УДК

Электронный ключ на базе программно-аппаратной синхронизации цепей Чуа

К.В. Кузнецов, В.В. Перепеловский

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Аннотация: в данной работе представлена концепция электронного ключа на базе программно-аппаратной синхронизации осцилляторов Чуа. Данный электронный ключ представляет собой две цепи Чуа, взаимодействующих по тракту аналого-цифрового преобразования, где передающая система является аппаратной реализацией цепи Чуа, принимающая система программной реализацией цепи Чуа.

Ключевые слова: динамический хаос, нелинейная динамика, синхронизация хаотический систем, цепь Чуа, аналого-цифровое преобразование, электронный ключ

1. Введение

Разработка криптографических систем на базе хаотических сигналов в последнее время обретает все большую актуальность, отражая стремление к повышению эффективности защиты информации в условиях ее экспоненциального роста и возрастающей ценности [1-3]. В этом контексте, ключевым элементом системы защиты данных выступают электронные ключи. Они представляют собой специализированные устройства, разработанные для обеспечения защиты программного обеспечения и приложений, доступ к которым должен оставаться ограниченным. Применение электронных ключей направлено на предотвращение неавторизованного распространения и копирования программного обеспечения, а также нелегального использования программ и устройств [4].

В данной работе анализируется электронный ключ, не подлежащий программированию, что обеспечивает его устойчивость к программным атакам. Основой концепции является использование системы, состоящей из приемника и передатчика хаотических сигналов. В качестве генератора хаотических сигналов предложено использовать электрическую цепь Чуа, отличающуюся простотой реализации и способностью к демонстрации динамики. Реализация приемника сигнала может быть выполнена на основе программной версии осциллятора Чуа. Ключевым аспектом системы является необходимость программно-аппаратной синхронизации между приемником и передатчиком для обеспечения передачи данных. Доступ к защищаемой информации обеспечивается при достижении состояния эквивалентности и полной синхронизации между осцилляторами [5].

Целью данного исследования является демонстрация разработки и реализации экспериментального стенда электронного ключа, основанного на синхронизации двух осцилляторов Чуа через интегрированную программно-аппаратную платформу.

В настоящем исследовании разрабатывается и представляется концепция электронного ключа, основанного на принципе программно-аппаратной синхронизации осцилляторов Чуа. Этот электронный ключ состоит из двух взаимосвязанных цепей Чуа, которые взаимодействуют через канал аналого-цифрового преобразования. Система передачи реализована в виде аппаратной цепи Чуа, в то время как система приема осуществляется через программную реализацию той же цепи.

2. Разработка и тестирование стенда для синхронизации цепей Чуа на основе программно-аппаратного взаимодействия

Подробная блок-схема рассматриваемого стенда приведена на рис. 1:

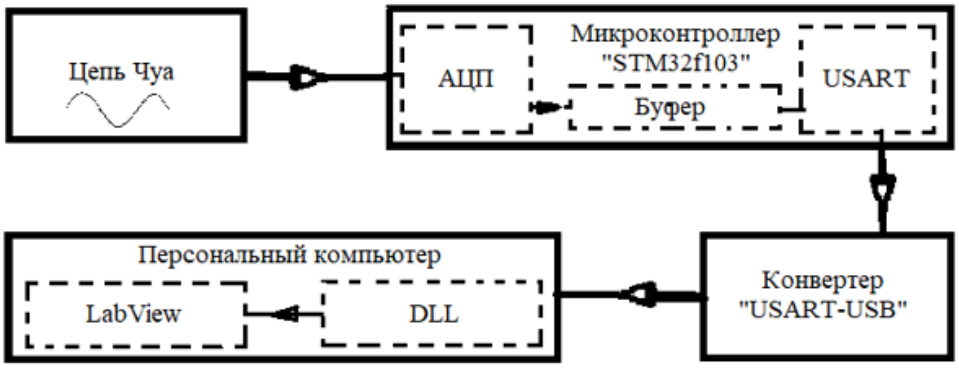

Рисунок 1. Блок-схема стенда «Программно-аппаратная синхронизация осцилляторов Чуа».

Схема Чуа была изготовлена с помощью лазерно-утюжной технологии (ЛУТ). Применение данной технологии позволило получить миниатюрную версию электрической цепи Чуа в форм-факторе «USB flash driver» (рисунок 2).

Рисунок 2. Миниатюрная версия электрической цепи Чуа в форм-факторе USB flash driver.

Для проверки корректности монтажа, был получен сигнал, демонстрирующий хаотическую динамику осциллятора (рис. 3):

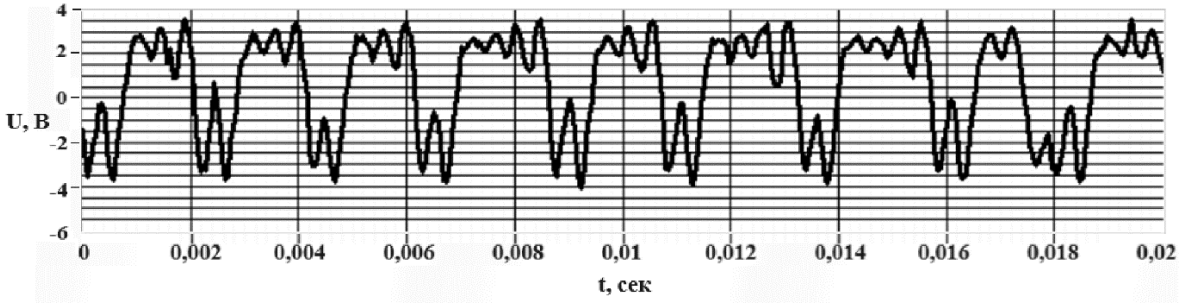

Рисунок 3. Хаотический сигнал сконструированной цепи Чуа.

Для аналого-цифрового преобразования сигнала цепи Чуа был выбран аналого-цифровой преобразователь (АЦП), входящий в состав периферийных устройств микроконтроллера STM32F102C6T6. Выбор данного АЦП был обусловлен соответствием его технических характеристик условиям возникновения программно-аппаратной синхронизации осцилляторов Чуа.

Стоит отметить, что для корректного аналого-цифрового преобразования сигнала цепи Чуа перед входом АЦП следует установить масштабирующую схему. Данная схема позволяет изменить диапазон входного напряжения АЦП.

На рис. 4 представлена аппаратная реализация испытательного стенда электронного ключа на базе программно-аппаратной синхронизации осцилляторов Чуа:

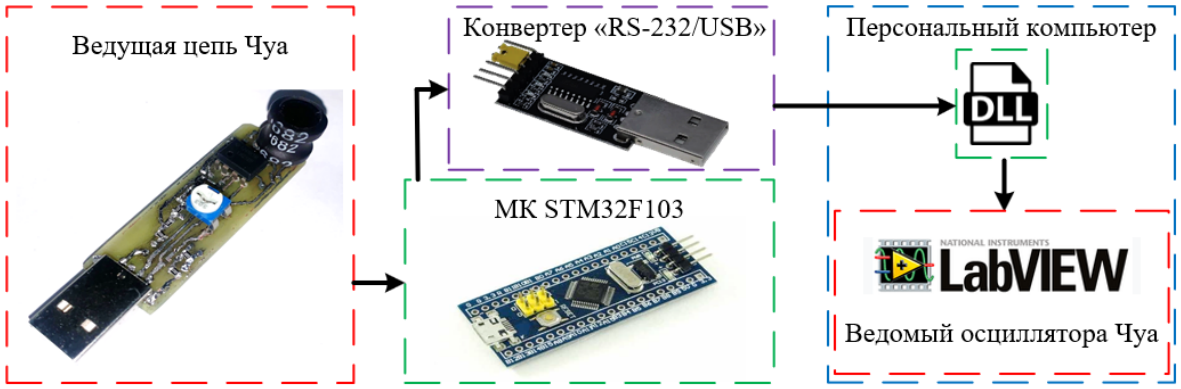

Рисунок 4. Итоговая реализация аппаратной реализации испытательного стенда.

В рамках представленной концепции, процесс авторизации доступа к защищенной информации осуществляется на основе анализа дисперсии разности фаз между ведущим и ведомым осцилляторами Чуа. Для этого используется критерий синхронизации D, значение которого устанавливается исходя из специфических параметров анализируемых систем Чуа. Этот подход позволяет оценить степень синхронизации между осцилляторами, предоставляя или ограничивая доступ к информации в зависимости от соответствия измеренной дисперсии установленному пороговому значению D.

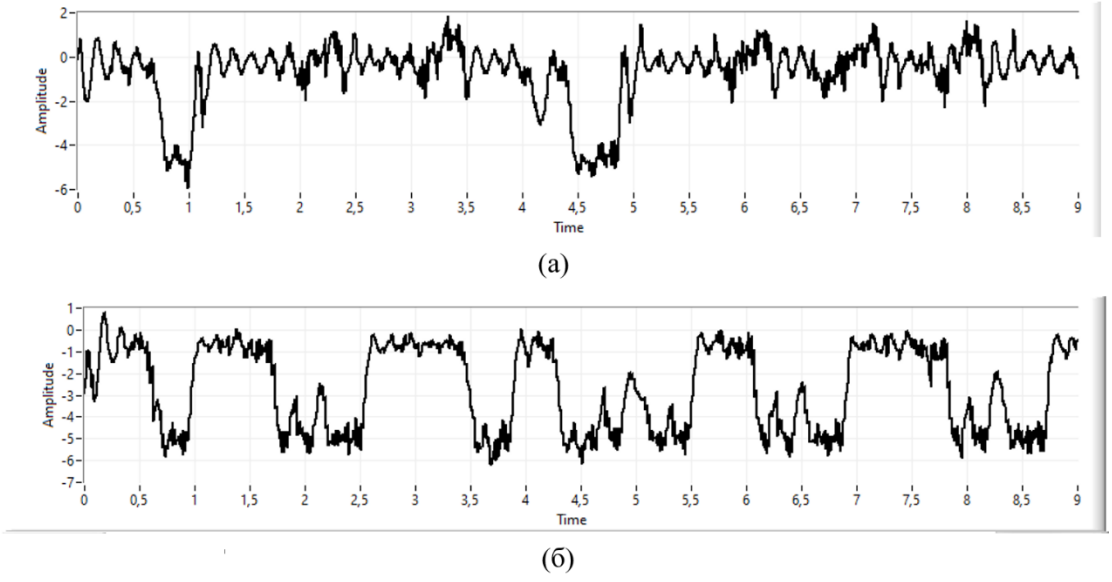

Рисунок 5. Визуализация работы электронного ключа на основе синхронизации осцилляторов Чуа с программно-аппаратной интеграцией. Показана разность значений ведомой и ведущей систем Чуа: (а) при идентичных параметрах; (б) при различиях в параметрах.

На рисунке 5 демонстрируются два режима функционирования электронного ключа на основе осцилляторов Чуа: (а) синхронизация ведущего осциллятора с ведомым, подтверждающая их параметрическую идентичность и, соответственно, авторизующая доступ к защищаемой информации; (б) наблюдаемое отсутствие синхронизации между осцилляторами свидетельствует о различии их параметров, что влечет за собой блокировку доступа к конфиденциальным данным.

3. Заключение

В данном исследовании была представлена концепция и практическая реализация электронного ключа, основанного на принципах программно-аппаратной синхронизации, используя цепи Чуа в качестве основного элемента. Разработка включала создание миниатюрной модели электрической цепи Чуа, интегрированной в форм-фактор USB-накопителя, которая функционировала как ведущий элемент системы. Особое внимание было уделено методологии взаимодействия между электронной и программной реализациями цепей Чуа, что позволило продемонстрировать потенциал данного подхода в создании надежных средств защиты информации.

Список литературы

1. Гребенев, М.С., А.В. Кондрашов, В.В. Перепеловский. "Передача двоичных данных на хаотически сформированных несущих частотах." // Известия высших учебных заведений России. Радиоэлектроника 5 (2018): 5-12.
2. Короновский, А.А., О.И. Москаленко, А.Е. Храмов. "О применении хаотической синхронизации для скрытой передачи информации." // Успехи физических наук 179.12 (2009): 1281-1310.
3. Соколова, В.К., А В. Кондрашов, А.Б. Устинов. "Передача цифрового сигнала в системе связанных хаотических осцилляторов."
4. Скляров Д. В. "Аппаратные ключи защиты "// Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. 288 с.
5. Кузнецов, К. В., В. В. Перепеловский. "Моделирование программно-аппаратной синхронизации осцилляторов Чуя."
6. R. C. Qiu et al., "Cognitive Radio Network for the Smart Grid: Experimental System Architecture, Control Algorithms, Security, and Microgrid Testbed," // IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 724-740, Dec. 2011, doi: 10.1109/TSG.2011.2160101.
7. Бутусов Д.Н., Каримов А.И., Тутуева А.В., Красильников А.В., Горяинов С.В., Вознесенский А.С. — Гибридное моделирование системы Рёсслера посредством синхронизации аналоговой и дискретной моделей // Программные системы и вычислительные методы. – 2018. – № 4. – С. 1 - 14. DOI: 10.7256/2454-0714.2018.4.27828
8. Chua L. O. et al. A universal circuit for studying and generating chaos. I. Routes to chaos //IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. – 1993. – V. 40. – №. 10. – P. 732-744
9. Астахов, В.В., и др. "Управление и синхронизация хаоса в системе связанных генераторов." // Радиотехника и электроника 41.11 (1996): 1323-1331.
10. Федерков Б.Г., Телец В.А., "Микросхемы ЦАП и АЦП: функционирование, параметры, применение" // М.: Энергоиздат, 1990. –320с
11. Шабунин, А. В. "Управление мультистабильностью и вынужденная синхронизация в связанных автоколебательных системах с бифуркациями удвоений периода." // Известия высших учебных заведений. Прикладная нелинейная динамика 20.2 (2012): 29-39.
12. Дмитриев А. С., Панас А.И. Динамический хаос: новые носители информации для систем связи.— М. \\ Издательство Физико-математической литературы, 2002.—252 с.—ISBN 5-94052-066-9