ЕЛЕКТРОНІКА

УДК 621.3.049
DOI https://doi.org/10.32838/2663-5941/2021.6/44

Олішевський Ю.С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Яма О.С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Колесник О.Ю.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Хохлов І.В.
Рочестерський технологічний інститут

Хохлов Ю.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Ямненко Ю.С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Мороз А.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Леон Резник
Рочестерський технологічний інститут

ЗАХИСТ МІКРОКОНТРОЛЕРА ВІД ЗЧИТУВАННЯ

Стаття надає уявлення, що частина апаратного забезпечення, або, точніше, мікросхема, споживає різну кількість енергії залежно від того, які операції виконуються. Також розкриває терміни і поняття, що пов'язані з витоком даних через побічні джерела, пояснює, що таке аналіз потужності. Наведено схеми підключення шунтуючих резисторів, для знімання осцилограм струму споживання мікроконтролера. Побудовано реальний стенд і знято осцилограми струму споживання тестової програми, яку виконує Atmega 328P. В результаті вимірювання справдилися наступні твердження: програма виконується циклічно, тому профіль струму споживання носить циклічний характер. Важливо підкреслити, при виконанні коду, деякі частини коду або змінні виконуються кілька раз за цикл, тому форма споживаного струму також однакова. Сьогодні машинне навчання прогресує від дослідження до основного і є мотиваційним стимулом в епоху інновацій. Сьогодні галузям необхідно подумати про те, як машинне навчання може допомогти їм створити конкурентну перевагу. Мало хто може використовувати дані, щоб визначити тенденції у продуктивності співробітників або їх ринкових продуктах.

Ключові слова: *мікроконтролер, аналіз потужності, атака методом побічних джерел, споживаний струм, машинне навчання.*

Постановка проблеми. Мікроконтролер вразливий навіть коли просто виконує певні операції – додавання або віднімання або виконує криптографічні операції. Вже навіть просто спостерігання за ним може бути дуже інформативним. Наприклад, через зміни миттєвого споживання електроенергії. Зловмисники можуть перехопити дані та розшифрувати їх багатьма методами. Одним із таких є аналіз миттєвої потужності споживання.

Аналіз потужності споживання – це різновид атак на побічні джерела інформації. У цьому випадку побічним джерелом є характер змін миттєвого споживання енергії. В електронних обчислювальних машинах на залежність миттєвої споживаної потужності від часу впливають дані , які обробляє машина , а також від операцій, які виконує вона виконує [2]. Мікроконтролери як різновид ЕОМ також демонструють такий ефект. Аналізуючи характер змін миттєвої потужності споживання під час виконання криптографічних операцій можна навіть визначити криптографічний ключ.

На рис. 1 комп'ютер вводить набір відомих відкритих текстів у криптографічний пристрій, який виконує шифрування. Поки пристрій виконує шифрування, осцилограф вимірює споживану потужність. Для кількох сотень зразків простого тексту отримують так звані відбитки потужності, а потім їх аналізують на комп'ютері за допомогою такого алгоритму, як Простий аналіз потужності (англ.-Simple Power Analysis (SPA)), Диференціальний аналіз потужності (англ.-Differential Power Analysis (DPA)) [3] або Кореляційний аналіз потужності (англ.-Correlation Power Analysis (CPA)) [4] щоб отримати секретний ключ системи. Оскільки звичайний текст у цьому випадку відомий зловмиснику, це відомі атаки із відкритим текстом.

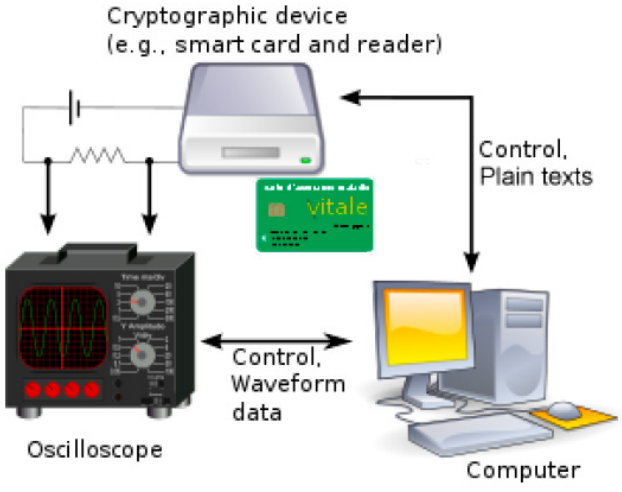

Рис. 1. Атака за допомогою аналізу потужності

Розглянемо рис. 1.1. Звичайний текст подається як вхід до системи, і система запускає шифрування для виведення зашифрованого тексту. Ключ, який використовується в системі, невідомий на зовні, але система ненавмисно розкриває інформацію різними бічними каналами. Ці дані бічного каналу збираються та аналізуються разом із вхідними даними для отримання секретного ключа. Цей же процес можна виконати і в операції дешифрування, де тепер вхідним буде зашифрований текст, а виведенням буде звичайний текст.

Постановка завдання. Мета статті – пояснити, що таке аналіз потужності, а також показати, підготовку плати *Arduino Uno Rev.3* для виконання цього дослідження. Надати іншим дослідниками уявлення, що частина апаратного забезпечення, або, точніше, мікросхема, споживає різну кількість енергії залежно від того, які операції виконуються.

Виклад основного матеріалу дослідження. *1. Схеми вимірювання потужності.* Дослідження вимагає вимірювання потужності, спожитої під час виконання операцій мікроконтролером. На перший погляд здається, простим рішенням було б розрізати USB-кабель і вставити резистор в лінію живлення, але це не спрацює. Перш за все, так буде виміряна вся потужність , що споживається , включаючи таку, що споживають світлодіоди та інший мікросхеми, наприклад, USB-UART. Буде отримано занадто багато шуму. Необхідно вимірювати якомога ближче до мікроконтролера. Резистор необхідно розташувати безпосередньо в лінії живлення мікросхеми. Оскільки можливості для безпосереднього вимірювання енергоспоживання пристрою недоступні, виникає необхідність непрямого методу. Отже, фактично, штифт мікросхеми буде піднято вгору, щоб було змога розташувати резистор між мікроконтролером і друкованою платою.

На рис. 2 показано просте налаштування мікроконтролера, підключеного до джерела живлення.

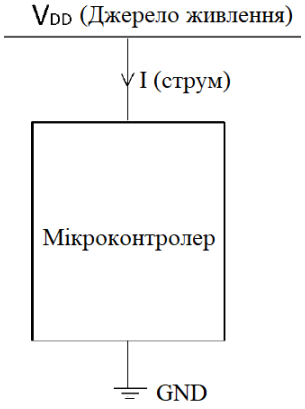

Рис. 2. Струм, що споживається мікроконтролером

Споживання потужності мікроконтролера у цьому випадку визначається рівнянням:

$$P = V_{DD}I,$$

де I – миттєвий струм, V_{DD} – напруга живлення. Оскільки V_{DD} постійна, струм I прямо пропорційний потужності P. Тому потужність можна визначити, вимірявши силу струму, але для вимірювання струму потрібен пристрій, який називається струмовим зондом, який є дорогим. Тому метод, за допомогою якого можна використовувати осцилограф, є кращим, але осцилографи вимірюють напругу, а не струм. Пропонується дві методики, які дозволяють використовувати осцилограф для вимірювання потужності.

1.1. Метод заземлюючого резистора для вимірювання потужності. Перший метод полягає в тому, щоб підключити резистор в ланці, в якій мікроконтролер заземлений, як показано на рис. 3. Тепер падіння напруги на резисторі визначається як $V = IR$, де R - опір. Оскільки опір можна вважати константою, вимірюючи напругу, ми можемо вивести струм, який, у свою чергу, можна використовувати для виведення потужності. Тому, підключивши осцилограф через резистор, потужність можна виміряти, як на рис. 3.

За допомогою цього методу можна отримано шукану потужність, однак за цим методом не всі експерименти успішні. Авторами з'ясувалося[1], що на неправильні результати вплинули два фактори.

1. Занадто малий опір резистора.
2. Неправильне заземлення.

У прикладі [2, с. 49–51] для своєї установки вимірювання потужності використано резистор 1 Ом. Запущений алгоритм CPA на вимірах, зібраних за допомогою резистора 1 Ом, автори не змогли отримати ключ. Але пізніше з'ясувалося, що коли використовується резистор 10 Ом або вище, можна успішно отримати ключ.

Рис. 3. Вимірювання потужності за допомогою методу заземлення

Показник потужності майже дорівнював 0, що означало, неправильні вимірювання. Після дослідження виявилося, що проблема була в неправильному розміщенні проводу заземлення осцилографа. На рис.4 а) заземлення USB підключено до верхньої частини резистора, а заземлення осцилографа – до нижньої частини резистора. Оскільки обидва значення заземлення однакові, це ставить напругу на резисторі до 0. Як рішення, підключили щуп осцилографа під'єднано, як показано на рис.4 б). Тепер обидві заземлення підключені до одного місця, але траса живлення буде інвертованою, оскільки вимірюється негативна напругу по відношенню до землі осцилографа. Але в осцилографах є функції для легкого інвертування хвилі.

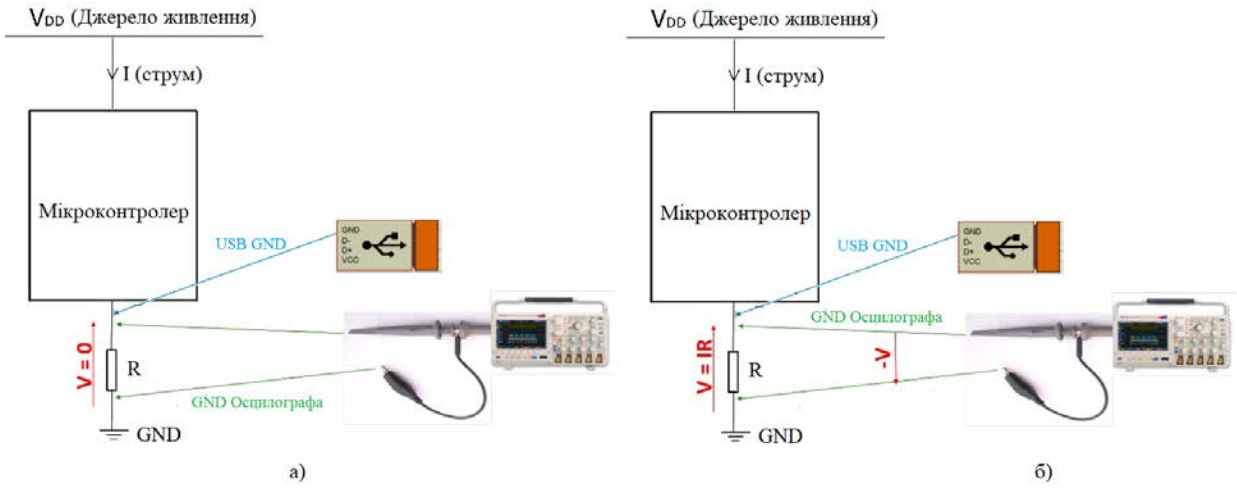

Рис. 4. а) Неправильний спосіб заземлення пробника осцилографа, б) Правильний спосіб заземлення пробника осцилографа

Після правильного підключення автори отримали правильні значення.

1.2 Метод резистора джерела живлення для вимірювання потужності. Іншим методом є розміщення резистора на ланці від джерела живлення, як показано на рис.5. Концепція подібна до попереднього методу, але тепер, якщо підключити звичайний щуп осцилографа для вимірювання напруги на точки A і B як на рис.5, резистор виходить із ладу. Причина у тому, що при підключенні заземлювального проводу щупа осцилографа до точки B ця точка заземлюється, і якщо значення резистора невелике, через неї буде протікати великий струм. Тому для вимірювання потужності на точках A та B необхідно використовувати спеціальний щуп, який називається диференціальним пробником, який є дорогим.

Як альтернатива можна використовувати два пробники осцилографа. Один щуп осцилографа можна під'єднати для вимірювання напруги між точками A та C, тоді як інший щуп можна під'єднати до точок B і C, переконавшись, що дроти заземлення обох зондів під'єднані до точки C. Тоді, віднімаючи напругу на першому щупі від напруги на другому щупі, можна отримати напругу між A і B. Однією з проблем із цим методом є непотрібні витрати на віднімання хвиль. Інша проблема полягає в тому, що більшість осцилографів зазвичай поставляються з двома щупами, і коли обидва щупи використовуються таким чином, не буде іншого щупа для використання в якості тригера.

Незважаючи на труднощі, метод V_{DD} резистора все ще є вигідним, оскільки для аналізу потрібна менша кількість вимірів потужності, що, у свою чергу, зменшить час.

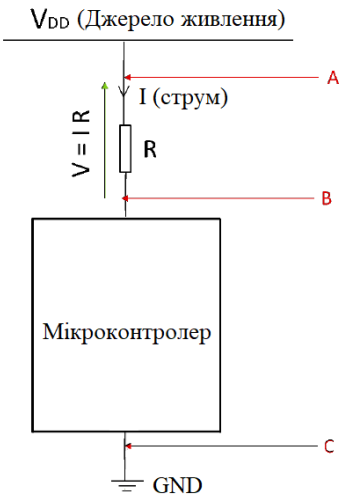

Рис. 5. Вимірювання потужності за допомогою методу резистора джерела живлення

Дещо змінивши попередній спосіб, можна використовувати лише один щуп для вимірювання потужності за допомогою методу V_{DD} резистора. Шляхом підключення щупа осцилографа між точками B і C. Тому тут вимірюється напругу на мікроконтролері, а не на резисторі. Вимірювання за допомогою цього методу дозволяє виконувати дослідження, використовуючи меншу кількість вимірів, ніж тих, що потрібні при використанні методу заземлення. Порівняння необхідної кількості проводиться в [1].

2. Практичне дослідження аналізу потужності. Як досліджуваний зразок обрано плату для розробки *Arduino Uno Rev.3* з мікроконтролером *Atmel Atmega328P*. Робоча частота контролера складає 16 МГц [5], тому потрібен цифровий осцилограф, яких дуже швидко зможе вимірювати невеликі відхилення. Обрано цифровий осцилограф Siglent SDS1052DL+, який може вимірювати дані з частотою до 70 МГц [6]. Зібраний за рис. 5 досліджуваний стенд зображено на рисунку нижче.

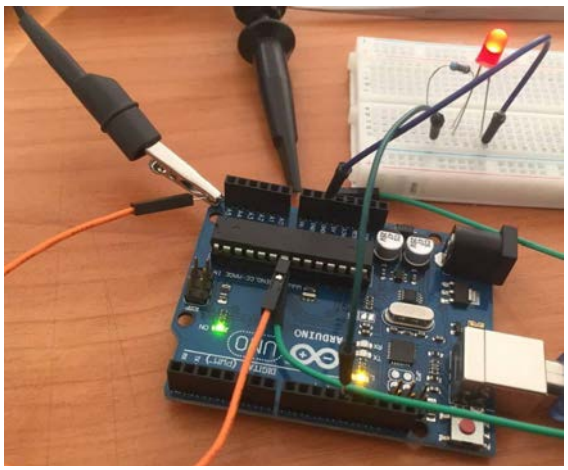

Рис. 6. Досліджувана установка

На рис. 7 зображено чотири виміри струмів під час прошивки тестової програми.

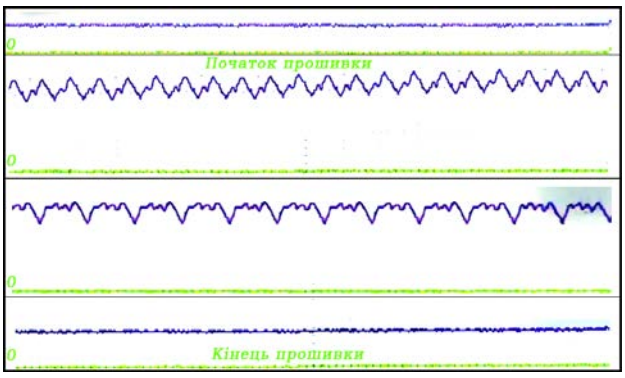

Рис. 7. Осцилограми струму при прошивці мікроконтролера

Далі була написана тестова програма мовами С++ та С++ зі вставками на Асемблері . Лістинг наведено нижче.

```
void setup() {
 DDRB = 0b00100000;
}
void loop() {
 PORTB = 0b00000000;
 delay(450);
 PORTB = 0b00100000;
 delay(50);
}
```

```
void setup() {
 asm volatile
 (
 "ldi R16, 0b00100000 \n"
 "out 0x04, R16 \n"
 );
}
void loop() {
 asm volatile
 (
 "ldi R16, 0b00000000 \n"
 "out 0x05, R16 \n"
 );
 delay(450);
 asm volatile
 (
 "ldi R16, 0b00100000 \n"
 "out 0x05, R16 \n"
 );
 delay(50);
}
```

Обидві програми виконують одну і ту саму функцію: вмикають та вимикають світлодіод. Але через особливості написання коду займають різну кількість пам'яті. Осцилограми споживання струму наведено нижче (рис.8). Синя –мова С++, червона – С++ зі вставками на Асемблері .

Оскільки програма виконується циклічно, профіль струму споживання носить також циклічний характер. На рис. 8 добре видно один період. Важливо підкреслити, при виконанні коду, деякі частини коду або змінні виконуються кілька раз за цикл, тому форма споживаного струму також однакова. Схожі елементи виділено на рис.8.

Подальша робота полягає в повному аналізі подібних профілей струму за допомогою методів машинного навчання (multilayer perceptron (NN), Random Forest (decision tree), J48 (decision tree)).

Публікація ґрунтується на роботі, що фінансувалась коштом гранту G-202105-67 «Security evaluation and improvement of the personal cyberinfrastructure with new tools and education development», одержаного від Фонду цивільних досліджень та розвитку США (CRDF Global). Будь-які думки, спостереження, висновки або рекомендації, викладені у цьому матеріалі, належать авторові (авторам) і можуть не віддзеркалювати поглядів CRDF Global.

Висновки. Стаття розкриває терміни і поняття, що пов'язані з витоком даних через побічні джерела, пояснює, що таке аналіз потужності. Наведено схеми підключення шунтуючих резисторів, для знімання осцилограм струму споживання мікроконтролера. Побудовано реальний стенд і знято осцилограми струму споживання тестової програми, яку виконує *Atmega 328P*.

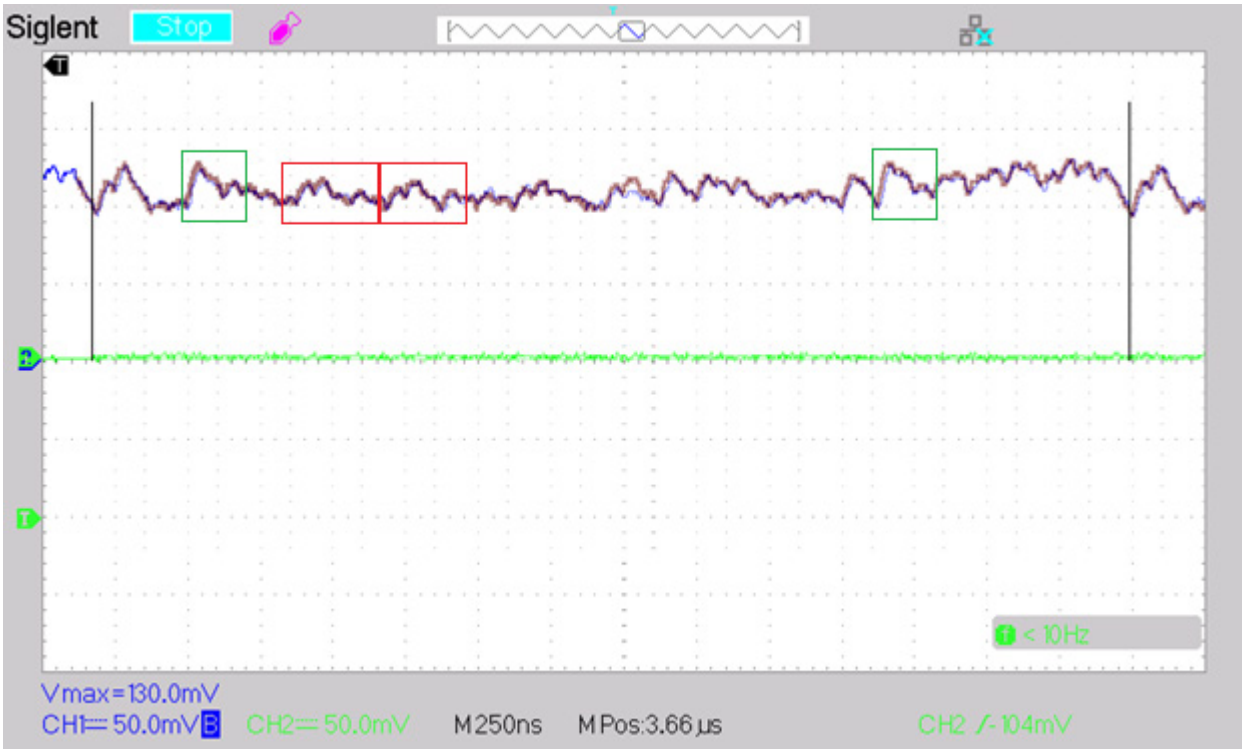

Рис. 8. Струм споживання мікроконтролера при виконанні тестової програми

Список літератури:

1. Gamaarachchi H., Ganegoda H. Power analysis based side channel attack. arXiv preprint arXiv:1801.00932. 2018. URL: https://arxiv.org/abs/1801.00932
2. Mangard S. et al., Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Secaucus, NJ, USA : Springer-Verlag New York, Inc., 2007. URL: https://www.iacr.org/books/2010_sp_MangardOswaldPopp_DPA.pdf/
3. Kocher P., Jaffe J., Jun B. (1999) Differential Power Analysis. In: Wiener M. (eds) Advances in Cryptology – CRYPTO' 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/3-540-48405-1_25
4. E. Brier et al. Correlation power analysis with a leakage model. *Cryptographic Hardware and Embedded Systems-CHES 2004. Springer*, 2004, pp. 16–29. DOI:10.1007/978-3-540-28632-5_2
5. Arduino Uno Rev.3 development board. URL: https://store.arduino.cc/products/arduino-uno-rev3.
6. Digital oscilloscope Siglent SDS1052DL +. URL: https://www.siglent.eu/product/1139150/siglent-sds1052dl-50mhz-dual-channel-oscilloscope.

Olishevsky Y.S., Yama O.S., Kolesnik O.Y., Khokhlov I.V., Khokhlov Y.V., Yamnenko Y.S., Moroz A.V., Leon Reznik. PROTECTION OF THE MICROCONTROLLER FROM READING

The microcontroller is vulnerable even when it simply performs certain operations – addition or subtraction, or performs cryptographic operations. Even just watching him can be very informative. For example, due to changes in instantaneous electricity consumption. Attackers can intercept data and decrypt it in many ways. One of these is the analysis of instantaneous power consumption. This article provides an idea that part of the hardware, or, more precisely, the chip, consumes different amounts of energy depending on what operations are performed. Power consumption analysis is a type of attack on side sources of information. In this case, a side source is the nature of changes in instantaneous energy consumption. In electronic computers, the dependence of instantaneous power consumption on time is influenced by the data processed by the machine, as well as on the operations it performs. Microcontrollers, as a type of computer, also demonstrate this effect. By analyzing the nature of changes in instantaneous power consumption during cryptographic operations, you can even determine the cryptographic key. It also reveals the terms and concepts associated with data leakage through incidental sources, explains what power analysis is. The connection diagrams of shunt resistors for oscillogram of current consumption of microcontroller are given. A real stand was built and current consumption oscillograms of the test program performed by Atmega 328P were taken. The Arduino Uno Rev.3 development board with Atmel Atmega328P microcontroller was selected as the test sample. The operating frequency of the controller is 16 MHz, so you need a digital oscilloscope, which can very quickly measure small deviations. The Siglent SDS1052DL + digital oscilloscope, which can measure data up to 70 MHz, has been selected. Because the program is run cyclically, the current consumption profile is also cyclical. It is important to emphasize, when executing the code, some parts of the code or variables are executed several times per cycle, so the form of current consumption is also the same. Today, machine learning is progressing from research to basic and is a motivational stimulus in the age of innovation. Today, industries need to think about how machine learning can help them create a competitive advantage. Few can use the data to identify trends in employee productivity or their market products.

Key words: *microcontroller, power analysis, attack by side sources, current consumption, machine learning.*