С Т А Н О В И Щ Е

върху дисертационен труд

Изследване на Условията за Линеен Криптоанализ в Мрежи на Файстел

за придобиване на образователната и научна степен „доктор“.

Област на висше образование: 4. Природни науки, математика и информатика.

Професионално направление: 4.6 Информатика и компютърни науки.

Автор: Роберт Йорданов Ценков

докторант на самостоятелна подготовка, отчислен с право на защита по научна специалност 01.01.12 Информатика към секция „Математически Основи на Информатиката“ на Институт по Математика и Информатика при БАН

от: доц. д-р Юри Любчов Борисов, ИМИ при БАН

Становището е изготвено на основание заповед № 298 от 31.10.2016 г. на Директора на ИМИ при БАН и решението на научното жури, прието на заседание проведено на 17.10.2016 г..

1. Биографични данни

Роберт Йорданов Ценков е роден на 07.01.1966 г. в с. Селановци, област Враца. Завършва МГ „Акад. Иван Ценов" Враца през 1984 г. и ФМИ на СУ „Св. Климент Охридски " през 1991 г.. От 1994 до 1995 г. е бил задочен докторант в катедра „Вероятности и Статистика" във ФМИ на СУ „Св. Климент Охридски ", по темата „Бейсови подходи в статистическия контрол на качеството и надеждността " , отчислен с право на защита.

В периода 1989 – 1994 г. работи като хоноруван асистент по „Теория на Вероятностите и Математическа Статистика" във ФМИ на СУ „Св. Климент Охридски ".

Работи последователно като експерт по защитени комуникации в МВР в периода 1994 – 1999 г., специалист по организация и изпълнение на проекти в областта на рекламата във фирмите „ГРАФЛИН-ООД" София (1999 - 2003) и „S TEAM IDEAS GROUP" София (2004), и отново като експерт по защитени комуникации в МВР в периода 2004 – 2008 г. и в ДАНС от 2008 г. до момента.

2. Данни за докторантурата

Роберт Ценков е зачислен в докторантура на самостоятелна подготовка по научната специалност 01.01.12 „Информатика" в ИМИ при БАН считано от 17.12.2012 г. и срок на обучение 3 години, съгласно заповед № 1329/19.12.2012 г. на Директора на ИМИ. Положил е успешно предвидените в работната програма изпити и докторантски минимуми. Отчислен е с право на защита съгласно заповед . № 789/16.12.2015 г. на Директора на ИМИ. Предзащитата е проведена на 17.10.2016 г. в ИМИ. Представените от Роберт Ценков документи са в съответствие с Правилника за условията и реда за придобиване на научни степени и за заемане на академични

длъжности в БАН и съответния правилник в ИМИ при БАН. Те съдържат необходимата информация за оценяване на дисертационния труд.

3. Данни за дисертацията и автореферата

Дисертацията е в обем от 143 стр.. Основните й части са Автореферат, Списък на публикациите по дисертацията, увод, пет глави, заключение, използвана литература с 131 заглавия и четири приложения.

Без всякакво съмнение в съвременния свят на електронни комуникации защитата на информацията е от решаващо значение за функциониране на обществото. Когато информацията е представена във „формализиран запис", науката криптография има водеща и в много случаи решаваща роля за реализиране на нейната защита. Още от самото възникване на тази наука паралелно се развиват и методите на така наречения криптанализ, които отразяват усилията за преодоляване на криптографските средства с цел нерагламентиран достъп. От друга страна развитието на криптоанализа сам за себе си също способства за построяване на все по-сигурни криптографски примитиви и протоколи. В началото на 90-те години на отминалия век в публичното пространство се появяват две основни техники за атака на модерните симетрични блокови шифри – диференциалния и линейния криптоанализ. Постепенно, тези техники придобиват голяма популярност сред академичните среди така, че днес един от първите въпроси на които всяко ново предложение за блоков криптографски алгоритъм трябва да отговори е дали то е устойчиво на тях. Дисертацията е посветена на един аспект на линейния криптоанализ спрямо шифрите от тип мрежа на Файстел, който доколкото ни е известно не дискутиран широко в литературата. А именно, познавайки ролята на така

наречените S-боксове за осигуряване на „нелинейност” в съответния шифър, до каква степен въвеждането на „минимален брой” допълнителни линейни връзки в изходите им, ще доведе до улесняване на съответния критоанализ. Още повече, че модификации от този сорт дават възможност да се детектира „разваляне то” на криптограмите при възникване на грешки в процеса на създаването им. Освен това, както отбелязва дисертантът, подобни модификации имат своето място при проектиране на така наречените скалируеми шифри, които предоставят механизъм на работа с различни стойности на параметрите на алгоритъма.

По-долу даваме в резюме съдържанието на 5-те глави на дисертацията.

Първа глава има въвеждащ характер. Даден е обзор на съвременните концепции в криптографията и криптоанализа като ударението е поставено върху метода на линейния криптанализ и шифрите от тип мрежа на Файстел.

Втората глава съдържа необходимите предварителни знания като дефиниции, стандартни означения, техники и предишни резултати насочени директно към проведените изследвания в дисертационния труд.

В трета глава най-напред е дефиниран основния обект на изследванията, а именно DES–подобна криптосистема в изходите на S-боксовете, на която са вградени проверки за контрол по четност. След това последователно е описан разработения основен алгоритъм за търсене на най-добри линейни характеристики, резултатите от проведеното експериментално изследване със съответния софтуер на модификация с фиксирана позиция на проверката по четност, както и анализ на резултатите.

В четвърта глава, след като въвежда разширена фамилия от DES–подобни криптосистеми, за които позицията на контрола по четност във всеки S-бокс се избира независимо от тези на останалите, дисертантът провежда аналогичното изследване на това от

предишната глава. В допълнение там се намират границите на вариация на ефективността на най-добрите характеристики при различен брой итерации. Освен това се установяват удобни и приложими критерии за оценяване на ефекта от предложената модификация на шифъра върху сложността на метода на линейния криптоанализ.
В последната глава (чрез въвеждане на афинни трансформации върху изходите на S-боксовете) се разглеждат обобщения на съответните шифри и резултати от предишните две глави.

Авторефератът е в обем от 40 стр. и правилно отразява приносите на дисертанта.

4. Публикации по темата на дисертацията и участия в научни форуми

Резултатите от дисертацията са излезли в 3 публикации. В две от тях дисертантът има двама съавтори, а в третата един.

Две от тези публикации са доклади от конференции (BalkanCryptSec 2015 в Словения и ACCT 2016 у нас), а останалата е в списанието *Cybernetics and Information Technologies. Изданието Lecture Notes in Computer Sciences*, където е публикувана статията от BalkanCryptSec 2015 има SJR-ранг 0.252, а списанието има SJR-ранг 0.170 за 2015 г..

Част от резултатите са докладвани на Националния семинар по Теория на Кодирането „Проф. Стефан Додунеков", В. Търново, 2014.

Дисертантът направи и кратко изложение на част от резултатите получени до момента на Rump- сесията на проведения в София EUROCRYPT 2015.

5. Научни приноси

Основните приноси на дисертацията са:

1. Разработен е алгоритъм за намиране на най-добри многорундови линейни характеристики в клас шифри от тип мрежа на Файстел;

2. Използвайки съответния софтуер е извършено експериментално изследване на ефекта, който оказва върху метода на линейния криптоанализ (в духа на M. Matsui) въвеждането на допълнителни линейни зависимости в изходите на S-боксовете на алгоритъма за криптиране DES. Освен това, но теоретично (без помощта на компютър) е проведено изследване имащо същите цели, когато броя на рундовете в алгоритмите от въпросната фамилия е малък (до 3 рунда).

3. Изводите, които можем да направим от изследванията описани в настоящата дисертация са, че (противно на очакваното и общоприето мнение) модификациите от разглеждания вид не водят непременно до подобряване на условията за прилагане на линеен криптоанализ. Като цяло, тези изследвания показват още, че методът на линейния криптоанализ не винаги е достатъчно ефективен, макар че в определени случаи е най-оптималния известен (например при автентичния DES и сценарий на атака с известен открит текст).

6. Заключение

Представеният дисертационен труд е в съответствие с изискванията на Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в Института по Математика и Информатика при БАН за получаване на образователната и научна степен „доктор“.

Получените резултати и публикуваните статии ми дават основание да подкрепя придобиването на образователната и научна степен „доктор“ от Роберт Йорданов Ценков в професионално направление 4.6 Информатика и компютърни науки.

06.01.2017 г. Юри Борисов: