УДК 519.1

Г.Л. Козіна, Г.І. Нікуліщев

Запорізький національний технічний університет, Запоріжжя

ЕЛІПТИЧНІ КРИВІ НАД СКІНЧЕНИМ ВЕКТОРНИМ ПОЛЕМ

Постановка задачі. В сучасній криптографії широко використовується математичний апарат еліптичних кривих. Алгоритми шифрування та електронного цифрового підпису (ЕЦП) будуються на основі операцій в групі точок еліптичної кривої. При цьому криптографічна стійкість подібних алгоритмів грунтується на складності завдання дискретного логарифмування в групі точок еліптичної кривої (ЕК). В державних стандартах Росії та України для забезпечення достатньої стійкості рекомендують використовувати числа порядку 2^{128}–2^{512} в якості параметрів кривої. При збільшенні розміру завдання збільшується і його ресурсомісткість. Одним зі шляхів зниження вимог до обчислювальних ресурсів є оптимізація групової операції на кривій. Авторами розглядається вирішення задачі шляхом визначення ЕК над скінченим векторним полем [1].

Векторні поля. Скінчене векторне поле (СВП) – одне з розширень скінченого поля Галуа GF(p). Елементами СВП є вектори кінцевої довжини n, представлені набором коефіцієнтів (a, b.. f) при відповідних базисних векторах e, i.. z. При цьому, коефіцієнти є елементами поля GF(p). Операція додавання двох векторів та множення на скаляр виконуються традиційно. Операція множення двох векторів ◦ визначається за принципом множення многочленів. Авторами розглядалося поле векторів довжиною 2, в якому операція множення базисних векторів визначається наступним співвідношенням

$$e \circ e = e;\ e \circ i = i \circ e = i;\ i \circ i = \tau \cdot e .$$

Множник τ належить полю GF(p) і обирається при формуванні СВП. Значення цих множників визначають порядок мультиплікативної групи поля. Одиничним елементом цієї групи є вектор з координатами (1, 0). Взаємно оберненими вважаються вектори, результатом операції множення над якими є одиничний вектор.

Еліптичні криві. При побудові ЕК над СВП координати точок є елементами СВП над GF(p), а в рівнянні, що задає ЕК, операція піднесення до степеня замінюється операцією множення в КВП. Якщо характеристика поля не дорівнює 2 або 3, то крива може бути задана у спрощеній формі з двома коефіцієнтами a і b[2]:

$$Y \circ Y = X \circ X \circ X + a \cdot X + b .$$

При виконанні операцій додавання і подвоєння точок ЕК зведення в ступінь також замінюється множенням.

Оцінка порядку групи точок ЕК над полем GF(p) визначається теоремою Хассе:

$$|\#E(p) - p - 1| < 2\sqrt{p} .$$

У випадку ЕК над СВП справедливо замінити величину p порядком мультиплікативної групи СВП. Таким чином, застосування СВП дозволяє за рахунок збільшення кількості нескладних арифметичних операцій домогтися збільшення порядку групи точок без збільшення порядку чисел.

Висновок. Застосування операцій в мультиплікативній групі СВП у криптографічних алгоритмах дозволяє домогтися зниження їхньої ресурсомісткості в порівнянні з використанням операцій в полі GF(p), що забезпечують ту ж саму крипостійкість. Авторами планується модифікація стандартів ЕЦП Росії та України з використанням СВП і оцінка продуктивності модифікованих алгоритмів. Для цього буде проведено дослідження векторних полів, побудованих на основі розширеного поля GF (2^m).

Список літератури

1. Nikolay A. Moldovyan. Acceleration of the Elliptic Cryptography with Vector Finite Fields // I.J. Network Security. – Trier: Universitat Trier, 2009. – № 9 (2). – С. 180-185.

2. Болотов А.А., Гашков С.Б. Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с.