УДК 004.056.53

Собінов О.Г.
Кіровоградський національний технічний університет

Криптогріфічні співпроцесори ARM мікроконтролерів сімейства STM32F4xx

Сучасний технологічний світ важко відокремити від мережних комп'ютерних технологій. Із зростанням мереж передачі даних кількість загроз безпеки передачі даних продовжує збільшуватися. Важлива персональна і конфіденційна інформація, розташована в мережі інтернет, щодня передається через бездротові з'єднання мільйонами людей по всьому світу. Крім того через бездротові з'єднання передається інформація від великої кількості датчиків телеметричних систем збору і обробки інформації, а також сигнали управління промисловими об'єктами та процесами і транспортними засобами.

Розробники мікроконтролерів переміщують криптографічну обробку даних в апаратні блоки своєї продукції. Прискорена апаратна криптографічна обробка замість програмного виконання цих же алгоритмів дозволяє розвантажити центральний процесор для виконання алгоритмів управління та підтримки призначеного для користувача інтерфейсу.

Розробники ARM-процесорів додають у свої вироби спеціальні апаратні блоки - криптографічні прискорювачі, які працюють окремо від основного ARM-ядра. Таким чином, ядро ARM може практично не брати участь в криптографічних процесах, зберігаючи свої ресурси для виконання тих завдань, з якими вони справляються найкращим чином. До таких завдань можна віднести обслуговування обміну з периферійними пристроями, обробку даних, реалізацію бездротового обміну з іншими пристроями,які виконують управління і інші алгоритми. Таким чином відбувається оптимізація продуктивності всієї системи.

Перехід до більш ефективних методів криптографічної обробки на ARM мікроконтролери був виконаний плавно і прозоро для розробників. У минулому при виконанні алгоритмів захисту ядро ARM викликало спеціальні функції API, і необхідні алгоритми виконувалися безпосередньо ядром ARM. В даний час при наявності апаратних криптографічних прискорювачів ядро ARM викликає ті ж самі функції криптографічного API, але самі алгоритми тепер виконуються спеціалізованим криптографічним модулем, а не ядром ARM. Перенесення криптографічної обробки з ядра ARM на окремий апаратний модуль значно зменшив вплив задач захисту на виконання інших додатних задач.

Компанія STMicroelectronics, також відповідно до світових тенденцій, додала в свої нові мікроконтролери STM32F415/STM32F417 з 32-розрядних ядром ARM Cortex-M4F криптографічний прискорювач, який було перевірено на мікроконтролерах STM32F215/STM32F217 з ядром ARM Cortex-M3.

Прискорювач дозволяє шифрувати дані за алгоритмами DES/TDES/AES, обчислювати хеш-функції SHA-1/MD5/HMAC і генерувати випадкові числа. Підвищення максимальної тактової частоти з 120 МГц (для STM32F2xx) до 168 МГц (для STM32F4xx) дозволило підвищити і продуктивність криптографічного прискорювача.

Мікроконтролери сімейства STM32F4xx компанії STMicroelectronics є високопродуктивними вбудованими процесорами з 32-розрядних ядром ARM Cortex-M4F, мають співпроцесор арифметики з плаваючою

крапкою одинарної точності FPU і великим набором периферійних модулів. До цих блоків відносяться:

1) криптографічний процесор CRYP, який реалізує на апаратному рівні алгоритми DES/ TDES/AES;

2) процесор обчислення хеш-функцій HASH, що дозволяє обчислювати хеш-функції по алгоритмам SHA-1/ MD5 і коди аутентифікації повідомлень (імітовставки) на HMAC основі хеш-функцій;

3) генератор (датчик) випадкових чисел RNG, що дозволяє на основі аналогових генераторів шуму отримувати 32-розрядні випадкові числа.

Криптографічний процесор (CRYP) розташований на 32-розрядній високошвидкісній шині AHB2 і призначений для зашифровування/розшифрування даних в режимах електронного одноразового блокноту (Electronic Codebook, ECB) або зачеплення по шифротексту (Cipher block chaining, CBC) для алгоритмів DES, Triple-DES і в режимі з лічильником (Counter mode, CTR) для алгоритму AES. Для алгоритму DES довжина ключа становить 64 біта, для TDES - 64, 128 або 192 біт, для AES - 128, 192 або 256 біт. У режимах CBC і CTR використовується синхропосилка або вектор ініціалізації (Initialization Vector, IV) довжиною в чотири 32-розрядних слова.

Модуль CRYP має апаратну реалізацію алгоритмів, які вказані вище і повністю сумісну з наступними стандартами:

- стандарт шифрування даних DES і Triple-DES (), розроблений IBM Inc., як визначено в публікації FIPS PUB 46-3 від 25 жовтня 1999 року та попередньому стандарті ANSI X9.52 від 1998р;

- сучасний стандарт шифрування даних AES, як визначено в публікації FIPS PUB 197 від 26 листопада 2001р.

Алгоритми TDES і AES є блоковими шифрами, тому неповні блоки вхідних даних перед зашифровуванням потрібно доповнювати деякими даними (в кінець останнього блоку повідомлення потрібно записувати деякі дані). Після розшифрування доповнення потрібно відкидати. Апаратний блок не може керувати операцією додавання/відкидання даних, тому цим повинне займатися програмне забезпечення.

Модуль CRYP забезпечує автоматичний контроль потоку даних з підтримкою прямого доступу до пам'яті (DMA), при цьому використовуються два канали: один - для прийому вхідних даних, інший - для видачі оброблених даних і має вхідний (IN) і вихідний (OUT) буфери FIFO, глибиною вісім слів кожен, які відповідатимуть чотирьом блокам DES/TDES або двом блокам AES. Логіка перестановки даних забезпечує роботу з 1-, 8-, 16- або 32-розрядними даними.

Таким чином ми бачимо, що захист інформації, переходячи на апаратний рівень, не тільки покращує працездатність самої апаратної чистини комп'ютеризованої системи, але й значно підвищує інформаційну безпеку інформаційних потоків даних цих систем.

Список використаних джерел

1. *DS8597. STM32F415xx-STM32F417xx. ARM Cortex-M4 32b MCU+FPU, 210DMIPS, up to 1MB Flash, 192+4KB RAM, crypto, USB OTG HS_FS, Ethernet, 17TIMs, 3ADCs, 15comm. interfaces&came.* http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/DATASHEET/DM00035129.pdf.
2. *RM0090. STM32F405xx, STM32F407xx, STM32F415xx and STM32F417xx advanced ARM-based 32-bit MCUs. Reference manual.*http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/REFERENCE_MANUAL/DM00031020.pdf.
3. *Сложные алгоритмы на 32-разрядном ядре Cortex-M4F. Новые микроконтроллеры STM32F4 компании STMicroelectronics/Андрей Самоделов//Вестник Электроники. – 2012. – № 1. – С. 10-16.*