МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

**КОРКІШКО Леся Мирославівна**



УДК 004.056.53

**Методи та засоби маскованої арифметики для пристроїв систем захисту інформації**

05.13.21 – «Системи захисту інформації»

**Автореферат**

дисертації на здобуття наукового ступеня

кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана в Тернопільському національному економічному університеті Міністерства освіти і науки України.

|  |  |
| --- | --- |
| Науковий керівник: | доктор технічних наук, професор  **Карпінський Микола Петрович,**  технічний Університет у Бєльсько-Бялій (Польща),  завідувач кафедри інформатики та автоматики. |
| Офіційні опоненти: | доктор технічних наук, доцент  **Терейковський Ігор Анатолійович,**  Національний технічний університет України  «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри спеціалізованих комп'ютерних систем; |
|  | кандидат технічних наук  **Хохлачова Юлія Євгеніївна,**  Національний авіаційний університет, доцент кафедри безпеки інформаційних технологій. |

Захист відбудеться «15» червня 2017 р. о 1300 годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, Київ, пр. Космонавта Комарова, 1, аудиторія 11-111.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «\_\_» \_\_\_\_\_\_\_ 2017 р.

В.о. ученого секретаря

спеціалізованої вченої ради

д.т.н., професор В.П. Квасніков

**ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ**

**Актуальність.** Зростання цінності інформації, яка зберігається, обробляється та передається у комп’ютерних системах зумовило зростання актуальності задач забезпечення конфіденційності, цілісності та автентичності інформації при зростанні ймовірності реалізації загроз несанкціонованого доступу до такої інформації. У комп’ютерних системах перелічені задачі часто вирішують шляхом криптографічних перетворень інформації. Сучасні криптографічні перетворення володіють належним рівнем стійкості до їх математичного аналізу з метою обчислення параметрів криптографічних перетворень. З іншого боку, набули широкого розповсюдження методи визначення параметрів криптографічних перетворень на основі аналізу залежності спостережуваних фізичних характеристик комп’ютерних пристроїв які їх реалізують (час обробки, споживаний струм, електромагнітне випромінювання, тощо) від даних, які обробляються – так звані "інженерно-криптографічні атаки". Одним із найбільш небезпечних напрямків атакування пристроїв є інженерно-криптографічні атаки на основі аналізу залежності споживаної потужності (АСП) пристрою від параметрів та даних криптографічного перетворення, де пристрій знаходиться під контролем порушника (введення даних, маніпулювання та встановлення сигналів синхронізації, під’єднання живлення). Відомі рішення для зменшення такої залежності і, як наслідок, значного ускладнення аналізу, передбачають рандомізоване виконання алгоритмів шифрування (перемішування порядку виконання елементарних операцій, випадкова зміна шляху виконання алгоритму), спотворення справжньої залежності характеристик споживаної потужності (введення шуму чи збільшення його рівня), вирівнювання споживаної потужності при обробці різних даних (фільтрування, спеціальні логічні елементи, тощо). Таким рішенням притаманні недоліки в частині їх високої вартості та низької технологічності виготовлення, підвищеного енергоспоживання, зменшеної продуктивності обробки даних, складності програмної реалізації. Тому дослідниками, зокрема Кочером П., Мессергесом Т. був розроблений альтернативний шлях захисту від атак на основі АСП, який полягає у введенні невизначеності у рівень споживаної потужності пристрою шляхом рандомізування проміжних значень, які виникають у процесі обчислень криптографічного перетворення. При цьому дані обробляються у так званому «маскованому представленні» (МП), яке містить хоча б одну випадкову маску та результат виконання деякої операції маскування над початковими даними та усіма масками. У ролі операції маскування використовують операцію додавання за модулем два, що, у деяких випадках, призводить до значного ускладнення методів виконання арифметичних операцій над даними. З огляду на те, що збільшення кількості масок у МП призводить до зменшення залежності споживаної потужності від немаскованих даних та значного ускладнення атак на основі АСП, розробка методів та засобів виконання базових операцій, характерних для криптографічних перетворень шифрування, над даними у МП із довільною кількістю масок, є актуальним напрямком наукових досліджень.

Значний внесок у розвиток захисту інформації від АСП внесли такі вчені як Голік Д., Квісквотер Я., Корон Дж., Кочер П., Мессергес Т., Трічіна Е., Освальд Е. та ін.

Однак, у зазначеній галузі залишається низка завдань, вирішення яких має важливе наукове та практичне значення. З цих позицій, побудова і дослідження методів та засобів виконання складових операцій криптографічних перетворень над даними у МП є *актуальним науковим завданням.*

**Зв'язок роботи з науковими програмами, планами, темами.** Одержані результати дисертаційної роботи відображені у звітах держбюджетних науково-дослідних робіт Тернопільського національного економічного університету «Методи та засоби реалізації алгоритмів захисту інформації стійких до атак на реалізацію» (д.р. № 0105U008181), та «Паралельні методи та засоби реалізації алгоритмів захисту інформації в комп’ютерних мережах з використанням математичного апарату еліптичних кривих» (д.р. № 0109U000035).

**Мета і задачі дослідження.** Метою дисертаційної роботи є підвищення ефективності захисту даних і ключів криптографічних алгоритмів від їх несанкціонованої реконструкції за допомогою інженерно-криптографічних атак на основі аналізу зміни споживаної потужності при реалізації цих алгоритмів у криптографічних операційних блоках термінальних обчислювальних пристроїв комп’ютерних систем за рахунок побудови їх структур на основі операцій над даними у маскованому представленні із довільною кількістю масок.

Для досягнення поставленої мети **необхідно розв’язати такі основні задачі:**

– проаналізувати можливості підвищення рівня захисту інформації від інженерно-криптографічних атак на основі аналізу споживаної потужності при її обробці компонентами шифрування з використанням маскованого представлення у сучасних системах захисту інформації та постановка задач дослідження;

– розробити методи виконання базових операцій для криптографічних операційних блоків, які оперують даними у маскованому представленні: логічних (кон’юнкції, диз’юнкції) із довільною кількістю масок, арифметичних (обчислення зворотнього елемента за модулем 2N, додавання за модулем 2N), табличних операцій, операцій перетворення маскованого представлення даних;

– на основі методів виконання базових операцій над даними у маскованому представленні, розробити структури криптографічних операційних блоків, масштабованих до кількості масок та дослідити їх характеристики складності при їх апаратній реалізації;

– на основі структур криптографічних операційних блоків розробити та експериментально дослідити програмні моделі ядер спеціалізованих апаратно-орієнтованих процесорів симетричного блокового шифрування даних у маскованому представленні.

**Об'єктом дослідження** є процеси виконання арифметичних та логічних операцій у апаратних криптографічних операційних блоках на термінальних обчислювальних пристроях комп’ютерних систем і мереж.

**Предметом дослідження** є алгоритми, методи, моделі, засоби виконання арифметичних та логічних операцій над даними у маскованому представленні для пристроїв захисту інформації.

**Методи дослідження** базуються на основі використання теорій множин, ймовірності та математичної статистики, математичної логіки, на основі методів математичного моделювання алгоритмів та експериментального дослідження прототипів апаратних засобів.

**Наукова новизна одержаних результатів** полягає в наступному:

– вперше запропоновано метод виконання операції диз’юнкції над даними у маскованому представленні, що, за рахунок обчислення функції корекції маски результату з використанням виключно даних у маскованому представленні та їх масок, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції диз’юнкції, масштабованих до кількості масок даних у їх маскованому представленні;

– вперше запропоновано метод перетворення маскованого представлення даних, що, за рахунок використання операції додавання за модулем 2N над даними у маскованому представленні, побудованої на основі маскованих логічних операцій, дозволяє перетворювати масковане представлення даних із арифметичним маскуванням у дані із логічним маскуванням та навпаки, а також використати таке перетворення для створення структур криптографічних операційних блоків, які використовують масковане представлення даних як з логічною, так і з арифметичною маскою;

– отримав подальший розвиток метод виконання операції кон’юнкції над даними у маскованому представленні, що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції кон’юнкції, масштабованих до кількості масок даних у їх маскованому представленні;

– отримав подальший розвиток метод інвертування даних у маскованому представленні у полях виду GF(2N), що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє обробляти дані із довільною кількістю масок, а також використати таке перетворення для побудови структур криптографічних операційних блоків інвертування даних у полях виду GF(2N), які використовують табличні методи виконання операцій у цих полях;

– удосконалено метод табличних перетворень даних у маскованому представленні, що, за рахунок введення додаткового проміжного маскування із узгодженим типом маски вхідних даних, дозволяє виконувати табличні перетворення над вхідними даними як із логічною, так і з арифметичною масками та отримувати результат із заданим типом маскування, а також дозволяє використати таку операцію для побудови структур криптографічних операційних блоків табличної заміни засобів шифрування даних у маскованому представленні.

**Практичне значення одержаних результатів**

Отримані в дисертаційній роботі результати можуть бути використані для розширення варіантів побудови криптографічних ОБ апаратних або програмних систем захисту інформації, які, за рахунок обробки даних у МП, володіють підвищеною стійкістю до інженерно-криптографічних атак на основі аналізу споживаної потужності. Практична цінність роботи полягає у такому:

– створено програмні Verilog-моделі структур криптографічних ОБ виконання операцій кон’юнкції та диз’юнкції, додавання за модулем 2N, пошуку інвертованого елемента у полі GF(2N) для даних у МП із довільною кількістю логічних масок, орієнтованих на подальше використання при створенні та дослідженні ядер спеціалізованих апаратно-орієнтованих криптографічних процесорів, що підтверджується актом про їх використання у науково-дослідних роботах Тернопільського національного економічного університету (акт від 18.06.2015);

– створені програмні Verilog-моделі ядер спеціалізованих апаратно-орієнтованих процесорів симетричного блокового шифрування, які обробляють дані із одною логічною маскою та володіють підвищеною стійкістю до атак на основі аналізу споживаної потужності, що підтверджується актом про впровадження у діяльність Інституту передових технологій Самсунг Електронікс (Республіка Корея) (акт від 11.01.2011);

– розроблені алгоритми оцінки характеристик складності криптографічних блоків для виконання операцій кон’юнкції, диз’юнкції, додавання за модулем 2N, табличних операцій, перетворення МП даних, пошуку інвертованого елемента у полі GF(2N) впроваджені у начальний процес підготовки фахівців у галузі інформаційної безпеки, що підтверджується актами про впровадження у навчальний процес Університету в Бєльсько-Бялій (Польща) (акт від 30.06.2015), Тернопільського національного економічного університету (акт від 18.06.2015) та Тернопільського національного технічного університету імені І. Пулюя (акт від 21.06.2016).

**Особистий внесок здобувача.** Усі положення, які становлять суть дисертаційної роботи, були сформульовані та вирішені автором самостійно. У друкованих працях, опублікованих у співавторстві, автору дисертації належать: [1, 21] – аналіз стійкості реалізацій алгоритмів симетричного блокового шифрування до атак на основі АСП; [2] – методи перетворення МП даних; [3] – спосіб виконання операцій інвертування у полі GF(2N) маскованих даних за допомогою табличних операцій; [4] – алгоритм криптографічного перетворення mCrypton над даними у МП, архітектура та Verilog модель процесора за цим алгоритмом; [5] – огляд методів зворотнього трасування адрес; [6, 8] – статистичні моделі двомісних логічних операцій та операції додавання за модулем 2N для атак за аналізом енергоспоживання; [7] – алгоритм атаки на основі АСП на програмно-апаратні реалізації криптографічного перетворення за чинним стандартом; [9] – метод виконання операції підстановки над даними у МП; [11, 17] – узагальнена архітектура комп’ютерних компонентів для обробки даних у МП; [12] – теоретичні оцінки рівня безпеки виконання арифметичних, логічних операцій, операцій перетворення МП даних та табличних перетворень над даними у МП; [14] – система тестування, програмні засоби обробки даних моделювання атаки; [15] – методи виконання логічних операцій та операції додавання за модулем 2N над даними у МП; [16] – методика рандомізованого виконання криптографічних перетворень з регулярною структурою; [18] – модифікований алгоритм криптографічного перетворення за ГОСТ 28147-89 над даними у МП, архітектура та Verilog модель процесора за цим алгоритмом.

**Апробація результатів дисертації.** Основні положення та результати дисертаційної роботи доповідалися і обговорювалися на 9-ти науково-технічних та міжнародних конференціях: International Workshop on Information Security Applications (WISA), Південна Корея, 2004, міжнародної конференція “Комп’ютерні науки та інформаційні технології” (CSIT), м. Львів, 2006, міжнародна конференція “Комп’ютерні науки та інженерія” (CSE), м. Львів, 2006, 2007, Науковій конференції Тернопільського державного технічного університету ім. І.Пулюя, м. Тернопіль, 2007, International Science Conference "Internet in the information society" (IIS), м. Домрова Гурніца, Польща, 2007, International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), м. Дортмунд, Німеччина, 2007, м. Варшава, Польща, 2015, International Conference Advanced Computer Systems and Networks:  Design and Application (ACSN), м. Львів, International conference on modern problems of telecommunication, computer science and engineering training (TCSET), Львів-Славське, 2008.

**Публікації.** Основні положення дисертації опубліковано у 21 науковій праці, у тому числі 2 розділи у закордонних монографіях, 10 статей у наукових журналах та збірниках наукових праць, які входять до переліку фахових наукових видань МОН України (серед них 2 статті у виданнях, що входять до міжнародних наукометричних баз даних), а також 9 тез доповідей і матеріалів конференцій.

**Структура роботи та її обсяг.** Дисертація складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 144 сторінки основного тексту, 39 рисунків, 9 таблиць, 11 сторінок додатків. Список використаних джерел містить 126 найменувань і займає 16 сторінок. Загальний обсяг роботи 176 сторінок.

**ОСНОВНА ЧАСТИНА**

У **вступі** представлена загальна характеристика роботи, обґрунтована актуальність, сформульовані мета і задачі досліджень, відображені наукова новизна та практична цінність отриманих результатів, наведено дані про їх апробації та впровадження.

**У першому розділі** проведено аналіз сучасних методів захисту від атак на основі аналізу споживаної потужності пристрою від параметрів та даних криптографічного перетворення. Споживана потужність пристрою залежить від енергоспоживання базових напівпровідникових структур (логічних елементів), з яких побудований пристрій, від хемінгової ваги/відстані оброблюваних даних та керуючих сигналів (чи їх послідовності). Аналіз методів проводився за критеріями вартості, технологічності, низького енергоспоживання, продуктивності обробки, масштабованості до кількості масок, універсальності застосування (апаратна, програмна реалізації). У результаті такого аналізу встановлено, що ці методи не є досконалими і мають певні обмеження щодо практичного застосування для розв’язання завдання побудови криптографічних пристроїв. Встановлено, що перспективний метод захисту від атак на основі аналізу залежності споживаної потужності пристрою повинен дозволяти будувати як програмні, так і апаратні засоби шифрування, не залежати від кількості даних, які обробляються, дозволяти реалізацію на існуючій технологічній базі із стандартними бібліотеками елементів ІС чи наборах команд процесора. Таким вимогам відповідає обробка даних у МП, що полягає у введенні невизначеності у рівень споживаної потужності пристрою шляхом рандомізування проміжних значень , які виникають у процесі обчислень криптографічного перетворення. З огляду на те, що збільшення кількості масок – незалежних випадкових чисел з рівномірним законом розподілу ймовірності у МП , де , призводить до зменшення залежності споживаної потужності від немаскованих даних та ускладнення атак на основі АСП, встановлено, що необхідно розробити методи обробки даних у МП, які повинні бути масштабованими до кількості масок. Найбільш часто застосовують операцію маскування "" – операція побітового додавання за модулем два (так зване "логічне маскування" (ЛМ)). Однак, використання даних з ЛМ може приводити до ускладнення методів обробки та структур криптографічних ОБ. Тому, інколи доцільно застосовувати операцію маскування "+" – операцію додавання за модулем 2N (так зване "арифметичне маскування" (АМ)).

**У другому** розділі розроблено методи виконання базових операцій алгоритмів криптографічних перетворень над даними у МП. Нехай дані  і  подані у МП з використанням логічного маскування. Задача обчислення логічної операції над даними у МП формулюється так: за заданими наборами ,  обчислити без використання немаскованих  і  результат , де , "" – позначення логічної операції,  – маски результату.

В основу методу виконання операції диз’юнкції над даними у МП закладено підхід з обчисленням так званої «функції корекції маски» для результату виконання операції диз’юнкції безпосередньо над даними у МП. За рахунок введення у цю функцію операцій над усіма масками та усіма маскованими даними, введення нової маски результату, такий метод дозволяє отримувати вирази для обчислення операції диз’юнкції над даними із довільною кількістю масок:

. , (1)

де "⋅" і "∨ " – позначення операції логічного множення та додавання відповідно, а частина виразу справа від  є функцією корекції маски.

Аналогічний підхід застосовано для розвитку методу виконання операції кон’юнкції над даними у МП, який, на відміну від існуючого, дозволяє отримувати вирази для обчислення операції кон’юнкції над даними із довільною кількістю масок:

 , (2)

де частина виразу справа від  є функцією корекції маски.

Для розроблених методів є важливою послідовність додавання часткових сум у функції корекції маски: спочатку виконують додавання масок результату до масок вхідних даних, далі додають до отриманого результату суми кон’юнкцій маскованих даних та масок.

У роботі удосконалено метод табличних перетворень даних у МП , який, на відміну від існуючого, дозволяє виконувати табличні перетворення над вхідними даними як із логічною, так і з арифметичною масками та отримувати результат із заданим типом маскування. Нехай для визначення МП вхідних даних використовується операція маскування “”, а для вихідних даних – операція "". Тоді задача обчислення функції  з використанням  та отриманого результату у МП формулюється так: обчислити  з використанням лише , ,  – таблиці, яка задає , таким чином, щоб не використовувати не масковані дані  та . Для розв’язання цієї задачі у роботі запропоновано модифікувати підготовчу процедуру обчислень шляхом вводу додаткового проміжного маскування із маскою та узгодженим типом маски вхідних даних. Отримана таблиця  та проміжна маска використовуються в основній процедурі обчислень (табл. 1). Розроблений метод дозволяє отримувати результат табличного перетворення як і з однаковим до вхідних даних типом маскування, так із іншим типом. Такий вибір визначається операцією «» у підготовчій процедурі та зумовлюється вибором МП даних у подальших операціях криптографічних перетворень.

Таблиця 1

Обчислення табличних перетворень для даних у МП

|  |  |  |
| --- | --- | --- |
|  | Підготовча процедура | Основна процедура |
| Вхід | ,  і .  Операції і . | Таблиця : , , . |
| Вихід | Таблиця: | . |
| Обчислення | Для всіх , обраних випадково з , обчислити .  Повернути . | Знайти , де  – інвертований елемент .  Знайти .  Повернути . |

У роботі удосконалено існуючий метод виконання операції інвертування у полі GF(2N) даних у МП з логічним маскуванням однією маскою. Аналогічно до методів обчислення операцій кон’юнкції та диз’юнкції, запропоновано обчислювати функцію корекції маски (МК), яка залежить лише від маскованих даних та масок. Дані та маски представлено як степені деякого генератора поля , де не масковані дані , а маски є . Тоді для заданого  операцію пошуку інвертованого елемента виконують згідно з таким виразом:

 . (3)

Тут МК представлена у вигляді, де уникнуто обчислень із немаскованими даними  та використано усі маски вхідних даних, що, у порівнянні з існуючим методом, дозволяє обчислювати вираз (3) для даних із довільною кількістю логічних масок.

Криптографічні перетворення можуть містити операції, для яких, з точки зору вартості чи продуктивності, доцільно використовувати не логічне, а арифметичне маскування. Тому у роботі розроблено метод перетворення типу МП даних, який у загальній формі задано функціями виду:

, (4)

. (5)

де – додаткова маска результату, «» та «» - відповідно операції логічного та арифметичного маскування.

На основі виразу (4) перетворення типу МП відбувається згідно з описом, наведеними у табл. 2, де в ролі другого операнду використовується випадкові числа. У роботі показано, що: аналогічні перетворення можна отримати на основі виразу (5), вираз (5) можна отримати із (4) та навпаки. Також запропоновано варіанти обчислень виразу (4) на основі суматора (табл. 2) та табличних перетворень.

Для обчислення виразу (4) на основі суматора у роботі запропоновано створювати суматори за модулем 2N даних у МП з логічним маскуванням шляхом заміни усіх операцій, які описують роботу суматора, на їх еквіваленти для даних у МП. При цьому для заміни операцій диз’юнкції та кон’юнкції використано відповідно вирази (1) і (2). Тоді операцію арифметичного додавання -х бітів двох операндів  і  можна подати у вигляді:

Таблиця 2

Перетворення типу МП даних

|  |  |  |  |
| --- | --- | --- | --- |
| Вхід | Вихід | Перетворення | Номер |
|  |  | Згенерувати випадкові числа .  Знайти .  Зняти маскування з :. | (6) |
|  |  | Згенерувати випадкові числа .  Обчислити . | (7) |

, (8)

, (9)

де ,  – МП біту суми,  – МП вихідного переносу, , а , , , ,  – випадкові маски, *MAND*, *MOR*, *MXOR* – позначають операції кон’юнкції, диз’юнкції та додавання за модулем два даних у МП, а операція *MXOR* задана виразом .

Скориставшись виразами (8) та (9), у роботі запропоновано будувати суматор *MADD* даних у МП із логічним маскуванням за модулем 2N:

. (10)

На основі виразів (6), (7) та (10) побудовано перетворення типу МП даних із логічною маскою у представлення із арифметичною маскою та навпаки, відповідно:

, (11)

. (12)

Результати дослідження отриманих методів виконання операцій над маскованими даними показали, що в процесі обчислень не використовуються немасковані дані, що дозволяє використати ці методи для побудови структур криптографічних ОБ. Реалізацію розроблених методів здійснюють у такі етапи: спочатку для підвищення стійкості до атаки на основі АСП заданого порядку спочатку обирають кількість масок, рівну, чи більшу заданому порядку атаки АСП. Далі генерують задану кількість випадкових незалежних масок, однакової розрядності до даних. Переводять дані із немаскованого представлення у МП. Після цього дані у МП обробляють згідно з розробленими методами, використовуючи, за необхідності додатково згенеровані маски. Якщо обробку даних необхідно продовжити, то дані у МП використовують у подальших обчисленнях. За необхідності остаточний результат обчислень переводять із МП у звичайне представлення. Використані додаткові маски повторно не використовують.

**Третій розділ** роботи присвячено розробці структур та дослідженню характеристик складності криптографічних ОБ обробки даних у МП. На основі виразів (1) та (2) розроблено структури криптографічних ОБ кон’юнкції та диз’юнкції, які є масштабовані до кількості використаних масок. Для таких блоків, з точки зору зменшення їх часової та апаратної складності, доцільно використовувати пряме відображення потокового графу алгоритму виконання операцій. Тоді для однобітових блоків їх часова та апаратна складності квадратично залежать від кількості масок  (табл. 3).

Таблиця 3

Характеристики складності блоків кон’юнкції та диз’юнкції над даними у МП

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Операція | Часова складність | Апаратна складність | | |
|  |  |  |
| Кон’юнкція |  | 0 |  |  |
| Диз’юнкція |  | 1 |  |  |

У табл. 3 – час додавання за модулем два однобітових даних, , ,  – відповідно кількість двовходових елементів кон’юнкції, диз’юнкції, додавання за модулем два.

Криптографічні пристрої використовують ОБ табличних перетворень (табл. 2) для виконання операцій заміни за таблицею (табл. 4). Обробка даних з різним типами МП здійснюється подібними структурами ОБ. Різниця у їх структурах полягає в: узгодженні операцій над вхідними даними із типом МП даних у підготовчій та основній процедурах; використанні у підготовчій процедурі операції маскування вихідних даних, узгодженої із потрібним типом МП вихідних даних.

Таблиця 4

Структури ОБ табличних перетворень над даними у МП

|  |  |  |  |
| --- | --- | --- | --- |
| Тип маски | | Підготовча процедура | Основна процедура |
| Вхід | Вихід |
| ЛМ | ЛМ |  |  |
| ЛМ | АМ |  |
| АМ | АМ |  |  |
| АМ | ЛМ |  |

У роботі здійснено оцінку залежності характеристик складності цих ОБ від розрядності даних *N* (табл. 5), де , ,  – час читання з запам’ятовуючого пристрою із таблицею *Т*, час запису у запам’ятовуючий пристрій для зберігання таблиці *Т’*, апаратна складність логічного елемента кон’юнкції відповідно. Встановлено, що у порівнянні із ОБ для обробки немаскованих даних, збільшується часова та апаратна складності. Основний вклад у збільшення часової складності вносить виконання підготовчої процедури за кожної зміни проміжної маски.

Додатково, основна процедура передбачає проведення двох додаткових операцій для заміни вхідної маски на проміжну. Місткістна складність розробленого блоку є співмірною до такої ж складності блоку заміни для немаскованих даних, однак потребує використання оперативного запам’ятовуючого пристрою. Внаслідок цього, розроблені ОБ доцільно використовувати для даних із невеликою розрядністю. Використовуючи ці ж ОБ, можна реалізувати операції перетворення типу МП даних, у яких у підготовчій процедурі таблиця *Т* не використовується.

У роботі розроблено ОБ перетворення типу МП даних. Оскільки перетворення (6) та (7) реалізуються за допомогою суматора *MADD* за модулем 2N даних у МП, то отримано структуру суматора з послідовним переносом, у якій комбінаційні схеми обробки бітів основані на виразах (8) та (9), а для заміни операцій диз’юнкції та кон’юнкції використано відповідно вирази (1) і (2).

Таблиця 5

Характеристики складності блоків табличних перетворень над даними у МП

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Тип маскування | | Часова(підготовча процедура) | Часова (основна процедура) | Апаратна |
| Вхід | Вихід |
| ЛМ | ЛМ |  |  |  |
| АМ | АМ |  |  |  |
| ЛМ | АМ |  |  |  |
| АМ | ЛМ |  |  |  |

Дослідження характеристик складності структури такого суматора дозволило встановити, що для заданої розрядності даних часова та апаратна складність суматора залежить квадратично від кількості масок. Процедура побудови структур інших типів суматорів аналогічна до описаного вище підходу: схема суматора адаптується до обробки даних шляхом заміни логічних елементів на їх еквіваленти, які обробляють дані у МП.

Блоки перетворення МП даних з АМ у ЛМ та із ЛМ у АМ володіють апаратною та часовою складністю, які описуються такими виразами, відповідно: , , та і , де , – відповідно апаратна та часова складності суматора даних у МП. У порівнянні із структурами блоків на основі табличних перетворень, блоки на основі суматора добре масштабуються як до кількості розрядів, так і до кількості масок.

У роботі розроблено структури ОБ інвертування даних у GF(2N) у МП із логічною маскою. Перша структура передбачає повторне використання уже існуючих апаратних блоків чи програмних процедур множення та інвертування у GF(2N) та основана на прямому відображенні потокового графу обчислень згідно з виразом (3). Друга структура основана на табличній реалізації операцій множення та інвертування у GF(2N). Як показано у роботі, у табличній операції множення та інвертування необхідно модифікувати вміст таблиць логарифмів (log) та антилогарифмів (alog) для уникнення перевірок на нуль даних. Для цього введено дві додаткові незалежні маски *V* і *W* для маскування кожного рядка початкової log-таблиці та alog-таблиці відповідно. Для цього можна використати розроблений у другому розділі метод виконання табличних перетворень над маскованими даними в такий спосіб, що для кожного , , справджуються рівності:  і . Враховуючи ці дві останні рівності, вираз (3) прийме вид:

 , (13)

а вираз для обчислення  можна записати у вигляді:

 , (14)

де знаком "+" позначено операцію додавання за модулем 2N–1.

У роботі досліджено апаратну та часову характеристики блоку інвертування на основі першої структури, та показано, їх можна оцінити згідно з виразами, відповідно:

, (15)

, (16)

де , – відповідно апаратна і часова складності блока інвертування елемента у ,  і – відповідно апаратна і часова складності помножувача у ,  і – відповідно апаратна і часова складності блока додавання даних у . Якщо використати табличні перетворення на основі виразів (13) і (14), то характеристики апаратної, часової, місткістної складності таких компонент можна оцінити згідно з такими відповідними виразами:

, (17)

, (18)

, (19)

де ,  – відповідно апаратна і часова складність ОБ додавання даних за модулем 2N–1.

Основною складовою апаратної складності ОБ на базі табличних перетворень є об’єм обладнання (17), необхідний для побудови таблиць логарифмів та антилогарифмів. При фіксованому розмірі вхідних даних апаратна складність ОБ зростає у квадратичній залежності від кількості масок, які використано для МП вхідних даних. Часова складність ОБ (18) росте лінійно із збільшенням кількості масок, які використано для представлення даних. Для заданого числа масок та змінної розрядності вхідних чисел часова складність ОБ визначається відповідними змінами часової складності суматора та запам’ятовуючого пристрою.

Результат аналізу залежності апаратної складності для блоку на основі табличних перетворень, показує, що із збільшенням розрядності даних, які обробляються, ОБ буде мати обмежене застосування внаслідок експоненційного зростання апаратної складності запам’ятовуючих пристроїв (19). Тому областю доцільного використання такого пристрою при апаратній реалізації є обробка даних розрядністю 2, 4, 8 бітів. Якщо необхідно обробляти дані більшої розрядності, то доцільно будувати блоки множення у GF(2N) на базі структур апаратних помножувачів та інверторів.

У результаті порівняння розроблених структур криптографічних ОБ на основі розроблених у другому розділі методів із відомими структурами на основі методів дерев перемикачів-мультиплексорів (SWITCH-MUX), мультиплексорів (MUX-TREE), набору логічних комірок (XOR-AND) для логічних операцій, дерева мультиплексорів (XOR-MUX-MR) та табличного (TABLE-MR) для перетворення МП даних, повного маскування таблиці (FULL-MASK), обчислень на льоту (ON-THE-FLY), швидкого обчислення на льоту (FAST-ON-THE-FLY) для табличних перетворень, мультиплікативного маскування (MULT-MASK) та адаптаційного мультиплікативного маскування (ADAPT-MULT-MASK) встановлено, що розроблені структури придатні як для програмної, так і для апаратної реалізації (табл. 6), де , , , , , , , – відповідно апаратна та часова складність блоків кон’юнкції, додавання за модулем два, помножувача за модулем 2N, інвертора у полі GF(2N). За рахунок використання існуючих стандартних бібліотек елементів напівзамовлених ІС досягається низька вартість, низьке енергоспоживання та висока технологічність апаратної реалізації та отримання нових якостей – повного маскування результату (ПМР), використанні нової маски результату (НМР), підтримки різнотипного маскування (ПРМ), адаптування до довільної кількості масок (М).

**Четвертий розділ** присвячений розробці програмних моделей поведінкових Verilog-моделей структур ОБ виконання операцій над даними у МП. Такі моделі використано для подальшого створення та дослідження ядер апаратно-орієнтованих процесорів симетричного блокового шифрування даних у МП для систем захисту інформації. У роботі розроблено програмні поведінкові Verilog-моделі процесорів шифрування даних за алгоритмами mCrypton та ГОСТ28147-89 із даними у МП із використанням ЛМ однією маскою, у яких базові операції здійснюються за допомогою розроблених у третьому розділі структур ОБ для даних у МП.

Для mCrypton визначено такий перелік базових операцій: заміна за таблицею елементів даних (нелінійне перетворення), бітові перестановки стовбців, транспозиції масиву, додавання ключа. При цьому проведено адаптування алгоритмів шляхом заміни їх базових операцій на операції, розроблені у другому та третьому розділах, які дозволяють обробляти дані у МП з ЛМ. Структури трактів обробки даних та ключів процесора (рис. 1) містять елементи обробки масок паралельно до обробки даних у МП, що дозволяє обробляти маски та в одному такті із обробкою даних та ключів.

Таблиця 6

Порівняльна характеристика розроблених структур ОБ для даних у МП

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Операція** | **Метод виконання** | **Характеристики складності структур ОБ** | | **ПМР** | **НМР** | **РМП** | **М** |
| **Апаратна** | **Часова** |
| **Кон’юнкція** | SWITCH-MUX |  | / 12 операцій | + | + | – | – |
| MUX-TREE |  | / 12 операцій | + | – | – | – |
| XOR-AND |  | / 12 операцій | + | + | – | – |
| Запропонований |  | / 8 операцій | **+** | **+** | – | **+** |
| **Диз’юнкція** | SWITCH-MUX |  | / 12 операцій | + | + | – | – |
| MUX-TREE |  | / 12 операцій | + | – | – | – |
| Запропонований |  | / 10 операцій | **+** | **+** | – | **+** |
| **Перетворення МП даних** | XOR-MUX-MR ЛА |  |  | + | – | – | – |
| TABLE-MR |  |  | + | – | – | – |
| Запропонований ЛА (комбінаційна схема) |  |  | **+** | **+** | – | – |
| Запропонований ЛА (табличний) |  |  | **+** | **+** | – | – |
| **Табличні перетворення** | FULL-MASK |  |  | + | + | – | – |
| ON-THE-FLY |  |  | + | + | – | – |
| FAST-ON-THE-FLY |  |  | + | + | – | – |
| Запропоновані |  |  | **+** | **+** | **+** | – |
| **Інвертування** | MULT-MASK |  |  | – | + | – | – |
| ADAPT-MULT-MASK |  |  | – | + | – | – |
| Запропонований |  |  | **+** | **+** | – | **+** |



а) б)

Рис. 1. Структури процесора обробки даних у МП за алгоритмом mCrypton: а) тракт обробки маскованих даних, б) тракт обробки маскованого ключа

Тракт обробки даних та ключа процесора апаратно відображає один цикл алгоритму шифрування. У тракті використано маскований суматор та ОБ табличних перетворень для збереження змінної таблиці підстановки МК. Обчислений маскований цикловий ключ та його маска подаються на кожен цикл обробки даних у МП. Проміжні значення масок даних та ключа зберігаються у регістрах RegX і ReqRQ, відповідно. Після завершення усіх циклів роботи, з виходу пристрою отримують дані у МП та відповідну маску . Для отримання розмаскованих даних необхідно додати за модулем два маску до вихідних даних. Аналогічно здійснено розробку моделі процесора шифрування за алгоритмом ГОСТ 28147-89 для даних у МП із ЛМ.

У результаті логічного синтезу поведінкових Verilog-моделей процесорів на структури напівзамовлених КМОН ІС з бібліотекою логічних елементів для технології виробництва 0.18 мкм отримано оцінки їх апаратної та програмної складності. Додатково, після етапу розміщення та трасування на кристалі, засобами фізичного синтезу було отримано анотовані моделі процесорів. Для анотації моделей обрано затримки встановлення сигналів та спрацювання елементів, інформацію про кількість перемикань логічних рівнів у схемі. Оскільки отримана модель дозволяє оцінити логічний стан внутрішніх елементів та логічні рівні на їх міжз’єднаннях, у роботі використано ці моделі для моделювання атак на основі диференційного аналізу споживаної потужності.

Система моделювання, створена на мові Verilog для симулятора Cadence NC-Sim, дозволяє контролювати входи моделей процесорів та отримувати від симулятора інформацію про хемінгову вагу усіх міжз’єднань із файлу активності складових елементів моделі. Цей файл, разом із інформацією про паразитні зв’язки, використано для аналізу споживаної потужності у динаміці за допомогою аналізатора Synopsys PrimePower. Для досліджень обиралися моменти часу додавання циклового ключа до блоку вхідних даних чи запису у регістр результату обчислень циклу, а також без прив’язки до якихось наперед відомих подій. Для отримання масок було використано випадкові числа, отримані з виходу апаратного генератора випадкових чисел, об’ємом 1Гб. У роботі порівняно стійкість розроблених моделей процесорів до атаки на основі АСП з використанням аналізу кореляційних коефіцієнтів без використання МП даних та з його використанням. У першому випадку на входи усіх масок було подано фіксоване нульове значення – у результаті вдалося визначити елементи циклових ключів (рис 2а). У другому випадку, на входи масок було подано отримані випадкові числа – у результаті проведення аналогічної атаки не вдалося визначити біти циклових ключів шифрування (рис. 2б).



*а) б)*

Рис. 2. Результати моделювання атаки на основі АСП з використанням аналізу кореляційних коефіцієнтів R для моделі процесора обробки даних у МП за алгоритмом mCrypton: а) успішне визначення восьми молодших бітів циклового ключа (8510) у часовій відмітці 51 при відсутності МП даних, б) вигляд кореляційних коефіцієнтів не дозволяє визначити біти циклового ключа при використанні розроблених елементів МП даних.

Виходячи з результатів моделювання, характеристики розроблених ядер процесорів дозволяють рекомендувати їх до використання у пристроях з обмеженими ресурсами (смарт-карти, криптографічні токени, мобільні пристрої зв’язку тощо), які будуть мати підвищену стійкість до атак на основі диференційного аналізу споживаної потужності.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи, опис атак АСП на основі кореляційних коефіцієнтів, використаних для реалізації практичної частини дисертаційного дослідження.

**ВИСНОВКИ**

Результатом виконаної роботи є розв’язання наукової задачі побудови і дослідження методів та засобів виконання маскованої арифметики, що можуть використовуватися для побудови криптографічних пристроїв із підвищеною стійкістю до інженерно-криптографічних атак на основі аналізу споживаної потужності. У процесі виконання дисертаційної роботи отримані такі результати:

1. Проведено аналіз існуючих методів та засобів захисту від інженерно-криптографічних атак на основі аналізу споживаної потужності, що дозволило виявити їх недоліки та сформулювати завдання щодо розробки нових та удосконалення існуючих методів та засобів виконання операцій маскованої арифметики для криптографічних пристроїв систем захисту інформації.

2. Запропоновано метод виконання операції диз’юнкції над даними у маскованому представленні із довільною кількістю масок, що, за рахунок обчислення функції корекції маски результату з використанням виключно даних у маскованому представленні та їх масок, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції диз’юнкції, рівень безпеки яких до атак на основі аналізу споживаної потужності визначається кількістю масок даних у маскованому представленні.

3. Запропоновано метод перетворення маскованого предствлення даних, що, за рахунок використання операції додавання за модулем 2N над даними у маскованому представленні, побудованої на основі маскованих логічних операцій, на відміну від існуючих, дозволяє перетворювати масковане представлення даних довільної розрядності із арифметичним маскуванням у дані із логічним маскуванням та навпаки, а також використати таке перетворення для створення структур криптографічних операційних блоків, які використовують часту зміну типу маскування. Завдяки використанню нової маски результату, розроблені структури операційних блоків будуть володіти підвищеною стійкістю до атак на основі аналізу споживаної потужності першого порядку.

4. Розвинуто метод виконання операції кон’юнкції над даними у маскованому представленні, що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції кон’юнкції, рівень безпеки яких до атак на основі аналізу споживаної потужності визначається кількістю масок даних у маскованому представленні.

5. Розвинуто метод інвертування даних у маскованому представленні у полях виду GF(2N), що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє обробляти дані із довільною кількістю масок, а також використати таке перетворення для побудови структур криптографічних операційних блоків інвертування даних у полях виду GF(2N), стійкість яких до атак на основі аналізу споживаної потужності задається кількістю використаних масок у маскованому представленні. На відміну від існуючих, розроблені методи не є вразливими до «нуль-атак».

6. Удосконалено метод табличних перетворень даних у маскованому представленні, що, за рахунок введення додаткового проміжного маскування із узгодженим типом маски вхідних даних, який, на відміну від існуючих, дозволяє виконувати табличні перетворення над вхідними даними як із логічною, так і з арифметичною масками та отримувати результат із заданим типом маскування, а також дозволяє використати таку операцію для побудови структур криптографічних операційних блоків табличної заміни засобів шифрування даних у маскованому представленні.

7. Розроблено структури криптографічних операційних блоків виконання зазначених вище операцій, придатні як для програмної, так і апаратної реалізації, що за рахунок орієнтування на використання існуючих стандартних бібліотек елементів напівзамовлених інтегральних схем, дозволяє досягнути низької вартості та енергоспоживання, високої технологічності реалізації. Додатково, на відміну від існуючих, програмна реалізація методів виконання операцій кон’юнкції над даними у маскованому представленні володіє на 33% меншою часовою складністю, а операції диз’юнкції – на 20%.

8. Створено програмні Verilog-моделі структур криптографічних операційних блоків виконання зазначених вище операцій та, на їх основі, ядер спеціалізованих апаратно-орієнтованих процесорів симетричного блокового шифрування за алгоритмами mCrypton та ГОСТ 28147-89, які обробляють дані із одною логічною маскою та, за результатами моделювання атаки на основі аналізу споживаної потужності, дозволяють створити криптографічні процесори з стійкістю до атак на основі аналізу споживаної потужності першого порядку, порівняно з моделями без використання маскованого представлення для даних, впроваджені у діяльність Тернопільського національного економічного університету (акт від 18.06.2015) та Інституту передових технологій Самсунг Електронікс (Республіка Корея) (акт від 01.11.2011).

9. Розроблено алгоритми та результати оцінки характеристик складності криптографічних блоків для виконання перелічених вище операцій та впроваджено у начальний процес підготовки фахівців у галузі інформаційної безпеки, що підтверджується актами про впровадження у навчальний процес Університету в Бєльсько-Бялій (Польща) (акт від 30.06.2015), Тернопільського національного економічного університету (акт від 18.06.2015) та Тернопільського національного технічного університету ім. І. Пулюя (акт від 21.06.2016).

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Korkiszko Ł. Odporność symetrycznych szyfrów blokowych na atak typu analizy mocy sensorowych / Ł. Korkiszko // Bezpieczeństwo informacji / M. Karpiński. – Warszawa: Wydawnictwo Pomiary Automatyka Kontrola. – 2012. – Rozd. 6. – S. 197-259. – ISBN 978-83-930505-3-6. [Information Security.– Warsaw: Measurements, Automation and Monitoring.– 280 p.] (in Polish) – Розділ в монографії.
2. Karpinski M. Masked arithmetic: transformations of masked data representation / M. Karpinski, L. Korkishko // Internet in the Information Society / Sc. Ed. Tadeusz Wieczorek. – Dąbrowa Górnicza: Publisher Academy of Business in Dąbrowa Górnicza. – 2007. – Pp. 101–115. – ISBN 978-83-88936-38-8. – Розділ в монографії.

3. Korkishko L., Trichina E. Secure and efficient AES software implementation for smart cards / L. Korkishko, E. Trichina // Lecture Notes in Computer Science: Proc. of 5th International Workshop on Information Security Applications. WISA-2004. – Berlin: Springer, 2004. – Vol. 3325. – P. 779-792.

4. Karpinskyy M. Masked Encryption Algorithm mCrypton for Resource-Constrained Devices / M. Karpinskyy, L. Korkishko, A. Furmanyuk // Proc. of 4th International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2007). – Dortmund (Germany), 2007. – P. 628-633.

5. Survey of Modern IP Traceback Methodologies / A. Balyk, U. Iatsykovska, M. Karpinski [et al.] // Proc. of the 2015 IEEE 8th International Conference on “Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications” (IDAACS’2015). – Warsaw (Poland), 2015. – Vol. 1. – P. 484-488.

6. Коркішко Л. М. Статистична модель операції додавання за модулем 2N для проведення інженерно-криптографічних атак за побічними каналами витоку інформації / Л. М. Коркішко, І. В. Васильцов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – №8. – С. 115- 121.

7. Карпінський М. Інженерно-криптографічна атака за аналізом споживаної потужності на програмно-апаратні реалізації криптографічного перетворення за чинним стандартом / M. Карпінський, Л. Коркішко, Т. Коркішко // Вісник Тернопільського державного технічного університету. – 2005. – №3. – С. 127-135.

8. Карпінський М. П. Статистичні моделі двомісних логічних операцій для проведення інженерно-криптографічних атак за побічними каналами витоку інформації / М. П. Карпінський, Л. М. Коркішко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип. 2(13). – С. 188-196.

9. Карпінський М. П. Узагальнений алгоритм виконання операції підстановки над даними у маскованому представленні / М. П. Карпінський, Л. М. Коркішко // Вісник Хмельницького національного університету. – 2006. – №6 (87)– С. 100-106.

10. Коркішко Л. М. Базові логічні елементи для комп’ютерних пристроїв захисту інформації / Л. М. Коркішко // Вісник Національного університету "Львівська політехніка" "Комп’ютерні системи та мережі". – Львів, 2006. – №573 – С. 103- 113.

11. Карпінський М. П. Адаптування алгоритмів криптографічних перетворень до обробки маскованих даних / М. П. Карпінський, Л. М. Коркішко, Т. А. Коркішко // Вісник хмельницького національного університету – 2007. – № 3, Том 1 – С. 67-70.

12. Карпінський М. Оцінка рівня безпеки виконуваних засобами захисту інформації операцій / М. Карпінський, Л. Коркішко, Т. Коркішко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1 (14), 2007. – С. 176-187.

13. Коркішко Л. M. Операційні пристрої логічних операцій над даними у маскованому представлені / Л. М. Коркішко // Проблеми інформатизації та управління: збірник наукових праць. – К: НАУ, 2008. – № 1. – С.176-181.

14. Карпінський М. Моделювання DPA атаки першого порядку / М. Карпінський, Л. Коркішко // Безпека інформації. – 2016. – № 2. – С.184-195.

15. Карпінський М. П. Захист двійкових суматорів від інженерно-криптографічних атак за побічними каналами витоку інформації / М. П. Карпінський, Л. М. Коркішко // Матеріали 1-ї міжнародної конференції “Комп’ютерні науки та інженерія” (CSE`2006). – Львів, 2006. – С. 58-61.

16. Karpinskyy M. Randomized execution of regular cryptographic algorithms / M. Karpinskyy, L. Korkishko, T. Korkishko // Proc. of 3-rd International Conf. "Advanced Computer Systems and Networks: Design and Application" (ACSN’2007). –Lviv, 2007. – P. 114-117.

17. Karpinskyy M. Architecture of cryptographic devices resistant to side-channel attacks / M. Karpinskyy, L. Korkishko // Proc. of the International Conf. on Computer Science and Information Technologies. CSIT-2006. – Lviv: Lviv Polytechnic National University,2006. – P. 167-170.

18. Карпінський М. П. Процесор симетричного блокового шифрування за ГОСТ 28147-89 для даних у маскованому представленні / М. П. Карпінський, Л. М. Коркішко // Матеріали 2-ї міжнародної конференції “Комп’ютерні науки та інженерія” (CSE`2007). – Львів, 2007. – С. 86-90.

19. Коркішко Л. Операція множення даних у маскованому представленні / Л. Коркішко // Матеріали XI наукової конференції Тернопільського державного технічного університету ім. І.Пулюя. – Тернопіль, 2007. – С. 83.

20. Korkishko L. Inversion of masked data in GF(2N) / L. Korkishko // Proc. of International Conf. TCSET-2008. – Lviv-Slavsko (Ukraine), 2008. – P. 573-576.

21. Karpinskyi V. Side-Channel Signal Processing and Modeling / V. Karpinskyi, L. Korkishko, M. Karpinski // Advanced Computer Systems and Networks: Design and Application – ACSN-2009 : 4th International Conference, November 9-11th, 2009 : Proc. of the Conference. – Lviv (Ukraine), 2009. – P. 199-202. – ISBN 978-966-345-190-9.

**АНОТАЦІЯ**

**Коркішко Л.М. Методи та засоби маскованої арифметики для пристроїв систем захисту інформації** –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 актуальної наукової задачі побудови і дослідження методів та засобів виконання маскованої арифметики, що можуть використовуватися для побудови криптографічних пристроїв із підвищеною стійкістю до інженерно-криптографічних атак на основі аналізу споживаної потужності.

У роботі запропоновано метод виконання операції диз’юнкції над даними у маскованому представленні, що, за рахунок обчислення функції корекції маски результату з використанням виключно маскованих даних та їх масок, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції диз’юнкції, масштабованих до кількості масок даних у їх маскованому представленні. Також запропоновано метод перетворення маскованого представлення даних, що, за рахунок використання операції додавання за модулем 2N над даними у маскованому представленні, побудованої на основі маскованих логічних операцій, дозволяє перетворювати масковане представлення даних із арифметичним маскуванням у дані із логічним маскуванням та навпаки, а також використати таке перетворення для створення структур криптографічних операційних блоків, які використовують часту зміну типу маскування. Розвинуто метод виконання операції кон’юнкції над даними у маскованому представленні, що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції кон’юнкції, масштабованих до кількості масок даних у їх маскованому представленні. Розвинуто метод інвертування даних у маскованому представленні у полях виду GF(2N), що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє обробляти дані із довільною кількістю масок, а також використати таке перетворення для побудови структур криптографічних операційних блоків інвертування даних у полях виду GF(2N), які використовують табличні методи виконання операцій у цих полях.

**Ключові слова:** захист інформації, масковане представлення даних, маскована арифметика, процесори обробки даних у маскованому представленні, аналіз споживаної потужності, система захисту інформації.

**АННОТАЦИЯ**

**Коркишко Л.М. Методы и средства маскированной арифметики для устройств систем защиты информации.** – Рукопись.

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

Диссертационная работа посвящена решению актуальной научной задачи построения и исследования методов и устройств выполнения маскированной арифметики, которые могут использоваться для построения криптографических устройств с повышенной стойкостью к инженерно-техническим атакам на основе анализа потребляемой мощности.

В работе предложены методы выполнения базовых операций алгоритмов криптографических преобразований над данными в маскированном представлении. В перечень операций, рассмотренных в работе, входят: логические операции конъюнкции и дизъюнкции, инвертирование данных в полях вида GF(2N), табличных преобразований, преобразование типа маскированного представления данных. Методы выполнения логических операций конъюнкции и дизъюнкции, инвертирования в полях вида GF(2N) над данными в маскированном представлении характеризуются возможностью обработки данных с произвольным количеством масок. Для построения метода преобразования типа маскированного представления данных дополнительно разработано метод сложения данных в маскированном представлении по модулю 2N. За счет этого разработанный метод позволяет преобразовывать маскированное представление данных с арифметическим маскированием в данные с логическим маскированием и наоборот. Особенностью разработанного метода табличных преобразований данных в маскированном представлении является введение дополнительного промежуточного маскирования с согласованным типом маски входных данных, что позволяет виполнять табличные преобразования над входными данными как с логической, так и с арифметической масками и получать результат с заданым типом маскирования. На основе разработанных в работе методов выполнения операций над данными в маскированном представлении созданы програмные Verilog-модели структур криптографических операционных блоков выполения перечисленных выше операций и ядер специализированных аппаратно-ориентированных процессоров симметрического блочного шифрования согласно алгоритмам mCrypton и ГОСТ 28147-89, которые обрабатывают данные в маскированном представлении с одной логической маской и позволяют создавать криптографические процессоры с повышенной стойкостью к атакам на основе анализа потребляемой мощности.

**Ключевые слова:** защита информации, маскированное представление данных, маскированная арифметика, процессоры обработки данных в маскированном представлении, анализ потребляемой мощности, система защиты информации.

**ABSTRACT**

**Korkishko L. Methods and structures of masked arithmetic for information security systems devices.** –Manuscript

The dissertation thesis is intended to proceed with PhD degree on specialty 05.13.21 – «Information security systems». – National Aviation University, Kyiv, 2017.

The thesis is devoted to solving actual scientific problem of development and research of methods and means of implementing the masked arithmetic, which can be used to build cryptographic devices with increased resistance to cryptographic engineering attacks based on analysis of power consumption. The methods for performing basic operations of cryptographic algorithms for masked data representation are proposed in this work. The list of considered operations are: logical operations of conjunction and disjunction, data inversion in fields GF(2N), table-based transformations, conversion of mask type for masked data. Developed methods for performing logical operations of conjunction and disjunction, data inversion in fields GF(2N) on the data in the masked representation are characterized by the ability to process data with any given number of masks. For method for conversion of mask type for masked data further developed a method of adding masked data modulo 2N. Due to this developed method allows one to convert masked presentation of data from arithmetic masking to logical masking and vice versa. For proposed method for table-based transformations of masked data, additional intermediate masking of agreed type of mask input was introduced. That allowed one to perform table-based transformations on input with either logical or arithmetic masking and get the result with the given masking type.

Based on developed methods for operations on masked data, developed Verilog-models of structures for cryptographic operation units performing the above operations and cores of specialized hardware-based processor of symmetric block encryption algorithms mCrypton and GOST 28147-89, which process masked data with one logical mask and allow a creation of cryptographic processor with high resistance to attacks by analyzing the power consumption.

**Keywords:** information protection, masked data representation, masked arithmetic, processors for masked data representation, side-channel analysis, power analysis, information protection system.