УДК 519.85

ПРЕОБРАЗОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

© О.В. Крючин, К.Р. Хабирова

Ключевые слова: криптография; параллельные алгоритмы.
Описана возможность использования параллельных алгоритмов для разработки криптографических программ. Приводится сравнение с существующими программами шифрования и дешифрования.

Актуальность шифрования большого объема информации возникла сравнительно недавно с появлением средств мультимедиа и сетей с высокой пропускной способностью, обеспечивающих передачу мультимедийных данных. Традиционно для преобразования (шифрования и дешифрования) данных используются различные методы криптографии.

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию [1, 2].

Хотя изначально криптография занималась лишь защитой текстовой или символьной информации, в современных информационных системах начинают применяться технологии, которые требуют передачи существенно бóльших объемов данных. Среди таких технологий факсимильная, видео и речевая связь, голосовая почта и системы видеоконференций [3].

Шифрование таких объемов информации требует значительных временных затрат, которые недопустимы при трансляции. В настоящее время эта проблема решается потоковой или блочной передачей информации, что позволяет снизить время ожидания, но не позволяет ускорить процесс шифрования. Другим методом решения этой проблемы является использование параллельных вычислений и кластерных вычислительных систем.

Кластерная система – это группа компьютеров, объединенных высокоскоростными каналами связи и представляющая с точки зрения пользователя единый аппаратный ресурс. Иными словами, это слабосвязанная совокупность нескольких вычислительных систем, работающих совместно для выполнения общих приложений и представляющихся пользователю единой системой.

В этом случае шифрование производит не один компьютер, а несколько машин, объединенных в локальную вычислительную сеть – кластерную систему. Для использования такой системы необходимо разработать параллельные алгоритмы шифрования. Для межпроцессорной передачи данных можно использовать высокоуровневую библиотеку *CrVMpi*, базирующуюся на известной технологии *MPI* [4]. В качестве кластерной системы может быть использована обычная локальная сеть с высокоскоростным интерконнектом.

Таким образом, использование параллельных алгоритмов криптографии позволяет значительно снизить временные затраты.

ЛИТЕРАТУРА

1. *Hakim J.* A History of US: War, Peace, and All That Jazz. 1918–1945. N. Y.: Oxford University Press, 2006.
2. *Нечаев В.И.* Элементы криптографии (Основы теории защиты информации). М.: Высш. шк., 1999. 109 с.
3. *Баричев С.* Криптография без секретов. М.: Горячая Линия – Телеком, 2004. 44 с.
4. *Крючин О.В., Королев А.Н.* Библиотека распараллеливания // Вестник Тамбовского университета. Серия Естественные и технические науки. Тамбов, 2009. Т. 14. Вып. 2. С. 465-467.

Поступила в редакцию 20 ноября 2013 г.

Kryuchin O.V., Khabirova K.R. CONVERTING DATA USING PARALLEL COMPUTING TECHNOLOGY

The use of parallel algorithms for the development of encryption software is described. The comparison with existing programs encryption and decryption is given.

Key words: cryptography; parallel algorithms.