dr inż. Piotr Bora
WAT Warszawa

Sprzętowa selekcja funkcji boolowskich

Funkcje boolowskie w kryptografii wykorzystywane są w wielu miejscach. Najczęściej na ich bazie buduje się skrzynki podstawieniowe w algorytmach blokowych, funkcje sprzężeń w algorytmach strumieniowych. Problem poszukiwania przydatnych dla kryptografii funkcji boolowskich jest problemem czasochłonnym. Funkcje te muszą spełniać wiele kryteriów. Wśród nich są: nieliniowość, zrównoważenie, odpowiedni stopień algebraiczny, kryteria lawinowe, kryterium propagacji, odporność korelacyjna, dobry profil XOR, brak liniowych struktur, brak stałych punktów i inne. Przestrzeń poszukiwań takich funkcji jest ogromna. Dla funkcji posiadających n wejść i jedno wyjście pełna przestrzeń wszystkich funkcji wynosi 2^{2^n}. Pewnym punktem zaczepienia jest poszukiwanie funkcji typu bent. Funkcje te są maksymalnie nieliniowe, posiadają znany stopień algebraiczny. Na bazie tych funkcji można budować rozwiązania przydatne w kryptografii. Jednak przy rosnącej skali poszukiwań wraz ze wzrostem n, pomimo że ilość tych funkcji również wzrasta, to gęstość ich rozmieszczenia bardzo szybko maleje.

Najczęściej funkcje te generuje się losowo i sprawdza, czy spełniają założone wcześniej parametry. Przy $n = 8$ i więcej jest to czasochłonne i obarczone pewną wadą. Generacja takich losowych wektorów nie może być obciążona powtarzalnością, gdyż będziemy trafiać ciągle na te same funkcje. Inna metoda polega na budowaniu większych funkcji na bazie mniejszych.

W artykule przedstawiono budowę narzędzia znajdowania funkcji bent dla ilości wejść od 4 w górę. Funkcje te są maksymalnie nieliniowe, posiadają odpowiedni stopień algebraiczny, jednak nie są zrównoważone. Definiowane są dla n parzystego i ich nieliniowość wynosi

$$2^{n-1} - 2^{\frac{n}{2}-1},$$

natomiast waga Hamminga (ilość jedynek w zapisie funkcji) wynosi

$$2^{n-1} \pm 2^{\frac{n}{2}-1},$$

a stopień algebraiczny $n/2$.

Problem wyszukiwania takich funkcji jest złożony i wspomaganie z wykorzystaniem układów cyfrowych jest tu bardzo pomocne. Przedstawiono rozwiązanie poszukiwania takich funkcji w oparciu o struktury programowalne FPGA firmy ALTERA. Wskazano możliwości praktycznej realizacji rozwiązania do stopnia $n = 10$, dla implementacji w układach rodziny STRATIX IV. Jednak przy obecnie wdrażanych nowych rodzinach układów perspektywy implementacyjne mogą wzrosnąć do nawet $n = 14$. Skala jest tu bardzo duża, gdyż otrzymujemy tu wzrost z poziomu 2^{1024} do poziomu 2^{16384} możliwości. Wykorzystano w procesie generowania prototypów funkcji wymaganie, że stopień algebraiczny funkcji musi być zadany jak wyżej, w związku z tym przestrzeń poszukiwań zawężono do ok. 2/3 zakresu wartości wykładników, jednak przy tej skali problemu i tak jest on bardzo duży.