К. В. Захарченко

# АППАРАТНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

*В настоящее время становится актуальным использование электронной цифровой подписи, получившей широкое распространение в наше время. Поскольку электронный документ без подписи является просто текстовым файлом, не несущим в себе никакой юридической силы, с нанесением такой подписи, он получает гораздо большую силу и функциональность.*

## Введение

Электронная подпись представляет собой реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭП и проверить принадлежность подписи владельцу сертификата ключа ЭП.

## I. Схема работы системы

Общая схема применения цифровых подписей приведена на рисунке 1. Пользователь А применяет специальный алгоритм для генерации пары ключей $(S_A, P_A)$. Если пользователь А хочет отослать пользователю Б подписанное сообщение $m$, он генерирует цифровую подпись $s := \sigma(S_A, m)$. Затем $m$ и $s$ отсылаются пользователю Б. Пользователь Б применяет принадлежащий пользователю А открытый ключ $P_A$ и алгоритм верификации $\upsilon(P_A, m, s)$ для проверки цифровой подписи.

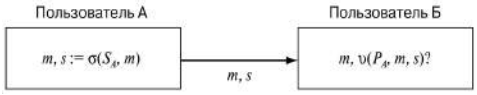


Рис. 1 – Общая схема применения цифровых подписей

На рисунке 2 изображена модульная структура аппаратных средств микропроцессорной системы. Модуль генератора случайных чисел и модуль под названием «Микропроцессорное устройство» выполнены с помощью отдельных микроконтроллеров. Обмен данными между микроконтроллерами происходит по протоколу USART.


Рис. 2 – Модульная структура аппаратных средств микропроцессорной системы

## II. Реализация системы

Для реализации системы ЭЦП в данной работе была использована схема RSA. В основу RSA положена давно известная проблема выделения множителей больших чисел, задача трудноразрешимая как в данный момент, так и в обозримом будущем. Так как система цифровой подписи нацелена на подпись файлов и документов большого размера, к документам применяется функция хеширования, и подписи подвергается хеш-сумма файла. Для этого в данной работе была реализована криптографическая хеш-функция sha256. Чтение документов для подписи производится с MMC-карты, а вывод ключевой пары и цифровой подписи возможен как на MMC-карту, так и по протоколу USART. При генерации ключевой пары использовался алгоритм Миллера-Рабина для тестирования больших чисел на простоту. Это вероятностный алгоритм, что значит, существует вероятность ошибок второго рода, однако ошибки первого рода невозможны.

## III. Выводы

Таким образом, была спроектирована и реализована система электронной цифровой подписи. В ходе анализа была установлена оптимальная длина ключей и другие параметры системы. Система была протестирована в среде схемотехнического моделирования Proteus. Благодаря большей программной части система имеет небольшой размер в виде схемы и недорога в реализации.

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.
2. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. – М.: Диалектика, 2004. – 432 с.
3. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп.– 3-е изд., перераб. идоп.– М.: Наука, 1982.– 288 с.

*Захарченко Константин Владимирович*, студент группы 021902 БГУИР, cvzakharchenko@gmail.com.

*Научный руководитель: Кукин Дмитрий Петрович*, доцент, кандидат технических наук, kukin@bsuir.by.