Московский Физико-Технический Институт
(государственный университет)

Научный проект по защите информации

name of your labwork

Авторы:
Филиппенко Павел Б01-009
Фролов Даниил Б01-009
Долгодворов Егор Б01-009
Белов Владислав Б01-009

Долгопрудный, 2023

1 Abstract

Для современных компьютерных систем важно, чтобы алгоритмы шифрования данных были не только надежными, но так же быстрыми с точки зрения вычислительных операций. В данной статье мы опишем векторную реализацию блочного шифра «Кузнечик» для процессорной архитектуры RISC-V, а так же сравним скорость ее работы с последовательной реализацией и векторной реализацией на других архитектурах.

2 Введение

В современном мире, где довольно значительную роль играют цифровые технологии, криптография является довольно важной частью обеспечения безопасности в цифровой среде. Защита интернет-соединений и каналов связи, надежность проведения банковских операций, подтверждение подлинности электронных документов. Современные методы защиты информации накладывают большое количество требований на современные алгоритмы шифрования, такие как теоретическая и вычислительная криптостойкость, а так же скорость работы.

Для современных компьютерных систем важно, чтобы алгоритмы шифрования данных были не только надежными, но так же быстрыми с точки зрения вычислительных операций. На сегодняшний день одним из популярных способов увеличения скорости работы программ является векторизация математических операций. Данный способ основывается на принципе компьютерных вычислений SIMD (анг. single instruction multiple data), позволяющем обеспечить параллелизм на уровне данных. И хотя, данный вид оптимизации требует индивидуальной реализации для разных архитектур, он является довольно мощным в плане увеличения производительности кода. Кроме того, векторизацию удобно использовать в алгоритмах с большим количеством однотипных математических операций, в частности, в алгоритмах блочного шифрования.

В данной статье мы опишем векторную реализацию блочного шифра «Кузнечик» для процессорной архитектуры RISC-V, а так же сравним скорость ее работы с последовательной реализацией и векторной реализацией на других архитектурах.

3 Шифр «Кузнечик»

Алгоритм шифрования «Кузнечик» является одним из двух шифров, принятых в 2015 г. в России в стандарт блочного шифрования ГОСТ Р 34.12-2015. «Кузнечик» относится к типу блочных симметричных шифров; это значит, что для зашифрования и расшифрования используется один и тот же ключ, и что при шифровании исходный текст разделяется на блоки фиксированной длины, каждый из которых шифруется отдельно.

На сегодняшний день, шифр все еще считается криптостойким.

4 Математическое описания шифра «Кузнечик»