Силовая электроника

УДК 621. 3. 011: 621. 314

А.В. Мороз, **Т.О. Терещенко**, д.-р., техн. наук
Національний технічний університет України «Київський політехнічний інститут»,
пр. Перемоги, 37, м. Київ, 03056, Україна.

Регульовані фільтри живлення мікроконтролерів з маскуванням струму споживання

В статті проведене моделювання генераторів шуму для використання в регульованих фільтрах з маскуванням струму споживання для живлення мікроконтролерів, запропоновані нові схеми регульованих фільтрів, показана їх ефективність. Бібл. 4, рис. 7, табл. 1.

Ключові слова: *регульований фільтр; маскування струму споживання; системи захисту; моделювання; мікроконтролер*.

Вступ

При розробці систем керування пристроями на мікроконтролерах, основна доля трудомісткості в більшості випадків припадає на програмне забезпечення. Для захисту авторських прав розробники використовують мікроконтролери із захистом інформації, наприклад з бітами захисту, що затрудняють зчитування програмного коду. В даному випадку розробнику системи важливо знати реальну інформацію про ступінь захищеності від несанкціонованого зчитування використовуваних компонентів та знати методи їх перевірки на надійність.

Існуючі методи несанкціонованого зчитування інформації з мікроконтролерів

Відомими методами несанкціонованого доступу до інформації в мікроконтролері є деструктивні та недеструктивні. Деструктивні методи передбачають відкриття корпуса мікросхеми та модифікацію внутрішніх електричних з'єднань, потребують дорогого обладнання, як-то електронних мікроскопів, лазерів, мікрощупів, тому їх рідко використовують для зчитування програмного забезпечення мікроконтролерів. Недеструктивні методи дозволяють отримати інформацію про внутрішній стан мікроконтролера без зняття упаковки мікросхеми, та не потребують дорогого обладнання зчитування інформації і може бути виконано тільки за допомогою цифрового осцилографа та комп'ютера. Недеструктивні методи атак включають у себе: дослідження часу виконання програми; атаки з повним перебором ключів доступу; генерування електричних завад з метою виклику збоїв; аналіз побічних каналів витоку інформації; простий та диференційний аналіз струму живлення. Відомі методи атаки за струмом споживання [1], такі як простий аналіз струму споживання (Simple Power Analysis, SPA) та диференційний аналіз струму споживання (Differential Power Analysis, DPA) легкі для виконання, мають низьку вартість, і проводяться без руйнування мікросхем, а отже представляють інтерес при несанкціонованому доступі зловмисників до інформації.

Маскування струму споживання для захисту інформації

Перспективним способом захисту інформації від зчитування за струмом живлення є маскування струму споживання. Даний спосіб тільки починає сьогодні застосовуватися. Авторами запропоновано створити такий фільтр живлення, який би вносив завади до струму споживання мікроконтролера, що в майбутньому не дало б зловмисникам зчитувати реальний струм споживання мікроконтролера [2].

Таким чином, задача розробки фільтрів живлення для захисту мікропроцесорних систем від несанкціонованого зчитування інформації за струмом споживання, є актуальною. Для вирішення даної задачі пропонується створити схеми та алгоритми регульованих фільтрів живлення із маскуванням інформаційних сигналів у струмі споживання, та дослідити ефективність запропонованих регульованих фільтрів джерел живлення мікроконтролерів, розроблених алгоритмів та пристроїв.

Визначення ефективності генераторів шуму для випадкової зміни параметрів фільтрів

Пропонується побудувати нові фільтри живлення із змінними параметрами, які характеризуються підвищенням рівня захищеності та відносно простою реалізацією.

Еквівалентна схема регульованого фільтру із змінними параметрами, представлена на

рис.1. Для RC-фільтру, опір R або ємність C змінюються за законом випадкових чисел.

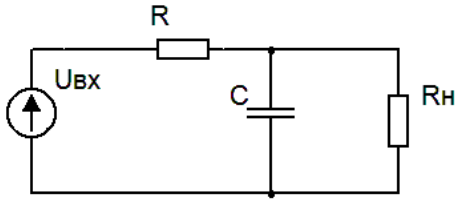

Рис. 1. Електрична схема регульованого фільтру із змінними параметрами

Важливо визначити, який тип розподілення генератора випадкових чисел слід вибрати для забезпечення високого рівня захисту від зчитування інформації за струмом споживання.

Для того, щоб дослідити вплив типу генератора шуму, а також частоти шуму, визначено коефіцієнти взаємної кореляції між струмом споживання без маскування та з маскуванням за допомогою регульованого фільтру в залежності від типу генератора шуму та від його частоти. В якості порівнюваних типів генераторів шуму використовувалися генератори, які дають гаусівський, рівномірний, раусівський, релеївський, білий шум відповідно. Співвідношення між періодом тактування мікроконтролера (Тт) та періодом відповідного генератора (Тг) змінювалася від 1 до 0,1.

Таблиця 1.

Тт/Тг	Гаусівский	Рівномірний	Райсівський	Релеївський	Білий
1	0,6001	0,598	0,5923	0,4937	0,659
0,5	0,5974	0,4854	0,5039	0,5448	0,6295
0,2	0,5076	0,4805	0,4658	0,4912	0,4761
0,1	0,4495	0,4034	0,4147	0,4266	0,2429

Чим менший коефіцієнт кореляції, тим менш схожі між собою дані струми споживання, і тим краще регульований фільтр. Відповідно, дані залежності відображаються у вигляді сімейства кривих (рис. 2):

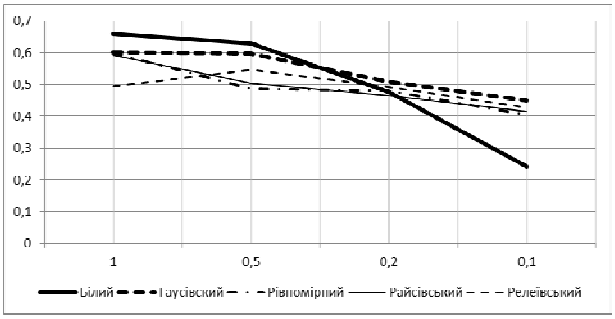

Рис. 2. Графічне зображення залежностей коєфіціентів кореляції від частоти генератора для різних типів шуму

Із наведених вимірювань видно, що зі збільшенням частоти генератора, коефіцієнт взаємної кореляції зменшується для всіх типів шуму. Зменшення коефіцієнта взаємної кореляції означає краще маскування струму мікроконтролера. Для отримання прийнятного коефіцієнта взаємної кореляції менше 0,5 частота генератора шуму повинна бути щонайменше у 10 разів вищою, за частоту тактування мікроконтролера.

Запропоновані схеми регульованих фільтрів живлення із маскуванням струму споживання

На базі генератора шуму розроблено чотири пристрої фільтрів живлення мікропроцесорної системи із захистом за струмом споживання. При розробці поставлено задачу: з однієї сторони – забезпечення якомога більшого значення рівня захисту, а з іншої – можливість реалізації такої системи захисту на сучасній елементній базі та економічна доцільність. Регульований фільтр з маскуванням інформаційних сигналів на основі змінного конденсатора (рис. 3), містить змінний конденсатор з електронним керуванням, підключений паралельно до виводів живлення [3]. Ємність конденсатора змінюється випадковим чином завдяки генератору шуму.

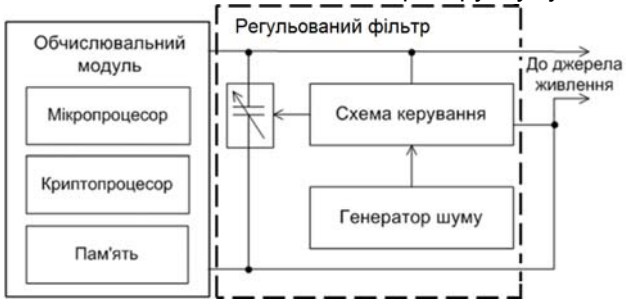

Рис. 2. Схема регульованого фільтра з маскуванням інформаційних сигналів на основі змінного конденсатора

Перевагою запропонованого регульованого фільтру є те, що відбувається підвищення шуму в споживаному струмі та забезпечення кращої захищеності секретної інформації без обмеження основного струму споживання. Деяким недоліком системи є те, що на кристалі необхідно реалізовувати змінний конденсатор, що складно.

Запропонований регульований фільтр живлення мікроконтролера[4] на основі блоку ключів (рис.4), в якому через інтерфейс зв'язку центральний процесор отримує інструкції для виконання дій з даними пам'яті, а результат виконання даних центральним процесором кодується, та передається через інтерфейс зв'язку до зовнішніх пристроїв. Живлення процесора здійснюється через блок ключів, ввімкнення різної кількості яких спотворює струм споживання пристрою в цілому. Керування блоком ключів здійснюється від генератора випадкових станів, з'єднаного через з пам'яттю мікроконтролера.

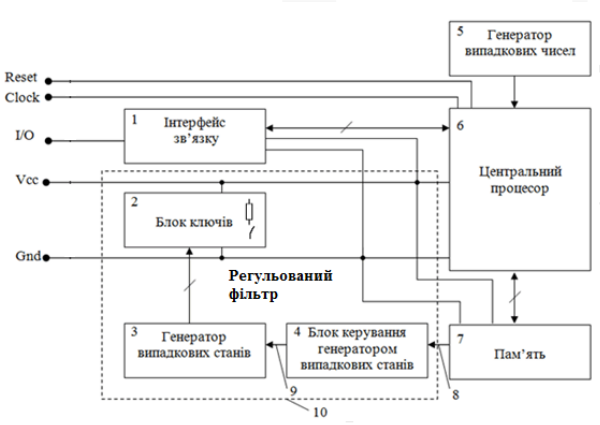

Рис. 4. Схема регульованого фільтра живлення мікроконтролера на основі блоку ключів

Перевагою такого регульованого фільтру живлення є те, що він не містить конденсаторів великої ємності, а отже займає меншу площу кристалу. Дану систему можна включати тільки по команді, що спричиняє економне енергоспоживання при незмінній захищеності. Крім того, є можливість програмно змінювати алгоритм генерації випадкових станів, а це дає покращення захисту в наступних версіях системи.

Регульований фільтр живлення виконаний на основі допоміжного процесорного ядра зображено на рис.5.

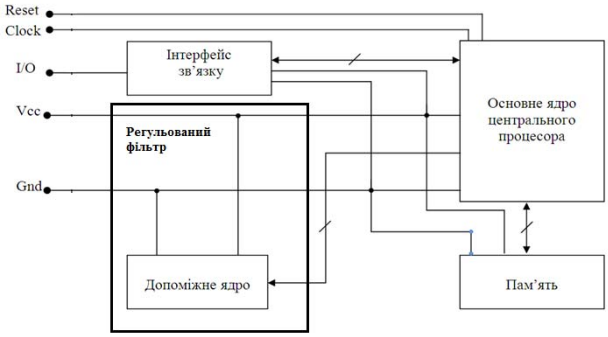

Рис. 5. Схема регульованого фільтра живлення виконаного на основі допоміжного процесорного ядра

Використання додаткового ядра дозволяє замінити два блоки: генератор випадкових чисел та цифровий блок ключів одним цифровим пристроєм. Додаткове ядро є програмованим пристроєм, і тому дозволяє використовувати алгоритми генерації випадкових чисел різної складності в залежності від потрібного ступеня захищеності, що дає можливість оптимізувати швидкодію мікроконтролера.

Зв'язок основного ядра з допоміжним дозволяє використовувати динамічні дані, якими оперує мікроконтролер та використовувати їх в алгоритмі генерації випадкових чисел, що значно поліпшує характеристики алгоритму.

Регульований фільтр живлення мікроконтролера з вимірюванням струму у реальному масштабі часу (рис.6) містить цифровий сигнальний процесор, який використовується для вимірювання струму споживання захищуваного мікроконтролера та генерації відповідних «хибних» команд у реальному часі.

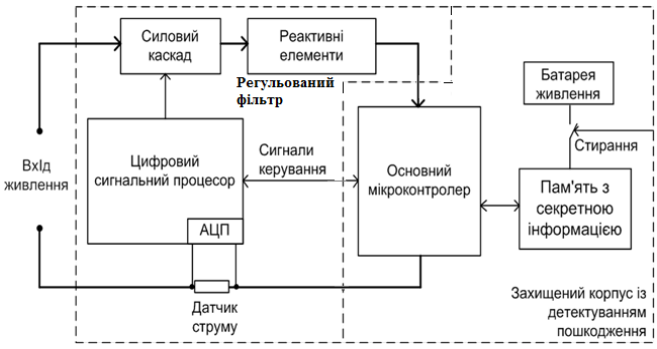

Рис. 6. Схема регульованого фільтра живлення мікроконтролера з вимірюванням струму у реальному масштабі часу

Регульований фільтр живлення містить силовий каскад, реактивні елементи, що разом спричиняють спотворення струму споживання заданої форми та систему керування на базі цифрового сигнального процесора. До процесора підключено сигнал зворотного зв'яжу по струму основного мікроконтролера, що перетворюється у двійковий код за допомогою АЦП, та оброблюються програмним забезпеченням. Джерело живлення та основний мікроконтролер знаходяться усередині корпуса, що відслідковує несанкціоноване відкриття, та стирає всю конфіденційну інформацію у енергозалежної пам'яті, тим самим зловмисник втрачає доступ до конфіденційної інформації. Наведений фільтр живлення є найбільш прогресивним на сьогодні серед аналогічних систем, має покращення захисту від зчитування за струмом споживання, та додатковий захист від генерації збоїв (глітч-атаки), крім того, система має можливість адаптивного генерування шумів, наприклад покращення алгоритму розробником у наступних версіях системи.

Експериментальне дослідження запропонованих регульованих фільтрів

В експериментальній частині дослідження визначено відхилення коефіцієнтів взаємної кореляції струмів деяких команд без використання системи захисту та з використанням запропонованих схем регульованих фільтрів.

Для дослідження ефективності застосовано критерій максимального відхилення коефіцієнтів кореляції 1,16, що свідчить про неможливість визначення не тільки правильної мікрокоманди чи підпрограми, а й про низьку ймовірність детектування в струмі споживання захищеного такою системою мікроконтролера раніше виміряної ділянки динамічного струму споживання.

Приймемо за одиницю ефективність найменш ефективної системи захисту (відома система на основі одного фільтруючого конденсатора), та побудуємо порівняльну діаграму у відносних одиницях (рис.7).

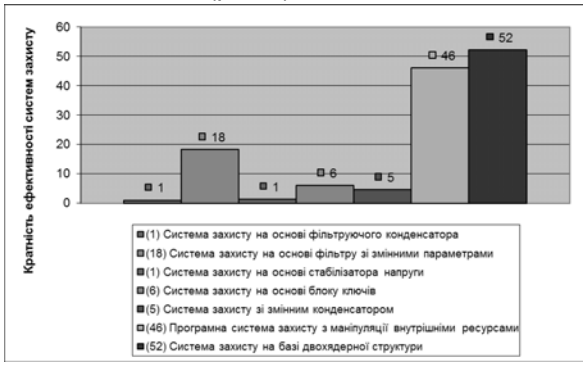

Рис. 7. Порівняльна діаграма ефективності системи захисту

Найбільшу ефективність мають запропоновані системи регульованих фільтрів для мікроконтролерів. Зокрема, фільтр живлення зі змінними параметрами в 18 разів ефективніший, фільтр на основі блоку ключів у 6 разів фільтр на основі двох ядерної структури ефективніший в 52 рази у порівнянні з простим фільтром живлення. У порівнянні зі схемою маніпуляції внутрішніми ресурсами захисту, фільтр на основі двох ядерної структури ефективніший в 1,13 рази.

Висновки

Застосування генератора шуму при реалізації системи керування регульованим фільтром живлення дозволяє в цілому збільшити ефективність захисту за струмом споживання. Для досягнення прийнятного рівня маскування струму споживання, частота генератора шуму повинна бути щонайменше у 10 разів вищою, за частоту тактування мікроконтролера.

Запропоновано чотири схеми та алгоритми роботи регульованих фільтрів із маскуванням струму споживання: на основі змінного конденсатора, на основі блоку ключів, на основі допоміжного процесорного ядра, та регульований фільтр з вимірюванням струму споживання у реальному масштабі часу.

Запропонована схема керування регульованим фільтром живлення на основі допоміжного ядра мікропроцесора може бути реалізована на сучасних двохядерних процесорах.

Для запропонованого фільтру живлення з вимірюванням у реальному масштабі часу, максимальне відхилення коефіцієнту кореляції становить 1,16, що свідчить про практичну неможливість виділення команди.

Порівняльний аналіз ефективності існуючих систем зі створеними фільтрами живлення, доводить перевагу останніх за ефективністю захисту. Зокрема, запропонований фільтр живлення з вимірюванням у реальному масштабі часу, має ефективність вище в 52 рази у порівнянні з простим фільтром живлення. У порівнянні зі схемою маніпуляції внутрішніми ресурсами захисту, фільтр на основі двоядерної структури ефективніший в 1,13 рази.

Список використаних джерел

1. *Kocher P.*, Differential Power Analysis / P. Kocher, J. Jaffe, B. Jun // Crypto 99 Proceedings, Lecture Notes in Computer Science. – M. Wiener, ed., Springer-Verlag, 1999. — Vol.1666.

2. *Беженар В.О.,* Цифрова система захисту від атак за струмом споживання, / В.О. Беженар, А.В. Мороз, Т.О. Терещенко // Электроника и связь. – 2010. – №2. – С.108-114.
3. Пат. UA 43634 Україна, МПК G06F 1/00 (2006.01). Мікропроцесорна система з захистом від зчитування за струмом споживання / В.О. Беженар, А.В. Мороз, Т.О. Терещенко; заявл. 25.03.2009 №u200902780, опубл. 25.08.2009.
4. Пат. UA 43673 Україна, МПК G06K 19/06 (2006.01). Мікроконтролер з системою захисту від атак за струмом споживання. / В.О. Беженар, А.В. Мороз, Т.О. Терещенко; заявл. 03.04.2009 № u200903207, опубл. 25.08.2009.

Поступила в редакцию 26 марта 2015 г.

УДК 621. 3. 011: 621. 314

А.В. Мороз, **Т.А. Терещенко**, д.-р. техн. наук
Национальный технический университет Украины «Киевский политехнический институт»
пр. Победы, 37, г. Киев, 03056, Украина.

Регулируемые фильтры питания микроконтроллеров с маскированием тока потребления

Для защиты авторских прав разработчику систем на микроконтроллерах важно знать реальную информацию о степени их защищенности от несанкционированного считывания. Известны методы несанкционированного считывания информации по току потребления, такие как простой анализ тока потребления и дифференциальный анализ тока потребления, просты для выполнения, имеют низкую стоимость, и проводятся без разрушения микросхем. Перспективным способом защиты от считывания является маскирование тока потребления. Авторами предложено создать такой регулируемый фильтр тока потребления, который бы вносил помехи в ток потребления микроконтроллера. Для того, чтобы определить тип генератора шума, необходимый для управления регулируемым фильтром, а также частоты шума, определены коэффициенты взаимной корреляции между током потребления без маскирования и с маскированием при помощи регулируемого фильтра, в зависимости от типа генератора шума и от его частоты. На базе генератора шума разработаны четыре устройства фильтров питания микропроцессорной системы с защитой по току потребления. Выполнено сравнение предложенных фильтров с существующими системами защиты, и установлено, что наибольшую эффективность имеют предложенные фильтры тока потребления микроконтроллеров. Библ. 4, рис. 7, табл. 1.

Ключевые слова: *регулируемый фильтр; маскирование тока потребления; системы защиты; моделирование; микроконтроллер.*

UDC 621. 3. 011: 621. 314

A.V. Moroz, **T.O. Tereshenko**, Dr.Sc.
National Technical University of Ukraine "Kyiv Polytechnic Institute",
Peremohy prosp., 37, Kyiv, 03056, Ukraine.

Adjustable power supply filters for microcontrollers with consumption current masking

For copyright protection of software for microcontrollers, it is important for developer to know real information about the degree of their security against unauthorized reading. Known methods of unauthorized reading of information by consumption current, such as the simple power analysis and the differential power analysis, are simple to perform, have low cost, and are carried out without destruction of chips. Perspective way of protection against such reading is masking of consumption current. Authors offer to create such adjustable filter of consumption currentб which would bring hindrances in consumption current of the microcontroller. To define type of the noise generator, which is necessary for control of adjustable

filter, and also noise frequency, coefficients of mutual correlation between consumption current without masking and with masking by means of adjustable filter, depending on type of the generator of noise and on its frequency are defined. On the basis of the generator of noise, four devices of filters of a microprocessor powering system with protection of consumption current are developed. Comparison of the offered filters against existing systems of protection is executed, and determined, that the offered consumption current filters have the best efficiency. References 5, Figures 6, tables 1.

Keywords: *adjustable power supply filter; consumption current masking; protection system; modeling; microcontroller.*

References

1. P. Kocher, J. Jaffe, B. Jun. (1999), Differential Power Analysis. Crypto 99 Proceedings, Lecture Notes in Computer Science. M. Wiener, ed., Springer-Verlag. Vol.1666.
2. V.O.Bezhenar, A.V.Moroz, T.O.Tereshchenko. (2010), Digital protection system against power supply attacks. Electronics and communication. No. 2. Pp. 108-114. (Ukr)
3. V.O.Bezhenar, A.V.Moroz, T.O.Tereshchenko. Patent UA 43634 Ukraine, IPC G06F 1/00 (2006.01). Microprocessor system with protection against supply current reading; filed 25.03.2009 No. u200902780 published. 25.08.2009. (Ukr)
4. V.O.Bezhenar, A.V.Moroz, T.O.Tereshchenko. Patent UA 43673 Ukraine, IPC G06K 19/06 (2006.01). Microcontroller with a protection system against supply current attacks.; filed 03.04.2009 No. u200903207, published 25.08.2009. (Ukr)