Р Е Ц Е Н З И Я

на дисертационен труд за получаване на научната и образователна степен „доктор“ в област на висшето образование 4. Природни науки, математика и информатика, професионално направление: 4.6. Информатика и компютърни науки, научна специалност 01.01.12 „Информатика“

Автор на дисертационния труд: Роберт Йорданов Ценков
Тема на дисертационния труд: „Изследване на условията за линеен криптоанализ в мрежи на Файстел“
Научни консултанти: проф. дмн Петър Бойваленков, доц. д-р Юри Борисов
Рецензент: проф. д-р Красимир Неделчев Манев

Тази рецензия е написана и представена на основание на Заповед № 298 от 31.10.2016 г. на директора на ИМИ, БАН, както и на решение на назначеното със Заповедта Научно жури по процедурата (Протокол 1 от 09.11.2016 г.). и е изготвена във основа на ЗРАСРБ, Правилника за прилагане на ЗРАСРБ, Правилника за развитие на академичния състав на БАН и на ИМИ при БАН.

1. Общо описание на дисертацията другите материали

Дисертационният труд е с обем 143 страници (35 реда и 70 знака на ред) и се състои от 116 страници основен текст, 13 страници цитирана в текста литература (общо 131 заглавия) и 14 страници приложения. Като неотменна част от работата разглеждаме също и представените Автореферат и копия на публикациите по дисертацията.

Основният текст започва с обичайните списъци на таблиците и фигурите. Неизвестно защо, според Съдържанието, на стр. 9 трябва да има *Списък на използваните съкращения и означения*, но такъв списък на стр. 9 няма – има *Списък на означенията*, но той е на друго място в текста. Изложението е разделено на Увод, 5 глави и Заключение. Като отделни елементи на Заключението са дадени Списъкът на публикациите по дисертацията, апробация на резултатите, Декларация за оригиналност и Благодарности.

Оформлението на работата е добро, типично за използваната система за текстообработка LATEX.

2. Актуалност на разработения в дисертационния труд проблем

Тематиката на която е посветен дисертационният труд е актуална. Защитата от нежелан достъп на данните, намиращи се в компютри, свързани в компютърни мрежи, включително и такива с поверителен характер (от гледна точка на личната, фирмената или националната сигурност), е ежедневна и неотменна задача, предвид непрекъснатия интерес на заинтересовани лица и организации да получат достъп до защитените данни. Затова разработването

на нови, по-надеждни техники за защита на данните, както и подобряването на съществуващите, е от особена важност. Един от важните проблеми в областта е намаляване на податливостта на класически линеен криптоанализ на много популярните итерационни шифри (и по специално мрежи на Файстел, като DES, например) и нуждата от повишаване надеждността на участващите в алгоритъмите *заместващи* (предпочитам да използвам тази дума вместо авторовото *заместителни*) таблици (накратко ЗТ или S-кутии).

3. Познава ли дисертантът съвременното състояние на областта?

От обширното представяне, в първа и втора глава, на свързаната със задачата теория – понятиен апарат и математически резултати, имащи отношение към поставената задача, можем да заключим, че докторантът познава отлично научната област на дисертационния труд. Това ни заключение се потвърждава и от списъка на използваната литература, която наброява 131 заглавия. От тези публикации, 76 са излезли от печат след 2000, а 27 – след 2010 година. Затова смятаме, че използваната литература отразява съвременното състояние на областта.

4. Съдържателен анализ на дисертационния труд

В **Уводът,** след кратка аргументация за актуалността на проблема е представена мотивацията на работата – все още недоизяснената податливост на симетричните итерационни шифри (и по-точно мрежи на Файстел) на линеен криптоанализ. Формулирана е целта на работата – да се изследва влиянието на определен вид модификации в алгоритмите (от тип „добавяне на линейност“) върху податливостта на линеен анализ. За постигане на целта са формулирани 7 конкретни задачи. В края на това въведение е представена накратко методологията на изследването и съдържанието на останалите глави на дисертацията.

Първа глава на работата е обзорна за науката за криптиране като като цяло, започвайки от деленето ѝ на криптография и криптоанализ и завършвайки с криптографския подход, който е основен за работата – мрежите на Файстел. Не мога да се съглася с названието на раздел 1.3. „Криптографски механизми“, в който по същество се изреждат различните **предназначения** или **цели (**защо авторът ги нарича „свойства“?) на криптографията, като осигуряване на поверителност, цялостност, автентичност и т.н., а за механизми само се споменава без да се посочи поне един, за да се разбере какво има предвид авторът.

Неудачно според нас е представянето на мрежите на Файстел чак в последния Раздел 1.8 на главата, при условие, че в някои от предните раздели се коментират характеристики или свойства на тези мрежи. Не спомагат за по-доброто възприемане на работата и изрежданията на недефинирани понятия

(виж например абзаците с булети на стр. 25). Така и не става ясно, например, как изредените без дефиниране „режими“ влияят на „структурата на крипто-графските алгоритми“. Защо трябва да се спомене списъкът от абревиатури в края на раздел 1.5, след като пестеливото им „разшифроване“ е в следващия раздел. Като цяло, главата оставя впечатление за несистематизирано и, на места, непълно изложение.

Глава втора започва с Раздел с възприетите от автора означения (който, според Съдържанието, би трябвало да бъде в справочния блок преди Увода). Главата е по-подробно въведение в същността на работата – линейния криптоанализ в мрежи на Файстел, на примера на DES. След кратко представяне на алгоритъма DES се въвеждат понятията линеен апроксимиращ израз и линейна характеристика (или линейна апроксимация, или линейно приближение). Оставаме с впечатление че с последните три понятия се нарича един и същ вид обекти, макар, че това не личи ясно от текста. Обсъждат се подходите за построяване на линейни характеристики и планиране на линейни атаки на шифъра. От текста не става ясно, как точно се определят един или повече бита на шифъра, което е важно за тази глава.

В **Глава трета** започва изложението на резултатите на докторанта. Описан е първият от трите експеримента, които са същност на дисертацията. Той се състои в замяна на един бит във всяка S-кутия (всички заменени битове са в една и съща позиция) на DES с бит за проверка на четност. Доказани са съответни теореми, които позволяват лесно да се получат линейните апроксимиращи таблиции (ЛАТ) за S-кутиите (основен обект на изследването в тази и следващите глави) при модифицирания алгоритъм. След това се повтарят стъпките на класическия линеен криптоанализ на Мацуи за получения алгоритъм, за всяка от четирите възможни позиции на модифицирания бит, като в края се сравняват помежду си качествата на двата типа характеристики (по Мацуи), получени след модификацията – от тип I (с не повече от една заместваща кутия на руд) и от тип II (с итериране на двурундови характеристики).

За целите на построяване на линейни характеристики на модифицирания метод авторът е разработил т.н. от него Базов алгоритъм за търсене (БАТ). Алгоритъмът, от тип backtracking, е описан по доста необичаен начин и трудно може да се проследи работата му – няколко пъти се среща указанието „тогава се върни“, без да личи точката за връщане. Добра характеристика на алгоритъма е че е приложим за произволна схема на Файстел и това оправдава наименованието на дисертационния труд. За целите на изследването на модифицирания DES, алгоритъмът е допълнен с упростяващи работата стъпки, чрез доказани от автора свойства.

От направените изследвания се вижда, че построяването на характеристики от тип I не намалява по-никакъв начин надеждноста на модифицирания алгоритъм, докато при характеристиките от тип II, това не е така. При влошената, като цяло, картина при характеристиките от тип II е интересно че в отделни случаи, би могло до се получи и подобрение при характеристика от тип II. Не е ясно защо са избрани за по-подробно представяне в края на главата точно 16-рундовите и 19-рундовите характеристики.

Основното ми възражение тук е, че без да се познават работите на Мацуи не може да се разбере какво общо имат ефективностите на линейните характеристики със стойностите в ЛАТ, дефиницията на които е доста далеч от дефиницията на линейна характеристика. Тази връзка е много съществена за работата и би трябвало да бъде представена детайлно.

Глава четвърта продължава започнатото в глава трета, като вторият експеримент е свързан с изследване на модификации на DES, при които се замества по един бит в изхода на всяка S-кутия, без заместваните битове да са в една и съща позиция. При това положение задачата е била да се изследват различните комбинации от позиции, в които ще стане заместването. Въведено е понятието инвариантен елемент на ЛАТ, но не става ясно с какво това понятие подпомага изследването. С изчерпващо търсене са определени оптималните характеристики за всяка комбинация от стойности на модифициращите 8 маски. Основните резултати са от пряко наблюдение на стойностите в две ЛАТ – S_7 и S_8 – при направените модификации. Може би останалите таблици да нямат отношение към оптималността на построяваните характеристики в този случай, но това не е казано в явен вид.

Общото заключение от работата в това направление е, че модификациите с въвеждане на бит по четност на произволни позиции в различните кутии не намалява по никакъв начин защитните свойства на DES, но и не носи съществено усилване на защитните свойства, освен в редки случаи.

Глава 5 е посветена на третия експеримент, при който въведената допълнителна линейност е произволна афинна трансформация на изходните битове на всяка кутия – различна за различните кутии. Такова обобщение е естествено, тъй като заместванията на единични битове с контрол на четност са крайни частни случаи на афинни трансформации. И тук е проведено изследването на измененията в устаочивостта на получения шифър в стил Мацуи, но само за характеристики на не много рундове. Използван е апарат от линейната алгебра, който може би не позволява ръчно изследване на многорундовите характеристики. Така е установено че ефективността на характеристиките при малък брой рундове в този случай се запазва.

В **Приложение А** са публикувани четирите модифицирани ЛАТ на DES кутията S_1. Струва ми се, че много по уместно би било да се публикуват

таблиците за някоя от кутиите S_7 или S_8, които са пряко използвани в доказателствата на теореми в Глава 4. Резултатите от изследванията в Глава 3, които са и най-стойностната част от работата, са представени в **Приложение Б**. За всяка от възможните проверки по четност са представени намерените оптимални многорундови характеристики за брой рундове от 3 до 20. В **Приложение В** специално внимание е отделено отново на получените 16-рундови характеристики от Глава 3, като са разгледани две от намерените от автора такива характеристики и са преценени възможностите да се атакува ключа стяхна помощ. Остава открит въпроса с какво тези характеристики привличат вниманието на докторанта. В **Приложение Г** е дадена своеобразна оценка за сложността на БАТ от глава 3. Доколкото това е сложна рекурсивна процедура оценката е емпирична, като са проследявани и регистрирани броят на рекурсивните извиквания – възможна мярка за сложността на алгоритъма. Защо получените резултати са в шестнадесетичен вид е неясно.

5.Приноси на дисертационния труд

1. Докторантът се е запознал в подробности с техниката на линейния криптоанализ на Мацуи за Файстелови шифри и по-специално за DES.
2. Предложени са три вида линейни модификации на класическия алгоритъм – със заместване на един и същ бит във всички S-кутии с бит с проверка на четност; със заместване на различни битове в различните S-кутии с бит с проверка на четност; различни афинни трансформации на изходите на различните кутии.
3. За всяка от предложените модификации е приложена техниката на линейния криптоанализ, като са търсени главно два вида характеристики – многорундови с по една S-кутия на рунд (тип I по Мацуи) и комбинации от двурундови характеристики, една от които с тривиална, като са оценявани промените в устойчивостта на шифъра при съответните модификации. Там където техниката не е позволила извличането на характеристики за голям брой рундове да извлечени характеристики за малък брой рундове.
4. Детайлно е изследван случая с многорундовите характеристики (тип I) при модификация на един и същ бит с разработен от автора софтуер. Намерни са оптималните линейни характеристики за различните позиции на бита за проверка по четност. Емпиричната оценка за сложността на алгоритъма показва работоспособността му при търсене на линейни характеристики в разумно време.
5. В останалите случай резултати са получени с наблюдения в модифицираните ЛАТ и доказване на съответни твърдения за свойствата им.
6. Показано е как добавената линейност на изходите на DES поражда нов вид двурундови итерационни характеристикипри коиито може дасе достигне ефективността, по-ниска от тази, достижима чрез нулеви входни маски.

6. Критични бележки

Забелязаните в текста неточности и неясноти са предоставени на докторанта в отделен документ. Към работата имаме следните по-сериозни критични забележки:

- ключова за работата е връзката между ефективността на линейните характеристики и стойностите в ЛАТ, а тази връзка не е представена детайлно в работата;
- трудно е да приемем като Теореми твърдения, които са резултат от наблюдения в конкретна ЛАТ или в дефиниицията на конкретна S-кутия;
- текстът не съдържа нито пълно описание на S-кутиите на DES, нито ЛАТ на базата на които са изведени съответни твърдения.

7. Преценка на публикациите по дисертационния труд.

По дисертацията има 3 публикации. Работата под номер 3 е публикувана в списанието Cybernetics and Information Technologies (издание на ИИКТ на БАН, с международна редакционна колегия). Работата под номер 1 е доклад на международна конференция и е измежду избраните за публикуване в тома на конференцията, издаден от Springer след сериозно рецензиране (12 от 27). Работата под номер 1 е публикувана в сборник доклади на реномирана международна конференция у нас. Затова можем да заключим че и трите публикации са рецензирани и изискването на Правилника е изпълнено. Самостоятелни работи докторантът няма. В две от публикациите съавтори са научните му консултанти, а в третата един от тях. Не забелязваме някакво правило при подреждането на съавторите. Това ни дава основание да предположим, че приносът на докторанта е поне равностоен.

Резултатите са докладвани на Семинар в ИМИ на БАН, на национални и международни конференции. Не ни е известно работите на докторанта да са цитирани. В заключение, публикациите достатъчно добре отразяват съдържанието на дисертационния труд и са получили публичността и признанието, необходими за положителна оценка на дисертацията.

8. Авторефератът е изготвен в съответствие с изискванията на Правилника за условията и реда за придобиване на научни степени и за заемане на научни длъжности на ИМИ–БАН, като отразява изчерпателно и точно съдържанието на дисертационния труд и приносите.

9. Не познавам докторанта лично.

10. Заключение. Поставената пред докторанта задача е изпълнена успешно. Изследвана е достатъчно пълно устойчивостта на DES при различните възможности за добавяне на нелинейност на изхода на S-кутиите. Разработената техника може дасе приложи успешно към всеки шифър оттип

схема на Файстел. Като имам предвид това, независимо от направените забележки, смятам че представеният дисертационен труд отговаря на изискванията на ЗРАСРБ, Правилника за прилагане на ЗРАСРБ, Правилника за развитие на академичния състав на БАН и на ИМИ при БАН, и му давам положителна оценка. Предлагам на уважаваното Жури да присъди на Роберт Йорданов Ценков научната и образователна степен "Доктор" в област на висшето образование 4. Природни науки, математика и информатика, професионално направление: 4.6. Информатика и компютърни науки, научна специалност 01.01.12 „Информатика”

София, 15.01.2017 г. Рецензент:

проф. д-р Красимир Манев