. Тук се има предвид атака при известен открит текст като в оценката на сложността влизат като най-съществена компонента двойките открит текст-криптотекст, които трябва да са налични.

В Глава 3 са описни модификациите на които се подлага базовия DES и които са обект на изследване по-нататък в дисертационния труд. Те се свеждат до модфициране на един от изходните битове на произволно избрана заместваща таблица така, че сумата от битовете на изхода да е нечетна (това докторантът нарича “проверка по нечетност”). В раздел 3.2 са подробно описани връзките между елементите на линейните апроксимиращи таблици при вграждане на проверка по нечетност. В раздел 3.3 е разгледан случая на търсене на характеристики (линейни връзки между части от открития текст, криптотекста и ключа) при една активна заместваща таблица на

рунд. В този раздел е описан и базовия алгоритъм за търсене на най-ефективните многорундови характеристики. Доказани са някои специални релации, които са в сила при прилагане на базовия алгоритъм за търсене към DES (Теорема 3.3.2).

В Глава 4 се усложняват разглежданите трансформации като се предполага независим избор на контролните битове за произволен набор от заместващи таблици (S-boxes). При това отново обект на изследване е вариативността на ефективността на най-добрите характеристики и това доколко тя се отличава от тази на базовия алгоритъм. Тези разглеждания са ключови за конструирането на линейни атаки срещу блокови шифри, където основно изискване е натрупването на достатъчен брой ефективни линейни характеристики (съотношения). В главата са представени резултатите от изследване на оптималния избор на контролните битове, основано на анализ на линейните апроксимиращи таблици.

Глава 5 е посветена на общите свойства на линейните апроксимиращи таблици на DES. Установяват се граници за ефективността на характеристиките, т.е на отклонението от средната стойност, за най-добрите линейни характеристики за малък брой рундове. Това е необходима стъпка в линейна атака срещу Файстелов шифър. Тази стъпка е още по-оправдана заради това, че в най-новите шифри броят на рундовете е параметър, който може да бъде променян в съответствие с избора на други параметри, като дължина на блока, дължина на ключа и пр. Направен е опит за оценка на сложността на търсенето (по точно броя на итерациите) за намиране на наи-добрите характеристики при модифицирани заместващи таблици с добавена проверка по четност. Доказани са интересни твърдения, отнасящи се до оптималните двурундови характеристики (Теорема 5.5.1). Показано е, че ефективността на линейните характеристики от тип I може да бъде запазена като при тази на основния алгоритъм.

Дисертационният труд завършва с четири приложения. В Приложение А е представена линайната апроксимираща таблица за първата заместваща кутия на модифицирания алгоритъм. Приложение Б е особено интересно. В него се съдържат най-добрите многорундови характерситики, получени при модификация на един бит в изхода на всички заместващи таблици. Допълнителни сведения за наи-добрите апроксимиращи изрази за 16-рунда са дадени в Приложение В. Приложение Г съдържа сведения за сложността на търсенето, зададено като брой рекурсивни извиквания.

Приноси на дисертационния труд

По мое мнение по-важните приноси в дисертационния труд се свеждат до следното:

(1) Изследвана е ефективността на промените в т.нар. линейни апроксимиращи таблици при модификация на заместващите таблици на един блоков шифър. Модификациите се състоят във внасяне на допълнителна линейна зависимост на изхода на заместващите таблици.

(2) Доказано е, че внасянето на допълнителни линейни зависимости не увеличава

задължително ефективността на най-добрите линейни характеристики.

(3) Разработен е алгоритъм за търсене на ефективни линейни характеристики на шифри от тип мрежа на Файстел.

(4) Намерени са ефективни линейни характеристики за двурундов модифициран DES.

(5) Изследвана е ролята на т.нар. инвариантни елементи в линейните апроксимиращи таблици.

(6) Изследвана е възможността за конструиране на линейна атака срещу блокови шифри от тип Файстел.

Забележки по дисертационния труд

Във връзка с дисертационния труд имам следните забележки:

(1) Струва ми се, че глава 1 е ненужно разширена. Описани са популярно общоизвестни факти повечето от които са ненужни за по-нататъшното изложение.

(2) На стр. 21: Не ми харесва обяснението на симетричните криптосистеми. Докторантът пише: "характерна особеност е, че всяка двойка ключове има единствен собственик." Не може да се дефинира криптосотема през начина ѝ за използване. Една асиметрична криптосистема може да се използва като симетрична (т.е. да се скрие ключа за шифриране), но от това тя не става симетрична.

(3) На няколко места се споменава за "първия метод за криптанализ на DES". Доколкото знам не съществува метод за криптанализ на DES, който да е по-ефективен от пълно изчерпване на половината ключове, т.е. 2^{55} проверки. Диференциалният криптанализ е по-ефективни от пълното изчерпване върху DES с по-малък брой рундове, докато линейният криптанализ изисква огромно количество двойки блокове открит текст-криптотекст, шифрирани с един и същи ключ.

(4) Номерацията в дисертационния труд е объркваща. Така например имаме Теорема 3.2.1 и Следствие 3.2.1. По-добре е да имаме единна номерация за всички твърдения (теореми, леми и следствия).

(5) Дисертационният труд изследва устойчивостта на Файстелови шифри при линейни модификации на техни компоненти. Демонстрирано е, че внасянето на допълнителни линейни зависимости не променя устойчивостта на разглежданите шифри срещу линеен криптанализ. Моето усещане е, че получените изводи се отнасят само до DES и варианти на DES. Вярно ли е това.

(6) На стр. 143, таблица Г.1: По каква причина броят итерации е представен в 16-ичен вид.

Публикации по дисертационния труд

Резултатите от дисертационния труд са публикувани в 3 статии. Две от статиите са излезли от печат в Lecture Notes in Computer Science на Springer, както и в сборника с доклади на международната конференция Algebraic and Combinatorial Coding Theory. Третата работа е приета за печат в Cybernetics and Information Technologies. Известно ми е, че към настоящия момент е приета за печат и четвърта работа с резултати от дисертационния труд – в Electronic Notes in Discrete Mathematics на Elsevier.

Авторство на получените резултати

От представените публикации две са с по двама съавтори и една е с един съвтор. Тъй като познавам научните интереси на докторанта и следя работата му в последните години, за мен няма съмнение, че приносът му е равностоен с този на останалите автори.

Цитирания на публикациите от дисертационния труд

Докторантът не е приложил списък с цитирания на статиите, в които са публикувани резултатите от дисертационния труд. Не са ми известни цитирания на статии на докторанта.

Автореферат и авторска справка

Авторефератът и авторската справка са направени съгласно изискванията и отразяват правилно резултатите и приносите в дисертационния труд.

Заключение

Дисертационният труд е посветен на криптографски проблеми, които са с имащи голямо практическо значение за конструирането и оценяването на сигурни криптографски примитиви. Направено е изследване на поведението на Файстелови мрежи при модифициране на заместващите таблици чрез внасяне на допълнителна линейност. При това направените изводи играят роля както при дизайна на нови шифри, така и при криптанализа на вече съществуващи шифри. Считам, че с това е постигнат напредък в една актуална област на криптографията.

Представеният дисертационен труд “Изследване на условията за линеен криптанализ в мрежи на Файстел” с автор Роберт Йорданов Ценков съдържа оригинални резултати, които представляват принос в криптографията. Докторантът показва задълбочени познания в областта на изследването на Файстелови мрежи, както и по-общо в конструирането и криптанализа на блокови шифри, Считам, че с това той отговаря на изискванията на “Закона за развитие на академичния състав в Република България”, както и на Првилника за условията и реда за придобибане на научни степени и заемане на академични длъжности, за придобиване на научната степен степен

“Доктор”. Гореизложеното ми дава основание да дам положителна оценка на представения дисертационен труд на и да препоръчам на Уважаемото Жури да присъди на Роберт Йорданов Ценков образователната и научна степен “Доктор”.

София, 23.01.2017 г.

Рецензент:

(проф. д.м.н. Иван Ланджев)