2. Comparing reliability and security: Concepts, requirements, and techniques / R.S. Hanmer [et al.] // Bell Labs Technical Journal. 2007. № 3. P. 65–78.

ИСПОЛНИТЕЛЬНЫЕ МЕХАНИЗМЫ МЕХАТРОННЫХ СИСТЕМ НА МНОГОКООРДИНАТНОМ КОЛЬЦЕВОМ ПРИВОДЕ

С.Е. Карпович, Г.Й. Салманзадех, М.М. Форутан

На сегодняшний день весьма актуальной является задача построения и исследования исполнительных механизмов параллельной кинематики для мехатронных систем координатных перемещений широкого спектра применений, в том числе и в технических средствах защиты информации. Они должны обеспечивать возможность структурного реконфигурирования в зависимости от требуемой реализации пространственных перемещений системы, в которую встраивается эта мехатронная система. Среди кинематических характеристик, в первую очередь, необходимо учитывать способность реализации программируемых движений с заданным числом степеней свободы, поскольку влияние данного параметра на выбор структуры, конструкции и остальные характеристики является определяющим.

Решение этой задачи нами было выполнено на структурно-топологическом уровне [1, 2], что позволило разработать концепцию построения управляемого движения в трехмерном пространстве на базе композиционного использования многокоординатного привода прямого действия и реконфигурируемых механизмов параллельной кинематики. В соответствие с этой концепцией в настоящей работе исследованы две системы перемещений, полученные нами путем реконфигурирования механизма параллельной кинематики на гибридном кольцевом приводе прямого действия.

Список литературы

1. Системы многокоординатных перемещений и исполни-тельные механизмы для прецизионного технологического оборудования / В.В. Жарский [и др.]. Минск: Бестпринт, 2013. 208 с.

2. Литвинов Е.А., Жарский В.В., Ареби М.А. Построение многокоординатной системы перемещений на базе механизма параллельной кинематики // Доклады БГУИР. 2009. № 8 (46). С. 79–84.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА DES НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Быстрое развитие систем связи и расширение использования Интернета привели к возросшей потребности в эффективной безопасности и надежности передачи, обработки и хранения данных. Алгоритмы шифрования являются одним из механизмов обеспечения этой безопасности, при этом выполнение этих алгоритмов для шифрования данных должно осуществляться в режиме реального времени. Кроме того, защищенным системам связи часто требуется способность шифровать сообщения несколькими различными алгоритмами с возможностью регулярной смены ключей. В докладе рассматривается модифицированный подход к формированию раундовых ключей, который можно использовать в различных конвейерных алгоритмах шифрования с закрытым ключом [1]. Подход поддерживает использование различных ключей в каждом такте, что повышает общую безопасность, поскольку пользователи не ограничены использованием одного и того же ключа во время любого сеанса передачи данных. Для иллюстрации способа формирования раундовых ключей используется алгоритм шифрования данных стандарта DES, который хорошо пригоден для конвейерной обработки.

В отличии от традиционного способа реализации генератора ключей алгоритма DES, который использует операции логического циклического сдвига на каждой ступени 16-ступенчатого конвейера для формирования раундовых ключей, рассматриваемый в докладе метод использует заранее сформированные для каждого раунда алгоритма DES перестановки входного ключа. Однако в отличии от [1], в модифицированном способе для правильного

формирования раундовых ключей по ступеням конвейера с использованием массива регистров перемещаются входные ключи, а не сами раундовые ключи. Такой подход позволяет получить более экономичную реализацию генератора ключей и конвейера алгоритма шифрования данных в целом.

Характеристики реализации процессора зашифрования с 32 конвейерами алгоритма DES после процесса MAP с использованием пакета ISE 14.7 для кристалла FPGA семейства Virtex7 XC7VX485T-1: 60027 триггеров секций, 48794 просмотровых таблиц (LUT), рабочая тактовая частота – 283 МГц.

Список литературы

1. McLoone M., McCanny J.V. High-performance FPGA implementation of DES using a novel method for implementing the key schedule // IEE Proc.-Circuits Devices Syst. 2003. Vol. 150, No. 5 URL: https://www.researchgate.net/ publication/3349437_High-performance_FPGA_ implementation_of_DES_using_a_novel_method_for_implementing_the_key_schedule (дата обращения: 03.05.2019).

НЕКОТОРЫЕ АСПЕКТЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА КАФЕДРЕ ИНЖЕНЕРНОЙ ПСИХОЛОГИИ И ЭРГОНОМИКИ БГУИР

П.И. Кирвель, Д.А. Мельниченко

В соответствии с Концепцией информационной безопасности Республики Беларусь цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений устойчивого развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели. Для решения этой задачи первостепенное значение имеет подготовка высококвалифицированных информационно- и практико- ориентированных специалистов в области защиты информации.

На кафедре инженерной психологии и эргономики проводится планомерная работа по подготовке специалистов в данной области: начиная с первой ступени высшего образования по специальностям «Инженерно-психологическое обеспечение информационных технологий» и «Информационные системы и технологии (в обеспечении промышленной безопасности)», с последующим углубленным обучением на второй ступени высшего образования по специальности «Управление безопасностью производственных процессов».

На кафедре разработан новый электронный учебно-методический комплекс по дисциплине «Информационные системы обеспечения безопасности» для подготовки магистров. Целью изучения данной дисциплины является формирование у магистрантов системы знаний об особенностях создания, функционирования и управления информационными системами в современных условиях развития общества, а так же освоение практико-ориентированных учебных материалов по применению инновационных стратегий, технологий и методов обеспечения безопасности в условиях производства и эксплуатации современных технических и программных средств, реализующих информационные технологии. После изучения дисциплины мы получим специалиста, обладающего комплексными предметными знаниями в области создания и управления информационными системами, адаптации и использования этих систем и технологий в профессиональной деятельности, а также имеющего навыки инновационной деятельности в области защиты информационных потоков в современных условиях развития общества.

Это, безусловно, будет способствовать формированию в Республике Беларусь прогрессивного информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и передового развития.