STM32 Releasing your creativity

na CD

STM32F4: rozwiązanie dla aplikacji kryptograficznych

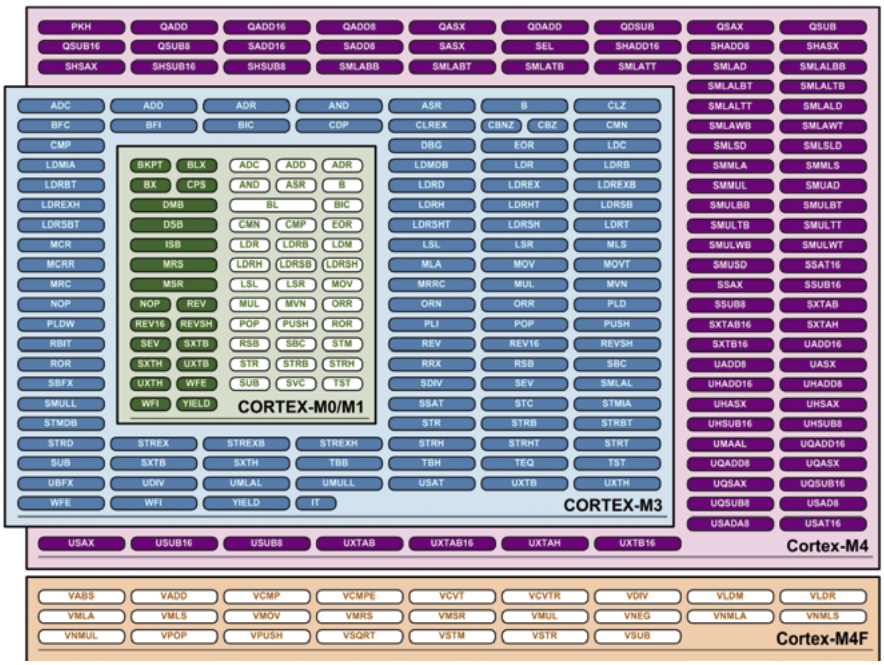
Mikrokontrolery z rodziny STM32F4 dzięki rdzeniowi Cortex-M4F i wysokiej częstotliwości taktowania doskonale nadają się do stosowania w aplikacjach DSP i dowolnych innych, wymagających dużej mocy obliczeniowej, także przy obliczeniach zmiennoprzecinkowych. Dzięki bogatemu i zaawansowanemu wyposażeniu wewnętrznemu, są także doskonałym rozwiązaniem dla bardziej specyficznych aplikacji, jak na przykład kryptografii.

Dodatkowe materiały na CD/FTP:
ftp://ep.com.pl, user: 16163, pass: 61skqs30

Mikrokontrolery STM32F4 uchodzą – nie bez racji – za szybszą (168 MHz vs 120 MHz) i lepiej wyposażoną wersję mikrokontrolerów STM32F2. „Lepszość" wyposażenia polega przede wszystkim na zastąpieniu rdzenia Cortex-M3 rdzeniem Cortex-M4F (F – oznacza, że rdzeń jest zintegrowany z FPU) co powoduje, że prawdziwe aplikacje DSP stoją przed mikrokontrolerami STM32F4 otworem. Na **rysunku 1** pokazano zestawienie „obszarów" instrukcji obsługiwanych przez wszystkie rdzenie Cortex-M: jak widać Cortex-M4 obsługuje znacznie więcej instrukcji niż Cortex-M3, co pozwala na wykonywanie wielu złożonych operacji na danych za pomocą pojedynczych poleceń asemblerowych.

Budowę mikrokontrolerów STM32F4 pokazano na **rysunku 2**. Schemat do złudzenia przypomina budowę mikrokontrolerów STM32F2. W nowych mikrokontrolerach zastosowano znany ze starszych rodzin moduł ART (**rysunek 3**) pozwalający na odczyt zawartości Flash z pełną prędkością taktowania CPU (o konieczności stosowania wait-state'ów podczas odczytu tej pamięci na razie nic nie wiadomo, jest dość prawdopodobne, że nie będą potrzebne), zastosowano w nich także zoptymalizowaną 7-poziomową magistralę AHB (**rysunek 4**), dzięki której użytkownik może wpływać na sposób komunikacji niektórych, najbardziej wymagających bloków peryferyjnych z CPU i innymi blokami peryferyjnymi. Producent zapewnia, że zachowano kompatybilność „w dół" bloków peryferyjnych wbudowanych w STM32-F4 z peryferiami zastosowanymi w STM32-F2. Z dostępnych obecnie opisów wynika, że parametry niektórych z nich poprawiono. I tak:

- timery-generatory PWM mogą być taktowane sygnałem o częstotliwości do 168 MHz,
- liczniki RTC zapewniają większą iż dotychczas rozdzielczość pomiaru (dziesiąte i setne części sekund),

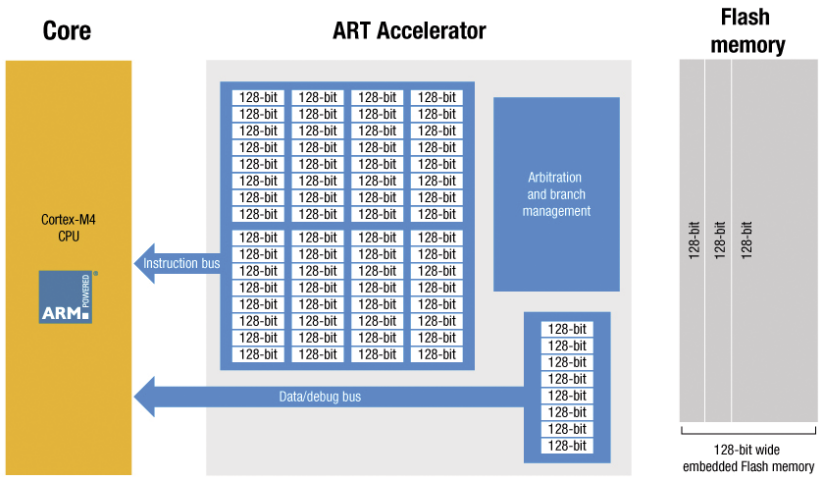


Rysunek 1. Zestawienie „obszarów" instrukcji obsługiwanych przez wszystkie rdzenie Cortex-M

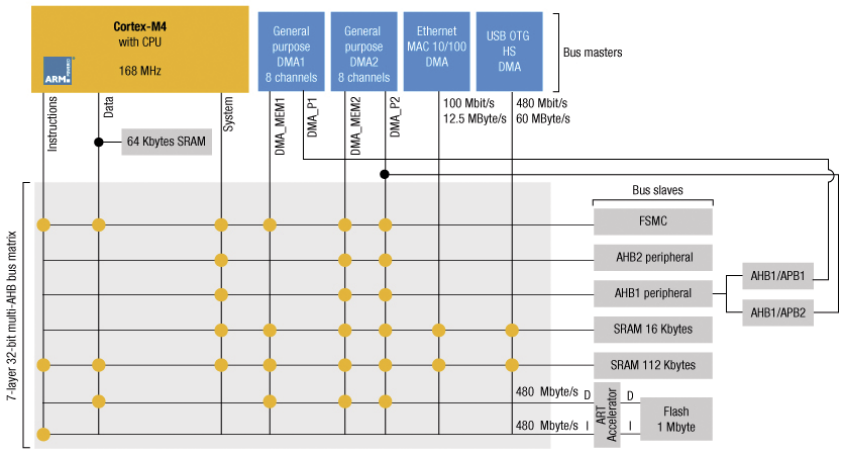
– interfejs cyfrowego audio I²S umożliwia w pełni dupleksowy transfer danych, co pozwala stosować mikrokontrolery STM32-F4 w profesjonalnym sprzęcie muzycznym,
– interfejs MAC Ethernet obsługuje protokół synchronizacji czasu IEEE1588 w nowej wersji v2.

Wprowadzono także kilka pomniejszych udoskonaleń, ale pomniemy je tutaj, nie są one bowiem głównym tematem naszych rozważań.

Rysunek 2. Schemat blokowy ilustrujący budowę mikrokontrolerów STM32F4



Rysunek 3. Schemat ilustrujący sposób działania interfejsu ART, który obsługuje dostęp CPU do pamięci Flash



Rysunek 4. Budowa ścieżek komunikacyjnych w STM32F4

STM32F4 w kryptografii: sprzęt

Wydajność obliczeniowa współczesnych mikrokontrolerów jest na tyle duża, że nie sprawi specjalnych trudności programowa realizacja większości popularnych algorytmów szyfrujących – tak jak się dzieje w szeroko rozumianych systemach PC, w których metodami kryptograficznymi chronione są m.in. łącza sieciowe czy zawartość twardych dysków. Prędkości szyfrowanego strumienia danych uzyskiwane w programowej realizacji algorytmów szyfrujących są wystarczające do wielu praktycznych zastosowań, a jakość ochrony akceptowalna nawet w aplikacjach komercyjnych.

Rozwiązanie „czysto" programowe ma jednak wadę polegającą na pochłanianiu sporej części mocy obliczeniowej, co może uniemożliwić implementację do wykonania przez mikrokontroler innych zadań. Był to podstawowy powód wyposażenia niektórych mikrokontrolerów STM32F2 i STM32F4 w sprzętowe, konfigurowalne bloki kryptograficzne:

– koprocesor kryptograficzny CRYP,
– generator skrótów HASH,
– generator liczb losowych RNG.

Koprocesor kryptograficzny CRYP (jego schemat pokazano na **rysunku 5**) jest konfigurowalnym blokiem obliczeniowym, na wejściu i wyjściu którego (od strony magistrali AHB2) znajdują się bufory FIFO danych wejściowych i wyjściowych o organizacji 8x32 bity. Silnik kryptograficzny wyposażono w zestaw rejestrów sterujących i pomocniczych, w tym dwa rejestry stanu początkowego oraz cztery rejestry dla wartości kluczy.

CRYP może pracować jako dwukierunkowy kryptoprocesor realizujący blokowe algorytmy symetryczne DES (standard FIPS PUB 46 z późniejszymi zmianami, w UE opisany w ISO/IEC18033-3), TripleDES (FIPS PUB 46-3, ISO/IEC 18033-3 (2005)) lub AES (FIPS PUB 197). W pierwszym przypadku do ochrony danych jest stosowany jeden klucz o długości 56 bitów, w przypadku TripleDES są stosowane trzy klucze o łącznej skutecz-

Cortex-M4 vs Cortex-M4F
Wdrożenie do produkcji mikrokontrolerów z rdzeniami Cortex-M4 stało się punktem honoru większości liczących się na świecie (a przynajmniej w Europie) producentów mikrokontrolerów. Niektórzy z nich wprowadzają do produkcji tańsze wersje układów z rdzeniem Cortex-M4 pozbawionym FPU. Są to z punktu widzenia użytkownika „zubożone" funkcjonalnie wersje rdzenia, chociaż rozszerzenie nazwy „kompletnych" rdzeni w nomenklaturze firmy ARM literą „F" (Cortex-M4F) sugeruje, że twórcy Corteksów (z firmy ARM) wpadli na pomysł doposażenia CPU w FPU nie tak całkiem od razu…

nej długości 168 bitów, w przypadku AES klucz może mieć długość 128, 192 lub 256 bitów. We wszystkich trybach szyfrowania/deszyfrowania, koprocesor kryptograficzny może pracować zarówno w elastycznym, pozwalającym kodować dowolne bloki danych trybie ECB (*Electronic Codebook*), jak i bezpieczniejszym, przeznaczonym do kodowania całych partii danych CBC (*Cipher Block Chaining*). W trybie AES koprocesor można wykorzystać także jako kryptoprocesor strumieniowy AES-CTR z 32-bitowym polem licznikowym i 64-bitowy wektorem początkowym (inicjującym).

Jak widać, możliwości konfiguracyjne bloku CRYP są duże i pozwalają wygodnie korzystać ze wszystkich wymienionych konfiguracji szyfrowania i deszyfrowania. Dzięki możliwości wymiany danych przez kanały DMA bez angażowania CPU, blok CRYP realnie spełnia rolę koprocesora wspomagającego CPU w specyficznych obliczeniach. Drobną, ale nieistotną z punktu widzenia większości aplikacji, niedoskonałością bloku CRYP jest brak możliwości samodzielnego konfigurowania przez użytkownika bloków substytucji S-Box, które zawsze mają wartości ustalone przez standardy (DES/TDES/AES), co nieco ogranicza możliwość zmiany stopnia ochrony kodowanych danych przez aplikację użytkownika.

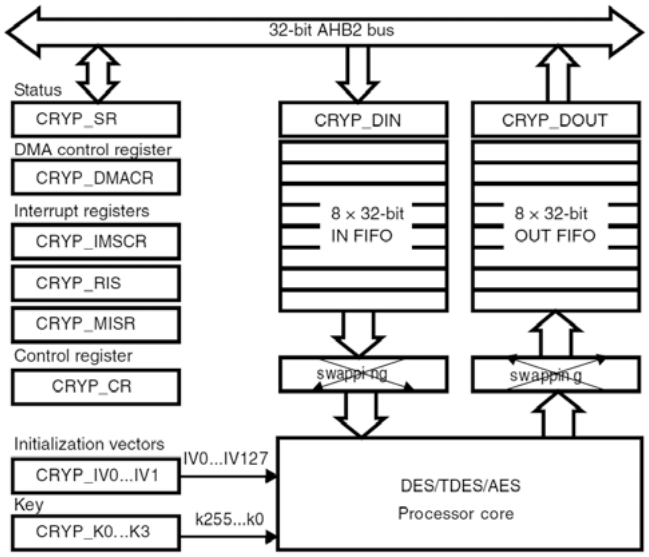
Czasy wykonania typowych operacji kryptograficznych przez CRYP umieszczono w **tabeli 1**.

W systemach kryptograficznych ważną rolę odgrywają generatory liczb losowych, których zadaniem jest m.in. tworzenie kluczy sesji lub stałych, których wartości są trudne do ustalenia dla osób postronnych. W mikrokontrolerach STM32F4 producent zastosował interesujący koncepcyjnie, choć nie do końca jawny od strony szczegółów budowy generator RNG, którego schemat blokowy pokazano na **rysunku 6**. Jego rdzeniem cyfrowym jest rejestr LFSR (*Linear Feedback Shift Register*), którego stan początkowy jest inicjowany przez wielokanałowy generator analogowy. Takie rozwiązanie powoduje - jak deklaruje producent – uzyskanie współczynnika losowości generowanych liczb na poziomie 85% wymaganych w FIPS 140-2 (*Security Requirements For Cryptographic Modules*).

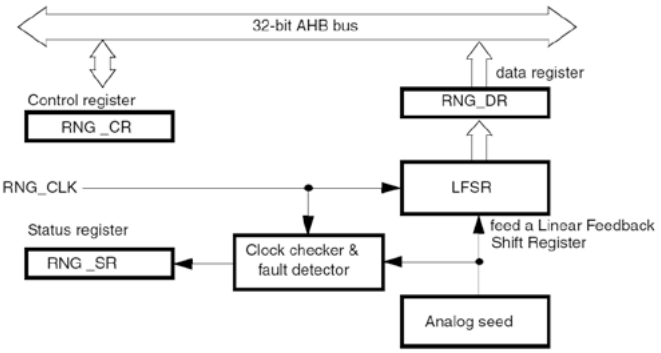
Za pomocą modułu RNG można uzyskać 32-bitową liczbę losową co każde 40 taktów zegara PLL48CLK. Generator wyposażono w system kontroli entropii i w przypadku jej braku zgłaszany jest błąd, co zapobiega nieskutecznej ochronie danych. Monitorowane są także: poprawność sygnału taktującego

Tabela 1. Czasy wykonania operacji przez CRYP

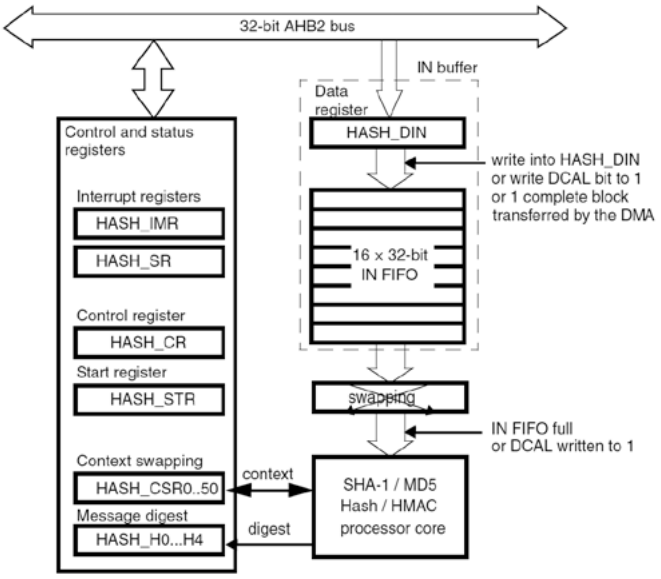
Algorytm	Klucz/długość	Liczba taktów HCLK
DES	1/56 b	16
TripleDES	1, 2, 3/168 b	48
AES	–/128	14
AES	–/192	16
AES	–/256	18



Rysunek 5. Schemat blokowy koprocesora CRYP



Rysunek 6. Schemat blokowy generator liczb losowych RNG

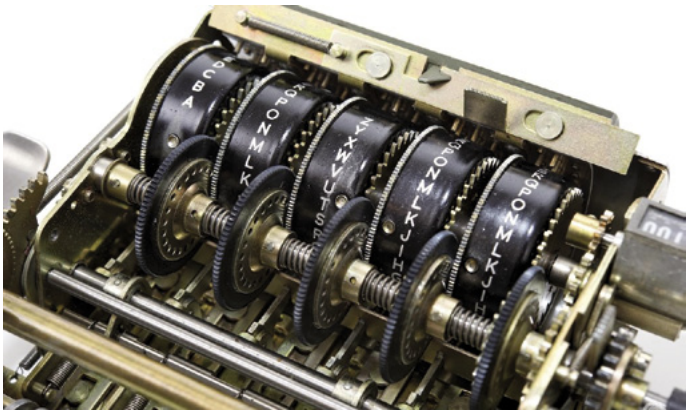


Rysunek 7. Schemat blokowy koprocesora HASH

PLL48CLK oraz jakość „zaczynu” na wejściu rejestru LFSR – wystąpienie błędów powoduje zgłoszenie przerwań.

Ostatnim blokiem peryferyjnym wbudowanym w STM32F4, związanym z kryptografią, jest sprzętowy generator skrótu (funkcji haszującej) HASH, obsługujący algorytmy SHA-1, MD5 oraz HMAC. Budowę bloku HASH pokazano na **rysunku 7**. Funkcje skrótu są stosowane najczęściej do autentykacji paczek danych (także bardzo dużych) za pomocą krótkich sygnatur, ich zadaniem jest ochrona danych przed modyfikacjami (skróty spełniają rolę zaawansowanych sum kontrolnych).

Koprocesor HASH wbudowany w mikrokontrolery STM32F4 generuje skrót SHA-1 o długości 160 bitów lub MD5 o długości 128 bitów dla wiadomości o długości do 2^{64}-1 bitów dostarczanych w blokach po 512 bitów. Czas trwania obliczania skrótu SHA-1 dla paczki danych wynosi 66 taktów zegara HCLK, czas trwania obliczeń skrótu MD5 wynosi 50 taktów HCLK – obydwa czasy bez uwzględnienia czasu niezbędnego do załadowania danych do koprocesora (16 taktów HCLK). Podobnie jak CRYP, także HASH jest obsługiwany przez DMA z dostępem do magistrali AHB2.



Podsumowanie

Przedstawione w artykule wyposażenie mikrokontrolerów STM32F4 ułatwia budowanie zaawansowanych aplikacji z wbudowanymi mechanizmami ochrony danych, zwłaszcza że producent chcąc ułatwić korzystanie z tych raczej nietypowych bloków peryferyjnych udostępnił pakiet bibliotek programistycznych zawierających ich obsługę. Są one dystrybuowane w pakiecie bibliotek CMSIS 2.0/SPL, za ich pomocą można wygodnie zainicjować i skonfigurować wszystkie opisane w artykule peryferia. W jej ramach są dostępne także „drivery” umożliwiające przyjazne dla użytkownika wykorzystywanie w aplikacjach możliwości funkcjonalnych bloków peryferyjnych, bez konieczności „wgryzania” się w szczegóły ich działania – zgodnie z zasadą „czas to pieniądz”. Programy przygotowane przez firmę STMicroelectronics są dość dokładnie skomentowane, co ułatwia zrozumienie co, jak i dlaczego się w nich odbywa.

W artykule przedstawiliśmy kolejny fragment możliwości nowych mikrokontrolerów STMicroelectronics, które poza dużą wydajnością, obsługą instrukcji SIMD i sprzętowym wspomaganiem obliczeń DSP, okazują się także silną i kompletną platformą kryptograficzną. W połączeniu z wbudowanym interfejsem MAC-Ethernet konstruktorzy otrzymują jednoukładowy komputer z możliwością obsługi protokołu SSL/TSL, którego zastosowania ogranicza wyłącznie ich wyobraźnia.

Piotr Zbysiński, EP