Michał Wroński
WAT Warszawa

Zastosowanie ciał rozszerzonych w celu przyspieszenia obliczeń na krzywych eliptycznych

Krzywe eliptyczne są jednym z podstawowych narzędzi wykorzystywanym we współczesnej kryptografii, przede wszystkim w protokołach podpisu cyfrowego. Poza oczywistymi zaletami, takimi jak odporność na podwykładnicze ataki na logarytm dyskretny, posiadają także pewne wady, z których największą wydaje się być złożoność (a tym samym czasochłonność) obliczania na nich krotności punktu na krzywej eliptycznej, dlatego też podejmowanych jest wiele prób przyspieszenia tego działania. W tym zakresie spotyka się dwa zasadnicze (niewykluczające się) podejścia. Pierwsze dotyczy optymalizacji samej metody obliczania krotności, tak aby zostało wykonanych jak najmniej podwojeń i dodawań punktów na krzywej eliptycznej. Drugie podejście dotyczy natomiast zminimalizowania liczby kroków niezbędnych do wykonania poszczególnych operacji. W tym celu najczęściej wykorzystuje się różne sposoby zapisu punktu na krzywej eliptycznej.

W roku 2007 pojawiła się nowa reprezentacja krzywych eliptycznych, znanych obecnie jako krzywe Edwardsa, a później również ich uogólnienie – skręcone krzywe Edwardsa. Pionierami w tej dziedzinie (oprócz Harolda Edwardsa) są przede wszystkim Daniel Bernstein i Tanja Lange. Większość literatury dotyczącej zastosowań krzywych Edwardsa i skręconych krzywych Edwardsa jest ich autorstwa.

Krzywe Edwardsa i skręcone krzywe Edwardsa posiadają dwie bardzo ważne zalety w porównaniu do krzywych eliptycznych w postaci Weierstrassa. Dodawanie i podwojenie punktu jest mniej czasochłonne oraz podwojenie punktu można wykonać jako dodawanie tych samych punktów, co uprzednio nie było możliwe. Jest to o tyle ważne, że znacznie utrudnia możliwość wyznaczania krotności punktu poprzez analizę charakterystyk poboru mocy. Minusem reprezentacji krzywej eliptycznej w postaci Edwardsa (skręconej Edwardsa) jest to, że nie dla każdej krzywej eliptycznej zapisanej w formie Wierestrassa można znaleźć krzywą Edwardsa (skręconą Edwardsa), która byłaby do niej izomorficzna. Dostępne są opracowania poruszające problematykę obliczenia krotności punktu na izogenicznej skręconej krzywej Edwardsa, ale w ciele rozszerzonym.

W niniejszym opracowaniu przedstawimy ideę przechodzenia z dowolnej krzywej eliptycznej w skróconej formie Weierstrassa w ciele $GF(p)$ na skręconą krzywą Edwardsa w ciele $GF(p^3)$ oraz przedstawimy efektywny sposób implementacji układu mnożącego w tym ciele, dzięki czemu łączna efektywność obliczeniowa wyznaczania krotności punktu na krzywej eliptycznej znacznie wzrasta.