Michał Wroński
Michał Kędzierski
WAT Warszawa

Realizacja koprocesora wspierającego kryptoanalizę problemów opartych na krzywych eliptycznych

Algorytmy krzywych eliptycznych są szeroko wykorzystywane we współczesnej kryptologii, w szczególności w algorytmach klucza publicznego i w schematach podpisu cyfrowego.

W niniejszej pracy podejmiemy się próby konstrukcji i realizacji w strukturach programowalnych koprocesora wspierającego kryptoanalizę algorytmów opartych na krzywych eliptycznych, wykorzystujących problem logarytmu dyskretnego na krzywych eliptycznych.

Główna idea realizacji koprocesora polega na zastosowaniu wielu podukładów zdolnych do obliczania krotności punktu, ale o stosunkowo niewielkiej złożoności w ten sposób, aby uzyskać jak najszybsze rozwiązanie.

Przedstawimy przypadek uproszczony, zakładając, że znamy l najbardziej znaczących bitów (spośród n) obliczanej krotności, wykorzystując metodę brutalnego ataku, a następnie przejdziemy w stronę uogólnienia i analizy przypadku, gdy trzeba przeszukać całą przestrzeń możliwych rozwiązań. Zastanowimy się nad wykorzystaniem różnych metod — od ataku brutalnego po metody Rho i Lambda Pollarda.