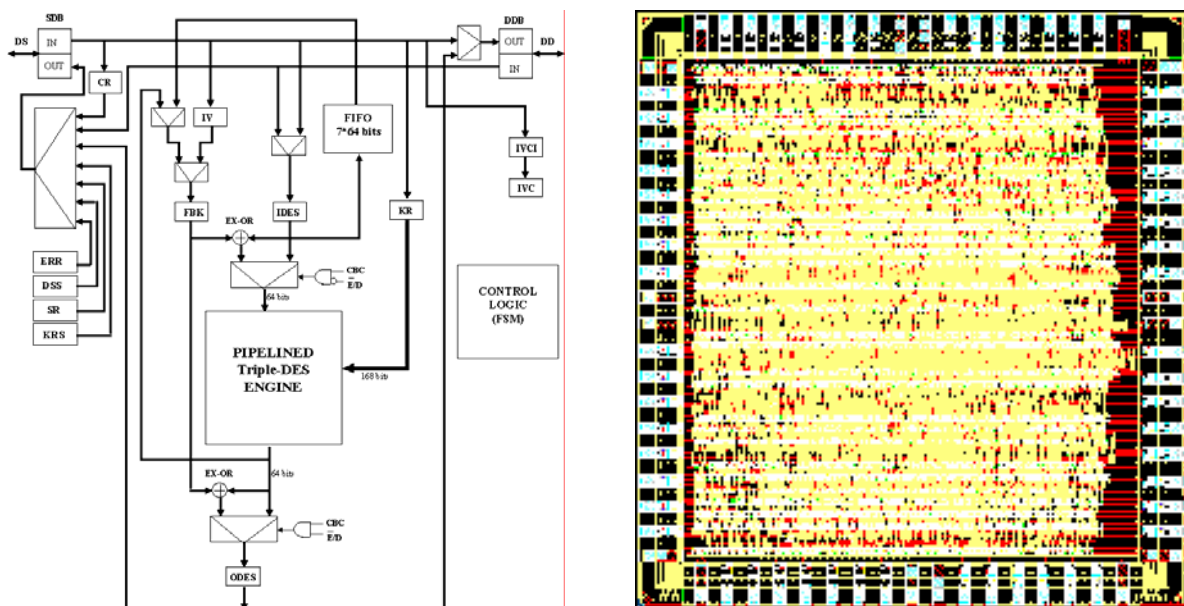


Procesor kryptograficzny MCY74C609 do szyfrowania i deszyfrowania danych na dyskach stałych komputerów PC

Opis osiągnięcia

W sytuacji wszechobecności komputerów PC w instytucjach administracji publicznej oraz szeroko rozumianej działalności biznesowej, problem właściwej ochrony danych przechowywanych na dyskach stałych komputerów jest kluczowy. Rozwiązanie problemu stwarza kryptografia, umożliwiającą szyfrowanie danych zapisywanych na dysku i deszyfrowanie podczas odczytu. Proces ten musi odbywać się na tyle szybko aby nie spowalniał transferów dyskowych w sposób zauważalny dla użytkownika systemu. W ITE opracowano specjalizowany układ scalony procesora kryptograficznego MCY74C609, umożliwiającą bardzo szybką, sprzętową realizację procesu szyfrowania i deszyfrowania danych dyskowych. W układzie zaimplementowano zaawansowany algorytm kryptograficzny 3DES, zapewniający bardzo wysoki poziom ochrony danych (klucz 168-bitowy). Prototyp układu wykonany został w technologii CMOS 0.8 μ m firmy AustriaMicrosystems (AMS) za pośrednictwem organizacji EUROPRACTICE. Wykonany w tej technologii układ MCY74C609 umożliwia szyfrowanie i deszyfrowanie danych z szybkością 20MB/s.



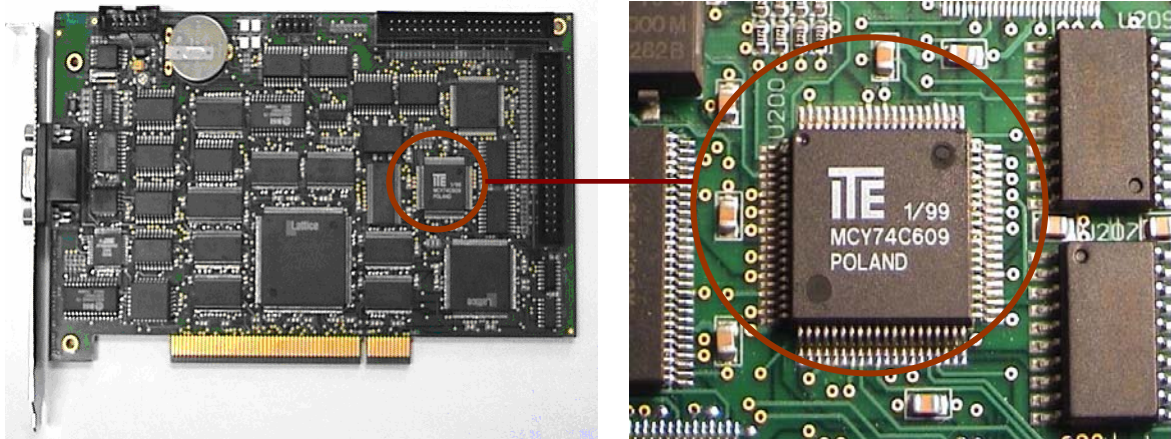
Rys.1. Architektura i topografia układu procesora kryptograficznego MCY74C609

Zastosowanie (w tym informacja o wdrożeniu)

Układ procesora kryptograficznego opracowano przy współpracy z zewnętrzną firmą sprzętową Techlab2000, która zdefiniowała specyfikację systemową układu oraz odpowiedzialna była za opracowanie docelowej aplikacji układu w postaci karty

rozszerzeniowej PC w standardzie ISA/PCI wraz z oprogramowaniem. Całość prac wykonano w ramach projektu celowego KBN, którego głównym wykonawcą i właścicielem aplikacji docelowej było ITE. Produkcję małoseryjną układu MCY74C609 uruchomiono w firmie AMS za pośrednictwem organizacji EUROPRACTICE.

Produkcję seryjną karty szyfratora dysków uruchomiono w firmie COMP S.A. na zasadzie sprzedaży licencji. Procesor MCY74C609 zastosowany został także w innych urządzeniach kryptograficznych firmy COMP S.A z rodziny *CompCrypt*.



Rys.2. Aplikacja procesora MCY74C609 - karta ISA do szyfrowania danych na dysku stałym komputera PC

Znaczenie naukowe, ekonomiczne i społeczne

Znaczenie omawianego osiągnięcia ma charakter ekonomiczny i społeczny. Powstałe w wyniku prowadzonych prac produkty końcowe w postaci urządzeń kryptograficznych (karta szyfratora dysków komputerów PC i inne) przyczyniły się do wzrostu poziomu ochrony danych w przedsiębiorstwach oraz instytucjach administracji publicznej.

Źródła finansowania

Prace nad układem procesora kryptograficznego oraz karty szyfratora dysków finansowane były w ramach projektu celowego KBN oraz ze środków własnych ITE..

Twórcy osiągnięcia:

ITE : projekt układu scalonego: Jerzy Wąsowski, Janusz Kaczmarczyk
Techlab2000: projekt karty szyfratora: Tomasz Borkowski, Wiktor Kunczewicz