УДК 004.056

РАЗРАБОТКА АППАРАТНОГО УСКОРИТЕЛЯ АЛГОРИТМА ХЕШИРОВАНИЯ ГОСТ 34.11-2018

Ануфриев И. В. (ИТМО)
Научный руководитель – к. т. н., Быковский С. В.
(ИТМО)

Введение. По мере развития технологий, встраиваемые системы находят все больше применений в самых разных областях, от сферы финансов до медицины. В таких условиях важным вопросом становится защита данных, которыми встраиваемые системы оперируют. Для обеспечения целостности данных используются криптографические хеш-функции, однако вычисление хеш-суммы является трудоёмкой задачей, требующей серьёзных временных и ресурсных затрат, что может накладывать ограничения на их применение во встраиваемых системах, нацеленных на минимальное потребление ресурсов. Создание специализированного ускорителя позволит ускорить вычисление хеш-суммы, что в свою очередь позволит использовать современные алгоритмы для обеспечения целостности данных во встраиваемых системах, повышая их безопасность.

Основная часть. Использование распространённых криптографических хеш-функций во встраиваемых системах осложняется тем, что при вычислениях хеш-сумм используются блоки большого размера (как правило, 256 или 512 бит), вследствие чего операции проводятся итеративно над меньшими порциями этих блоков. Большое количество итераций на микроконтроллерах или микропроцессорах может занимать существенное количество времени, что может сделать применение некоторых алгоритмов нецелесообразным [1]. Существуют облегчённые криптографические функции, созданные специально для встраиваемых систем, однако их использование сопряжено с определёнными компромиссами в отношении пропускной способности, потребления ресурсов или безопасности [2]. Применение стандартных хеш-функций может быть возможным при использовании специальных специальных аппаратных ускорителей. Целью данной работы является повышение безопасности встраиваемых систем с помощью функций хеширования для обеспечения целостности системного ПО на примере алгоритма ГОСТ 34.11-2018 (неофициальное название - «Стрибог»). В работе представлены результаты профилирования программной реализации данного алгоритма. Приведена микроархитектура аппаратного ускорителя для вычисления хеш-суммы с помощью ГОСТ-34.11.2018.

Выводы. В ходе исследования была разработана программная реализация алгоритма ГОСТ 34.11-2018, было проведено его профилирование. Благодаря полученным данным была дана оценка применимости алгоритма во встраиваемых системах и спроектирована микроархитектура аппаратного ускорителя для данного алгоритма. Полученная микроархитектура в дальнейшем может быть реализована с помощью языка описания аппаратуры и использована во встраиваемых системах.

Список использованных источников:

1. Cuellar C. C. Performance Analysis of Cryptographic Hash Function on 32-Bits Embedded Systems // International Journal of Difference Equations (IJDE). – 2023. – V. 18. – P. 91-106. – Режим доступа: https://www.ripublication.com/ijde23/v18n1p07.pdf (Дата обращения 17.02.2025)

2. Mufidah N.F., Nuha H.H. Performance and Security Analysis of Lightweight Hash Functions in IoT // Jurnal Informatika: Jurnal Pengembangan IT – 2024. – V. 9. – N. 3. – P. 264-270. – Режим доступа: https://ejournal.poltekharber.ac.id/index.php/informatika/article/viewFile/7633/3229 (Дата обращения 17.02.2025)