ФТК78-НС1-062
30.01.2017

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ * СОФИЯ * ФТК НАУЧНО ЖУРИ

Р Е Ц Е Н З И Я

върху дисертационен труд за придобиване на образователна и научна степен "доктор".

Автор на дисертационния труд: **маг. инж. Иван Динков Иванов**.

Тема на дисертационния труд: **Методи и алгоритми за повишаване на сигурността и съхранението на данните при предаването на информация в телеметрични системи.**

Рецензент: проф. д-р инж. Георги Димитров Ненов

1. Актуалност на разработвания проблем. Защитата на информация от от несанкциониран достъп има широко и важно значение. Тя обхваща голяма част от обществените институции и личните данни и дела на гражданите. Поради това е обект на законодателни норми у нас и в други страни.

Злоумишленото използване на данни от компютърните мрежи придоби значителни размери и това отдавна наложи създаването на мерки за защита, които са насочени едновременно към хардуера и софтуера на мрежите.

Наченките на криптографията са в далечното минало, но през последните десетилетия тя се обогати с много методи и алгоритми. В напредналите страни са приети съответни стандарти и протоколи. Като пример за нашата страна е Законът за защита на класифицираната информация, както и подзаконовите актове (правилник, наредби и пр.).

Надежността на криптографската защита на информацията зависи от много фактори, но и в тази област "абсолютната" (стопроцентова) надежност е идеализация. Потвърждение са кибератаките, за които се съобщава в средствата за масово осведомяване в последно време. Ето защо всяко постижение в тази област, каквото е тази дисертация, трябва да се признае за актуално.

2. Степен на познаване на проблема. За доброто познаване на проблема от дисертанта може да се съди по много от постановките, които са залегнали в дисертациятя. На около 30 страници е направен критичен обзор и по убедителен начин се разкриват целите и задачите (стр. 33). Прецизирани са определени понятия от телеметрията, изтъкнати са предимствата и недостатъците на известните методи и алгоритми в криптографията, като се орбъща внимание на предназначението. За насочеността към приложение формулирани доста оригинално 8 изисквания за реализиране на съответни алгоритми, които може да се проследят по-нататък в труда във връзка с конкретни решения.

Добро познаване на материята показват синтезирането на оригинален алгоритъм и неговото изследване относно функциалността, устойчивостта, бързодействието и пр.

Преподавателският опит на дисертанта е намерил отражение в стил, който прави изложението на материала методично издържано, прави го ясно, достъпно и убедително.

3. Кратка аналитична характеристика на дисертацията. Трудът обхваща 143 машинописни страници с голям брой графики към текста, които представят информацията в удобен вид за възприемане и използване. В срая са дадени три приложения (копия от документи).

Материалът е подреден в четири глави, увод, основни изводи и приноси, списък на литература по проблема.

За съдържанието и достойнствата на **първа глава** е отделено достатъчно място в първите две точки на рецензията. Тук може да се добави и това, че тя е много добре свързана със списъка на литературата. Посочени са 117 заглавия, които са преди всичко на английски език. Само 9 са на кирилица, сред които учебно пособие на дисертанта [87]. Например в труд (Ръководство...) на Бърнет и Пейн, преведено на руски език (стр. 105) се твърди, че бившият Съветски съюз и Китай се въздържат да публикуват оригинални материали за алгоритми с открит ключ (PKC - Public - Key Certificate). Това показва колко е трудна една задълбочена литературна справка, и колко важен е проблемът за надеждното шифриране.

Във **втора глава** е отразено създаването на метод и съответен алгоритъм за криптография с повишена защита и възможности за по-широко приложение. В дискусионен вид се разглеждат операциите *разбъркване* (confusion) и *разсейване* (diffusion), чрез който се усложняват съответно връзката между ключа и шифрования текст, и между явния и шифрования текст. Обсъжда се значението на "лавинния" ефект, при който смяната на символ в явния текст променя значително крайния резултат. По-нататък вниманието е насочено към параметрите на алгоритъма. Обосновани са изисквания за броя на циклите (16 бр.) и относно функцията на шифрирането F (критерии за матрицата S и за функцията на входа P).

В тази логична последователност е предложено собствено решение чрез алгоритъма IDA (**I**vanov, **D**ikov, **A**rnaudov). То се свързва с алгоритъма DES (**D**ata **E**ncryption **S**tandard) и схемата на Фейстел. Показана е общата блокова схема на алгоритъма (фиг. 2.1) и са проследени (фиг. 2.2 и фиг. 2.3) началното и крайно разместване, функциите на криптиране F, на разширяване E, за разместването на изхода P, кутиите S и E. Предимствата на предложения са отразени на стр. 55.

В **трета глава** са описани изследването на функционалността на алгоритъма и възможностите за неговото внедряване. В т. 3.1 са поставени 5 задачи. "Ръчното разписване" е своеобразно моделиране на алгоритъма.

За целта са използвани таблици за операции. Задачата за програмната реализация е решена чрез стандартния език "C" в среда VSE 2010, Windows 7.

Възможностите за внедряването са илюстриране чрез фигурите: 3.3, 3.4 и 3.5. На първата от тях е дадена блокова схема на система от замисления вид. Внедряването засяга софтуерните продукти за обслужване на собственика на моторно превозно средство (МПС), на съответни оторизирани органи и застрахователи, и на полицията.

Четвърта глава е един добър завършек на дисертационния труд. Приведени са резултати от изследването на основните параметри, криптографската устойчивост и бързодействието на предложения алгоритъм IDA. Резултатите са представени в компактен вид чрез таблици и графики. Обобщаващи са табл. 4.34 и изводите на стр. 128. Показани са преди всичко предимствата на IDA и някои негови недостатъци в сравнение с утвърдените в практиката алгоритми: DES, IDEA, AES и Blowfish.

4. Приноси. Претенциите на докторанта по отношение на приносите са изложени на стр. 133 и стр. 134. *Научноприложните приноси* са формулирани в 6 пункта, а приложните в два. На преден план са: оригинален метод и алгоритъм, проблеми на синтеза и зависимости, свързани с "лавинния" ефект, устойчивостта и бързодействието.

Доказателство за *приложните приноси* е фактът **внедряване.** Представен е съответен документ (Приложение А3) от фирмата "Ентърпрайс Комюникейшънс Груп" ООД, която използва алгоритъма в системата "eCall" за постигане на целите, показани на фиг. 3.3.

Не мога да не споделя с членовете на Уважаемото Научно жури задоволството си от това, че в представения дисертационен труд е отразено решение на актуален проблем от неговото разкриване, и неговия изследователски анализ-синтез до внедряването на резултатите в материалната сфера. Такива са повече от дисертациите и научните изследвания в престижните образователни и научни институти в света.

5. Лично участие на дисертанта. Личното участие на дисертанта проличава от публикациите и представените документи. Това беше потвърдено на предварителната защита пред кат. "Радиокомуникации и видеотехнологии" в ТУ - София. Видно е, че дисертацията е негово лично дело, без да се омаловажава и най-малко ролята на научните ръководители проф. Арнаудов и доц. Диков.

6. Преценка на публикациите. Дисертантът има 6 публикации във връзка с дисертацията и заявка за патент (Приложение А1). Две от публикациите са самостоятелни. Едната е на международна научна конференция, а другата в Известия на Съюза на учените в България.

Публикациите в съавторство също са пред престижни научни форуми.

Очевидно е, че е получено признание от по-широка научна аудитория, както и от практиката.

7. Мнения и препоръки. В становището ми пред разширения катедрен съвет във връзка с докладването на дисертацията отправих някои препоръки, които дисертантът е взел под внимание и е внесъл съответните корекции. Естествено е да се желае още.

Колегата Иванов е преподавател и в негова полза е да се заостри вниманието му върху някои редакционни и терминологични пропуски. Например честото използване на причастия, което не се препоръчва, на полусляти форми вместо сляти и др.

Не се разграничават достотъчно добре "надежност" и "безопасност", които се припокриват частично.

Докторантът не е обърнал внимание на предишната ми забележка, че дисертационният труд е за "придобиване", а не за "получаване" на... Законодателят по този начин подчертава, че това е по заслуга, че се постига, а не се само взема.

Редно е да се избягва именуването на предложения алгоритъм и въобще чрез прилаганата форма "IDA алгоритъм" вместо "алгоритъм IDA" и пр.

Заключение. Представеният дисертационен труд от маг. инж. Иван Динков Иванов отразява цялостно изследване и новаторско решение в областта на криптографията, при което са създадени метод и алгоритъм за телеметрични системи с повишена сигурност на пренасянето и съхранението на данните.

Изключително достойнство на труда е съчетанието между задълбочени анализи, които предшестват синтеза на алгоритъм и система и тяхното обхватно тестване, насочено към приложения.

Висока оценка заслужават усилията, свързани с внедряването на многофункционална система в областа на автомобилния транспорт.

В този завършен вид на цялостно решение на изследователски проблем, трудът отговаря напълно на условията, предвидени в гл. 2, чл. 6 от Закона за развитие на академичния състав в Република България за придобиване на образователна и научна степен "доктор".

София, 18.01.2017 г.

Рецензент:
/проф. д-р инж. Г. Д. Ненов/