УДК: 005

АНАЛІЗ АЛГОРИТМІВ СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ З ТОЧКИ ЗОРУ МОЖЛИВОСТІ ЇХ ПОЛІМОРФНОЇ РЕАЛІЗАЦІЇ

Гринь Я.В.

Національний технічний університет України «Київський політехнічний інститут», Україна, Київ

Проведені дослідження, спрямовані на вивчення можливостей використання поліморфізму для захисту ключових елементів криптографічних алгоритмів симетричного шифрування від несанкціонованої реконструкції за результатами вимірювання та аналізу динаміки споживання потужності в процесі виконання цих алгоритмів на мікроконтролерах і смарт-картах, а також розробки способів реалізації поліморфізму з конкретизацією їх для стандартизованого на Україні ГОСТ 28.147-89 і світового стандарту нового покоління Rijndael. Розглянутий спосіб реалізації поліморфізму на рівні оброблюваних блоків з поліморфізмом програмної реалізації обробки одного блоку.

Ключові слова: алгоритм симетричного шифрування даних, секретний ключ, реконструкція ключових елементів, диференціальний аналіз, поліморфна реалізація, стохачтичність, цикл.

Гринь Я.В. Анализ алгоритмов симметричного шифрования данных с точки зрения возможности их полиморфной реализации / Национальный технический университет Украины «Киевский политехнический институт», Украина, Киев

Проведенные исследования, направленных на изучение возможностей использования программного полиморфизма для

защиты ключевых элементов криптографических алгоритмов симметричного шифрования от несанкционированной реконструкции по результатам измерения и анализа динамики потребления мощности в процессе выполнения этих алгоритмов на микроконтроллерах и смарт-картах, а также разработки способов реализации полиморфизма с конкретизацией их для стандартизированного на Украине ГОСТ 28.147-89 и мирового стандарта нового поколения Rijndael. Рассмотрен способ реализации полиморфизма на уровне обрабатываемых блоков в сочетании с полиморфизмом программной реализации обработки одного блока.

Ключевые слова: алгоритм симметричного шифрования данных, секретный ключ, реконструкция ключевых элементов, дифференциальный анализ, полиморфная реализация, стохастичность, цикл.

Hryn Y. V. The analysis of symmetric cryptographic algorithms of data from the point of view of a possibility of their polymorphic implementation / National technical university of Ukraine "Kiev polytechnic institute", Ukraine, Kiev

The conducted researches, the opportunities of use of program polymorphism for protection of key elements of cryptographic algorithms of the symmetric encoding against unauthorized reconstruction directed to study by results of measurement and the analysis of dynamics of consuming of power in the course of execution of these algorithms on microcontrollers and smart cards, and also development of methods of implementation of polymorphism with their specification for GOST 28.147-89 standardized in Ukraine and the international standard of new generation of Rijndael. The method of implementation of polymorphism at

the level of processed units in combination with polymorphism of program implementation of processing of one unit is considered.

Keywords: symmetric cryptographic algorithm of data, secret key, reconstruction of key elements, differential analysis, polymorphic implementation, stochasticity, cycle.

Вступ. Характерною особливістю обчислювальних процедур алгоритмів симетричного шифрування даних є те, що послідовність проходження операцій не залежить від секретного ключа. Це означає, що найбільшу потенційність з точки зору можливості реконструкції ключових елементів аналізом динаміки споживаної потужності представляють технології диференціального аналізу[1].

Оскільки диференціальний аналіз споживаної потужності заснований на встановленні кореляційних залежностей між потужністю, споживаної в кожен момент часу виконання програми і розрядами ключа, то найбільш дієвий спосіб протидії такого аналізу є зміна порядку проходження команд при кожному виконанні програми, тобто стохастичний поліморфізм.

Мета даної статті: Провести дослідження, яке спрямоване на вивчення можливостей використання поліморфізму для захисту ключових елементів криптографічних алгоритмів симетричного шифрування від несанкціонованої реконструкції за результатами вимірювання та аналізу динаміки споживання потужності в процесі виконання цих алгоритмів на мікроконтролерах і смарт-картах[3].

Розроблено спосіб поліморфної реалізації блокових алгоритмів шифрування, що відрізняється тим, що обробляється відразу кілька блоків даних з випадковим вибором моментів переходів і послідовності проходження блоків, що забезпечує великі значення варіації в часі виконання команд і, тим самим, істотно ускладнює

реконструкцію ключів алгоритмів з використанням диференціального аналізу динаміки потужності.

При поліморфній реалізації алгоритму необхідно забезпечити підвищення складності тимчасової локалізації команд, яка практично виключала можливість їх зіставлення діаграмі споживання потужності при можливо менших витратах обчислювальних ресурсів на здійснення поліморфізму.

Для здійснення поліморфної реалізації алгоритму необхідно:

- виконати аналіз залежності виконуваного потоку команд за даними;

- з урахуванням зазначеної залежності стохастично згенерувати послідовність виконання команд.

Основною характеристикою варіації моменту часу виконання *i*-тої команди ($i \in \{1,..,N\}$, де N -загальна кількість команд) є інтервал v_i часу між пізнім t_{li} і раннім t_{ei} часом її виконання: $v_i = t_{li} - t_{ei}$. Узагальненою характеристикою тимчасових варіацій виконання алгоритму є: середня варіація T_a моменту виконання команд і мінімальний час T_m варіації моменту виконання команд.

$$T_a = \frac{1}{N} \cdot \sum_{i=1}^{N} v_i ;$$

(1)

$$T_m = \min_{i=1,..,N} v_i .$$

Використання блокових алгоритмів передбачає розбиття інформаційного повідомлення на блоки фіксованої довжини, кожен з яких шифрується незалежно. Структура обробки блоків даних симетричними алгоритмами шифрування показана на рис.1.

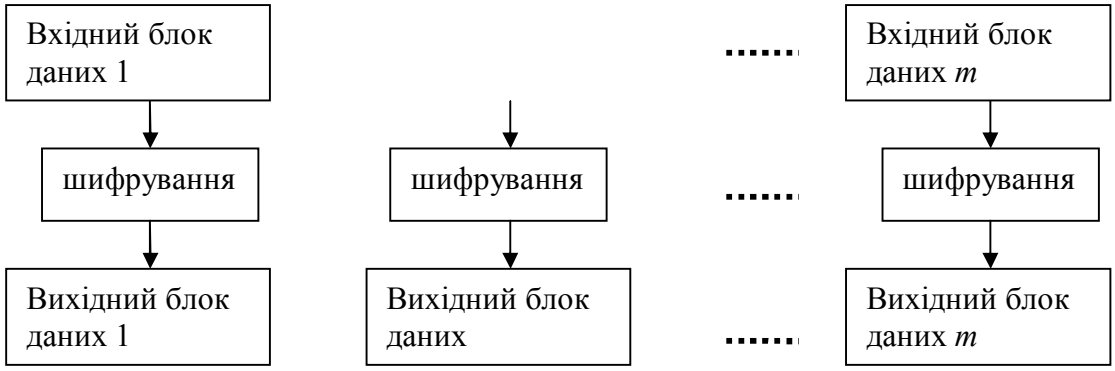

Рис. 1. Структурна організація блоків даних алгоритмами симетричного шифрування

Це дозволяє організувати квазіпараллельну обробку кількох блоків даних, тобто створює потенційні можливості для реалізації поліморфізму на рівні обробки блоків даних.

Таким чином, верхній рівень поліморфної реалізації алгоритмів симетричного шифрування полягає в стохастичному перемиканні з виконання команд одного блоку на інший. Реалізація верхнього рівня поліморфізму пов'язана з витратами ресурсів пам'яті, що вимагається для збереження проміжних даних блоків, обробка яких перервана і з витратами часу на реалізацію збереження і відновлення проміжних даних. Витрати часу істотно залежать від обсягу збережених і відновлюваних даних, а також від частоти перемикань. Поліморфізм реалізації симетричних алгоритмів шифрування особливо ефективний як засіб протидії інтегральним видам диференціального аналізу споживаної потужності.

На рис.2. в якості ілюстрації наведено приклад поліморфної обробки декількох блоків даних.

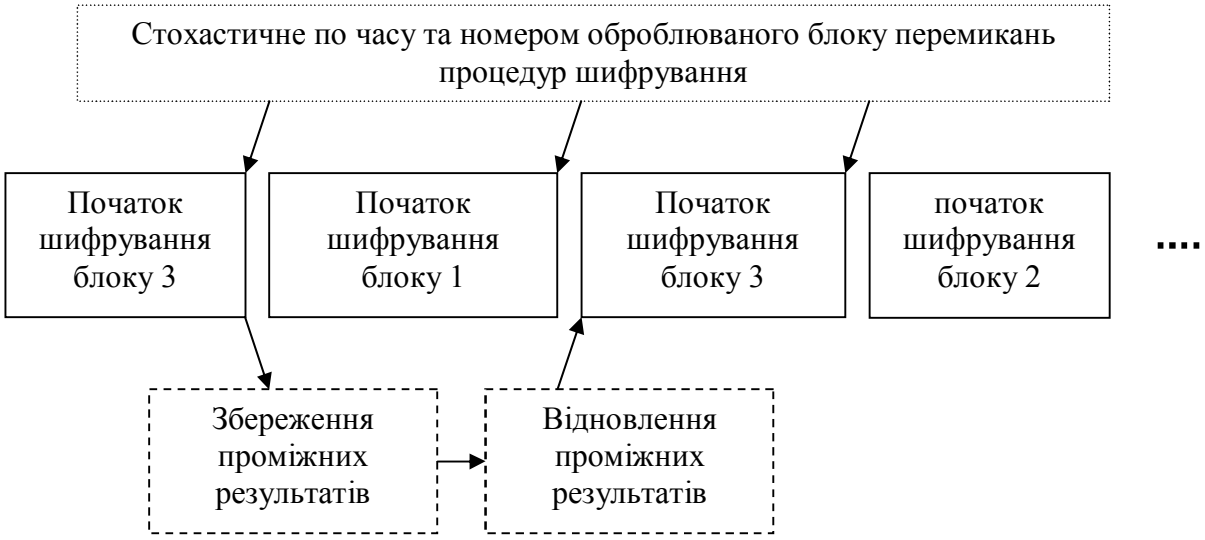

Рис. 2. Приклад поліморфізму шифрування на рівні оброблюваних блоків даних

Нижній рівень поліморфної реалізації алгоритмів полягає в тому, що стохастично змінюється порядок виконання команд обробки одного блоку.

В узагальненому вигляді всі алгоритми симетричного шифрування даних складаються з декількох повторюваних циклів. У деяких алгоритмах число циклів фіксоване, а в деяких може змінюватися. Так, в алгоритмі Rijndael[2] воно може змінюватися, а в ГОСТ 28.147-89 - воно постійне і дорівнює 32. Циклічна організації обчислювальних процедур симетричних алгоритмів шифрування схематично показано на рис.3.

Для кожного з циклів ключі формуються шляхом модифікації спочатку заданого ключа. Всі модифікації ключів зазвичай обчислюються один раз і зберігаються в пам'яті.

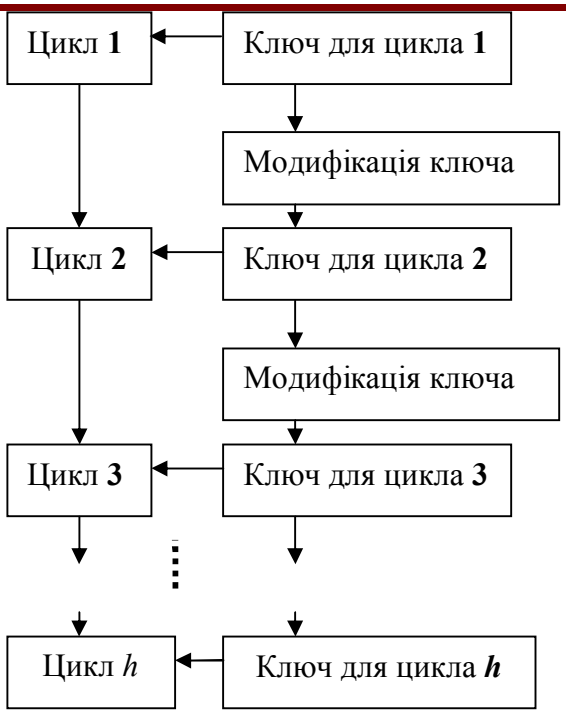

Рис. 3. Циклічна організації обчислювальних процедур симетричних алгоритмів шифрування

Таким чином, оборотність алгоритмів в основі яких лежить принцип К.Шеннона заснована на оборотності операції підсумовування по модулю 2.

Такі алгоритми отримали назву лінійні, оскільки текст вихідного повідомлення входить лінійно в шифротекст. Структурною основою більшості лінійних симетричних алгоритмів є Фейстелова перестановка [6], показана на рис.4.

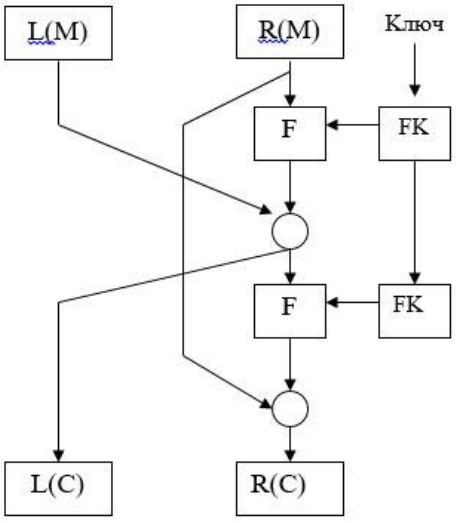

Рис. 4. Фейстелова перестановка

До цього класу належить більшість використовуваних в даний час симетричних криптографічних алгоритмів[4], в тому числі DES, ГОСТ 28147-89, IDEA, SAFER, RC-6. Основними елементами таких алгоритмів є операції формування розширення ключів (FK), нелінійні функціональні перетворення (F) і підсумовування по модулю 2. Узагальнена структура нелінійних алгоритмів показана на рис.5.

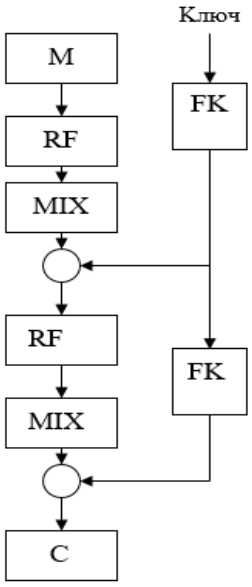

Рис. 5. Узагальнена структура нелінійних алгоритмів

Нелінійні симетричні алгоритми засновані на використанні оборотної функції $\phi(K)$ такий, що $C=\phi(K,M)$ і $M=\phi(K,C)$. В якості таких функцій використовуються оборотні симетричні перетворення на кінцевих полях Галуа $GF(2^n)$. При перетвореннях чергуються цикли оборотних нелінійних перетворень *(RF)* і перемішування блоків даних *(MIX)*. Найбільш характерним симетричним криптографічним алгоритмом розглянутого класу є алгоритм Rijndael, в якому здійснюється для шифрування багаторазове оборотне, залежне від ключа функціональне перетворення на кінцевих полях Галуа для дешифрування з метою відновлення початкового тексту ці ж функціональні перетворення виконуються в зворотному порядку.

Істотним недоліком симетричних алгоритмів цього класу є те, що структура прямого і зворотного перетворень, як і самі базові операції відмінні. Циклічні ключі при зворотному перетворенні в таких алгоритмах повинні використовуватися в інверсному порядку.

Характеристики розрядності блоків даних і ключів, витрат обчислювальних ресурсів, необхідних для розкриття за даними, показники і швидкості програмної реалізації найбільш широко використовуваних на практиці симетричних алгоритмів зведені в табл.1.

В основі практично всіх алгоритмів симетричного шифрування даних лежить аналітично нерозв'язна задача булевих функцій[5]. Це обумовлює те, що рівень захисту визначається специфічними властивостями використовуваних в них нелінійних перетворень. Саме наявність нелінійних перетворень є основною перешкодою використання маскування для захисту від диференціального аналізу.

Таблиця 1.

Характеристики симметричных алгоритмов

Алгоритм	Довж. блоку	Довж. ключа	К-сть Циклів	Число проб для розкриття	Необхідний обсяг пам'ят для розкрит	Продуктивність у Мбайта/с		Рік розробки
						С	Ассемб	
DES	64	56	16	2^{43}	2^{13}	4.0	8.0	1978
3-DES	64	112	48	256	256	1.5	3.0	1985
IDEA	64	128	8	270	249	3.0	4.9	1990
SAFER-64	64	64	8	246	232	4.8	10.1	1994
SAFER-128	64	128	8	264	232	2.9	8.4	1996
Blowfish-16	64	80	16	232	232	8.7	11.9	1994
SHARK	128	128	6	-	-	3.2	4.6	1996
RC5-128	128	128	16	-	-	4.9	10.8	1995
SQUARE	128	128	8	273	232	9.2	13.8	1996
RC6	128	256	20	-	-	5.19	12.6	1999
Rijndael	128	256	14	-	-	2.15	4.1	1998

Висновок

В результаті проведених досліджень, спрямованих на вивчення можливостей використання програмного поліморфізму для захисту ключових елементів криптографічних алгоритмів симетричного шифрування від несанкціонованої реконструкції зроблені наступні висновки:

1. Сучасні алгоритми симетричного шифрування орієнтовані на широке коло обчислювальних платформ, включаючи пристрої з обмеженими ресурсами, такі як мікроконтролери і смарт-карти, для виконання нелінійних булевих функціональних перетворень, в них широко використовуються збережені в пам'яті таблиці. Це обумовлює малу розрядність одночасно оброблюваних даних, що є наслідком схильності таких алгоритмів диференціального аналізу споживаної потужності.
2. Розроблено спосіб поліморфної реалізації блокових алгоритмів шифрування, що відрізняється тим, що обробляється відразу кілька блоків даних з випадковим вибором моментів переходів і послідовності проходження блоків, що забезпечує великі значення варіації в часі виконання команд і, тим самим, істотно ускладнює реконструкцію ключів алгоритмів з використанням диференціального аналізу динаміки потужності, споживаної мікроконтролерами і смарт-картами в процесі шифрування.

Література:

1. *Messerges T.S., Dabblish E.A., Sloan R.H. Examining Smart-Cart Sequruty under the threat of Power-Analysis Attacks // IEEE Transaction on Computers.- Vol. 51.- № 5.- 2002.- pp.541-522.*

2. *Samofalov K.H., Markovskyi A.P., Ziuzia A.A., Lëzyn A.S. Stokhastychesky polymorfnaia realyzatsyia alhorytma Rijndael na mykrokontrollerakh y smart-kartakh // Problemy informatyzatsii ta upravlinnia. Zbirnyk naukovykh prats. K.:NAU.- 2010.- Vyp. 1(29).- s.150-158.Mayer-Sommer R., Smartly analyzing the simplicity and power of simple power analysis on smartcards // Proceeding of 2-th International Workshop "Cryptographic Hardware and Embedded Systems"(CHES-2000), LNCS-1965. Springer-Verlag.- 2000.- P. 78-92.*
3. *Menezer A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC-Press,- 1997.- 780 p.*
4. *Markovskyi A.P., Ziuzia A.A., Sherstiuk V.D. Poluchenye bulevykh pre-obrazovanyi spetsyalnykh klassov dlia postroenyia эffektyvnыkh alhorytmov zashchyty ynformatsyy / A.P. // Visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy "KPI". Informatyka, upravlinnia ta obchysliuvalna tekhnika. K.,"VEK++",- 2008.- № 49.- s.7-13*
5. *Serhei Panasenko. «Sovremennye alhorytmy shyfrovanyia» // Zhurnal «Byte». Vypusk № 8 (60), avhust 2003.*