РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

УДК 004.056.5

РАЗРАБОТКА СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ВЫСОКОСКОРОСТНЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Шаги Л.М.
Студент 4 курса Евразийского национального университета им. Л.Н.Гумилева
Научный руководитель – Атанов С.К.

Введение

В наши дни ощущается необходимость постоянно совершенствовать методы защиты информации. Бурный рост производительности плохо сказывается на стойкости алгоритмов шифрования. Но всегда наряду со стойкостью шла скорость этих алгоритмов, так как информация может потерять актуальность за время процесса шифрования. Скорость – немаловажная характеристика, особенно, когда речь идет о высокоскоростных каналах передачи данных. Более того, мы наблюдаем, как растет качество изображений, аудио и видео, что в свою очередь порождает нужду в шифровании данных колоссальных масштабов за короткий промежуток времени.

Гибридные вычислительные системы на основе ПЛИС

Программируемая логическая интегральная схема (ПЛИС) – электронный компонент, используемый для создания цифровых интегральных схем. В отличие от обычных цифровых микросхем, логика работы ПЛИС не определяется при изготовлении, а задаётся посредством программирования (проектирования), как сказано в [1].

Современные вычислительные системы с высокой производительностью стремятся к гибридизации, как показано в работе. Применение специализированных вычислителей позволяет использовать их преимущества и компенсирует недостатки универсальных процессоров, одним из которых является высокая потребляемая мощность. В составе гибридных систем наряду с другими могут использоваться вычислители на базе программируемых логических интегральных схем (ПЛИС). Они позволяют создать аппаратную реализацию алгоритмов, благодаря возможности конфигурации микросхемы. Традиционно на подобной элементной базе эффективно реализуются алгоритмы потоковой обработки информации, допускающие конвейеризацию. Российские ученые в своих исследованиях [2] добились повышения вычислительной мощности до 200 раз, используя гибридную систему.

Такой скачок в производительности дает нам возможность беспрепятственно шифровать данные высокоскоростных каналов. Еще одним из примеров аппаратной реализации алгоритмов шифрования может послужить работа ученных из Индии [3], где они подробно описали процесс аппаратной реализации потокового алгоритма шифрования RC4. Данная реализация была основана на так называемых Block Random Access Memory(BRAM), которые были использованы как аппаратная версия S-box. В результате им удалось добиться скорости 3 такта на символ зашифрованного сообщения. Что примечательно, у алгоритма RC4 ключ с переменной длиной от 1 до 256, и то, что производительность такой вычислительной системы можно экстенсивно увеличивать, путем расширения ОЗУ.

Так же одним из достоинств гибридных вычислительных систем является малое потребление энергии. Как описано в совместной статье исследователей из Америки и Иордании, создание гибридной системы позволило им уменьшить потребление энергии в 60%. В своих исследованиях они реализовали алгоритм шифрования HIGHT. Этот алгоритм шифрования отличается тем, что он в основном применяется для устройств с ограниченными ресурсами. Как заметили в работе [4], с каждым днем на свет производиться всё больше и больше устройств с ограниченными ресурсами, которые требуют не меньшей защиты информации.

Легко заметить, что данная практика использования ПЛИС для ускорения алгоритмов шифрования наблюдается по всему миру. Как подчеркнул исследователь из Китая, в своей

работе [5], нетрудно было предсказать, что алгоритм AES будет играть важную роль в области информационной безопасности в течении долгого времени в будущем после того, как алгоритм Rijndael был объявлен как расширенный стандарт шифрования. Аппаратная реализация на основе ПЛИС алгоритма AES имеет преимущества скорости, гибкости, короткого цикла разработки и т. д.

Исследователи из Индии не стоят на месте. В работе [6] они четко показали эффективность реализации алгоритма AES на ПЛИС, утверждая тот факт, что алгоритмы можно реализовывать программным путем и чисто аппаратным, а ПЛИС является оптимальным и быстрым решением. В своих опытах они реализовали алгоритм с 128 битовым блоком и 128 битовым ключом. А результаты работы были проверены наборами текстов и шифртекстов предоставленными Национальным институтом стандартов и технологий США(NIST).

В общих чертах, существует уже не мола подобных попыток реализации различных алгоритмов шифрования на гибридных системах с использование ПЛИС, которые существенно повышают скорость шифрования данных. Применяя такие гибридные системы можно обеспечить криптографическую защиту высокоскоростным каналам передачи данных, используя меньше вычислительных ресурсов, энергии и финансов, так как ПЛИС являются одновременно дешевым и эффективным решением. Шифрование изображений со спутника или беспилотных летательных аппаратов в высоком качестве, дабы сохранить актуальность информации, должны передаваться через высокоскоростные каналы передачи данных, и, чтобы справиться с таким потоком, необходима соответствующая скорость шифрования этой информации, которую могут обеспечить выше описанные гибридные системы на основе ПЛИС. И конечно не стоит забывать, что аппаратная реализация алгоритма автоматический защищает от программного вмешательства злоумышленников.

Мы проверили нашу программную реализацию на файлах изображения. Сравним наши исходные и конечные файлы изображения. Результаты представлены на рисунки 6.

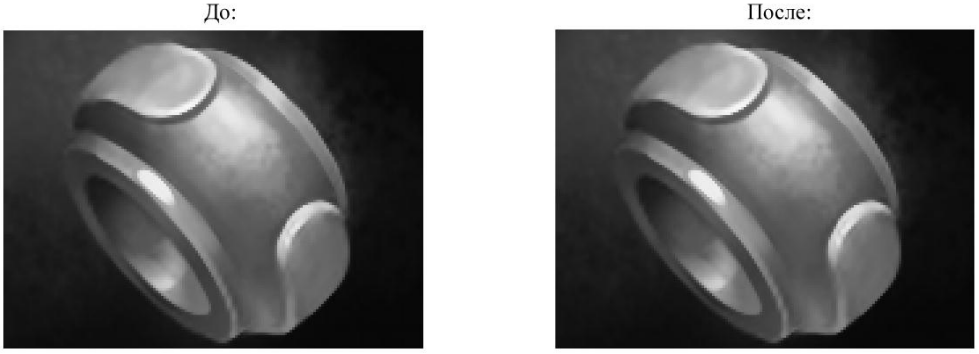


Рисунок 1 – Результаты операций шифрования и дешифрования файла изображения

Как видно, исходное и конечное изображение идентичны. На шифрование данного рисунка, размером в 25339 байт, программе потребовалось 32мс времяни, а для дештфрование 42 мс. Быстро, но недостаточно, так как данная программа исполнялась на универсальном процессоре. Если вынести этот алгоритм на ПЛИС, то результаты могут ускориться в до 200 раз. Если программа будет шифровать потоковое видеовещание, то она должна работать с токой скоростью, которая сможет обеспесить комфортную частоту обновления кадров (30-60 кадр/сек).

Реализаци алгоритма шифрования на ПЛИС

После мы взялись за разработку собственного симметричного алгоритма шифрования на основе AES, но всего лишь для 12 битной длины блока, так как у микроконтроллера, который мы используем АЦП и ЦАП 12-ти битной разрядности. Реализовав алгоритм на микроконтроллере, и оптимизировав код программы, мы добились результатов, которые по-прежнему нас не устраивали. В следствии, мы решились на реализацию нашего алгоритма на

ПЛИС. Для начала мы реализовали схему на логических элементах в MultiSim. Ниже на рисунке представлена схема реализации алгоритма.

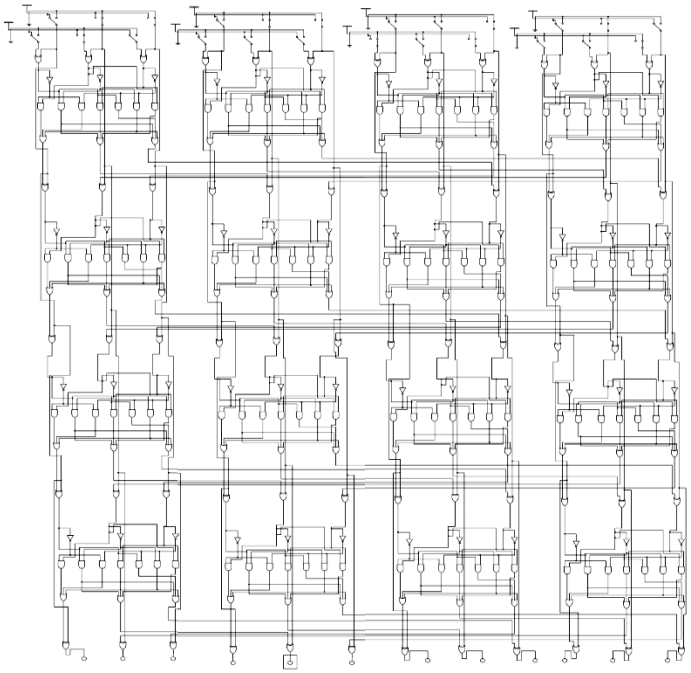
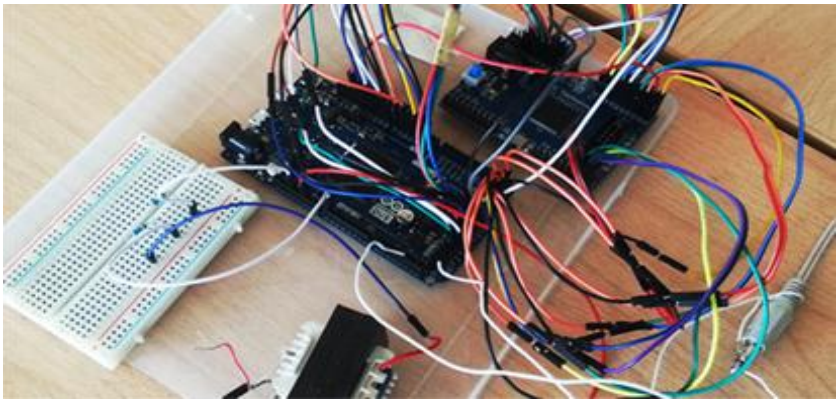


Рисунок 2 – Схема реализации алгоритма

Данную схему мы перенесли на среду разработки Quartus и прошили её в ПЛИС. Так мы добились практически моментального шифрования 12 битного входа с 12 битным ключом.



После надо было лишь организовать передачу данных, и эту задачу мы предоставили микроконтроллеру, и в итоге получили гибридную вычислительную систему.

Заключение

Информационная безопасность является одним из важнейших факторов успешного функционирования любой системы. Всякое нарушение целостности информации, её хищение и уничтожение может повлечь за собой сбой работоспособности, что приведет к краху системы. В этой статье были описаны различные попытки аппаратных реализации алгоритмов шифрования на основе ПЛИС. Подобные решения в мировой практике показывают ряд преимуществ по сравнению с универсальными процессорами, в частности, как скорость шифрования.

Выбор и использование оптимальной криптосистемы является наиважнейшим шагом для достижения безопасности данных и их передачи. Подобные криптосистемы являются решением для шифрования данных высокоскоростных каналов. В итого можно сказать, что

это была попытка пожертвовать универсальностью для достижения высокой производительности.

Список использованных источников

1. Угрюмов Е. П. Глава 7. Программируемые логические матрицы, программируемая матричная логика, базовые матричные кристаллы / Цифровая схемотехника. Учеб. пособие для вузов. Изд.2, БХВ-Петербург, 2004. С. 357.

2. А.Е. Андреев, Е.И. Духнич, В.А. Егунов, Д.Н. Жариков, С.В. Ноздренков. Реализация шифрования с использованием кватернионов на схемах программируемой логики с помощью Altera OpenCL SDK // Параллельные вычислительные технологии (ПаВТ'2016). Т. 1576, Архангельск, Март 2016. С. 396–401.

3. Chandra Mouli.R, K.R.K.Sastry. Hardware Implementation of High Speed RC4 Algorithm in FPGA // International Journal of Computer Applications (0975 – 8887). Volume 83 – No4, December 2013. P. 20–23.

4. Bassam Jamil Mohd, Thaier Hayajneh, Zaid Abu Khalaf, Khalil Mustafa Ahmad Yousef. Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation // Security and Communication Networks. Volume 9, Issue 13, 10 September 2016. P. 2200–2216.

5. Shi-hai Zhu. Hardware Implementation Based on FPGA of AES Encryption and Decryption System // Scholars Journal of Engineering and Technology (SJET).Vol. 2, Hangzhou, 2014. P. 352–357.

6. Kirat Pal Singh, Shiwani Dod. An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm // International Journal of Recent Advances inEngineering & Technology (IJRAET). Volume 4, Issue 2, Gurgaon, February 2016. P. 5–9.

МОДЕЛИРОВАНИЕ АРХИТЕКТУРЫ КОРПОРАТИВНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СРЕДЫ EVE-NG

Морозинский[*] А. А., Сатыбалдина Д.Ж.
*Национальный исследовательский ядерный университет «МИФИ», Москва, РФ
Евразийский национальный университет имени Л.Н. Гумилева, Астана, РК
E-mail: morozinskiy@mail.ru

Развитие и распространение цифровых технологий оказывают глубокое влияние на различные сектора экономики, приводя к сокращению издержек, повышению общей эффективности, вытеснению посредников, сокращению времени и расширению коммуникаций. Кроме этого тенденции глобализации значительно увеличивают масштабы и сложность современных предприятий, многие из которых преобразованы распределенные корпоративные структуры. В настоящее время взаимодействие распределенных бизнес структур в большинстве случаев реализуется путем формирования виртуальных частных сетей на базе транспортных структур технологии IP/MPLS [1]. Единой талонной архитектуры для IP/MPLS - магистралей не существует. Для корпоративных сетей связи необходимо находить индивидуальные решения с учетом различных факторов, например, особенности распределения трафика, необходимый уровень качества обслуживания, существующая транспортная инфраструктура традиционных операторов связи.

В связи с этим в данной работы разработка архитектуры корпоративной сети связи для одной из горнодобывающих компаний Республики Казахстан на основе визуального проектирования и эмуляции на платформе EVE-NG.