Jerzy Gawinecki, Piotr Bora, Mariusz Jurkiewicz, Tomasz Kijko
Wojskowa Akademia Techniczna, Wydział Cybernetyki
Instytut Matematyki i Kryptologii, Warszawa

Zastosowanie krzywych eliptycznych do konstrukcji bezpiecznych algorytmów i protokołów kryptograficznych

Obecnie w celu uzgodnienia kluczy kryptograficznych a także realizacji podpisu cyfrowego wykorzystywane są algorytmy klucza publicznego. Podstawą bezpieczeństwa tych algorytmów są problemy trudne obliczeniowo, takie jak faktoryzacja dużych liczb (algorytm RSA) albo wyznaczanie logarytmu dyskretnego (protokół Diffiego–Hellmana). Przykładem dziedziny wykorzystującej trudność znajdowania logarytmu dyskretnego jest grupa punktów krzywej eliptycznej zdefiniowana nad ciałem skończonym. Okazuje się, że nie każda grupa punktów zapewnia odpowiedni poziom bezpieczeństwa. W referacie przedstawimy metody doboru bezpiecznych krzywych eliptycznych mających zastosowanie w konstrukcji algorytmów kryptograficznych.

W referacie zaprezentujemy również sprzętową implementację koprocesora realizującego operacje na krzywych eliptycznych zrealizowaną w układach programowalnych. Wspomaganie sprzętowe obliczeń dla systemów klucza publicznego na krzywych eliptycznych musi być rozpatrywane w trzech warstwach:

- wykonywanie operacji elementarnych w ciele,
- metody reprezentacji punktu, a co za tym idzie, potok obliczeń dla podwajania i dodania punktów na krzywej eliptycznej,
- metody realizacji krotności punktu na krzywej eliptycznej.

Generalnie najczęściej spotykanymi rozwiązaniami są systemy budowane na krzywych nad ciałami liczbowymi lub nad ciałami wielomianów o współczynnikach z ciała charakterystyki 2. Spośród operacji elementarnych w ciele najbardziej czaso- i elementochłonną jest mnożenie modularne. Zarówno w rozwiązaniu budowanym nad ciałem liczbowym, jak i nad ciałem wielomianów najmniej efektywnym jest rozwiązanie mnożenia modularnego tzw. podstawowe. Najczęściej przechodzi się w reprezentacji czynników działania na postać czy to residuów, czy baz normalnych. W przypadku metod reprezentacji punktu na krzywej również odchodzi się od reprezentacji bezpośredniej — afinicznej, na rzecz reprezentacji ogónie nazywanych rzutowymi. Unikamy tu częstego liczenia inwersji elementu w ciele, zostawiając ją na koniec obliczeń liczenia krotności celem korekcji wyniku do reprezentacji we współrzędnych afinicznych.

Ostatnią grupą zagadnień są metody liczenia krotności punktu. Podstawowym rozwiązaniem jest metoda binarna, jednak często przechodzi się na metodę dodawań-odejmowań, okien w-szerokich, m-arną, „drabiny Montgomery'ego", metodę z dzieleniem punktu lub innych.

Dobre zestawienie operacji we wszystkich trzech warstwach obliczeń umożliwia nam uzyskanie rozwiązania sprzętowego modułu wyznaczania krotności punktu o stosunkowo małych wymaganiach sprzętowych i szybkim wyznaczaniu wyniku.