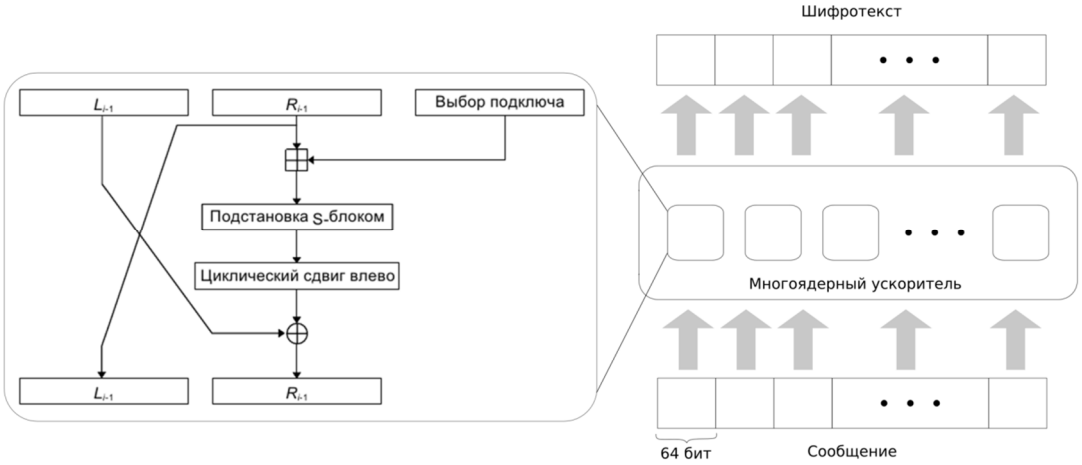
Разработка параллельного алгоритма шифрования ГОСТ 28147-89 на платформе IntelXeonPhi

М.С. Миниахметова, М.Л. Цымблер

Южно-Уральский государственный университет

В соответствии с российским законодательством технические средства защиты информации должны осуществлять шифрование данных, используя криптографический стандарт ГОСТ 28147-89. Блочная реализация алгоритма ГОСТ 28147-89 предполагает разбиение сообщения на блоки равной длины, шифрование которых осуществляется независимо (см. рис. 1а). Таким образом, при использовании блочного метода шифрования возможна параллельная обработка всех блоков сообщения на многопроцессорной и/или многоядерной системе (см. рис. 1б).



а) последовательный алгоритм б) схема распараллеливания

Рис. 1. Шифрование по ГОСТ 28147-89

На сегодняшний день известны параллельные реализации блочного алгоритма шифрования ГОСТ 28147-89 с использованием технологий OpenGL, DirectX и CUDA [2, 3].

В данной работе в качестве аппаратной платформы параллельного алгоритма шифрования ГОСТ 28147-89 предлагается использовать сопроцессоры Intel Xeon Phi с архитектурой Many Integrated Core (MIC). Представленная корпорацией Intel в 2012 г. аппаратная платформа гибридных многопроцессорных систем с многоядерными ускорителями Intel Xeon Phi совмещает в себе преимущества графических ускорителей с традиционной архитектурой x86. По результатам экспериментов компании-разработчика, гибридная многопроцессорная платформа с использованием MIC превосходит по производительности и эффективности многопроцессорные системы с графическими ускорителями [1].

Целью данной работы является создание параллельного алгоритма шифрования ГОСТ 28147-89, адаптированного для многопроцессорных систем с многоядерными ускорителями Intel XeonPhi.

Литература

1. Hughes C.J, Changkyu K., Yen-Kuang C. Performance and Energy Implications of Many-Core Caches for Throughput Computing // IEEE Micro. 2010. Vol. 3, No. 6. P. 25-35.
2. Коробицын В.В., Ильин С.С. Реализация симметричного шифрования по алгоритму ГОСТ 28147 на графическом процессоре // Информационные технологии. 2008. № 10. С. 46-51.
3. Коробицын В.В., Ильин С.С. Реализация симметричного шифрования по алгоритму ГОСТ 28147 на графическом процессоре с использованием технологии CUDA // Информационные технологии. 2011. № 4. С. 41-46.