УДК 004.056.53

Колісніченко О.Ю., Собінов О.Г.
Кіровоградський національний технічний університет

Представлення структури криптографічної бібліотеки STM32

У «звичайних» системах програмування, криптографічні засоби знаходиться на рівні софту і таким чином ми отримуємо непродуктивні затрати на шифрування та дешифрування інформації. Особливо цей момент є критичним для мікроконтролерних систем, в яких ресурси обмежені (оперативна та жорстка пам'ять, швидкість процесору і т.і.).

На сьогоднішній день, базовими мікроконтролерами для більшості мережних гаджетів, стали ARM-процесори, яких на поточну дату випустили більше чотирнадцяти мільярдів. Будь яка мережа вимагає захисту різних рівнів і таким чином, в кожну з таких систем треба вводити криптографічний захист. Виходячи із використання на різних приладах різних ОС, потрібен відповідний захисний софт. Тому розробники ARM пішли іншим шляхом : вони розробили спеціальний апаратний криптографічний модуль, вбудований в архітектуру мікроконтролера.

Особливо цікавою є програмна архітектура криптографічного модулю.

Бібліотека побудована навколо модульної програмної моделі, яка забезпечує:

- незалежність між компонентами структури, яка складає основну систему
- просту адаптацію між великою кількістю різних продуктів
- використання в інтегрованих компонентах в інших продуктах, із мінімальними змінами в коді

Наступне зображення загальну структуру роботи та взаємодії криптографічної бібліотеки STM32 із іншими компонентами.

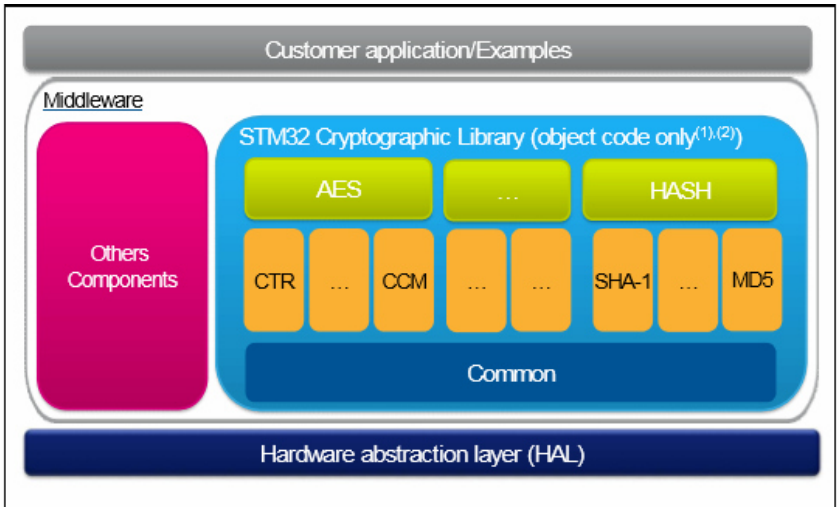

Рисунок 1 – Архітектура криптографічної бібліотеки STM32

HAL контролює системні регістри STM32 і працює на двох основних бібліотеках :

CMSIS:

- Рівень ядра периферійного доступу;

- Рівень пристрою периферійного доступу STM32xx;
- Стандартний периферійний драйвер STM32xx;
- Криптографічна бібліотека STM32.

Як представлено но рисунку 1, криптографічна бібліотека STM32 базована на модульній архітектурі, що означає можливість додавання нових алгоритмів, без впливу на поточну реалізацію пристрою. Щоб додати гнучкості криптографічним функціям, кожний алгоритм можна компілювати із різними налаштуваннями, таким чином, впливаючи на швидкість їх обробки.

Прикладний рівень. Прикладний рівень складається із набору прикладів, що покривають усі можливі алгоритми через шаблони для роботи із найрозповсюдженішими засобами програмування. Навіть без потрібної апаратної розрахункової плати, цей рівень дозволить вам швидко почати створювати нову криптографічну бібліотеку STM32.

Організація пакету. Криптографічні бібліотеки знаходяться у зжатому вигляді, запаковані у zip архівах. При розпаковці генерується папка із назвою «STM32_Cryptographic_Lib_VX.Y.Z», яка містить наступні підпапки:

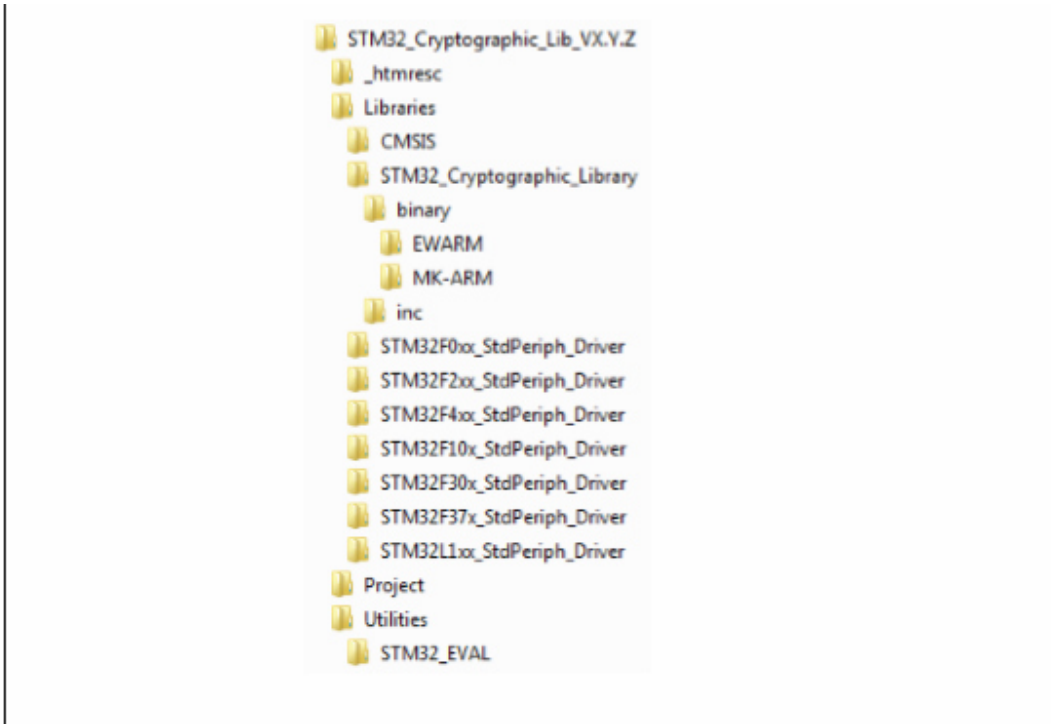

Рисунок 2 – Організація пакету криптографічної бібліотеки STM32

Отже, вбудований криптографічний модуль в процесорах ARM, є дуже вдалим засобом поліпшення шифрування та дешифрування інформації в сучасних мережевих пристроях, завдяки своїй архітектурі, яка легко адаптується, та принципу роботи. Також, цей модуль дозволяє легко й швидко створювати власні універсальні криптографічні бібліотеки.