ИСПОЛЬЗОВАНИЕ МАГНИТООПТИЧЕСКИХ ВОЛНОВОДНЫХ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ

Жуманов Хакберди Ахмедович
Самаркандский филиал ТУИТ, Узбекистан, jumanov56@mail.ru
Хидиров Абдували Махмадалиевич
Самаркандский филиал ТУИТ, Узбекистан, abduvali.xidirov@mail.ru
Муродов Абдулазиз Дилшоджон угли
Самаркандский филиал ТУИТ, Узбекистан, murodovabdulaziz37@gmail.com

Аннотация. В целях криптографической обработки информации с применением алгоритма шифрования Вернама разработан функционирующий симулятор логического элемента «исключающее ИЛИ» (XOR), основанный на принципах, аналогичных магнитооптическим логическим элементам. Проведена экспериментальная проверка устройства-имитатора с использованием ASCII-кодирования, а также создан алгоритм шифрования и дешифрования текстовой информации.

Ключевые слова: Логические вентили, криптография, шифрование данных, алгоритм шифрования Вернама.

Среди множества методов защиты данных от несанкционированного доступа особое значение имеют криптографические подходы. Основу криптографической защиты составляет шифрование информации. На сегодняшний день существует большое количество алгоритмов шифрования, многие из которых приняты в качестве стандартов в различных странах. В рамках данной работы выбран метод шифрования Вернама [1].

Принцип работы шифра Вернама достаточно прост для понимания и реализации на компьютере. Для шифрования открытого текста необходимо выполнить побитовое сложение (операцию XOR) двоичного представления текста с двоичным представлением ключа. Полученный результат,

преобразованный в символьную форму, представляет собой зашифрованное сообщение [2].

Кратко рассмотрим основные этапы, использованные при создании макета устройства для шифрования и дешифрования текстовой информации в двоичном формате ASCII. Был разработан и реализован действующий макет имитатора устройства, выполняющего шифрование и дешифрование на основе алгоритма Вернама, функционирующего по принципам, аналогичным магнитооптическим логическим элементам. Созданный и экспериментально исследованный магнитооптический (МО) волноводный полусумматор способен реализовывать различные логические операции, включая И, исключающее ИЛИ (XOR), НЕ и другие [3].

В качестве основного элемента магнитооптического волновода в работе использовался образец оргстекла Х-образной формы, тщательно обработанный и отполированный для минимизации оптических потерь, связанных с рассеянием и поглощением. Назначение и функции остальных компонентов являются очевидными и не требуют дополнительных пояснений (рис. 1).

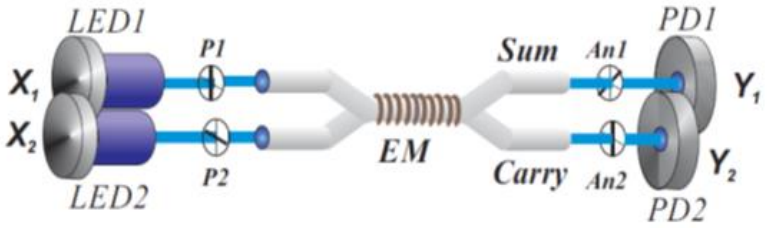

Рисунок 1. Схема магнитооптического полусумматора (периферийная электроника не показана): LED1 и LED2 - светоизлучающие диоды (λ= 440 нм) для сигналов X_1 и X_2 с ориентациями поляризации света HP и VP,

EM - электромагнит; Sum - суммарный волноводный канал; Carry - канал передачи; A_{n1} и A_{n2} - анализаторы; PD1 и PD2 - фотодиоды для каналов суммирования и передачи.

При помещении волновода в переменное магнитное поле возникает

эффект вращения Фарадея, в результате чего оптический сигнал приобретает магнитооптический характер. Таким образом, вместо чисто оптических сигналов X_1 и X_2 целесообразно рассматривать магнитооптические сигналы x_1 и x_2, формирующиеся при их прохождении через область волновода, охваченную катушкой электромагнита (область Фарадея, рис. 2).

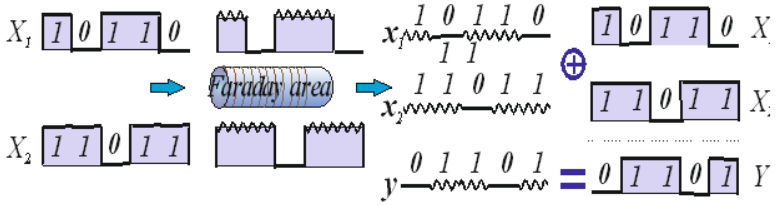

Рисунок 2. Эволюция обработанных сигналов для конфигурации элемента XOR.

Сигнал y регистрируется фотодиодом, после чего усиливается и преобразуется в электрическую форму, пригодную для последующей обработки, хранения или передачи данных.

Дальнейшие этапы, связанные с имитацией системы, организованы следующим образом. Алиса (источник) передаёт зашифрованное сообщение Бобу (приёмнику), при этом протокол и порядок использования одноразовых ключей согласуются заранее. Предполагается применение простых, компактных и надёжных оптико-электронных периферийных устройств для процессов шифрования и дешифрования. Вместо набора магнитооптических волноводов используется их электронная модель — так называемый имитатор устройства.

Корректная криптографическая обработка информации, предназначенной для шифрования, а также её последующее дешифрование возможны только при обеспечении строгой временной синхронизации. В противном случае невозможно добиться исходной синфазности обрабатываемых сигналов. Кроме того, такая синхронизация позволяет однозначно определить начало и конец файлов, используемых для представления сигналов. Для решения данной задачи в начале записи данных

в каждом из каналов (channel info и channel desi) вводятся специальные маркеры, как показано на рисунке 3.

В соответствующих блоках, обозначенных I, K и D для каналов 1, 2 и 3, записываются сигналы, представляющие информацию (I), ключ (K) и результат (D), полученный после прохождения через устройство-имитатор (Simulator Device). Эти сигналы представлены в виде последовательностей символов в двоичной кодировке ASCII:

канал 1 (информация): 11101000 11101101 11110100 11100000;

канал 2 (key_1): 11101011 11101011 11111110 11110111;

канал 3 (disi): результат побитового сложения по модулю 2 каналов 1 и 2, как показано на рисунке 3.

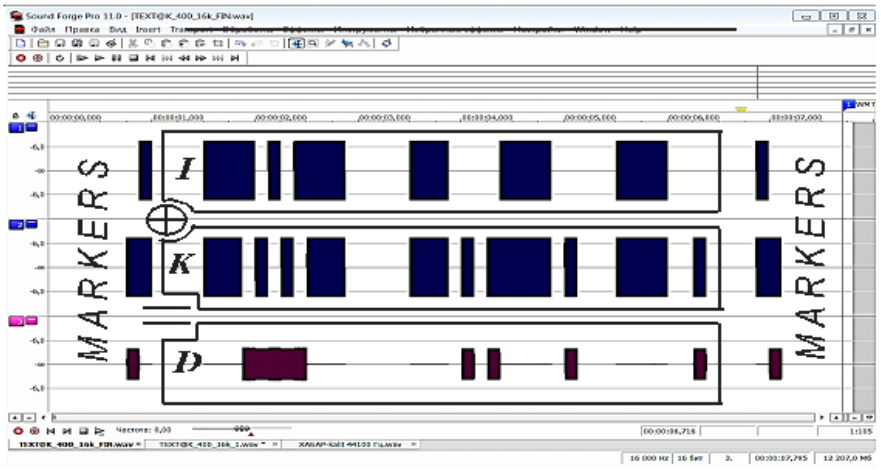

Рисунок 3. Процесс шифрования и получения дезинформации на PC_ALICE.

Ввод последовательности:

- 11101000 11101101 11110100 11100000 (информация) - канал 1;

-11101011 11101011 11111110 11110111 (ключ_1) - канал 2;

- результат сложения по модулю 2 каналов 1 и 2 - канал 3 (disi).

Таким образом, можно заключить, что предложенный метод криптографической обработки шифротекстов удовлетворяет требованиям, предъявляемым к передаче информации по каналам, предназначенным для конфиденциальной связи.

Список литературы:

[1] Bruce Schneier "Applied Cryptography" 2nd edition (1996). Source Code in C".John Wiley & Sons).

[2] Nigel "Smart.Cryptography: An Introduction" A McCraw-Hili Publication, ISBN 0077099877.

[3] Sh. Egamov, A.Khidirov, Kh.Urinov, Kh. Zhumanov. Waveguide Logic Gates for Magneto-optical Qubits. Technical Physics Letters, 2020, Vol. 46, No. 10, pp. 947–949. DOI: 10.1134/S1063785020100041.