УДК 004.434

ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО ДЛЯ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ АППАРАТНЫХ УСКОРИТЕЛЕЙ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ

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

Введение

Использование криптографических хеш-функций в современных проектах и технологиях является необходимым условием для обеспечения информационной безопасности. Они являются одними из наиболее базовых криптографических примитивов, используемых в механизмах аутентификации, контроля целостности, генерации псевдослучайных чисел и криптографических ключей [1]. Тем не менее, несмотря на развитие информационных технологий и вычислительной техники, применение данных функций во встраиваемых системах все еще затруднительно.

Современные криптографические хеш-функции используют сложнообратимые математические операции над большими числами для обеспечения собственной криптографической стойкости [2]. Многие вычислительные системы ограничены по мощности, что может приводить к значительному замедлению вычислений. Кроме того, хранение статических данных, таких как раундовые константы и таблицы подстановок, требует значительных объёмов памяти, что также критично для встраиваемых систем с ограниченными ресурсами.

Основная часть

Аппаратные ускорители позволяют снять нагрузку с основной системы, сократить время вычислений и снизить энергопотребление благодаря специализированному выполнению алгоритма. Однако их реализация требует принятия множества технических решений, влияющих на итоговые показатели производительности и требовательности к ресурсам. На итоговый результат влияет большое количество параметров: последовательность операций, количество функциональных блоков и т.д. Требования разнятся от проекта к проекту, и в случае, если итоговые показатели окажутся неудовлетворительными, работа должна быть переделана. Современные стандарты языков описания аппаратуры постепенно вводят дополнительные возможности для параметризации и высокоуровневого проектирования интегральных схем, однако на данный момент этих возможностей недостаточно [3]. Целью исследования является автоматизация процесса исследования пространства проектных решений при разработке аппаратных ускорителей криптографических хеш-функций с помощью специализированного средства высокоуровневого синтеза. Такое средство будет использовать алгоритмоспецифичные оптимизации для подбора отвечающей требованиям конфигурации будущего ускорителя. В докладе приведены структура средства и результаты его профилирования, а также результаты профилирования разработанных с помощью него аппаратных ускорителей.

Выводы

В результате исследования было разработано специализированное средство высокоуровневого синтеза, позволяющее автоматизировать процесс исследования пространства проектных решений при создании аппаратных ускорителей криптографических хеш-функций. Было проведено профилирование средства и разрабатываемых с его

помощью ускорителей. Полученные данные позволяют оценить эффективность разработанного средства и его применимость для разработки широкого набора функций хеширования.

Литература

1. FIPS-202. Secure Hashing Algorithm 3: Permutation-Based Hash and Extendable-Output Functions. URL: https://csrc.nist.gov/pubs/fips/202/final (Дата обращения: 21.10.2025)

2. FIPS PUB 180-4. Secure Hash Standard (SHS). URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf (Дата обращения: 21.10.2025)

3. Numan M. W., Phillips B. J., Puddy G. S., Falkner K. Towards Automatic High-Level Code Deployment on Reconfigurable Platforms: A Survey of High-Level Synthesis Tools and Toolchains // IEEE Access. — 2020. — V. 8. — P. 174692-174722. — DOI: 10.1109/ACCESS.2020.3024098.