параметра динамического диапазона D и эффективной полосы частот ω_h, определяемой для СМ как верхняя граница частотного диапазона.

III Выводы

В результате анализа методов исследования информационных параметров и характеристик сигналов маскирования речи на ОИД можно констатировать факт ***противоречия между методами идентификации информационных параметров и характеристик при синтезе сигнала аддитивного маскирования*** $Sn(t)$ ***и информационными параметрами и характеристиками при анализе речевого сигнала*** $Si(t)$ ***в точке НСД ТРП,*** влияющего на процесс исследования и анализа разведзащищенности информационной составляющей РС.

Литература: ***1.*** *ДСТУ 3396.2-97. Державний стандарт України. Захист інформації, Технічний захист інформації. Терміни та визначення. Київ. - 1998. – с. 12.* ***2****. Психоакустические аспекты восприятия речи. Механизмы деятельности мозга / Под. ред. Н. П. Бехтеревой. — М. Наука. 1988. –с. 504.* ***3****. Фланаган Дж. Анализ, синтез и восприятие речи: Пер. с англ./ Под ред. А. А. Пирогова. – М. Связь. 1968. – с. 396.* ***4****. Вокодерная телефония. Методы и проблемы. Под ред. А. А. Пирогова – М. Связь. 1974. – с. 536.* ***5****. Назаров М. В., Прохоров Ю. Н. Методы цифровой обработки и передачи речевых сигналов. – М. Радио и связь. 1985. – с. 176.* ***6.*** *Михайлов В. Г., Златоустова Л. В. Измерение параметров речи /Под ред. М. А. Сапожкова. – М. Радио и связь. 1987. – с. 168. 7. Вемян Г. В. Передача речи по цепям электросвязи. – М. Радио и связь. - 1985. – с. 272.* ***8.*** *ГОСТ Р 50840-95. Государственный стандарт Российской Федерации. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. Издание официальное. – М. Госстандарт России, 1997.* ***9****. НД ТЗІ – Р – 001 – 2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. НД ТЗІ – Р – 001 – 2000. ДСТСЗІ СБ України. – Київ. - 2000. – с. 9.* ***10****. Советский энциклопедический словарь. /Гл. ред. А. М. Прохоров. 4 – изд. – М. Сов. энциклопедия, 1989. – с. 1632.* ***11.*** *Брандт З. Статистические методы анализа наблюдений. – М. Мир. 1975. – с. 312.* ***12****. Калинин С. В. Исследование систем виброакустического зашумления. www.mascom.ru. - 2003.* ***13****. Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации//Специальная техника. – М. 2000.– № 4. С. 28 - 33.* ***14.*** *Иванов В. М., Хорев А. А. Способ и устройство формирования "речеподобных" шумовых помех// Вопросы защиты информации. – М. 1999. – № 4. С. 37 - 44.* ***15****. Shakhnov V. A., Vlasov A. I. Das Realisirungkonzept der aktiven Unterdruckung der Akustiklarme der Electronengerate.//Proceeding of 15th International Congress on Acoustics. Trondheim, Norway, 26 - 30 June 1995.*

УДК 004.31, 004.056.55, 003.26

ОЦІНКА РІВНЯ БЕЗПЕКИ ОПЕРАЦІЙ, ВИКОНУВАНИХ ЗАСОБАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Микола Карпінський, Леся Коркішко*, Тимур Коркішко**

*Університет в Бєльську-Бяла, Польща, *Тернопільський національний економічний університет, **Інститут передових технологій Самсунг Електронікс, Південна Корея*

Анотація: **Розвинуто методику оцінки рівня безпеки виконуваних засобами захисту інформації базових операцій алгоритмів криптографічних перетворень над даними у маскованому представленні.**

Summary: **A methodology for estimation of security level of basic operations execution on masked data for cryptographic transformations algorithms by information protection means was further developed.**

Ключові слова: **Масковане представлення даних, витік інформації, аналіз споживаної потужності, рівень безпеки виконання операцій, елементи пристроїв захисту інформації.**

Вступ

Для успішних практичних реалізацій алгоритмів криптографічних перетворень необхідно розв’язувати цілий комплекс задач, серед яких традиційне місце займають задачі досягнення мінімальної споживаної потужності, забезпечення малогабаритних вимог, продуктивності обчислень. Разом з тим, широке

впровадження і використання мобільних (портативних) комп'ютерних засобів для виконання алгоритмів криптографічних перетворень зумовлюють необхідність розв'язання додаткових задач, пов'язаних з загрозами безпеки обробки даних, що містять конфіденційну інформацію. Однією із таких загроз є загроза знаходження зловмисником конфіденційної інформації шляхом спостережень за роботою пристрою. При цьому, інформацію про конфіденційні дані, які використовуються в алгоритмах криптографічних перетворень, зловмисник отримує із побічних каналів витоку інформації (надалі – побічних каналів) з комп'ютерного пристрою. Такі побічні канали з'являються внаслідок залежності деяких характеристик засобів реалізації алгоритмів криптографічних перетворень від використаного ключа. Прикладами цих характеристик є споживана потужність пристрою, час обробки даних, електромагнітне випромінювання тощо, які є наслідком виконання алгоритму криптографічного перетворення [1 – 3]. Сучасні комп'ютерні пристрої для виконання алгоритмів криптографічних перетворень реалізуються як програмно, так і апаратно на інтегральних мікросхемах. Найпоширеніша технологія виготовлення цих мікросхем базується на комплементарних метало-оксидних напівпровідниках (КМОН). Особливістю роботи інтегральних мікросхем, виконаних за КМОН технологією, є залежність їх споживаного струму від значень, які записуються у елементи пам'яті (регістри) мікросхеми. При обробленні інформації з використанням алгоритмів криптографічних перетворень у елементи пам'яті записуються результати, отримані при виконанні деякої операції із застосуванням відомих даних і конфіденційних даних. Таким чином, зміна споживаного струму при такому записуванні несе в собі інформацію про результат виконання цієї операції, а тому і про конфіденційні дані. Зокрема, як було показано у [4, 5], споживаний струм залежить від Хемінгової ваги результату – пристрій споживає більший струм під час обробки даних з більшою Хемінговою вагою.

Пряме вимірювання споживаного струму не є зручним для проведення атак на комп'ютерні засоби реалізації криптографічних перетворень. Тому використовується вимірювання напруги на резисторі (шунті), ввімкненому в розрив кола живлення комп'ютерного пристрою. Таке проведення атаки в літературі [4 – 7] названо "атака на основі аналізу споживаної потужності" та знайшло найширше застосування для отримання конфіденційної інформації із комп'ютерних пристроїв реалізації алгоритмів криптографічних перетворень.

З метою підвищення рівня захищеності комп'ютерних засобів реалізації алгоритмів криптографічних перетворень від атак, що ґрунтуються на аналізі споживаної потужності, було запропоновано методи усунення кореляції між споживаною пристроєм потужністю і конфіденційними даними. Серед цих методів відзначимо: технологічні, алгоритмічні і системні [8]. Найефективнішими з точки зору вартості реалізації виявилися алгоритмічні методи з використанням рандомізування обчислень алгоритмів криптографічних перетворень на основі маскованого представлення даних. Однак, основними труднощами у використанні таких методів є: а) складність побудови алгоритмів виконання базових операцій криптографічних перетворень над даними у маскованому представленні без розголошення відомостей про дані; б) оцінка рівня безпеки процесу виконання розроблених алгоритмів. Відомі роботи [9 – 11] присвячені розв'язанню означених задач. Однак, згадані праці здебільшого зосереджені на розробці алгоритмів виконання лише однієї базової операції – обчислення оберненого елемента у полі Галуа. Відомі також роботи [12 – 14], в яких висвітлено розробку алгоритмів виконання додаткових базових операцій криптографічних перетворень над даними у маскованому представленні. Однак, в останніх працях не наводиться оцінка рівня безпеки процесу виконання цих алгоритмів. Тому, метою даної роботи є розвиток методів оцінки рівня безпеки виконання базових операцій криптографічних операцій над даними у маскованому представленні. Для цього за основу обрано методику оцінки рівня безпеки виконання операцій, вперше запропоновану в [15] і розвинуту в [16]. Оскільки в запропонованих в [12 – 14] алгоритмах використано розширений набір операцій для роботи з маскованими даними, то в даній роботі додатково проводиться оцінка рівня безпеки процесу виконання цих операцій.

І Базові операції алгоритмів криптографічних перетворень і масковане представлення даних

Серед неповного переліку базових операцій сучасних алгоритмів криптографічних перетворень найбільше розповсюдження отримали [17]: операції бітової перестановки (включаючи циклічні зсуви), логічні операції над даними у двійковому представленні – операції Булевої алгебри логіки, арифметичне додавання за модулем, операції у полях Галуа (додавання, множення, пошук оберненого елемента), операції підстановки. Для уникнення загрози витоку інформації побічними каналами використовують алгоритмічні методи захисту процесу обчислень, базовані на перетвореннях даних у маскованому представленні.

Нехай задано: 1) множину цілих чисел $Z_n = \{0,1,...,n\text{-}1\}$, $n = 2^l$ $l = 1,2,...$; 2) адитивну бінарну операцію "$+$" додавання за модулем n, яка разом з множиною Z_n утворює Абелеву групу G_+; 3) дві операції – адитивну "$\oplus$" і мультиплікативну "$\otimes$", які разом з Z_n утворюють поле $GF(2^l)$. Введемо наступні означення.

Означення 1 (масковане представлення). Маскованим представленням даних $a \in Z_n$ називається його подання у вигляді пари $\{\breve{a}, x\}$, де $\breve{a} = a \, op \, x$, op – одна із бінарних операцій "$+$", "$\oplus$" або "$\otimes$", $x \in Z_n$ – елемент маски, випадково обраний з рівномірним розподілом ймовірностей із Z_n.

Отримання немаскованого представлення даних згідно з означенням 1 означає виконання операції op над маскованим даним і з елементом, оберненим до маски (інший варіант – використання оберненої операції з тією ж маскою).

Означення 2 (логічне маскування). Маскованим представленням з використанням логічної маски називається представлення $\{\tilde{a}, x\} = \{a \oplus x, x\}$.

Означення 3 (арифметичне маскування). Маскованим представленням з використанням арифметичної маски називається представлення $\{\hat{a}, x\} = \{a + x, x\}$.

Означення 4 (мультиплікативне маскування). Маскованим представленням з використанням мультиплікативної маски називається представлення $\{\widehat{a}, x\} = \{a \otimes x, x\}$.

Пряме виконання базових операцій алгоритмічних криптографічних перетворень над даними у маскованому представленні не є тривіальним, оскільки в процесі отримання результату необхідно уникати розголошення відомостей про немасковані дані. Для цього необхідно використовувати спеціальні алгоритми виконання цих базових операцій, які забезпечують отримання необхідного результату у маскованому представленні. При цьому практичні реалізації таких алгоритмів використовують джерело випадкових чисел з рівномірним розподілом ймовірностей. Приклад архітектури пристрою для виконання операцій над даними у маскованому представленні наведено у [18].

Наведені означення 2 – 4 охоплюють типи маскувань, які використовуються на практиці. Зауважимо, що складність виконання алгоритмів (чи їх базових операцій) суттєво змінюється при використанні маскування даних різного типу. Наприклад, застосування логічного маскування виправдане при виконанні логічних операцій, разом з тим, використання арифметичного маскування при здійсненні логічних операцій над маскованими даними суттєво збільшує складність виконання таких операцій. Тому, якщо до набору базових операцій алгоритму криптографічного перетворення входять операції різних груп (наприклад, арифметичні, логічні, бітові перестановки), то при переході від операції з однієї групи до операції з іншої групи доцільно виконувати перетворення маскованого представлення даних з тим, щоб спростити подальше здійснення операції. Такі перетворення отримали назву "перетворення маски" чи "перетворення маскованого представлення" даних. На практиці найчастіше використовують перетворення логічної маски у арифметичну і навпаки. Практичне використання мультиплікативної маски є дещо обмеженим внаслідок можливості проведення атак спеціального виду – так званих "нуль-атак" [19].

Розробка алгоритмів здійснення операцій над даними у маскованому представленні пов'язана з труднощами оцінки рівня безпеки процесу виконання отриманих операцій для заданого переліку атак. Один із шляхів оцінки цього рівня полягає у проведенні всіх заданих атак на комп'ютерну реалізацію алгоритму. Однак такому підходу притаманний недолік – якість (успішність) атак на реалізації часто залежить від параметрів використовуваної системи вимірювання характеристик пристрою (наприклад, споживаної потужності). Із покращенням цих параметрів (швидкодії, роздільної здатності, динамічного діапазону вимірювань, чутливості тощо) зростає ймовірність успішного атакування. Тому все частіше для таких оцінок використовуються формальні методи, які дозволяють оцінити рівень безпеки процесу виконання тих чи інших операцій на основі їх математичного опису.

II Методика оцінки рівня безпеки виконання операцій маскованої арифметики

Для оцінки рівня безпеки процесу виконання алгоритмів операцій над даними у маскованому представленні скористаємось методикою, вперше запропонованою у [15] і розвинутою у [16]. Розглянемо деяке криптографічне перетворення ENC, яке необхідно виконати без витоку відомостей через побічні канали. Аргументами перетворення ENC є деякий відкритий текст a і конфіденційні дані k. Проаналізуємо, згідно з ENC, процес обчислення послідовності проміжних результатів

$I_1(a,k,r),...,I_t(a,k,r) = ENC(a,k)$. Кожен проміжний результат $I_i()$ залежить від відкритого тексту a, конфіденційних даних k і деякого $r \in \{0,1\}^s$. Елемент r використовується для внесення випадкового чинника в обчислення і володіє рівномірним розподілом ймовірностей з $\{0,1\}^s$. Результат виконання $ENC(a,k)$ залежить лише від a і k, однак на нього не впливає r.

Розглянемо модель зловмисника, згідно з якою він володіє відомими парами відкритий-зашифрований текст $(a, ENC(a,k))$. Додатково, припустимо, що для кожної пари $(a, ENC(a,k))$ зловмисник отримав деякий набір проміжних результатів $I_1(a,k,r),...,I_d(a,k,r)$. Для різних пар $(a, ENC(a,k))$ зловмиснику може бути відомий різний набір проміжних результатів. Якщо зловмисник може отримати щонайбільше d проміжних результатів для кожної пари $(a, ENC(a,k))$, то такий зловмисник називається зловмисником d-го порядку. Метою зловмисника є обчислення конфіденційних даних k.

Зловмисник досягає успіху, якщо сумісний розподіл ймовірностей отриманих ним проміжних результатів залежить від a і k. Зафіксуємо деякий набір $I_1,...,I_d$ проміжних результатів. Для кожної пари (a,k) позначимо $D_{a,k}(R)$ сумісний розподіл ймовірностей проміжних результатів $I_1,...,I_d$, отриманих шляхом випадкового вибору r із $\{0,1\}^s$ з рівномірним розподілом ймовірностей.

Означення 5 (повне маскування). Процес обчислення результатів перетворення ENC володіє властивістю повного маскування d-го порядку, якщо для усіх наборів $I_1,...,I_d$ проміжних результатів виконується рівність $D_{a,k}(R) = D_{a',k'}(R)$ для усіх пар (a,k), (a',k'). Для $d=1$ приймають, що процесу обчислень притаманна властивість повного маскування від зловмисника першого порядку.

Частковий аналіз розподілу ймовірностей проміжних результатів з використанням операції у полі $GF(256)$ здійснено у [16]. Подальший аналіз для операцій з поля $GF(2^l)$ наведено у [20]. Проведемо аналіз розподілу ймовірностей проміжних даних для деякої скінченої адитивної Абелевої групи і деякого скінченного поля.

Нехай задано: а) множину Z_n, $|Z_n| = n$ наділену бінарною операцією "$\bullet$", утворюючу адитивну Абелеву групу $G_\bullet$; б) скінчену множину Z_n, $|Z_n| = n$ та дві бінарні операції – адитивну "$\bullet$" і мультиплікативну "$*$", такі, що разом з Z_n утворюють поле F. Z_n утворює Абелеву групу з нейтральним елементом 0 відносно операції "$\bullet$", тоді як $Z_n^* = Z_n \setminus \{0\}$ – Абелеву групу з нейтральним елементом 1 відносно операції "$*$", причому операція "$*$" є дистрибутивна з операцією "$\bullet$".

Лема 1

Нехай $a, x \in Z_n$, де a – фіксований (заданий, відомий наперед) елемент, x – елемент, вибраний випадково з рівномірним розподілом ймовірності незалежно від a. Тоді $\hat{a} = a \bullet x \in Z_n$ є випадковим елементом з рівномірним розподілом ймовірності.

Доведення леми 1

Елемент $\hat{a} = a \bullet x$ належить множині Z_n внаслідок замкнутості групи $G_\bullet$. Тоді обчислення елемента $\hat{a} = a \bullet x$ еквівалентне до взаємно однозначного відображення (бієкції) множини Z_n самої в себе: $B : Z_n \xrightarrow{a \bullet x} Z_n$ для фіксованого (заданого) $a \in Z_n$ і випадкового x. Вибір певного нового x призводить до вибору деякого нового взаємно однозначного відображення B. При цьому, внаслідок ін'єктивності бієктивного відображення, для різних x обране нове відображення B також буде різним, а кількість таких відображень дорівнює кількості варіантів вибору x і становить $|Z_n| = n$. Беручи до уваги, що a є фіксованим (відомим, ймовірність його появи дорівнює одиниці), то ймовірність появи різних відображень B дорівнює ймовірності появи значення x. Оскільки, за умовою, x володіє рівномірним розподілом ймовірностей, то ймовірність появи довільного значення x дорівнює $1/n$. Тому, ймовірність появи різних відображень B характеризується значенням $1/n$.

Із ін'єктивності відображень B випливає, що кожен елемент із Z_n буде відображатися у інший елемент із цієї ж множини (в тому числі і сам у себе), а ймовірність такого відображення дорівнює ймовірності появи відображення B і становить $1/n$. Таким чином, $\hat{a} \in Z_n$ володіє рівномірним розподілом ймовірностей.

Наслідок з леми 1:

Нехай $a, x \in Z_n$, де a і x – вибрані випадково з Z_n рівномірним розподілом ймовірності і незалежно один від одного. Тоді $\hat{a} = a \bullet x \in Z_n$ є випадковим елементом з рівномірним розподілом ймовірності.

Лема 2

Нехай $a, a' \in F$ є заданими (відомими наперед) і $x, x' \in F$ є незалежними і рівномірно розподіленими на множині Z_n. Встановимо $I_1 = a \bullet x$ і $I_2 = a' \bullet x'$. Тоді добуток $Z = I_1 * I_2$ володіє розподілом ймовірності:

$$P(Z = i) = \begin{cases} (2 \mid Z_n \mid -1) / \mid Z_n \mid^2, & якщо\ i = 0, \\ (\mid Z_n \mid -1) / \mid Z_n \mid^2, & якщо\ i \neq 0, \end{cases} \quad (1)$$

де $i \in Z_n$.

Доведення леми 2

Згідно з лемою 1 $I_1 = a \bullet x$ і $I_2 = a' \bullet x'$ володіють рівномірним розподілом ймовірностей. Кількість усіх можливих комбінацій I_1 і I_2 дорівнює $\mid Z_n \mid^2$, де $\mid Z_n \mid$ – потужність множини Z_n, а кількість різних варіантів добутків $I_1 * I_2$ становить $\mid Z_n \mid$ внаслідок замкнутості поля F та незалежності I_1 і I_2.

Подія $Z = I_1 * I_2 = 0$ можлива за таких умов: $I_1 = I_2 = 0$, $\{I_1 = 0, I_2 \neq 0\}$ чи $\{I_1 \neq 0, I_2 = 0\}$. Кількість випадків, коли справджується кожен вираз, є відповідно: 1, $\mid Z_n \mid -1$ і $\mid Z_n \mid -1$. Загальна кількість комбінацій змінних I_1 і I_2, що призводить до справдження виразів, становитиме $1 + \mid Z_n \mid -1 + \mid Z_n \mid -1 = 2 \mid Z_n \mid -1$.

Загальна кількість комбінацій змінних I_1 і I_2, що призводить до появи події $Z = I_1 * I_2 \neq 0$, дорівнюватиме $\mid Z_n \mid^2 - 2 \mid Z_n \mid + 1 = (\mid Z_n \mid -1)^2$. Однак, різних значень $Z = I_1 * I_2$ буде лише $\mid Z_n \mid -1$ (внаслідок замкнутості поля). Тоді $P(Z = 0) = (2 \mid Z_n \mid -1) / \mid Z_n \mid^2$ і $P(Z \neq 0) = (\mid Z_n \mid -1) / \mid Z_n \mid^2$, що й треба було довести.

Лема 3

Нехай $a, a' \in F$ є заданими (відомими наперед) і $x, x' \in F$ є незалежними та рівномірно розподіленими на множині $Z_n = \{0, 1, \ldots, 2^l - 1\}$. Встановимо $I_1 = a \bullet x$ і $I_2 = a' \bullet x'$. Тоді результат виконання операції побітового логічного додавання $Z = I_1 \vee I_2$ володіє розподілом ймовірності: $P(Z = i) = \dfrac{3^{HW(i)}}{4^l}$, а результату здійснення операції побітового логічного множення $Z = I_1 \wedge I_2$ притаманний розподіл ймовірності $P(Z = i) = \dfrac{3^{l - HW(i)}}{4^l}$, де $i \in Z_n$, $HW()$ – функція, яка повертає кількість одиниць (Хемінгову вагу) у двійковому представленні i.

Доведення леми 3

Згідно з лемою 1 $I_1 = a \bullet x$ і $I_2 = a' \bullet x'$ володіють рівномірним розподілом ймовірностей. З іншого боку результат виконання операції логічного додавання над однорозрядними даними характеризується законом розподілу ймовірностей, що описується виразом: $P(z = i) = \begin{cases} 1/4, & якщо\ i = 0, \\ 3/4, & якщо\ i = 1. \end{cases}$. Оскільки I_1 і I_2 незалежні і володіють рівномірним розподілом ймовірності, то значення результату $Z = I_1 \vee I_2$ при

$l > 1$ буде залежати від кількості та позицій одиниць у двійковому представленні I_1 і I_2. Ймовірність появи деякого двійкового представлення результату $Z = \{z_{l-1}, z_{l-2}, ..., z_1, z_0\}$, де z_i – значення *i*-го розряду двійкового представлення Z, можна знайти з таких міркувань. Оберемо довільне $0 \le k \le l-1$, яке позначає кількість одиниць у двійковому представленні Z. Тоді кількість нулів у цьому ж представленні дорівнюватиме $l-k$, а ймовірність появи деякої комбінації $i = \{z_{l-1}, z_{l-2}, ..., z_1, z_0\}$ із $l-k$ нулями та k одиницями становитиме $P(Z=i) = p(z_{l-1} = i_{i-1}) \cdot p(z_{l-2} = i_{i-2}) \cdot ... \cdot p(z_0 = i_0) = P(z=0)^{l-k} P(z=1)^k$. Підставивши в останній вираз значення $P(z=i)$, маємо: $P(Z=i) = \left(\frac{1}{4}\right)^{l-k} \cdot \left(\frac{3}{4}\right)^k = \frac{3^k}{4^l}$. Враховуючи, що кількість одиниць k визначає Хемінгову вагу результату, отримаємо твердження першої частини леми.

Для доведення другої частини леми зауважимо, що, згідно з лемою 2, результат виконання операції логічного множення над однорозрядними даними володіє законом розподілу ймовірностей, який отримуємо з виразу (1): $P(z=i) = \begin{cases} 3/4, & якщо\ i = 0, \\ 1/4, & якщо\ i = 1. \end{cases}$. Використовуючи аналогічний до першої частини підхід, знаходимо, що $P(Z=i) = \left(\frac{3}{4}\right)^{l-k} \cdot \left(\frac{1}{4}\right)^k = \frac{3^{l-k}}{4^l}$. Враховуючи, що кількість одиниць k визначає Хемінгову вагу результату, отримаємо твердження другої частини леми.

Лема 4

Нехай $a, x \in Z_n = \{0,1,...,2^l - 1\}$, де a – фіксований (заданий, відомий наперед) елемент, x – елемент, вибраний випадково з рівномірним розподілом ймовірності незалежно від a. Тоді $\bar{\tilde{a}} = \tilde{\bar{a}} \in Z_n$ є випадковим елементом з рівномірним розподілом ймовірності, де "¯" позначає операцію логічного заперечення.

Доведення леми 4

Зауважимо, що операцію логічного заперечення, виконану над двійковим представленням $\tilde{a}$, можна подати у вигляді: $\bar{\tilde{a}} = \tilde{a} \oplus \{1\}^l = a \oplus x \oplus \{1\}^l = (a \oplus \{1\}^l) \oplus x = \tilde{\bar{a}}$, а елемент $\{1\}^l = 2^l - 1 \in Z_n$. Тоді, згідно з лемою 1, результат $\tilde{\bar{a}}$ володіє рівномірним розподілом ймовірностей.

На основі отриманих лем 1 – 4 проведемо формальну оцінку рівня безпеки виконання операцій над даними у маскованому представленні.

III Оцінка рівня безпеки процесу виконання операцій над даними у маскованому представленні

Розглянемо алгоритми виконання базових операцій алгоритмів криптографічних перетворень, зокрема, логічних операцій, бітових перестановок, операції заміни за таблицею, додавання, множення і пошуку оберненого елемента, перетворення маскованого представлення даних.

3. 1 Логічні операції

Логічні операції над маскованими даними включають в себе операції побітового логічного додавання, логічного множення, додавання за модулем два, логічного заперечення. Розглянемо алгоритми виконання логічних операцій над даними у маскованому представленні з використанням логічної маски.

Операція логічного множення двох однорозрядних операндів, поданих у маскованому представленні $\{\tilde{a}, x\}$ і $\{\tilde{b}, y\}$ у полі $GF(2)$, виконується згідно з виразом [21]:

$$MAND(\{\tilde{a}, x\}, \{\tilde{b}, y\}, z\} = \{(a \otimes b) \oplus z, z\} = \{\tilde{a} \otimes \tilde{b} \oplus (\tilde{a} \otimes y \oplus (\tilde{b} \otimes x \oplus (x \otimes y \oplus z))), z\}, \quad (2)$$

де $x \in Z_2$ – елемент маски, випадково вибраний з рівномірним розподілом ймовірностей із Z_2.

Для оцінки рівня безпеки виконання (2) розглянемо властивості проміжних змінних. Оскільки маски x і y вибираються незалежно і володіють рівномірним розподілом ймовірностей, то згідно з другою частиною леми 3 результати виконання кожного з проміжних добутків $\tilde{a} \otimes \tilde{b}$, $\tilde{a} \otimes y$, $\tilde{b} \otimes x$ і $x \otimes y$

характеризуються розподілом ймовірностей і є незалежними від немаскованих даних. Обчислення проміжної суми шляхом додавання проміжного добутку $x \otimes y$ до нової маски z згідно з лемою 1 приводить до рівномірного розподілу ймовірностей результатів проміжної суми. Продовжуючи застосування леми 1 до наступних проміжних сум, отримуємо, що результат виконання (2) володіє рівномірним розподілом ймовірностей, є незалежним від даних a і b, а тому, згідно з означенням 5, процес обчислень згідно з виразом (2) характеризується властивістю повного маскування обчислень від зловмисника першого порядку.

Операція логічного додавання двох операндів, поданих у маскованому представленні $\{\widetilde{a}, x\}$ і $\{\widetilde{b}, y\}$ у полі $GF(2)$, виконується згідно з наступним виразом [13]:

$$\begin{aligned} MOR(\{\widetilde{a}, x\}, \{\widetilde{b}, y\}, z) = \{(a \vee b) \oplus z, z\} = \\ = \{\widetilde{a} \vee \widetilde{b} \oplus (\widetilde{a} \otimes y \oplus (\widetilde{b} \otimes x \oplus (x \otimes y \oplus (x \oplus (y \oplus z))))), z\} \end{aligned}, \quad (3)$$

де $x \in Z_2$ – випадковий елемент маски з рівномірним розподілом ймовірностей, що належить множині Z_2.

Для оцінки рівня безпеки виконання (3) розглянемо властивості проміжних змінних. Оскільки маски x і y вибираються незалежно і володіють рівномірним розподілом ймовірностей, то результати виконання кожного з проміжних добутків, $\widetilde{a} \otimes y$, $\widetilde{b} \otimes x$ і $x \otimes y$ характеризуються розподілом ймовірностей, визначеним згідно з першою частиною лемою 2, тобто є незалежними від немаскованих даних. Проміжному результату $\widetilde{a} \vee \widetilde{b}$ притаманний розподіл ймовірностей, визначений згідно з другою частиною леми 3. Обчислення проміжної суми шляхом додавання проміжного добутку $x \otimes y$ до нової маски z, відповідно до леми 1, приводить до рівномірного розподілу ймовірностей результатів проміжної суми. Продовжуючи застосування леми 1 до наступних проміжних сум, отримуємо, що результат виконання (3) володіє рівномірним розподілом ймовірностей, є незалежним від даних a і b, а тому, за означенням 5, процес обчислень згідно з виразом (3) характеризується властивістю повного маскування обчислень від зловмисника першого порядку.

Операція додавання за модулем два двох операндів, поданих у маскованому представленні $\{\widetilde{a}, x\}$ і $\{\widetilde{b}, y\}$ у полі $GF(2)$, виконується згідно з виразом:

$$MXOR(\{\widetilde{a}, x\}, \{\widetilde{b}, y\}, z) = \{(a \oplus b) \oplus z, z\} = \{(\widetilde{a} \oplus \widetilde{b} \oplus z) \oplus x \oplus y, z\}. \quad (4)$$

Альтернативне виконання (4) без використання додаткової маски z можна здійснити згідно з таким виразом:

$$MXOR(\{\widetilde{a}, x\}, \{\widetilde{b}, y\}) = \{(a \oplus b) \oplus (x \oplus y), x \oplus y\} = \{\widetilde{a} \oplus \widetilde{b}, x \oplus y\}.$$

Для оцінки рівня безпеки виконання (4) розглянемо властивості проміжних результатів. Проміжний результат $\widetilde{a} \oplus \widetilde{b} \oplus z$, обчислений у будь-якому порядку, згідно з наслідком з леми 1 володіє рівномірним розподілом ймовірностей. Подальше виконання додавання x і y у довільній послідовності також приводить до рівномірного розподілу ймовірностей результату. Застосувавши аналогічний підхід до аналізу спрощеного варіанту виразу (4), отримуємо, що, за означенням 5, процес обчислення згідно з виразом (4) та його спрощеним варіантом володіє властивістю повного маскування обчислень від зловмисника першого порядку.

Операція логічного заперечення операнду, поданого у маскованому представленні $\{\widetilde{a}, x\}$ у полі $GF(2)$ виконується згідно з виразом:

$$MNOT(\{\widetilde{a}, x\}) = \{\overline{\widetilde{a}}, x\} = \{\widetilde{\overline{a}}, x\}. \quad (5)$$

Для оцінки рівня безпеки виконання (5) зауважимо, що, згідно з лемою 4, результат інвертування $\widetilde{a}$, який володіє рівномірним розподілом ймовірностей, призводить до рівномірного розподілу ймовірностей результату $\widetilde{\overline{a}}$. Тому, згідно з означенням 5, процес виконання виразу (5) володіє властивістю повного маскування обчислень від зловмисника першого порядку.

Аналогічно можна побудувати алгоритми та оцінити рівень безпеки процесу їх виконання для обчислень інших операцій, наприклад обчислення штриху Шиффера та стрілки Пірса, тощо. Зауважимо,

що виконання логічних операцій над даними у маскованому представленні з використанням арифметичного маскування пов'язане зі збільшенням складності виконання логічних операцій внаслідок залежності бітів результату маскування від попередніх бітів. Тому для спрощення виконання таких операцій використовують алгоритми перетворення маскованого представлення даних, метою яких є заміна арифметичного маскування на логічне.

3. 2 Арифметичні операції

Складність алгоритмів виконання арифметичних операцій над даними у маскованому представленні залежить від типів маскування – арифметичного чи логічного. Розглянемо виконання арифметичних операцій додавання за модулем $n = 2^l$, $l > 1$ та пошук оберненого елемента у G_+.

Операція арифметичного додавання двох операндів $\{\hat{a}, x\}$ і $\{\hat{b}, y\}$ виконується згідно з виразом:

$$MADD(\{\hat{a}, x\}, \{\hat{b}, y\}, z) = \{(a+b)+z, z\} = \{(\hat{a}+\hat{b}+z)-x-y, z\}, \quad (6)$$

де для представлення суми використовується нова маска z. Альтернативним виразом для обчислення суми є:

$$MADD(\{\hat{a}, x\}, \{\hat{b}, y\}) = \{(a+b)+(x+y), x+y\} = \{\hat{a}+\hat{b}, x+y\}, \quad (7)$$

де для представлення суми повторно застосовуються маски операндів.

Оцінка рівня безпеки виконання операції арифметичного додавання згідно з виразами (6), (7) проводиться аналогічно до оцінки рівня безпеки для виконання операції додавання за модулем 2 відповідно до виразу (4) та його спрощеного варіанту. Тому, згідно з означенням 5, процес виконання виразів (6), (7) володіє властивістю повного маскування обчислень від зловмисника першого порядку.

Операція арифметичного додавання i-х бітів двох операндів $\{\widetilde{a}_i, x_i\}$ і $\{\widetilde{b}_i, y_i\}$, де $i = 0,...,l-1$, виконується згідно з виразами:

$$\{\widetilde{s}_i, u_i\} = MXOR(MXOR(\{\widetilde{a}_i, x_i\}, \{\widetilde{b}_i, x_i\}, z), \{\widetilde{p}_{i-1}, r_{i-1}\}, u_i), \quad (8)$$

$$\{\widetilde{p}_i, r_i\} = MOR(MAND(\{\widetilde{a}_i, x_i\}, \{\widetilde{b}_i, y_i\}, z), MAND(\{\widetilde{p}_{i-1}, r_{i-1}\}, \{\widetilde{s}_i, u_i\}, v), r_i), \quad (9)$$

де $\{\widetilde{s}_i, u_i\}$ – масковане представлення суми, а $\{\widetilde{p}_i, r_i\}$ – масковане представлення вихідного переносу, $p_{-1} = 0$, z, u_i, r_i, v, r_{-1} – випадкові маски із рівномірним розподілом ймовірностей.

Скориставшись виразами (8), (9), можна спростити запис операції додавання двох l-бітових даних за модулем $n = 2^l$:

$$MADD(\{\widetilde{a}, x\}, \{\widetilde{b}, y\}, \{z_s, \{q\}\}) = \{(a+b) \oplus z_s, z_s\} = \{\widetilde{s}, z_s\}, \quad (10)$$

де $\{q\}$ – набір випадкових масок, які використовуються для проміжних обчислень згідно з виразами (8), (9).

Для оцінки рівня безпеки виконання операції додавання у G_+ згідно з виразами (8), (9) розглянемо статистичні властивості проміжних результатів. Оскільки z, u_i, r_i, v, r_l є незалежними масками з рівномірним розподілом ймовірностей, то результат виконання всіх операцій $MXOR$, $MAND$ і MOR буде володіти також рівномірним розподілом ймовірностей. Тому, згідно з означенням 5, процеси виконання обчислень згідно з виразами (8) – (10) характеризуються властивістю повного маскування обчислень від зловмисника першого порядку.

Обчислення оберненого елемента $-b$ до елемента $b \in G_+$ без розголошення його немаскованого представлення зручно виконувати за допомогою виразів (5) і (10) при використанні логічного маскування. Для цього зауважимо, що обернений елемент легко знайти шляхом обчислення доповняльного коду до двійкового представлення елемента b. Відомий алгоритм обчислення доповняльного коду двійкового представлення числа передбачає побітове інвертування двійкового числа з наступним додаванням одиниці за модулем n:

$$\{-b \oplus z, z\} = MADD(\{x \oplus 1, x\}, MNOT(\{\widetilde{b}, y\}), \{z, \{q\}\}). \quad (11)$$

Для оцінки рівня безпеки виконання виразу (11) зауважимо, що, згідно з лемою 4, результат обчислення $MNOT(\{\widetilde{b}, y\})$ володіє рівномірним розподілом ймовірностей. Відповідно до леми 1

результат виконання $x \oplus 1$ також характеризується рівномірним розподілом ймовірностей. Як було показано вище, результату додавання двох проміжних результатів за допомогою функції $MADD()$ також притаманний рівномірний розподіл ймовірностей. Тому, за означенням 5, процес виконання обчислень згідно з виразом (11) володіє властивістю повного маскування обчислень від зловмисника першого порядку.

Виконання віднімання за модулем n можна виконати за допомогою виразу (10): $\{(a-b) \oplus z, z\} = MADD(\{\widetilde{a}, x\}, \{-\widetilde{b}, y\}, \{z_s, \{q\}\})$, де $\{-\widetilde{b}, y\}$ – масковане представлення оберненого до b елемента, знайдене, наприклад за допомогою обчислень згідно з виразом (11). Аналогічно виконується пошук різниці елементів, поданих у маскованому представленні з використанням арифметичної маски: $\{(a-b) \oplus z, z\} = MADD(\{\hat{a}, x\}, \{-\hat{b}, y\})$. Оскільки, процеси обчислення згідно з функцією $MADD()$ володіють властивістю повного маскування обчислень від зловмисника першого порядку, то процеси обчислення відповідно до виразів для знаходження різниці також характеризуються аналогічною властивістю.

Вираз для виконання множення даних у полі $GF(2^l)$ у маскованому представленні з використанням логічної маски аналогічний загалом до виразу (2), де "$\otimes$" означає операцію множення у полі $GF(2^l)$, а $\oplus$ – додавання у полі $GF(2^l)$. Оцінка безпеки виконання множення даних у полі $GF(2^l)$ у маскованому представленні з використанням логічної маски є аналогічною до оцінки безпеки виконання (2) з використанням леми 2 для оцінки розподілу ймовірностей проміжних добутків. Тому, процес обчислення згідно з виразом (2) над даними із $GF(2^l)$ володіє властивістю повного маскування обчислень від зловмисника першого порядку.

3. 3 Бітові перестановки

Для виконання бітової перестановки π над даними у маскованому представленні з використанням логічного маскування необхідно виконати операцію перестановки маскованих вхідних даних і маски згідно з заданою перестановкою:

$$\{\pi(a) \oplus x', x'\} = \{\pi(\widetilde{a}), \pi(x)\}. \qquad (12)$$

Справедливість виразу (12) зумовлюється тим, що при виконанні операції логічного маскування кожен біт аргументу a маскується незалежно від інших бітів. Тому побітове переставляння a еквівалентне до побітового переставляння $\widetilde{a}$ з відповідним представленням маски. Отже, маска результату дорівнюватиме результату виконання перестановки π над маскою x аргументу.

Для оцінки рівня безпеки виконання виразу (12) зауважимо, що виконання операції бітової перестановки приводить лише до зміни позицій бітів маскованого операнду без зміни значень цих бітів. Тоді для рівномірного розподілу ймовірностей $\widetilde{a}$ результат виконання $\pi(\widetilde{a})$ також володіє рівномірним розподілом ймовірностей. Тому, згідно з означенням 5, процес обчислення за формулою (12) володіє властивістю повного маскування обчислень від зловмисника першого порядку.

Виконання операції бітової перестановки над даними, поданими у маскованому представленні з використанням арифметичної маски, є більш складним, оскільки значення кожного біту у такому представленні залежить від значень попередніх бітів аргументу і маски. Тому перед виконанням бітової перестановки доцільно перетворити масковане представлення даних – замінити арифметичне маскування на логічне. Далі операцію бітової перестановки можна виконати згідно з виразом (12). Обернене перетворення маскованого представлення результату виконання (12) дозволяє отримати масковане представлення даних з використанням арифметичного маскування.

3. 4 Перетворення маскованого представлення даних

Перетворення маскованого представлення даних використовується для спрощення виконання подальших операцій над даними у маскованому представленні. Як було зазначено вище, при використанні арифметичного маскування складно проводити бітові маніпуляції над даними. Разом з тим, використання логічного маскування ускладнює арифметичні операції у групі G_+. Розглянемо алгоритми перетворення маскованого представлення даних на основі виразу (10).

Нехай задано $\{\hat{d}, p\}$ з використанням арифметичної маски. Тоді задача перетворення $\hat{d}$ у $\{\widetilde{d}, t\}$ зводиться до знаходження маски t та маскованих даних $\widetilde{d}$ без розкриття відомостей про Хемінгову вагу

d. Скориставшись виразом (10) та ввівши заміну змінних $\{\tilde{a},x\}=\{\hat{d}\oplus x,x\}$ і $\{\tilde{b},y\}=\{(-p)\oplus y\},y\}$, отримаємо:

$$MADD(\{\hat{d}\oplus x,x\},\{(-p)\oplus y,y\},z_s,\{q\})=\{(\hat{d}-p)\oplus z_s,z_s\}=\{\tilde{d},z_s\}. \quad (13)$$

Для оцінки рівня безпеки процесу виконання обчислень згідно з виразом (13) зауважимо, що, як було показано вище, процеси обчислень за формулою (10) та обчислень оберненого елемента володіють властивістю повного маскування обчислень від зловмисника першого порядку, тому аналогічна властивість притаманна обчисленням відповідно до виразу (13).

Для перетворення маскованого представлення даних з логічною маскою у представлення з арифметичною маскою приймемо, що задано масковане представлення $\{\tilde{d},t\}$ з використанням логічного маскування. Тоді задача перетворення $\{\tilde{d},t\}$ у $\{\hat{d},p\}$ полягає у знаходженні маски p та $\hat{d}$ без розкриття відомостей про d. Скориставшись виразом (10) та ввівши заміну змінних $\{\tilde{a},x\}=\{\tilde{d},t\}$ і $\{\tilde{b},y\}=\{p\oplus y\},y\}$, де p – випадкове число з рівномірним розподілом ймовірностей, отримаємо:

$$MADD(\{\tilde{d},t\},\{p\oplus y,y\},z_s,\{q\})=\{(d+p)\oplus z_s,z_s\}=\{\tilde{\hat{d}},z_s\}.$$

Оскільки p і z_s є незалежними випадковими числами, то $\tilde{\hat{d}}$ означає $\hat{d}$ у маскованому представленні з логічною маскою z_s. Тоді $\hat{d}=\tilde{\hat{d}}\oplus z_s$. Виходячи з міркувань, аналогічних до оцінки рівня безпеки процесу виконання обчислень, згідно з виразом (12), процес виконання обчислень останнього результату володіє властивістю повного маскування обчислень від зловмисника першого порядку.

3. 5 Операція заміни за таблицею

Операції заміни даних чи їх частин широко використовуються у криптографічних перетвореннях і часто є основним засобом реалізації нелінійних операцій. Розглянемо процес виконання операцій заміни за таблицею над даними, поданими у маскованому представленні з використанням арифметичного та логічного маскувань [14].

Нехай задано: а) множину Z_n цілих чисел, наділену бінарними операціями "$\circ$" та "$\bullet$", які утворюють адитивні Абелеві групи $G_\circ$ та $G_\bullet$ відповідно; б) бієктивну функцію $f(a)$, $a\in Z_n$, сформовану для усіх $a\in Z_n$ за допомогою таблиці $f(a)=T[a]$, яка визначає вузли заміни у векторі заміни; в) маску аргументу x, проміжну маску y, маску результату z, які є незалежними випадковими числами з рівномірними розподілами ймовірностей, $x,y,z\in Z_n$. На практиці замість операцій "$\circ$" та "$\bullet$" використовують операції "$\oplus$" та "+" у довільній комбінації (в тому числі й однакові операції).

Задача обчислення функції $f(a)$ із застосуванням маскованого аргументу, маски та отриманого маскованого результату формулюється так: обчислити $\tilde{f}(a)=f(a)\bullet z$, використовуючи лише $\{\tilde{a},x\}$, z, $T[a]$ без розголошення відомостей про проміжні результати та a. Для розв'язання цієї задачі здійснюють дві процедури: підготовчу та основну. Підготовча процедура виконується щоразу при зміні y або z. Результатом її виконання є модифікована таблиця заміни T' з властивістю $T'[b\circ y]=T[b]\bullet z$.

Підготовча процедура:

Вхід: $T[a]$, y і z.

Вихід: таблиця T' з властивістю $T'[b\circ y]=T[b]\bullet z$.

Для усіх $i\in Z_n$, обраних випадково з рівномірним розподілом ймовірності з Z_n, обчислити $T'[i]=T[i\circ y]\bullet z$.

Видати T'.

Основна процедура призначена для обчислення $\tilde{f}(a)=f(a)\bullet z$ з використанням результатів підготовчої процедури, значень даних $\{\tilde{a},x\}$, y, z.

Основна процедура:

Вхід: таблиця T' з властивістю $T'[b \circ y] = T[b] \bullet z$, $\{\widetilde{a}, x\}$, y, z.

Вихід: $\widetilde{f}(a) = T[a] \bullet z$.

Обчислити $\widetilde{b}_1 = \widetilde{a} \circ y$.

Обчислити $\widetilde{b}_2 = \widetilde{b}_1 \circ x^{-1}$, де x^{-1} – обернений елемент до x.

Обчислити $\widetilde{f}(a) = T'[\widetilde{b}_2] = T[a] \bullet z$.

Повернути $\widetilde{f}(a)$.

Для оцінки рівня безпеки процесу виконання процедури заміни за таблицею з'ясуємо окремо рівень безпеки процесів виконання підготовчої і основної процедур. При виконанні підготовчої процедури здійснюється вибір $i \in Z_n$ із рівномірним розподілом ймовірностей. Результат виконання операції $i \circ y$, згідно з лемою 1, володіє рівномірним розподілом ймовірності. Згідно з наведеною в [22] лемою про виконання операції табличної підстановки над числом з рівномірним розподілом ймовірності та лемою 1, результат $T'[i] = T[i \circ y] \bullet z$ також володіє рівномірним розподілом ймовірності. Таким чином, беручи до уваги означення 5, процесу обчислення T' притаманна властивість повного маскування. Для оцінки рівня безпеки процесу виконання основної процедури проаналізуємо рівень безпеки процесу виконання окремих її кроків. Згідно з лемою 1, результати виконання першого $\widetilde{b}_1 = \widetilde{a} \circ y$ та другого кроків $\widetilde{b}_2 = \widetilde{b}_1 \circ x^{-1}$ володіють рівномірними розподілами ймовірностей. На підставі використання аналогічного підходу до оцінки рівня безпеки процесу виконання підготовчої процедури можна констатувати, що результат виконання третього кроку основної процедури $\widetilde{f}(a) = T'[\widetilde{b}_2] = T[a] \bullet z$ володіє рівномірним законом розподілу ймовірностей. Тоді, за означенням 5, процесу обчислень згідно з основною процедурою властиве повне маскування обчислень від зловмисника першого порядку.

Висновки

У роботі розвинуто метод оцінки рівня безпеки процесу виконання операцій над даними у маскованому представленні. Для цього сформульовано та доведено леми про види розподілу ймовірностей результатів виконання деяких операцій над даними в маскованому представленні. До переліку розглянутих операцій входять: адитивна операція скінченої Абелевої групи, мультиплікативна операція скінченого поля, порозрядні логічні множення та додавання двійкових чисел, порозрядне інвертування двійкових чисел.

Використовуючи отримані леми, проведено оцінку рівня безпеки процесу виконання операцій над маскованими даними. Показано, що запропоновані алгоритми виконання операцій над даними у маскованому представленні володіють властивістю повного маскування процесу обчислень від порушника першого порядку. До переліку розглянутих алгоритмів виконання операцій над даними у маскованому представленні входять:

- алгоритми виконання операцій Булевої алгебри логіки (логічне множення, додавання, інвертування), операція порозрядного додавання за модулем два;
- алгоритми виконання операції додавання та пошуку оберненого елемента за модулем у групі, утвореній операцією додавання за модулем;
- алгоритм виконання бітової перестановки даних;
- алгоритми виконання перетворення маскованого представлення даних;
- алгоритм виконання операції заміни за таблицею;
- алгоритми виконання множення у полі $GF(2^l)$.

Отримані результати можна застосувати при проектуванні та сертифікуванні комп'ютерних пристроїв реалізації алгоритмів криптографічних перетворень, даних у маскованому представленні з використанням арифметичних або логічних масок. Перевагами розглянутих алгоритмів виконання операцій над даними у маскованому представленні є: 1) можливість їх реалізації на основі існуючих технологій виготовлення інтегральних схем чи на основі універсальних програмованих процесорів у вигляді програмних модулів; 2) можливість формальної оцінки рівня безпеки процесу виконання алгоритмів криптографічних перетворень над даними у маскованому представленні

Література ***1.*** *Kelsey J., Schneier B., Wagner D., Hall C. Side Channel Cryptanalysis of Product Ciphers // In 5th European Symposium on Research in Computer Security – ESORICS '98, vol. 1485 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 1998. – p. 97 – 110.* ***2.*** *Messerges T. Using second-order power analysis to attack DPA resistant software // C.K. Koc, C.Paar, Eds., Cryptographic Hardware and Embedded Systems – CHESS 2000, vol. 1956 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2000. – p. 238 – 251.* ***3.*** *Messerges T., Dabbish E., Sloan R. Eximining smart-card security under the threat of power analysis attack // IEEE Transactions on computers, Vol. 51, No 5, 2002. – p. 541 – 552.* ***4.*** *Messerges T., Dabbish E., Sloan R. Power analysis attacks of modular exponentiation in smartcards // C. K. Koc, C. Paar, Eds., Cryptographic Hardware and Embedded Systems – CHESS 1999, vol. 1717 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 1999. – p. 144 – 157.* ***5.*** *Lv J., Han Y. Enhanced DES Implementation Secure against High-Order Differential Power Analysis in Smartcards // In Proceedings of ACISP'05 — Tenth Australian Conference on Information Security and Privacy, Volume 3574 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2005. – p. 195 – 206.* ***6.*** *Messerges T. S. Securing the AES Finalists Against Power Analysis Attacks // In Proceedings of Fast Software Encryption Workshop 2000, Springer-Verlag, 2000.* ***7.*** *Koecher et al. Using Unpredictable Information to Minimize Leakage from Smartcards and other Cryptosystems., USA patent 6327661., Dec. 4, 2001. – 14 p.* ***8.*** *Zhou Y. B., Feng D. G.. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing // National Institute of Standardization Physical Security Testing Workshop. http://csrc.nist.gov/cryptval/physec/papers/physecpaper19.pdf.* ***9.*** *Trichina E., De Seta D., Germani L. Simplified adaptive Multiplicative masking for AES // In proceedings of CHESS 2002, LNCS 2532, Springer-Verlag Berlin Heidelberg, 2003. – p. 187 – 197.* ***10.*** *Korkishko L., Trichina E. Secure and efficient AES software implementation for smart cards // 5th International Workshop on Information Security Applications - WISA 2004, Jeju Island, Korea, 2004. – p. 779 – 792.* ***11.*** *Schramm K., Paar C. High-order masking of the AES // CT-RSA 2006, Vol. 3860 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2006 – p. 208 – 225.* ***12.*** *Коркішко Л. М. Базові логічні елементи для комп'ютерних пристроїв захисту інформації// Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – 2006. – прийнято до друку.* ***13.*** *Карпінський М. П., Коркішко Л. М. Захист двійкових суматорів від інженерно-криптографічних атак за побічними каналами витоку інформації // Матеріали 1-ї міжнародної конференції "Комп'ютерні науки та інженерія" (CSE`2006), 11-13 жовтня, 2006, м. Львів, Україна. – С. 58 – 61.* ***14.*** *Карпінський М .П., Коркішко Л. М. Узагальнений алгоритм виконання операції підстановки над даними у маскованому представленні // Вісник Хмельницького національного університету. – 2006. – №6 (87)– С. 100 – 106.* ***15.*** *Chari S., Jutla C. S., Rao J. R., Rohatgi P. Towards sound approaches to counteract power analysis attacks // In proceedings of Advances in Cryptology – CRYPTO'99, August 1999. Vol. 1666 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 1999. – p. 398 – 412.* ***16.*** *Blomer J., Merchant J. G., Krummel V. Provably secure masking of AES // Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Vol. 3357 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2004 – p. 69 – 83.* ***17.*** *Коркішко Т. А., Мельник А. О., Мельник В. А. Захист інформації в комп'ютерних і телекомунікаційних мережах: Алгоритми та процесори симетричного блокового шифрування. Львів: БАК, 2003. – 168 с.* ***18.*** *Karpinskyy M., Korkishko L. Architecture of cryptographic devices resistant to side-channel attacks // In proceedings of the International Conference on Computer Science and Information Technologies CSIT'2006 (September 28th-30th, 2006, Lviv, Ukraine). – Lviv: Publishing House of Lviv Polytechnic National University. – 2006. – p. 167-170.* ***19.*** *Coron J. S., Tchulkine A., Walter C, Koc C. K., Paar C. A new algorithm for switching from arithmetic to boolean masking // In Proceedings of . International workshop CHES 2003: Cryptographic hardware and embedded systems, Vol. 2779 of Lecture notes in computer science, Springer-Verlag, 2003. – p. 89 – 97.* ***20.*** *Oswald E., Mangard S., Herbst C., Tillich S. Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers // In Proc. CT-RSA 2006, Vol. 3860 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2006 – p. 192 – 207.* ***21.*** *Trichina E. Combinatorial logic design for AES sybbyte transformation on masked data. Cryptology eprint archive: Report 2003/236, IACR, November 11, 2003.* ***22.*** *Oswald E., Schramm K. An efficient masking scheme for AES software implementations// In proceedings of 6th International Workshop on Information Security Applications – WISA 2005, Jeju Island, Korea, Vol. 3786 of Lecture notes in computer science, Springer-Verlag, 2005. – p. 292 – 305.*