3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : Питер, 2011.
4. FTTH Council Europe Webinar [Electronic resours] – April 23rd, 2020. – Mode of access: https://www.telepolis.pl/images/2020/04/swiatlowod-eu-092019.pdf. – Date of access: 29.08.2021.

АЛГОРИТМ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ ДЛЯ МАГНИТООПТИЧЕСКИХ ВОЛНОВОДНЫХ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ

Хидиров Абдували Махмадалиевич
Самаркандский филиал ТУИТ, Узбекистан
к.ф.-м.н. Эгамов Шухрат Ваххабович
Самаркандский филиал ТУИТ, Узбекистан
к.ф.-м.н., доцент Жуманов Хакберди Ахмедович
Самаркандский филиал ТУИТ, Узбекистан
jumanov56@mail.ru

Аннотация: Для криптообработки информации с использованием шифрования Вернам разработан рабочий симулятор логического элемента *XOR*, основанный на тех же принципах, что и магнитооптические логические элементы. Проведена экспериментальная проверка устройства-имитатора с использованием кодирования *ASCII* и разработан алгоритм шифрования и дешифрования текстовой информации.
Ключевые слова: Логические элементы, криптография, шифрование данных, алгоритм шифрования Вернама.

Обмен информацией, как открытой, так и закрытой, происходит в основном с использованием цифровых технологий и персональных компьютеров, поэтому есть возможность использовать все преимущества программного обеспечения, разработанного для обработки сигналов в цифровом и аналоговом формате. Суть шифрования с помощью шифра Вернама легко понять и реализовать на компьютере. Для того чтобы зашифровать открытый текст, вам просто нужно объединить двоичный код открытого текста с двоичным кодом ключа с помощью операции *XOR*, результирующий двоичный код, представленный в символьной форме, будет шифрованием шифра Вернама. Если мы попытаемся снова зашифровать шифрование, полученное шифром Вернама, с помощью того же ключа, мы снова получим открытый текст. Фактически, шифрование шифра Вернама идентично его расшифровке, что говорит нам о том, что шифр Вернама является симметричным шифром [1].

Давайте кратко рассмотрим шаги, которые мы непосредственно использовали для создания макета устройства для шифрования и дешифрования текстовой информации в кодировке двоичного формата *ASCII*. Поскольку одной из целей этого проекта было найти механизм, позволяющий кодировать (для

простоты мы выбрали *ASCII*) информационные сигналы, было применено программное обеспечение "*Sound Forge*" от Sony. Кодирование текстовой информации не вызывает особых трудностей, поскольку соответствующие стандарты, такие как *ASCII*, известны давно и широко используются в современных информационных технологиях. Мы создали рабочий макет имитатора устройства, предназначенного для шифрования и дешифрования информации с использованием алгоритма Вернама, основанного на тех же принципах, что и магнитооптические логические элементы. Разработанный и экспериментально протестированный магнитооптический (МО) волноводный полусумматор может быть использован для выполнения различных логических операций, таких как *И, ИСКЛЮЧАЮЩЕЕ ИЛИ (XOR), НЕТ* и другие [2].

Основным элементом, использованным в качестве магнитооптического волновода в нашем исследовании, был образец оргстекла *X*-образной формы, тщательно обработанный и отполированный, чтобы избежать оптических потерь при рассеянии и поглощении. Электромагнит представляет собой многослойную катушку из медной проволоки. Назначение и функции других частей понятны без дополнительных пояснений (рис. 1). Первичное двоичное кодирование входных сигналов выполняется с использованием импульсной модуляции, т.е. светодиод включен - "*1*", выключен - "*0*". Дальнейшие процедуры, связанные с имитацией, заключаются в следующем.

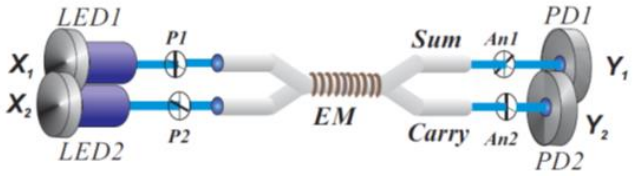

Рисунок 1. Схема магнитооптического полусумматора (периферийная электроника не показана): *LED1* и *LED2* - светоизлучающие диоды ($\lambda = 440$ *нм*) для сигналов X_1 и X_2 с ориентациями поляризации света *HP* и *VP*, *EM* - электромагнит; Sum - суммарный волноводный канал; *Carry* - канал передачи; A_{n1} и A_{n2} - анализаторы; *PD1* и *PD2* - фотодиоды для каналов суммирования и передачи

Алиса (источник) должна передать зашифрованную информацию Бобу (получателю). Протокол и последовательность использования одноразовых ключей согласовываются заранее. Предполагается, что для шифрования и дешифрования передаваемой и принимаемой информации следует использовать простые, компактные и надежные оптико-электронные периферийные устройства. Вместо набора магнитооптических волноводов мы будем использовать его электронную модель, названную имитатором устройства. Для практических целей, после проведения предварительных испытаний, был выбран вариант по следующей схеме (рисунок 2).

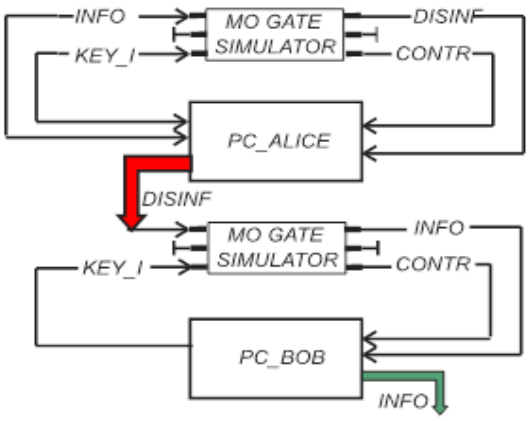

Рис. 2. Эволюция обработанных сигналов для конфигурации элемента XOR. Схема подключения, используемая для получения шифра Вернама в режиме логического магнитооптического элемента XOR (двоичный счетчик)

Рассмотрим более подробно действия Алисы по передаче и шифрованию информации (*info*) в 8-битной кодировке общепринятого стандарта с использованием программного обеспечения аудиоредактора "*Sound Forge*" и предложенной схемы. Боб, в свою очередь, записывает полученную зашифрованную информацию (*дезинформацию*) в виде аудиосигналов с помощью той же программы "*Sound Forge*" в один из каналов созданного файла, а затем вставляет заранее согласованный ключ во второй канал. После выполнения временного выравнивания Боб пропускает созданный файл через свое устройство-симулятор (которое теперь действует как дешифратор), подает его на линейный вход звуковой карты своего компьютера и получает расшифровку информации, отправленной Алисой по третьему каналу.

Таким образом, Боб, получив и записав шифрование, выполняет почти те же действия, что и Алиса, с той разницей, что вместо *информации* с *ключом* он запускает *Дезинформацию* с ключом через устройство-симулятор. В результате на выходе получается расшифрованное сообщение - исходная *информация*. В предлагаемом способе шифрование и дешифрование происходят одним и тем же способом и с использованием одного и того же аппаратного обеспечения. Результаты описанных действий показаны на рисунке 3. Для удобства результаты действий Алисы и Боба показаны в виде одного общего файла.

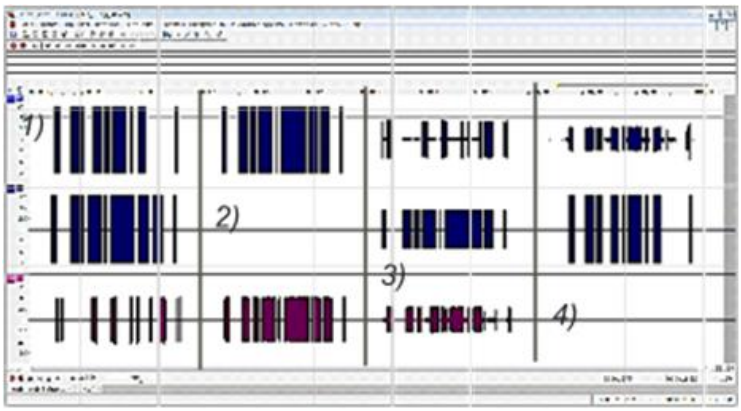

Рисунок 3. Процессы шифрования и дешифрования текстовой информации с использованием прототипа устройства

В крайнем левом углу, через обозначение 1), показано, как Алиса получает *дезинформацию* (третий канал ниже), пропуская *информацию* и *ключ* через устройство. Обратите внимание, что результирующая амплитуда для *дезинформации* оказалась меньше, чем у *информации* или *ключа*. Следовательно, во время следующих операций криптообработки необходимо, чтобы ключ Боба имел ту же амплитуду, соизмеримую с принятым сигналом, чтобы получить правильные результаты. Следовательно, Боб должен сначала пропустить ключ через устройство, как показано в области *2*).

Далее Боб записывает полученную *дезинформацию* и обработанный *ключ*, соответственно, на первый и второй каналы своего компьютера, затем проходит через свое устройство и получает желаемую *информацию* по каналу *3*. Результаты операций, выполненных Бобом, показаны в области *3*) рисунка 3. Область 4) показывает для сравнения исходную информацию (канал 2), подготовленную Алисой, и результат расшифровки на компьютере Боба (информация окончательная - канал 1). Амплитуда сигналов на компьютере Боба несколько меньше начальных значений, подготовленных Алисой, но это не важно.

Мы видим, что информация, восстановленная на компьютере Боба, полностью соответствует оригинальному тексту, подготовленному Алисой для секретной передачи. Таким образом, можно сделать вывод, что предлагаемый способ криптографической обработки шифротекстов полностью соответствует критериям отправки информации по каналам, предназначенным для конфиденциальных сообщений.

Использованная литература:

1. Nigel “Smart.Cryptography: An Introduction” A McCraw-Hili Publication, ISBN 0077099877.

2. 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.

3. Sh. Egamov, A.Khidirov. “Magneto-Optical Waveguide Gates for Digital Logic Operations”. 2020 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent, Uzbekistan. DOI: 10.1109/ICISCT50599.2020.9351417

AXBOROTLASHGAN JAMIYATDA SUN’IY INTELLEKT: IJTIMOIY-FALSAFIY TAHLIL

Mirzaxolov Nodirbek Tojiboyevich
Namangan davlat universiteti, O‘zbekiston
nodirbek_mustafo@mail.ru

Annotatsiya. Maqolada axborotlashgan jamiyatda sun’iy intellektning muvaffaqiyati natijasida yuzaga keladigan jarayonlar, jumladan, mehnat, aqlli