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]:

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

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

функціонування алгоритмів шифрування також характеризують окремі складові алгоритмів. Тому на сьогодні поняття ефективності є комплексним і включає різні складові, такі як: стійкість схеми шифрування, продуктивність засобів шифрування, гнучкість та переносимість реалізації, тощо [1].

Для забезпечення необхідного рівня продуктивності сучасних систем захисту інформації обов'язковою є наявність апаратної складової. Сучасна технологія проектування та виробництва пристроїв захисту інформації все більшу увагу приділяє використанню програмованих логічних інтегральних схем (ПЛІС). Розроблені спеціальні програмні засоби для синтезу цифрових пристроїв на основі різних типів матричних ВІС, що дозволяє користувачу спростити процес проектування та суттєво зменшити час виробництва. Окрім того значно спрощується процедура перенесення проектного рішення з однієї елементної бази на іншу. У роботі [3] наведено переваги застосування ПЛІС для задач захисту інформації. До таких можна віднести: зручність поновлення та модифікації версій алгоритмів шифрування, економічна ефективність використання ресурсів, висока продуктивність, тощо. Тому очевидно, що існуючі передумови акцентують увагу розробників систем захисту інформації не лише на оцінці показників стійкості, але й також ефективності реалізації.

З іншого боку поява апаратних засобів захисту інформації спричинила появу принципово нових методів крипто-аналізу - атаки на реалізацію. До них можна віднести цілий спектр самих різноманітних сучасних атак: аналіз часу виконання окремих операцій, аналіз енергоспоживання, диференційний аналіз помилок, аналіз електромагнітного випромінювання тощо [4 – 8]. Аналіз останніх наукових публікацій показує, що такі атаки можуть бути надзвичайно ефективними, тому при оцінці сучасних алгоритмів шифрування також необхідно враховувати стійкість до таких спеціальних атак на реалізацію.

III Мета роботи

У даній роботі ставиться задача визначити мінімальну кількість показників ефективності алгоритмів шифрування на ЕК, а також формування критеріїв для оцінки вказаних показників.

IV Оцінка ефективності функціонування алгоритмів шифрування

В [1] наведено класифікацію показників і критеріїв ефективності функціонування схем потокового шифрування. Спираючись на підхід, запропонований в [1], а також аналізуючи сучасний стан області застосування ЕК у даній роботі запропоновано використати системний підхід щодо оцінки стійкості та ефективності функціонування алгоритмів шифрування на ЕК.

Основною задачею розробників є забезпечення стійкості алгоритмів на ЕК до відомих методів криптоаналізу. В наш час, за інтенсивного росту інформаційних технологій невід'ємними вимогами до алгоритмів шифрування стали швидкодія, обсяги потрібної пам'яті і т. д.

На рис. 1 зображено показники ефективності функціонування алгоритмів шифрування на ЕК, розділені на чотири категорії:

- показники оцінки стійкості алгоритмів на ЕК;
- програмно-реалізаційні показники;
- апаратно-реалізаційні показники;
- конструктивно-технологічні показники.

Формалізовану модель оцінки ефективності функціонування алгоритмів шифрування на ЕК $R_{пр}$ можна описати наступним чином:

$$\begin{cases} R_{пр} = \alpha_1 \cdot П_{ст} + \alpha_2 \cdot П_{ппр} + \alpha_3 \cdot П_{ар} + \alpha_4 \cdot П_{кт} \\ \sum_{i=1}^{4} \alpha_i = 1 \\ П_{ст} = \left\langle R_{дл}\left\langle R_{гбт}, R_{гп}\right\rangle, R_{сасв}\left\langle R_{го}, R_{ро}\right\rangle\right\rangle \\ П_{ппр} = \left\langle R_{овп}, R_{шші}, R_{квао}\right\rangle \\ П_{ар} = \left\langle R_{аз}\left\langle R_{ле}, R_{еп}, R_{вв}\right\rangle, R_{отч}, R_{оп}\right\rangle \\ П_{кт} = \left\langle R_{пк}, R_{ппа}, R_{п}, R_{зс}\right\rangle \end{cases}, \quad (2)$$

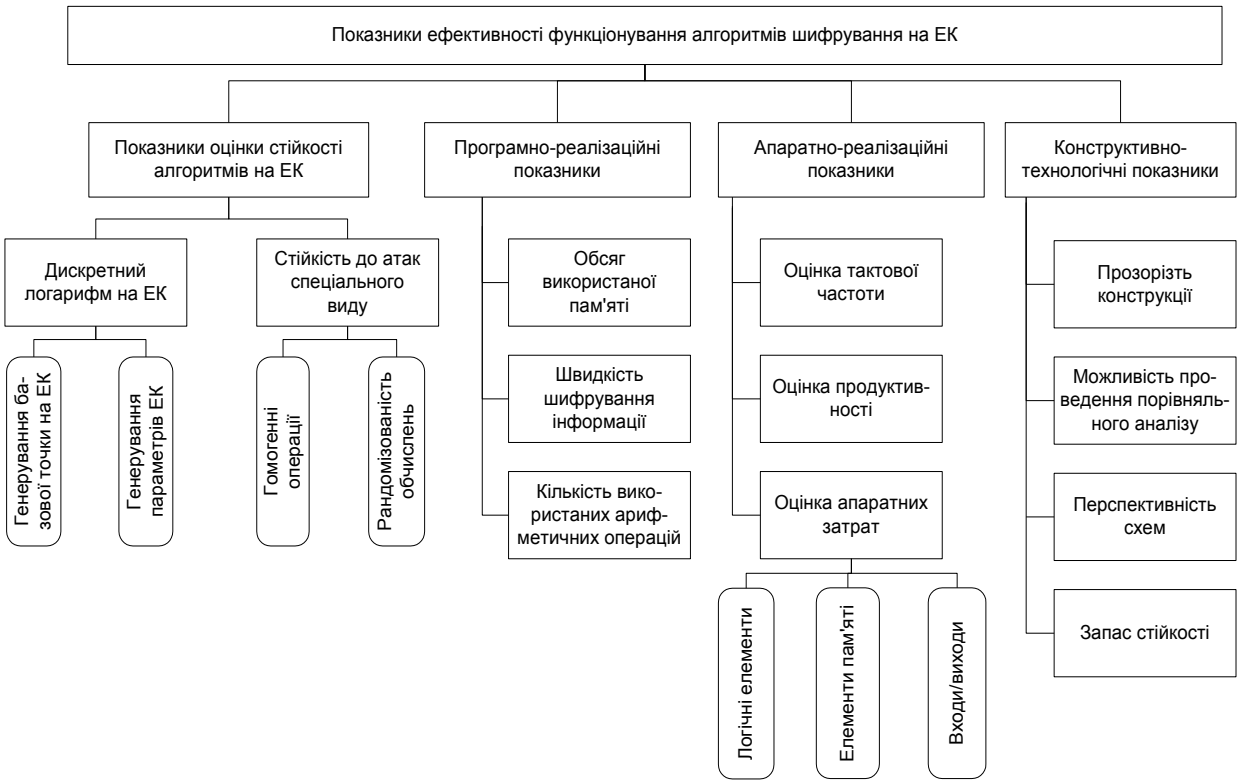

Рисунок 1 – Показники оцінки ефективності функціонування алгоритмів шифрування на ЕК.

де $П_{ст}$ – показники стійкості алгоритмів шифрування на ЕК, характеризують стійкість до аналітичних методів криптоаналізу. Ці показники є домінуючими, бо будь-яке криптографічне перетворення інформації ґрунтується насамперед, на оцінці стійкості алгоритмів шифрування до відомих на сьогодні атак, а також атак спеціального виду. Стійкість алгоритмів шифрування на ЕК залежить від обчислювальної складності дискретного логарифму . Основними складовими показників стійкості є наступні критерії:

$R_{дл}$ – критерій обчислювальної складності дискретного алгоритму на ЕК [9], що залежить від: $R_{гбт}$ – генерування базової точки на ЕК, $R_{гп}$ – генерування параметрів ЕК [10, 11]; $R_{сасв}$ – стійкості до атак спеціального вигляду, що залежить від: $R_{го}$ – гомогенні операції, $R_{ро}$ – рандомізованість обчислень [8]; $П_{пр}$ – програмно-реалізаційні характеризують ефективність програмної реалізації і вказують на практичну цінність схем криптографічного перетворення. Вони включають наступні критерії: $R_{овп}$ – обсяг використаної пам’яті для реалізації алгоритму шифрування на ЕК, $R_{шші}$ – швидкодія шифрування інформації, $R_{квао}$ – кількість використаних арифметичних операцій;

$П_{ар}$ – апаратно –реалізаційні показники характеризують ефективність апаратної реалізації, які вказують на практичні цінності алгоритмів шифрування, і включають наступні критерії: $R_{оз}$ – оцінка апаратних затрат (кількість примітивів): $R_{ле}$ – логічні елементи, $R_{еп}$ – елементи пам’яті, $R_{вв}$ – входи/виходи; $R_{отч}$ – оцінка тактової частоти, $R_{оп}$ – оцінка продуктивності.

$П_{кт}$ – конструктивно-технологічні показники характеризують: $R_{пк}$ – прозорість конструкції, $R_{мтпа}$ – можливість проведення порівняльного аналізу, $R_{п}$ – перспективність схем, $R_{зс}$ – запас їхньої стійкості.

α_i – вагові коефіцієнти, що визначають міру впливу кожного з показників на результуюче значення ефективності. Вони визначаються на основі експертних оцінок залежно від пріоритетного напрямку застосування алгоритмів шифрування в реальних прикладних задачах захисту інформаційних ресурсів.

V Висновки

У роботі формалізовано модель оцінки ефективності функціонування алгоритмів шифрування інформації на ЕК. Дана модель не претендує на повноту, але розглядається як базова, є відкритою і може бути легко доповнена та деталізована в подальшому. Дана модель може бути використана для порівняльного аналізу та квазі-оптимального вибору алгоритму шифрування інформації на ЕК для практичної реалізації засобів захисту інформації. Особливістю вказаної моделі є те, що поряд із традиційними підходами вона дозволяє також враховувати стійкість алгоритму до сучасних атак.

*Література.**1**. Система показателей оценки эффективности функционирования схем поточного шифрования / А. В.Потий, Ю. А.Избенко // Радіотехніка:Всеукр. міжвід. наук.-техн. зб. 2003. вип.. 134. с. 49-61. **2**. К. Шеннон "Теорія зв`язку в секретних системах", 1949 р. **3**. Thomas Wollinger and Christof Paar. How Secure Are FPGAs in Cryptographic Applications. In 13th International Conference on Field Programmable Logic and Applications - FPL 2003, Lisbon, Portugal, September 1-3, 2003. **4**. А. Л. Чмора. Современная прикладная криптография. 2-е изд., стер. – М.:Гелиос АРВ, 2002. – 256 с.: ил. **5**. Молдовян А. А., Молдовян В. А., и др. Криптография. – Серия "Учебники для вузов. Специальная литература". – Спб.: Издательство "Лань", 2000. – 224 с., ил. **6**. 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. **7**. Okeya, K., Sakurai, K., How to Implement Scalar Multiplication Algorithm on Elliptic Curves for Resisting against Power Attacks, Proceedings of the 2000 Engineering Sciences Society Conference of IEICE, A-7-13, (2000). **8**. Okeya K., Sakurai K., Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack, Progress in Cryptology – INDOCRYPT 2000, LNCS1977, (2000), 178-190. **9**. Smar , N .P., The Discrete Logarithm Problem on Elliptic Curves of Trace One, Journal of Cryptology, Vol.12, No.2, (1999), 141-151. **10**. М. Карпінський, І. Васильцов, І. Якименко, Я. Кінах, "Метод генерування параметрів еліптичних кривих", Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні, Київ, випуск 6, с. 74, 2003. **11.** М. Карпінський, І. Васильцов, І. Якименко, А. Гончарик. Elliptic curve Parameters Generetion // Proceedings of the Integrational Conference TCSET'2004 "Modern problems of radio engineering, Telecomunications and computer science", february 24-28, 2004, p. 294-295*

УДК 681.31

ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

Сергей Емельянов, Игорь Яковлев
Одесская национальная юридическая академия

Аннотация: **Рассмотрены общие принципы построения комплексной системы антивирусной защиты (КСАЗ). Проанализированы основные составляющие КСАЗ, показаны проблемные аспекты их практической реализации.**
Summary: **In the article represents the basic principles of construction of complex system of anti-virus protection (CSAP). Basic components CSAP are analyzed, problem aspects of their practical realization are shown.**
Ключевые слова: **Компьютерные вирусы, комплексная система антивирусной защиты, правовые, организационные, программно-технические методы антивирусной защиты.**

I Введение

В настоящее время одной из реальных угроз конфиденциальности, целостности и доступности информации в компьютерных системах и сетях (КСС) являются компьютерные вирусы (КВ). Под КВ понимаются автономно функционирующие программы (программные коды), способные к самовключению в тела других программ и последующему самовоспроизведению и самораспространению в КСС [1 – 3].

Первые КВ появились в конце 80 годов. С этого времени их количество растет по экспоненциальному закону, достигая сегодня нескольких десятков тысяч видов.

Несмотря на достигнутые успехи в новом научном направлении – компьютерной вирусологии, новостийные WEB–сайты пестрят сообщениями о новых "успешных" и отраженных вирусных атаках и угрозах [4]. Несомненное лидерство среди КВ занимают сегодня почтовые сетевые черви, имеющие