STUDIA INFORMATICA 2002
Volume 23 Number 2B (49)

Adam ZIĘBIŃSKI
Politechnika Śląska, Instytut Informatyki

ADAPTACYJNY SYSTEM KRYPTOGRAFICZNY

Streszczenie. W ramach prowadzonych badań nad implementacją algorytmów kryptograficznych w układach FPGA powstał pewien zasób elementów w języku VHDL. Elementy te realizują funkcje lub części poszczególnych funkcji algorytmów: DES, IDEA, BLOWFISH. Powstałe elementy można wykorzystać do stworzenia adaptacyjnego systemu kryptograficznego. W artykule przedstawiono propozycje budowy takiego systemu oraz przedstawiono wyniki pierwszych badań wykonanych na karcie HOT2 firmy VCC.

THE ADAPTATION CRYPTOGRAPHIC SYSTEM

Summary. Certain range of elements in the VHDL language was created as a result of the research concerning the cryptographic algorithms implementation. Those elements execute functions or parts of particular functions of algorithms: DES, IDEA, BLOWFISH. The resultant elements can be used for making the adaptation cryptographic system. The article presents structure of such a system and the first results of the research done on the HOT2 card from VCC company.

1. Wprowadzenie

W ramach prowadzonych badań nad implementacją kryptograficznych algorytmów blokowych iteracyjno podstawieniowo-permutacyjnych [1] w matrycach programowalnych zaproponowano metodę implementacji tych algorytmów w układach FPGA. W wyniku przeprowadzonych prac powstała biblioteka kryptograficzna VHDL [11] elementów realizujących funkcje algorytmu DES [4, 5, 10]. Z wykorzystaniem opracowanej biblioteki i na podstawie przyjętej metody implementacji rozpoczęto projektowanie elementów realizujących funkcje innych algorytmów kryptograficznych [6], w tym IDEA [2] i BLOWFISH [3]. Prace nad budową elementów realizujących funkcje tych algorytmów

zostały zakończone na etapie pełnej implementacji w środowisku ACTIVE-HDL firmy Aldec [9] oraz implementacji złożonych funkcji tych algorytmów w środowisku FOUNDATION 2.1 firmy XILINX [8]. Wykorzystanie doświadczeń zdobytych podczas implementacji algorytmu DES pozwoliło na sprawne i szybkie wykonanie elementów realizujących funkcje tych algorytmów. Proponowana metoda dała również pozytywne wyniki podczas implementacji innych algorytmów i funkcji kryptograficznych lub ich części, w tym:

- funkcji skrótu SHA,
- algorytmu Rabina Millera – testowanie liczb pierwszych,
- generatorów liczb pseudolosowych.

W efekcie prowadzonych badań powstał pewien zasób elementów realizujących funkcje różnych algorytmów kryptograficznych wykonanych w języku VHDL. Pierwszym zastosowaniem powstałych elementów jest implementacja każdego z nich z osobna w układzie programowalnym. Element szyfrujący umieszcza się w systemie kryptograficznym, w którym będzie pełnił funkcje koprocesora kryptograficznego. Powstałe elementy realizujące funkcje algorytmów kryptograficznych można jednak wykorzystać znacznie efektywniej, co umożliwiają właściwości matryc programowalnych. Właściwość wielokrotnego programowania tych układów oraz dostępne coraz większe zasoby pozwalają na stworzenie adaptacyjnego systemu kryptograficznego. System taki można wykonać wyłącznie na matrycach programowalnych lub w postaci hybrydowej programowo-sprzętowej. W każdym z tych przypadków otrzymujemy nową jakość i wyższy poziom bezpieczeństwa niż w tego rodzaju systemach programowych. W efekcie możliwe będzie stosowanie zrealizowanych na podstawie matryc programowalnych układów kryptograficznych, w systemach wymagających dynamicznej zmiany algorytmów szyfrujących i deszyfrujących.

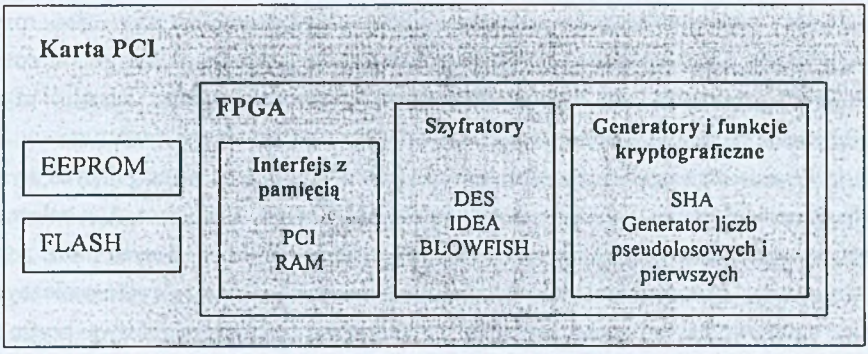
2. Sprzętowy adaptacyjny system kryptograficzny

W wyniku prowadzonych badań powstał pewien zasób elementów realizujących funkcje różnych algorytmów kryptograficznych wykonanych w języku VHDL (DES, IDEA, BLOWFISH, funkcja skrótu SHA oraz generator liczb pierwszych i pseudolosowych). Tak duży zasób funkcji kryptograficznych stosowany jest obecnie w rozwiązaniach programowych, w bardzo złożonych systemach zapewniających duży poziom bezpieczeństwa danych przechowywanych na dyskach, jak i przesyłanych w sieciach publicznych. Do tego typu aplikacji należą między innymi: *PGP* [14], *PEM* czy też *SecMail* [16]. Większość z nich zawiera kilka algorytmów kryptograficznych, wśród których implementowane są np.: RSA, DES, CAST, IDEA, GOST, BLOWFISH. Implementacja

kilku algorytmów w jednym produkcie pozwala na szyfrowanie danych różnymi algorytmami, co dodatkowo wpływa na zwiększenie poziomu bezpieczeństwa przechowywanych danych.

Złożone systemy kryptograficzne realizowane są również w rozwiązaniach sprzętowych. W produkcie firmy Analog Devices ADSP-2141L [14] zaimplementowano algorytm DES, RSA i DSA funkcje mieszające SHA-1 i MD-5. Natomiast w produkcie firmy Motorola MPC190 [16] zaimplementowano algorytmy: DES, RSA, Diffie-Hellman, ECC, DSA, Eliptic Curve, a także funkcje mieszające RC4, SHA-1 i MD-5. Ponadto układ ten zawiera 32-bitowy generator liczb pseudolosowych, IPSecurity protocol (IPSEC), Internet Key Exchange (IKE), Secure Socet Layer (SSL), WAP gateways oraz inne aplikacje.

Wykonanie tak złożonego systemu kryptograficznego możliwe jest obecnie również w środowisku matryc programowalnych. System taki może składać się modułów: interfejsu z pamięcią, szyfratorów, generatorów i funkcji kryptograficznych. Moduł interfejsu z pamięcią mógłby zawierać element PCI do komunikacji z systemem komputerowym oraz pamięć pełniącą funkcje bufora danych przeznaczonych do szyfrowania i deszyfrowania. Moduł szyfratorów mógłby zawierać elementy realizujące funkcje algorytmów DES, IDEA i BLOWFISH. Natomiast moduł generatorów i funkcji kryptograficznych mógłby zawierać generatory liczb pierwszych i pseudolosowych oraz funkcje skrótu np. SHA. Rys. 1 przedstawia propozycję adaptacyjnego systemu kryptograficznego z wykorzystaniem matryc programowalnych.



Rys. 1. Adaptacyjny system kryptograficzny
Fig. 1. The adaptation cryptographic system

Obecnie dostępne układy programowalne posiadają duże zasoby sprzętowe rzędu milionów bramek. Układy te można programować wielokrotnie, co pozwala zmieniać połączenia wewnętrzne bez uszczerbku dla układu. Zaprojektowane w VHDL-u elementy realizujące funkcje kryptograficzne są bardzo złożone i zajmują sporo zasobów sprzętowych. Ze względu na zbyt małą liczbę dostępnych zasobów sprzętowych niemożliwa jest obecnie implementacja dużego systemu kryptograficznego, np. typu PGP w jednym układzie

programowalnym. Do tego celu można jednak wykorzystać wiele układów programowalnych lub skorzystać z możliwości przeprogramowania tych układów. System kryptograficzny może być modyfikowany w zależności od potrzeb użytkownika lub ustawień systemu komputerowego. Jeżeli system lub użytkownik wymaga, by dane były szyfrowane algorytmem DES, to przed rozpoczęciem tej operacji wykonywane jest programowanie układu FPGA implementacją algorytmu DES. W ten sam sposób odbywać się to może dla każdej innej funkcji kryptograficznej. Funkcje kryptograficzne mogą być przechowywane w pamięci EEPROM, FLASH lub ściągane z pamięci masowej systemu, w którym zainstalowany jest sprzętowy system kryptograficzny. Rozwiązanie z pamięcią EEPROM wpływa znacznie na zwiększenie bezpieczeństwa, gdyż w tym przypadku sprzętowy system kryptograficzny można modyfikować tylko funkcjami zaprogramowanymi w pamięci. W przypadku korzystania z pamięci masowej zawsze istnieje możliwość uszkodzenia pliku lub prób jego podmiany. W każdym z tych rozwiązań możliwe jest wprowadzanie do systemu nowych algorytmów i funkcji kryptograficznych. Rozwiązanie takie nie jest obecnie możliwe w systemach sprzętowych opartych na układach ASIC. W tym przypadku zawsze kończy się to wymianą układu na nowy. Sprzętowy adaptacyjny system kryptograficzny mógłby pozwalać na korzystanie z starych projektów dla niego napisanych i wprowadzanie nowych projektów bez potrzeby zmiany fizycznej części systemu, a jedynie poprzez wymianę oprogramowania. Jest to więc struktura bardzo elastyczna, pozwalająca w dodatku na modyfikacje w trakcie pracy systemu. Jak widać, proponowany system ma wiele zalet. Właściwość reprogramowania układów FPGA bardzo zbliża go do rozwiązań programowych. Możliwość wykonywania równoległego operacji zbliża go do rozwiązań sprzętowych opartych na technologii ASIC, pozwalając przy okazji uzyskiwać porównywalne prędkości przetwarzania i dając podobny poziom bezpieczeństwa.

Rozwiązanie tego typu może mieć zastosowanie w aplikacjach wymagających wysokiego stopnia bezpieczeństwa. Użytkownik może dobierać funkcje zabezpieczeń w zależności od potrzeb i wprowadzać nowe funkcje. Dodatkowo protokół wymiany danych może zostać tak skonstruowany, by zajmował się wyborem stosowanych funkcji kryptograficznych bez wiedzy użytkownika, co może wpłynąć na podwyższenie bezpieczeństwa szyfrowanych danych. System mógłby być również wykonany w taki sposób, by rozpoznawał, jakim algorytmem ma zdeszyfrować dany plik. Następnie wykonywana byłaby wymiana algorytmu szyfrującego na aktualnie potrzebny poprzez przeprogramowanie układu FPGA. System taki może być również wykonany jako hybryda programowo-sprzętowa, w której część funkcji kryptograficznych realizowana jest przez komputer, a tylko funkcje najbardziej złożone przez sprzęt. Rozwiązanie takie pozwala na szybsze stworzenie takiego systemu, wpływa jednak na zmniejszenie poziomu bezpieczeństwa.

3. Adaptacyjny system kryptograficzny na karcie HOT2 PCI

Doskonałym przykładem środowiska, w którym można przeprowadzić badania nad implementacją adaptacyjnego systemu kryptograficznego, jest karta HOT2 PCI [12] firmy Virtual Computer Corporation, na której zostały wykonane pierwsze badania związane z budową systemu kryptograficznego opartego na algorytmie DES. Karta ta umożliwia wielokrotne reprogramowanie zawartego w niej układu FPGA. W efekcie możliwa jest wymiana systemu kryptograficznego lub samego elementu szyfrującego w układzie FPGA. Zatem możliwe jest stosowanie zrealizowanych na podstawie matryc programowalnych układów kryptograficznych, w systemach wymagających dynamicznej zmiany algorytmów szyfrujących.

Karta HOT2 PCI pozwala budować 32-bitowe systemy z pełną obsługa magistrali PCI. Na karcie znajdują się między innymi:

- układ FPGA,
- dwa moduły pamięci SRAM 2 MB połączone niezależnymi magistralami 32-bitowymi z układem FPGA,
- złącza do kart rozszerzeń,
- pamięć typu FLASH przechowująca konfigurację PCI_CORE oraz HOS (system operacyjny sterujący komunikacją z otoczeniem),
- pamięć CACHE wykorzystywana jest w rekonfiguracji elementu FPGA wraz z układem CCM zarządzającym programowaniem układu FPGA.

Karta dostępna jest w kilku wersjach z różnymi układami FPGA firmy XILINX, od układu Spartan XCS40 poprzez XC4062XLA, aż do ostatnio udostępnianego układu XC4085XLA. Karta z układem XC4062XLA udostępnia użytkownikowi ponad 45 000 bramek, w tym ponad 2100 komórek logicznych na własne projekty. Wielkość ta jest jednak niewystarczająca do implementacji każdego elementu kryptograficznego wykonanego w VHDL-u i zawartego w stworzonej bibliotece kryptograficznej. Natomiast możliwe jest przeprowadzenie badań wstępnych z wykorzystaniem wcześniej wykonanych elementów realizujących funkcję algorytmu DES.

Implementację elementu DES na karcie HOT2 PCI rozpoczęto od budowy rejestru umożliwiającego podawanie klucza i danych do zaszyfrowania. Zastosowanie komunikacji poprzez rejestr znacznie ułatwia przeprowadzenie pierwszych badań i testów, ograniczając złożoność implementacji do minimum. Całość projektu składa się z PCI_CORE [7], rejestru zawierający 64-bitowy klucz i daną do zaszyfrowania oraz elementu DES. Badania implementacji zostały przeprowadzone dla elementu XC4062 w różnych wersjach szybkościowych od 7 do 9ns. Tak przeprowadzone badanie dodatkowo mogło wykazać, jaki wpływ na szybkość szyfrowania ma sama wymiana elementu FPGA na szybszy.

Na podstawie otrzymanych wyników (tabela 1) można stwierdzić, że implementacja synchroniczna sekwencyjna jest najmniej efektywna i jest porównywalna z wersją programową. Cały projekt zajmuje 1110 komórek CLB. Układ może pracować z częstotliwością od 21 do 28 MHz. Operacja szyfrowania jest wykonywana w ciągu 90 taktów, a szybkość szyfrowania, może wynieść od 1,8 do 2,5 MB/s.

Tabela 1

Wyniki implementacji elementu DES z rejestrem i PCI

Wersja elementu DES	CLB	MB/s	MHz	takty
Synchroniczna sekwencyjna	1110	1,8 - 2,5	20,8 - 28,6	90
Synchroniczna kombinacyjna - sygnały	937	8,7 - 12,2	19,5 - 27,4	18
Synchroniczno kombinacyjna - zmienne	977	8,2 - 11	18,5 - 25	18

W wersji synchronicznej z elementami kombinacyjnymi z wykorzystaniem sygnałów szyfrowanie jest wykonywane w 18 taktach. Projekt zajmuje 937 komórek CLB i może pracować z częstotliwością od 19 do 27 MHz. W efekcie układ z zaimplementowanym elementem DES mógłby szyfrować z szybkością od 8,7 do 12,2 MB/s.

Wersja synchroniczna z elementami kombinacyjnymi z wykorzystaniem zmiennych zajmuje 977 komórek CLB. Zaimplementowany element DES może pracować z częstotliwością od 18 do 25 MHz. Wersja ta również wykonuje operację szyfrowania w 18 taktach, co pozwoli szyfrować z szybkością od 8,2 do 11 MB/s.

Najlepsze rezultaty osiągnięto w implementacji z elementem DES w wersji synchronicznej z elementami kombinacyjnymi z wykorzystaniem sygnałów. Implementacja w układzie XC4062 9ns zainstalowanym na karcie HOT2 PCI pozwala szyfrować z szybkością prawie 9 MB/s, co jest rezultatem zdecydowanie lepszym od wersji programowych. Rozwiązanie to można porównać z PC DES/RSA Card [12] firmy VASCO pozwalającym na szyfrowanie z prędkością do 10 MB/s. Wymiana układu FPGA na XC4062 7ns umożliwiłaby zwiększenie prędkości szyfrowania o prawie 40% do ponad 12 MB/s.

4. Wnioski

W wyniku przeprowadzonych prac przedstawiono propozycję budowy adaptacyjnego systemu kryptograficznego z wykorzystaniem układów programowalnych. Do przeprowadzenia pierwszych badań nad jego budową wybrano kartę HOT2 PCI firmy VCC. Dla układu programowalnego znajdującego się na karcie wykonano w środowisku Foundation 2.1 firmy Xilinx implementację systemu kryptograficznego realizującego funkcję

szyfrowania algorytmem DES. Wykonana implementacja pozwala szyfrować z szybkością prawie 9 MB/s, co jest rezultatem zdecydowanie lepszym od wersji programowych. Rozwiązanie to można porównać z kartą PC DES/RSA firmy Vasco Data Security, pozwalającą szyfrować z szybkością ponad 10 MB/s. Wymiana układu FPGA na szybszy umożliwiłaby zwiększenie szybkości szyfrowania o prawie 40% do ponad 12 MB/s. Ponieważ układy FPGA można programować wielokrotnie, możliwe jest wykonanie urządzenia szyfrującego pozwalającego na dynamiczną wymianę algorytmów szyfrujących, w zależności od potrzeb użytkownika. W dalszym etapie prac wykonana zostanie implementacja algorytmu 3DES na karcie HOT2, co pozwoli na przeprowadzenie pierwszych badań nad wymianą algorytmów kryptograficznych w budowanym adaptacyjnym systemie kryptograficznym.

LITERATURA

1. Schneier B.: Kryptografia dla praktyków. Protokoły, algorytmy źródłowe w języku C. Wydawnictwa Naukowo-Techniczne, Warszawa 1995.
2. IDEA Algorithm – www.ascom.ch/infosec/idea.
3. The Blowfish Encryption Algorithm – www.counterpane.com/blowfish.html.
4. Ziębiński A.: Sprzętowe metody ochrony informacji. Bezpieczeństwo informacji w systemach komputerowych, Bielsko-Biała 2002.
5. Ziębiński A.: Implementacje blokowych algorytmów kryptograficznych w środowisku ACTIVE-CAD. Reprogramowalne Układy Cyfrowe, Szczecin 2001.
6. Ziębiński A., Bagiński J., Fałek K.: Implementacje blokowych algorytmów kryptograficznych w języku VHDL. Studia Informatica, czerwiec 2000.
7. Xilinx Inc.: LogiCORE PCI Data Book, San Jose 1997.
8. Xilinx Inc.: Xilinx Foundation Series, version 2.1i, San Jose 1999.
9. Active-HDL ver. 3.5, Aldec Inc, Henderson 1998.
10. Znamirowski L., Ziębiński A.: Projekt rozwiązania sprzętowego szyfratora i deszyfratora opartego o matryce programowalne FPGA. T. IV, PC KBN nr 8T11C 026 98C/4258. Instytut Informatyki, Politechnika Śląska, Gliwice 1999.
11. Standard VHDL Language Reference Manual. IEEE Std 1076-1993, New York 1994.
12. PC DES/RSA – Card. www.vasco.com
13. H.O.T. II, Hardware Guide. Version 2.0. Virtual Computer Corporation, Reseda 1999.
14. ANALOG DEVICES, ADSP-2141L - www.analog.com/pdf/ADSP-2141L_0.pdf, Norwood 2000.

15. PGP. www.nai.com
16. SecMail. www.sotel.com.pl
17. MPC190. www.motorola.com/smartnetworks

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 11 kwietnia 2002 r.

Abstract

This paper presents the project of construction of the adaptation cryptographic system by means of programmable circuits. The implementation of the cryptographic system executing the cipher function with the DES algorithm on the HOT2 card from Virtual Computer Corporation company was made during the research. This implementation enables you to cipher at a speed of nearly 9MB/sec. This result is comparable to the ciphering speed of the PC DES/RSA card from Vasco Data Security company – i.e. over 10 MB/sec. Since the FPGA circuits can be programmed repeatedly, the construction of a ciphering device that allows for dynamic change of the ciphering algorithms, which depends on the user's needs, is possible. The implementation of the 3DES algorithm in the environment of on the HOT2 card will be the next stage. Further research leads to the construction the adaptation cryptographic system in the environment of FPGA.