НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

НАВРОЦЬКИЙ Денис Олександрович

УДК 681.3.06:004.056.5 (043.3)

МЕТОД ПОБУДОВИ СИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ШИФРІВ НА ОСНОВІ ТРИВИМІРНИХ КЕРОВАНИХ ПЕРЕТВОРЕНЬ

05.13.21 – Системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана у Національному авіаційному університеті Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор, лауреат Державної премії України, Заслужений діяч науки і техніки України, професор кафедри електроніки **Білецький Анатолій Якович** (Національний авіаційний університет).

Офіційні опоненти: доктор технічних наук, професор, завідувач кафедри захисту інформації **Лужецький Володимир Андрійович** (Вінницький національний технічний університет);

доктор технічних наук, професор, завідувач кафедри інформаційної безпеки та комп'ютерної інженерії **Рудницький Володимир Миколайович** (Черкаський державний технологічний університет).

Захист відбудеться 13 квітня 2017 р. о $13^{\underline{00}}$ годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, Київ, просп. Космонавта Комарова, 1, навч. корп. 11, ауд. 111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий 13 березня 2017 р.

В.о. ученого секретаря
спеціалізованої вченої ради Д 26.062.17 _____ В.П. Квасніков

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Обчислювальні системи постійно вдосконалюються і набувають нових функціональних властивостей, до яких належать можливості розподілених паралельних розрахунків, хмарні технології, просторові (графічні) розрахунки тощо. З розвитком електроніки і програмування зростають ризики в криптографічному захисті. Проведені конкурси з обрання стандартів шифрування AES, NESSIE, CRYPTREC тощо були розраховані на апаратні та програмні можливості того часу. На сьогодні доволі поширені на ринку шифри з репутацією стійких і швидких, такі як AES, ГОСТ 28147-89, ДСТУ 7624:2014, 3DES та ін. Ці шифри намагаються адаптувати під сучасні потреби захисту даних. З поширенням технологій інтернет-речей і безпілотних літальних апаратів (БПЛА) постала проблема захищеності даних малою обчислювальною потужністю. В комп'ютерах гострої проблеми зі швидкодією й об'ємами пам'яті не існує, проте в мікроконтролерах ця проблема актуальна. Оскільки будь-які розрахунки займають багато часу і споживають енергію, для автономних систем, які живляться від акумуляторів, це вкрай критично. Наприклад БПЛА, у якому на одному мікроконтролері має бути реалізована як навігаційна система, так і шифрування даних для командної, телеметричної, відеоінформації. Адаптація існуючих шифрів під нові задачі не є тривіальною і її вирішують за допомогою сторонніх фірм-розробників, які досить часто використовують закритий код і *know-how* принцип. Це спричиняє виникнення шпаринок (англ. *backdoor*) у реалізаціях шифрів. Отже, слід зазначити відмінність між криптографічною стійкістю алгоритму й апаратно-програмною реалізацією цього алгоритму на конкретному обладнанні. Останнім часом склалась така ситуація, що під брендом відомих шифрів на ринку наявні безліч вразливих систем шифрування. Це підтверджується тим, що досить часто виробники шифрувального обладнання заявляють, що мають можливість відновити зашифровані дані на їх обладнанні у випадку втрати ключа шифрування користувачем. Отже, існує нагальна потреба розробити шифри під потреби сучасних завдань захисту даних.

Значний внесок у розвиток криптографічних методів захисту інформації внесли такі відомі вчені, як І.Д. Горбенко, В.І. Долгов, В.К. Задірака, І.Л. Єрош, М.А. Іванов, Л.В. Ковальчук, Г.В. Кузнецов, О.О. Кузнецов, М.Е. Масленніков, А.А. Молдовян, Н.А. Молдовян, А.М. Олексійчук, А.А. Петров, А.Г. Ростовцев, Ю.С. Харін та ін. З-поміж закордонних науковців варто згадати таких: А. Бірюков, Е. Біхам, Й. Даймен, В. Діффі, Л. Кнудсен, Н. Кобліц, М. Мацуі, Дж. Мессі, Н. Смарт, Р. Смит, В. Столінгс, Р. Рівест, В. Реймен, Х. К. А. ван Тілборг, Х. Фейстель, Н. Фергюсон, А. Шамір, Б. Шнаєр, М. Хеллман та ін.

Переважна більшість досліджень, орієнтовані на методи, які ускладнюють розрахунки, тобто йдуть шляхом збільшення розрахунків. Такий підхід спричиняє великі витрати машинного часу і відповідно споживає багато енергії.

Таким чином, розроблення і дослідження методів швидких криптографічних перетворень для систем з малою швидкодією й обмеженою кількістю пам'яті є актуальними науковими завданнями, які мають теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами

Тематика дисертаційної роботи та отримані результати безпосередньо пов'язані із:

1. Концепцією інформаційної безпеки України;

2. Концепцією розвитку сектору безпеки й оборони України;

3. Указом Президента України № 92/2016 від 4 березня 2016 року «Про Стратегію кібербезпеки України»;

4. «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки» в частині п.1.2.8.1 «Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії»;

5. Стратегією національної безпеки України від 26 травня 2015 року № 287/2015 у контексті п.4.12 «Забезпечення кібербезпеки і безпеки інформаційних ресурсів, зокрема реформування системи технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС з досліджень та інновацій;

6. «Горизонт-2020», зокрема за напрямами DS-05-2016 та DS-06-2017 («Визначення нових напрямів інноваційних наукових досліджень в Європі щодо забезпечення кібербезпеки як відповідь на нові тенденції і передові технології»);

7. НДР «Розробка та впровадження програмних засобів захисту інформації від несанкціонованого доступу в електронних системах документообігу у вищих навчальних закладах України» (2010–2011 рр., номер державної реєстрації 0110U000222).

Мета і завдання дослідження. Мета дисертаційної роботи полягає у підвищенні ефективності (стійкості, швидкодії, зменшення ресурсоємності) криптографічного захисту інформації на основі застосування нових блокових і потокових шифрів з використанням динамічно керованих тривимірних криптографічних примітивів.

Для досягнення поставленої мети необхідно розв'язати такі основні завдання:

- провести аналіз сучасних криптографічних методів захисту інформації за критеріями стійкості, швидкодії та необхідних ресурсів для розрахунків, а також обґрунтувати шляхи вдосконалення алгоритмів симетричного шифрування;

- розробити методи формування динамічно керованих примітивів лінійного розсіювання, нелінійної заміни та «ковзного кодування» на основі узагальнених перетворень Грея та матриць Галуа для тривимірного простору;

- на основі запропонованих криптографічних примітивів розробити методи криптографічної обробки даних (блокового, потокового) тривимірного шифрування даних з метою підвищення ефективності (стійкості, швидкодії, менш ресурсоємні) криптографічного захисту інформації;

- розробити апаратно-програмне забезпечення і провести лабораторні випробування засобів захисту командно-телеметричної (КТ) та відеоінформації (ВІ) в каналах зв'язку наземного пункту керування з безпілотним літальним апаратом (НПК–БПЛА).

Об'єктом дослідження є процес перетворення інформації в симетричних криптографічних шифрах на основі тривимірних примітивів.

Предметом дослідження є методи побудови симетричних криптосистем, що забезпечують підвищення ефективності захисту інформації.

Методи дослідження. Проведені дослідження ґрунтуються на сучасній теорії криптографічного захисту інформації, теорії чисел, алгебричній теорії груп, скінчених полях Галуа, теорії незвідних і примітивних поліномів, а також теорії синтезу генераторів псевдовипадкових послідовностей, що засновані на узагальнених лінійних регістрах зсуву з лінійними зворотними зв'язками, теорії ймовірностей та математичній статистиці, об'єктно-орієнтованого програмування тощо.

Наукова новизна отриманих результатів полягає в такому:

– *уперше* розроблено метод і його модифікації для формування динамічно керованих примітивів лінійного розсіювання, нелінійної заміни та «ковзного кодування» на основі узагальнених перетворень Грея та матриць Галуа для тривимірного простору, які за рахунок розроблених динамічних дискретних математичних моделей на базі операцій над тривимірними матрицями, властивостями невироджених тривимірних матриць у полі Галуа; класичних (*лівосторонніх*) і так званих *правосторонніх* та *складених* кодів та рандомізованих *кодів Грея* в тривимірному просторі дали можливість на їх основі синтезувати та розробити динамічно керовані тривимірні криптографічні методи побудови перемішування (permutation 3D), нелінійної заміни (substitution 3D), матричного перетворення (matrix 3D), стохастичного циклічного зсуву (shift 3D), «ковзного» кодування 3D (slider code 3D), що дало можливість збільшити швидкодію і стійкість шифрів та зменшити необхідний об'єм пам'яті для роботи шифру;

– *удосконалено* метод синтезу матриць для таблиць підстановки і перестановки на основі запропонованих криптографічних примітивів і розробленого методу криптографічної обробки даних (блокового, потокового) тривимірного шифрування даних, які за рахунок методів синтезу примітивних матриць Галуа і Фібоначчі, сполучених варіантів, над простими полями Галуа характеристики 2, дали можливість розширити множину узагальнених генераторів псевдовипадкових послідовностей, а також запропонувати нові підходи до розв'язання проблеми формування таємних ключів шифрування абонентами мережі з відкритими каналами зв'язку;

– *отримали подальший розвиток* методи розробки засобів захисту командно-телеметричної та відеоінформації в каналах зв'язку наземного пункту керування з безпілотним літальним апаратом, які за рахунок методів симетричного блокового криптографічного перетворення інформації з динамічно керованими параметрами шифрування (криптографічні перетворення виконуються в тривимірному просторі) дали можливість в алгоритмах шифрування здійснювати оперативну модифікацію параметрів криптографічних примітивів при переході до чергового блоку тексту, що перетворюється.

Практичне значення отриманих результатів. Практична цінність роботи полягає в такому:

– запропоновано спосіб тривимірних перетворень блокових та потокових шифрів (БШ і ПШ) на основі розроблених методів формування динамічно

керованих примітивів лінійного розсіювання, нелінійної заміни та «ковзного кодування» на основі узагальнених перетворень Грея та матриць Галуа для тривимірного простору для побудови більш швидких і таких, що потребують меншого об'єму пам'яті криптосистем;

– розроблені та впроваджені алгоритми симетричних RSB-64-3D блокових і 3DMatrix потокового шифрування інформації, які доведені до рівня програмної реалізації на мові C# і C++ для ПК і мікроконтролера, що дало можливість провести експериментальне дослідження запропонованих рішень для криптографічного захисту командно-телеметричної інформації в каналі зв'язку НПК–БПЛА і дало можливість підвищити швидкодію і зменшити необхідний об'єм пам'яті для забезпечення криптографічного захисту інформації як для мікроконтролерних пристроїв, так і для комп'ютерів;

– розроблено ПЗ для статистичного аналізу криптограм на базі тестів NIST STS і DIEHARD, які доповнені власними методами оцінювання шифрограм;

– за результатами дисертаційних розробок отримано дев'ять патентів України на «Спосіб криптографічного захисту інформації»;

– результати дисертаційної роботи впроваджено у навчальному процесі кафедри електроніки Національного авіаційного університету, кафедри виробництва приладів Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», та у науково-технічних розробках ТОВ «Агфар», ТОВ «Гратис, Лтд», що підтверджено відповідними актами впровадження.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – програмне моделювання процесу розпізнавання; [2] – множина секвентних функцій; [3] – алгоритм синхронного потокового шифрування; [5] – синтез і реалізація SCSPS шифратора; [6] – синтез програмно-моделюючого комплексу захисту каналу зв'язку БПЛА; [7] – досліджено криптографічний примітив нелінійної підстановки у тривимірному просторі для шифру RSB3D; [8] – дослідження та розробка криптографічних примітивів за допомогою примітивних поліномів; [9] – програмна модель Ch-CRC; [11] – метод направленого машинного перебору для синтезу квазіеквідистантних кодів.

Із робіт, опублікованих у співавторстві, у дисертаційній роботі використовуються результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися більш ніж на 10 міжнародних та всеукраїнських наукових конференціях, серед яких: міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (Львів, 2012); всеукраїнська науково-практична конференція «Проблеми та перспективи розвитку авіації та космонавтики» (Київ, 2012); науково-технічна конференція «Наукоємні технології» (Київ, 2012); міжнародна науково-технічна конференція «АВІА–2013» (Київ, 2013); всеукраїнська науково-практична конференція «Проблеми навігації і управління рухом» (Київ, 2013); міжнародна науково-технічна конференція «Розвиток наукових досліджень 2013» (Полтава, 2013); науково-технічна конференція «Проблеми роз-

витку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM» (Київ, 2014); міжнародна науково-технічна конференція «ITSEC» (Київ, 2015); міжнародна науково-технічна конференція «ABIA–2015» (Київ, 2015); науково-практична конференція «Сучасні тенденції розвитку системного програмування» (Київ, 2015); науково-методичних семінарах кафедри електроніки Національного авіаційного університету.

Публікації. Основні положення дисертації опубліковано у 32 наукових працях, у тому числі 1 стаття входить у наукометричну базу даних Scopus, 12 статей – у фахових виданнях України, які входять до міжнародних наукометричних баз даних, а також 9 патентах України на корисну модель та 10 тезах доповідей на конференціях.

Структура роботи та її обсяг. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел, а також має 155 сторінок основного тексту, 81 рисунок, 25 таблиць, 68 сторінок додатків. Список використаних джерел містить 133 найменування і займає 20 сторінок. Загальний обсяг роботи − 243 сторінки.

ОСНОВНА ЧАСТИНА

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність проблеми, сформульовано мету та основні завдання дисертаційної роботи, визначені методи досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено відомості про апробацію, впровадження, публікації основних та допоміжних результатів.

У **першому розділі** проведено аналіз сучасних криптографічних методів захисту інформації за критеріями стійкості, швидкодії та необхідних ресурсів для проведення перетворень, а також обґрунтовані шляхи вдосконалення алгоритмів симетричного шифрування, розглянуто вітчизняну та зарубіжну літературу за темою дисертаційної роботи. Визначено основні поняття, пов'язані із криптографічним захистом інформації, проаналізовано основні завдання, які може розв'язувати криптографія у процесі захисту інформації. Крім того, формалізовано вимоги до сучасних БШ (на основі критеріїв міжнародного (AES), європейського (NESSIE) та вітчизняного конкурсів).

Виявлені переваги і недоліки розповсюджених БШ. ГОСТ 28147-89 хоч і забезпечує практичну стійкість, але для нього вже розроблені теоретичні методи криптоаналізу. Зараз його замінюють шифри СТБ 34.101.31-2007, ДСТУ 7624:2014, ГОСТ Р 34.12-2015. Оскільки AES реалізовано в багатьох мікросхемах на апаратному рівні, то дедалі більше підлягають сумніву пристрої, захищені AES на апаратному рівні (табл.1), оскільки проведені дослідження – це статті, у яких описано як саме реалізована уразливість у реалізаціях AES (рис.1). Тому світові лідери IT-індустрії вже використовують нові алгоритми, наприклад Google в 2014 р. впровадив шифр ChaCha20 для захисту каналів зв'язку пристроїв на базі Android. ДСТУ 7624:2014 (БШ «Калина») розроблений під малоресурсну (lightweight) криптографію, яка передбачає компактну реалізацію і мінімальне енергоживлення, забезпечуючи прийнятний рівень криптостійкості і має порівняно малу швидкодію.

Алгоритми AES і ДСТУ 7624:2014 основані на архітектурі «Square» (квадрат), що являє собою прямі перетворення шифрованих блоків, які представлені у вигляді двувимірного байтового масиву. Алгоритм ДСТУ 7624:2014 має більш повільну апаратну реалізацю. Алгоритм ГОСТ 28147-89 базується на архітектурі «мережа Файстеля», недоліком якої порівняно з використовуваною в алгоритмах AES і ДСТУ 7624:2014 є те, що за один раунд шифрується тільки половина блоку. Шифри AES і ДСТУ 7624:2014 використовують 2D-перетворення, а шифри 3DES і ГОСТ 28147-89 – 1D-перетворення.

Таблиця 1

Порівняльний аналіз сучасних шифрів на мікроконтролерах з архітектурою AVR і ARM, а також FPGA

Шифр	Довжина ключа, (біт)	Завантаженість МК, (%)	Статистична стійкість	Уразливість (backdoor)	Ресурсоємність, (%)
AES	128, 192, 256	10…90	1	Так	10…100
3DES	112, 168	70	0,9	Так	30
RC4	40–1024	10	0,7	Так	50
ДСТУ 7624:2014	128, 256, 512	80	1	Ні	100
ГОСТ Р 34.12-2015	256	80	1	Ні	100

Виявлені апаратні уразливості шифраторів (англ. backdoor або trapdoor).

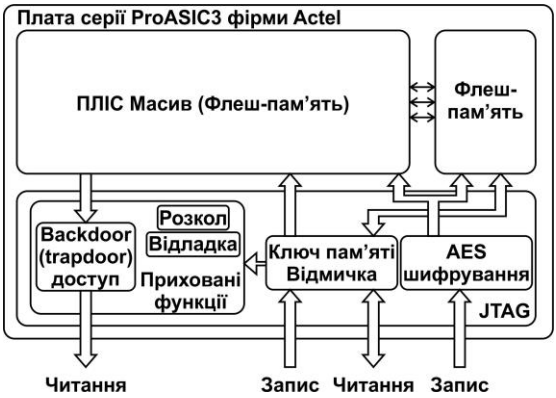

Рисунок 1 – Структурна схема плати серії ProASIC3 фірми Actel з апаратною уразливістю шифру AES

Розглянуті ітеративні БШ і їх структура, принципи побудови, стандартизація і застосування БШ. Наведені способи оцінювання захищеності інформації під час використання БШ: диференціальний, лінійний, інтегральний, статистичний та інші методи криптоаналізу.

Другий розділ присвячено розробленню методів формування динамічно керованих примітивів лінійного розсіювання, нелінійній заміні та «ковзному

кодуванню» на основі узагальнених перетворень Грея та матриць Галуа для тривимірного простору.

У класичній криптографії використовуються одновимірні і двовимірні криптографічні перетворення. Зараз розробляються носії інформації, що орієнтовані на зберігання тривимірних даних і їх оброблення. Постає завдання аналізу існуючих і синтезу нових методів оброблення тривимірних структур.

Основна класифікація криптошифрів така:

1. За способом організації перетворень – потокові, блокові.

2. За числом ключів шифрування – безключові (геш-функції), одноключові (симетричні), двоключові (асиметричні).

Доцільно ввести класифікацію вже існуючих шифрів за розмірністю простору, у якому представлені ключі і дані:

– 1D (DES, GOST);

– 2D (AES).

Ланцюжок криптографічних перетворень, ланками якого є 1D- і 2D-шифри, природним чином стимулює залучення криптологів в область дослідження майже не розроблених алгоритмів і засобів 3D-шифрування, у яких ключі і дані повинні бути упаковані у тривимірні об'єкти – кубічні просторові матриці.

Для підвищення швидкості роботи при зменшенні ресурсоємності шифратора запропоновано ***метод синтезу тривимірних узагальнених матриць Галуа*** (УМГ) для криптографічних перетворень, який грунтується на тривимірних операторах.

Будь-яка система з n^3 елементів $A_{i,j,k}$ $(i,j,k=1,2,\ldots,n)$ поля $GF(p)$, розташованих у точках тривимірного простору, що визначається координатами i,j,k, називається *тривимірною (кубічною) матрицею n-го порядку над* полем $GF(p)$ і позначається як $\|A_{i,j,k}\|$ або $Q^{(n)}$. Сукупність елементів матриці $\|A_{i,j,k}\|$ з фіксованим значенням індекса i називається *перетином орієнтації* (i) та для простоти позначають так $A_1, A_2, \ldots, A_n$. Аналогічно визначаються перетини орієнтацій (j) і (k).

Нехай $\circ$ це деякий оператор, завдяки якому перетини $A_1, A_2, \ldots, A_n$ утворюють кубічну матрицю

$$Q^{(n)} = A_1 \circ A_2 \circ \cdots \circ A_n ,$$

що дозволяє формально ввести правила:

1. $\overline{Q}^{(n)} = \overline{A}_n \circ \overline{A}_{n-1} \circ \cdots \circ \overline{A}_2 \circ \overline{A}_1$.
2. $\det\left(Q^{(n)}\right) = \det(A_1) \circ \det(A_2) \circ \cdots \circ \det(A_n)$.

Як оператор $\circ$ може бути обраний оператор модульного множення $\otimes$, конкатенації $\|$ тощо.

Завдяки цікавим криптографічним властивостям, як матриці $A_1, A_2, \ldots, A_n$ обрані так звані узагальнені примітивні матриці Галуа $G^{(n)}_{f,\theta}$. Термін «матриця Галуа» запозичений з теорії кодування і криптографії, у якій широко використовуються

генератори ПВП в конфігурації Галуа, що засновані на лінійних регістрах зсуву (ЛРЗ) з лінійними зворотними зв'язками. Відомо, що для того, щоб ЛРЗ був регістром (генератором) максимального періоду, відповідний поліном зворотного зв'язку повинен бути примітивним поліномом. Кожен лінійний генератор ПВП на ЛРЗ може бути представлений відповідною матрицею Галуа, що формує ту саму послідовність, що і генератор ПВП.

Синтез примітивних узагальнених матриць Галуа n-го порядку відбувається за методом діагонального заповнення, суть якого полягає в наступному: у нижньому рядку матриці записується примітивний елемент поля $GF\left(2^n\right)$, що породжується незвідним поліномом f_n, який не обов'язково має бути примітивним. Наступні рядки матриці утворюються зсувом попереднього рядка на один розряд ліворуч. Якщо при цьому старший ненульовий розряд рядка виходить за межі матриці, то поліноми, що відповідають таким рядкам, приводяться до залишку за модулем f_n і рядок знову стане n розрядним.

Із теорії поліномів однієї змінної x відомо, що множення довільного полінома $\omega_k(x)$ ступеня k на x еквівалентно його зсуву на один розряд ліворуч і, відповідно, збільшення на один ступінь полінома. Або, іншими словами,

$$x \cdot \omega_k(x) = \omega_{k+1}(x),$$

що дає можливість виконати такі перетворення над $G_{f,\omega}^{(n)}$

$$G_{f,\omega}^{(n)} \Rightarrow \begin{pmatrix} x^{n-1} \cdot \omega \\ x^{n-2} \cdot \omega \\ \vdots \\ x \cdot \omega \\ \omega \end{pmatrix} \bmod f_n = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \vdots \\ x \\ 1 \end{pmatrix} \bmod f_n = \omega \cdot$$

Твердження. *Узагальнені матриці Галуа* $G_{f,\omega}^{(n)}$ *порядку* n *над незвідними поліномами* f_n *ступеня* n *з коефіцієнтами* $a_i \in GF(p)$, $i = \overline{0,n}$ *ізоморфні їх утворюючим елементам* ω*, які належать полю* $GF\left(p^n\right)$ *довільної характеристики* p*, тобто*

$$G_{f,\omega}^{(n)} \cong \omega .$$

Таким чином, між $G_{f,\omega}^{(n)}$ і їх утворюючими елементами ω (зовсім не обов'язково примітивними) існує взаємно однозначна відповідність (*ізоморфізм* або *бієкція*).

Наслідок 1. Узагальнені матриці Галуа $G_{f,\omega}^{(n,2)}$ невироджені за будь-яких параметрів f_n і ω, оскільки утворені лінійно незалежними рядками (стовбцями) матриць.

Наслідок 2. Для того щоб піднести матрицю $G_{f,\omega}^{(n,2)}$ до ступеня k, достатньо вирахувати утворюючий елемент $\omega_k = \omega^k (\mathrm{mod}\, f_n)$ і за методом діагонального заповнення скласти матрицю $G_{f,\omega_k}^{(n,2)}$ за модулем f_n.

Наслідок 3. Мінімальне ненульове значення ступеня e, яке забезпечує рівність $G_{f,\omega}^{e} = E$, збігається з порядком ord елемента ω, утворюючого матрицю $G_{f,\omega}^{(n,2)}$.

Наслідок 4. Матриця Галуа $G_{f,\omega}^{(n,2)}$ примітивна, якщо примітивним є утворюючий її елемент ω, тобто якщо $\omega = \theta$.

Наслідок 5. Матриці Галуа $G_{f,\omega_1}^{(n,2)}$ і $G_{f,\omega_2}^{(n,2)}$, $\omega_1 \neq \omega_2$ комутативні, оскільки є елементами однієї і тієї самої мільтиплікативної групи GF^* максимального порядку, складеної зі ступеней матриці $G_{f,\theta}^{(n,2)}$, довільний примітивний утворюючий елемент якої θ належить полю $GF(p^n)$, породженому НП f_n.

Наслідок 6. Довільні алгебричні перетворення (підсумовування, віднімання, множення і ділення) над матрицею Галуа або сукупністю матриць Галуа ізоморфні таким самим перетворенням над утворюючими елементами цих матриць.

Наслідок 7. Добуток матриці Галуа $G_{f,\omega}^{(n,2)}$ на вектор n-го порядку $\overline{V}$ збігається з добутком цього вектора на утворюючий елемент ω матриці G, тобто $G_{f,\omega}^{(n,2)} \cdot \overline{V} = (\overline{V} \cdot \omega) \mathrm{mod}\, f_n$.

Для реалізації запропонованого протоколу обміну секретними ключами шифрування по відкритих каналах зв'язку використовуються подібні матриці Галуа

$$^{*}G_{f,\omega}^{(n,2)} = P^{-1} \cdot G_{f,\omega}^{(n,2)} \cdot P,$$

де $P-$ матриця подібності.

Як матрицю подібності можа прийняти будь-яку невироджену матрицю. Для простоти використовується переставна (комутативна) матриця.

Для підвищення стійкості шифратора запропоновано **метод односторонніх функцій з використанням обернених матриць Галуа** (ОМГ).

На відміну від початкових УМГ $G_{f,\omega}^{(n,2)}$ подібні матриці $^{*}G_{f,\omega}^{(n,2)}$, залишаючись комутативними, втрачають властивість ізоморфізму. Ця особливість подібних матриць Галуа саме і забезпечує можливість побудови односторонніх функцій, які використовуються в запропонованих протоколах обміну ключами шифрування.

Визначення. *Функція* φ: $X \to Y$ *називається односторонньою, якщо* $\varphi(x)$ *може бути легко обчислена для кожного* $x \in X$, *тоді як майже для всіх* $y \in X$ *обчислення такого* $x \in X$, *що* $\varphi(x) = y$ *(за умови, що хоча б один такий* x *існує) є складним*.

Нижче наведені короткі пояснення до пропонованого ОМГ-протоколу обміну ключами у відкритих комунікаційних мережах. Протоколом передбачається формування абонентами мережі нової односторонньої функції, за допомогою якої і обчислюється загальний секретний ключ шифрування.

Як відкритий ключ протоколу прийняті: вектор ініціалізації *V*, який є *n*-бітовим вектором; незвідний двійковий поліном f_n ступеня *n* і перестановки *P*-матриця *n*-го порядку. Кожен з абонентів мережі *A* і *B* виробляє секретні *n* - бітові ключі ω_α і ω_β відповідно. Загальний секретний ключ *K* визначається в результаті виконання абонентами таких двох етапів обчислень:

Етап 1. Абонент *A* генерує випадковий вектор ω_α, знаходить спочатку ОМГ $G^{(n)}_{f,\omega_\alpha}$, потім подібну матрицю ${}^*G^{(n)}_{f,\omega_\alpha}$, обчислює вектор $V_\alpha = V \cdot G^{(n)}_{f,\omega_\alpha}$ і напрямляє його абоненту *B*. Аналогічні операції здійснює абонент *B*, визначаючи вектор $V_\beta = V \cdot G^{(n)}_{f,\omega_\beta}$, який напрямляє абоненту *A*. Вектори V_α і V_β саме і є тими односторонніми функціями φ, які побудовані на основі подібних ОМГ.

Етап 2. Абонент *A* примножує отриманий від абонента *B* вектор V_β на свою секретну матрицю ${}^*G^{(n)}_{f,\omega_\alpha}$, формуючи ключ

$$K_\alpha = V_\beta \cdot {}^*G^{(n)}_{f,\omega_\alpha} = V \cdot {}^*G^{(n)}_{f,\omega_\beta} \cdot {}^*G^{(n)}_{f,\omega_\alpha} = V \cdot (P^{-1} \cdot G^{(n)}_{f,\omega_\beta} \cdot P) \cdot (P^{-1} \cdot G^{(n)}_{f,\omega_\alpha} \cdot P) = V \cdot \left(P^{-1} \cdot G^{(n)}_{f,\omega_\beta} \cdot G^{(n)}_{f,\omega_\alpha} \cdot P\right) \quad (1)$$

Такі самі ж обчислення виконує абонент B, розраховуючи вектор

$$K_\beta = V \cdot \left(P^{-1} \cdot G^{(n)}_{f,\omega_\alpha} \cdot G^{(n)}_{f,\omega_\beta} \cdot P\right). \quad (2)$$

Оскільки ОМГ $G^{(n)}_{f,\omega_\alpha}$ і $G^{(n)}_{f,\omega_\beta}$ комутативні, зі співвідношень (1) і (2) випливає, що $K_\alpha = K_\beta$ і, отже, обидва абоненти мережі отримують однаковий секретний ключ шифрування *K*.

Якщо ж замість подібних матриць ${}^*G^{(n)}_{f,\omega}$ використовувати звичайні ОМГ $G^{(n)}_{f,\omega}$, то через їх ізоморфізм супротивник, перехопивши вектори V_α і V_β, може обчислити секретні ключі ω_α і ω_β, оскільки в загальному випадку

$$V_\gamma = V \cdot G^{(n)}_{f,\omega_\gamma} = V \cdot \omega_\gamma \geq (\mathrm{mod}\ f_n),\ \gamma = \alpha \text{ або } \beta. \quad (3)$$

З огляду на те, що *V* і f_n – відомі величини, противник, розраховує рівність (3) щодо ω_γ, обчислює ключі ω_α і ω_β, це призводить до зламу загального секретного ключа *K*.

Структурно-аналітична модель примітиву ShiftRow, призначена для здійснення стохастичного колового прокручування блоків, що перетворюються (рис.2). Напрямок залежить від раундового ключа RK_i.

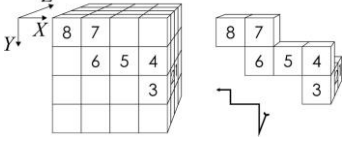

Рисунок 2 – Структура Shift 3D

Структурно-аналітична модель примітиву SlideCode ковзного кодування (рис.3). В результаті цього раундовий ключ i-го блоку ($i \geq 2$) стає залежним як від базового раундового ключа RK_i, так і від попередніх $i-1$ блоків даних, що перетворюються.

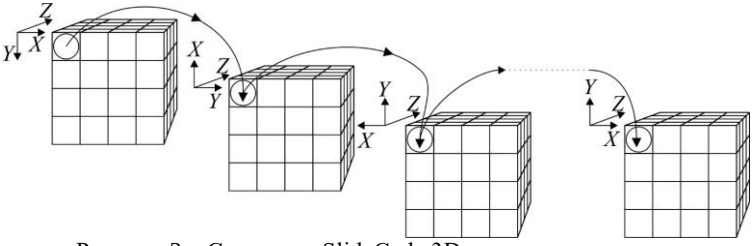

Рисунок 3 – Структура SlideCode 3D ковзного кодування

Структурно-аналітична модель примітиву SubByte 3D (рис. 4) взаємодія двовимірного S-блоку підстановки з перетином тривимірної матриці.

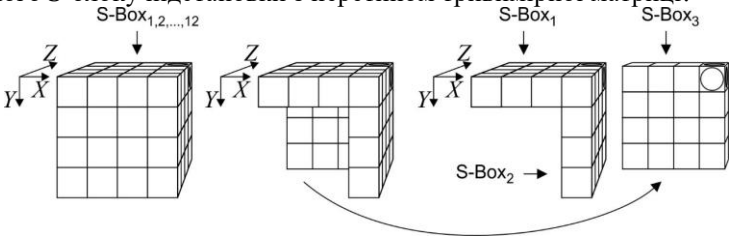

Рисунок 4 – Структура примітиву SubByte 3D

У третьому розділі на основі запропонованих методів і математичних моделей розроблені криптографічні примітиви для блокового і потокового тривимірного шифрування даних.

Розв'язані завдання синтезу й аналізу 3D криптографічних примітивів на основі запропонованих методів тривимірних криптографічних перетворень. Перелік основних примітивів (розроблених як тривимірні), з яких сформовано шифр, показаний на рис. 5 та наведено нижче:

ShiftRow – стохастична прокрутка блоку; SlideCode – ковзне кодування; SubByte – нелінійна підстановка байтів блоку; PermutBox – стохастична перестановка 16-бітних слів блоку.

Програмні цикли RSB (Round-Step-Block) шифру виконують такі функції: зовнішній цикл (i) задає крок шифрування; внутрішній цикл (i) визначає r-раундове шифрування. Керування примітивами здійснюється змістом раундових ключів RK (як базових, так і блокових), структура яких має вигляд (рис. 5).

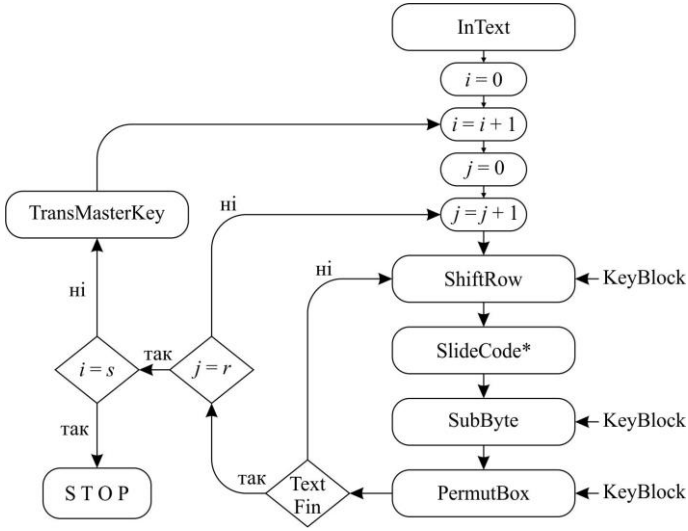

Рисунок 5 – Узагальнена структурна схема RSB-шифру

Байт-орієнтовне потокове шифрування на основі рівномірно щільних блоків нелінійної підстановки засновано на використанні технічного рішення, відображеного на рис. 6 і 7.

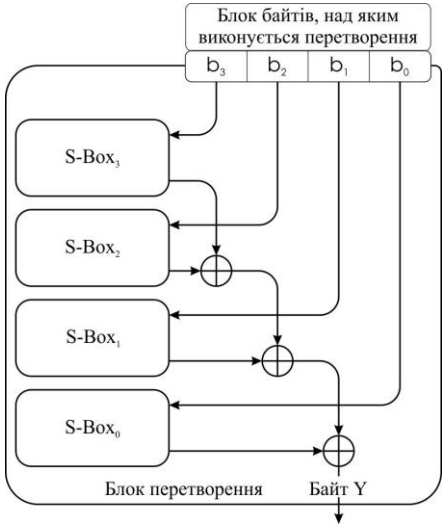

Рисунок 6 – Блок перетворення байтів

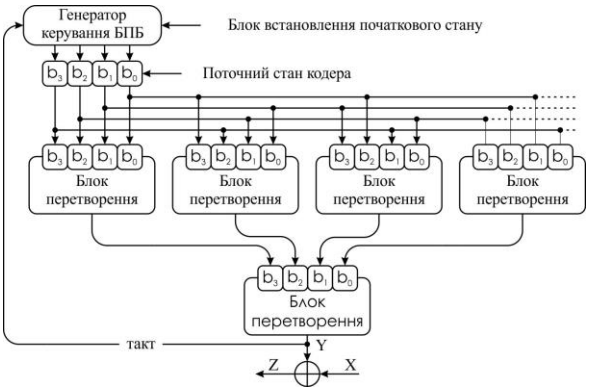

Рисунок 7 – Структурно-логічна схема алгоритму потокового шифрування

Відбувається динамічна модифікація SBox в блоках перетворення ключем шифрування.

У **четвертому розділі** дисертації метод перевірено на розробленому апаратно-програмному забезпеченні; розроблено пакети програмного забезпечення для оцінювання ефективності блокових RSB і потокових байт-орієнтованих ПНП (табл.2); створено алгоритмічно-програмне забезпечення та комплекс апаратних засобів захисту командно-телеметричної інформації в каналах зв'язку НПК-БПЛА; проведено лабораторні випробування апаратно-програмних засобів захисту командно-телеметричної інформації в каналах зв'язку НПК з бортом БПЛА.

Таблиця 2

Аналітичні верхні межі стійкості відносно методів ЛДК шифрів

Розмір ключа K (біт)	RSB-64-3D		M3DCrypt	
	Диференціальний криптоаналіз	Лінійний криптоаналіз	Диференціальний криптоаналіз	Лінійний криптоаналіз
128	$EDP(\Omega) \le 2^{-193}$	$ELP(\Omega) \le 2^{-186}$	$EDP(\Omega) \le 2^{-185}$	$ELP(\Omega) \le 2^{-179}$
256	$EDP(\Omega) \le 2^{-257}$	$ELP(\Omega) \le 2^{-247}$	$EDP(\Omega) \le 2^{-263}$	$ELP(\Omega) \le 2^{-237}$

Тестування відбувалось над текстовими, графічними, архівними і порожніми інформаційними послідовностями (файлами). Результати тестування шифрограм показали, що шифри на базі 3D, порівняно з 2D перетвореннями проходять більшу кількість криптографічних статистичних тестів пакетів NIST STS та DIEHARD.

ВИСНОВКИ

У дисертаційній роботі на основі апарату 3D модулярної алгебри розв'язано актуальне науково-технічне завдання щодо розроблення методів побудови симетричних криптосистем (блокових та потокових шифрів) для підвищення ефективності захисту інформації.

Основні наукові та практичні результати дисертаційної роботи полягають у такому:

1. Проведено аналіз сучасних криптографічних методів захисту інформації за критеріями стійкості, швидкодії та необхідних ресурсів для розрахунків, що дало можливість виявити переваги за зазначеними критеріями шифрів на основі 2D перетворень над 1D, а також обґрунтувати необхідність розроблення нових методів за рахунок використання в шифраторах керованих 3D криптографічних перетворень.

2. Розроблені методи формування динамічно керованих примітивів лінійного розсіювання, нелінійної заміни та «ковзного кодування» на основі узагальнених перетворень Грея та матриць Галуа для тривимірного простору, що дало можливість запропонувати клас симетричних алгоритмів шифрування (потокових і блокових шифрів), орієнтованих на максимально можливе використання керованих 3D криптографічних примітивів. За рахунок того, що всі перетворення, які виконуються алгоритмом, стають залежними не лише від секретного ключа, але і від даних, що шифруються. Тим самим примітиви набувають властивість керованих криптоперетворень.

3. На основі запропонованих алгоритмічних рішень розроблено методи криптографічної обробки даних (блокового, потокового) тривимірного шифрування даних, що сприяло підвищенню стійкості, швидкодії і зменшенню необхідних ресурсів для забезпечення криптографічного захисту інформації за рахунок розроблених алгоритмічних методів побудови просторових кубічних матриць четвертого порядку, які використовуються для зберігання ключів і даних. В основу синтезу просторових матриць покладені так звані узагальнені матриці Галуа. На відміну від відомих (класичних) матриць Галуа, які будуються виключно на основі примітивних незвідних поліномів, узагальнені матриці Галуа можуть бути побудовані за допомогою поліномів, які не обов'язково повинні бути примітивними, за умови, що примітивним є елемент, породжуючий матрицю Галуа, завдяки цьому значно поширюється множина просторових матриць Галуа.

4. Розроблено апаратно-програмне забезпечення і проведені лабораторні випробування засобів захисту командно-телеметричної та відеоінформації в каналах зв'язку наземного пункту керування з безпілотним літальним апаратом, це надало можливість суттєво збільшити як довжину періоду гамма-послідовності, так і швидкість криптографічних перетворень за рахунок запропонованого оригінального байт-орієнтовного потокового шифрування даних на основі рівномірно щільних блоків нелінійної підстановки.

5. Практичне значення отриманих результатів полягає в тому, що: а) запропоновано спосіб тривимірних перетворень блокових та потокових шифрів (БШ і ПШ) для побудови більш ефективних криптосистем; б) розроблені та впроваджені алгоритми симетричного блокового і 3DMatrix потокового шифрування інформації, які доведені до рівня програмної реалізації на мовах C# і C++, що дають можливість підвищити ефективність криптографічного захисту інформації; в) розроблено ПЗ на основі запропонованих шифрів, що сприяло проведенню експериментального дослідження запропонованих рішень для криптографічного захисту командно-телеметричної інформації в каналі зв'язку НПК-БПЛА; г) за результатами дисертаційних досліджень отримано дев'ять патентів України на «Спосіб криптографічного захисту інформації».

6. Результати дисертаційної роботи впроваджено у навчальному процесі кафедри електроніки Національного авіаційного університету (акт впровадження від 13.02.17 р.), кафедри виробництва приладів Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (акт впровадження від 15.02.17 р.) та в науково-технічних розробках ТОВ «Агфар» (акт впровадження від 07.02.17 р.), ТОВ «Гратис, Лтд» (акт впровадження від 13.02.17 р.), що підтверджено відповідними актами впровадження.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. *Shutko V. N.* Possibility of images recognition in navigation by artificial system / V.N. Shutko, O.M. Klyuchko, D.O. Navrotskyi // Methods and Systems of Navigation and Motion Control (MSNMC): 2014 IEEE 3rd International Conference. – 2014. – P. 165–169.

2. *Белецкий А. Я.* Синтез систем дискретных Уолша-подобных секвентных функций восьмого порядка / А. Я. Белецкий, Д. А. Навроцкий // Безпека інформації. – 2016. – Т. 22, № 2. – С. 163–174.

3. *Белецкий А. Я.* Алгоритм байт-ориентированного поточного шифрования на основе равномерно плотных блоков нелинейной подстановки // А. Я. Белецкий, Д. А. Навроцкий, А.И. Семенюк // Захист інформації. – 2016. – Т. 18, № 2. – С. 114–123.

4. *Навроцький Д.О.* Криптографічна система захисту радіоканалів БПЛА від несанкціонованого втручання / Д. О. Навроцький // Безпека інформації. – 2014. – Т. 20, № 3. – С. 248–252.

5. *Белецкий А.* Программно-моделирующий комплекс SCSPS алгоритма поточного шифрования / А. Белецкий, Д. Навроцкий, А. Семенюк // Захист інформації. – 2014. – Т. 16, № 2. – С. 113-121.

6. *Программно-моделирующий* комплекс BPC алгоритма поточного шифрования и помехоустойчивого кодирования видеосигналов, передаваемых с борта БПЛА / [А. Я. Белецкий, А. В. Максименко, Д. А. Навроцкий та інші] // Захист інформації. – 2014. – Т. 16, № 3. – С. 184–191.

7. *Программно-моделирующий* комплекс криптографических AES-подобных примитивов нелинейной подстановки / [А. А. Белецкий, А. Я. Белецкий, Д. А. Навроцкий, А.И. Семенюк] // Захист інформації. – 2014. – Т. 16, № 1. – С. 12–22.

8. *Примитивные* полиномы в криптографических приложениях / А. Я. Белецкий, Е. А. Белецкий, Р. Ю. Кандиба, Д. А. Навроцкий // Сучасний захист інформації. – 2011. – № 4. – С. 5–18.

9. *The* set of program models for ecological monitoring technical system based on principles of biophysics / [O. M. Klyuchko, V. N. Shutko, D. O. Navrotskyi, A. M. Mikolushko] // Електроніка та системи управління. – 2014. – № 4. – С. 135–142.

10. *Навроцький Д.О.* Дослідження результатів стеганографічного приховування повідомлень у файлах зображення // Д.О. Навроцький / Вісник Національного технічного університету України «Київський політехнічний інститут» – Серія «Радіотехніка. Радіоапаратобудування». – 2012. – № 50. – С.121–128.

11.Двоичные квазиэквидистантные и отраженные коды в смешанных системах счисления / [А. Я. Белецкий, Е. А. Белецкий, Р. Ю. Кандиба, Д. А. Навроцкий] // Вісник СумДУ. Серія «Технічні науки». – 2012. – № 1. – С. 42–58.

12.Навроцький Д.О. Методи комп'ютерної стеганографії / Д. О. Навроцький // Вісник Національного технічного університету України «Київський політехнічний інститут» – Серія «Радіотехніка. Радіоапаратобудування». – 2007. – № 35. – С. 105–108.

13.Навроцький Д.О. Представлення і прогнозування ефективності нового протоколу оцінки якості реалізації розроблюваних алгоритмів комп'ютерної стеганографії / Д. О. Навроцький // Вісник Національного технічного університету України «Київський політехнічний інститут» – Серія «Радіотехніка. Радіоапаратобудування». – 2007. – № 34. – С. 150–156.

*14.*Патент України на корисну модель № 94189, МПК G09C 1/00 (2014.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201312117 ; заявл. 16.10.2013; опубл. 10.11.2014, Бюл.№ 21 – 5 с. : іл.

*15.*Патент України на корисну модель № 95753, МПК G09C 1/00 (2015.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201406124 ; заявл. 04.06.2014; опубл. 12.01.2015, Бюл.№ 1 – 5 с. : іл.

*16.*Патент України на корисну модель № 98731, МПК G09C 1/00 (2015.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201410960 ; заявл. 07.10.2014; опубл. 12.05.2015, Бюл.№ 9 – 5 с. : іл.

*17.*Патент України на корисну модель № 99696, МПК G09C 1/00 (2015.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201404060 ; заявл. 16.04.2014; опубл. 25.06.2015, Бюл.№ 12 – 5 с.

*18.*Патент України на корисну модель № 99698, МПК G09C 1/00 (2015.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201404063 ; заявл. 16.04.2014; опубл. 25.06.2015, Бюл.№ 12 – 5 с.

*19.*Патент України на корисну модель № 113149, МПК G09C 1/00 (2016.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201608329 ; заявл. 28.07.2016; опубл. 10.01.2017, Бюл.№ 1 – 5 с.

*20.*Патент України на корисну модель № 113150, МПК G09C 1/00 (2016.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201608330 ; заявл. 28.07.2016; опубл. 10.01.2017, Бюл.№ 1 – 5 с.

*21.*Патент України на корисну модель № 113464, МПК G09C 1/00 (2016.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201608330 ; заявл. 28.07.2016; опубл. 10.01.2017, Бюл.№ 2 – 5 с.

22. Патент України на корисну модель № 113465, МПК G09C 1/00 (2016.01). Спосіб криптографічного перетворення інформації / Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. – № u201608330 ; заявл. 28.07.2016; опубл. 10.01.2017, Бюл.№ 1 – 5 с.

23. Навроцький Д.О. Шифратор на МК під'єднаний до ПК через USB / О.Д. Навроцький // Сучасні тенденції розвитку системного програмування: науково-практична конференція. – 25-26 листоп. 2015р.: тези доп. – К., 2015. – С. 82.

24. Навроцький Д.О. Перехоплення і модифікація даних за допомогою перехідника USB-UART / Д.О. Навроцький // ITSEC: матеріали V міжнародної науково-технічної конференції. – 19-22 трав. 2015р.: тези доп. – К.: НАУ, 2015. – С. 36.

25. Навроцький Д.О. Несанкціоноване перехоплення і модифікація даних каналу зв'язку БПЛА / Д. О. Навроцький // Матеріали XII міжнародної науково-технічної конференції «АВІА-2015». – 28–29 квіт. 2015р.: тези доп. – К. НАУ, 2015. – Т.1. – С. 2.50–2.53.

26. Навроцький Д.О. Захист радіоканалів БПЛА від несанкціонованого втручання / Д. О. Навроцький // Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM: науково-практична конференція. – 17–19 листоп. 2014 р.: тези доп. – К., 2014. – С.164.

27. Навроцький Д.О. Криптоаналіз з застосуванням ланцюгових дробів / Д. О. Навроцький // Розвиток наукових досліджень 2013: IX міжнародна науково-практична конференція. – 25–27 листоп. 2013 р.: тези доп. – К., 2013. – С.9.

28. Navrotskyi D.O. Hardware and software complex with encrypted communication channel of Ground-to-UAV-to-Ground / D.O. Navrotskyi // Проблеми навігації і управління рухом: Всеукраїнська науково-практична конференція молодих учених і студентів. – 18–20 листоп. 2013 р.: тези доп. – К., 2013. – С.9.

29. Navrotskyi D.O. Ground-to-UAV-to-Ground hardware and software complex with encrypted communication channel / D.O. Navrotskyi // System analysis and information technologies (SAIT): 15-th International conference SAIT 2013, Kyiv, Ukraine, May 27–31, 2013. Proceedings. – ESC «IASA» NTUU «KPI», 2013. – 516 p.

30. Навроцький Д.О. Апаратно-програмний комплекс «Земля – БПЛА – Земля» з захищеним шифрованим каналом зв'язку / Д. О. Навроцький // Наукоємні технології: Науково-технічна конференція студентів та молодих учених, 12–16 листоп. 2012 р.: тези доп. – К., 2012. – С. 9.

31. Навроцький Д.О. Апаратно-програмний комплекс із шифрованим каналом зв'язку «Земля – БПЛА – Земля» / Д. О. Навроцький // Проблеми та перспективи розвитку авіації та космонавтики: Всеукраїнська науково-практична конференція молодих учених і студентів, 24–25 жовт. 2012 р.: тези доп. – К., 2012. – С. 223.

32. Beletsky A. Ja. Matrix analogues of the Diffi-Hellman protocol / A. Ja. Beletsky, O.I. Volivach, R. Ju. Kandiba, D. O. Navrotskyi // Safety in Aviation and Space Technologies: Proceedings. The firth world congress «Aviation in the XXI-st century», September 25-27, 2012,: abstracts, – K., 2012. – P. 1.7.5 – 1.7.9.

АНОТАЦІЯ

Навроцький Д. О. Методи побудови симетричних криптографічних шифрів з використанням тривимірних керованих перетворень. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Національний авіаційний університет, Київ, 2017.

Дисертаційна робота присвячена розв'язанню актуального науково-практичного завдання розроблення і дослідження нових більш ефективних методів побудови симетричних криптосистем (блокових та потокових шифрів) для підвищення ефективності захисту інформації. Отримані в дисертаційній роботі результати можуть бути використані для підвищення ефективності (захищеності, швидкості роботи, зменшення ресурсоємності) систем захисту. У роботі розроблено методи тривимірних матричних перетворень, на основі яких побудовані динамчно керовані криптографічні примітиви. Розроблені елементи узагальнених тривимірних перетворень Грея, які окрім класичних (лівосторонніх) і так званих правосторонніх та складених кодів містять рандомізовані коди Грея, на основі яких вирішені окремі проблеми побудови динамічно керованих криптографічних примітивів. Синтезовані тривимірні криптографічні примітиви перемішування, нелінійної заміни, матричного перетворення, стохастичного циклічного зсуву, «ковзного» кодування. Удосконалено методики синтезу примітивних матриць Галуа і Фібоначчі, а також їх сполучених варіантів над простими полями Галуа характеристики 2, що дозволило як розширити множину узагальнених генераторів псевдовипадкових послідовностей, так і запропонувати нові підходи до розв'язання проблеми формування таємних ключів шифрування абонентами мережі з відкритими каналами зв'язку. Отримали подальший розвиток методи симетричного блокового криптографічного перетворення інформації з динамічно керованими параметрами шифрування (криптографічні перетворення виконуються в тривимірному простору і в алгоритмах шифрування здійснюється оперативна модифікація параметрів криптографічних примітивів під час переходу до чергового блоку тексту, що перетворюється). Розроблено криптографічний протокол для захисту командної і телеметричної інформації БПЛА. Розроблено, виготовлено і апробовано апаратно-програмні реалізації 3D шифраторів.

Ключові слова: захист електронних інформаційних ресурсів, блокові шифри, потокові шифри, метод побудови блокових шифрів з рандомізованими вузлами замін, лінійний та диференціальний криптоаналіз, тривимірні криптографічні перетворення, захист командної і телеметричної інформації БПЛА.

АННОТАЦИЯ

Навроцкий Д. А. Методы построения симметричных криптографических шифров с использованием трехмерных управляемых преобразований. **–** Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 «Системы защиты информации». **–** Национальный авиационный университет, Киев, 2017.

Диссертация посвящена решению актуальной научно-практической задачи разработки и исследования новых более эффективных методов построения симметричных криптосистем (блочных и поточных шифров) для повышения эффективности защиты информации. Полученные в диссертационной работе результаты могут быть использованы для повышения эффективности (защищенности, скорости работы, уменьшению ресурсоемкости) систем защиты. В работе были рассмотрены криптоаналитические линейный, дифференциальный методы, атака бумерангом, интегральный метод, алгебраический, интерполяционный, атака с помощью боковых каналов, скользящая атака, статистические методы. Приведены основные понятия и определения для трехмерных расчетов, указаны операторы для работы с линейными и нелинейными трехмерными преобразованиями. Показано как проводить параллельные вычисления при работе с трехмерными структурами данных. Выявлены особенности трехмерных преобразований, которые отсутствовали в двухмерных и одномерных, что позволило сэкономить память и ускорить быстродействие при выполнении криптографических примитивов с использованием трехмерных структур и операций над ними. В работе разработаны методы трехмерных матричных преобразований, на основе которых построены динамически управляемые криптографические примитивы. Разработаны элементы обобщенных трехмерных преобразований Грея, которые кроме классических (левосторонних) и так называемых правосторонних и так же составных кодов содержат рандомизированные коды Грея, на основе которых решены отдельные проблемы построения динамически управляемых криптографических примитивов; разработаны структурно-аналитические модели и на их основе синтезированы трехмерные криптографические примитивы перемешивания, нелинейной замены, матричного преобразования, стохастического циклического сдвига, «скользящего» кодирования. Разработаны блочный и поточный шифры с модификациями. Параметры криптографических примитивов зависят от вида аддитивных компонент, которые влияют на структуру шифров и последовательность выполнения криптографических примитивов. Параметры криптографических примитивов определяют направление выполнения преобразований и систему координат для них. Усовершенствованы методики синтеза примитивных матриц Галуа и Фибоначчи, а также их совмещенные варианты, над простыми полями Галуа характеристики 2, что позволило как расширить множество обобщенных генераторов псевдослучайных последовательностей, так и предложить новые подходы к решению проблемы формирования тайных ключей шифрования абонентами сети с открытыми каналами связи. Получили дальнейшее развитие методы симметричного блочного криптографического преобразования информации с динамически управляемыми параметрами шифрования (криптографические преобразования выполняются в трехмерном пространстве и в алгоритмах шифрования осуществляется оперативная модификация параметров криптографических примитивов при переходе к очередному блоку текста преобразования). Разработан криптографический протокол для защиты командной и телеметрической информации БПЛА и проведены лабораторные испытания, которые показали универсальность предложенного метода для разных платформ. Разработаны, изготовлены и апробированы аппаратно-программные реализации 3D шифраторов.

Ключевые слова: защита электронных информационных ресурсов, блочные шифры, поточные шифры, метод построения блочных шифров с рандомизированными узлами замен, линейный и дифференциальный криптоанализ, трехмерные криптографические преобразования, защита командной и телеметрической информации БПЛА.

ABSTRACT

Navrotskyi D. Methods of Constructing Symmetric Cryptographic Ciphers Using Three-Dimensional Controlled Transformations. – Manuscript.

Dissertation for the Scientific Degree of Candidate of Technical Sciences for Specialty 05.13.21 «Information Security Systems». – National Aviation University, Kyiv, 2017.

The dissertation addresses practical problems in modern cryptography by presenting new and more effective methods of constructing symmetric key cryptosystems (i.e. block and stream ciphers) in order to improve information security. Obtained results prove efficiency increase (improved quality of cryptography, increased speed, improved resource management) of the presented cipher implementation. This work deals with the three-dimensional matrix transformation methods of building dynamically controlled cryptographic primitives. In particular, a generalization of the three-dimensional Gray transformations has been developed, which apart from the classical (left-side) and the so-called right-side and compound code, also includes randomized Gray codes, allowing to solve a number of problems related to constructing dynamically controlled cryptographic primitives. Besides, three-dimensional cryptographic shuffle primitives have been synthesized, as well as primitives for non-linear substitutions, matrix transformation, stochastic cyclic shift and «sliding» encoding. Furthermore, methods for a primitive Galois and Fibonacci matrices synthesis are improved, as are their jointed compounds over finite Galois fields of characteristic two, allowing to expand generalized pseudo-random sequence generators' set, as well as to propose new approaches to a problem of providing secret encryption keys for communication network participants over open channels. A further development in the methods of symmetric block transformation with dynamically controlled parameters of encryption is provided, in particular, the cryptographic transformations are performed in a three-dimensional space and the parameters of cryptographic primitives during encryption are modified each time a new block of text is being processed. Moreover, a cryptographic communication protocol is developed to encode telemetry information of unmanned aerial vehicle. Hardware and software for 3D cipher prototype are manufactured and successfully tested.

Key words: electronic information resources security, block ciphers, stream ciphers, constructing block ciphers with randomized replacement nodes, linear and differential cryptanalysis, three-dimensional cryptographic transformation, security, security of unmanned aerial vehicle.