УДК 004.9

Ю.А. Тарнавський, Київ
О.В. Канівець, Київ

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Abstract. The generation of stable elliptic curves is simulated. Based on the results of the simulation, we make conclusions about the effectiveness of different generation strategies and the distribution of the curves according to the stability levels.

Вступ

У сучасній криптографії для забезпечення високого рівня крипостійкості при невеликій довжині ключа використовуються алгебраїчні об‘єкти високої складності – еліптичні криві. Сьогодні засоби використання еліптичних кривих для криптографічного захисту інформації утворюють самостійний розділ еліптичної криптографії [1 – 2].

Основною перевагою еліптичної криптографії є те що на даний момент не відомо субекспоненціальних алгоритмів для вирішення задачі дискретного логарифмування у групах їх точок. При цьому порядок групи точок еліптичної кривої задає складність задачі, а для досягнення такого ж рівня безпеки, як і у RSA, потрібні групи менших порядків. Зокрема для захисту інформації найвищого рівня секретності в еліптичній криптографії виявляється достатнім використання 384-бітових ключів.

Основна частина

Асиметричні криптосистеми на еліптичних кривих є найбільш стійкими серед криптосистем з відкритим ключем [3, 4], оскільки для обчислення кратності точки еліптичної кривої не відомі такі ефективні алгоритми, як для обчислення дискретного логарифма в криптосистемах на базі модульного зведення в ступінь.

Ключовою умовою ефективного функціонування таких криптосистем є використання криптографічно стійких еліптичних кривих. Стійкою називається така еліптична крива, для якої задача дискретного логарифмування на еліптичній кривій є важкою. В [5] показано, що стосовно кращих з відомих на сьогоднішній день алгоритмів дискретного логарифмування на еліптичних кривих стійкою може вважатись еліптична крива над полем з $q = p^n$ елементів, $Q \in E(F_q)$ і $\#\langle Q \rangle = r$, яка має наступні властивості:

- r є великим простим числом, причому $r < 2^d$;
- $p^t \neq 1 (\mathrm{mod}\ r)$ для всіх цілих $t = 1,2,\ldots,B$, $B \geq m$;
- $r \neq p$.

Тут r – порядок циклічної групи точок еліптичної кривої, m і d – так називані параметри криптостійкості.

Значення параметрів криптостійкості визначаються відповідними стандартами шифрування. Одним з найбільш поширеним є стандарт ECSDA [6], прийнятий в США і Європі. Він, для прикладу, містить такі вимоги: $p>2^{160}$, d=254, m=31.

Таким чином отримання криптографічно стійкої еліптичної кривої зводиться до генерування еліптичної кривої з відомим порядком циклічної групи точок. Для досягнення цієї мети запропоновано два підходи [7]: випадковий вибір і детермінована генерація.

Стратегія випадкового вибору полягає у випадковому виборі еліптичної кривої F_q, обчисленні для неї кількості точок q і порядку групи r та перевірку на стійкість.

Стратегія детермінованої генерації полягає у використанні методу комплексного множення [8] для побудови еліптичної кривої з відомим r, стійкість якої може бути перевірена ще до отримання рівняння кривої.

Практичне застосування вказаних стратегій вимагає побудови програмної системи. Для її реалізації запропонована наступна структура (рис. 1).

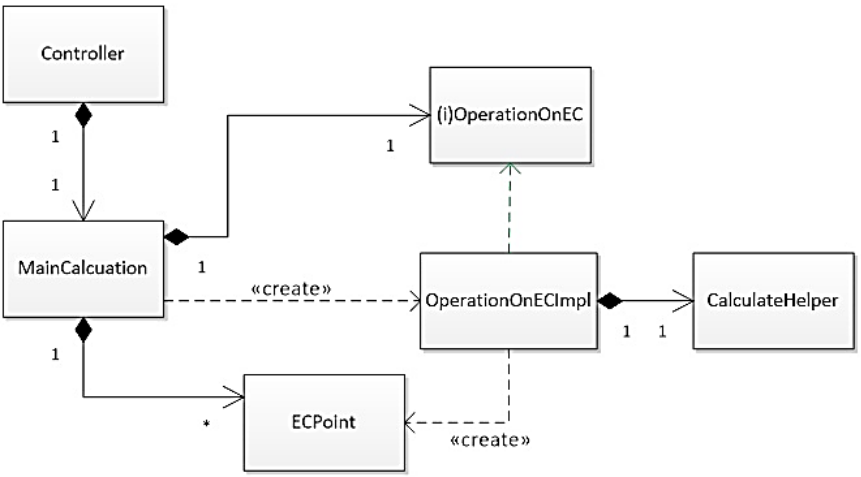

Рис. 1. Структура програмної системи

Модуль *Controller* забезпечує введення/виведення даних через графічний інтерфейс. Модуль *MainCalculation* реалізує основні обчислення, використовуючи при цьому операції над точками еліптичної кривої з модуля *OperationOnECImpl*. Взаємодія між модулями *MainCalculation* і *OperationOnECImpl* забезпечується через програмний інтерфейс *OperationOnEC*. Модуль ECPoint забезпечує роботу з окремими точками

еліптичної кривої, а модуль *CalculateHelper* – виконання різноманітних допоміжних операцій, необхідних для цього.

Прикладна система реалізована на платформі Java SE 8. Для тестування системи використовувався персональний комп'ютер з процесором Intel Core i7, тактовою частотою 2,2 ГГц і об'ємом оперативної пам'яті 16 Гб.

Графічний інтерфейс побудованої системи показаний на рис. 2.

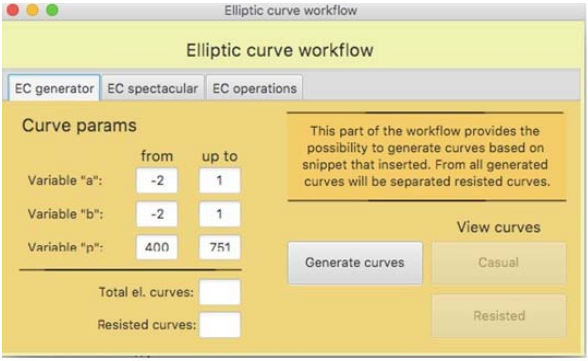

Рис. 2. Інтерфейс прикладної системи

На вкладці "*EC generator*" задається інтервал значень досліджуваних параметрів. Генерація відповідних стійких еліптичних кривих, а також визначення їх рівня стійкості за тривимірною шкалою відбувається після натиснення кнопки "Generate curves", а результат в табличному виді відображається на вкладці "*EC spectacular*". Вкладка "*EC operation*" є своєрідним калькулятором, який дозволяє за необхідності виконати операції над окремими точками еліптичної кривої (додавання, віднімання, подвоєння, множення).

Результати

В результаті моделювання процесу генерації стійких еліптичних кривих з'ясувалось, що стратегія випадкового вибору є значно менш ефективна, ніж стратегія детермінованої генерації. Для порівняння скажемо, що у випадку використання першої стратегії середній час знаходження стійкої кривої складав ~44 хвилини, тоді як для другої він складав ~2 секунди. Проте кожна з них забезпечує отримання позитивного результату. Незалежно від стратегії генерації кількість знайдених стійких еліптичних кривих з найвищим рівнем стійкості (індекс 3) складає ~8%, з середнім (індекс 2) ~25%, з низьким (індекс 1) ~67%.

Висновки

Генерація стійких еліптичних кривих є ресурсозатратним процесом, який вимагає часу і значних обчислювальних потужностей. Проте для його

моделювання в обмеженій області параметрів достатньо потужностей персонального комп'ютера. Моделювання дозволило визначити ефективність стратегій генерації стійких еліптичних кривих, а також отримати уявлення про їх кількісний розподіл за рівнями стійкості.

1. *Жданов О.Н.* Применение эллиптических кривых в криптографии / О.Н. Жданов, Т.А. Чалкин. – Красноярск: СибГАУ, 2011. – 65 с.
2. *Баричев С.Г.* Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия – Телеком, 2002. – С.123.
3. *Lencier R.* Finding good random elliptic curves for cryptosystems defined F2n / R. Lencier // Lecture Notes in Computer Science. – 1997. – Vol.1233. – P.379-392.
4. *Oorschot P.C.* Parallel collision search with cryptanalytic application / P.C. van Oorschot, M.J. Wiener // J. Cryptology. – 1999. – Vol.12. – P.1-28.
5. *Пылин В.В.* Параметры асимметричной криптосистемы на эллиптических кривых / В.В. Пылин // Информационные технологии в профессиональной деятельности и научной работе: сборник материалов региональной научно-практической конференции. – Йошкар-Ола: Марийский государственный технический университет, 2006. – С.90-92.
6. ANSI. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, ANSI X9.62, 1998.
7. *Пылин В.В.* Алгоритмы и методы генерации эллиптической кривой для асимметричной криптосистемы: дис. канд. техн. наук. Марийский. гос. техн. университет, Йошкар-Ола, 2008.
8. Atkin A.O. Elliptic curves and primality proving / A.O. Atkin, F. Morain // Mathematics of Computation. – 1993. – Vol. 61. – P.29-68

Поступила 27.08.2018р.

УДК 004.7

В.Ю. Зубок, Київ

РОЗПІЗНАВАННЯ АНОМАЛІЙ В ГЛОБАЛЬНІЙ ІНТЕРНЕТ-МАРШРУТИЗАЦІЇ ПРИ НЕЧІТКОМУ ОПИСІ ПОДІЙ

Abstract. As part of any network computing system, there are monitoring subsystems – the software which monitors the changes in the numerous network parameters, as well as the state and performance of the servers. It uses flexible alerting mechanisms, allowing the administrator to set up alerts via e-mail, sms, online messengers for virtually any event. Knowledge of the principles and mechanisms of implementing cyber attacks on global routing makes it possible to formulate criteria for changing the status of routing tables under the influence of cyber attacks. Multifactor analysis of the data obtained as a result of observing the changes in the routing tables makes it possible to detect harmful external influences in the absence of clear characteristics of such impact and without a prior description of the inherent

