2. *Нормативний документ Системи технічного захисту інформації "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД" (НД ТЗІ 2.5 – 004 – 99).* ***3***. *Нормативний документ Системи технічного захисту інформації "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [НД ТЗІ 2.5. – 005 – 99].* ***4***. *Введение в криптографию / Под. Ред. В. В. Ященко.– СПб .: Питер, 2001, – 288 с.: ил.* ***5***. *Василенко В. С., Короленко М. П. Цілісність інформації в автоматизованих системах.// Корпоративні системи.1999.– № 3.– с.52–57.* ***6***. *Василенко В. С., Курочкін С. Г. Використання методу завадостійкої криптографії в системах обробки кредитно-фінансової інформації // Машинна обробка інформації. Міжвідомчий науковий збірник.– Вип.60, 1997.– с.169–174.* ***7***. *Будько М. М., Василенко В. С., Короленко М. П. Механізми контролю цілісності та її поновлення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, – К., 2000.– с.130 – 139.* ***8***. *Василенко В. С. Горицький В. М. Варіант завадостійкого криптографічного перетворення // "Современные проблемы телекоммуникаций", збірка доповідей на 6–ій міжнародній науково – технічній конференції, 19 – 22 серпня 2003 р.(ч.1) // Одеська національна академія зв'язку ім. А. С. Попова – с. 71 – 73.*

УДК 681.3

МЕТОДИ СТРУКТУРНОЇ НАДЛИШКОВОСТІ ЯК ПРОТИДІЯ АТАКАМ АПАРАТНИХ ПОМИЛОК

Ігор Васильцов
Тернопільська академія народного господарства

Анотація: **Досліджено особливості застосування методів структурної надлишковості для підвищення стійкості апаратних засобів захисту інформації до атаки апаратних помилок. Розглянуто традиційні види структурної надлишковості та резервування Мак-Класкі. Наведено математичні співвідношення для оцінки ефективності застосування різних видів надлишковості.**
*Summary:***In this paper the particularities of structural redundancy technique usage to increase the resistance of data protection hardware to different fault analysis have been investigated. Traditional structural redundancy as well as Mac-Cluskey redundancy have been considered. The mathematical models to estimate the efficiency of different structural redundancy technique usage have been developed.**
Ключові слова: **Атака апаратних помилок, методи захисту, структурна надлишковість.**

І Постановка проблеми

Задачі захисту інформації в умовах сучасного розвитку інформаційних технологій можуть успішно бути вирішеними лише за умови застосування апаратних засобів захисту, оскільки постійне зростання потоків конфіденційної інформації ставить жорсткі вимоги щодо забезпечення відповідного рівня пропускної здатності каналів зв'язку. Такі апаратні засоби є складовою частиною системи захисту інформації і реалізують криптографічні алгоритми забезпечення конфіденційності, цілісності та працездатності автоматизованих систем обробки інформації [1, 2]. Проте тенденції до апаратної реалізації засобів криптографічного захисту інформації в свою чергу обумовили появу принципово нових видів криптоаналізу, які умовно можна назвати "Атаки спеціальних впливів", або ж "Атаки на основі нестандартних (побічних) каналів витоку інформації" (англ. мовою side-channel attacks, covert-channel attacks) [3 – 13]. Однією з перспективних є атака на основі апаратних помилок. Суть цієї атаки полягає у наступному: криптоаналітик має доступ до апаратури захисту інформації, і має змогу проводити штатні операції стосовно криптографічного перетворення вхідних даних, а також може спеціальним чином впливати на процес обробки інформації, щоб спричинити некоректну роботу засобів захисту інформації, а відтак отримати спотворений шифротекст. Подальша робота полягає в диференційному аналізі криптотексту, отриманого у нормальному режимі роботи, та у режимі виникнення помилок. Незважаючи на очікувану велику складність такого процесу, Е. Біхам та А. Шамір теоретично довели, що в загальному випадку достатньо від 50 до 200 пар незалежних криптотекстів для зламу алгоритму DES [8]. Останні дослідження зарубіжних вчених в цій області показують, що така атака може бути ефективно проведена за умови залучення невеликих коштів [11]. Тому розробка підходів, методів та засобів проектування пристроїв захисту інформації, стійких до атак спеціальних впливів, набуває особливої актуальності.

ІІ Аналіз літератури

Для боротьби з атаками спеціальних впливів застосовують різноманітні підходи, що базуються на

застосуванні певних видів надлишковості [3 – 7, 14 – 17], найбільш популярними з яких є:

- алгоритмічна, яка полягає в тому, що розробник видозмінює сам криптографічний алгоритм (чи деякі критичні його частини) з метою зменшити дисперсію статистичних характеристик процесу криптографічного перетворення залежно від ключової інформації;
- інформаційна, яка полягає в тому, що регістри даних, в яких містяться ключі (чи інша критична інформація), використовують спеціальні види кодування інформації;
- часова, яка полягає в тому, що крипто-пристрій виконує кількаразове обчислення результату, чи інверсні операції;
- топологічна, яка полягає в дублюванні сигнальних ліній та деякому перетворенню логічної функції.

У даній роботі розглядається ефективність застосування структурної надлишковості для вирішення задач підвищення стійкості криптографічних пристроїв до атак спеціальних впливів.

III Мета роботи

Метою даної роботи є формалізація та розробка математичних співвідношень для оцінки ефективності застосування різних видів структурної надлишковості як способу протидії атакам апаратних помилок. На основі таких оцінок розробник ще на ранніх етапах проектування апаратних засобів захисту інформаційних ресурсів має змогу провести порівняльний аналіз та вибрати оптимальний варіант архітектурної реалізації криптографічного пристрою.

IV Методи структурної надлишковості

На відміну від алгоритмічних методів, які можуть застосовуватися лише до певного класу алгоритмів, запропоновані методи структурної надлишковості дозволяють ефективно підвищити стійкість до атаки апаратних помилок незалежно від класу алгоритмів та елементної бази реалізації. Характерною ознакою даного підходу є те, що він дозволяє боротися з атаками, що базуються на однократних помилках, оскільки зловмисник змушений згенерувати більше як одну (в загальному випадку більше n, де n - кількість елементів резервування) помилку. Відомо, що для зменшення складності криптографічної атаки на основі апаратних помилок криптоаналітик прагне генерувати лише однократні помилки, оскільки при збільшенні кратності помилок складність атаки зростає комбінаторно. Нижче розглянуто деякі методи застосування структурної надлишковості для підвищення рівня захищеності апаратних засобів захисту інформації.

Традиційне резервування однотипними модулями з мажоритарним пристроєм.

Традиційно для підвищення надійності апаратури використовують різні архітектури структурної надлишковості – резервування. На рис. 1 зображено узагальнену архітектуру традиційного резервування з однотипними модулями. На виході мажоритарний пристрій порівнює значення усіх виходів кожного з модулів і відповідно до функції прийняття рішення формує сигнал на виході.

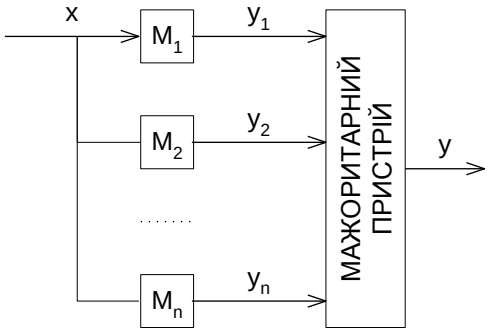

Рисунок 1 - Узагальнена архітектура традиційного резервування з однотипними модулями

Оскільки за означенням усі модулі однотипні $M_1 = M_2 = ... = M_i ... = M_n$, то імовірності правильної (безпомилкової) роботи будуть рівні $P_1 = P_2 = ... = P_i ... = P_n = P_0$. Імовірність правильної (безпомилкової) роботи мажоритарного пристрою в загальному випадку не рівна імовірності модулів $P_M \neq P_0$. Значення функції кожного з модулів визначається як:

$$y_i = f_o(x) \ \forall\ i = 1, \ldots, n; n = 2l+1, \quad (1)$$

де $f_o(x)$ – задана функція роботи модуля.

Значення сигналу на виході пристрою визначається як:

$$y = y_i \Big| \sum \{ y_i = y_j \} \geq Maj(n) \ \forall\ i = 1, \ldots, n \wedge i \neq j, \quad (2)$$

де $Maj(n)$ – мажоритарна функція. Традиційно, для непарної кількості блоків резервування вона визначається як:

$$Maj(n) = \frac{n+1}{2}. \quad (3)$$

З точки зору ефективного проектування апаратних засобів для оцінки якості проектованого пристрою застосовують такі критерії як продуктивність (час затримки опрацювання сигналу пристроєм), апаратні затрати, надійність роботи. З точки зору стійкості до атак спеціальних впливів важливим критерієм оцінки ефективності проектування є складність виконання такої атаки, яка може бути виражена через імовірність успішного виконання атаки. Нижче наведено загальні співвідношення для оцінки цих критеріїв щодо криптопристроїв, побудованих за схемою рис. 1.

Час затримки опрацювання сигналу пристроєм, який впливає на швидкість надходження даних на вхід пристрою, а отже на продуктивність роботи пристрою в цілому:

$$d_\Sigma = \max(d_i) + d_M \cong d_0 + d_M. \quad (4)$$

Апаратні затрати:

$$c_\Sigma = \sum_{i=1}^{n} c_i + c_M \cong n \cdot c_0 + c_M. \quad (5)$$

Надійність роботи пристрою, що виражається через імовірність безпомилкової роботи за умови, що функціонування мажоритарного пристрою визначається співвідношенням (3), можна визначити за такою формулою:

$$P_\Sigma = \left(1 - \frac{n+1}{2n} \cdot (1 - P_0)\right) \cdot P_M. \quad (6)$$

Формула (6) означає, що хоча б $\frac{n+1}{2}$ модулів спрацювали правильно, і одночасно правильно спрацював мажоритарний пристрій.

Цікаво дослідити залежність надійності роботи пристрою при різних співвідношеннях імовірностей правильної роботи базового модуля P_0 та мажоритарного пристрою P_M. Для цього зручно скористатися таким виразом $P_M = \alpha \cdot P_0$. На рис. 2 зображено залежність надійності роботи пристрою від кількості модулів резервування та для різних співвідношень між імовірностями P_0 та P_M ($P_0 = 0.9$).

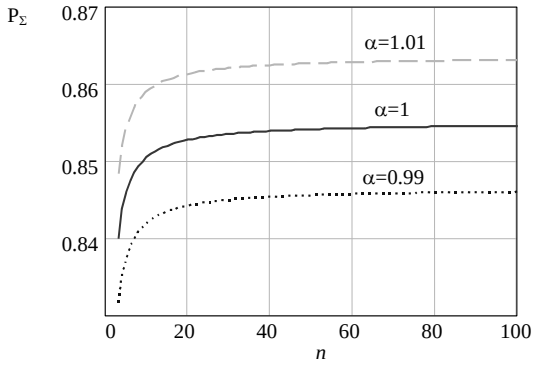

Рисунок 2 – Залежність надійності роботи пристрою від кількості модулів резервування для різних співвідношень між імовірностями P_0 та P_M

Аналіз рис. 2 показує, що збільшення кількості резервних модулів більше 20 не впливає суттєво на імовірність безпомилкової роботи пристрою в цілому, в той час як для імовірності правильної роботи мажоритарного пристрою P_M слід забезпечувати високий рівень.

У деяких випадках доцільно застосовувати сильнішу умову мажоритування для забезпечення гарантованого рівня безпеки. Для цього можна запропонувати таке співвідношення:

$$Maj(n) = \left\lceil \frac{2}{3} n \right\rceil, \tag{7}$$

яке означає, що сигнал на виході криптопристрою формуватиметься лише за умови, коли не менше аніж дві третини усіх резервних модулів приймуть якесь одне конкретне значення. В іншому випадку результат невизначений. Більше того, при такій мажоритарній функції кількість резервних модулів може бути парною.

Для пристрою з такою мажоритарною функцією параметри продуктивності та апаратні затрати будуть обчислюватися за тими ж формулами, що й в попередньому випадку, а надійність роботи пристрою можна визначити за такою формулою:

$$P_\Sigma = \left(1 - \left\lceil \frac{2}{3} n \right\rceil \cdot \frac{1}{n}\left(1 - P_0\right)\right) \cdot P_M \cong \left(1 - \frac{2}{3}\left(1 - P_0\right)\right) \cdot P_M . \tag{8}$$

Як видно з формули, в цьому випадку імовірність безпомилкової роботи є константою і не залежить від кількості задіяних модулів резервування (для випадку $P_0 = P_M = 0.9$ розраховане значення $P_\Sigma = 0.840$). Отже, розробник, вибираючи різні функції мажоритування, може гарантовано вибирати той чи інший рівень безпеки стосовно атаки апаратних помилок.

Для оцінки складності виконання атаки апаратних помилок приймаємо, що усі пристрої перевірки (мажоритарні та інші типові) є стійкими до атак апаратних помилок. Це можна здійснити шляхом застосування методу подвійних сигнальних ліній [15] . Застосування такого методу до самих функціональних блоків не завжди є ефективним, оскільки функціональні блоки на відміну від мажоритарних модулів (які виконуються як комбінаційні цифрові пристрої) є доволі складними з великою кількістю внутрішніх зв'язків.

Тоді якщо за P_0^A позначити імовірність успішної реалізації атаки зловмисником для одного модуля, то загальна імовірність успішного виконання атаки для криптопристрою, побудованого за схемою рис. 1 з мажоритарною функцією (3) буде визначатися як:

$$P_\Sigma^A = \left(P_0^A\right)^{\frac{n+1}{2}}, \tag{9}$$

а для крипто-пристрою з мажоритарною функцією (7) як:

$$P_\Sigma^A = \left(P_0^A\right)^{\frac{2n}{3}}. \tag{10}$$

На рис. 3 для порівняння зображено залежність імовірності успішного виконання атаки апаратних помилок для криптопристроїв, що використовують мажоритарні функції (3) та (7). Імовірність успішної атаки для одного базового блока резервування $P_0^A = 0.9$. Як видно з рис. 3 мажоритарна функція (7) дає більшу стійкість стосовно атаки апаратних помилок.

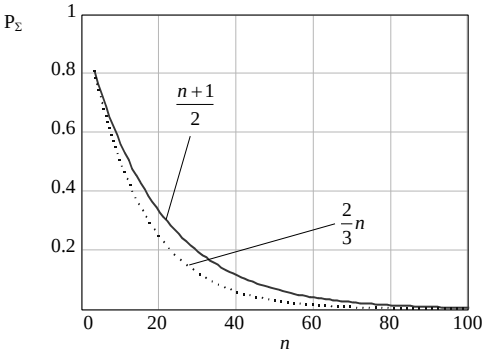

Рисунок 3 – Імовірність успішного виконання атаки апаратних помилок для криптопристроїв, що використовують різні мажоритарні функції

Підвищення продуктивності при структурній надлишковості.

Для вирішення проблеми забезпечення високого рівня продуктивності, як правило, застосовують спеціальні конвеєрні архітектури пристроїв для апаратної реалізації. Проте конвеєрні архітектури не можуть бути застосовані до деяких типів криптопристроїв, наприклад, для пристроїв потокового шифрування. Тому у даному пункті запропоновано використовувати каскади з модулів, що реалізують задану криптографічну функцію. Нижче також наведено теоретичні співвідношення, що можуть слугувати за критерії стосовно знаходження оптимальної архітектури крипто-пристрою з точки зору як забезпечення необхідного рівня продуктивності, так і високого рівня стійкості до атак апаратних помилок.

На рис.4 зображено узагальнену архітектуру двокаскадного криптопристрою, побудованого на базі традиційного резервування з однотипними модулями.

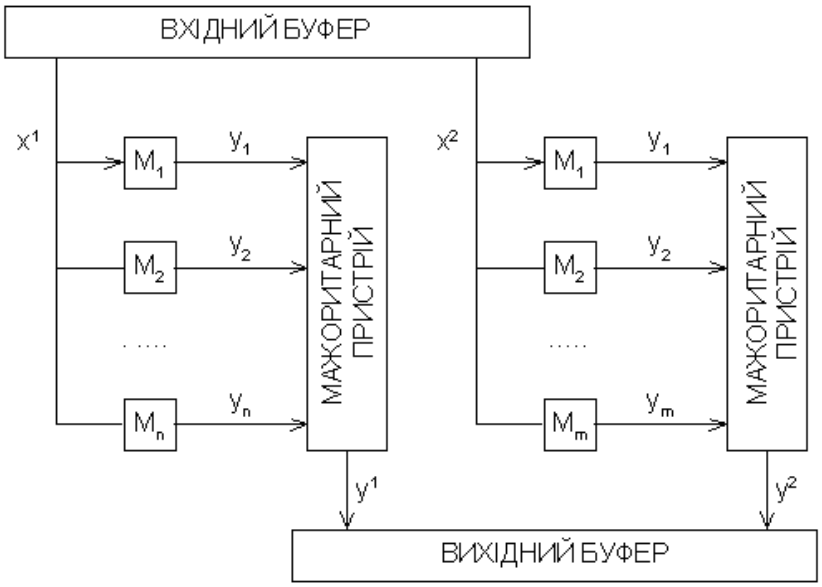

Рисунок 4 – Узагальнена архітектура двокаскадного криптопристрою з однотипним резервуванням

У загальному випадку кількість модулів резервування може не співпадати в каскадах ($m \neq n$). Час затримки опрацювання сигналу пристроєм для двокаскадної архітектури визначається як :

$$d_{\Sigma} = \frac{\max(d_i^1, d_i^2) + \max(d_M^1, d_M^2)}{2} \cong \frac{d_0 + d_M}{2}, \tag{11}$$

а для загального випадку однотипного резервування при *k* каскадах:

$$d_{\Sigma} = \frac{\max(d_i^k) + \max(d_M^k)}{k} \cong \frac{d_0 + d_M}{k}. \tag{12}$$

Апаратні затрати визначаються такими співвідношеннями:

а) двокаскадний випадок :

$$c_{\Sigma} = \sum_{i=1}^{n} c_i^1 + \sum_{j=1}^{m} c_j^2 + c_м^1 + c_м^2 \cong n \cdot c_0^1 + m \cdot c_0^2 + c_м^1 + c_м^2 \cong (m+n)c_0 + 2c_м ; \tag{13}$$

б) загальний випадок при використанні усіх однотипних блоків та при однаковій кількості блоків резервування у кожному з каскадів:

$$c_{\Sigma} = \sum_{j=1}^{k} \sum_{i=1}^{n} c_{ij}^0 + \sum_{j=1}^{k} c_j^M \cong k \cdot \left(n \cdot c_0 + c_м\right). \tag{14}$$

Надійність роботи такого складного пристрою в загальному випадку буде визначитися за формулою:

$$P_{\Sigma} = \prod_k \left(1 - \frac{Maj^k(n)}{n} \cdot \left(1 - P_0^k\right)\right) \cdot P_м^k . \tag{15}$$

У випадку використання всіх однотипних блоків та при однаковій кількості блоків резервування у кожному з каскадів формула (15) набуде вигляду:

$$P_{\Sigma} = P_{м}^{k} \cdot \left(1 - \frac{Maj\ (n)}{n} \cdot \left(1 - P_{0}\right)\right)^{k}. \tag{16}$$

Для оцінки складності виконання атаки апаратних помилок застосуємо ті ж самі теоретичні викладки, що й раніше. Тоді загальна імовірність успішного виконання атаки для криптопристрою, побудованого за схемою рис. 4, буде визначатися як:

$$P_{\Sigma}^{A} = \left({}^{1}P_{0}^{A}\right)^{Maj^{1}(n)} \cdot \left({}^{2}P_{0}^{A}\right)^{Maj^{2}(m)}, \tag{17}$$

для загального випадку інвертування *k* бітів:

$$P_{\Sigma}^{A} = \prod_{k} \left({}^{k}P_{0}^{A}\right)^{Maj^{k}(n)}, \tag{18}$$

а для випадку використання усіх однотипних блоків та при однаковій кількості блоків резервування у кожному з каскадів отримаємо:

$$P_{\Sigma}^{A} = \left(P_{0}^{A}\right)^{Maj(n)^{k}}. \tag{19}$$

На рис. 5 зображено сімейства залежностей імовірності правильної роботи пристрою та імовірності успішної атаки на криптопристрій для випадку застосування мажоритарної функції (3). Були вибрані такі параметри: імовірність успішної атаки для одного базового блока резервування $P_{0}^{A} = 0.9$, імовірності правильної роботи вузлів пристрою $P_{0} = P_{M} = 0.9$, а кількість блоків резервування в одному каскаді *n* була рівна відповідно 3, 5 та 7.

Аналіз рисунку показує, що навіть за умови однакової імовірності як правильного функціонування блока резервування, так і криптоатаки на нього загальне значення надійності роботи пристрою є суттєво вищим за імовірність атаки при застосуванні багато-каскадного резервування.

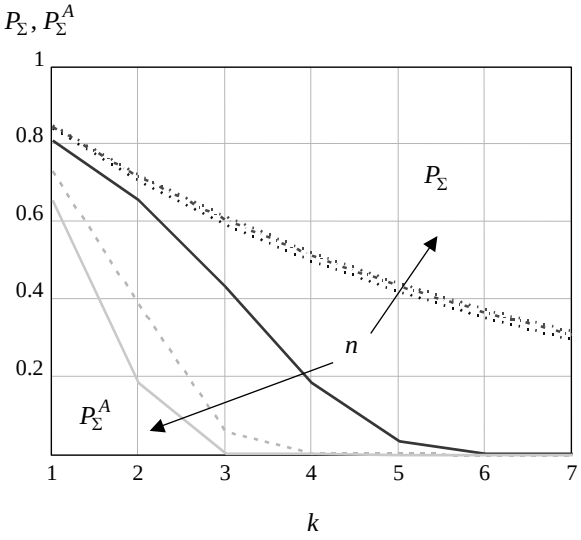

Рисунок 5 – Сімейства залежностей імовірності правильної роботи пристрою та імовірності успішної атаки на криптопристрій

Проте слід зауважити, що в деяких випадках для зловмисника не лише не є необхідністю інвертувати кілька бітів одночасно, а навпаки, корисно мати можливість інвертувати лише один біт даних. У такому випадку імовірність успішного виконання атаки буде меншою і буде визначатися відповідно формулами:

$$P_{\Sigma}^{A} = \min\left(\min\left({}^{k}P_{0}^{A}\right)^{Maj^{k}(n)}\right) \ \forall k, \tag{20}$$

$$P_{\Sigma}^{A} = \left(P_0^{\mathrm{A}}\right)^{Maj(n)}. \tag{21}$$

Цю особливість слід враховувати при проектуванні високопродуктивних криптопристроїв, що можуть піддаватися атакам спеціальних впливів.

Резервування Мак-Класкі.

У роботі [18] Мак-Класкі запропонував для підвищення працездатності пристроїв при резервуванні використовувати не однотипні, а різнотипні модулі, що реалізують одну й ту ж функцію. Такий підхід суттєво дозволяє підвищити виживаність складних космічних систем. У даній роботі запропоновано використати ідею Мак-Класкі для побудови криптопристроїв, стійких до атаки апаратних помилок.

За означенням усі модулі різнотипні, тобто $M_1 \neq M_2 \neq ... \neq M_i ... \neq M_n$, а також $P_1 \neq P_2 \neq ... \neq P_i ... \neq P_n$ (див. рис. 1).

Час затримки опрацювання сигналу пристроєм визначається як:

$$d_{\Sigma} = \max(d_i) + d_M . \tag{22}$$

Апаратні затрати:

$$c_{\Sigma} = \sum_{i=1}^{n} c_i + c_M . \tag{23}$$

Імовірність безпомилкової роботи пристрою можна визначити як:

$$P_{\Sigma} = \left(1 - \frac{1}{n} \cdot \prod_{i=1}^{Maj(n)} (1 - P_i)\right) \cdot P_M . \tag{24}$$

Проте, оскільки $P_1 \neq P_2 \neq ... \neq P_i ... \neq P_n$, то існує певна невизначеність стосовно остаточного значення параметру P_{Σ}. Тому від оцінки конкретних параметрів імовірності безпомилкової роботи слід перейти до оцінок їх математичного сподівання та дисперсії, що дасть змогу оцінити найгірший/найкращий випадок, а також тенденції щодо зменшення надійності роботи пристрою.

Якщо математичне сподівання та дисперсію імовірності правильної роботи мажоритарного пристрою позначити за $M[P_M]$ та $D[P_M]$, а також припустити, що усі параметри розподілені за нормальним законом, то можна визначити співвідношення для оцінки математичного сподівання та дисперсії імовірності безпомилкової роботи цілого пристрою:

$$M[P_{\Sigma}] = \left(1 - \frac{Maj(n)}{n} \cdot (1 - M[P_i])\right) \cdot M[P_M], \tag{25}$$

$$D[P_{\Sigma}] = D[P_M] \cdot \left(1 + \frac{Maj(n)}{n}\right) + \frac{Maj(n)}{n} \cdot \left(D[P_M]D[P_i] + M^2[P_M]D[P_i] + D[P_M]M^2[P_i]\right). \tag{26}$$

Якщо за P_i^A позначити імовірність успішної реалізації атаки зловмисником для одного модуля, то загальна імовірність успішного виконання атаки для криптопристрою, побудованого за резервуванням Мак-Класкі з мажоритарною функцією (3) буде визначатися як:

$$P_{\Sigma}^{A} = S\left(\frac{\mathrm{n}+1}{2}\right) \prod_{\mathrm{i}=1}^{\frac{\mathrm{n}+1}{2}} \left(P_i^A\right), \tag{27}$$

а для крипто-пристрою з мажоритарною функцією (7) як:

$$P_{\Sigma}^{A} = S\left(\frac{2\mathrm{n}}{3}\right) \prod_{i=1}^{\frac{2\mathrm{n}}{3}} \left(P_i^A\right), \tag{28}$$

де $S(\bullet)$ – функція складності виконання атаки для кожного блоку резервування.

V Висновки

Структурна надлишковість може бути ефективним способом боротьби з атаками апаратних помилок. В даній роботі автором розроблено математичні співвідношення для оцінки продуктивності, апаратних затрат,

надійності роботи пристрою та імовірності успішної атаки криптоаналітиком на апаратні засоби захисту інформації. Показано, що вказані параметри суттєво залежать від типу використаної мажоритарної функції та надійнісних характеристик базових модулів. Цікавим є застосування резервування Мак-Класкі, що характеризується певною нерегулярністю надійнісних показників базових модулів. Отримані автором результати розширюють теоретичний базис проектування апаратних засобів захисту інформації і можуть бути використанні для побудови реальних криптографічних пристроїв з підвищеним рівнем стійкості до атаки апаратних помилок.

Література: ***1.*** *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф.Шаньгина, - М.: Радио и связь, 1999. -328 с.* ***2*** *.Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Изд. Дом «Вильямс», 2001 – 672 с.: ил.* ***3****. Proceedings of 1st International Workshop on Cryptographic Hardware and Embedded Systems – CHES 1999, Worcester, MA, USA, August 1999, LNCS 1717.* ***4****. Proceedings of 2nd International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2000, Worcester, MA, USA, August 17 – 18, 2000, LNCS 1965.* ***5****. Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2001, Paris, France, May 14 – 16, 2001, LNCS 2162.* ***6.*** *Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2002, Redwood Shores, CA, USA, August 13 – 15, 2002, LNCS 2523.* ***7****. Proceedings of 5th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2003, Cologne, Germany, September 8 – 10, 2003, LNCS 2779.* ***8*** *.Biham E., Shamir A. Differential Fault Analysis of Secret Key Crypthosystems // In Proceedings of the 17-th Int. Conf. "Advance in Cryptology - CRYPTO`97". Santa Barbara, USA, 1997, V.1294, pp.513 – 525.* ***9****. Alexander Muir. Techniques of Side Channel Cryptanalysis / Thesis for the degree of Master of Mathematics in Combinatorics and Optimization, Waterloo, Ontario, Canada, 2001, p. 92.* ***10****. Thomas Wollinger and Christof Paar. How Secure Are FPGAs in Cryptographic Applications? // In Proceedings of the 13-th International Conference on Field Programmable Logic and Applications - FPL 2003, Lisbon, Portugal, September 1 - 3, 2003. 11.Sergei P. Skorobogatov and Ross J. Anderson. Optical Fault Induction Attacks. // In Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2002, Redwood Shores, CA, USA, August 13 – 15, 2002, LNCS 2523, pp. 2 - 12.* ***12****. А. Л. Чмора. Современная прикладная криптография. 2-е изд., стер. – М.:Гелиос АРВ, 2002. – 256 с.: ил.* ***13.*** *Молдовян А. А., Молдовян В. А., и др. Криптография. – Серия "Учебники для вузов. Специальная литература". – Спб.: Издательство "Лань", 2000. – 224 с., ил.* ***14****. Benoit Chevallier-Mames, Mathieu Ciet and Marc Joye. Low-Cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity. // Cryptology ePrint Archive, Report 2003/237.* ***15****. G3 Card. / Public Final Report. IST-1999-13515. G3 Card Consortium – January 2003.* ***16****. Ramesh Karri, Grigori Kuznetsov, and Michael Goessel. Parity-Based Concurrent Error Detection of Substitution-Permutation Network Block Ciphers. // In Proceedings of 5th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2003, Cologne, Germany, September 8–10, 2003, LNCS 2779, pp.113-124.* ***17****. Ramesh Karri, Kaijie Wu, Piyush Mishra and Yongkook Kim. Concurrent Error Detection of Fault-Based Side-Channel Cryptanalysis of 128-bit Symmetric Block Ciphers // IEEE Transactions on CAD, Dec. 2002.* ***18****. Proceedings of International Conference on Evolvable Hardware EH 2002 NASA/DoD, 15-18 July 2002, Alexandria, USA, IEEE Computer Press ISBN 0-7695-1718-8*

УДК 621.3

СТАТИСТИЧНА МОДЕЛЬ СУМАТОРА ЗА МОДУЛЕМ 2^N ДЛЯ ПРОВЕДЕННЯ ІНЖЕНЕРНО-КРИПТОГРАФІЧНИХ АТАК ЗА ПОБІЧНИМИ КАНАЛАМИ ВИТОКУ ІНФОРМАЦІЇ

Леся Коркішко, Ігор Васильцов
Тернопільська академія народного господарства

Анотація: **Запропоновано статистичну модель, досліджено її властивості та запропоновано методику проведення інженерно-криптографічних атак за побічними каналами витоку інформації на комп'ютерну реалізацію операції додавання за модулем 2N.**
Summary: **For realization of modular addition with 2N modulus the statistical model has been proposed. Its properties were investigated and a method for the side-channel attack has been proposed.**
Ключові слова: **Інженерно-криптографічні атаки, статистична модель, витік інформації.**