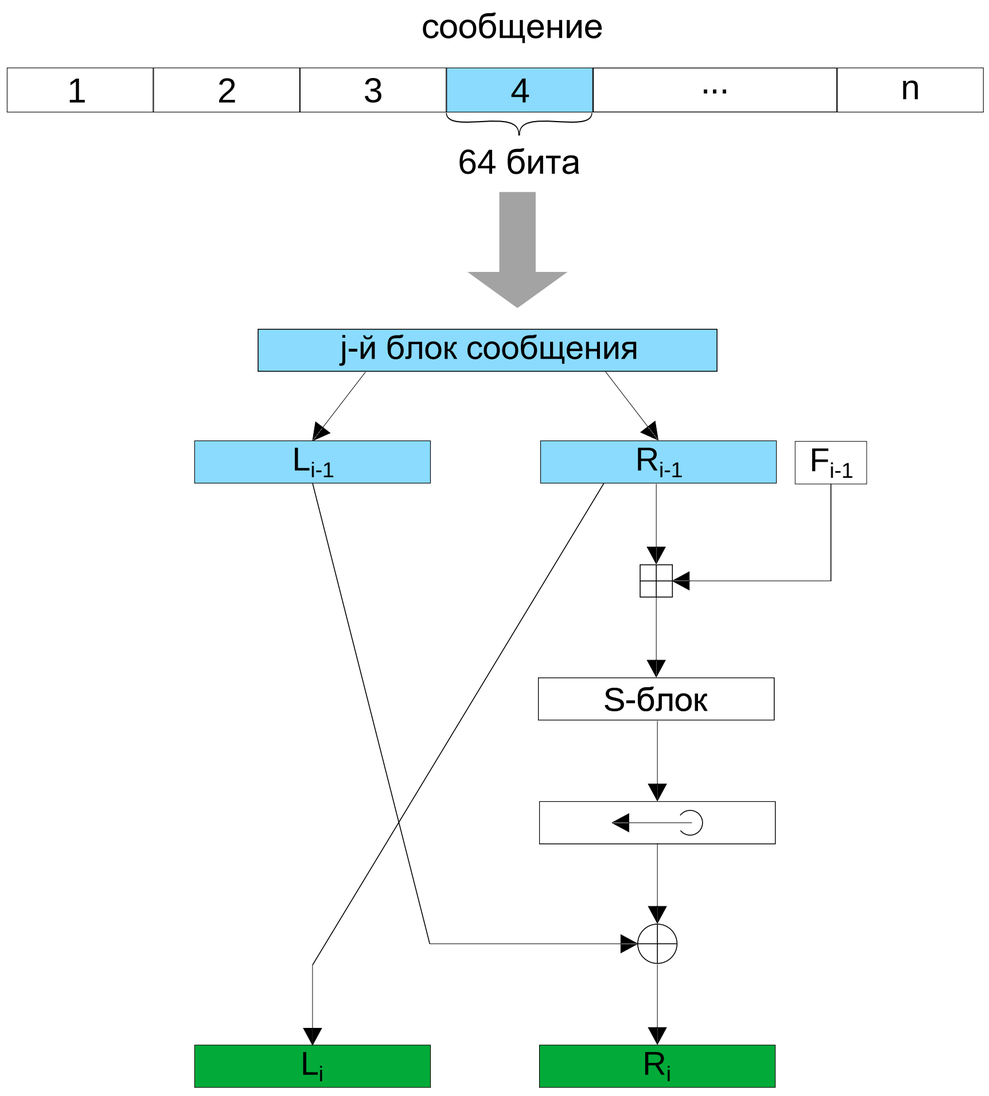
Разработка параллельного алгоритма шифрования ГОСТ 28147-89 на платформе Intel Xeon Phi

М.С. Миниахметова, М.Л. Цымблер
Южно-Уральский государственный университет

Целью данной работы является адаптация алгоритма ГОСТ для выполнения на вычислительной системе, использующей многоядерные ускорители Intel Xeon Phi.

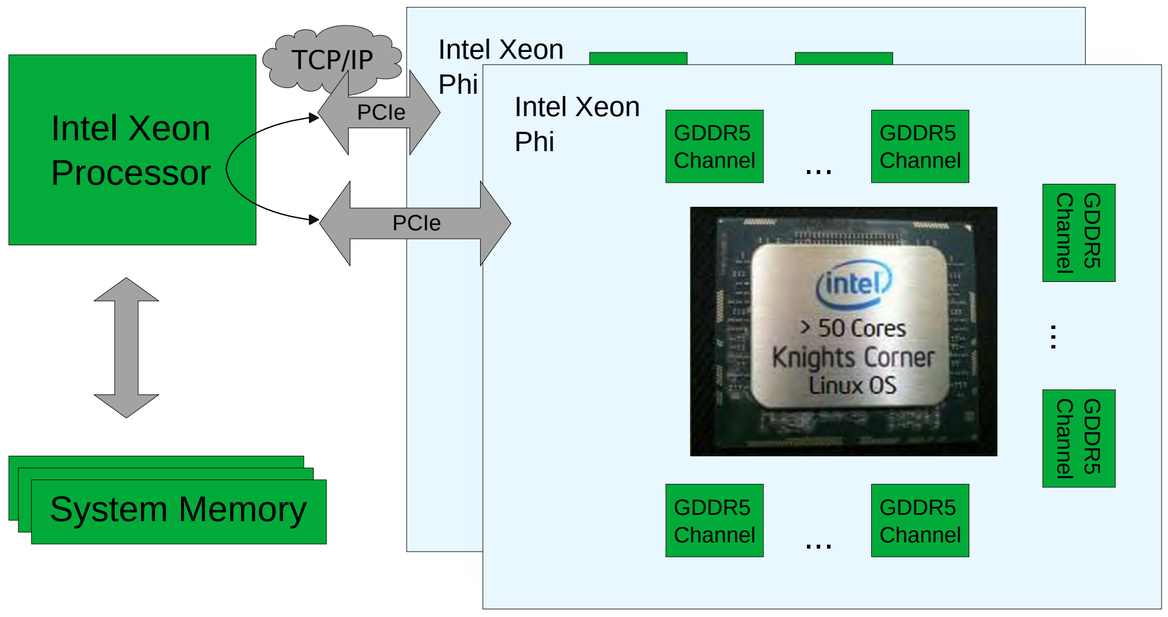
ГОСТ 28147-89

Алгоритм ГОСТ - 64-битный блочный криптографический алгоритм с 256-битным ключом.



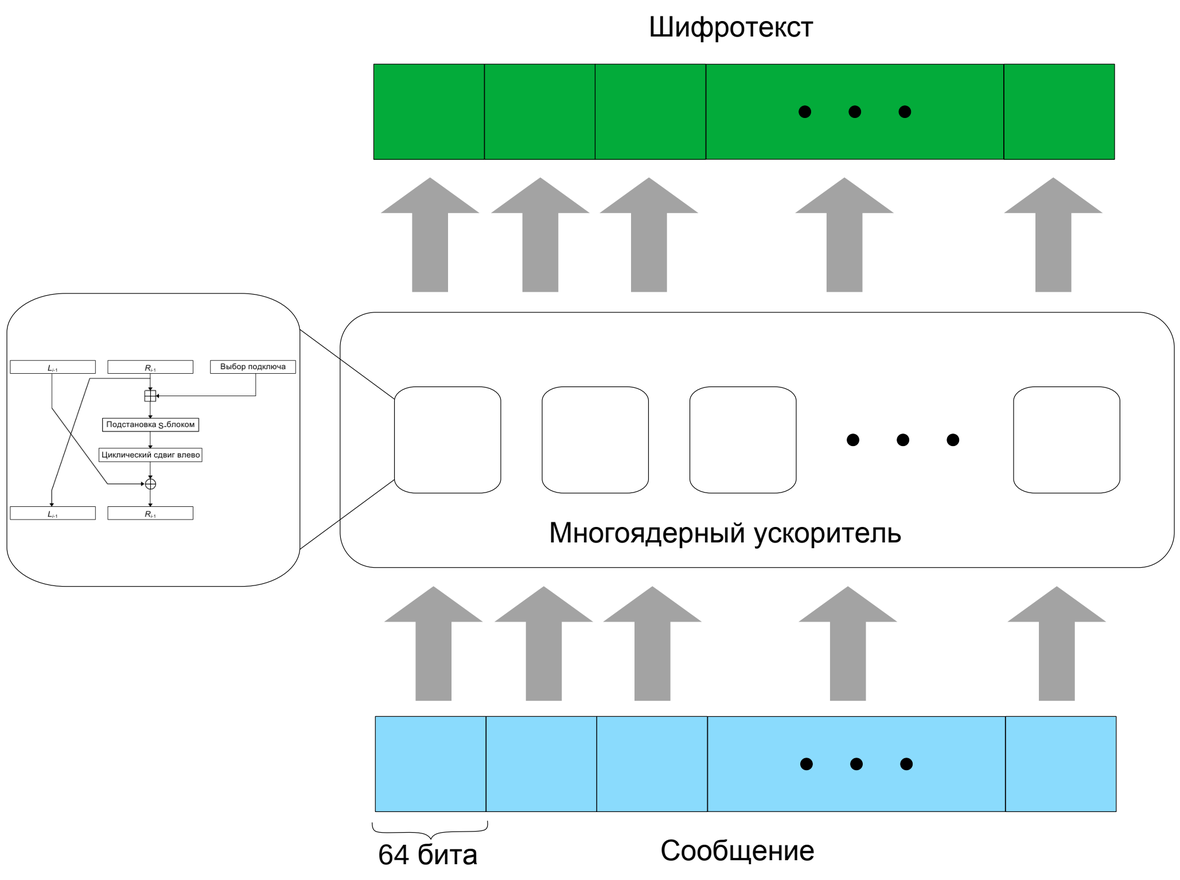
Сопроцессоры Intel Xeon Phi

Intel Xeon Phi - новейшие сопроцессоры корпорации Intel с архитектурой Many Integrated Core (Intel MIC).



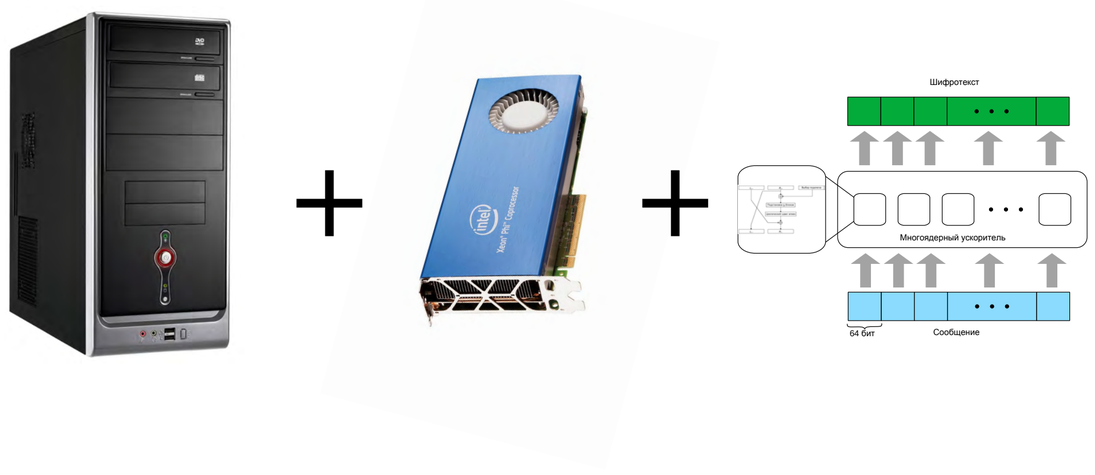
Использование в проекте Intel Xeon Phi позволяет существенно повысить производительность (до триллионов вычислений в секунду).

Параллельная реализация ГОСТ 28147-89



Независимость шифрования каждого блока от остальных позволяет реализовать параллельную обработку блоков сообщения на сопроцессоре Intel Xeon Phi.

Практическое применение: бизнес-проект «Аппаратно-программный криптошлюз на основе сопроцессоров Intel Xeon Phi»



Использование параллельного алгоритма ГОСТ 28147-89, оптимизированного для Intel MIC позволит создать эффективный и масштабируемый криптошлюз.

Сфера использования криптошлюза: госпредприятия и организации (ВПК, властные структуры и др.), которые в соответствии с законодательством должны выполнять шифрование исходящего трафика.