УДК 004.056.55:004.056.53

# АНАЛІЗ СТІЙКОСТІ AES-256 BOOTLOADER-А ДО АТАК ЧЕРЕЗ ПОБІЧНІ КАНАЛИ НА ОСНОВІ ВИМІРЮВАНЬ ЕНЕРГОСПОЖИВАННЯ

В. О. Шнуренко[1,a], В. М. Степаненко[1]

[1] *Навчально-науковий Фізико-технічний інститут*

## Анотація

У роботі розглянуто стійкість програмної реалізації AES-256-CBC у bootloader-і вбудованої системи до атак побічними каналами на основі вимірювання енергоспоживання. Основну увагу приділено формалізації моделі витоку, аналізу кореляційних залежностей між проміжними станами AES та енергетичними трасами, а також оцінюванню показників Global Success Rate і Partial Guessing Entropy. Показано, що використання криптографічно стійкого алгоритму не гарантує захищеності реалізації, якщо обчислення створюють вимірювані залежності між оброблюваними даними та фізичними характеристиками пристрою. Окремо розглянуто роль синхронізації трас, особливості відновлення раундових ключів AES-256 і складність аналізу вектора ініціалізації в режимі CBC. Результати підкреслюють необхідність урахування побічних каналів під час проектування захищених bootloader-ів для мікроконтролерів.

**Ключові слова**: AES-256, CBC, bootloader, побічний канал, CPA, енергоспоживання.

## Вступ

Захищені bootloader-и широко застосовуються у вбудованих системах для оновлення програмного забезпечення без фізичного доступу до мікроконтролера. Одним із поширених підходів до захисту прошивки є шифрування даних симетричними алгоритмами, зокрема AES із довжиною ключа 256 біт. Однак криптографічна стійкість алгоритму не завжди еквівалентна стійкості його конкретної реалізації. У процесі виконання обчислень цифровий пристрій формує фізичні сигнали, які можуть корелювати з проміжними даними алгоритму. До таких сигналів належать споживаний струм, електромагнітне випромінювання та час виконання окремих операцій [1, 2, 6].

Атаки через побічні канали є особливо актуальними для мікроконтролерів, оскільки вони часто працюють без апаратних криптографічних прискорювачів і без спеціалізованих контрзаходів. У такому випадку навіть реалізація AES-256 може створювати статистично помітні залежності між значеннями внутрішнього стану та енергетичними трасами. Метою роботи є аналіз принципів кореляційного аналізу енергоспоживання для AES-256-CBC bootloader-а, узагальнення математичної моделі атаки та оцінювання інформативності показників GSR і PGE для характеристики стійкості реалізації [9].

[a]viktsnu-ipt27@lll.kpi.ua

## 1. Структура захищеного bootloader-а

Розглянута схема bootloader-а передбачає передавання зашифрованих блоків даних до мікроконтролера. Вхідні дані поділяються на фрагменти, до яких додається фіксована службова послідовність, після чого формується блок довжиною 16 байтів. Далі блок шифрується AES-256 у режимі CBC. Комунікаційна частина додатково містить контрольну суму CRC-16, яка дає змогу виявляти помилки передавання.

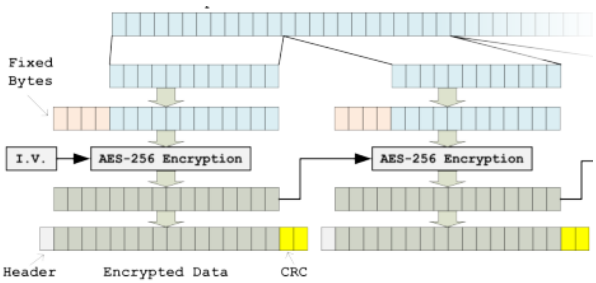


Рис. 1. Формат даних AES-256 bootloader-а та загальна структура протоколу передавання. [9].

На рис. 1 показано, що службові дані, блок шифротексту та поля перевірки цілісності утворюють єдиний формат обміну. Така структура зручна для обмежених за ресурсами пристроїв, однак без додаткових механізмів захисту вона не усуває ризику витоку через фізичні параметри виконання криптографічних операцій.

## 2. Теоретичні основи AES-256-CBC

Вхідний шифротекст одного блоку AES подається як масив із 16 байтів:

$$C = [c_0, c_1, \dots, c_{15}]. \quad (1)$$

Проміжний стан алгоритму після раунду $r$ позначається як

$$X^r = [x_0^r, x_1^r, \dots, x_{15}^r]. \quad (2)$$

У AES-256 ключ має довжину 32 байти та розгортається у набір раундових ключів. Для розшифрування перший оброблюваний раунд відповідає останньому раунду шифрування. Тому проміжний стан першого етапу розшифрування можна записати як

$$X^{14} = Sub^{-1}\left(Shift^{-1}(C \oplus K^{14})\right), \quad (3)$$

де $K^{14}$ - раундовий ключ, $Sub^{-1}$ - обернена підстановка, $Shift^{-1}$ - обернене переставлення рядків, а $\oplus$ позначає операцію XOR.

Для наступного раунду розшифрування враховується також обернене перетворення стовпців:

$$X^{13} = Sub^{-1}\left(Mix^{-1}\left(Shift^{-1}(X^{14} \oplus K^{13})\right)\right). \quad (4)$$

Через лінійність $Mix^{-1}$ вираз можна перетворити так, щоб аналізувати байти ключа незалежно [3, 4]:

$$X^{13} = Sub^{-1}\left(Mix^{-1}(Shift^{-1}(X^{14})) \oplus Y^{13}\right), \quad (5)$$

де

$$Y^{13} = Mix^{-1}(Shift^{-1}(K^{13})). \quad (6)$$

Після визначення $Y^{13}$ відповідний раундовий ключ відновлюється як

$$K^{13} = Mix(Shift(Y^{13})). \quad (7)$$

Режим CBC додає залежність кожного блоку відкритого тексту від попереднього блоку шифротексту або від вектора ініціалізації для першого блоку. Узагальнену схему розшифрування наведено на рис. 2.

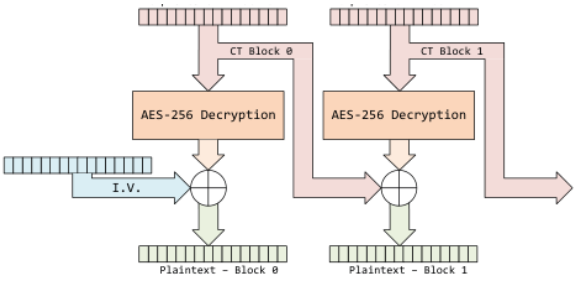


Рис. 2. Розшифрування AES-256 у режимі Cipher Block Chaining. [9].

## 3. Модель витоку та кореляційний аналіз

У моделі витоку за вагою Геммінга припускається, що споживання енергії у певний момент часу статистично пов'язане з кількістю одиничних бітів у проміжному значенні. Для 8-бітного значення $z$ вага Геммінга визначається як кількість бітів, що дорівнюють одиниці. Якщо проміжне значення залежить від байта ключа, то для кожної гіпотези ключа можна обчислити прогнозовану вагу Геммінга та порівняти її з виміряними трасами за допомогою коефіцієнта кореляції Пірсона.

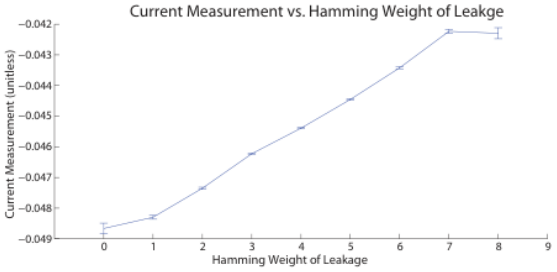


Рис. 3. Залежність середнього вимірювання струму від ваги Геммінга проміжного значення. [9].

На рис. 3 показано приклад лінійної тенденції між вагою Геммінга та споживанням енергії. Така залежність є основою для Correlation Power Analysis (CPA): правильна гіпотеза ключа зазвичай створює вищу кореляцію між прогнозованим витоком і виміряною трасою, ніж хибні гіпотези.

## 4. Синхронізація енергетичних трас

Якість кореляційного аналізу істотно залежить від синхронізації трас; подібні вимірювання зазвичай виконуються на спеціалізованих платформах для аналізу вбудованих систем [5]. Якщо однакові операції AES виконуються у різні моменти часу, кореляційний максимум розмивається, а кількість необхідних трас зростає. Для вирівнювання сигналів може використовуватись критерій суми абсолютних різниць:

$$SAD = \sum_{p=0}^{127} \left|T_p - R_p\right|, \quad (8)$$

де $T_p$ - поточна вибірка сигналу, а $R_p$ - відповідна точка еталонної форми сигналу.

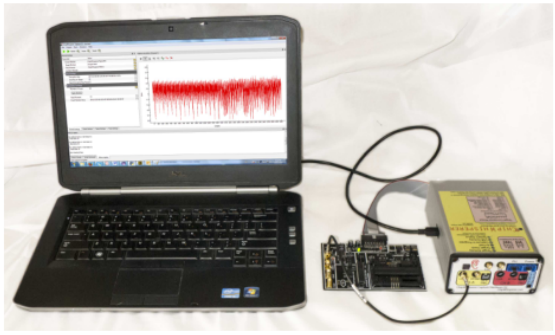

Рис. 4. Приклад лабораторної конфігурації для захоплення енергетичних трас мікроконтролера. [9].

Рис. 4 і рис. 5 ілюструють, що апаратна конфігурація та часовий зсув сигналів безпосередньо впливають на якість подальшого аналізу. Для AES-256 це особливо важливо під час переходу від аналізу 14-го раунду до 13-го, оскільки накопичення часових відхилень може зменшити відтворюваність кореляційних

піків; часові варіації виконання також розглядаються як окремий тип побічного каналу [6, 7].

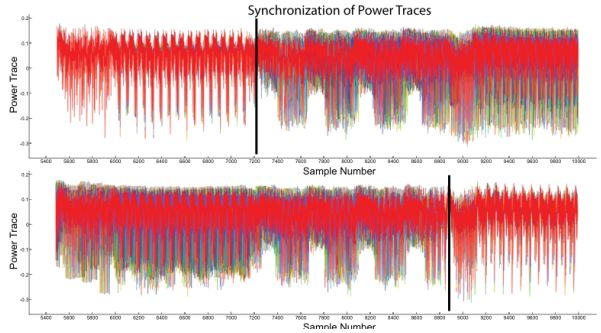


Рис. 5. Порівняння несинхронізованих і повторно синхронізованих енергетичних трас. [9].

## 5. Показники результативності: GSR та PGE

Для кількісної оцінки атаки доцільно використовувати два показники. Global Success Rate (GSR) характеризує частку випадків, у яких повний ключ або потрібна його частина визначається коректно за заданої кількості трас. Partial Guessing Entropy (PGE) показує позицію правильного байта ключа в ранжованому списку гіпотез і пов'язаний із підходом до оцінювання ентропії вгадування [8]. Значення $PGE = 0$ означає, що правильна гіпотеза має найвищий ранг.

На рис. 6 наведено залежність GSR від кількості трас для аналізу ключів 14-го та 13-го раундів AES-256. Крива для 14-го раунду зростає швидше, оскільки відповідний проміжний стан безпосередньо залежить від відомого шифротексту та одного байта ключа. Для 13-го раунду потрібна додаткова трансформація, наведена у формулах (5)-(7).

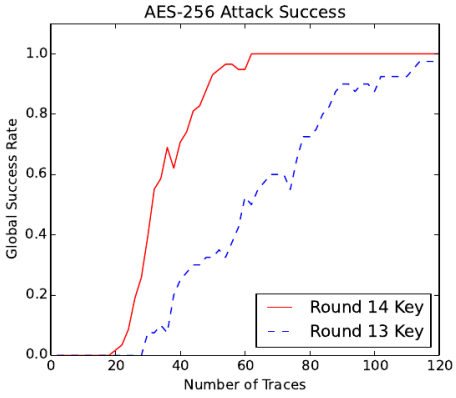


Рис. 6. Global Success Rate для CPA-аналізу раундових ключів AES-256. [9].

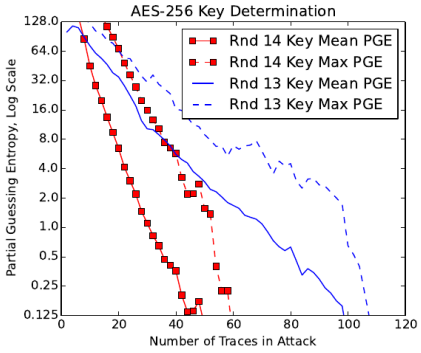


Рис. 7. Partial Guessing Entropy для CPA-аналізу раундових ключів AES-256. [9].

На рис. 7 видно, що збільшення кількості трас поступово зменшує ентропію вгадування. Це означає не лише підвищення ймовірності прямого визначення ключа, але й звуження простору пошуку, у якому правильне значення має високий ранг серед кандидатів.

## 6. Аналіз вектора ініціалізації

У режимі CBC перший блок відкритого тексту залежить від вектора ініціалізації. Узагальнено це можна записати як

$$P = X^0 \oplus IV, \tag{9}$$

де $P$ - відкритий текст першого блоку, $X^0$ - результат блочного розшифрування, а $IV$ - вектор ініціалізації.

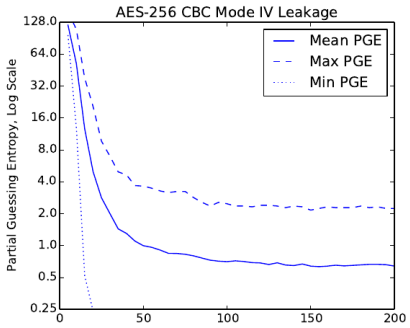


Рис. 8. Partial Guessing Entropy під час аналізу вектора ініціалізації AES-256-CBC. [9].

На рис. 8 наведено поведінку PGE для аналізу $IV$. На відміну від атаки на вихід S-box, операція XOR є лінійною, тому близькі за бітовою структурою гіпотези можуть мати подібні значення кореляції. Це пояснює повільніше зменшення PGE та асимптотичну поведінку кривих у межах кореляційної моделі витоку [2].

Табл. 1 демонструє, що для лінійного поєднання з $IV$ модуль кореляції не завжди є достатнім критерієм вибору правильної гіпотези. Побітова інверсія може давати близьке абсолютне значення кореляції з протилежним знаком, що ускладнює ранжування кандидатів.

Таблиця 1. Приклад ранжування кореляційних гіпотез для одного байта $IV$ за [9].

| Здогадка, Hex | Здогадка, Bin | Кореляція |
|---|---|---|
| 4A | 01001010 | 0.8250 |
| 5A | 01011010 | 0.8150 |
| DA | 11011010 | 0.7912 |
| 25 | 00100101 | -0.7912 |
| A5 | 10100101 | -0.8150 |
| B5 | 10110101 | -0.8250 |

## 7. Обговорення контрзаходів

Аналіз показує, що захист bootloader-а не може обмежуватися лише вибором довгого криптографічного ключа. Оскільки CPA-аналіз спирається на статистичну залежність між проміжними станами AES та енергоспоживанням, основним напрямом захисту є зменшення або порушення цієї залежності. Одним із практичних підходів є маскування проміжних значень: байти стану поєднуються з випадковими масками, тому вага Геммінга окремого проміжного значення вже не відображає безпосередньо байт ключа. Це ускладнює побудову кореляційної моделі витоку, але потребує коректного оновлення масок між операціями SubBytes, ShiftRows і MixColumns.

Другий напрям пов'язаний із часовою невизначеністю виконання. Випадковізація порядку незалежних операцій, додавання змінних затримок або повторне вирівнювання часу виконання зменшують точність синхронізації трас. Для CPA це означає розмиття кореляційного максимуму, збільшення кількості необхідних трас і повільніше зниження PGE. Водночас такі засоби потрібно застосовувати обережно, оскільки самі часові відмінності можуть утворювати окремий побічний канал, якщо вони залежать від секретних даних.

Для мікроконтролерних bootloader-ів також доцільно використовувати реалізації AES з урахуванням стійкості до побічних каналів або апаратні криптографічні модулі, якщо вони доступні на цільовій платформі. Вибір контрзаходів має враховувати обмеження за пам'яттю, швидкодією та розміром коду: маскування збільшує обсяг обчислень, часові контрзаходи можуть уповільнювати оновлення прошивки, а апаратні засоби залежать від можливостей конкретного мікроконтролера. Тому стійкість AES-256-CBC bootloader-а доцільно оцінювати не лише за довжиною ключа, а й за тим, наскільки реалізація зменшує вимірювану залежність між секретними даними та фізичними характеристиками пристрою.

## Висновки

У роботі проаналізовано стійкість AES-256-CBC bootloader-а до кореляційного аналізу енергоспоживання. Наведена модель показує, що проміжні стани AES можуть мати статистичний зв'язок із вимірюваними енергетичними трасами, а це створює ризик відновлення раундових ключів навіть для AES-256. Формули для 14-го та 13-го раундів демонструють, що лінійність окремих перетворень AES дає змогу організувати аналіз другого раундового ключа без повного перебору кількох байтів одночасно.

Показники GSR та PGE є зручними для оцінювання ефективності кореляційного аналізу: перший відображає імовірність повного успіху, а другий характеризує зменшення простору гіпотез. Для вектора ініціалізації режиму CBC аналіз є складнішим через лінійність операції XOR і близькість кореляційних значень для схожих бітових шаблонів. Отже, безпека вбудованого bootloader-а повинна оцінюватися не лише за криптографічною стійкістю AES-256, а й за властивостями його реалізації щодо побічних каналів. Подальший розвиток таких систем доцільно пов'язувати з упровадженням контрзаходів і комплексним оцінюванням їх ефективності.

## Перелік використаних джерел


1. *Kocher P.*, *Jaffe J.*, *Jun B.* Differential Power Analysis // Advances in Cryptology - CRYPTO '99. — Springer-Verlag, 1999. — С. 388—397.
2. *Brier E.*, *Clavier C.*, *Olivier F.* Correlation Power Analysis with a Leakage Model // Cryptographic Hardware and Embedded Systems - CHES 2004. — 2004. — С. 135—152.
3. *Neve M.*, *Tiri K.* On the Complexity of Side-Channel Attacks on AES-256: Methodology and Quantitative Results on Cache Attacks : тех. звіт. / Cryptology ePrint Archive. — 2007. — Report 2007/318.
4. *Moradi A.*, *Kasper M.*, *Paar C.* Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures // Topics in Cryptology - CT-RSA 2012. Т. 7178. — Springer Berlin Heidelberg, 2012. — С. 1—18. — (Lecture Notes in Computer Science).
5. *O'Flynn C.*, *Chen Z. D.* ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research // Constructive Side-Channel Analysis and Secure Design. — Springer International Publishing, 2014. — С. 243—260. — (Lecture Notes in Computer Science).
6. *Kocher P. C.* Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems // Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. — Springer-Verlag, 1996. — С. 104—113.
7. *Koeune F.*, *Quisquater J.-J.* A Timing Attack Against Rijndael : тех. звіт. / Technical report. — 1999.
8. *Massey J. L.* Guessing and Entropy // Proceedings of the 1994 IEEE International Symposium on Information Theory. — 1994. — С. 204.
9. *O'Flynn C.*, *Chen Z. D.* Side Channel Power Analysis of an AES-256 Bootloader // Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). — Halifax, NS, Canada, 2015.