УДК 004.051

ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМА AES НА ПРОЦЕССОРАХ АРХИТЕКТУРЫ RISC-V С ПОДДЕРЖКОЙ ВЕКТОРНЫХ КРИПТОГРАФИЧЕСКИХ РАСШИРЕНИЙ

Дронов В. Ю.[1]
Научный руководитель – канд. техн. наук, доцент Гирик А. В.[1]
[1]Университет ИТМО
vjdronov@yandex.ru

Работа выполнена в рамках темы НИР №623106 «Автономные интеллектуальные системы».

Введение

Реализации общеизвестных криптографических алгоритмов, таких как AES, SHA2 и других, продолжают развиваться. В 2021 году была утверждена версия 1.0 спецификации векторного расширения совершенствующейся и набирающей популярность архитектуры процессоров RSIC-V. В конце 2023 года же была утверждена спецификация векторных криптографических расширений, поддерживающих инструкции, соответствующие элементам широко используемых криптографических алгоритмов [1-2]. Учитывая относительную новизну, на момент выполнения работы встречаются широко используемые реализации, имеющие потенциальные возможности для совершенствования с учётом преимуществ и особенностей векторной обработки данных, в том числе распараллеливание вычислений. В данной работе в качестве конкретного примера рассматриваются реализации векторных криптографических алгоритмов для процессоров архитектуры RISC-V в криптографической библиотеке с открытым исходным кодом OpenSSL [3].

Основная часть

Среди возможностей повышения производительности, обнаруженных в реализациях криптографической библиотеке с открытым исходным кодом OpenSSL, были выделены следующие: понижение частоты смены векторной конфигурации инструкциями вида vset{i}vl{i}, повышение количества одновременно обрабатываемых данных и инструкций за счёт задействования различных функциональных блоков процессора, выполнение многоблочной обработки данных вместо одноблочной в процессе вычислений. Результаты оцениваются путём сравнения производительности относительно исходной версией алгоритма, а также скалярной реализацией алгоритма.

Выводы

В результате проделанной работы были выбраны реализации алгоритма AES в репозитории OpenSSL для оптимизации производительности, выявлены аспекты, требующие более глубокого исследования, а также предложены варианты усовершенствования производительности. На основании описанных способов представлено программное решение, реализующее данные оптимизации, а также выполнены соответствующие измерения результирующей производительности с применением потактового симулятора с открытым исходным кодом gem5. В ходе работы в потактовый симулятор с открытым исходным кодом gem5, используемый при измерении и оценке производительности, также была добавлена поддержка инструкций векторных криптографических расширений архитектуры RISC-V.

Литература

1. Perotti M., Cavalcante M., Wistoff N. et al. A “new ara” for vector computing: An open source highly efficient risc-v v 1.0 vector processor design // 2022 IEEE 33rd International Conference on Application-specific Systems, Architectures and Processors (ASAP). – IEEE, 2022. – P. 43-51.
2. Szymkowiak T., Isufi E., Saarinen M. J. Poster: Marian: An Open Source RISC-V Processor with Zvk Vector Cryptography Extensions // Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. – 2024. – P. 4931-4933.
3. openssl/openssl: TLS/SSL and crypto library [Электронный ресурс]. – 2026. – URL : https://github.com/openssl/openssl (дата обращения: 17.02.2026).

Дронов В.Ю. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись