Contribution ID: **124** Type: **sectional reports**

АЛГОРИТМ ГЕНЕРАЦИЙ 1024 БИТНОГО КЛЮЧА С ИСПОЛЬЗОВАНИЕМ CUDA АРХИТЕКТУРЫ

Monday, 30 June 2014 15:30 (15 minutes)

Мы тестировали алгоритм генераций 2048 битного RSA ключа на Nvidia графическом акселераторе с использованием CUDA программирования.
Веб сайты и сетевые компьютеры используют криптосистемы с открытыми ключами для идентификации. RSA используется в основном для расшифровки трафика между клиентом и сервером. Защита RSA криптосистемы построена на факторизации больших чисел. Открытый ключ RSA состоит из пары целых чисел: открытой экспоненты e и модуля N, являющимся произведением двух больших простых чисел p и q. Задача разложения натурального числа N на простые множители является задачей вычисления односторонней функции: зная сомножители p и q, нетрудно вычислить их произведение N = p • q, но обратная задача нахождения делителей p и q по известному N является сложной задачей, решение которой требует значительных вычислительных ресурсов.
Мы использовали openSSL библиотеку для генерации 2048 битного числа. Чтобы проверить генерированное число является ли простым AKS тест на простоту чисел [1].
Для вычисления использовали Intel Core i3 процессор с 2.92 ГГц тактовой частотой, и , Nvidia GTX 650 графический акселератор с двумя поточными мультипроцессорами. Для отображения числа на памяти использовали следующую форму:
, (1).
Здесь B- основа системы исчесления , и - множители "цифры". GTX 650 графическая карта имеет 32 битовый регистр в каждом ядре мы выбрали основу B = .
Для вычисления НОД-а использовали расширенный алгоритм Эвклида [1].

Список литературы

[1] Введение в криптографию. Под общ. ред. В.В.Ященко//М., МЦНМО, 2008

Primary authors: Dr ДАЛАНБАЯР, Болормаа (Монгольский Государственный Университет, Факультет Прикладной Науки и Инженеринга); Dr ДАМБАСҮРЭН, Нанзадрагчаа (Монгольский Государственный Университет, Факультет Прикладной Науки и Инженеринга)

Presenter: Dr ДАЛАНБАЯР, Болормаа (Монгольский Государственный Университет, Факультет Прикладной Науки и Инженеринга)

Session Classification: Algorithms and methods of application tasks solving in distributed computing environments