Підвищення швидкодії методів цифрового підписування на основі еліптичних кривих з використанням паралельних обчислень GPGPU

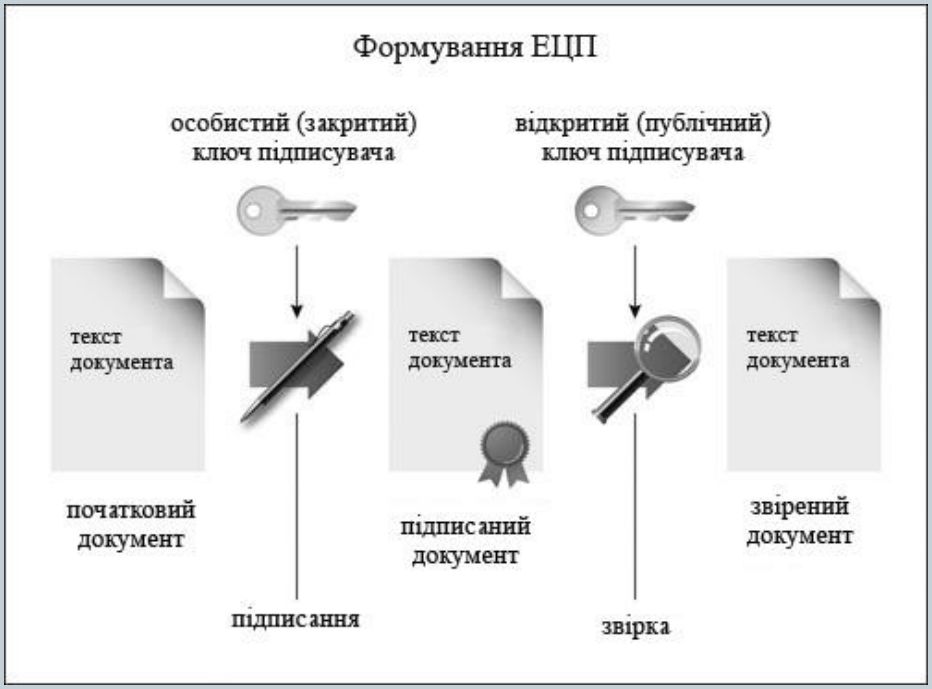
РОБОТА СТУДЕНТА ГРУПИ УБ – 18М
СОКОЛОВСЬКОГО ВЛАДИСЛАВА
НАУКОВИЙ КЕРІВНИК К.Т.Н., ДОЦ. КАРПІНЕЦЬ В.В.

Актуальність та новизна роботи

- Актуальність роботи зумовлена задачею забезпечення цілісності інформації, а також її достовірністю. Здійснити задачу забезпечення захисту даних та засвідчення прав на них може електронний – цифровий підпис, процес нанесення та перевірки якого потребує постійного вдосконалення.

- Наукова новизна – підвищення швидкодії методів цифрового підписування на основі еліптичних кривих з використанням паралельних обчислень GPGPU.

Процес формування електронного підпису та переваги його застосування



- Конфіденційність (автентичність і унікальність автора);
- Не піддається підробці або перенесенню по документах;
- Захищає від підробки та спотворення інформації документа;
- Економія часу при роботі із звітними документами.

Порівняльний аналіз існуючих методів

Алгоритм	Розмір ключа	Швидкість підпису, мс	Швидкість перевірки, мс
RSA	1024	1.48	0.07
	2048	6.05	0.16
DSA	1024	0.42	0.52
Ель – Гамаля	1024	0.45	1.18
	2048	0.83	3.84

Модифікація JSFmod

Для обчислення значення $R=53P+102Q$ виконуються наступні дії:

1. Отримати подання JSF для чисел $k=53$ та $l=102$.

   $k=\{1, 0, 0, -1, 0, -1, -1\}$, $l=\{1, 0, -1, 0, 0, 1, 1, 0\}$.

2. Для кожного номера розряду i отримати значення з таблиці передобчислених точок, тобто значення $Val=2^i k_i P+2^i l_i Q$.

   Додати до результату. Наприклад, для $i=2$, $R=R+Val$, де $Val=2^2 * 0 * P+2^2 * (-1) * Q=-4Q$.

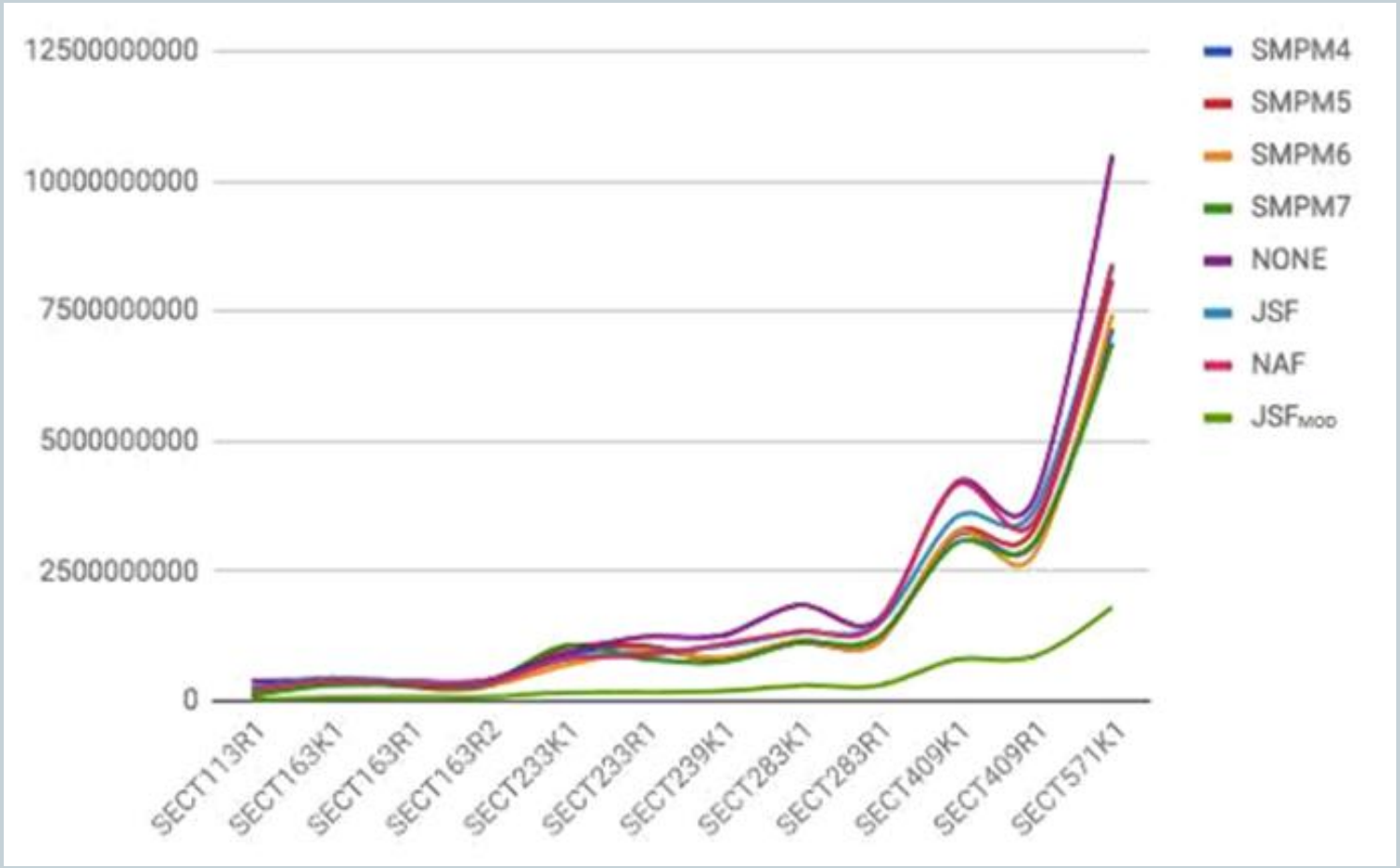
Значення часу перевірки ЕЦПдля еліптичних кривих з параметрами визначеними над полем GF(p), (мс)

	SMPM4	SMPM5	SMPM6	SMPM7	NONE	JSF	NAF	JSFmod
SECP112R1	11,9	10,6	7,2	7,9	9,2	16,7	12,8	4,2
SECP112R2	4,3	3,9	6,7	5,1	7,3	16,4	16,3	3,2
SECP128R1	11,1	5,5	6,2	8,5	7,9	10,4	25,3	5
SECP128R2	5,3	5,2	4,8	25,4	13,4	9,5	11,6	4,3
SECP192K1	19,3	13,9	18,3	12,5	14,7	26,4	29,4	11,4
SECP192R1	13,8	14,6	17,1	20,5	16	22,5	22,1	11,6
SECP224K1	31,3	16,4	15,5	13,8	19,8	30,9	28,8	16,6
SECP224R1	21,2	13,9	14	14,8	25,3	30,1	32,3	17,9
SECP256K1	19,2	25,8	18,5	19,4	25,8	42,8	46	25
SECP256R1	18,8	18,4	19,5	23,3	29,7	54,6	40,7	23,5
SECP384R1	49,9	50,8	46,4	47	68,3	108,2	114,9	66,8
SECP521R1	110,6	123,1	107,9	106,1	145	246,3	238,7	166

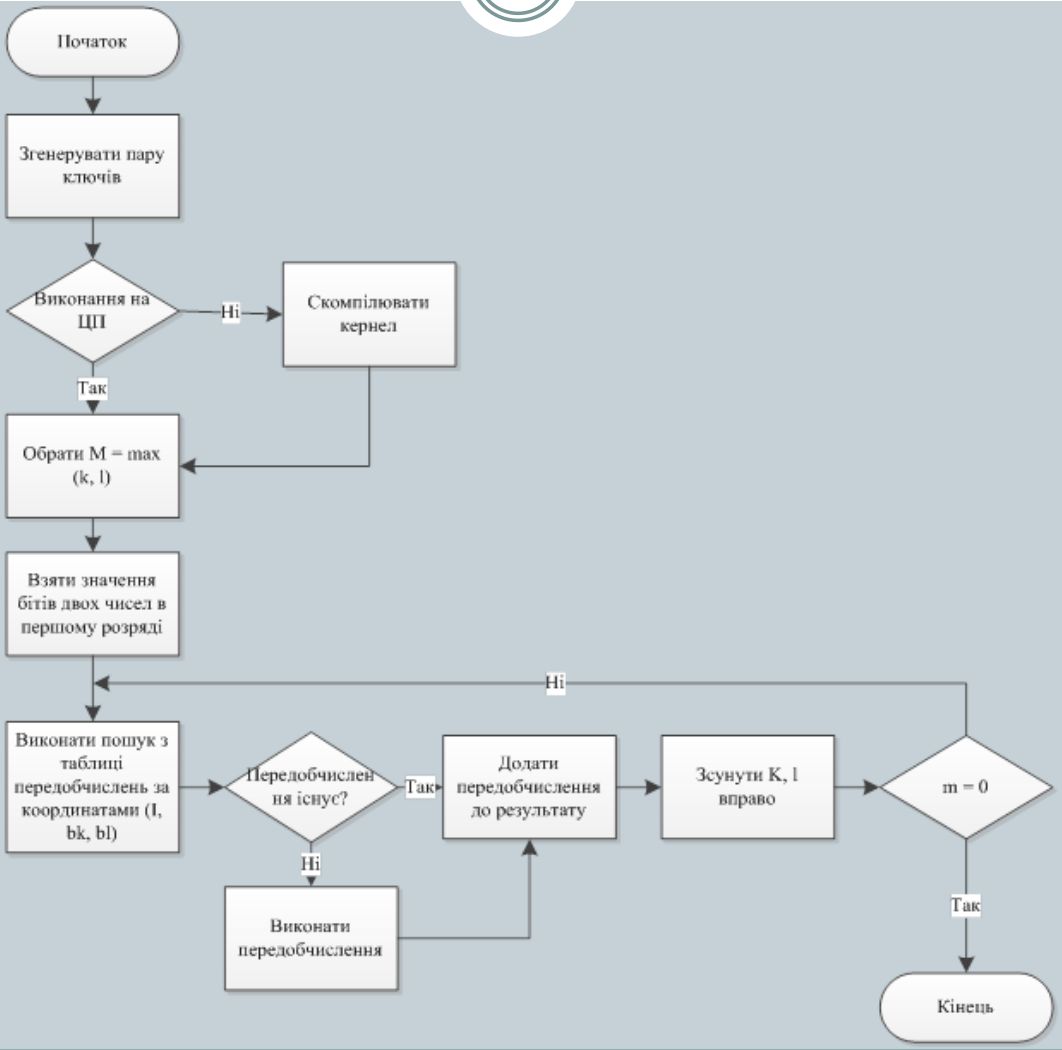
Значення часу перевірки ЕЦП для еліптичних кривих з параметрами визначеними над полем (2m)GF , (мс)

	SMPM4	SMPM5	SMPM6	SMPM7	NONE	JSF	NAF	JSFmod
SECT113R1	119,63	132,76	113,79	107,37	394,04	272,85	212,08	25,3
SECT163K1	382,31	448,27	343,17	308,83	417,16	437,67	398,19	60,2
SECT163R1	348,89	284,97	329,49	310,63	385,1	378,53	349,87	72,5
SECT163R2	349,55	284,17	296,77	336,07	399,61	333,97	349,3	67,4
SECT233K1	882,59	1027,2	683,72	1066,35	922,84	829,23	799,91	144,8
SECT233R1	1066,4	1052,14	969,35	818,54	1241,4	901,1	880,04	172,2
SECT239K1	791,88	807,24	834,56	751,31	1255,24	1061,03	1089,73	181,4
SECT283K1	1141,25	1133,76	1166,88	1132,89	1852,08	1326,8	1339,85	288,2
SECT283R1	1179,77	1123,88	1136,88	1216,29	1558,77	1470,38	1479,51	226,3
SECT409K1	3187,36	3244,52	3235,17	3044,42	4202,8	3540,57	4149,11	693,6
SECT409R1	3022,08	3307,61	2810,1	3047,54	3900,77	3670,78	3452,5	818,2
SECT571K1	7165,59	8101,03	7443,83	6889,09	10513,73	8386,25	8420,83	1712,8

Залежність часу перевірки ЕЦП при застосуванні різних методів для еліптичних кривих

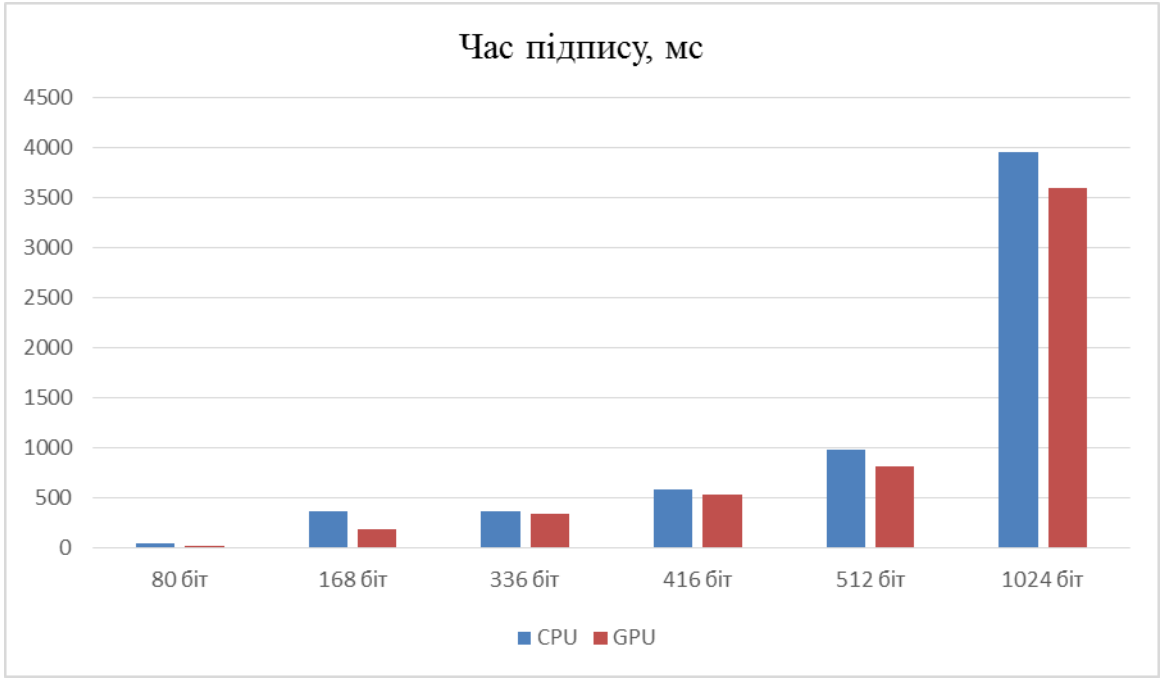


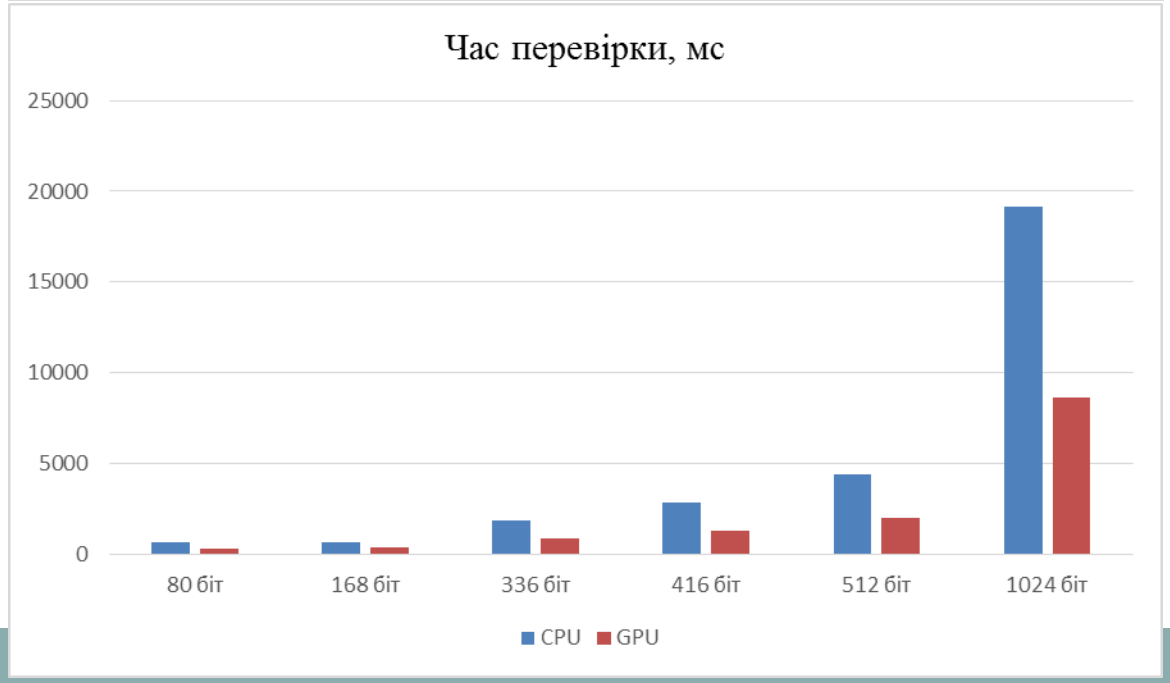
Блок – схема алгоритму розробленого методу



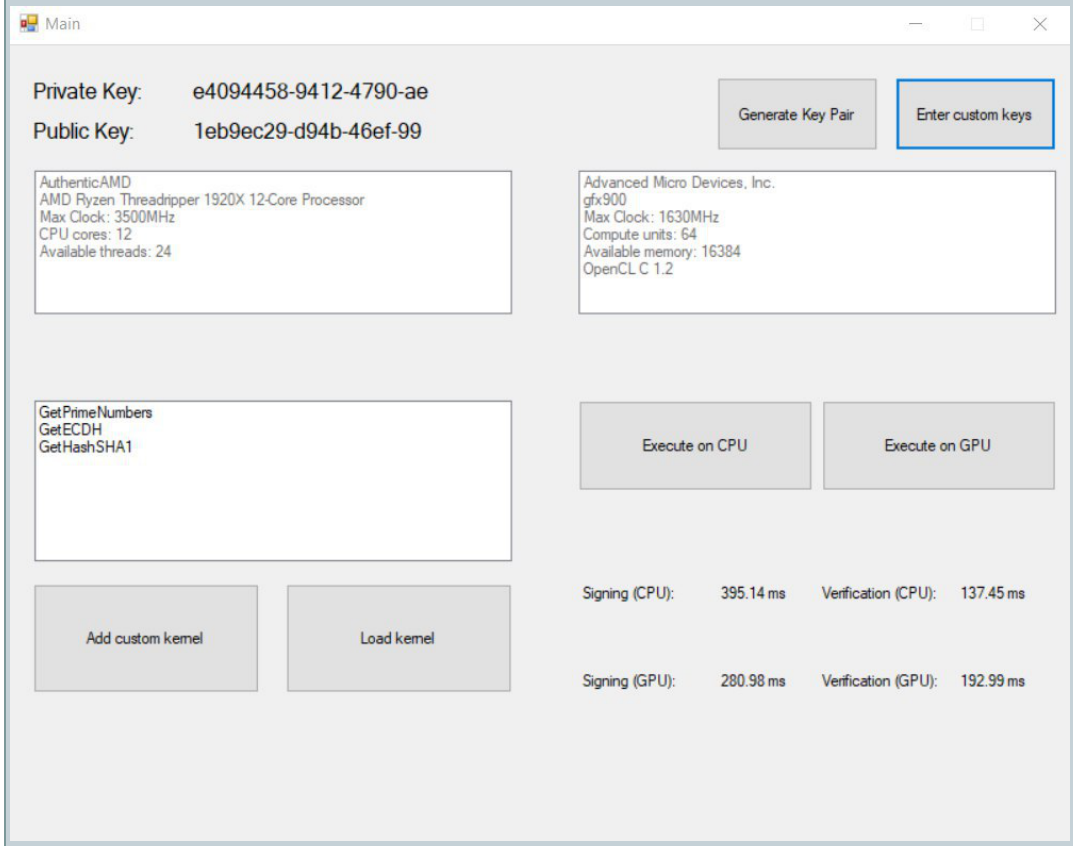
Порівняння часу формування/перевірки підпису з допомогою CPU та GPU

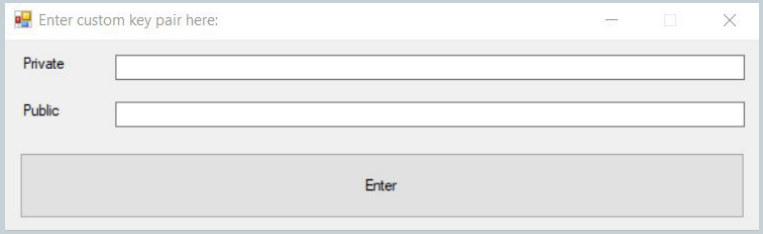
Довжина ключа, біт	Час виконання процесу формування ЦП, мс		Час виконання процесу перевірки ЦП, мс	
	CPU	GPU	CPU	GPU
80	53.7	27.9	94.38	42.9
168	373.8	192.6	434.8	195.6
336	374.3	341.2	1818.3	818.2
416	582.3	532.2	2838.3	1277.2
512	986.4	822.0	4341.0	1973.2
1024	3952.3	3593.0	18968.8	8622.2

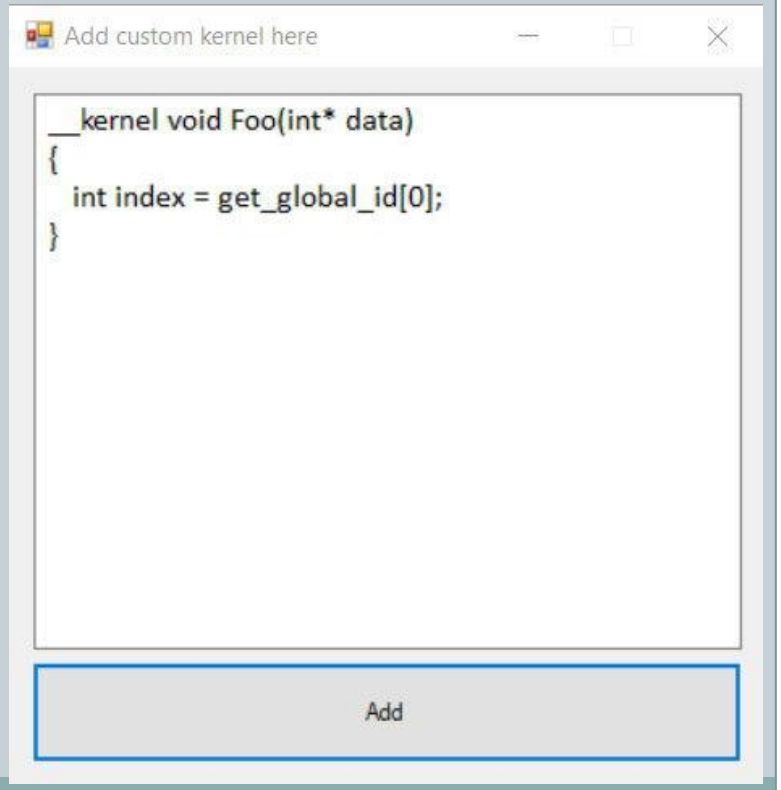

Час підпису, мс
4500
4000
3500
3000
2500
2000
1500
1000
500
0
80 біт
168 біт
336 біт
416 біт
512 біт
1024 біт
CPU
GPU


Час перевірки, мс
25000
20000
15000
10000
5000
0
80 біт
168 біт
336 біт
416 біт
512 біт
1024 біт
CPU
GPU

Інтерфейс додатку

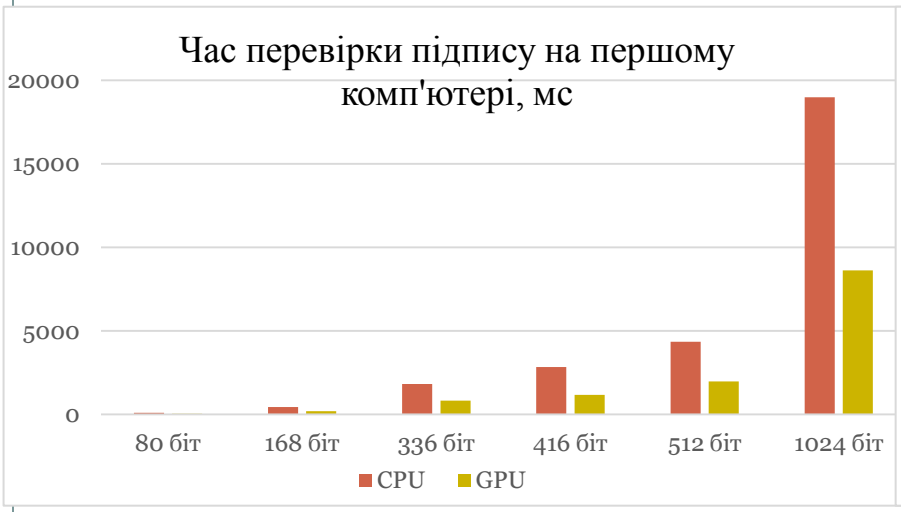


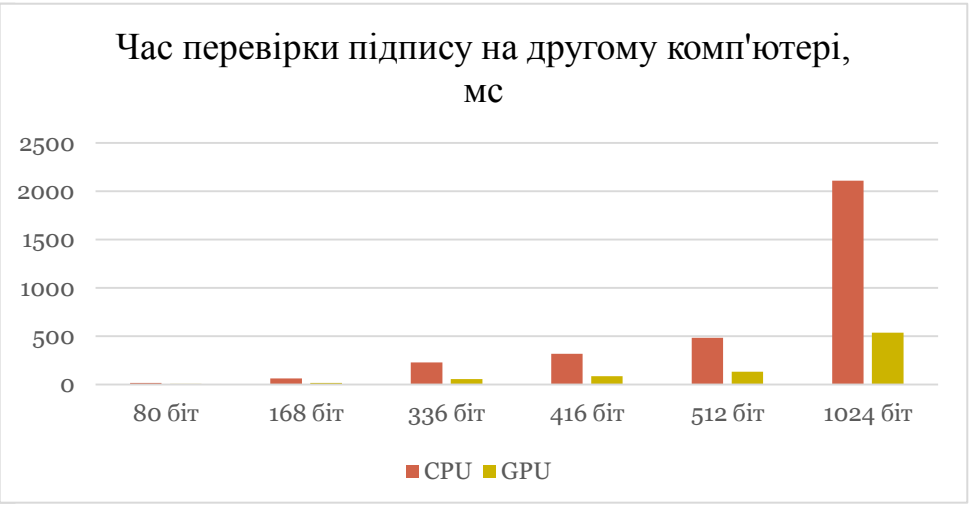


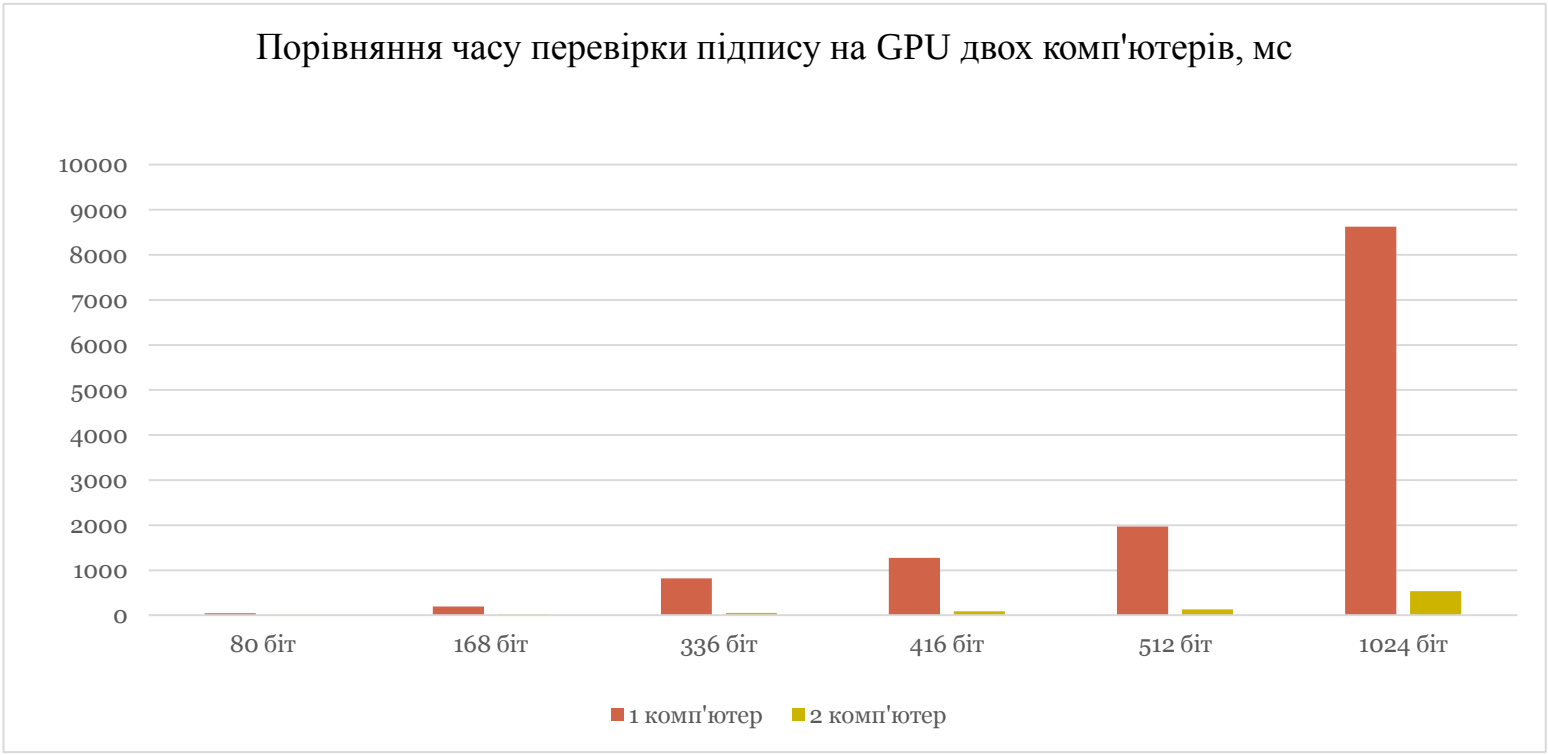


Порівняння часу перевірки підпису з допомогою CPU та GPU на двох різних комп'ютерах

Довжина ключа, біт	Перший комп'ютер		Другий комп'ютер	
	CPU(мс)	GPU(мс)	CPU(мс)	GPU(мс)
80	94,4	42,9	15,8	3,6
168	434,8	195,6	62,1	14,0
336	1818,3	818,2	227,3	54,5
416	2838,3	1277,2	315,4	85,1
512	4341,0	1973,3	482,0	131,5
1024	18968,8	8622,2	2107,6	574,8


Час перевірки підпису на першому комп'ютері, мс
20000
15000
10000
5000
0
80 біт
168 біт
336 біт
416 біт
512 біт
1024 біт
CPU
GPU


Час перевірки підпису на другому комп'ютері, мс
2500
2000
1500
1000
500
0
80 біт
168 біт
336 біт
416 біт
512 біт
1024 біт
CPU
GPU


Порівняння часу перевірки підпису на GPU двох комп'ютерів, мс
10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
80 біт
168 біт
336 біт
416 біт
512 біт
1024 біт
1 комп'ютер
2 комп'ютер

Висновок

- Завдяки математичним підрахункам було встановлено, що запропонована модифікація дає вищу швидкодію при перевірці електронно-цифрового підпису за алгоритмом ECDSA над еліптичною кривою з параметрами, визначеними над скінченним полем (2m)GF, а обчислювальна складність виконання передобчислень для запропонованої модифікації є набагато меншою, ніж при використанні інших методів.
- Дослідження практичних результатів роботи розробленого програмного додатку показали, що швидкість виконання тих самих обчислень на графічному та центральному процесорі різна.
- Наведені вище обчислення з використанням GPU дозволяють значно прискорити процес цифрового підписування, оскільки надають можливість майже лінійно збільшувати швидкість підписування залежно від кількості процесорів та потоків на які було виконано розпаралелювання.

Дякую за увагу!