Bezpieczeństwo oprogramowania - lab 10

Zadanie 1

Koncepcja bitslicing polega na przedstawieniu funkcji w postaci operacji na pojedynczych bitach, tak, jakby implementowało się bramkę logiczną. Te operacje są następnie równolegle przenoszone na wiele instancji tej funkcji, korzystając z operacji bitowych w procesorze. Implementacja bitslicing zakłada użycie przykładowo ośmiu zmiennych (slice'ów) zamiast pojedynczej zmiennej typu long. Pierwsza zmienna przechowuje pierwszy bit liczby, druga przechowuje drugi bit itd. Równoległość jest ograniczona jedynie przez długość rejestru architektury maszyny.
Kod jest bardzo liniowy, dzięki czemu uruchamia się bardzo dobrze na mocno obciążonych, nowoczesnych procesorach. Znacznie zmniejsza ryzyko zatrzymania wykonywania instrukcji (ponieważ istnieje bardzo mała szansa na błędne przewidzenie kolejnej gałęzi), a także posiada wiele możliwości na optymalną zmianę kolejności instrukcji dla efektywnego planowania dostępu do danych.
Z rejestrem długości n bitów, tak długo jak implementacja bistslicing nie jest n razy wolniesza dla uruchomienia pojedynczej instancji algorytmu kryptograficznego, uzyskuje się znaczny wzrost przepustowości, jednak to stanowi prawdę tylko dla architektur wspierających wielowątkowość. Algorytmy CTR i ECB zawsze zyskują na przepustowości, CBC i CFB tylko podczas deszyfrowania.