УДК 621

Р. В. Бачинський
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

МЕТОД ЗАХИСТУ КЛЮЧІВ ШИФРУВАННЯ В МІКРОКОНТРОЛЕРАХ З ВИКОРИСТАННЯМ СПЕЦІАЛЬНИХ АПАРАТНИХ БЛОКІВ

Наведено метод захисту окремих ділянок пам'яті в мікроконтролерах фірми STM, які можуть бути використані для зберігання секретних ключів шифрування даних, за допомогою спеціального апаратного блоку «Firewall». Цей метод забезпечує доступ до певних областей пам'яті мікроконтролера тільки з визначених конфігурацією апаратного блоку ділянок пам'яті програм і блокує доступ з інших областей пам'яті. Оскільки до мікроконтролерів фірми STM можна підключати зовнішню як Flash, так і SRAM (для розширення пам'яті програм і даних), було досліджено як захист ділянок зовнішньої пам'яті, так і спроби доступу з них до захищених областей.

Ключові слова: мікроконтролери, шифрування, ключі шифрування.

R. Bachynskyy
Lviv Polytechnic National University,
Computer Engineering Department

SECRET KEYS PROTECTION METHOD FOR MICROCONTROLLERS, BASED ON SPECIAL HARDWARE BLOCKS USING

The proposed article demonstrates how to protect some memory areas in STM microcontrollers, what could be used for secret cypher keys storing, by using special hardware block "Firewall". This method provides access to predefined microcontroller's memory areas form configured in "Firewall" address space and blocks access from another program memory space. Since, STM microcontrollers provides connection to external Flash and SRAM for address space expanding, memory protection with "Firewall" was investigated when unauthorized code from external memory tries to get access to protected memory areas.

Key words: microcontrollers, cyphering, secret keys.

Вступ

Стрімкий розвиток портативних мобільних пристроїв, які виконують збирання, аналіз та передавання даних для подальшої обробки та зберігання, спричинив необхідність об'єднання таких пристроїв у мережі. Процес масового розвитку таких "розумних" пристроїв та їх об'єднання в мережі назвали Інтернетом речей (IoT). Це дало змогу створювати комплексні системи, які складаються з багатьох компонент, для забезпечення різних потреб як окремих людей, так і великих галузей науки та техніки. Напрямок IoT є відносно молодим, що спричиняє різноманітність підходів до побудови таких систем та різноманітність топологій їхнього об'єднання в мережі. Проте

основні особливості та обмеження таких систем випливають із їх способів застосування. Серед них варто назвати такі:

- Компактність. Зазвичай пристрої IoT являють собою малогабаритні автономні пристрої з обмеженою функціональністю.
- Автономність. У більшості випадків пристрої IoT не мають прямого доступу до стаціонарних/провідних джерел живлення.
- Мобільність. Значна частина пристроїв IoT "прив'язана" до рухомих об'єктів (людей, машин, …).
- Наведені вище особливості накладають такі обмеження на пристрої IoT:
- Мережеві апаратні засоби, які є складовою IoT пристроїв, мають бути малогабаритними (в ідеальному випадку – бути частиною центрального процесора пристрою IoT);
- Апаратні засоби пристроїв IoT, зокрема їхня підсистема передавання даних, мають споживати мало енергії і функціонувати тривалий час від автономних джерел живлення, що накладає обмеження на протоколи та відстань передавання даних;
- Передавання даних від та до пристроїв IoT переважно має здійснюватись по безпровідним каналам, що, враховуючи друге обмеження, не так просто забезпечити.

Враховуючи, що пристрої IoT використовують у різних областях – від керування домашніми побутовими приладами до мобільних медичних пристроїв – виникає необхідність у забезпеченні надійних, шифрованих каналів передавання даних з аутентифікацією передавальної та приймальної сторін. Оскільки апаратні засоби IoT пристроїв мають бути енергоефективними та малопотужними, використання складних та ресурсомістких алгоритмів шифрування та обміну ключами переважно неможливо. Отже, найпридатніші в цьому випадку симетричні алгоритми шифрування з використанням секретних ключів. Виробники мікроконтролерів загального призначення, які найчастіше використовують для побудови пристроїв IoT, почали додавати до своїх продуктів апаратні блоки шифрування та цифрового підпису для найвживаніших алгоритмів, таких як AES. Це дає змогу пришвидшити процес шифрування/дешифрування та аутентифікації повідомлень без використання ресурсів ядра процесора та без збільшення споживання пристроєм енергії під час шифрування.

При цьому однією з найбільших проблем стають надійне зберігання секретних ключів та недопущення їхнього зчитування зловмисниками при отриманні ними фізичного доступу до пристрою.

Постановка задачі

Для забезпечення надійного зберігання секретних ключів шифрування для пристроїв IoT система має відповідати таким вимогам:

Блокування зчитування секретних ключів з використанням зовнішніх пристроїв (JTAG, SWD відлагоджувачів)	+
Блокування зчитування ключів з виконанням несанкціонованого коду	+

Дослідити відповідність системи на базі мікроконтролерів фірми ST із апаратним блоком захисту ділянок пам'яті зазначеним вимогам при використанні різних апаратних конфігурацій.

Блокування зчитування секретних ключів з використанням зовнішніх пристроїв (JTAG/SWD відлагоджувачів)

Мікроконтролери фірми ST підтримують можливість захисту від зчитування та запису окремих ділянок флеш- пам'яті, як і більшість інших контролерів інших виробників. Ці засоби сторінкового захисту від зчитування є стандартними та не потребують детального розгляду. Для захисту від зчитування з підключенням JTAG/SWD відлагоджувачів мікроконтролери дають змогу заборонити внутрішній відлагоджувач на етапі ініціалізації та в разі потреби одноразово відключити відлагоджувач таким чином, що його стане неможливо ввімкнути навіть при спробі змінити програмне забезпечення мікроконтролера. Тобто, мікроконтролери фірми ST забезпечують стандартні засоби блокування несанкціонованого доступу до пам'яті програм, як і більшість інших мікроконтролерів, для захисту від зчитування внутрішньої мікропрограми та подальшого аналізу

несанкціонованими для цього особами. Зазначені методи захисту детально розглянуті в документації мікроконтролерів і не потребують подальшого аналізу.

Блокування зчитування ключів з виконанням несанкціонованого коду

Для отримання доступу до секретних ключів пристрою зловмисники можуть інтегрувати в мікроконтролер спеціальний код для зчитування ключів з області пам'яті, в якій вони зберігаються, та передати йому управління. При цьому після зчитування ключів програма зловмисників може передати їх по одному із вбудованих у мікроконтролер комунікаційних інтерфейсів. Для блокування такої можливості зчитування секретних даних з внутрішньої пам'яті мікроконтролера фірма STM інтегрувала в свої мікроконтролери додатковий апаратний блок "Firewall". Цей апаратний блок конфігурується для забезпечення доступу до певних ділянок пам'яті (як флеш-, так і оперативної пам'яті) тільки з інших, дозволених, областей пам'яті.

Оскільки мікроконтролери фірми ST дозволяють підключати зовнішні мікросхеми флеш- та оперативної пам'яті для розширення пам'яті програм та даних, виникає необхідність дослідити можливість зчитування захищених ділянок пам'яті як при виконанні коду з внутрішньої пам'яті, так і з зовнішньої пам'яті. Тобто, необхідно дослідити дві апаратні конфігурації.

Конфігурація без використання зовнішньої пам'яті програм

У найпростіших та в найбільш вживаних випадках пристрої IoT використовують внутрішню пам'ять програм та даних, які є частиною мікроконтролера. При цьому зовнішню пам'ять як програм, так і даних не використовують. Схему підключення та взаємодії основних внутрішніх блоків мікроконтролера зображено на рис.1, де:

- Cortex M4 – процесорне ядро;
- DMA – контролер прямого доступу до пам'яті;
- Flash – пам'ять програм;
- SRAM1 – пам'ять даних;
- AHB master – інтерфейс головного пристрою шини AMBA;
- AHB slave – інтерфейс підпорядкованого пристрою шини AMBA;
- Firewall – апаратний блок захисту окремих ділянок пам'яті;
- Bus Matrix – шина AMBA.

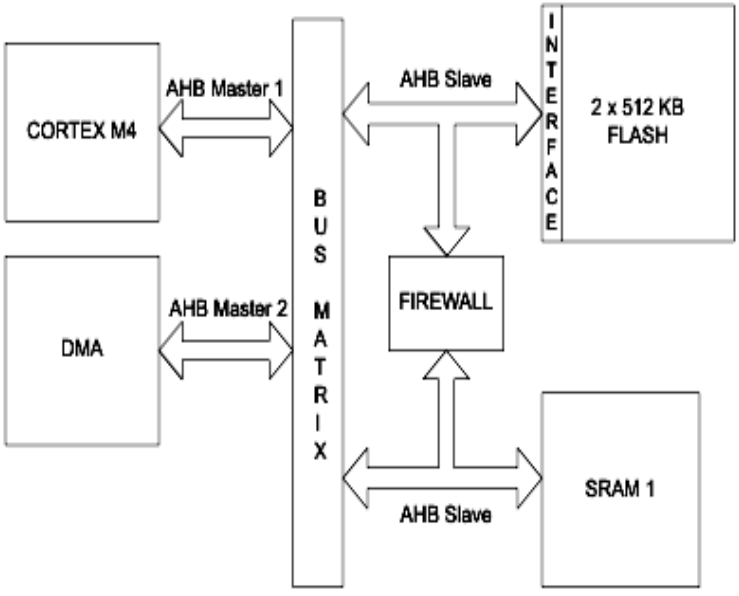

Рис. 1. Схема підключення та взаємодії основних блоків у мікроконтролерах STM32L4x6 без використання зовнішньої пам'яті

Було досліджено такі конфігурації при спробі зчитування захищених ділянок у флеш-пам’яті:

- Код зі спробою несанкціонованого доступу до захищеної ділянки розташовано в блоці Flash;
- Код зі спробою несанкціонованого доступу до захищеної ділянки розташовано в блоці SRAM1.

В обидвох випадках доступ до захищених ділянок пам’яті блокувався, а мікроконтролер перезавантажувався. Можна зробити висновок, що захищені апаратним блоком “**Firewall”** ділянки пам’яті не можуть бути зчитані навіть при спробі виконання несанкціонованого коду. При такій конфігурації секретні набори даних надійно захищені блоком “**Firewall”.**

Конфігурація з використанням зовнішньої пам’яті програм

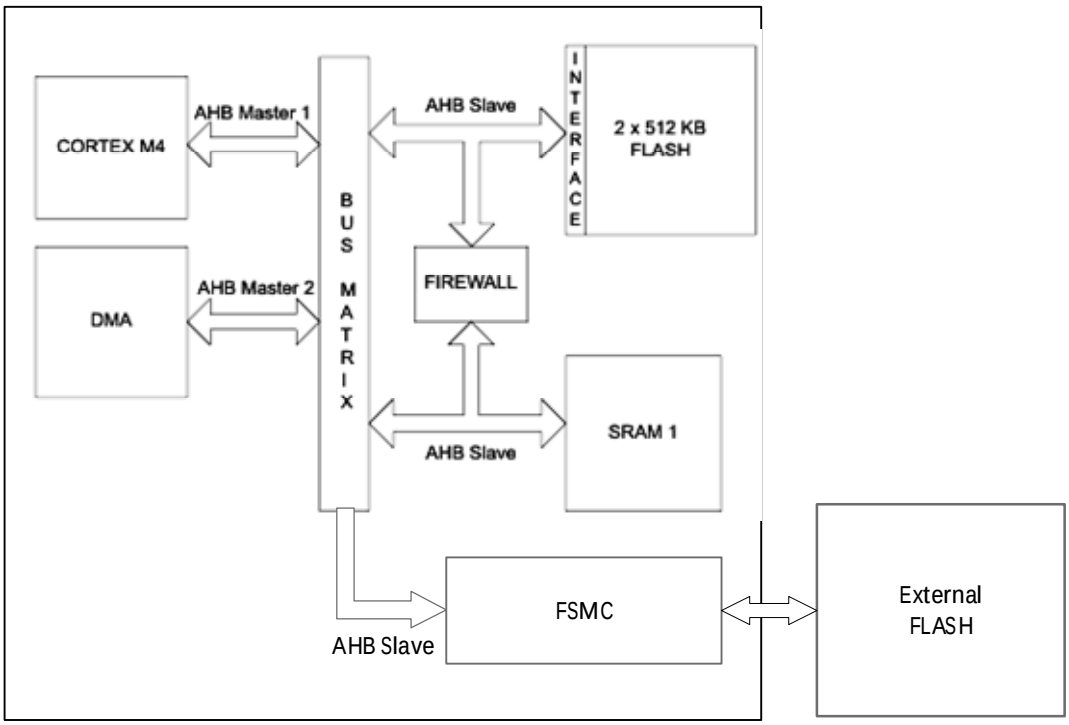

Рис. 2. Схема підключення та взаємодії основних блоків у мікроконтролерах STM32L4x6 з використанням зовнішньої пам’яті

Використання зовнішніх блоків пам’яті, які можуть використовуватись як пам'ять програм, значно спрощує зловмисникам процес інтеграції несанкціонованого коду (рис. 2). Тому така конфігурація є більш вразливою до можливих спроб злому. Було досліджено конфігурацію з інтегрованим у зовнішню флеш несанкціонованим кодом для зчитування захищених ділянок у внутрішній флеш-пам’яті. Експеримент виявив, що за цієї конфігурації несанкціонований код отримав доступ до захищених апаратним блоком **“Firewall”** ділянок пам'яті, що робить зберігання секретних даних у конфігураціях з використанням зовнішніх блоків пам’яті програм ненадійним.

Висновки

Проаналізовано метод захисту секретних ключів для пристроїв IoT за допомогою спеціального апаратного блоку захисту ділянок пам’яті, який є в мікроконтролерах фірми STM. У результаті аналізу було виявлено, що цей метод захисту працює тільки у випадку використання внутрішньої флеш-пам’яті і не працює у випадку підключення зовнішньої пам’яті, в яку можна записати спеціальний код для вичитування захищених областей пам’яті для подальшого

передавання зловмисникам. Отже, цей метод захисту секретних ключів не можна вважати надійним для апаратних конфігурацій із використанням зовнішньої пам’яті програм.

1. RM0351 Reference manual, STM32L4x5 and STM32L4x6 advanced Arm-based 32-bit MCUs ./ https://www.st.com/content/ccc/resource/technical/document/reference_manual/02/35/09/0c/4f/f7/40/03/DM00083560.pdf/files/DM00083560.pdf/jcr:content/translations/en.DM00083560.pdf 2. AN4729 Application note, STM32L0/L4 FIREWALL overview./ https://www.st.com/content/ccc/resource/technical/document/application_note/43/66/7c/63/87/9f/4c/b2/DM00209768.pdf/files/DM00209768.pdf/jcr:content/translations/en.DM00209768.pdf 3. AN4758: Proprietary code read-out protection on microcontrollers of the STM32L4 Series./ https://www.st.com/content/ccc/resource/technical/document/application_note/group0/1f/99/ef/d6/24/8d/44/08/DM00226247/files/DM00226247.pdf/jcr:content/translations/en.DM00226247.pdf