Tomasz Kijko, Krzysztof Mańk, Michał Wroński
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Matematyki i Kryptologii

Analiza czasu faktoryzacji dużych liczb w zależności od liczby czynników pierwszych

Na problemie faktoryzacji opartych jest wiele algorytmów klucza publicznego. Autorzy wielu spośród nich określają bezpieczeństwo swoich rozwiązań w odniesieniu do algorytmu GNFS, który jest najszybszym algorytmem faktoryzacji dużych liczb (ponad 200-cyfrowych). Jednak często nie biorą oni pod uwagę pewnej własności: asymptotyczna złożoność czasowa algorytmu GNFS zależy tylko od wielkości faktoryzowanej liczby. Powstaje w związku z tym pytanie: jaki algorytm będzie najszybszy, jeżeli faktoryzowana liczba jest duża i ma więcej niż dwa czynniki pierwsze?

Odpowiedź na to pytanie nie jest jednoznaczna. Istnieją algorytmy wrażliwe na najmniejsze czynniki pierwsze faktoryzowanej liczby. Jednym z takich algorytmów jest Metoda Krzywych Eliptycznych (ECM).

W niniejszej pracy przedstawiliśmy uzyskane oszacowania czasu działania algorytmu GNFS w zależności od długości liczby oraz algorytmu ECM w zależności od długości liczby i długości czynników pierwszych. Na tej podstawie określiliśmy, jakiego rodzaju moduły są w danym przypadku bezpieczniejsze i oszacowaliśmy długości liczb i wielkość ich czynników, dla których faktoryzacja obydwoma algorytmami daje taki sam czas oczekiwany.

Próby tego rodzaju były już podejmowane w przeszłości (głównie po pojawieniu się algorytmu MultiPrime RSA), jednak w naszej opinii wyniki zawarte w opracowaniach dotyczących tych prób są dalekie od rzeczywistych. Jest to przede wszystkim wynik złego doboru funkcji aproksymujących i brak odniesienia do rzeczywistych wyników, a jedynie do heurystycznych oszacowań.

Na potrzeby niniejszego opracowania wykonaliśmy wiele serii badań dla algorytmu ECM. Dla algorytmu GNFS zostały wykorzystane rzeczywiste wyniki faktoryzacji dużych liczb pierwszych, wykonanych na potrzeby konkursu RSA Challenge.