СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2015. – № 2(80).** – 87–95

УДК 004.31

СОЗДАНИЕ РЕКОНФИГУРИРУЕМОГО ВЫСОКОСКОРОСТНОГО КОДЕКА (ШИФРАТОРА/ДЕШИФРАТОРА)*

И.А. КАШИРИН[1], Д.Р. УСМАНОВ[2], И.Л. РЕВА[3], К.В. ЗАХАРОВ[4]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, бакалавр кафедры автоматики по направлению «Управление в технических системах». E-mail: ivakashirin@yandex.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, бакалавр кафедры автоматики по направлению «Управление в технических системах». E-mail: usmanov-denis@mail.com*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, декан факультета автоматики и вычислительной техники, доцент кафедры защиты информации. E-mail: reva@corp.nstu.ru*
[4] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: zakharov@-ft-ds.com*

Защита информации в современном мире остается наиболее важной и востребованной задачей, особенно когда это касается каналов передачи данных. В настоящее время можно найти достаточно много средств защиты каналов передачи данных как программных, так и программно-аппаратных. Программные средства защиты менее эффективны по отношению к программно-аппаратным, при этом программно-аппаратные гораздо дороже, да и почти все они иностранного производства. В работе решается ряд проблем безопасной передачи данных по оптическому каналу путем разработки реконфигурируемого высокоскоростного кодека (шифратора/дешифратора) на основе стандарта шифрования AES-128. Разработано устройство, которое с помощью оптического SFP модуля присоединяется к сетевой плате компьютера на приемной и передающей стороне, образуя тем самым защищенное соединение. Устройство сможет принимать информацию от сетевой платы и передавать далее без дополнительного драйвера, что делает его полностью универсальным. Помимо универсальной архитектуры, создание реконфигурируемого высокоскоростного кодека подразумевает создание некой логической схемы, которая включает в себя реконфигурируемую область алгоритма шифрования. Другими словами, это позволит в режиме реального времени работы устройства в зависимости от поставленной задачи изменять алгоритм шифрования. Эффективность такого подхода заключается в возможности использования множества алгоритмов шифрования. Проведено тестирование кодека на базе отладочных плат от Xilinx. Разработанное устройство в конечном итоге имеет компактные размеры, совмещает при этом уникальную архитектуру и унифицированный интерфейс.

* Статья получена 20 февраля 2015 г.

Ключевые слова: защита информации, программно-аппаратные средства, частичное реконфигурирование FPGA, шифратор/дешифратор, средство шифрования, шифрование в оптическом канале передачи данных, защищенный канал передачи данных, оптический канал

DOI: 10.17212/2307-6879-2015-2-87-95

ВВЕДЕНИЕ

Защита информации в современном мире остается наиболее важной и востребованной задачей. Решаются актуальные задачи по защите информации от утечки по техническим каналам, речевой (акустической) информации [1–7], утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) [8], защита цифровых каналов передачи данных [9]. На сегодняшний день существует множество способов и мероприятий, направленных на обеспечение защиты систем цифровой связи. К основным средствам можно отнести программные, программно-аппаратные и аппаратные средства защиты. На данный момент аппаратные средства являются более дорогостоящими, но в то же время остаются наиболее эффективными. Анализ существующего российского рынка средств защиты информации показывает, что большинство из них относятся к программным и программно-аппаратным средствам защиты, что, в свою очередь, не исключает воздействие человеческого фактора на данные устройства. Также в случае программно-аппаратных средств остается проблема универсальности данных устройств, поскольку для связи с компьютером необходимо использовать стороннее ПО разработчика устройства средства защиты. Помимо этого, данные устройства используют вычислительные ресурсы машины, к которой они подключены, что уменьшает производительность обрабатываемой информации и значительно увеличивает ее время шифрования и дешифрования. Еще одна не менее важная проблема – это скорость передачи данных, которая является достаточно низкой, и цена, которая остается очень высокой. На данный момент нет эффективных аппаратных устройств шифрования, обеспечивающих гигабитное соединение передачи данных без их задержки и имеющих приемлемую цену.

1. ОПИСАНИЕ ПРИНЦИПА РАБОТЫ РЕКОНФИГУРИРУЕМОГО ВЫСОКОСКОРОСТНОГО КОДЕКА (ШИФРАТОРА/ДЕШИФРАТОРА)

Авторами разработано устройство, которое с помощью оптического SFP модуля присоединяется к сетевой плате компьютера на приемной и передающей стороне, образуя тем самым защищенное соединение [10]. Трансивер вы-

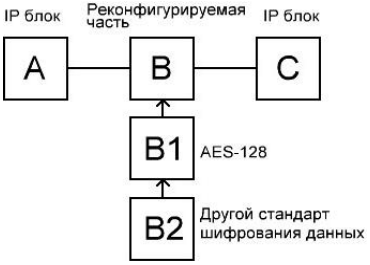
полнен на базе FPGA Artix7(XC7A15T) от Xilinx [11]. Размеры кристалла составляют 10×10 мм. Устройство сможет принимать информацию от сетевой платы и передавать далее без дополнительного драйвера, что делает его полностью универсальным.

Помимо универсальной архитектуры создание реконфигурируемого высокоскоростного кодека подразумевает создание некоего статичного дизайна схемы (логической схемы или части логической схемы), включающей в себя реконфигурируемую область алгоритма шифрования. Другими словами, это позволит в режиме реального времени работы устройства в зависимости от поставленной задачи изменять алгоритм шифрования. Эффективность такого подхода заключается в возможности использования множества алгоритмов шифрования, а также в сокращении потребления и общем снижении цены конечного устройства.

2. СОЗДАНИЕ РЕКОНФИГУРИРУЕМОГО ВЫСОКОСКОРОСТНОГО КОДЕКА (ШИФРАТОРА/ДЕШИФРАТОРА)

Инструменты для разработки реконфигурируемого высокоскоростного кодека (шифратора/дешифратора) присутствуют в современной системе автоматизированного проектирования (САПР) Vivado. В целом весь маршрут проектирования ориентирован на использование IP блоков – готовых функциональных компонентов, призванных обеспечить графическое представление проекта. Основная идея при создании высокоскоростного кодека (шифратора/дешифратора) в Vivado заключается в формировании блок-дизайна. Этот дизайн будет состоять из статичных IP блоков (стандартных блоков) и реконфигурируемых IP блоков, описанных при помощи языка HDL. Схематичное представление такого блок-дизайна изображено на рисунке. Блоки *A* и *C* являются статичными IP блоками физического уровня, которые служат в качестве интерфейса данных для блока *B*. Блок *B* является реконфигурируемым и в процессе работы устройства может быть заменен другим (например, блок *B*1 или *B*2), которые, в свою очередь, подразумевают различные алгоритмы шифрования данных, изменяющиеся в зависимости от поставленной задачи.

Генерация конфигурационного файла будет включать в себя как конфигурационный файл всего проекта, т. е., возвращаясь к примеру на рисунке (*A*, *B*, *C*), который записывается в устройство при первоначальном его программировании, так и файлы отдельных реконфигурируемых модулей (*B*1, *B*2), которые могут быть записаны в устройство в дальнейшем для изменения алгоритма работы устройства без необходимости его перезагрузки.



Схематичное представление
блок-дизайна проекта

При практической реализации высокоскоростного кодека (шифратора/дешифратора) в САПР Vivado был создан статический блок-дизайн из стандартных IP блоков и реконфигурируемый IP блок, включающий в себя стандарт шифрования AES-128. Advanced Encryption Standard (AES), также известный как Rijndael (Рэндал) – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). Данный стандарт принят в качестве стандарта шифрования Правительством США по результатам конкурса AES. Этот алгоритм достаточно хорошо зарекомендовал себя и сейчас довольно широко используется [12]. Также данный алгоритм является открытым и находится в свободном доступе.

Получившийся блок-дизайн позволяет с легкостью заменять реконфигурируемый блок на другой, при этом изменяя стандарт шифрования данных.

3. РЕЗУЛЬТАТЫ

Для тестирования высокоскоростного кодека (шифратора/ дешифратора) на основе стандарта шифрования AES-128 была использована отладочная плата Zed Board [13]. Тактовая частота отладочной платы составляет 250 Мгц. При такой частоте были получены следующие результаты: шифрование данных осуществляется за 60 тактов работы схемы, а дешифрование – за 90 тактов. Это позволяет сделать вывод о том, что скорость шифрования данных высокоскоростного кодека (шифратора/дешифратора) на основе стандарта шифрования AES-128 составляет 63,57 Мбайт/с, а скорость дешифрования данных 42,39 Мбайт/с. Поскольку реализация устройства предполагается на базе FPGA Artix7(XC7A15T), имеющей частоту тактирования в первом Speedgrade 464 Мгц [13], приблизительные скорости шифрования и дешифрования увеличатся и будут составлять 117,98 Мбайт/с и 78,67 Мбайт/с соответственно. В теории максимальная пропускная способность гигабитного соеди-

нения составляет 125 Мбайт/с, на практике данное значение достигается редко и только при идеальных условиях. Следовательно, получившиеся скорости шифрования и дешифрования приближаются к максимально возможным при использовании данного канала связи. Также был проведен анализ программы на основе метода, представленного в работах [14–15].

ЗАКЛЮЧЕНИЕ

В процессе создания реконфигурируемого высокоскоростного кодека (шифратора/дешифратора) на основе стандарта шифрования AES-128 удалось решить проблемы современных программных и программно-аппаратных средств шифрования. Разработанное устройство в конечном итоге имеет компактные размеры, совмещает при этом уникальную архитектуру и унифицированный интерфейс. Также благодаря возможности частичной реконфигурации в данном устройстве присутствует возможность смены алгоритма шифрования «на лету», что повышает его надежность.

СПИСОК ЛИТЕРАТУРЫ

1. О достоверности оценки защищенности речевой информации от утечки по техническим каналам / А.П. Бацула, А.А. Иванов, И.Л. Рева, В.А. Трушин // Доклады ТУСУР. – 2010. – № 1 (21), ч. 1. – С. 89–92.

2. *Рева И.Л.* Организация эксперимента по оценки разборчивости речи со связными текстами // Сборник научных трудов НГТУ. – 2010. – № 4 (62). – С. 125–132.

3. *Рева И.Л., Трошина Г.В.* Белый шум в задачах идентификации // Сборник научных трудов НГТУ. – 2015. – № 1 (79). – С. 7–22. – doi: 10.17212/2307-6879-2015-1-7-22.

4. *Иванов А.В., Рева И.Л., Трушин В.А*. Реализация оптимальной помехи при защите речевой информации от утечки по акустическому и виброакустическому каналам // Научный вестник НГТУ. – 2011. – № 4 (45). – С. 151–154.

5. *Трушин В.А., Рева И.Л., Иванов А.В.* О методических погрешностях оценки словесной разборчивости речи в задачах защиты информации // Доклады ТУСУР. – 2012. – № 1 (25), ч. 2. – С. 180–185.

6. *Трушин В.А., Рева И.Л., Иванов А.В*. Усовершенствование методики оценки разборчивости речи в задачах защиты информации // Ползуновский вестник. – 2012. – № 3/2. – С. 238–241.

7. Корректировка методики оценки защищенности речевой информации от утечки по техническим каналам в условиях форсирования речи / А.В. Иванов, И.Л. Рева, В.А. Трушин, У. Тудэвдагва // Научный вестник НГТУ. – 2014. – № 2 (55). – С. 183–189.

8. *Иванов А.В., Трушин В.А., Шатров Г.В.* Погрешность косвенных измерений расстояния возможного перехвата побочных электромагнитных излучений // Материалы XI международной конференции «Актуальные проблемы электронного приборостроения»: АПЭП–2012, Новосибирск, 2–4 октября, 2012 г.: в 7 т. – Новосибирск: Изд-во НГТУ, 2012. – Т. 3. – С. 150–152.

9. Цифровые каналы передачи данных: учебно-методическое пособие / сост. Д.Н. Ивлев. – Нижний Новгород: Изд-во Нижегор. гос. ун-та, 2013. – 53 с.

10. SFP модули, трансиверы SFP [Электронный ресурс] // ФТИ-оптроник: оптоэлектронные компоненты: каталог продукции. – URL: http://www.fti-optronic.com/SFP.html (дата обращения: 31.05.2015).

11. All programmable 7 series. Product selection guide [Electronic resource] / Xilinx. – San Jose, California, USA, 2014. – 10 p. – URL: http: //spotidoc.com/doc/678270/all-programmable-7-series-product-selection-guide (accessed: 31.05.2015).

12. *Пан К.С., Цымблер М.Л.* Алгоритм блочного симметричного шифрования Advanced Encryption Standard (AES): технический отчет CELLAES-01 [Электронный ресурс] / Южно-Уральский государственный университет, кафедра системного программирования. – Челябинск, 2009. – 14 с. – URL: http://pcs.susu.ru/projects/3/aes.pdf (дата обращения: 31.05.2015).

13. Zedboard [Electronic resource]: official website. – URL: http://zedboard.org/ (accessed: 31.05.2015).

14. *Воевода А.А., Романников Д.О.* О методе анализа программ // Сборник научных трудов НГТУ. – 2014. – № 4 (78). – С. 125–138. – doi: 10.17212/2307-6879-2014-4-125-138.

15. *Воевода А.А., Романников Д.О.* Способы представления программ и их анализ // Сборник научных трудов НГТУ. – 2014. – № 3 (77). – С. 81–98.

Усманов Денис Рафикович – бакалавр кафедры автоматики по направлению «Управление в технических системах» Новосибирского государственного технического университета. E-mail: usmanov-denis@mail.com

Каширин Иван Андреевич – бакалавр кафедры автоматики по направлению «Управление в технических системах» Новосибирского государственного технического университета. E-mail: ivakashirin@yandex.ru

Рева Иван Леонидович – кандидат технических наук, декан факультета автоматики и вычислительной техники Новосибирского государственного технического университета. Основное направление научных исследований – защита информации. Имеет более 20 публикаций. E-mail: reva@corp.nstu.ru

Захаров Константин Владимирович – аспирант кафедры защиты информации Новосибирского государственного технического университета. E-mail: zakharov@ft-ds.com

The creation of high-speed reconfigurable codec (encoder / decoders)*

I.A. Kashirin[1], D.R. Usmanov[2], I.L. Reva[3], K.V. Zaharov[4]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, bachelor of Automation department by control in technical systems specialty. E-mail: ivakashirin@yandex.ru*

[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, bachelor of Automation department by control in technical systems specialty. E-mail: usmanov-denis@mail.com*

[3] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, Ph. D. (Eng.), dean, faculty of automation and computer engineering, associate professor of the information Security department. E-mail: reva@-corp.nstu.ru*

[4] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, post graduate student information security department. E-mail*: *zakharov@ft-ds.com*

Protection of information in the modern world it is an important and relevant challenge, especially when it comes to data transmission channels. Currently, you can find a lot of means of protection of data transmission channels, software and hardware - software. Software means of protection less efficient with respect to the hardware – software. Software - hardware is much more expensive, and almost all of them are of foreign manufacture. The paper solves a number of problems of secure data transmission on the optical channel through the development of high-speed reconfigurable codec (encoder / decoder) based on the encryption standard AES-128. Developed the device that is using the optical SFP module is attached to a computer network adapter for transmitting and receiving, thereby forming a secure connection. The device able to receive information from network card and pass on without additional driver. This makes it completely universal. In addition to a universal architecture, the creation of high-speed reconfigurable codec involves the creation of a kind of logical scheme, which includes the area of reconfigurable encryption algorithm. This will allow mode of the device, depending on the task, to change the encryption algorithm. The effectiveness of this approach lies in the possibility using multiple encryption algorithms. Testing of the codec the boards Xilinx. The results of the study. Invented device ultimately is compact, thus combining the unique architecture and unified interface.

* *Received 20 February 2015.*

Keywords: protection of information, software - hardware, partial reconfiguration FPGA, encoder / decoder, encryption tool, encryption in the optical data transmission channel, protected data transmission channel, optical channel

DOI: 10.17212/2307-6879-2015-2-87-95

REFERENCES

1. Batsula A.P., Ivanov A.A., Reva I.L., Trushin V.A. O dostovernosti otsenki zashchishchennosti rechevoi informatsii ot utechki po tekhnicheskim kanalam [The reliability of estimate of security of voice information from leaking by technical channels]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki – Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2010, no. 1 (21), pt. 1, pp. 89–92.

2. Reva I.L. Organizatsiya eksperimenta po otsenki razborchivosti rechi so svyaznymi tekstami [The organization of experiment according to legibility of speech with texts coherent]. *Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2010, no. 4 (62), pp. 125–132.

3. Reva I.L., Troshina G.V. Belyi shum v zadachakh identifikatsii [White noise in the identification problem]. *Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2015, no. 1 (79), pp. 7–22. doi: 10.17212/2307-6879-2015-1-7-22

4. Ivanov A.V., Reva I.L., Trushin V.A. Realizatsiya optimal'noi pomekhi pri zashchite rechevoi informatsii ot utechki po akusticheskomu i vibroakusticheskomu kanalam [Optimum noise detection for voice data protecting from leaking through acoustic and vibroacoustic channels]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Science Bulletin of the Novosibirsk state technical university*, 2011, no. 4 (45), pp. 151–154.

5. Trushin V.A., Reva I.L., Ivanov A.V. O metodicheskikh pogreshnostyakh otsenki slovesnoi razborchivosti rechi v zadachakh zashchity informatsii [Method errors of estimate of speech intelligibility for information security]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki – Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2012, no. 1 (25), pt. 2, pp. 180–185.

6. Trushin V.A., Reva I.L., Ivanov A.V. Usovershenstvovanie metodiki otsenki razborchivosti rechi v zadachakh zashchity informatsii [Improvement of methods for estimating intelligibility of speech in problems of information security]. *Polzunovskii vestnik – Polzunov Bulletin*, 2012, no. 3–2, pp. 238–241.

7. Ivanov A.V., Reva I.L., Trushin V.A., Tudevdagva U. Korrektirovka metodiki ocenki zashhishhennosti rechevoj informacii ot utechki po tehnicheskim

kanalam v uslovijah forsirovanija rechi [Corrected methods for the assessment of audio information security against leakage through engineering channels for forced speech]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Science Bulletin of the Novosibirsk state technical university*, 2014, no. 2 (55), pp. 183–189.

8. Ivanov A.V., Trushin V.A., Shatrov G.V. [Indirect measurements error of the possible interception distance of compromising emanation]. *Materialy XI mezhdunarodnoi konferentsii «Aktual'nye problemy elektronnogo priborostroeniya»: APEP–2012*, Novosibirsk, 2–4 oktyabrya, 2012 g. V 7 t. [11th International Conference on Actual Problems of Electronics Instrument Engineering: proceedings, 2–4 October 2012. In 7 vol.], Novosibirsk, Russia, 2012, vol. 3, pp. 150–152. (In Russian)

9. Ivlev D.N., comp. *Tsifrovye kanaly peredachi dannykh* [Digital data transmission channels]. Nizhnii Novgorod, Nizhegorodskii gosuniversitet Publ., 2013. 53 p.

10. SFP moduli, transivery SFP [SFP modules, transceivers CFP]. *FTI-optronik: optoelektronnye komponenty: katalog produktsii* [PTI-optronics: optoelectronic components: product catalog]. Available at: http://www.fti-optronic.com/SFP.html (accessed 31.05.2015)

11. *All Programmable 7 Series. Product Selection Guide*. San Jose, California, USA, Xilinx, 2014. 10 p. Available at: http: //spotidoc.com/doc/678270/all-programmable-7-series-product-selection-guide (accessed 31.05.2015)

12. Pan K.S., Tsymbler M.L. *Algoritm blochnogo simmetrichnogo shifrovaniya Advanced Encryption Standard (AES): tekhnicheskii otchet CELLAES-01* [Algorithm block symmetric encryption Advanced Encryption Standard (AES). Technical report CELLAES-01]. Chelyabinsk, South Ural State University, Department of System Programming, 2009. Available at: http://pcs.susu.ru/projects/3/aes.pdf (accessed 31.05.2015)

13. *Zedboard*: official website. Available at: http://zedboard.org/ (accessed 31.05.2015).

14. Voevoda A.A., Romannikov D.O. O metode analiza programm [About the method of program analysis]. *Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2014, no. 4 (78), pp. 125–138. doi: 10.17212/2307-6879-2014-4-125-138

15. Voevoda A.A., Romannikov D.O. Sposoby predstavleniya programm i ikh analiz [Methods of program representation and analysis]. *Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2014, no. 3 (77), pp. 81–98.