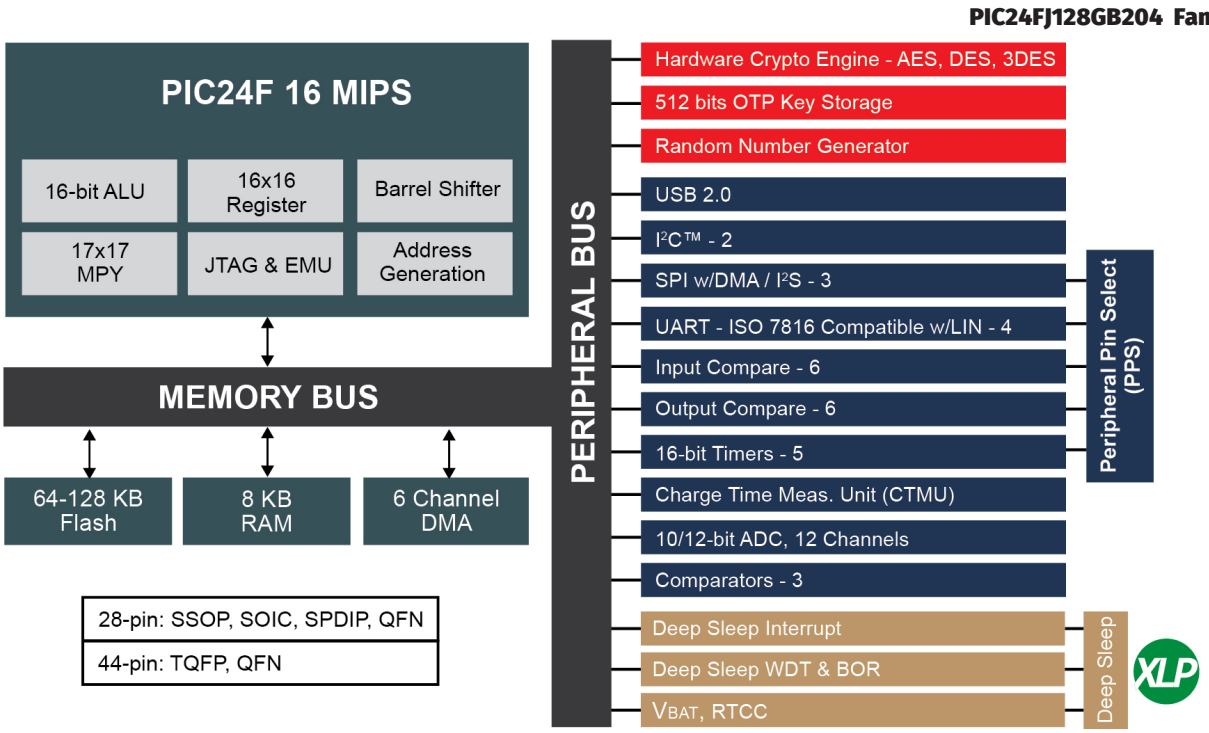


Rysunek 1. Schemat blokowy przykładowego układu z omawianej rodziny

Ochrona danych w systemach wbudowanych zasilanych akumulatorowo

Rosnąca liczba urządzeń przenośnych, podłączonych do Internetu i zasilanych z akumulatorów sprawia, że inżynierowie coraz częściej potrzebują dobrych rozwiązań, umożliwiających zabezpieczenie danych. Problemem jest nie tylko ochrona informacji przed niepowołanym dostępem, ale również zapewnienie ich poprawności przechowywania także wtedy, gdy nastąpi utrata zasilania. Mikrokontrolery Microchip PIC24F serii GB2 zawierają mechanizm kryptograficzny, generator liczb losowych oraz pamięć jednorazowo programowalną, które pomagają zachować bezpieczeństwo w aplikacjach.

Mikrokontrolery PIC24F serii GB2 są też przystosowane do tworzenia aplikacji o ekstremalnie małym poborze prądu, dzięki implementacji technologii Microchip XLP (eXtreme Low Power). Pobierają nawet jedynie 18 nA prądu w trybie uśpienia o 180 µA w przeliczeniu na megaherc w trakcie normalnej pracy.

Nowoczesne systemy wbudowane nierzadko wymagają licznych interfejsów komunikacyjnych. Układy GB2 mają zintegrowaną obsługę USB, co pozwala bardzo łatwo podłączać je do peryferiów elektronicznych i komputerów. Można też zastosować moduły Microchipa do interfejsów Wi-Fi, ZigBee czy Bluetooth Smart o niskim poborze mocy.

Polecane zastosowania

Dzięki małemu poborowi prądu oraz mechanizmom bezpieczeństwa danych, seria układów GB2 znajduje zastosowanie w szerokim zakresie komputerów przemysłowych oraz w sprzęcie medycznym i sportowym. Może posłużyć do tworzenia elektronicznych zamków do drzwi i systemów kontroli dostępu, niezależnie od tego, czy pracują w oparciu o klawiaturę, karty magnetyczne, czy interfejsy bezprzewodowe. Inne typowe aplikacje obejmują kamery bezpieczeństwa oraz zautomatyzowane systemy sprzedaży – gdyż oba te rodzaje projektów wymagają zapewnienia wysokiego stopnia bezpieczeństwa. Układy GB2 będą też użyteczne w inteligentnych czujnikach, wpisujących się w trend Internetu Przedmiotów, np. do monitorowania ciśnienia, temperatury, natężenia światła czy wilgotności i przesyłania zebranych informacji bezprzewodowo.

Układy PIC24F GB2 mogą też zostać użyte do produkcji peryferiów komputerowych o małym poborze mocy, zasilanych przez USB lub z baterii i łączących się bezprzewodowo; zestawy słuchawkowe i bezprzewodowe drukarki mają takie właśnie cechy.

W przypadku urządzeń medycznych i związanych z fitnessem, mikrokontrolery serii GB2 mogą przetwarzać dane w krokomierzach oraz wszelkich urządzeniach, które gromadzą wrażliwe dane i łączą się z smartfonami i tabletami.

Bezpiecznie zapisane dane mogą też zawierać informacje konfiguracyjne, zarówno w pamięci na tej samej płytce drukowanej, jak i w zewnętrznych urządzeniach, choćby podłączanych bezprzewodowo przez szyfrowane łącza.

Mechanizm kryptograficzny

Układy PIC24 serii GB2 zawierają w pełni sprzętowy mechanizm szyfrowania, wspierający algorytmy AES, DES i 3DES. Obsługuje wiele opcji konfiguracyjnych, a w tym szyfrowanie i deszyfrowanie 128-, 196- i 256-bitowego AESu oraz wszystkie tryby pracy (ECB, CBC, CFB, OFB i CTR) w ramach tych algorytmów. Fakt, że funkcje te są realizowane

sprzętowo, znacząco zmniejszone jest zapotrzebowanie na moc obliczeniową. Obliczenia w układach sprzętowych są wykonywane wiele razy szybciej niż programowo. Dokładniej – implementacje sprzętowe sprawiają, że potrzeba jedynie kilkuset cykli pracy procesora na przetworzenie bloku danych, podczas gdy w aplikacjach całkowicie programowych, taki sam blok będzie wymagał kilkunastu tysięcy cykli. Oznacza to zarazem, że procesor używając obwodów sprzętowych do kryptografii nie musi wstrzymywać wykonywania głównej części programu, na czas szyfrowania czy deszyfrowania. Pokazano to w **tabeli 1**, w której zawarto liczby cyklów potrzebnych na wykonanie poszczególnych operacji w układach PIC24F serii GB2.

Tabela 1. Liczba cykli potrzebnych na poszczególne operacje kryptograficzne przy użyciu jednostek kryptograficznych układów z serii GB2

Tryb	Liczba cykli (w przybliżeniu)	
	Na blok	Dodatkowo na załadowanie i rozładowanie
DES szyfrowanie/deszyfrowanie	10*	2
3DES szyfrowanie/deszyfrowanie	26*	2
128-bitowy AES szyfrowanie/deszyfrowanie	219** ***	32
192-bitowy AES szyfrowanie/deszyfrowanie	275** ***	32
256-bitowy AES szyfrowanie/deszyfrowanie	299** ***	32
DES 64-bity szyfrowanie klucza sesji	10	2
DES 2x 64-bity szyfrowanie klucza sesji	10	2
DES 3x 64-bity szyfrowanie klucza sesji	20	4
AES 128-bity szyfrowanie klucza sesji (128-bit KEK)	219	32
AES 128-bity szyfrowanie klucza sesji (192-bit KEK)	275	32
AES 128-bity szyfrowanie klucza sesji (256-bit KEK)	299	32
AES 192/256-bitów – szyfrowanie klucza sesji (128-bit KEK)	438	48
AES 192/256-bitów – szyfrowanie klucza sesji (192-bit KEK)	550	48
AES 192/256-bitów – szyfrowanie klucza sesji (256-bit KEK)	598	48
DES 64-bity ładowanie klucza sesji	10	2
DES 2x 64-bity ładowanie klucza sesji	10	2
DES 3x 64-bity ładowanie klucza sesji	20	4
AES 128-bity ładowanie klucza sesji (128-bit KEK)	219***	32
AES 128-bity ładowanie klucza sesji (192-bit KEK)	275***	32
AES 128-bity ładowanie klucza sesji (256-bit KEK)	299***	32
AES 192/256-bitów – ładowanie klucza sesji (128-bit KEK)	438***	48
AES 192/256-bitów – ładowanie klucza sesji (192-bit KEK)	550***	48
AES 192/256-bitów – ładowanie klucza sesji (256-bit KEK)	598***	48

* 64-bitowe bloki
** 128-bitowe bloki
*** Nie wliczono cykli potrzebnych na inicjalizację deszyfrowania AES po zmianie kluczy

Szybsze skończenie pracy nad przetwarzanymi blokami prowadzi do ograniczenia zużycia energii, gdyż układ może pracować z pełnym obciążeniem przez krótszy czas. Alternatywnie można po prostu zastosować wolniejsze taktowanie, które zmniejsza zapotrzebowanie na moc. Oszczędność dotyczy także pamięci – sprzętowe algorytmy nie wymagają używania dużych, szybkich układów RAM, ani nie zajmują tyle miejsca w pamięci programu.

Korzyści płynące z użycia algorytmów sprzętowych łatwo obliczyć. Weźmy pod uwagę realizację 128-bitowego algorytmu AES, w którym przetworzenie każdego 16-bajtowego bloku wymaga 250 cykli pracy procesora. Przy taktowaniu 32 MHz uzyskujemy w praktyce 16 mln cykli pracy na sekundę, a więc w ciągu sekundy procesor przetwarza 1024 tysiące bajtów.

Przyjmijmy, że chcemy przetworzyć jedynie 1024 bajty danych. Przy wyliczonym tempie, potrzebna będzie jedynie 1 ms na taką operację. Maksymalny prąd, jaki układ może pobierać przy taktowaniu 32 MHz i napięciu 2 V to 7,6 mA. Ponieważ 1 ms to 1/3600000 godziny, na przetworzenie 1024 bajtów danych potrzebne będzie 4,2 nWh (nano-wato-godzin) energii.

Generowanie kluczy

Do generowania kluczy potrzebnych do szyfrowania i deszyfrowania danych oraz autentykacji wykorzystuje się liczby losowe. Mikrokontrolery serii GB2 pozwalają tworzyć zarówno liczby prawdziwie losowe, jak i pseudolosowe. Te pierwsze zapewniają większe bezpieczeństwo, gdyż nie da się ich odtworzyć, co ogranicza możliwości złamania zabezpieczeń. Ponadto liczby prawdziwie losowe są przydatne także w systemach gier. W niektórych przypadkach, np. w symulacjach i w modelowaniu, korzystne jest używanie liczb z generatora pseudolosowego. Układy serii GB2 umożliwiają swobodny wybór rodzaju generowanych liczb.

Bezpieczne przechowywanie kluczy

Wbudowana pamięć jednorazowego programowania pozwala bezpiecznie przechowywać klucze zabezpieczające, uniemożliwiając ich niepowołany odczyt. Dostęp do nich ma tylko algorytm szyfrujący, a odczytanie tej pamięci z poziomu aplikacji nie jest możliwe. Ta jednokrotnie programowania pamięć mieści 512 bitów, co pozwala na przechowanie kilku kluczy. W przypadku 256-botpwegp szyfru AES, zmieszczą się tam 2 klucze, w 128-bitowym AESie – 4 klucze, a gdy używany jest 64-bitowy DES – pamięć wystarczy na 8 kluczy.

Jeśli zaistnieje potrzeba użycia większej liczby kluczy, można je bezpiecznie przechowywać dzięki koncepcji klucza szyfrującego klucze (KEK – Key Encryption Key). Polega ona na tym, że zapisany w bezpiecznej pamięci klucz służy do deszyfrowania fragmentu pamięci Flash lub RAM, w której zapisana jest dowolna liczba zaszyfrowanych kluczy. Cały algorytm został przygotowany w taki sposób, by klucze po odszyfrowaniu również nie były dostępne do bezpośredniego odczytu z poziomu oprogramowania, ale by mogły zostać użyte w dalszych sprzętowych procesach kryptograficznych. Są bowiem – po deszyfracji – przechowywane w specjalnie zarezerwowanym na ten cel rejestrze, niedostępnym dla oprogramowania.

Przykładowa aplikacja: elektroniczne zamki do drzwi

Dobrym przykładem użycia omawianych mikrokontrolerów jest projekt elektronicznego zamka do drzwi. Schemat blokowy takiego rozwiązania został przedstawiony na rysunku XXXXXXX. Obwody kryptograficzne mikrokontrolerów rodziny GB2 pozwalają zaszyfrować dane użytkownika, takie jak np. imiona i nazwiska pracowników, kody oraz daty i godziny czasów wejść i wyjść. Mogą być też użyte do autentykacji w trakcie prób dostępu do zabezpieczonych stref budynków, w oparciu o przedstawione przez użytkownika dane. Wszystkie krytyczne informacje są w bezpieczny sposób zapisane

Tabela 2. Dostępne modele mikrokontrolerów PIC24FJ GB2 I GA2

Model	USB	Flash	L. wyprowadzeń	Obudowy
PIC24FJ128GB204	tak	128 kB	44	TQFP, QFN
PIC24FJ128GB202	tak	128 kB	28	SOIC, SSOP, QFN, SPDIP
PIC24FJ64GB204	tak	64 kB	44	TQFP, QFN
PIC24FJ64GB202	tak	64 kB	28	SOIC, SSOP, QFN, SPDIP
PIC24FJ128GA204	nie	128 kB	44	TQFP, QFN
PIC24FJ128GA202	nie	128 kB	28	SOIC, SSOP, QFN, SPDIP
PIC24FJ64GA204	nie	64 kB	44	TQFP, QFN
PIC24FJ64GA202	nie	64 kB	28	SOIC, SSOP, QFN, SPDIP

i wczytywane tylko wtedy, gdy procesor potrzebuje ich użyć do realizacji algorytmów szyfrowania lub deszyfrowania.

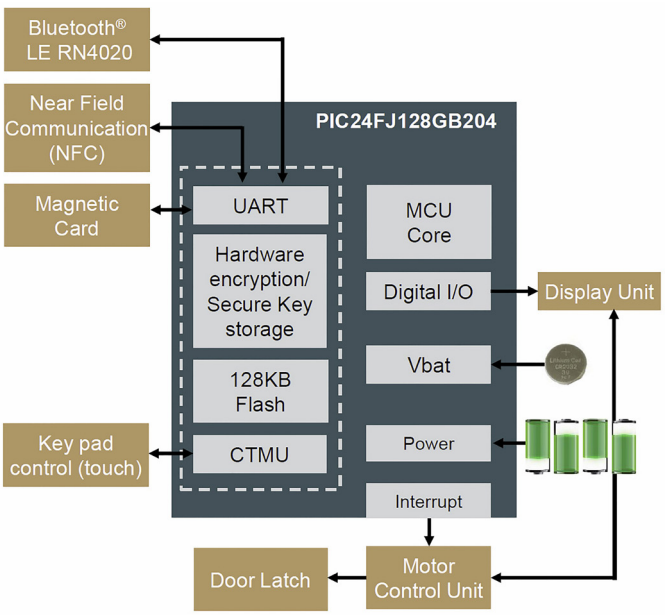
Dodatkowo, użyteczna w takim projekcie może okazać się zintegrowana jednostka CTMU (Charge Time Measurement Unit), która pozwala na wykrywanie dotyku i realizację przycisków zbliżeniowych – np. w postaci klawiatury numerycznej. Jeśli użytkownik nie wchodzi w interakcje z systemem, urządzenie może przejść w stan spoczynku – do trybu o najmniejszym poborze mocy, by zaoszczędzić energię z baterii.

Silnik odryglowujący drzwi jest uruchamiany za pomocą prostego przerwania. Niektóre z systemów mogą być zasilane bezpośrednio, ale w przypadku większych rygli używa się czterech baterii AA. Cały system może działać tylko z zasilania bateryjnego, co w typowej aplikacji oznacza konieczność wymiany źródła zasilania co kilka lat. Co więcej, mikrokontrolery serii GB2 mają dodatkowo wejście VBAT, które pozwala na podłączenie baterii podtrzymującej pracę kalendarza i zegara czasu rzeczywistego (RTCC – Real Time Clock Calendar), użytecznego np. do rejestracji czasu wejść i wyjść pracowników. Dzięki temu urządzenie nie wymaga aktualizacji czasu, gdy główna bateria zostanie wyczerpana i wymieniona.

Do odczytu kart magnetycznych lub komunikujących się bezprzewodowo, używany jest interfejs UART. W bardziej zaawansowanych aplikacjach użytkownik może dostawać kod potrzebny do odblokowania drzwi na telefon i używać smartfona do otwierania zamka – np. przez Bluetooth Smart lub NFC.

Przykładowa aplikacja: zabezpieczanie pamięci EEPROM

Wiele różnorodnych aplikacji wymaga przechowywania ważnych danych konfiguracyjnych, potrzebnych do pracy urządzenia, w zewnętrznej pamięci EEPROM, zlokalizowanej na płytce drukowanej. Choć dane te są przechowywane lokalnie, problem ich ochrony nie jest trywialny. Bywa tak, że użytkownicy usuwają układy EEPROM z płytek i zastępują je swoimi, w których zapisano inne parametry. Świetnym przykładem jest motoryzacja, w której w ten sposób można zmienić parametry pracy silnika, zwiększając jego maksymalną moc, ale też skracając żywotność oraz podwyższając



Rysunek 2. Przykład aplikacji szyfrowego zamka cyfrowego do drzwi

emisję szkodliwych substancji. Podobny problem pojawia się też w grach, gdzie użytkownicy mogą zwiększyć swoje szanse, właśnie poprzez zmianę zawartości pamięci konfiguracyjnej. Wszystkich tych problemów można uniknąć, jeśli pamięć się zaszyfruje, bezpiecznie przechowywanym kluczem.

Narzędzia deweloperskie

Układy PIC24 serii GB2 współpracują z całym ekosystemem płytek deweloperskich Microchip Explorer 16. Potrzebny jest jedynie nowy moduł procesorowy (PIM – Processor plug-In Module). Dwa takie nowe moduły znalazły się w tabeli XXXX.

Dodatkowe karty rozszerzeń pozwalają na realizowanie połączeń USB, obsługę inteligentnych kart lub kart SIM. Dostępne są też karty z interfejsami bezprzewodowymi, w tym Wi-Fi i Bluetooth Smart.

Podsumowanie

Układy PIC24F serii GB2 spełniają wiele oczekiwań, stawianych przed mikroprocesorami stosowanymi w przenośnych systemach wbudowanych. Zapewniają wysoki stopień bezpieczeństwa dzięki zintegrowanym obwodom kryptograficznym, generatorom liczb losowych oraz jednorazowo programowanej pamięci. Projektanci mogą tworzyć bezpieczne systemy, bez podnoszenia zużycia energii, co pozwala tworzyć produkty o długim czasie pracy na baterii. Bogate interfejsy komunikacyjne, ułatwiają tworzenie projektów wpisujących się w trend Internetu Rzeczy.

Alexis Alcott
Senior Manager
Dział mikrokontrolerów 16-bitowych
Microchip Technology Inc.

Tabela 3. Narzędzia deweloperskie kompatybilne z omawianymi układami

Rodzaj	Model	Numer	Cena
Płytka deweloperska	Explorer 16 Board	DM240002	$ 129,99
Moduł procesorowy	PIC24FJ128GB204 USB	MA240037	$ 25,00
	PIC24FJ128GB204 bez USB	MA240036	$ 25,00
Płytka rozszerzeń PICtail Plus	USB PICtail Plus	AC164131	$ 60,00
	Smart Card/SIM Card PICtail	AC164141	$ 29,99
Płytki rozszerzeń do modułów komunikacyjnych	RN4020 Bluetooth LE PICtail/PICtail Plus	RN-4020-PICtail	$ 49,00
	Wi-Fi- PICtail	RN-171-PICtail	$ 39,95
	802.15.4 ZigBee MRF24J40MA PICtail Plus	AC164134-1	$ 24,99
	Sub-GHz MRF89XAM8A PICtail Plus	AC164138-1	$ 39,99