Дипломна робота
на здобуття ступеня бакалавра
на тему:

Дослідження алгоритмів та засобів реалізації конфіденційного цифрового підпису

Винонав: Кеба Сергій, ДА-62

Науковий курівник: Капшук О. О.

МЕТА РОБОТИ

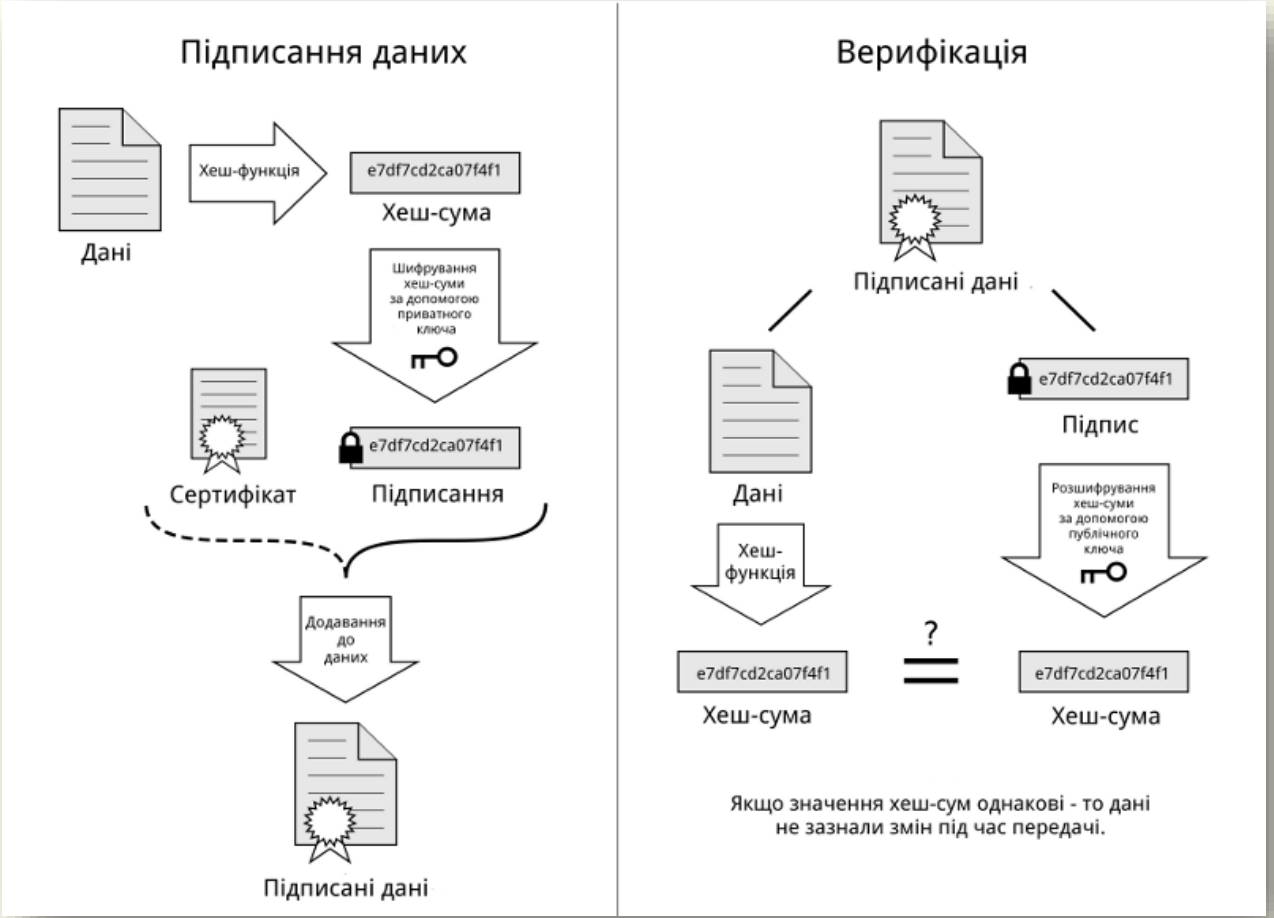
Метою роботи є дослідження безпеки існуючих алгоритмів та засобів реалізації конфіденційного цифрового підпису в електронному документообігу.

Актуальність

- Постійне зростання темпів використання електронного цифрового підпису супроводжується недостатнім приділенням уваги вирішенню питань безпеки;
- В умовах карантину і ізоляції, електронний цифровий підпис – це не просто зручний, а найбільш пріоритетний засіб контролю документообігу;
- Майже повна відсутність будь-яких досліджень теми конфіденційного цифрового підпису в неангломовному сегменті.

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

Алгоритм функціонування традиційного цифрового підпису:



БЕЗПЕКА ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Види атак:

- Атака з використанням відкритого ключа;
- Атака на основі відомих повідомлень;
- Адаптивна атака на основі вибраних повідомлень.

Результати атак:

- Повний взлом підпису;
- Універсальна підробка підпису;
- Вибіркова підробка підпису (пошук колізії другого роду);
- Екзистенціальна підробка підпису (пошук колізія першого роду).

Рекомендація до покращення: поступове збільшення складності обчислювальних алгоритмів пропорційне покращенню потужності обчислювальної техніки; розробка хешів, що менше піддаються колізіям.

КОНФІДЕНЦІЙНИЙ ЦИФРОВИЙ ПІДПИС

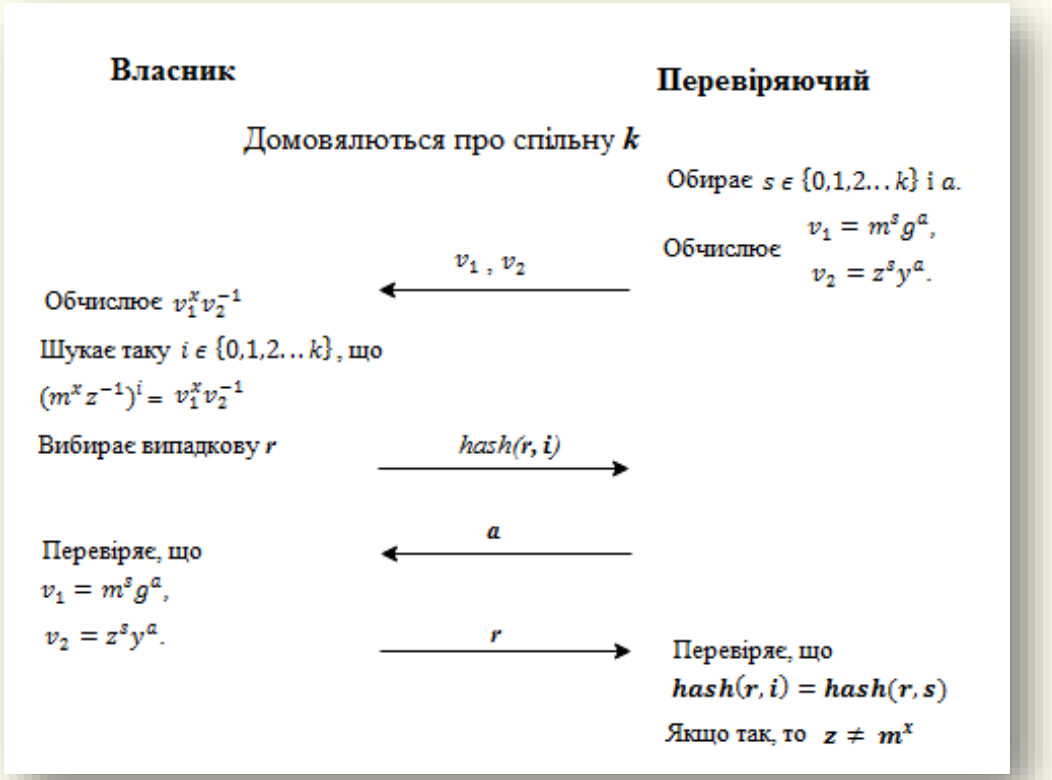
- Конфіденційний цифровий підпис не може бути перевірений без дозволу власника, оскільки, на відміну від звичайного ЕЦП, у процедурі верифікації беруть участь дві особи;
- Існує спеціальний протокол відмови, а тому підписувачу неможливо хибно відмовитися від свого справжнього підпису.

КОНФІДЕНЦІЙНИЙ ЦИФРОВИЙ ПІДПИС

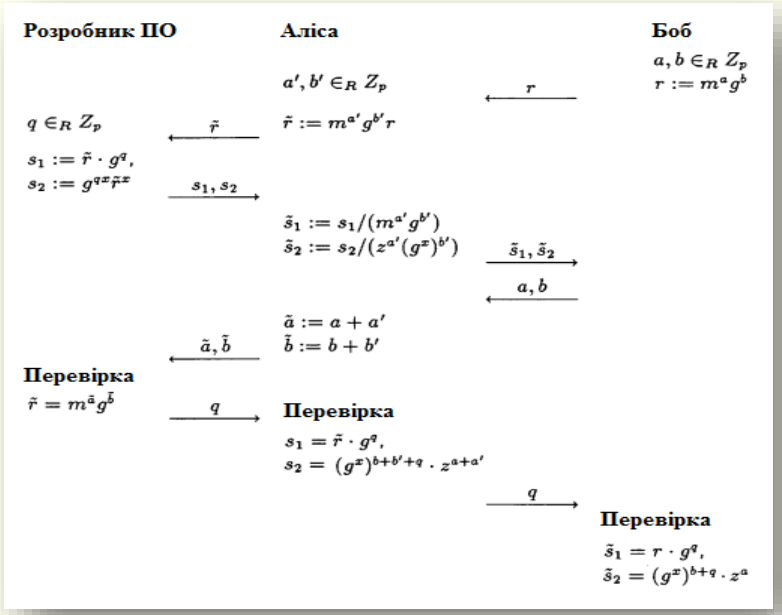
1) Вибираються прості числа ***p*** і ***g***;
2) Вибирається пара: ***x*** – закритий, g^x – відкритий;
3) Для повідомлення ***m*** створюється підпис m^x.
4) Протокол перевірки:

КОНФІДЕНЦІЙНИЙ ЦИФРОВИЙ ПІДПИС

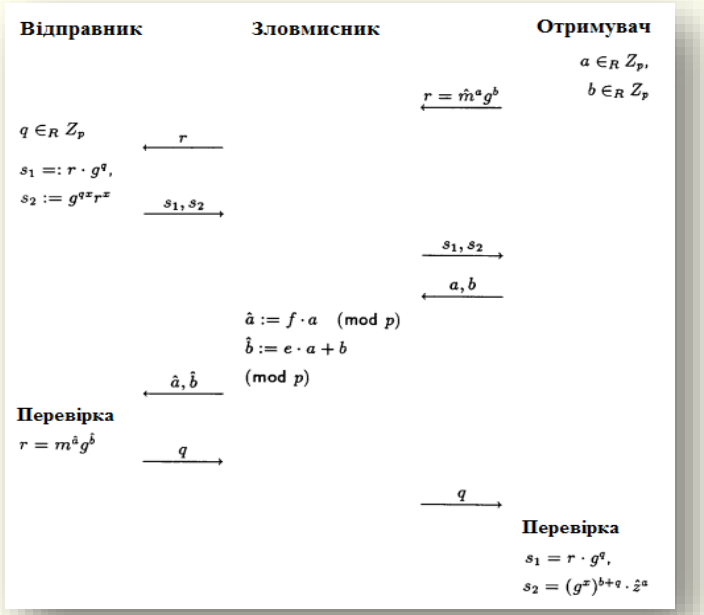
5) Протокол відмови, де ***z*** – потенційно хибний підпис:



БЕЗПЕКА ВИКОРИСТАННЯ КОНФІДЕНЦІЙНОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ



Атака з невірним верифікатором



Атака перешкодами

Рекомендація до покращення: залучення інших засобів верифікації, додавання неупередженої особи арбітра, наявність центрів аналогічних АЦСК для ЕЦП, введення певних фізичних обмежень.

КОНВЕРТОВАНИЙ КОНФІДЕНЦІЙНИЙ ЦИФРОВИЙ ПІДПИС

- Надає можливість, шляхом розкриття частини секретного ключа, перетворити конфіденційний цифровий підпис в звичайний;
- Надає можливість здійснювати процедуру верифікації колу довірених осіб власника підпису (агентам);
- Протокол відмови від підпису для агентів також існує, але використовується рідко. Як правило, відмовою, виключно в судових процесах, займається сам власник підпису;
- Досить громіздкий в реалізації.

АНАЛІЗ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ КОНФІДЕНЦІЙНОГО ЦИФРОВОГО ПІДПИСУ

Швидкодія RSA:

- Раунд генерації ключів:

RSA-512	RSA-1024	RSA-2048	RSA-4096
0,1739	0,5564	3,6815	148,08

- Раунд створення підпису:

RSA-512	RSA-1024	RSA-2048	RSA-4096
0,0000731	0,000264	0,00201568	0,0140617

- Раунд перевірки підпису:

RSA-512	RSA-1024	RSA-2048	RSA-4096
0,0000063	0,000017	0,00006044	0,0002161

АНАЛІЗ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ КОНФІДЕНЦІЙНОГО ЦИФРОВОГО ПІДПИСУ

Швидкодія ECDSA:

- Раунд генерації ключів:

ECDSA-160	ECDSA-192	ECDSA-224	ECDSA-265	ECDSA-384	ECDSA-521
0,2093	0,2145	0,2964	0,3965	1,0387	2,0592

- Раунд створення підпису:

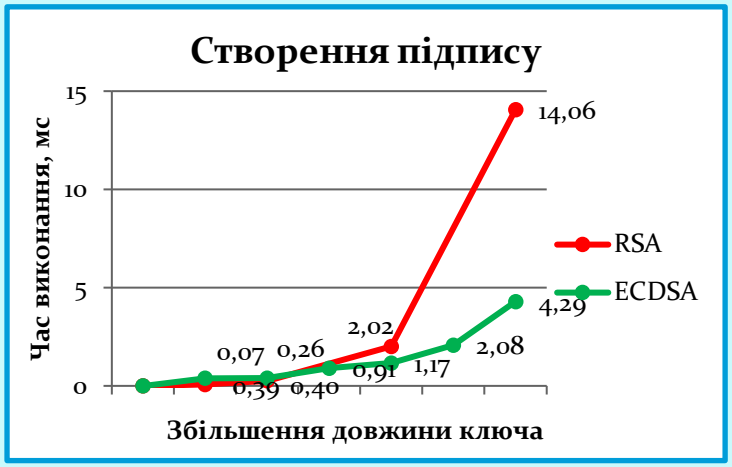
ECDSA-160	ECDSA-192	ECDSA-224	ECDSA-265	ECDSA-384	ECDSA-521
0,00039	0,000403	0,00091	0,00117	0,00208	0,00429

- Раунд перевірки підпису:

ECDSA-160	ECDSA-192	ECDSA-224	ECDSA-265	ECDSA-384	ECDSA-521
0,00195	0,0026	0,00312	0,00507	0,01066	0,0234

АНАЛІЗ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ КОНФІДЕНЦІЙНОГО ЦИФРОВОГО ПІДПИСУ

Співставлення часу виконання та ступеня безпеки:



РЕКОМЕНДОВАНІ НАПРЯМКИ ЗАСТОСУВАННЯ ДЛЯ КОЖНОЇ РОЗГЛЯНУТОЇ ТЕХНОЛОГІЇ

- **Електронний цифровий підпис**
  - підписання майже будь-яких документів в електронній формі;
  - перевірка сторонніми особами не має зашкодити власнику підпису;
  - немає конкретних зловмисників, які зацікавлені у взломі підпису.
- **Конфіденційний цифровий підпис**
  - є необхідність обмежити коло осіб-верифікаторів;
  - власник здатний встигати обробляти запити на підтвердження чи відмову від підпису.
- **Конвертований конфіденційний цифровий підпис**
  - є необхідність обмежити коло осіб-верифікаторів, однак в майбутньому допускається можливість зняття обмеження;
  - є необхідність розділення обов'язку перевірки між колом довірених облич.

ВИСНОВКИ

ДЯКУЮ ЗА УВАГУ !