mgr inż. Marek Grądzki
Wojskowa Akademia Techniczna, Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Rozkład złożoności baz normalnych w ciałach charakterystyki 2

Protokoły asymetryczne pozwalają na bezpieczną wymianę klucza, nawet jeśli komunikacja między stronami może być podsłuchiwana i modyfikowana przez atakującego. Ich bezpieczeństwo opiera się na problemach trudnych obliczeniowo. Do podstawowych problemów tego typu należy problem logarytmu dyskretnego w grupie skończonej.

Podstawową wadą systemów asymetrycznych jest znacznie wolniejszy czas działania w porównaniu z szyframi symetrycznymi. W przypadku problemu logarytmu dyskretnego, najlepsze efekty implementacji zarówno programowych jak i sprzętowych otrzymuje się wykorzystując ciała skończone o charakterystyce 2.

Ciało skończone $GF(2^n)$ jest przestrzenią liniową nad podciałem $GF(2)$. Elementy tego ciała dają się wiec przedstawić jako kombinacje liniowe elementów bazy o współczynnikach z $GF(2)$. Baza ta może być postaci $\{1, \alpha, \ldots, \alpha^{n-1}\}$, gdzie $\alpha \in GF(2^n)$ (baza wielomianowa). Dużo efektywniejsze (jak i tańsze — w przypadku sprzętowym) implementacje można uzyskać wykorzystując tzw. bazy normalne postaci $\{\beta, \beta^2, \ldots, \beta^{2^{n-1}}\}$, gdzie $\beta \in GF(2^n)$.

Operacja podniesienia do kwadratu elementu ciała w bazie normalnej jest cyklicznym przesunięciem — zwiększa to znacznie efektywność szyfrów asymetrycznych. Mnożenie dwóch elementów ciała $GF(2^n)$ a i b przedstawionych w bazie normalnej realizuje się z wykorzystaniem pewnej macierzy T, zależnej od wybranej bazy. Mnożenie jest najefektywniejsze, jeśli liczba niezerowych elementów w macierzy T jest minimalna. Bazy, dla których macierz T posiada tę własność, nazywamy optymalnymi. Niestety nie dla wszystkich stopni n takie bazy istnieją. Również nie dla wszystkich n potrafimy efektywnie wyznaczać bazy o minimalnej lub wystarczająco małej złożoności.

Interesującym zagadnieniem jest wyznaczenie rozkładu złożoności baz normalnych. Znajomość rozkładu pozwoliłaby na określenie prawdopodobieństwa wylosowania elementu normalnego o pożądanej złożoności. W pracy [1], na podstawie analizy wszystkich elementów normalnych dla $n = 2 \ldots 39$, postawiono hipotezę, że rozkład ten jest normalny. W referacie pokażemy jak przyspieszyć wyznaczanie rozkładu. Odniesiemy się również do wspomnianej hipotezy, analizując złożoności wszystkich elementów normalnych dla $n = 2 \ldots 47$.

Bibliografia

[1] Masuda et al., *Low Complexity Normal Elements over Finite Fields of Characteristic Two*, IEEE Transactions on Computers, 2008.

[2] Jerzy Gawinecki, Janusz Szmidt, *Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii*, Wojskowa Akademia Techniczna, Warszawa 1999.