УДК 681.322:621.391

АНАЛІЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ МАТЕМАТИЧНОГО АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ

Ратнюк К.В
Наукові керівники - доц., к.т.н. Яремчук Ю.Є., Черняхович К.В.

Вихідні дані генераторів випадкових та псевдовипадкових послідовностей сьогодні, використовуються в багатьох криптографічних застосуваннях, наприклад, при генерації ключів та загальносистемних параметрів.

У загальному випадку для побудови генераторів псевдовипадкових послідовностей використовується однобічна функція. Для побудови таких однобічних функцій використовуються функції, складність яких ґрунтується на складності дискретного логарифмування або на складності факторизації великого числа.

У криптографічних системах на основі математичного апарату еліптичних кривих в якості однобічної функції використовується дискретне логарифмування в групі точок еліптичних кривих.

На сьогодні одними з кращих генераторів псевдовипадкових послідовностей є генератор ANSI X9.17. Але зважаючи на досить широке поширення теорії еліптичних кривих, почали розроблятись і поширюватись генератори псевдовипадкових послідовностей на основі математичного апарату еліптичних кривих, які по останнім оцінкам є перспективними для криптографічних застосувань так як здатні забезпечити високу криптостійкість; хороші статистичні властивості; достатньо високу швидкість.

Проведений аналіз генераторів псевдовипадкових послідовностей на основі математичного апарату еліптичних кривих, який показав, що швидкість функціонування генераторів псевдовипадкових послідовностей залежить від обраного методу і способу формування псевдовипадкових послідовностей. При цьому, мінімальна складність досягається для алгоритмів, які побудовані за формулою вигляду $Z_i = Z_{i-1} + P$, де $Z_i, Z_{i-1} \in E$, $E: y^2 + xy = x^3 + ax^2 + b$. Але незважаючи на це, такі генератори залишаються повільними у порівнянні із відомими.

Також, аналіз показав, що координати точки еліптичної кривої утворюють кореляційну функцію, що відповідає рівнянню еліптичної кривої, що в свою чергу може призвести до кореляції значень псевдовипадкової послідовності. При цьому, декореляцію можна здійснити за допомогою обчислення значень геш-функції від поточного числа $z_i = x_i$, де $Z_i(x_i, y_i) \in E$.

Таким чином, застосування генераторів псевдовипадкових послідовностей на основі математичного апарату еліптичних кривих в криптографічних методах захисту інформації на сьогодні є актуальними але по ряду причин такі генератори потребують додаткових досліджень.