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.**

Вступ

Із розширенням областей застосування електронного обміну інформацією загострюється проблема неавторизованого доступу до даних, які передаються, зберігаються чи обробляються. Одним із можливих варіантів вирішення цієї проблеми є застосування до даних перед їх відправленням криптографічних перетворень, наприклад зашифрування із використанням невідомих даних – таємного ключа. При компрометації алгоритму шифрування (успішного його математичного криптографічного аналізу) виникає можливість доступу до даних, які піддавалися зашифруванню без відомостей про ключ зашифрування. У сучасних комп'ютерних системах, які реалізують криптографічні перетворення для забезпечення захисту даних, використовуються достатньо стійкі до математичного криптографічного аналізу алгоритми криптографічних перетворень. Тому для визначення ключа шифрування і наступного доступу до даних використовується інженерно-криптографічний аналіз [1 – 8]. Інженерно-криптографічний аналіз передбачає використання інформації, що отримується, шляхом спостереження за роботою пристроїв, які реалізують криптографічні перетворення. Цей аналіз часто називають інженерно-криптографічними атаками. Основними каналами отримання такої інформації, так званими побічними каналами, є час виконання криптографічних операцій, споживана потужність пристрою, електромагнітне випромінювання пристрою [1 – 8]. Аналіз споживаної потужності криптографічного пристрою в процесі опрацювання ним інформації є одним із найбільш ефективних та дешевих способів атаки. Тому актуальною задачею при розробці комп'ютерних пристроїв для реалізації криптографічних перетворень є мінімізація інформації, яка доступна за побічними каналами її витоку, зокрема інформації про статистичні відмінності споживаної потужності пристрою в залежності від опрацьовуваних даних.

Відомі роботи з проведення інженерно-криптографічного аналізу комп'ютерних реалізацій алгоритмів криптографічних перетворень, наприклад, DES [3, 4, 6], RSA [2, 5], AES [6] тощо. Базою для проведення цього аналізу є інженерно-криптографічні атаки з використанням статистичних моделей складових операцій криптографічних перетворень та моделі витоку інформації з комп'ютерних засобів. Оскільки статистична модель для побітової операції додавання за модулем 2 є достатньо добре описаною та дослідженою [7, 8], дана робота присвячена актуальній задачі створенню статистичної моделі операції додавання за модулем 2^N і розробці методики атакування реалізацій цієї операції. Дана статистична модель базується на лінійній моделі витоку інформації про Хемінгову вагу даних, які обробляються [8], і дозволяє проводити інженерно-криптографічні атаки з використанням інформації з споживаної потужності комп'ютерного пристрою, який реалізує операцію додавання за модулем 2^N.

I Модель витоку інформації для інженерно-криптографічних атак

Для проведення інженерно-криптографічних атак приймемо, що [8]:

- аргументами операції додавання за модулем 2^N є відкритий текст P і таємні дані K;
- комп'ютерний пристрій, який реалізує алгоритм криптографічного перетворення з використанням операції додавання за модулем 2^N, уможливлює витік інформації про Хемінгову вагу результату S;
- витік інформації можливий завдяки зміні значення споживаного струму, а тому і завдяки зміні споживаної потужності, яку споживає пристрій;
- пристрій споживає більший струм при обробці даних з більшою Хемінговою вагою, залежність споживаного струму від Хемінгової ваги є лінійною.

Нехай потужність, що споживається у момент часу j, представлена у вигляді $P[j]$. Для моделювання каналу витоку інформації у сигналі $P[j]$ скористаємося лінійною залежністю, запропонованою у [8]:

$$P[j] = \varepsilon \cdot d[j] + L + n \qquad (1)$$

де $d[j]$ репрезентує Хемінгову вагу результату в момент часу j, ε – вклад у споживану потужність кожної одиниці Хемінгової ваги даних, L – споживана постійна загальна потужність, n – шум з нульовим середнім значенням.

II Атака на реалізацію операції додавання за модулем 2

Нехай j позначає момент часу, коли виконується операція додавання за модулем 2. Тоді сума $S = K \oplus P$, де K – N-бітовий невідомий доданок, P – N-бітовий відкритий текст. Розглянемо атаку, запропоновану в [8] на N-бітовий суматор за модулем 2, метою якої є визначення бітів K без відомостей про значення бітів S. Припустимо, що залежність між споживаною потужністю у момент часу j і Хеммінговою вагою результату, який отримується, описується виразом (1). Тоді узагальнений алгоритм атаки на реалізацію операції додавання за модулем 2 є таким:

```
Для і від 0 до N-1 {
        Для b=0 до 1 {
                Обчислити усереднене значення сигналу споживаної потужності Ab[j] {
                Встановити і-й біт P рівним b;
                Встановити решту бітів P у випадкові значення;
                Зібрати дані про споживану потужність пристрою;
                }
        }
      Обчислити диференційний сигнал T[j] = A0[j] – A1[j];
      Якщо T[j] > 0, то і-й біт K є "1", якщо T[j] < 0 то і-й біт K є "0";
}
```

Результативність цієї атаки базується на незалежності очікуваного значення Хемінгової ваги результату додавання за модулем 2 від позиції біту, який піддається аналізу. Тут очікуване значення *E* Хемінгової ваги *d* залежить лише від комбінації значень бітів k_i і p_i та розрядності *N* суматора [8]:

$$E\left[d \middle| k_i \oplus p_i = 0\right] = \frac{N-1}{2}, \tag{2}$$

$$E\left[d \middle| k_i \oplus p_i = 1\right] = \frac{N+1}{2}. \tag{3}$$

Якщо $k_i = 0$, то для моменту часу j^* виконання операції додавання за модулем 2 вирази для $A_0[j^*]$ і $A_1[j^*]$ можна переписати з врахуванням (2) і (3) у термінах очікуваних значень Хемінгової ваги суми і *P* з (1):

$$A_0[j^*] \approx E\left[P \middle| k_i = 0, p_i = 0\right] = E\left[d \cdot \varepsilon + L + n \middle| k_i = 0, p_i = 0\right] = \frac{N-1}{2} \cdot \varepsilon + L, \tag{4}$$

$$A_1[j^*] \approx E\left[P \middle| k_i = 0, p_i = 1\right] = E\left[d \cdot \varepsilon + L + n \middle| k_i = 0, p_i = 1\right] = \frac{N+1}{2} \cdot \varepsilon + L. \tag{5}$$

Тоді значення диференційного сигналу

$$T_0[j^*] = A_0[j^*] - A_1[j^*] \approx -\varepsilon, \text{ за умови, що } k_i = 0. \tag{6}$$

Аналогічно можна побудувати вирази для $A_0[j^*]$ і $A_1[j^*]$ для випадку $k_i = 1$. Тоді значення диференційного сигналу складе

$$T_1[j^*] = A_0[j^*] - A_1[j^*] \approx \varepsilon, \text{ за умови, що } k_i = 1. \tag{7}$$

Отже, з виразів (6) і (7) випливає, що диференційний сигнал буде містити додатній пік за умови $k_i = 1$ і від'ємний пік за умови $k_i = 0$.

Розглянута статистична модель виконання операції додавання за модулем 2 дозволяє проводити інженерно-криптографічну атаку за споживаною потужністю і успішно визначати невідомий доданок *K* [8].

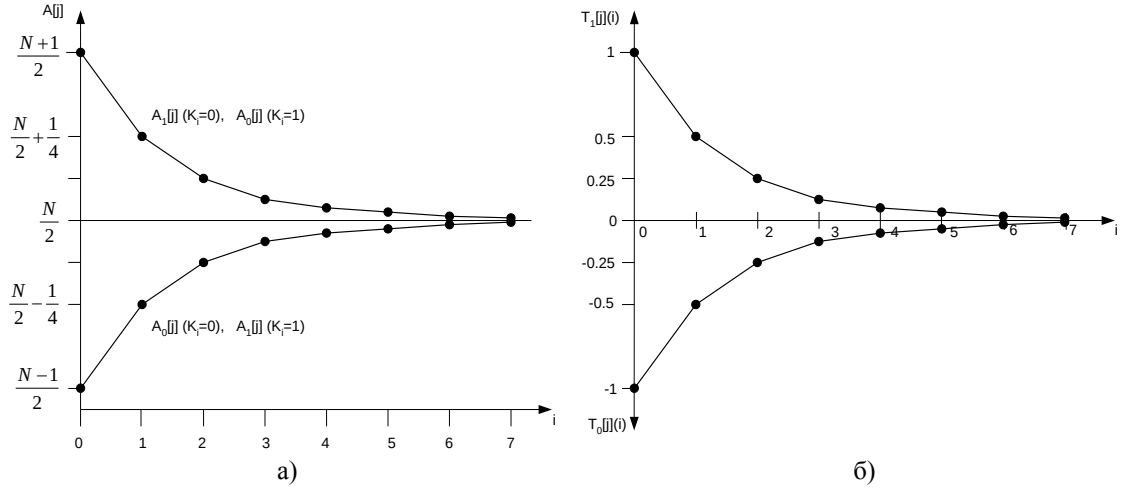
III Побудова статистичної моделі суматора за модулем 2^N

Однак, при проведенні даної атаки на операцію додавання за модулем 2^N очікувані значення Хемінгової ваги результату додавання $S = (K + P) \bmod 2^N$ будуть залежати від бітів переносу з молодших розрядів:

- для $k_i = 0$: $A_0[j^*] \approx \varepsilon \cdot \left(\frac{N}{2} - \frac{1}{2^{i+1}}\right) + L$, $A_1[j^*] \approx \varepsilon \cdot \left(\frac{N}{2} + \frac{1}{2^{i+1}}\right) + L$, $T_0[j^*] \approx -\frac{\varepsilon}{2^i}$;
- для $k_i = 1$: $A_0[j^*] \approx \varepsilon \cdot \left(\frac{N}{2} + \frac{1}{2^{i+1}}\right) + L$, $A_1[j^*] \approx \varepsilon \cdot \left(\frac{N}{2} - \frac{1}{2^{i+1}}\right) + L$, $T_1[j^*] \approx \frac{\varepsilon}{2^i}$.

Отже, очікуване значення Хемінгової ваги результату додавання буде різним для кожного біту, а для визначення *i*-го біту невідомого доданка *K* в процесі аналізу суматора за модулем 2^N потребує роздільної здатності вимірювального пристрою мінімум $\varepsilon/2^{i+2}$.

Із збільшенням номеру біта, який піддається аналізу, зменшується різниця між $A_0[j^*]$ і $A_1[j^*]$ (рис. 1, а), що ускладнює реєстрацію сигналу споживаної потужності та наступне виділення корисної інформації з диференційного сигналу, оскільки завжди є вплив шуму на результати вимірювання (рис. 1, б).



а) б)

Рисунок 1 – Вплив номера позиції біту *i* доданка операції додавання за модулем 2^N на: а) очікуване значення Хемінгової ваги при різних значеннях невідомого доданку, б) значення диференційного сигналу

Отримані результати пояснюються впливом значень бітів з номерами i – 1,..., 0 на значення i–го біту, який аналізується. Тому, проведемо аналіз залежності величини очікуваного значення Хемінгової ваги результату від значень бітів доданку K з номерами i – 1,..., 0.

Позначимо біти доданка K через $\{k_{N-1}, k_{N-2}, ..., k_i, ..., k_1, k_0\}$. Тоді очікуване значення Хемінгової ваги суми за модулем 2^N для $k_i = \nu$, $i > 0$, $\nu = \{0, 1\}$ можна визначити з виразів:

$$A_0^{\nu}[j^*] \approx \varepsilon \cdot \begin{cases} 1 + \sum_{r=0}^{i-1} k_r \cdot 2^{r-i}, & \nu = 0 \\ 2 - \sum_{r=0}^{i-1} k_r \cdot 2^{r-i}, & \nu = 1 \end{cases}, \tag{8}$$

$$A_1^{\nu}[j^*] \approx \varepsilon \cdot \begin{cases} 2 - \sum_{r=0}^{i-1} k_r \cdot 2^{r-i}, & \nu = 0 \\ 1 + \sum_{r=0}^{i-1} k_r \cdot 2^{r-i}, & \nu = 1 \end{cases}. \tag{9}$$

Використовуючи (8) і (9), можна визначити значення диференційного сигналу $T_{\nu}[j^*]$:

$$T_{\nu}[j^*] \approx \varepsilon \cdot \begin{cases} 2\sum_{r=0}^{i-1} k_r \cdot 2^{r-i} - 1, & \nu = 0 \\ 1 - 2\sum_{r=0}^{i-1} k_r \cdot 2^{r-i}, & \nu = 1 \end{cases}. \tag{10}$$

Зауважимо, що амплітуда диференційного сигналу не залежить від значень старших бітів $\{k_{N-1}, k_{N-2}, ..., k_{i+2}, k_{i+1}\}$, а визначення значення деякого біту базується на здатності відрізняти значення різних диференційних сигналів $T_{\nu}[j^*]$. Покажемо, що при аналізуванні диференційного сигналу існують випадки, коли неможливо визначити значення k_i. Для цього розглянемо випадок $T_0[j^*] = T_1[j^*]$, тобто

випадок, коли очікувані значення Хемінгової ваги суми для $k_i = 0$ і $k_i = 1$ є рівними. Виконання останньої рівності можливе за умови виконання рівності:

$$\sum_{r=0}^{i-1} k_r \cdot 2^{r-i} = \frac{1}{2}. \tag{11}$$

Виконання рівності (11) можливе лише за умов $k_{i-1} = 1$ і $\{k_{i-2} = 0, ..., k_1 = 0, k_0 = 0\}$. Інші комбінації значень $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$ будуть зумовлювати появу різних значень диференційних сигналів $T_v[j^*]$. Тому при однаковій ймовірності появи одиничних значень бітів k_i, щонайменше половина бітів *K* буде визначена неправильно.

IV Методика атаки на реалізацію операції додавання за модулем 2^N

Для однозначного визначення значень бітів невідомого доданку *K* необхідно усунути або зменшити вплив попередніх бітів на результат додавання бітів k_i і p_i. Врахуємо, що при визначенні значення біту k_0 значення диференційного сигналу є ±ε і не залежить від значення інших бітів.

Оскільки значення попередніх бітів впливають на значення суми поточного біту через переноси з молодших розрядів у старші, задачу зменшення впливу бітів можна сформулювати як задачу усунення генерування переносів із молодших бітів у аналізований.

Для цього розглянемо задачу отримання максимальної амплітуди $T_v[j^*]$ у вигляді:

$$T_v[j^*] = \max, v = \{0,1\}. \tag{12}$$

Із врахуванням (10), вираз (12) можна переписати у вигляді:

$$T_v[j^*] \approx \varepsilon \cdot \begin{cases} 2\sum_{r=0}^{i-1} k_r \cdot 2^{r-i} - 1, & v = 0 \\ 1 - 2\sum_{r=0}^{i-1} k_r \cdot 2^{r-i}, & v = 1 \end{cases} = \max \Rightarrow T_v[j^*] \approx \varepsilon \cdot \begin{cases} \sum_{r=0}^{i-1} k_r \cdot 2^{r-i} = 0, & v = 0 \\ \sum_{r=0}^{i-1} k_r \cdot 2^{r-i} = 0, & v = 1 \end{cases}. \tag{13}$$

Виконання правої частини виразу (13) можливе лише за умови, що усі молодші біти $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$ рівні нулю. Однак, оскільки ми не маємо змоги контролювати значення бітів $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$, вираз (13) може застосовуватися лише для визначення бітів невідомого доданка *K* з низькою Хемінговою вагою та розрідженим розташуванням бітів з одиничними значеннями.

Для визначення бітів довільних *K* можна встановлювати молодші біти $\{p_{i-1}, p_{i-2}, ..., p_1, p_0\}$ у нульове значення чи у інвертовані значення вже визначених бітів $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$. У першому випадку біти суми $\{s_{i-1}, s_{i-2}, ..., s_1, s_0\}$ будуть рівними $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$, біти переносів генеруватися не будуть. Другий випадок передбачає встановлення $\{p_{i-1}, p_{i-2}, ..., p_1, p_0\}$ у відповідні значення $\{\overline{k_{i-1}}, \overline{k_{i-2}}, ..., \overline{k_1}, \overline{k_0}\}$. Це, у свою чергу, призведе до встановлення бітів суми $\{s_{i-1}, s_{i-2}, ..., s_1, s_0\}$ у одиничні значення, перенос у біт з номером *i* генеруватися не буде.

В обох випадках значення $A_0^v[j^*]$ і $A_1^v[j^*]$ будуть містити константні адитивні компоненти, пропорційні Хемінговій вазі коду $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$. Тому при подальшому обчисленні диференційних сигналів $T_v[j^*]$ ці адитивні значення будуть взаємно компенсовані, а значення диференційних сигналів для визначення значення біту k_i будуть максимальні і складати ± ε.

Встановлювати $\{p_{i-1}, p_{i-2}, ..., p_1, p_0\}$ в одиничні значення чи у значення вже визначених бітів $\{k_{i-1}, k_{i-2}, ..., k_1, k_0\}$ є недоцільним, бо у цьому випадку будуть генеруватися переноси між розрядами і визначення бітів доданку *K* не буде однозначним.

Таким чином, атаку на реалізацію операції додавання за модулем 2^N можна проводити згідно з таким алгоритмом:

```
Для і від 0 до N-1 {
        Для b=0 до 1 {
                Обчислити усереднене значення сигналу споживаної потужності A_b[j] {
                Встановити і-й біт P рівним b;
                Якщо i>0, встановити біти P з номерами i-1,...,0 у нуль.
                Встановити решту біти P з номерами N-1,...,i+1 у випадкові значення;
                Зібрати дані про споживану потужність пристрою;
                }
        }
        Обчислити диференційний сигнал T[j] = A_0[j] – A_1[j];
        Якщо T[j] > 0, то і-й біт K є “1”, якщо T[j] < 0 то і-й біт K є “0”;
}
```

Наведений алгоритм дозволяє визначати усі невідомі біти доданка *K*. При цьому постійні складові очікуваного значення Хемінгової ваги суми будуть змінюватися для кожного розряду. Аналогічного результату можна досягти, використавши модифікацію наведеного алгоритму, встановлюючи біти $\{p_{i-1}, p_{i-2}, \ldots, p_1, p_0\}$ у інвертовані значення вже визначених бітів доданку *K*. При цьому очікуване значення Хемінгової ваги суми буде лінійно зростати для кожного невідомого розряду.

Висновки

Інженерно-криптографічні атаки на реалізацію криптографічних алгоритмів є потужними методами визначення невідомої інформації, яка використовується для перетворення даних. В роботі розглянуто проведення такої атаки на реалізацію операції додавання за модулем 2^N з використанням одного з можливих каналів витоку інформації – споживаної потужності пристрою. При цьому визначено очікувані значення Хемінгової ваги суми для визначення значення кожного біту невідомого доданку. Встановлено, що використання відомого алгоритму атаки на реалізацію операції додавання за модулем 2 призводить до зменшення очікуваних значень. Це, у свою чергу, призводить до необхідності висування жорстких вимог до вимірювальних пристроїв, зниження завад при вимірюванні для ідентифікації значень бітів.

Проведено дослідження залежності величини очікуваного значення Хемінгової ваги результату додавання за модулем 2^N від значень попередніх до аналізованого бітів невідомого доданку та встановлено, що можливі такі комбінації значень бітів невідомого доданку, за яких неможливо однозначно встановити значення біту, який аналізується.

З метою однозначної ідентифікації бітів невідомого доданку сформульовано та розв’язано задачу отримання максимального диференційного сигналу за допомогою маніпулювання значеннями бітів відкритого тексту. Для цього запропоновано два варіанти модифікування бітів відкритого тексту – встановлення усіх молодших бітів від аналізованого біту у нульові значення і встановлення цих бітів рівними інвертованим значенням бітів невідомого доданку, визначених на попередніх етапах.

На основі відомого алгоритму атаки на реалізацію операції додавання за модулем 2 запропоновано алгоритм атаки на реалізації операції додавання за модулем 2^N з усуненням впливу попередніх розрядів, що дало змогу отримати максимальну величину диференційного сигналу. Запропонований алгоритм атаки на реалізацію операції додавання за модулем 2^N можна використати при дослідженні і сертифікуванні комп’ютерних засобів [9], які реалізують алгоритми криптографічних перетворень з використанням операції додавання за модулем 2^N відкритого тексту і невідомих даних.

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. Clavier C., Coron J.-S., Dabbous N., Differential power analysis in the presence of hardware countermeasures // 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. 252 – 263. 3. Kocher P., Jaffe J., Jun B., Differential Power Analysis // In proceedings of International conference CRYPTO’99, vol. 1666 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 1999. – P. 388 – 397. 4. 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. 5. 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. 6. Akkar, M., Giraud, C. An

implementation of DES and AES, secure against some attacks // In Proc. Cryptographic Hardware and Embedded Systems – CHES 2001, volume 2162 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2001. – P. 309-318. 7. Akkar M.-L., Bevan R., Dischamp P., Moyart D., Power analysis, what is now possible // T. Okamoto, Eds., International conference ASIACRYPT 2000, vol. 1976 of Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, 2000. – P. 489 – 502. 8. 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. 9. Federal information processing standards publication. Security requirements for cryptographic modules. FIPS 140 – 2. National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2001. – 68 p.

УДК 691.3.06

ПОКАЗНИКИ ОЦІНКИ ЕФЕКТИВНОСТІ АЛГОРИТМІВ ШИФРУВАННЯ НА ЕЛІПТИЧНИХ КРИВИХ

Микола Карпінський*, Ігор Васильцов, Ігор Якименко
**Університет в Бєльську-Бялей, Польща,*
Тернопільська академія народного господарства

Анотація: **Запропоновано показники для оцінки ефективності застосування алгоритмів шифрування на еліптичних кривих для задач захисту інформації. Для оцінки вказаних показників сформовано критерії.**
Summary: **In this paper the authors have proposed the parameters to estimate the effectiveness of elliptic curve cipher algorithms usage to solve the data protection tasks. To evaluate these parameters some criteria have been formed.**
Ключові слова: **Еліптичні криві, показники ефективності.**

I Постановка задачі

Сучасний системний підхід щодо розробки нових алгоритмів криптографічного перетворення інформації полягає не тільки в забезпеченні криптографічної стійкості алгоритмів, але й ефективності функціонування алгоритму шифрування. Зі стрімким розвитком обчислювальної техніки зростає потреба в передачі великих об'ємів інформаційних ресурсів, що обумовлює жорсткіші вимоги до алгоритмів шифрування стосовно продуктивності та пропускної здатності.

Проте ефективність і стійкість алгоритмів є суперечливими відносно цілей. З одного боку, сучасні алгоритми шифрування повинні бути стійкими не тільки до відомих криптографічних атак, але і до нових методів криптоаналізу. З іншого боку, необхідною умовою для надійного функціонування алгоритмів є ефективність розроблених засобів шифрування.

Ефективність функціонування алгоритмів шифрування можна оцінити ступенем співвідношення отриманих результатів функціонування алгоритмів $R_{рфа}$ і потрібним результатом $R_{пр}$ [1]:

$$P = \left\langle R_{рфа} / R_{пр} \right\rangle . \qquad (1)$$

Потрібний результат $R_{пр}$ полягає у забезпеченні функції конфіденційності шляхом реалізації механізму шифрування. Отриманим результатом функціонування алгоритмів $R_{рфа}$ є реальний рівень забезпечення функції конфіденційності. Співвідношення між $R_{рфа}$ і $R_{пр}$ здійснюється за допомогою показників і показує, наскільки повно реалізована функція конфіденційності.

На сьогоднішній день не існує систематизованої множини показників, які б могли охарактеризувати ефективність функціонування алгоритмів шифрування на еліптичних кривих (ЕК). Формалізація моделі оцінки таких показників дозволить розробникам ще на ранніх етапах проектування здійснювати обґрунтований вибір алгоритму шифрування для ефективної реалізації задач захисту інформації.

II Аналіз літератури

Класичні критерії оцінки секретних систем висвітлені у роботі К. Шенона "Теорія зв`язку в секретних системах": кількість секретності, об'єм ключа, складність операцій шифрування і дешифрування, розмноження помилок, збільшення об'єму повідомлення [2]. Сучасні показники оцінки ефективності