С Т А Н О В И Щ Е

по 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

Тема на дисертационния труд: „New Heuristic Methods for Generation of Bijective S-boxes with Good Cryptographic Properties”

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

Изготвил становището: доц. д-р Валентин Пенев Бакоев,
ФМИ на ВТУ „Св. св. Кирил и Методий”

Становището е изготвено на основание заповед № 282/07.10.2016 г. на Директора на ИМИ при БАН и решенията от първото заседание на научното жури, проведено на 14.10.2016 г.

1. Данни за дисертанта

Георги Велков Иванов е роден на 7.05.1976 г. в гр. София. През 1994 г. завършва НПМГ „Акад. Любомир Чакалов”, гр. София, а през 1999 г. – ФМИ на СУ „Св. Климент Охридски”. Дипломира се с ОКС „Магистър” по специалност „Математика”. През периода 1999 – 2000 г. работи като хоноруван асистент по „Математическо оптимиране” във ФМИ на СУ „Св. Климент Охридски”, през периода 2001 – 2008 г. – в „Дирекция защита средствата за връзка” към МВР, а от 2008 г. – в „Орган по криптографска сигурност” към ДАНС.

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 ИД Директор на ИМИ. По време на обучението са положени успешно необходимите изпити и докторантски минимуми. Със заповед № 788/16.12.2015 г. на Директора на ИМИ е отчислен с право на защита. Предварителната защита на дисертацията е проведена на 14.09.2016 г. в ИМИ. Георги Иванов 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 129 стр. и е написана на английски език. Структурирана е както следва: Ключови думи, Резюме, Съдържание, Списък на таблиците, Списък на публикациите по темата на дисертацията, Увод, пет глави, Заключение, Приложения и Литература (включваща 94 заглавия, всички на английски език). Актуалността на темата на дисертацията е безспорна – конструирането на биективни заместителни таблици (bijective substitution tables или накратко S-боксове) с възможно най-добри криптографски свойства е от решаващо значение за сигурността на съвременните блокови шифри, както и на някои видове потокови шифри.

Първа глава от дисертацията представлява увод, в който са представени: мотивацията на изследванията, целите и произтичащите от тях задачи, коментари по очакваните и постигнатите резултати, както и резюмета на отделните части в дисертацията. Във втора глава в две основни части са дадени основните понятия, представяния, твърдения и криптографски свойства на булевите функции, използвани при конструирането на S-боксове, както и тези за самите S-боксове. Показани са връзките и конфликтите между тях – търсенето на оптималност при някои криптографски критерии е свързано с влошаването на други такива. Затова и във връзка с използваните криптоатаки срещу S-боксове, при конструирането им се търси разумен компромис: критериите се степенуват по важност, като при тези с най-голяма тежест се търсят оптимални стойности, а при по-второстепенните – стойности, близки до оптималните. В трета глава са представени трите основни подхода (основаващи се на алгебрични конструкции, на псевдослучайно генериране и на използването на евристични техники), използвани за конструирането на S-боксове. В четвърта глава са представени двете групи евристични алгоритми, разработени от дисертанта, които са в основата на изследванията в дисертацията. Първата група съдържа 3 разновидности на реверсивен генетичен алгоритъм (третата разновидност има два варианта), а втората – две разновидности на специализиран имунен алгоритъм. В пета глава са представени получените резултати от петте алгоритъма, направен е сравнителен анализ както на получените чрез алгоритмите нови S-боксове, така и на самите алгоритми. Шеста глава представлява заключение в три части: обобщение на получените резултати, приноси и насоки за продължение на изследванията. Седма глава е приложение в пет части, включващи някои характерни S-боксове, получени от съответните алгоритми.

Авторефератът е в обем от 30 страници и представя коректно основните части на дисертацията, постигнатите резултати, тяхната апробация, публикациите и приносите в нея.

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

Георги Иванов е представил 4 публикации по темата на дисертацията: 2 статии и 2 доклада, всички на английски език. Във всички тях дисертантът има по двама съавтори: Николай Николов (във всички публикации), научния консултант Светла Никова (в публикациите с номера 2, 3 и 4 според номерацията им в дисертацията и в автореферата) и Виолета Дъчева (в публикацията с № 1). Публикациите са:

- № 1 е доклад на международната конференция MATTEX, организирана от ШУ „Еп. Константин Преславски“ през 2014 г.;
- № 2 е статия, публикувана в Cryptology ePrint Archive през 2014 г.;
- № 3 е статия, публикувана в Journal of Cryptography and Communications. Descrete Structures, Boolean Functions and Sequences (издание на Springer) през 2016 г. Списанието има IF 0.742 за 2015 г.;
- № 4 е доклад на международната конференция BalkanCryptSec 2015, проведена от 3 до 4 септ. 2015 г. в Словения. Сборникът от доклади на конференцията е публикуван от Springer International Publishing Switzerland през 2016 г.

Статията с № 3 съдържа изцяло в себе си тази под № 2 и затова приемам двете като една публикация. Така пак са изпълнени 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). В статията с № 3 са представени трите версии на реверсивния генетичен алгоритъм и резултатите, получени чрез него (в статията с № 2 – първите две версии). В доклада с № 4 е представена първата версия на специализирания имунен алгоритъм и получените резултати.

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

- Националния семинар по Теория на кодирането „Проф. Стефан Додунеков”, В. Търново, 2013 г.;
- International Conference on Cryptography and Information Security BalkanCrypt, София, 2013 г.

Въпреки че публикациите на Георги Иванов са сравнително нови (публикувани са през последните 2 години), те вече имат по няколко цитирания от чуждестранни автори: статията с № 2 – 2 цитирания; тази с № 3 – 5 цитирания, докладът с № 4 – 2 цитирания, или общо 9 цитирания. Това, като и публикацията в списание с импакт-фактор, са достатъчно красноречиви показатели както за високото ниво на проведените изследвания и получените резултати, така и за приема и отражението им в научните среди по света.

5. Научни приноси

Основните приноси в дисертацията са представени в част 6.2 Thesis Contribution. В автореферата те са дадени в авторската справка, като са систематизирани в 5 групи. Поради обема им те трудно могат да бъдат изброени тук. Най-общо приносите се свеждат до разработване на два вида евристични алгоритми: реверсивен генетичен алгоритъм в 3 разновидности (третата има два варианта) и специализиран имунен алгоритъм в 2 разновидности, с помощта на които са получени редица нови резултати – биективни $(n \times n)$ S-боксове с различни размерности (за $n =$ 6, 8, 10, 12, 14 16), съчетаващи различни комбинации от криптографски свойства. Те са представени чрез редица таблици в дисертацията, като са сравнени с най-добрите публикувани такива. За получените в дисертацията S-боксове най-общо може да се каже, че:

- Някои от тях са нови – други S-боксове с толкова добри съчетания на параметри не са публикувани;
- Криптографските свойства при някои от тях са много близо до най-добрите съчетания на криптографски свойства, известни досега – тези, получени чрез алгебрични конструкции. При някои свойства те достигат или се доближават много до най-добрите стойности известни към момента, а при други (например като брой на получените S-боксове и брой на нееквивалентните сред тях, линейна остатъчност) даже ги превъзхождат.

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

6. Критични бележки и препоръки

Чрез предложените в дисертацията алгоритми са получени резултати на световно ниво, но не е представена оценка на тяхната сложност. Не става ясно дали и доколко алгоритмите биха могли да се оптимизират и по този начин, пак за същото време, да се получат още по-добри резултати. Тези въпроси са важни както по принцип, така и по отношение насоките за бъдещи изследвания, а също и от гледна точка на криптоанализа на самите алгоритми. Считам, че една допълнителна част към четвърта глава, представяща елементи от реализацията на алгоритмите и изследване на сложността на им, би ѝ предала наистина завършен вид. По този начин и обемът на главите би станал по-балансиран – втора глава заема цели 55 страници (би могло частта за S-боксове да се прехвърли към трета глава). От една страна втора глава съдържа дефиниции и твърдения, които не се ползват в следващите части и би могла да бъде съкратена. От друга страна, в този си вид тя може да служи за основа на учебник по темата – остава само да се добавят подходящи примери, илюстрации и задачи. Аз не съм срещал подобен учебник и силно препоръчвам на автора да го подготви и издаде.

Отбелязвам, че забележките и препоръките, които имам към дисертацията не омаловажават качеството и коректността на получените резултати.

7. Заключение

На основание казаното дотук съм убеден, че са налице всички необходими предпоставки за успешна защита на дисертационния труд на тема „New Heuristic Methods for Generation of Bijective S-boxes with Good Cryptographic Properties". Предлагам на уважаемото Научно жури да гласуваме „ЗА" придобиването на образователната и научна степен „доктор" от Георги Велков Иванов в професионално направление „4.6. Информатика и компютърни науки".

08.12.2016 г. Изготвил становището:

(доц. д-р Валентин Бакоев)