Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»

Інструментальні засоби реалізації вітчизняного стандарту цифрового підпису на основі еліптичних кривих

Виконав: студент гр.ТВ-61с Коваль П. І.

Науковий керівник: к.ф.м.н. Тарнавський Ю. А.

Актуальність

На сьогоднішній день ЕЦП широко використовується юридичними та фізичними особами, активно впроваджується в державних установах і органах державної влади. Відповідно до наказу мін'юст України 29.03.2017 № 1017/5/206 до державного стандарту ДСТУ 4145 було внесено зміни, та прийнято новий стандарт створення групового ЕЦП, який базується на ДСТУ 4145, проте даний стандарт на сьогоднішній день немає програмних реалізацій, які давали б змогу легко інтегрувати цифровий підпис в існуючі системи, не залежно від платформи і в майбутньому розвивати та підтримувати криптопровайдер в актуальному стані.

Мета і завдання

Мета: Створення криптопровайдера з функціями генерації та перевірки цифрового підпису згідно стандарту ДСТУ4145, який надавав би можливість легкої інтеграції з існуючими системами.

Завдання:

- реалізація операції на еліптичних кривих необхідні для виконання математичних операцій згідно стандарту;
- аналіз існуючих програмних реалізацій;
- реалізація всіх необхідних пунктів стандарту ДСТУ-4145 для забезпечення повноцінного створення та верифікації цифрового підпису;

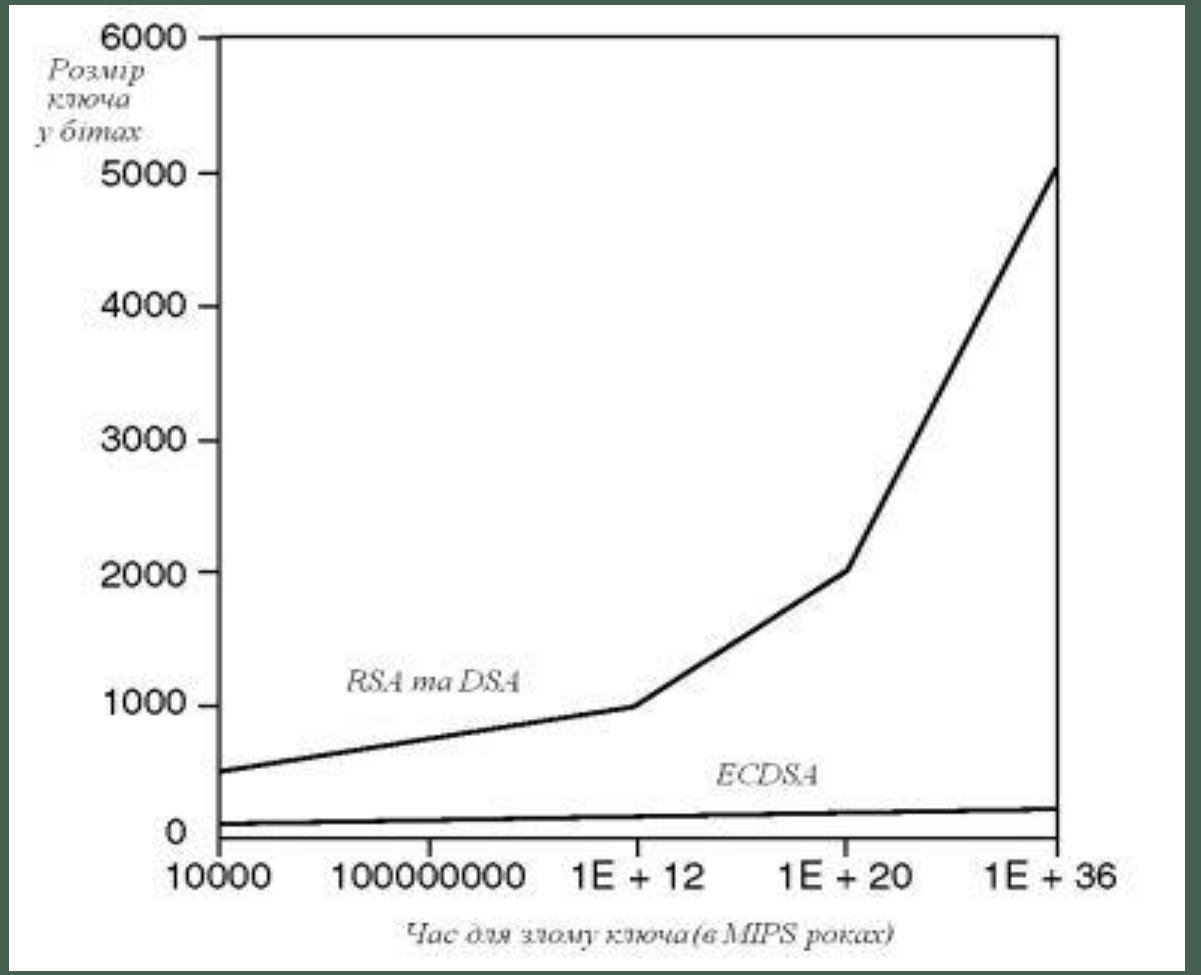
Цифровий підпис- – це блок даних невеликого розміру, одержаний в результаті криптографічного перетворення повідомлення довільної довжини з використанням особистого (таємного) ключа відправника.

Загальна схема створення та верифікації цифрового підпису

Порівняння алгоритму на еліптичних кривих та інших асиметричних алгоритмів

Ознака порівняння	Алгоритм ЕЦП		
	RSA	DSA	ECDSA
Проблема що лежить в основі алгоритму	ПФЧ	ПДЛ	ПДЛЕК
Розмір системних параметрів в бітах	1024	2208	481
Розмір отриманого підпису в бітах	1024	320	320
Розмір відкритого ключа в бітах	1088	1024	161
Розмір закритого ключа в бітах	2048	160	160

	Створення підпису	Перевірка підпису
RSA(1024 bit)	25мс	<2мс
ECDSA(160 bit)	32мс	33мс
RSA(2048 bit)	120мс	5мс
ECDSA(216 bit)	68мс	70мс



Порівняння алгоритму на еліптичних кривих та інших асиметричних алгоритмів

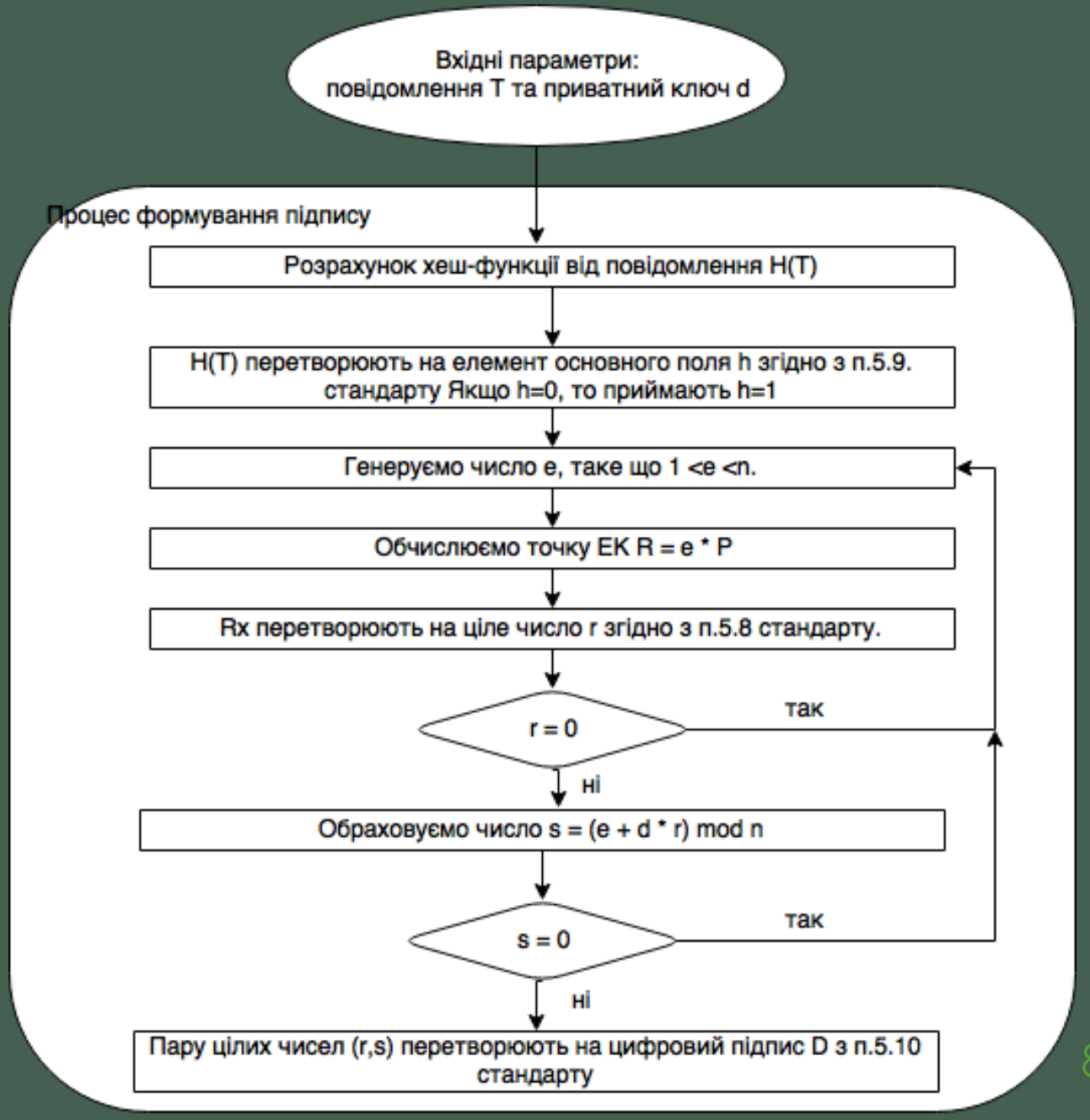
При збільшенні розмірів ключа створення підписів за допомогою ECDSA відбувається значно швидше, ніж в аналогічних RSA системах. Ця різниця в ще більшому ступені проявляється для однопроцесорних систем. З іншого боку перевірка підпису за допомогою ECDSA відбувається набагато повільніше, ніж ця ж процедура в системах RSA і ця різниця посилюється для систем з одним процесором.

Загальні парметри алгоритму ДСТУ 4145

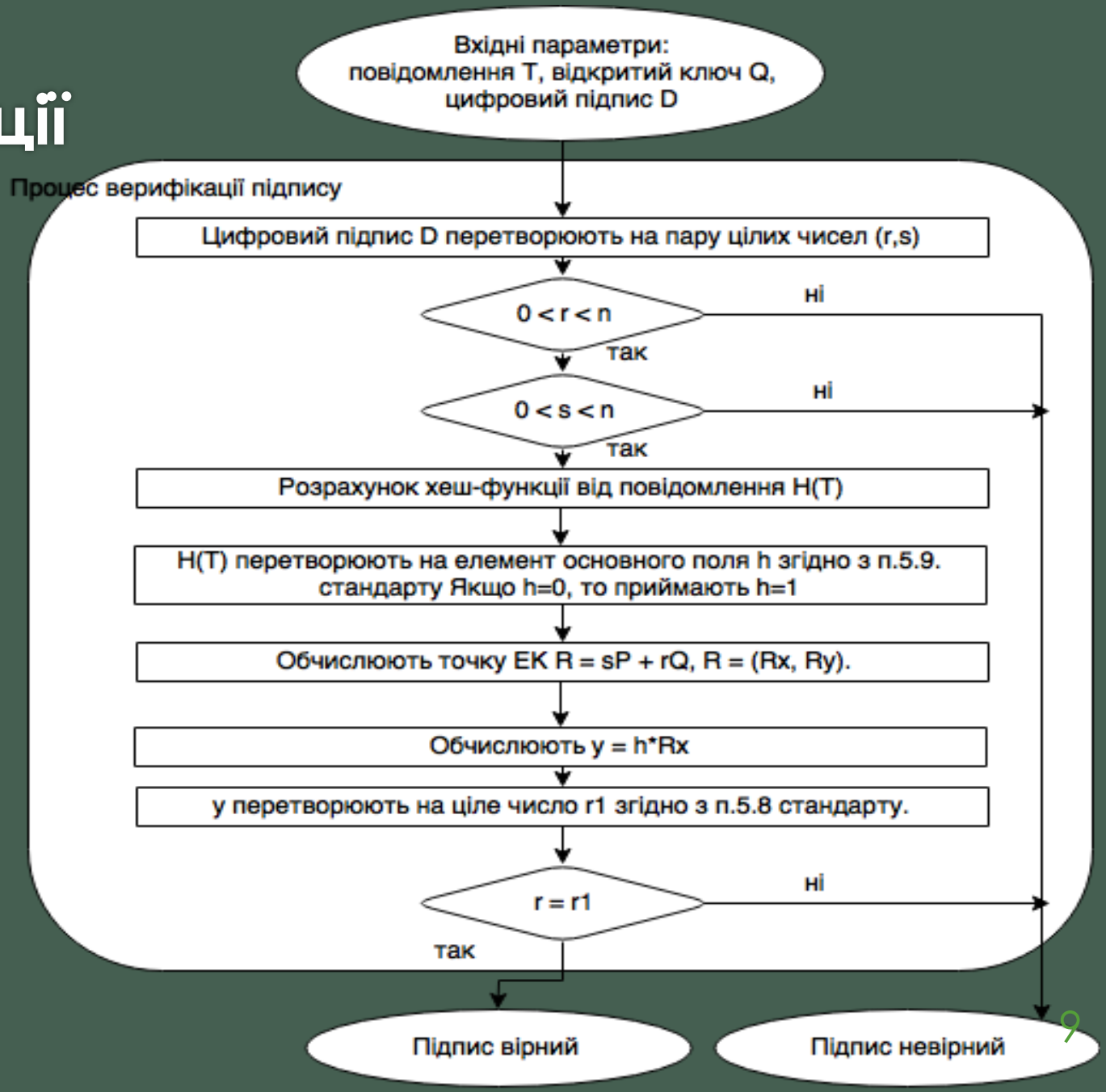
Алгоритм задається наступними параметрами:

- A, B - коефіцієнти рівняння ЕК y^2+xy=x^3+Ax^2+B
- k, m - кількість членів і старша ступінь основного многочлена, по модулю якого виконуються всі арифметичні операції. Наприклад, k = 5, m = 5 задає наступне многочлен: $x^5 + x^3 + x + 1$.
- P - Базова точка порядку n.
- Пара ключів складається з секретного ключа d і публічного ключа Q = -d * P.

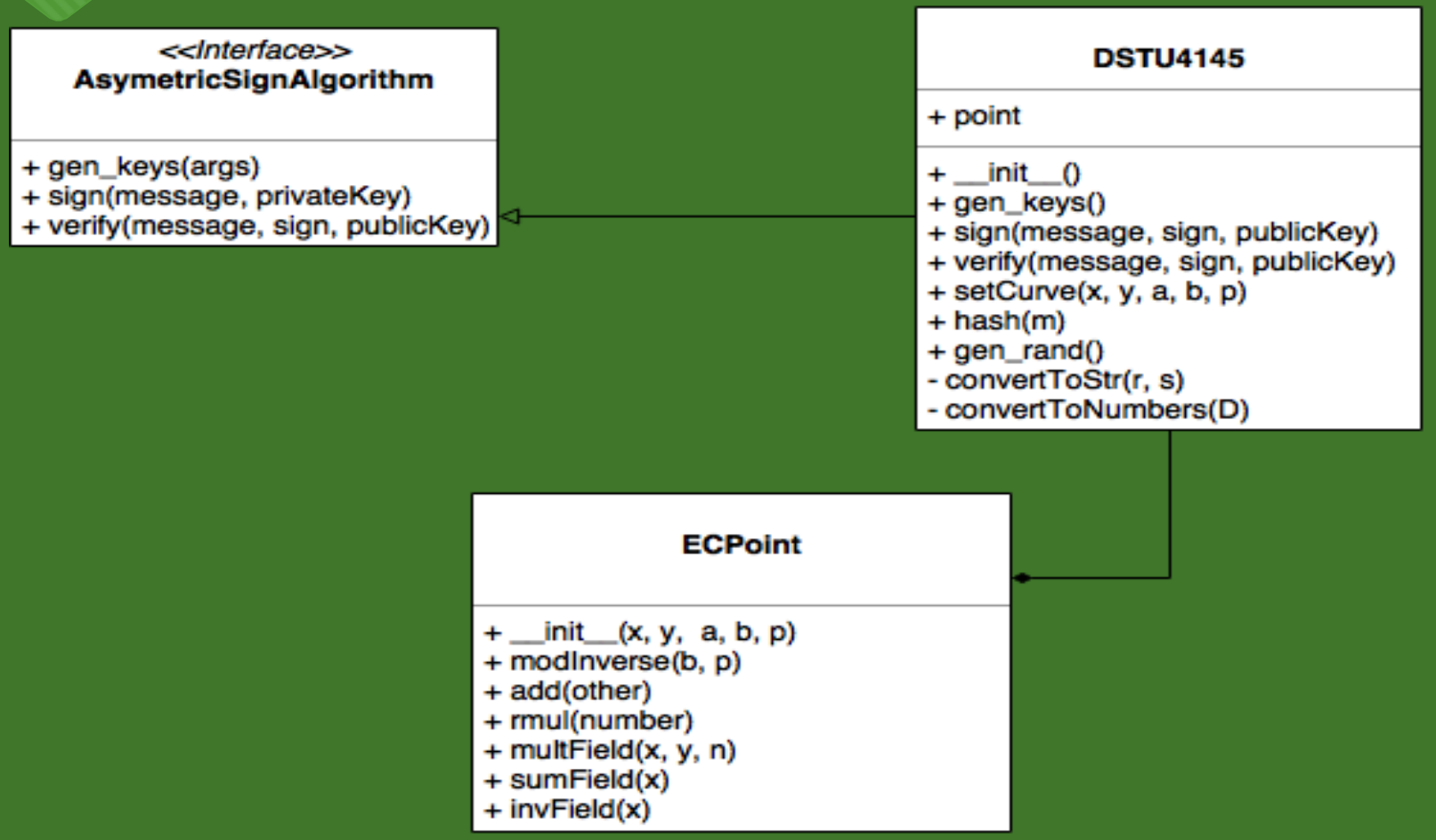
Алгоритм підпису



Алгоритм верифікації

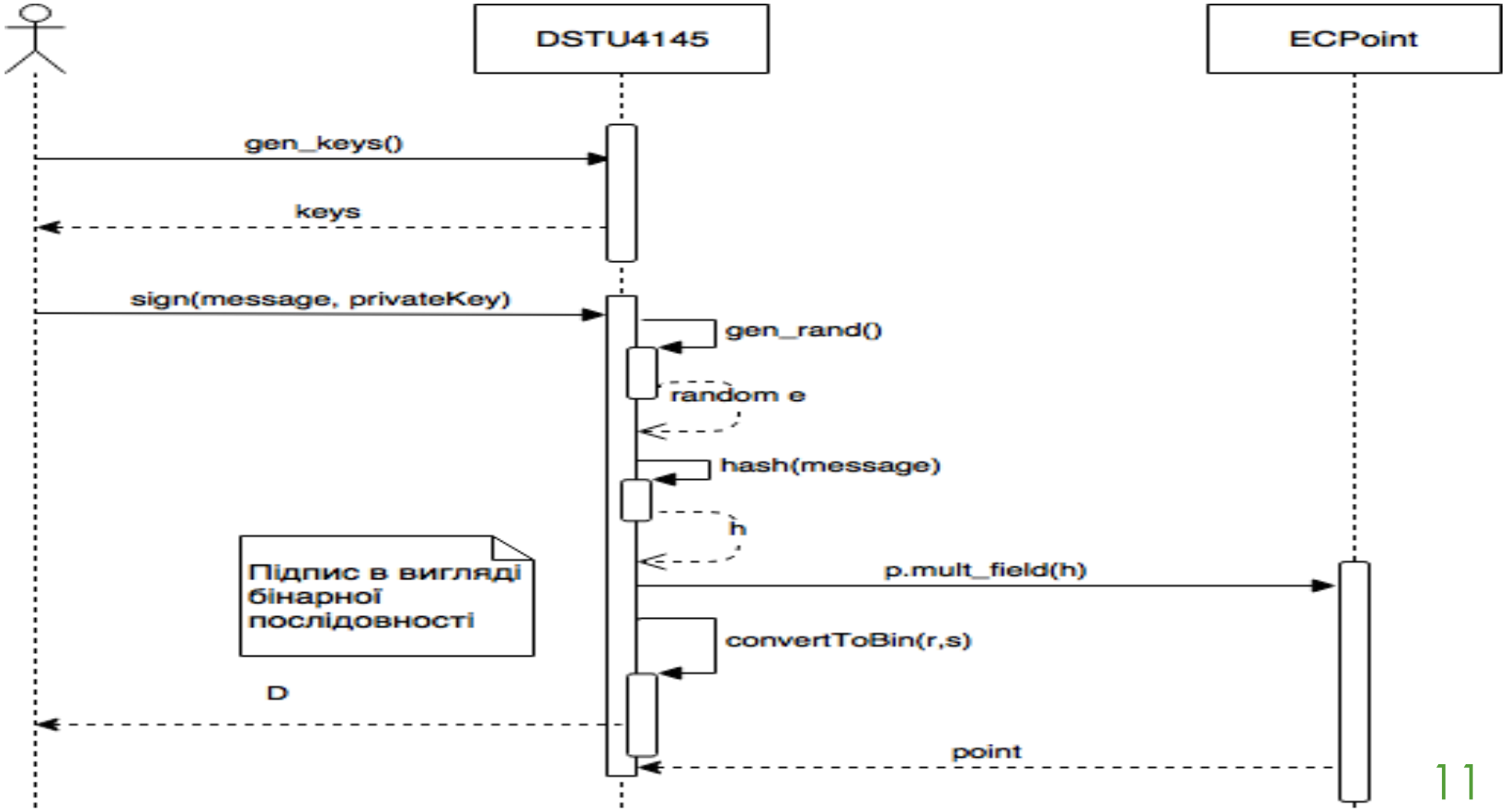


Діаграма класів



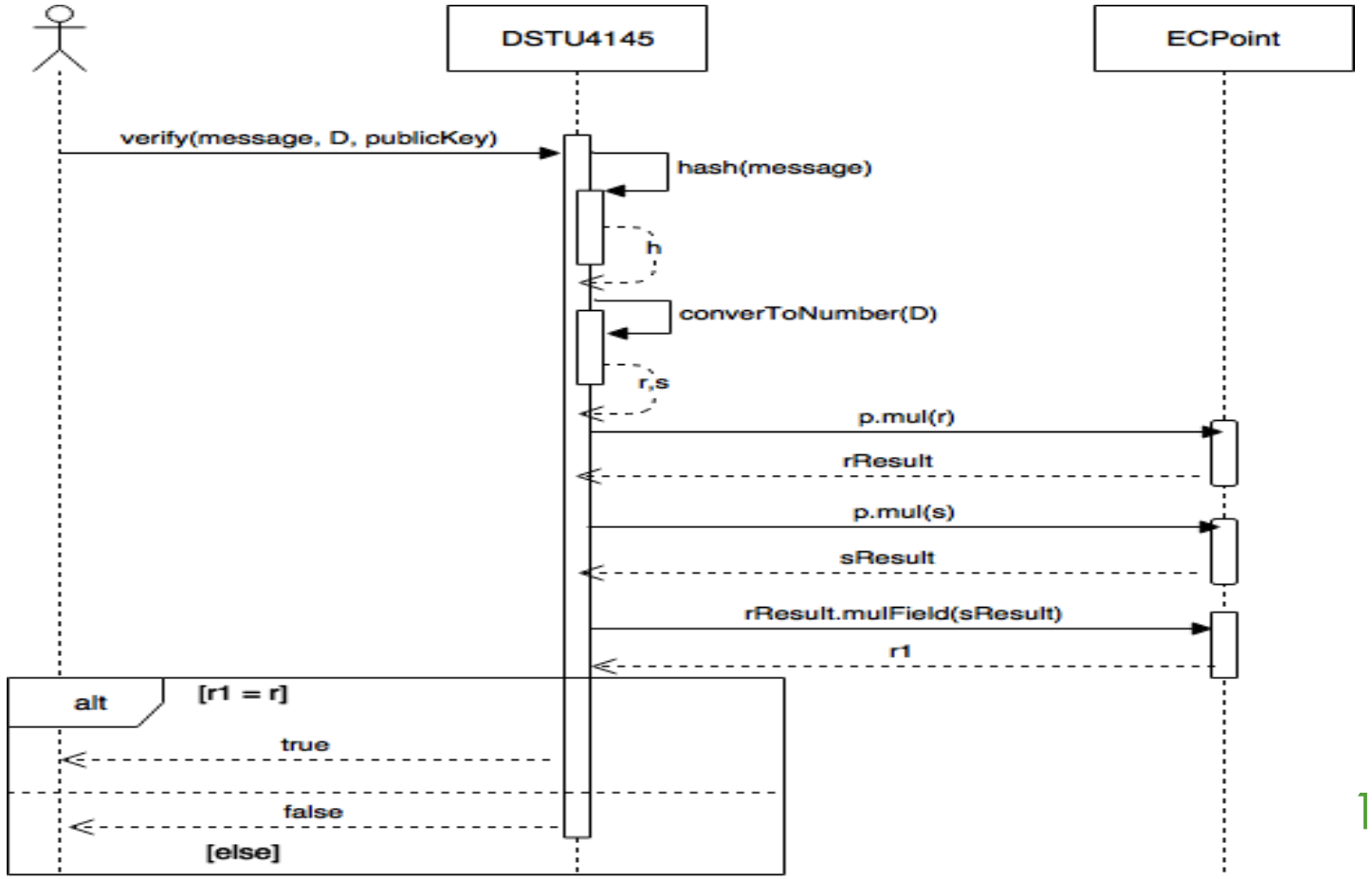
Діаграма послідовності створення цифрового підпису

```
...
dstu = DSTU4145()
secretKey, publicKey = dstu.gen_keys()
signature = dstu.sign(message, secretKey, True)
f = open('signature', 'w')
f.writelines(["%s\n" % item for item in signature])
f.close()
f = open('public_key', 'w')
pickle.dump(publicKey, f)
f.close()
...
```



Діаграма послідовності верифікації цифрового підпису

```
...
f = open('signature', 'r')
D = f.read()
f.close()
publicKey = pickle.load(open('public_key', 'r'))
signature = [int(line.rstrip('\n')) for line in open('signature')]
dstu = DSTU4145()
print dstu.verify(message, signature, publicKey)
...
```



Потенційні користувачі

- Створений криптопровайдер можна розглядати як API для існуючих систем, тому потенційними користувачами можуть бути компанії, які збираються інтегрувати в свої існуючі системи електронний цифровий підпис як засіб для проведення автентифікації та захисту інформації від змін.
- **Отримано акт впровадження в організації «Скай сіті груп».**

Висновки

- В результаті виконання роботи було реаліззовано інструментальні засоби цифрового підпису згідно обраного вітчизняного стандарту ДСТУ 4145-2002, які являють собою крипто-провайдер(бібліотеку класів), який реалізовує підпис та його перевірку, а також інші функції та математичні операції описані в вітчизняному стандарті ДСТУ 4145-2002.
- реалізовано операції на еліптичних кривих необхідні для виконання математичних операцій згідно вітчизняного стандарту;
- проведено аналіз існуючих програмних реалізацій;
- реалізація всіх необхідних пунктів стандарту ДСТУ-4145 для забезпечення повноцінного створення та верифікації цифрового підпису;

Дякую за увагу!