Р Е Ц Е Н З И Я

на дисертационен труд
за придобиване на образователната и научна степен "Доктор"

по научната специалност 01.01.12 "Информатика"

Тема: "New Heuristic Methods for Generation of Bijective S-Boxes with Good Cryptographic Properties"
Нови евристични методи за генериране на биективни S-таблици с добри криптографски свойства

Автор: Георги Велков Иванов

Научни консултанти: доц. д-р Светла Никова, доц. дмн Емил Колев

Рецензент: проф. д.м.н. Иван Николов Ланджев

Тема на дисертационния труд

В представения дисертационен труд са разгледани въпроси отнасящи се до конструирането и изследването на криптографската устойчивост на субституционни таблици (S-таблици, заместващи таблици, S-boxes). Този въпрос може да се счита за центарлен при създаването и изпитването на блокови шифри, тъй като голяма част от сигурността им се дължи на внимателното конструиране на съответните субституционни таблици. Още от създаването на DES в края на 60-те години на XX век бяха повдигнати въпросите относно методите за конструиране и създаване на критерии за устойчивост S-таблици. Предложените тогава S-таблици се оказаха с добри криптографска устойчивост, но неясни принципи на създаване, което повдигна въпроси около надеждността им и наличието на "задни вратички". Беше осъзнато, че въпросът за дизайна на S-таблиците е централен при дизайна на блокови шифри, независимо дали се касае за файстелови шифри или SPN-мрежи. Ясно е, че променянето на S-таблиците при запазване на всички останали характеристики създава на практика нов блоков шифър. По тази причина развитието на средства за създаване и оценка на криптографските свойства на S -таблици е от голямо значение.

Целите, които дисертантът си поставя в настоящия труд са следните:

1) Да изследват общите връзки между криптографските свойства на булевите функции и субституционните таблици; тъй като криптографските свойства, изисквани от тях, са често взаимноизключващи се, то не съществуват очевидни начини за генерирането им и задачата за с ъздаване на S-таблици с определени параметри е нетривиална.

2) Да се предложат и обосноват евристични методи за генериране и оптимизиране на S-таблици.

3) Да се разработят алгоритми, основаващи се на предложените евристични методи за ефективно генериране на голям брой S-таблици с достатъчно добри характеристики.

4) Да се намерят и обосноват критерии за криптографска пригодност на S-таблици.

5) Да се разработят биективни S-таблици с малки размери – от 6×6 до 16×16 – които са криптографски сигурни.

Литературен обзор

Общото ми впечатление е, че дисертантът познава много добре съвременното състояние на разглеждания проблем. Голяма част от изследванията му са върху един кръг от задачи и хипотези от криптографията, разглеждани като значими и имащи голяма важност за приложенията, по-специално в дизайна и анализа на блокови шифри. Дисертацията включва разработване на алгоритми, които се използват по-нататък за намиране на конструкции на нови S-таблици и подобрения на известни резултати. С това дисертантът демонстрира дълбоко познаване на областта си и възможности творчески да прилага знанията си. Дисертантът показва добра информираност по голяма част от разглежданите проблеми.

Методика

В изследванията си дисертантът използва основно комбинаторни техники, почиващи на сериозни компютърни изчисления. На места дисертантът използва алгебрични резултати за булеви функции и специални двоични редици. Почти всички резултати, получени в дисертацията, са получени в разултат на тежки и технически трудни компютърни пресмятания.

Съдържание и резултати на дисертационния труд

Дисертационният труд е в обем от 129 нестандартни машинописни страници и се състои от пет глави, заключение, приложение и списък на използваната литература, включващ 94 заглавия. Дисертационният труд е написан на английски език.

По долу ще изложа накратко съдържанието на отделните глави от дисертационния труд.

Глава 1 представлява увод в дисертационния труд. Докторантът излага целите, които си поставя с настоящия текст, както и основните идеи, заложени в него. Една от тях е за генетичен алгоритъм, започващ работа от някаква добра S-таблица, например получена от алгебрична конструкция (взимане на обратен в крайно поле), и търсене в полседователни итерации на нови таблици, оптимизирайки предварително заложени критерии. Друга идея използва търсене, започващо със случайна S-таблица. Такова таблици биха били по защитени при евентуално намиране на атака срещу алгебрично дефинираните S-таблици.

В глава 2, наречена "Предварителни сведения" (Preliminaries), са изложени основните дефиниции и някои важни сведения за булеви функции и S-таблици. Описани са най-важните криптографски атаки, както и криптографските критерии, произтичащи от тях, които се налагат върху S-таблиците за достигане на достатъчна криптографска устойчивост. Главата представлява добър обзор на най-важните разултати за булеви функции, за криптографските им приложения, както и за криптографските атаки срещу S-таблици (линеен, диференциален, корелационен криптанализ, диференциален криптанализ от по-висок ред).

Глава 3 е посветена на подробното описание на трите основни метода за генериране на S-таблици: генериране по псевдослучаен начин, генериране, използващо алгебрични структури и генериране, използващо специални евристики. Изследванията в този труд са съсредоточени върху третата група методи като между тях вниманието е фокусирано върху hill climbing методи, на методи за "симулирано закаляване" (simulated annealing), на генетични алгоритми и алгоритми с имунитет. В метода, наречен hill climbing, се променя един или повече компоненти в решението (което е S-таблица) и се следи изменението на една или повече негови характеристики. В този случай на всяка стъпка се променят два бита в таблицата и се следи за изменението (изисква се повишаване) на нелинейността N_f. Методът, наречен симулирано закаляване (simulated annealing) се явява продължение на метода hill climbing. Разликата се състои в следното: ако при промяна на таблицата се получава по-добра стойност на наблюдавания параметър, то това решение се взима винаги (загряване); в противен случай то се взима с някаква вероятност в зависимост от отклонението от най-добрата стойност на намерения параметър (охлаждане). Това позволява избягване на ситуацията, при която се оказваме хванати в локален оптимум, който не може да се напусне с използване на hill climbing техниката, тъй като всички съседни решения са по-лоши. По нататък са описани възможностите за използване на т. нар. генетични алгоритми и алгоритми с имунитет. При първите се поддържа популация от възможни решения, притежаващи едно или няколко желани свойства. На всяка стъпка те се трансформират в нови като се оценява тяхната годност и най-добрите се избират за по-нататъшните стъпки. При втората група се започва от решения (таблици) "с имунитет". На всяка стъпка се създават нови решения чрез вариране на старите, за които се проверява, в каква степен е налично желаното свойство (устойчивост на патоген). Приложение на алго-

ритъм с имунитет за генериране на S-таблици се предлага за пръв път в настоящата работа.

Глава 4 е централна за дисертационния труд. В нея са изложени три основни метода евристично генериране на криптографски устойчиви, биективни S-таблици с размер $n \times n$. Описани са четири варианта на нов генетичен алгоритъм както и няколко варианта на алгоритъм "с имунитет" (immune algorithm). Тези алгоритми са използвани по-нататък за построяване на S-таблици с усложнена алгебрична структура за сметка на незначително разваляне на нелинейността и диференциалната еднородност (uniformity). На входа се подава таблица, получена от намиране на обратен елемент в крайно поле, която се преобразува до намиране на нови таблици с по-сложна алгебрична структура и криптографски свойства достатъчно близки до оптималните. Свойствата, които се следят са нелинейност, алгебрична степен, автокорелация и δ-еднородност. Предложени са три такива генетични алгоритъма (RGA1–RGA3). Описани са и два специални алгоритъма с имунитет (SIA1, SIA2). Последните са използвани за атакуване на една специална задача за пораждане на нова 6×6 APN-пермутация (almost perfect non-linear), която не е еквивалентна на известната към момента.

В глава 5 се описват и анализират най-добрите S-таблици, получени чрез методите от глава 4.

Глава 6 представлява заключение, в което са обобщени получените резултати, описани са приносите на дисертационния труд и са набелязни някои идеи за бъдеща насока на изследванията по тази тематика.

Глава 7 е приложение, съдържащо в явен вид списък от 8×8 S-таблици в явен вид, получени чрез разработените в дисертацията алгоритми.

Приноси на дисертационния труд

По мое мнение по-важните приноси в дисертационния труд се свеждат до следното:

(1) Направен е обзор и критичен анализ на известните методи за генериране и изследване на S-таблици.

(2) Развити са евристики за модификация на съществуващи S-таблици.

(3) Разработени са няколко нови алгоритъма (генетични алгоритми и алгоритми "с имунитет") за генериране на относително големи S-таблици със свойства близки до тези на S_{inv} (S-таблицата, получена от взимане на обратен лемент в подходящо крайно поле), но с по-голяма алгебрична сложност.

(4) Предложени са имплементации на приложените алгоритми.

(5) Конструирани са нови S-таблици, някои от които побобряват характеристиките на най-добрите известни до момента.

Забележки по дисертационния труд

Във връзка с дисертационния труд имам следните забележки:

(1) Работата е стегнато и ясно написана. На места обясненията са твърде оскъдни, което малко затруднява разбирането на текста.

(2) Техническото оформление на работата е изпълнено на LaTeX. Появящите се на места печатни грешки не променят общото добро впечатление. Приветствам написването на дисертацията на английски език. Това ще я направи достъпна за по-широк кръг читатели. От друга страна съм на мнение, че стилът има нужда от известно подобрение. На места са използвани неточни понятия като (vectorial function щм. vector function . i t.n.)

Публикации по дисертационния труд

Резултатите от дисертационния труд са публикувани в 4 статии. Три от статиите са излезли от печат в Journal of Cryptography and Communications на Springer, Lecture Notes in Computer Science и сборник с доклади на конференцията MATTEX. Четвъртата работа е абстракт, публикуван в електронен архив.

Списанието Journal of Cryptography and Communications има импакт-фактор 0.742 за 2015 г.

Авторство на получените резултати

Всички четири представени публикации са с по двама съавтори. Тъй като познавам научните интереси на докторанта и следя работата му в последните пет години, за мен няма съмнение, че приносът му е поне равностоен с този на останалите автори.

Цитирания на публикациите от дисертационния труд

Дисертантът е приложил списък на девет цитирания на статиите, в които са публикувани резултатите от дисертационния труд.

Автореферат и авторска справка

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

Заключение

Дисертацията е посветена на един кръг от интересни криптографски проблеми, имащи голямо практическо значение за конструирането и оценяването на сигурни криптографски примитиви. Направено е задълбочено изследване на поведението и

надеждността на специални S-таблици. разработени са нови алгоритми и са направени конструкции на голям брой нови S-таблици. С това е постигнат напредък в актуална област на криптографията.

Считам, че представеният дисертационен труд "New Heuristic Methods for Generation of Bijective S-Boxes with Good Cryptographic Properties" с автор Георги Велков Иванов съдържа резултати, които представляват оригинален принос в криптографията. Дисертантът показва задълбочени теоретични знания в областта на изследването на S-таблици и по-общо в конструирането и анализа на блокови шифри, както и способност за самостоятелни научни изследвания. С това считам, че той отговаря на изискванията на "Закона за развитие на академичния състав" за даване на научната степен "Доктор". Гореизложеното ми дава основание да дам положителна оценка на представения дисертационен труд на и да препоръчам на Уважаемото жури да присъди на Георги Велков Иванов образователната и научна степен "Доктор".

София, 07.12.2016 г.