УДК 681.3.06
Скоморохов А. – ст. гр. КСМс-52
Тернопільська академія народного господарства

ВИКОРИСТАННЯ СИМВОЛУ ЯКОБІ ДЛЯ ГЕНЕРУВАННЯ ПАРАМЕТРІВ ТА БАЗОВИХ ТОЧОК НА ЕЛІПТИЧНІЙ КРИВІЙ

Науковий керівник: аспірант Якименко І.З.

Широке використання інформаційних технологій в комерційних та державних цілях зумовлює необхідність збільшувати ефективність систем інформаційної безпеки. Невід'ємним елементом таких систем є криптографія. Криптографія, яка використовує еліптичні криві (ЕК) є однією із найефективніших. Проте широкому використанню заважають труднощі в обчисленні на деяких кроках алгоритму.

Перелік ЕК, які можуть використовуватися був представлений в стандарті FIPS 186-2 . Стандартна специфікація IEEE P1363 [1] була заснована на наступному представленні гладкості кривої:

$$cb^2 (\text{mod } p) \equiv a^2 (\text{mod } p) \qquad (1)$$

Для вирішення задач генерації параметрів ЕС взято за методику алгоритм A.12.4. із стандарту IEEE P1363, а також статтю [2]. На основі цього програмно реалізовано алгоритм генерації параметрів, які базуються на використані символу Якобі (Jacobi Symbols) і квадратних залишків.

Взявши до уваги існуючий підхід з статті [2], автором запропоновано алгоритм з використанням символів Якобі для пошуку базових точок на ЕК. За основу взято алгоритм A.11.1. із стандарту IEEE P1363 [1]. На основі цього було вирішено рівняння (2) наступним чином:

$$\beta^2 \equiv \alpha (\text{mod } p) \qquad (2)$$

Вхід: простий p>3 і параметри *a, b* еліптичної кривої E за модулем p.

Вихід: точка (окрім *O*), що випадково генерується, на E.

1. Вибрати випадковий x з $0 \le x < p$;
2. Встановити $\alpha \leftarrow x^3 + ax + b \bmod p$;
3. Якщо $\alpha = 0$, тоді вихід (x, 0) і зупинка;
4. Функція SqrtExist:
   a. Обчислити $\left(\frac{\alpha}{\beta}\right)$;
   b. Якщо $\left(\frac{\alpha}{\beta}\right)=1$, тоді $\beta^2 \equiv \alpha (\text{mod } p)$;
   c. Інакше, якщо $\left(\frac{\alpha}{\beta}\right)\neq 1$, тоді з генерувати β ;
6. Згенерувати випадковий bit μ і встановити $y \leftarrow (-1)^{\mu} \beta$;
7. Вивести (x, y).

Кафедра БІТ ТАНГу провидить дослідження щодо покращення ефективності використання криптографії еліптичних кривих. Зокрема мною проводиться розробка програмних засобів та аналіз їх швидкодії.

Література

[1] IEEE P1363 – 1998 "Стандартна Специфікація для Криптографії Відкритого Ключа"

[2]Mykola Karpynskyy, Ihor Vasyltsov, Ihor Yakymenko, Andriy Honcharyk. Elliptic curve Parameters Generation.