СТАНОВИЩЕ

за дисертационен труд
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,
секция „Математически основи на информатиката”,
Институт по математика и информатика – БАН

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

Изготвил становището: проф. дмн Стефка Христова Буюклиева,
факултет „Математика и информатика”,
ВТУ ”Св. Св. Кирил и Методий”

Становището е изготвено на основание заповед № 298/31.10.2016 г. на Директора на ИМИ при БАН и решенията от първото заседание на научното жури, проведено на 11.11.2016 г.

1. Данни за дисертанта.

Роберт Ценков е роден на 7.01.1966 г. в с. Селановци, обл. Враца. През 1991 г. завършва ФМИ на СУ „Св. Климент Охридски”, специалност „Математика”, специалнизация „Вероятности и статистика”. В периода 1992–1995 г. е редовен докторант в СУ по спец. „Вероятности и статистика”, откъдето е отчислен с право на защита. Работил е като хоноруван асистент по „Вероятности и статистика” във ФМИ на СУ „Св. Климент Охридски” от 1989 до 1994 г. В периода 1994-1999 г. работи като експерт по защитени комуникации към МВР, от 1999 до 2004 работи в частни фирми, а от 2004 г. е експерт по защитени комуникации в ДАНС.

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., със срок

на обучение 3 години. По време на обучението са положени успешно необходимите изпити и докторантски минимуми. Със заповед № 789/16.12.2015 г. на Директора на ИМИ е отчислен с право на защита. Предварителната защита на дисертацията е проведена на 17.10.2016 г. в ИМИ. Роберт Ценков е представил всички необходими документи съгласно Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в БАН и аналогичния правилник в ИМИ на БАН.

3. Данни за дисертацията и автореферата.

Дисертацията е в обем от 143 страници и е структурирана както следва: Списък на фугурите, Списък на таблиците, Списък на използвани съкращения и означения, Увод, пет глави, Заключение, Литература (включваща 131 заглавия, всички на английски език) и четири приложения. Актуалността на темата на дисертацията е безспорна – мрежите на Файстел са сред основните обекти на изследване в криптографията и всеки нов резултат за техните свойства би допринесъл за усъвършенстването им и тяхното приложение в различни криптосистеми.

В първа глава от дисертацията се дава общ преглед на съвременните концепции в криптографията и криптанализа, като се обръща специално внимание на шифрите със структура от тип мрежа на Файстел, а също и на линейния криптоанализ. Втора глава съдържа описание на основните понятия, дефиниции, техники и резултати, свързани с изследванията на дисертационния труд. В трета глава е представена основната концепция за въвеждане на допълнителна линейност в структурата на един шифър чрез контрол по четност в изходите на заместителните таблици (S-boxes). Разгледани са и основните техники, използвани за търсене и анализ на най-добри линейни характеристики. Представен и анализиран е базов алгоритъм за търсене (БАТ). В четвърта глава въвеждането на контрол по четност се разглежда в широк кръг от трансформации, предлагащи независим избор на позиции за контролните битове за различните субституционни кутии, представят се граници за ефективността на някои характеристики при различен брой рундове и други. Преобразуванията, в които контролът по четност е част от най-общо зададена афинна трансформация, са разгледани в пета глава. Дадени са общите свойства на линейно апроксимиращите таблици за S-кутиите в този случай и са установени граници за ефективността на някои линейни характеристики за малък брой рундове. В заключението са направени обобщени изводи от получените резултати и е добавена информация за апробирането им.

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

4. Публикации по темата на дисертацията.

Роберт Ценков е представил 3 публикации по темата на дисертацията, две от които са в сборници от конференции. И трите статии са на английски език. Две от статиите са в съавторство с двамата консултанти на докторанта – проф. Петър Бойваленков и доц. Юри Борисов, а третата, само с доц. Юри Борисов. Публикациите са:

- № 1 е доклад на втората международната конференция Cryptography and Information Security in the Balkans - BalkanCryptSec 2015, Словения. Избрани след рецензиране доклади от конференцията са публикувани в сборник от поредицата *Lecture Notes in Computer Sciences*, издаден от издателство Springer под редакцията на Enes Pasalic и Lars Knudsen. *Lecture Notes in Computer Sciences* има SJR-ранг 0.252 за 2015 г.
- № 2 е доклад на международната конференция *International Workshop on Algebraic and Combinatorial Coding Theory*, 2016, Албена.
- № 3 е статия, приета за публикуване в *Cybernetics and Information Technologies*. Списанието има SJR-ранг 0.170 за 2015 г.

Изискванията за минимален брой и вид публикации (чл. 6 от гл. IV на правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в ИМИ на БАН) са изпълнени.

Освен на посочените конференции, резултати от дисертацията са докладвани и на:

- Националния семинар по теория на кодирането „Проф. Стефан Додунеков”, Велико Търново, 2014 г.;
- 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques „Advances in Cryptology - EUROCRYPT 2015”, София, 2015.

5. Научни приноси

Основните приноси в дисертацията според автора са представени в авторската справка, включена в автореферата. Тези приноси са систематизирани в 7 точки. По-важните от тях според мен са:

- Изследван е механизмът на влияние на допълнителни линейни зависимости на изхода на субституционните кутии на блоков шифър върху свойствата на техните линейно апроксимиращи таблици (ЛАТ), както и върху механизмите за конструкция на многорундови линейни характеристики за него.

- Резултатите от изследванията опровергават очакването за влошаване на устойчивостта на блоков шифър при наличие на повече линейни зависимости. Ефектът от модификацията съществено зависи от мястото на въвеждане на допълнителни зависимости и от конкретните компоненти на шифъра.
- Разработен е алгоритъм за търсене на многорундови линейни характеристики на Файстел шифри.

Считам, че представените от автора приносни моменти са коректни и основателни.

6. Критични бележки и препоръки

Уводът и Глава 1 се четат леко и дават много добра представа за съдържанието на дисертацията, задачите, които си поставя авторът с това изследване, и методите, които използва. Глава 2 продължава в същия (леко литературен) стил, като по този начин представя основните понятия и твърдения малко повърхностно и не достатъчно ясно. Следващите глави представят по-стегнато математически основните идеи, подходи и резултати. Текстът е изпъстрен с фигури и таблици. Много добро впечатление ми направи и описанието на алгоритъма от стр. 64-65 (с псевдокод на български).

Основната ми критична бележка е свързана с малкия брой публикации, макар причините да са ясни за мен.

7. Заключение

Считам, че представеният дисертационен труд отговаря на изискванията на Закона за развитие на академичния състав в Република България. Постигнатите резултати ми дават основание да предложа да бъде придобита научната степен „Доктор" от Роберт Йорданов Ценков в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6. Информатика и компютърни науки.

11.01.2016 г.

Подпис:
/проф.дмн Стефка Буюклиева /