НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМ. ІГОРЯ СІКОРСЬКОГО"

Забезпечення стійкості криптографічних алгоритмів на основі еліптичних кривих

Виконав:

Студент 6 курсу
групи ТМ-61м
Канівець О.В.

Керівник:

доц. к.ф.-м.н.
Тарнавський Ю.А.

Київ – 2018

Цілі та задачі

Метою дослідження є удосконалення способів забезпечення стійкості криптографічних алгоритмів на основі еліптичних кривих.

Для досягнення поставленої мети мають бути вирішені такі **задачі**:

- визначення методики для підвищення стійкості алгоритмів на основі еліптичних кривих;
- розробка програмних засобів для генерації стійких еліптичних кривих;
- дослідження та рекомендації щодо генерації стійких еліптичних кривих.

Об'єкт дослідження: Комп'ютерні технології криптографічного захисту.

Предмет дослідження: Комп'ютерні технології криптографічного захисту на основі еліптичних кривих.

Постановка задачі

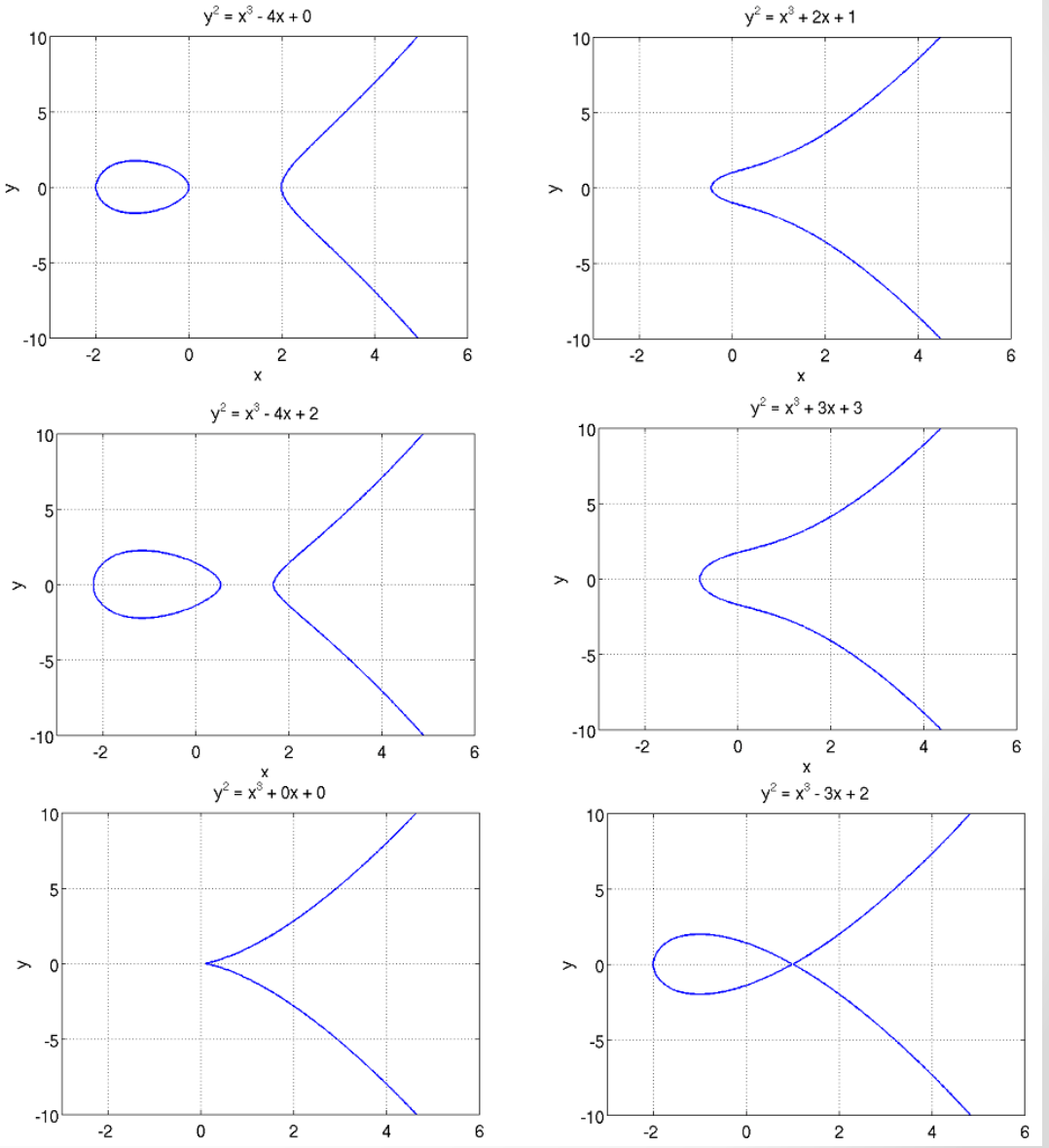
У сучасній криптографії з метою забезпечення високого рівня крипостійкості при невеликій довжині ключа використовуються алгебраїчні об'єкти високої складності – еліптичні криві. Постійне збільшення потужностей сучасних комп'ютерів робить необхідним постійне підвищення крипостійкості вже існуючих алгоритмів. Тому було поставлено задачу розробки методів забезпечення стійкості криптографічних алгоритмів на основі еліптичних кривих або удосконалення вже існуючих.

Еліптична крива

Це крива задана формулою:

$$y^2 = x^3 + ax + b$$

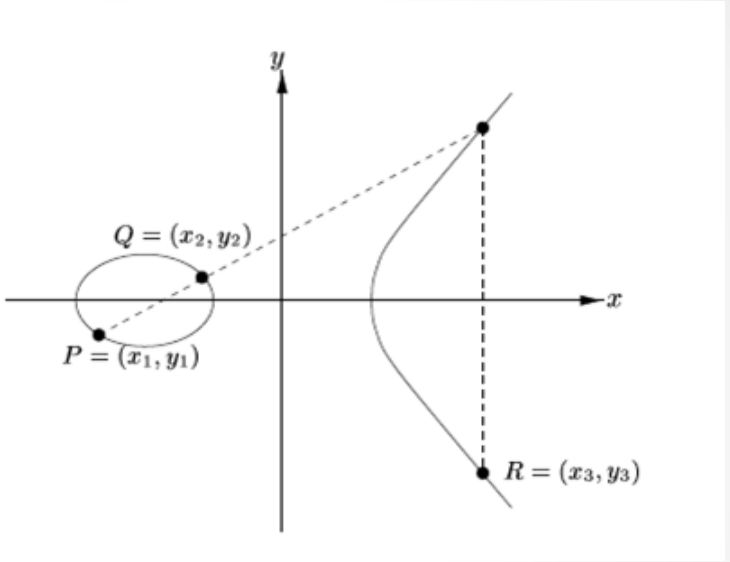
Еліптичні криві зображені на перших чотирьох малюнках називаються гладкими, а останні 2 відносяться до так званих сингулярних кривих.

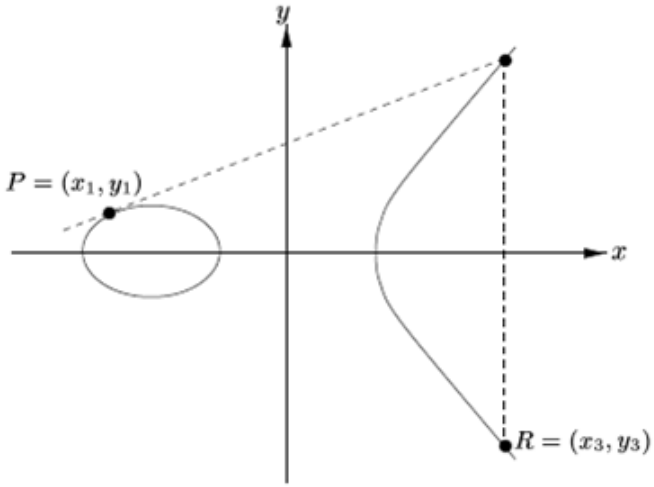


Операції над точками еліптичної кривої

Базові операції над точками кривої:

- Додавання 2х точок;
- Подвоєння точки;





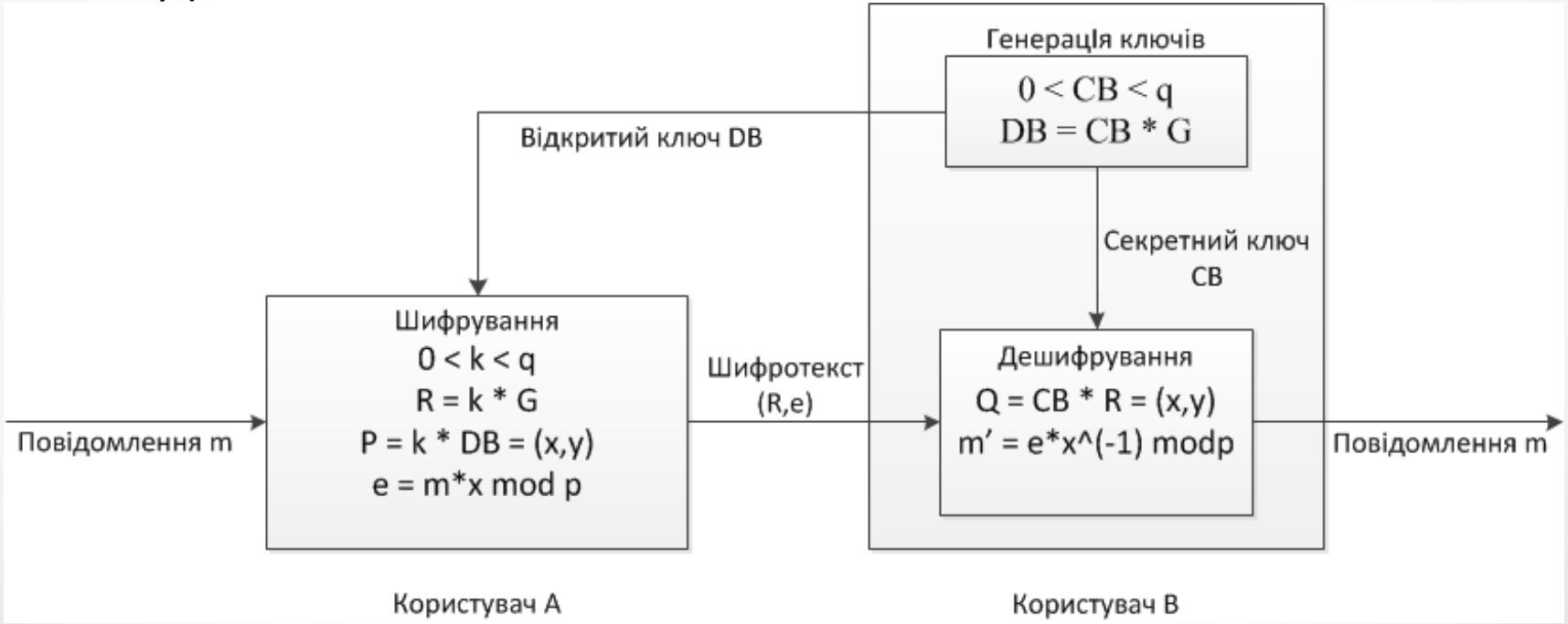
Перехід від числа до точки

Будь-яку систему, яка базується на дискретному логарифмуванні, легко можна перенести на еліптичні криві.

$$y = g^x \bmod p \rightarrow Y = [x]G \bmod p$$

Схема Ель-Гамаля

Даний метод асиметричного шифрування при переносі на еліптичні криві має наступний вигляд:



m' = m

Стійка еліптична крива

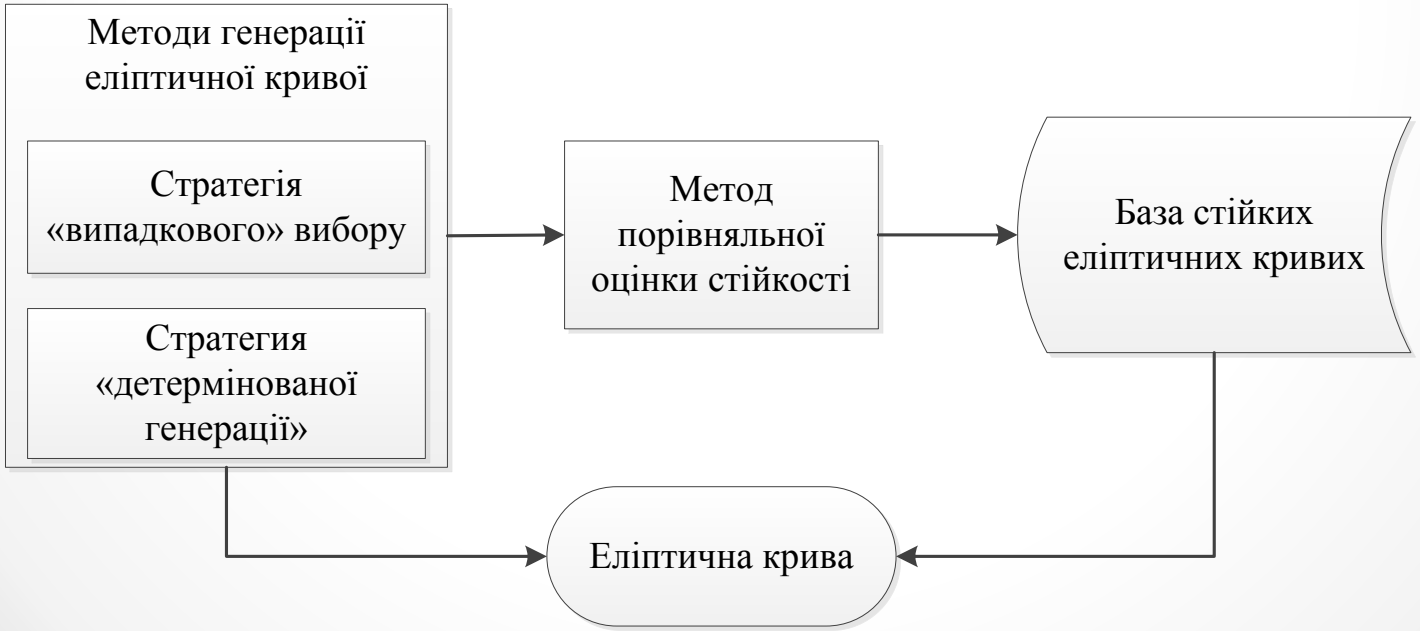
Стійка еліптична крива – це еліптична крива яка задовольняє наступним умовам:

- $r \geq 2^d$ або r є простим числом;
- для усіх $t = 1,2, \dots, m$ не виконується $p^t = 1(mod\ r)$;
- $r \neq p$.

Використання цих кривих у асиметричних алгоритмах шифрування збільшує криптографічну стійкість усього алгоритму в цілому.

Алгоритми генерації стійких еліптичних кривих

- Стратегія «випадкового» вибору;
- Стратегія детермінованої генерації.



Стратегія «випадкового» вибору

Полягає у випадковому виборі кривої над полем F_q (саме випадковим є визначення коефіцієнтів кривої a та b). Для цієї кривої обчислюється кількість її точок і порядок циклічної групи точок за допомогою алгоритму обчислення порядку групи точок. Далі, знаючи всі параметри, можна здійснити перевірку на крипостійкість.

Особливості:

- Середній час генерації становить понад 40 хвилин.
- Для досягнення найбільшого ступеня безпеки при використанні криптосистем на еліптичних кривих віддають перевагу кривим, що згенеровано на основі цієї стратегії, через те що ці криві не мають такої особливості як комплексне множення точок. Це може послабити крипостійкість.

Стратегія детермінованої генерації

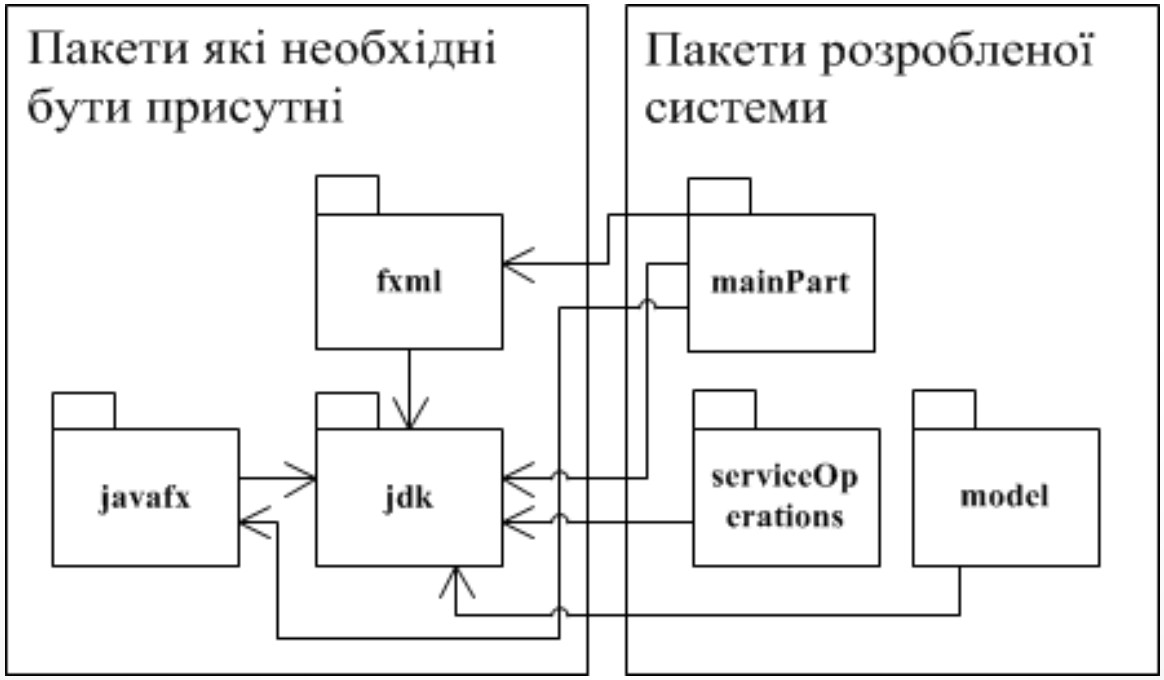
Полягає в використанні методу комплексного множення для побудови кривої з відомим r - порядком циклічної групи точок. Тобто спочатку обчислюється число r, і для нього будується крива, і в загальному випадку для обчисленого r може бути побудовано декілька еліптичних кривих. Причому на відміну від попередньої стратегії вже після етапу обчислення r (тобто ще не знаючи рівняння кривої) можна протестувати криву на крипостійкість.

Особливості:

- Характерна велика швидкість генерації кривих, близько 1-2 секунд для криптографічно стійкої кривої;
- Мають меншу крипостійкість через комплексне множення

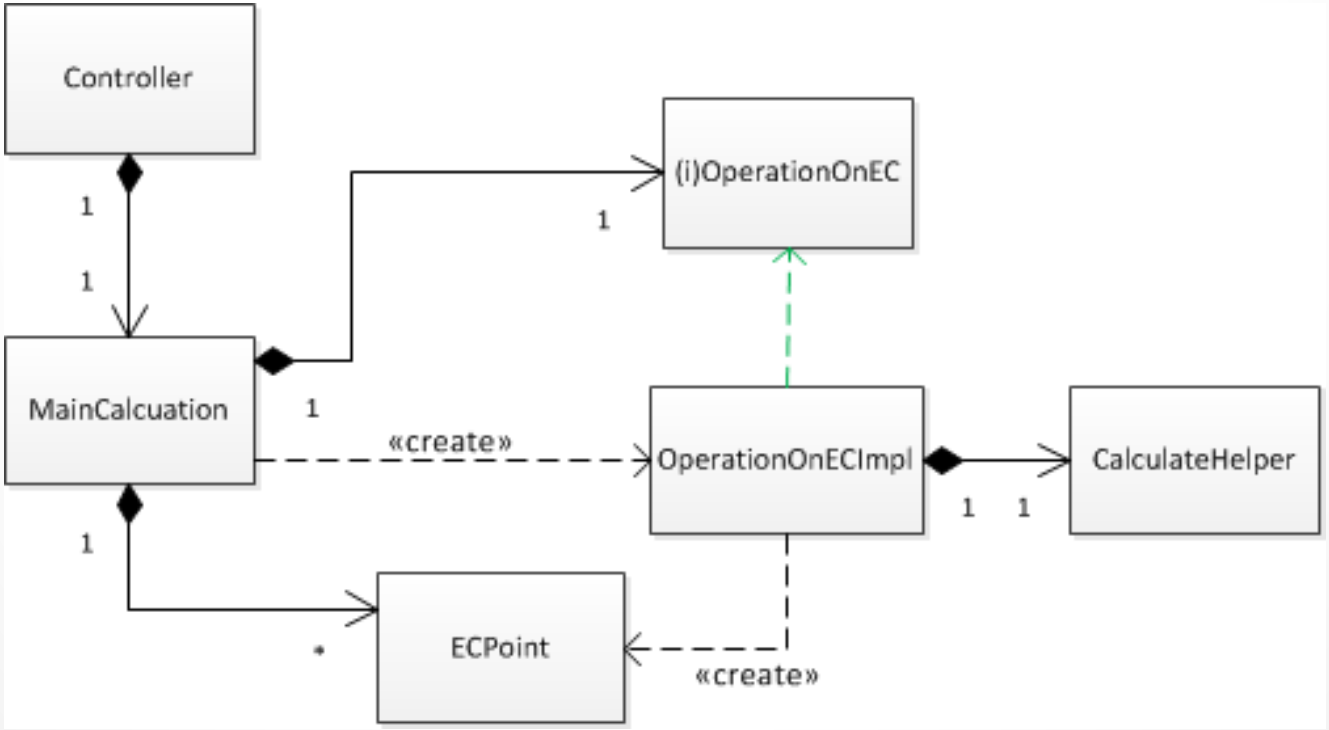
Діаграма пакетів

На діаграмі показані пакети які необхідні бути присутні у середі розробки, а також пакети самої розробленої системи.

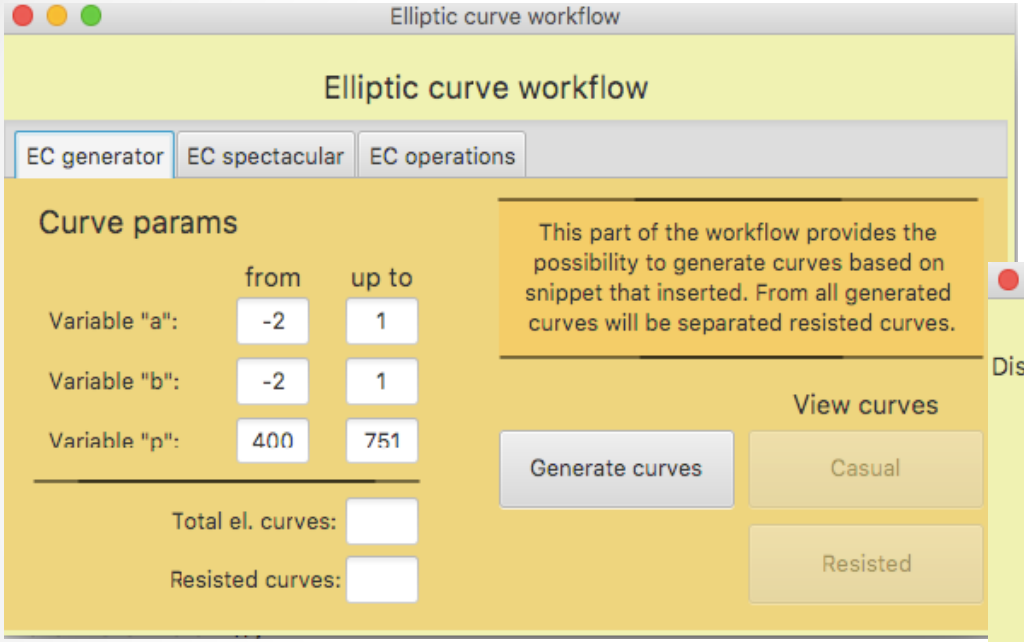


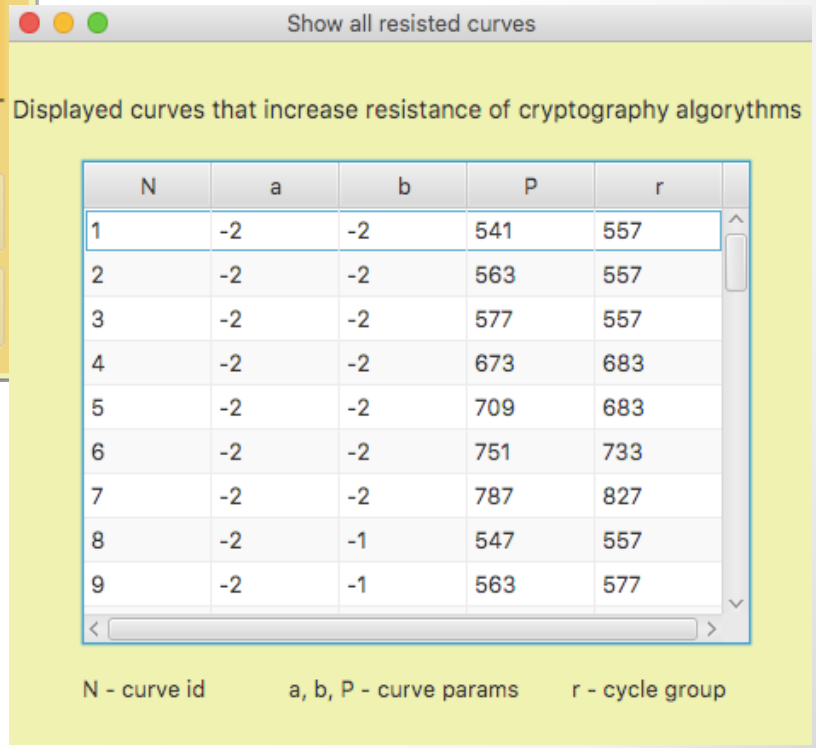
Ієрархія класів розробленої системи

На рисунку показано ієрархію класів розробленої системи.



Приклад генерації стійких еліптичних кривих



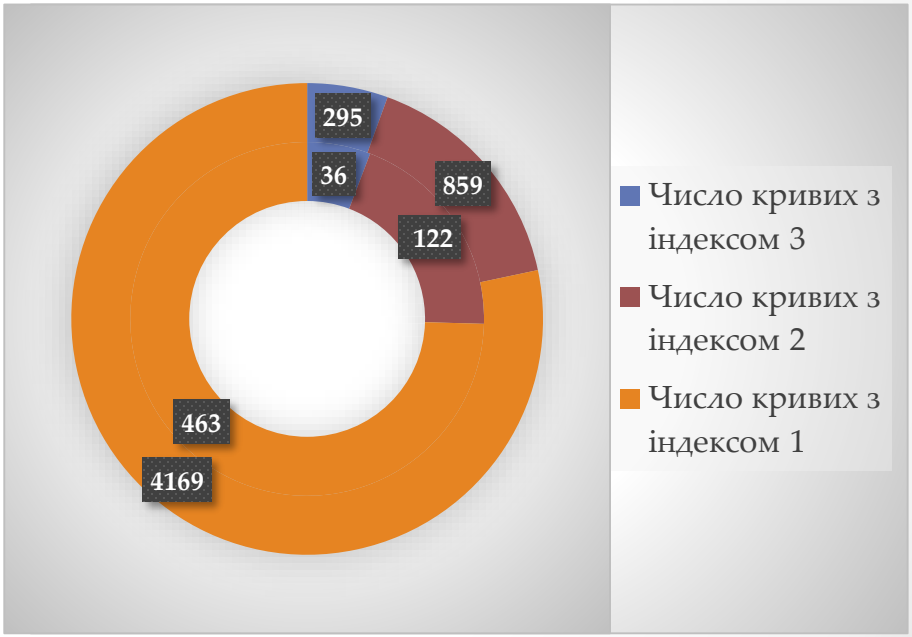


N	a	b	P	r
1	-2	-2	541	557
2	-2	-2	563	557
3	-2	-2	577	557
4	-2	-2	673	683
5	-2	-2	709	683
6	-2	-2	751	733
7	-2	-2	787	827
8	-2	-1	547	557
9	-2	-1	563	577

Результати дослідження на основі розробленої програмної системи

Порівняльне співвідношення кривих при розподілі за криптографічної стійкістю.

Внутрішнє коло – генерація за стратегією випадкового вибору. Зовнішнє – за стратегією детермінованої генерації.



Рекомендації до обрання методу генерації стійких еліптичних кривих

Для стратегії «детермінованої генерації» характерна велика швидкість генерації кривих, близько 1-2 секунд для криптографічно стійкої кривої. При цьому, кількість таких кривих більша, ніж кількість криптографічно стійких, які можна отримати за допомогою стратегії «випадкового вибору», для отриманих за допомогою стратегії «випадкового вибору», середній час генерації становить понад 40 хвилин. Особливістю кривих, отриманих за допомогою стратегії «детермінованою генерації» є той факт, що вони мають «спеціальну» властивість, а саме комплексне множення, яке теоретично може послабити їх криптографічну стійкість. У зв'язку з цим для досягнення найбільшого ступеня безпеки при використанні криптосистем на еліптичних кривих віддають перевагу кривим, що згенеровано на основі стратегії «випадкового вибору».

Висновки

Було досліджено методи генерації еліптичних кривих, а також вироблено певні рекомендації щодо їх застосування. Дослідження було проведено на основі програмної системи, що розроблена для генерації та наступного використання стійких еліптичних кривих. Після генерації кривої розроблена програмна система дає можливість шифрування на основі використання методів еліптичної криптографії, а також виконання арифметичних операцій над точками еліптичних кривих.

Дякую за увагу!