dr inż. Piotr Bora
mgr inż. Tomasz Kijko
mgr inż. Łukasz Dzieł
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Matematyki i Kryptologii

Koprocesor klucza publicznego dla ciała $GF(p)$

Systemy klucza publicznego są szeroko stosowanymi rozwiązaniami w kryptografii współczesnej. Są wykorzystywane szczególnie w procesie negocjacji kluczy sesji oraz podczas składania podpisu elektronicznego.

Współcześnie projektowane i wdrażane rozwiązania w tej dziedzinie powinny opierać się na rozwiązaniach bazujących na teorii krzywych eliptycznych. Wynika to z tego, że długości kluczy są o rząd wielkości mniejsze oraz bezpieczeństwo takich rozwiązań jest większe. Jest to oczywiście możliwe tylko pod warunkiem zachowania odpowiednich wymagań dla parametrów krzywych eliptycznych i właściwego doboru punktów na krzywej. Podstawowym problemem, na którym opiera się bezpieczeństwo większości współczesnych algorytmów kryptograficznych opartych o teorię krzywych eliptycznych, jest problem wyznaczenia logarytmu dyskretnego na krzywej eliptycznej. Głównym elementem obliczeń w systemie kryptograficznym tego typu jest wyznaczenie krotności punktu na krzywej eliptycznej. Formalnie jest to obliczenie

$$Q = n * P,$$

gdzie $*$ jest rozumiane jako n-krotne dodanie punktu P do siebie.

Problemem trudnym obliczeniowo jest wyznaczenie krotności n, gdy mamy dane punkt bazowy P i jego n-tą krotność Q.

W referacie przedstawiono zagadnienia związane z konstrukcją bezpiecznej krzywej eliptycznej, bezpiecznego punktu na krzywej oraz algorytmów i efektywności wyznaczania krotności punktu na krzywej dla elementów z ciała liczbowego.