С Т А Н О В И Щ Е

на дисертационен труд

New Heuristic Methods for Generation of Bijective S-boxes with Good Cryptographic Properties

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: Георги Велков Иванов

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, БАН

от доц. дмн Емил Миланов Колев,
Институт по математика и информатика, БАН

Становището е изготвено на основание заповед номер 282 от 07.10.2016 г. на Директора на ИМИ при БАН и решение на научното жури, прието на заседание, проведено на 14.10.2016 г.

1. Биографични дании

Георги Велков Иванов е роден на 7.05.1976 г. в гр. София. Завършва НПМГ „Акад. Любомир Чакалов“ през 1994 г. и ФМИ на СУ „Св. Климент Охридски“ през 1999 г.

През 1999 - 2000 г. работи като асистент по „Математическо оптимиране“ във ФМИ на СУ „Св. Климент Охридски“.

Работи последователно в „Дирекция защита средствата за връзка“ към МВР (през периода 2001 - 2008 г.) и в „Орган по криптографска сигурност“ към ДАНС (от 2008 г. до сега).

2. Данни за докторантурата

Георги Иванов 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 със срок на обучение 3 години, съгласно заповед 1342/20.12.2012 г. на Директора на ИМИ. Положил е успешно предвидените в работната програма изпити и докторантски минимуми. Отчислен е с право на защита със заповед номер 788 от 16.12.2015 г. на Директора на ИМИ. Предзащитата е проведена на 14.09.2016 г. в ИМИ. Представените от Георги Иванов документи са в съответствие с 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. Те съдържат необходимата информация за оценяване на дисертационния труд.

3. Данни за дисертацията и автореферата

Дисертацията е написана на английски език и е в обем от 129 стр. Основните части на дисертационния труд са Резюме, Списък на публикациите по дисертацията, увод, пет глави, заключение и използвана литература с 94 заглавия.

В съвременния свят на електронни комуникации защитата на предаваната информация е от решаващо значение за функционирането на банки, правителства и на обществото като цяло. Биективните заместителни таблици (или S-боксове) са един от важните елементи на всеки блоков шифър. От техните криптографски характеристики до голяма степен зависи сигурността на използвания шифър. Ето защо конструирането на биективни заместителни таблици с добри криптографски свойства е една изключително актуална задача. Дисертацията е посветена на конструиране на заместителни таблици с използване на евристични методи. Получените по този начин таблици (поради случайния им характер) се отличават с по-сложна структура и са приложими в практически шифри.

Първа глава от дисертацията има въвеждащ характер. В нея са представени основните цели на дисертацията и са коментирани постигнатите резултати.

Във втора глава са въведени основните изисквания към S-боксовете. Представена е теорията на Булевите функции в частта, необходима за следващите изследвания.

Трета глава е посветена на запознаване с трите основни подхода при генериране на S-боксове. За всеки от тях са дискутиране техните предимства и недостатъци, както и най-добрите получени резултати.

Четвърта глава съдържа двата основни евристични алгоритъма, разработени от дисертанта. Това е основния принос на дисертанта за получаване на S-боксове с добри криптографски свойства. Представени са три разновидности на реверсивен генетичен алгоритъм и две разновидности на специализиран имунен алгоритъм.

В пета глава са представени резултатите, получени с използването на разработените алгоритми. Коментирани са свойствата на получените S-боксове.

Шеста глава представлява обобщение на получените резултати и насоки за продължение на изследванията.

В седма глава са представени някои от получените S-боксове.

Авторефератът е в обем от 30 страници и правилно отразява приносите на дисертанта.

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

Резултатите от дисертацията са публикувани в 4 публикации, като във всички публикации дисертантът има по двама съавтори. В три от публикациите съавторциса Николай Николов и научния консултант Светла Никова, а в една публикация съавтори са Николай Николов и Виолета Дъчева.

Две от публикацийте са доклади от конференции (MATTEX на Шуменския Университет и BalkanCryptSec в Словения), а другите две са статии в списания (Cryptology ePrint Archive и Journal of Cryptography and Communications. Descrete Structures, Boolean Functions and Sequences). Второто списание е с IF.

Част от резултатите са докладвани на Националния семинар по Теория на кодирането „Проф. Стефан Додунеков“, В. Търново, 2013 г.

Добро впечатление прави факта, че публикациите са цитирани 9 пъти.

5. Научни приноси

Основните приноси на дисертацията са:

1. Описание и сравнение на известните методи за генериране на биективни криптографски добри S-боксове за размерности от (6×6) до (16×16).

2. Разработване на различни варианти на алгоритми (три варианта на реверсивен генетичени алгоритъм и две разновидности на специализиран имунен алгоритъм), които са използвани за получаване на S-боксове с добри криптографски свойства.

6. Заключение

Представения дисертационен труд удовлетворява изискванията на Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в Института по математика и информатика на БАН за получаване на образователната и научна степен „доктор“.

Получените резултати, публикуваните статии и броя на цитиранията ми дават основание да подкрепя придобиването на образователната и научна степен „доктор“ от Георги Велков Иванов в професионално направление 4.6. Информатика и компютърни науки.

15.12.2016 г. Емил Колев: