Michał Wroński
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Matematyki i Kryptologii

Analiza możliwości realizacji sprzętowej dodawania i podwojenia dywizora na krzywej hipereliptycznej nad ciałem $GF(2^n)$

Głównym celem pracy była optymalizacja (minimalizacja) liczby rejestrów niezbędnych do wykonania podstawowych działań na krzywych hipereliptycznych o genusie $g = 2$, co może mieć wpływ na usprawnienie tworzenia sprzętowych układów realizujących algorytmy oparte na krzywych hipereliptycznych.

Głównym zadaniem projektowym w niniejszej pracy było skonstruowanie potoku obliczeń i zaprojektowanie koprocesora w strukturze FPGA do obliczania dodawania i podwajania dywizora na krzywej hipereliptycznej w $GF(2^n)$. Zadanie niniejsze zostało wykonane dla współrzędnych rzutowych i afinicznych. Wynik obliczenia wykonany we współrzędnych rzutowych jest przekształcany na afiniczne.

Wykorzystane w pracy techniki realizacji sprzętowej koprocesora w postaci użycia szybkiego układu mnożącego, szybkiej inwersji oraz baz normalnych, zaowocowało uzyskaniem interesującego rozwiązania, niespotykanego dotąd w literaturze.

Uzyskane tu rozwiązanie może być podstawą do poszukiwania nowych, alternatywnych rozwiązań rozpatrywanego w pracy zagadnienia i otrzymania innych, być może równie ciekawych wyników.

W przyszłości możliwe jest rozwinięcie projektu, poprzez zaprogramowanie rzeczywistej struktury FPGA i wykorzystania tego układu w kryptografii.