Altera Cyclone III LS

FPGA z systemami antywłamaniowymi

Według niektórych źródeł straty wynikłe z kradzieży własności intelektualnej i fałszowania produktów mogą w 2009 roku przekroczyć 1,5 biliona dolarów (10^{12}!). Przestępstwa takie dotyczą również rynku elektronicznego. Wielu producentów podzespołów wprowadza więc coraz więcej mechanizmów podnoszących poziom zabezpieczeń projektu. W artykule opisano najnowsze układy FPGA firmy Altera z zaawansowanymi funkcjami zabezpieczającymi projekt przed kopiowaniem.

Rodzina układów Cyclone III, jak sama nazwa wskazuje, jest już trzecią generacją „popularnych" układów FPGA firmy Altera. Są to układy łączące małe zapotrzebowanie na energię (moc statyczna układów przy 200 tys. elementów logicznych LE wynosi 0,25 W) i niską cenę z dużą funkcjonalnością.

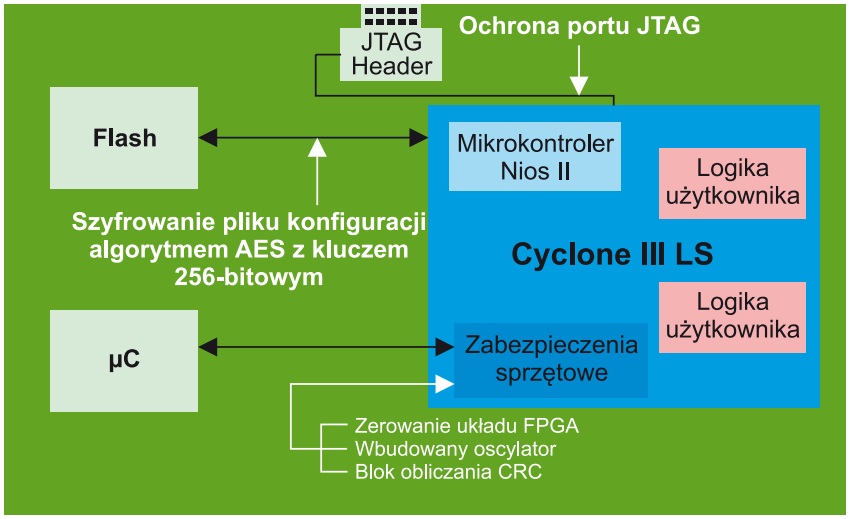
Układy są wykonane w procesie technologicznym 65 nm. W skład rodziny Cyclone III wchodzi 12 układów, wśród których są cztery nowe, „bezpieczne" Cyclone III LS. Układy te mogą być stosowane w wielu różnych aplikacjach, gdyż w skład rodziny Cyclone III wchodzą zarówno układy stosunkowo małe (o 5 tys. elementów logicznych), jak i rozbudowane układy przeznaczone do aplikacji multimedialnych (do 198 tys. elementów logicznych). Oprócz pokaźnych zasobów logicznych mają one również od 414 kb do 7,8 Mb wbudowanej pamięci RAM. Funkcje DSP wspierane są przez układy mnożące 18×18 bitów, których jest 23...396. W **tab. 1** zestawiono porównanie najważniejszych parametrów układów z rodziny Cyclone III.

Układy z oznaczeniem LS są nowymi układami w rodzinie Cyclone III. Odznaczają się rozwiązaniami sprzętowymi, które zabez-

Fot. 1. Najczęściej podrabiane są najbardziej znane urządzenia

Tab. 1. Porównanie układów Cyclone III i Cyclone III LS

Rodzina	Układ	Elementy logiczne [tyś.]	Bloki pamięci M9K	Całkowita pojemność RAM [bit]	Układy mnożące 18×18	Pętle PLL	Globalne sieci sygnału zegarowego	Maks. liczba końcówek I/O użytkownika
Cyclone III	EP3C5	5136	46	423936	23	2	10	182
	EP3C10	10320	46	423936	23	2	10	182
	EP3C16	15408	56	516096	56	4	20	346
	EP3C25	24624	66	608256	66	4	20	215
	EP3C40	39600	126	1161216	126	4	20	535
	EP3C55	55856	260	2396160	156	4	20	377
	EP3C80	81264	305	2810880	244	4	20	429
	EP3C120	119088	432	3981312	288	4	20	531
Cyclone III LS	EP3CLS70	70208	333	3068928	200	4	20	413
	EP3CLS100	100448	483	4451328	276	4	20	413
	EP3CLS150	150848	666	6137856	320	4	20	413
	EP3CLS200	198464	891	8211456	396	4	20	413



Rys. 2. Zabezpieczenia układów Cyclone III LS

pieczają projekt przed kradzieżą. Przeznaczone są więc do aplikacji, w których wymagany jest niski pobór mocy oraz szczególne zabezpieczenia projektu.

Bezpieczne układy

Ochrona projektu jest jednym z kluczowych aspektów konkurencyjności wielu firm. Praktycznie żadna firma produkująca urządzenia elektroniczne nie może sobie pozwolić na udostępnianie bezpłatnie swoich projektów, zwłaszcza tych innowacyjnych. Wiele firm z krajów, w których ochrona własności intelektualnej stoi na niższym poziomie niż w Unii Europejskiej, wprowadza niskim kosztem urządzenia łudząco podobne lub będące kopią 1:1 znanych, markowych urządzeń (**fot. 1**). Zdarza się nawet, że powielane są błędy konstrukcyjne, które średnio zaawansowany elektronik może łatwo wychwycić i skorygować. W przypadku firm produkujących urządzenia na rynek masowy, kradzież projektu może oznaczać poważne straty finansowe. W przypadku firm produkujących urządzenia elektroniczne na potrzeby wojskowe odtworzenie danego urządzenia może mieć o wiele poważniejsze konsekwencje.

Kopiowanie projektu implementowanego w układzie programowalnym jest stosunkowo łatwe. Wystarczy skopiować zawartość pamięci konfiguracyjnej, aby można było uruchomić skradziony projekt na kolejnych układach. Firmy produkujące układy FPGA dość dawno zauważyły potrzebę zabezpieczania zawartości pamięci konfiguracji przed nieuprawnionym dostępem lub przed tzw. inżynierią odtwarzającą *(reverse enginering)*. Najprostszym rozwiązaniem jest nieudostępnianie (lub zmiana) formatu danych, w którym przechowywana jest konfiguracja układu. Rozwiązaniem, które jest obecnie najszerzej stosowane, jest szyfrowanie zawartości pamięci konfiguracji.

W skład zabezpieczeń układów Cyclone III LS wchodzą mechanizmy zabezpieczenia zarówno przed tradycyjnymi atakami na pamięć Flash przechowującą plik konfiguracji, jak i przed atakami inwazyjnymi. W celu ochrony szczególnie wrażliwych projektów, układy oferują oprócz standardowego szyfrowania pamięci konfiguracji ochronę portu JTAG, sprzętowe obwody wykrywania ataku inwazyjnego oraz nieustanne sprawdzanie sumy kontrolnej CRC zaprogramowanej pamięci konfiguracji.

W skład kompletu zabezpieczeń układów Cyclone III LS wchodzą (**rys. 2**):

- Zabezpieczenia sprzętowe:
  - szyfrowanie pliku konfiguracyjnego algorytmem AES z kluczem 256-bitowym,
  - ochrona portu JTAG,
  - wewnętrzny oscylator,
  - aktywne zerowanie zawartości pamięci konfiguracji,
  - obliczanie sumy kontrolnej CRC zaprogramowanego projektu.
- Zabezpieczenia na poziomie oprogramowania projektowego:
  - separacja modułów projektowych.
- Zabezpieczenia na poziomie modułów IP:
  - moduł IP nadzorcy (Supervisor IP).

Zabezpieczenia sprzętowe

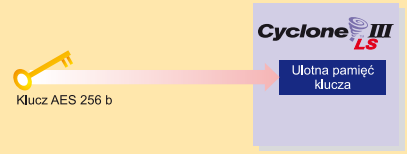
Zabezpieczenia sprzętowe mają za zadanie chronić projekt w układzie FPGA (pamięć konfiguracji) przed, w trakcie i po etapie konfigurowania układu programowalnego. Wszystkie układy Cyclone III (nie tylko LS) ograniczają możliwość bezpośredniego odczytania bieżącej konfiguracji poprzez port JTAG. Nie istnieje żadna metoda ani przyrząd firmy Altera, które pozwalałoby na odczytanie konfiguracji układu FPGA tej firmy.

Już o tym pisaliśmy

W artykule „Atak na mikrokontrolery!" w EP2/2009 opisaliśmy stosunkowo tanie i przystępne metody ingerencji i odczytu zawartości pamięci nieulotnej popularnych mikrokontrolerów. W EP8...10/2002 zajmowaliśmy się natomiast zagadnieniami bezpieczeństwa danych zapisanych w pamięci mikrokontrolera.

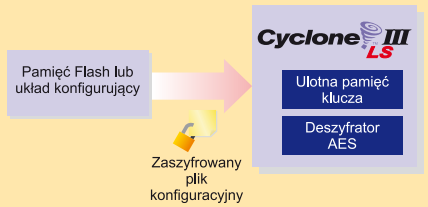
Proces zabezpieczania projektu dla układu Cyclone III LS

Pierwszym krokiem jest zaprogramowanie układu FPGA w systemie kluczem AES o długości 256 bitów. Klucz poddawany jest zaciemnieniu i zapisywany w dedykowanej ulotnej pamięci SRAM (*volatile register*).



Wynikowy plik konfiguracji układu (z rozszerzeniem .pof) jest szyfrowany za pomocą wybranego w poprzednim kroku klucza AES w programie Quartus II i umieszczany w nieulotnej pamięci konfiguracji Flash (EPC lub EPCS).

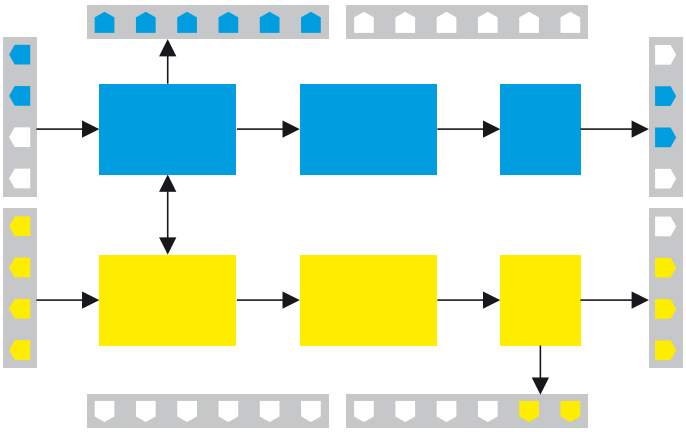
Po włączeniu zasilania zaszyfrowany plik konfigurujący jest przesyłany z nieulotnej pamięci konfiguracji do układu Cyclone III LS. Wewnętrzny moduł układu Cyclone III LS dokonuje deszyfracji pliku konfiguracyjnego, po czym następuje proces konfigurowania układu FPGA.



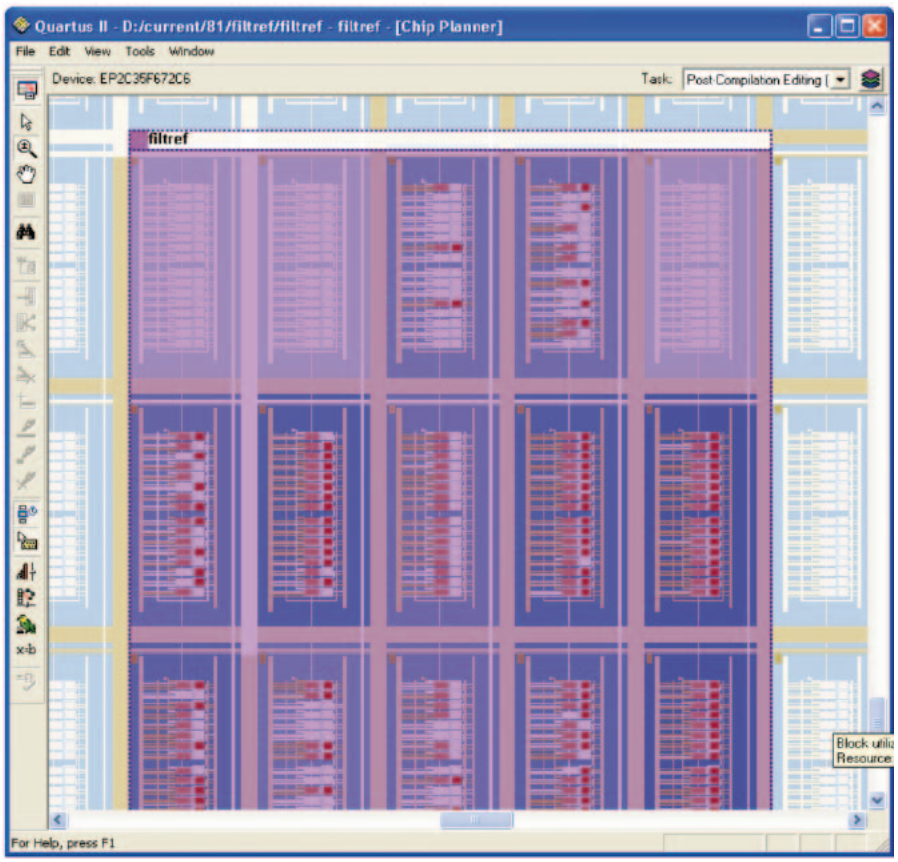
Odczytanie pliku .pof z zewnętrznej pamięci konfiguracji nie może więc posłużyć do zaprogramowania innego układu Cyclone III LS, gdyż nie jest znany klucz AES.

Po włączeniu zasilania układy Cyclone III LS obsługują wyłącznie obligatoryjne komendy JTAG (BYPASS, SAMPLE/PRELOAD, EXTEST oraz FACTORY). Dostęp do pozostałych komend opisany jest w dokumentacji układów. Odbywa się on po wysłaniu komendy FACTORY. Po wysłaniu tej komendy pamięć konfiguracji CRAM oraz klucz AES są wyzerowane.

Ochronie podlega również *bitstream*, czyli dane przesyłane do pamięci konfiguracji układu FPGA z zewnętrznej pamięci FLASH podczas etapu konfiguracji układu po włączeniu zasilania. *Bitream* jest szyfrowany algorytmem AES z 256-bitowym kluczem. Przed zapisaniem w układzie klucz poddawany jest zaciemnieniu (*obfuscation*) i przechowywany w pamięci o długości 512 B. Klucz przechowywany jest wewnątrz układu FPGA w pamięci ulotnej, której zawartość musi być podtrzymywana bateryjne po odłączeniu zasilania. Dodatkowo pamięć służąca do przechowywania tego klucza jest umieszczona pod warstwami metalicznymi, aby uniemożliwić do niej fizyczny dostęp. W ramce obok przedstawiono etapy konfigurowania układu do pracy z zaszyfrowanym plikiem konfiguracji.



Rys. 3. Partycjonowanie projektu dla układu FPGA



Rys. 4. Umieszczanie modułów projektowych za pomocą funkcji LogicLock w programie Quartus II

Powyższe metody mają chronić pamięć konfiguracji oraz sam plik konfiguracji przed nieautoryzowanym odczytem. Jak wiadomo, zawartość pamięci RAM można przy zastosowaniu pewnych metod (EP02/2009) zmienić w trakcie pracy układu. W celu monitorowania spójności danych pamięci konfiguracji CRAM, układy Cyclone III LS są wyposażone w jednostkę obliczania sumy kontrolnej CRC tej pamięci. Drugim elementem poprawiającym bezpieczeństwo systemu w trakcie jego pracy jest wewnętrzny oscylator, który służy jako źródło sygnału zegarowego dla systemów nadzorujących pracę układu. Wewnętrzny oscylator służy jako pewne źródło sygnału zegarowego. W przypadku prób manipulowania zewnętrznym sygnałem zegarowym, krytyczne funkcje bezpieczeństwa układu nieprzerwanie monitorują stan jego pracy (np. obliczanie sumy kontrolnej CRC). Nawet przy wyłączonym zewnętrznym sygnale zegarowym układ może zainicjować i przeprowadzić proces zerowania.

Zabezpieczenia na poziomie projektu

Układy Cyclone III LS są obsługiwane przez najnowsze wersje środowiska projektowego Quartus II w wersji 9.0 SP2. Wśród metod podnoszących poziom bezpieczeństwa projektu na etapie jego opracowywania znajdują się techniki znane z wcześniejszych wersji tego programu. Są to kompilacja przyrostowa (*incremental compilation*) oraz możliwość umiejscowienia modułu projek-

towego w zadanym bloku logicznym układu (LogicLock). Funkcja LogicLock umożliwia logiczne i fizyczne podzielenie projektu, dzięki czemu uzyskuje się pewność, że oddzielne partycje projektu działają niezależnie (**rys. 3**). Rozdzielenie projektu na kilka oddzielnych partycji ma zapobiegać przeciekom danych pomiędzy partycjami.

Funkcja LogicLock pozwala na umiejscowienie partycji projektowych w określonych blokach logicznych układu FPGA (**rys. 4**). W momencie, gdy w oprogramowaniu projektowym włączona jest tryb pracy z separacją partycji (*design separation flow*), każda z zabezpieczanych partycji projektu ma zdefiniowany region zastrzeżony. Działa on jak linia demarkacyjna, której nie mogą przekroczyć inne funkcje logiczne w etapie kompilowania projektu. Również wewnętrzne połączenia pomiędzy komórkami logicznymi układu nie mogą nachodzić na zabezpieczone strefy.

Budowa wewnętrzna układów Cyclone III LS została przystosowana do zabezpieczania partycji projektowych. W układach z rozszerzeniem LS separacja projektowa została rozszerzona również na porty I/O.

Nadzorca

Układy Cyclone III LS są wyposażone w mechanizm samozerowania. W przypadku wykrycia próby odczytania danych z układu FPGA, błędnej sumy kontrolnej CRC pamięci CRAM, układ może się samoistnie wyzerować. Przy domyślnych ustawieniach zerowana jest pamięć konfiguracji CRAM i wbudowana pamięć RAM układu FPGA. Dodatkowo przechowywany klucz AES może być niezależnie wyzerowany.

Nadzorca IP (*Supervisor IP*) jest modułem projektowym z biblioteki bloków IP firmy Altera, który służy jako interfejs do komunikacji ze sprzętowymi zabezpieczeniami układów Cyclone III LS. Blok ten nieprzerwanie monitoruje port JTAG przed nieuprawnionym dostępem, sprawdza sumę kontrolną CRC pamięci konfiguracji w trakcie pracy układu i może zainicjować proces jego zerowania i ponownego konfigurowania.

Podsumowanie

Kradzież projektów, czy tak zwana inżynieria odtwórcza, nie są zjawiskami nowymi. Trudno też jednoznacznie stwierdzić ich powszechność, ale z pewnością wśród Czytelników EP znajdą się pracownicy firm, które padły ofiarą tego procederu.

Układy Cyclone III są przeznaczone do wydajnych aplikacji multimedialnych, jak np. SDR (*Software Defined Radio*) czy odtwarzaczy wideo, systemów kryptograficznych i projektowanych na zamówienie sterowników przemysłowych, w których istotna jest ochrona danych, jak na przykład w urządzeniach wojskowych, kryptograficznych czy aplikacjach finansowych. Producenci urządzeń elektronicznych tego rodzaju, którzy chcą podnieść bezpieczeństwo swoich produktów, powinni wziąć pod uwagę właśnie układy Cyclone III LS.

Maciej Gołaszewski, EP
maciej.golaszewski@ep.com.pl