УДК 622.242

РЕАЛІЗАЦІЯ RSA НА CUDA API

Я. І. Заячук, О. В. Мойсеєнко, І. М. Сухецький, Р. В. Цвілинюк

ІФНТУНГ; 15, вул. Карпатська, м. Івано-Франківськ, 76019. E-mail y.zaiachuk@nung.edu.ua

На початку 2007 nVidia запропонувала технологію, що дозволяє використовувати її відеокарти для обчислень - Compute Unified Device Architecture, CUDA. Програмування здійснюється дещо урізаним варіантом С чи С++, доповненим кількома ключовими словами.

Графік від nVidia з порівнянням росту теоретичної продуктивності процесорів та відеокарт показано на рис. 1.

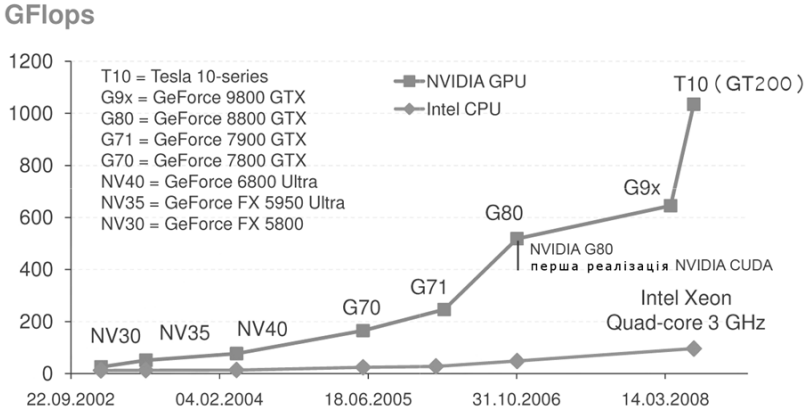

Рисунок 1 - Порівняння росту теоретичної продуктивності процесорів та відеокарт

Як інтегроване середовище розробки (IDE) для розробки програм на С (зокрема з використання CUDA API) під ОС Windows застосовують Microsoft© Visual Studio© (на даний момент акуальна версія Microsoft© Visual Studio© 2013, проте в ній були певні проблеми з інтеграцією CUDA SDK 5.0, тому для розробки використано Visual studio 2010).

Авторами було розробено власну реалізацію системи довгої арифметики (СДА), в якій можна виконувати основні арифметичні операції, порівняння, бітові зсуви, піднесення до степеня, ділення за модулем. Реалізація розширеного алгоритму Евкліда для СДА має вигляд:

```
x2[ MAX-1 ] = 1; x1[ MAX-1 ] = 0; y2[ MAX-1 ] = 0; y1[ MAX-1 ] = 1;
while ( cmp( temp_b, zero ) > 0) {
div ( temp_a, temp_b, q);//q = a / b,
mul ( q, temp_b, temp ); sub ( temp_a, temp, r);//r = a - q * b;
clearLongVariable ( temp );
mul ( q, x1, temp ); sub ( x2, temp, x );//*x = x2 - q * x1,
clearLongVariable ( temp );
mul( q, y1, temp ); sub( y2, temp, y );//*y = y2 - q * y1;
copyVariable( temp_b, temp_a );//a = b,
copyVariable( r, temp_b );//b = r;
copyVariable( x1, x2 ); //x2 = x1,
copyVariable( x, x1 );//x1 = *x,
copyVariable( y1, y2 ); //y2 = y1,
copyVariable( y, y1 );//y1 = *y;}
copyVariable( temp_a, d );//*d = a,
copyVariable( x2, x );//*x = x2,
```

Алгоритм роботи програми шифрування зображено на рис. 2.

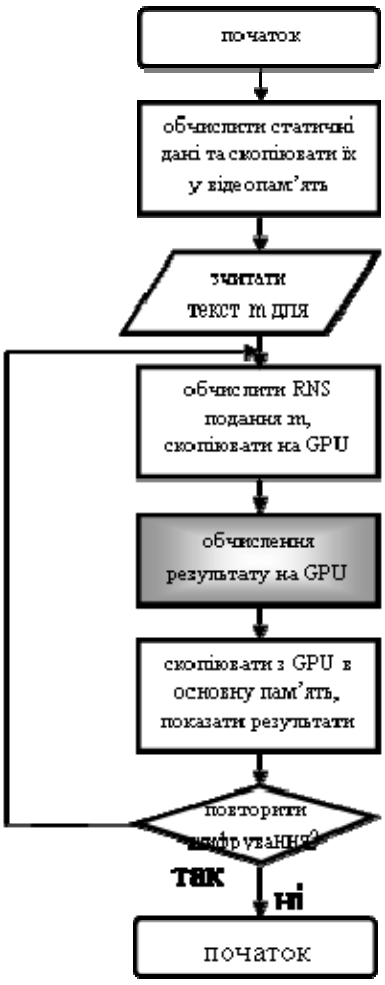

Рисунок 2 – Алгоритм роботи програми для шифрування на RSA-1024

На основі теоретичних положень була розроблена програма для шифрування вхідного повідомлення, яке є hex-числом, що вводиться з клавіатури, довжиною менше ніж 256 символів (тобто до 1024 біт інформації). Після обчислення – на виході маємо також hex-результат, який є зашифрованим RSA-1024 повідомленням.

Отримано прискорення RSA шифрування приблизно в 25 разів. Теоретичне значення – 32 рази не було досягнуте, в першу чергу через неповну паралельність: загалом в програмі тричі використовується команда синхронізації потоків, внаслідок чого, частина потоків простоює, і знижується продуктивність.

Літературні джерела

1 Заячук Я. І. Використання системи залишкових класів для реалізації асиметричних криптоалгоритмів на SIMD-архітектурах на прикладі RSA / Я. І. Заячук, О.В. Мойсеєнко, М.М. Клим'юк // Вісник ДУІКТ - 2013.-С. 36-43.

2 Sandee M. RSA-512 Certificates abused in the wild. [Електронний ресурс] // – Режим доступу: http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/.

3 Modular arithmetic [Електронний ресурс] // – Режим доступу: http://en. wikipedia.org/wiki/Modular_arithmetic.