The undertaken researches showed that the by-products and modified wastes from sulfate pulp production could be used as foaming agents. For example - the water solution of detergent Taiga" and emulsion of tall pitch.

High dispersive of the amorphous microsilica (S=250000 cm^2/g), the wastes of crystal silicon and at lover level the high calcium concentration ach predefine the high water consumption of the compound. In addition, adding the foam to this system demand to use the compounds with high water consumption. Insufficient mobility of the mixture cause the destruction of the foam bubbles and the excessive humidity also changes the theological properties of the mixture ad prevents its structurization. The results of the researches showed that to get the material with the density of 400-800 kg/m^3 on the base of the above mentioned wastes the relation water-to-solid of the mixtures should be 1,3-0,9.

This high water trapping considerably slow down the setting of the mixture and decrease the rigidity properties of the dried semi finished and final products.

Adding of Na_2CO_3 increase the rigidity of the construction materials, ashes and microsilica and also the porous materials. When adding 4-10% of mass of dried compounds the rigidity of the semi finished product during its pressing increases in 20-30% due to the reaction of hydration setting. Na_2CO_3, acts also as diluter and when its concentration increases to 5-10% the water consumption decreases in one third (water-to-solids=0,68) maintaining the same consistency. During the firing the additive Na_2C0_3 know for its flux properties intensify the collection of melt silicon, which make the monolith from hard melting particles. Due to the flux action the rigidity of the burnt material increases in 35-40%.

It should be noted that the beginning of the setting of this mixture begins in 10-20 minutes, though the stability of the foam based on detergent "Taiga" is 40-60 min, that means that the structurization of the system is taking place before the destruction of the foam.

To eliminate the distortion and high shrinking deformation the drying of the material should be done at the temperature not more than 60°C. To have the possibility of easy taking away of forms, the material should have some residual humidity, which is necessary for particles adhesion due to intermolecular interaction, when the water in very thin films has the adhesive effect.

The rigidity properties of the material also depend on the modes of thermal treatment. The researches showed that the increasing of the standby time at the maximum firing temperature (900°C) increase the rigidity of the material (up to 50%), accompanied by the increase of firing shrinking from 6-7 to 8-10%.

The mathematical model of the experiment aimed to evaluate the influence of throe major factors (content of Na_2CO_3, flow of foaming agent - detergent "Taiga" and temperature of firing) helped to define the optimum compound composition and the temperature of thermal treatment.

The compound having more balanced characteristics should be fired at 900°C and have 7% of foaming agent and 6% of soda: Compressive strength - 1,63 MPa, average density - 0,68 g/cm^3, the construction quality factor - $22,1*10^{-4}$, thermal conductivity (according the empirical formula of V. P. Nickrassov) - 0,24.

The alternative version of additive instead of soda is wastes containing fluorine of Bratsk Aluminium Plant. The using of spent coal living gave a chance to get effective wall ceramics and foam ceramics with a minimum shrinkage.

ОБЗОР ОСНОВНЫХ МЕТОДОВ ФОРМИРОВАНИЯ КВАНТОВО-КРИПТОГРАФИЧЕСКОГО КЛЮЧА, С КОДИРОВАНИЕМ ОДНОФОТОННЫХ ИМПУЛЬСОВ ПО ОТНОСИТЕЛЬНОЙ ФАЗЕ

Хайров И.Е., Румянцев К.Е.,
Дзейкало А.А., Жуков М.А., Полывяная В.В.
Таганрогский государственный радиотехнический университет

В настоящее время для шифрования секретной информации широкое распространение получили криптографические методы, основанные на специальных секретных ключах.

Все современные криптографические системы делятся на симметричные и несимметричные. Симметричные или системы с секретным ключом представляют собой такие системы, в которых Алиса и Боб (принятые в научной литературе условные имена для передающей и принимающей сторон соответственно) владеют конфиденциальной информацией (например, ключом), которая не известна Еве (условное имя для обозначения подслушивающей стороны). Ключ применяется каждый раз для кодирования и декодирования передаваемой информации. В несимметричных системах или системах с открытым ключом используется два ключа. Один из них (публичный ключ) используется для шифрования, в то время как другой (секретный ключ), используется для дешифрования сообщений.

Бурное развитие квантовых технологий привело к появлению нового направления в криптографии - квантовой криптографии. Генерация ключа методами квантовой криптографии осуществляется непосредственно в процессе передачи единичных фотонов по каналу связи. Надежность этих методов базируется на незыблемости фундаментальных законов квантовой физики.

Первоначально квантово-криптографические системы были предназначены для отдельных пар пользователей, но затем стали рассматривать и для большого количества людей. Для генерации секретного ключа было предложено достаточно большое количество протоколов. Однако наиболее распространенным является BB84.

В этом протоколе для передачи ключевой информации однофотонные импульсы кодируются по поляризации, либо по относительной фазе. Эти методы кодирования имеют как преимущества, так и недостатки.

Рассмотрим основные системы с фазовым кодированием.

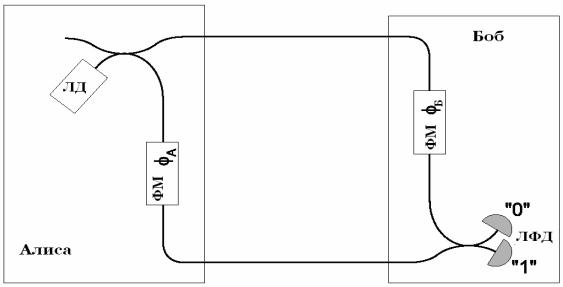

Рисунок 1. Интерферометр Маха-Цендера (ЛД - лазерный диод, ФМ - фазовый модулятор, ЛФД - лавинный фотодиод)

Эти системы преимущественно используются для передачи информации по волоконно-оптическим линиям связи, где основным недостатком поляризационного кодирования является случайная деполяризация сигнала.

Главным звеном в системе с кодированием по фазе является интерферометр Маха-Цендера (рис.1), который выполнен из двух волоконно-оптических разветвителей, соединённых между собой, и двух фазовых модуляторов – по одному в каждом плече. В такую систему можно ввести свет, используя классический непрерывный источник, и наблюдать наличие или отсутствие интерференционной картины на выходе. Данное устройство работает как оптический переключатель. Необходимо отметить, что крайне важным является сохранение постоянной и малой разности длин плеч для получения устойчивой интерференции.

Описанное выше поведение интерферометра справедливо и для одиночных фотонов. Вероятность зарегистрировать фотон на одном из выходов будет изменяться с изменением фазы.

В квантовой криптографии интерферометр используется вместе с однофотонным источником и детекторами, подсчитывающими фотоны. Установка Алисы содержит источник, первый разветвитель и первый фазовый модулятор, а установка Боба состоит из второго модулятора, разветвителя и детекторов (см. рис. 1.).

Данная схема прекрасно работает в лабораторных условиях на оптическом столе, но в случае, когда Алиса и Боб отделены друг от друга более чем на несколько метров из-за нестабильности плеч интерферометра приводит к дрейфу фазы, в результате чего возникают ошибки в передаваемом ключе. Для устранения этой проблемы в [1] предложено использовать два несбалансированных интерферометра Маха-Цендера, соединённых последовательно оптическим волокном (см. рис. 2).

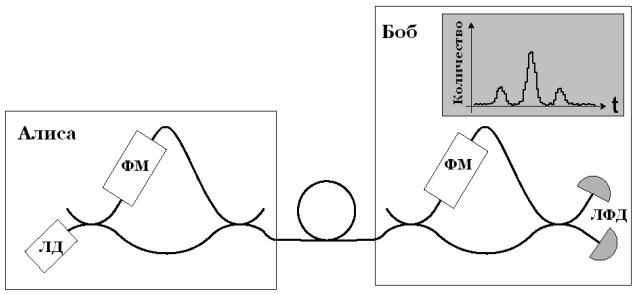

Рисунок 2. Система для квантовой криптографии с двумя интерферометрами Маха-Цендера (ЛД - лазерный диод, ФМ - фазовый модулятор, ЛФД - лавинный фотодиод).

Данная система работает следующим образом. Регистрируя количество отсчётов во времени, Боб получает три пика. Первый пик соответствует случаям, когда фотоны прошли по коротким плечам в интерферометрах Алисы и Боба, третий – случаям, когда они прошли по длинным плечам. Наконец, центральный пик соответствует фотонам, прошедшим через короткое плечо у Алисы и через длинное у Боба и наоборот. Такие фотоны интерферируют между собой. Для того чтобы отделить проинтерферировавшие фотоны (то есть центральный пик) от остальных, используется временное "окно". Результат интерференции будет зависеть от состояния фазовых модуляторов Алисы и Боба.

Преимущество этой установки заключается в том, что обе "половинки" фотона проходят по одному и тому же волокну [2]. Следовательно, они проходят пути равной длины в той части системы, которая является наиболее чувствительной к изменениям состояния окружающей среды.

Помимо описанных выше систем, существует так же система Plug&Play. Благодаря этой системе существует возможность автоматически и в пассивном режиме компенсировать все поляризационные флуктуации в оптическом волокне [3]. В данной схеме импульсы, которые излучаются Бобом, могут проходить через короткое плечо у Боба, отражаться от зеркала Фарадея у Алисы и возвращаться уже через длинное плечо у Боба, либо наоборот – проходить через длинное плечо, отражаться и проходить через короткое на обратном пути. Эти два типа импульсов интерферируют на разветвителе. Лавинный же фотодиод расположен только в приемном модуле. Главным недостатком систем "Plug&Play" является уязвимость по отношению к атакам типа "Троянский конь".

Таким образом, в результате проведённой работы были проанализированы основные способы кодирования однофотонных импульсов, применяемые в квантово- криптографических системах, рассмотрены их достоинства и недостатки. Выявлено, что для передачи информации по волоконно-оптическим линиям связи наиболее предпочтительным является кодирование по относительной фазе.

СПИСОК ЛИТЕРАТУРЫ

1. Charles H. Bennett et al. Experimental Quantum Cryptography, Journal of Cryptology, no. 5, 1992.

2. Wolfgang Tittel, Gregoire Ribordy and Nicolas Gisin. Quantum Cryptography, Physics World, March 1998.

3. Martinelli M., A universal compensator for polarization changes induced by birefringence on a retracting beam. Opt. Commun., 1989, vol. 72, pp. 341-344.

АНАЛИЗ КВАНТОВО-КРОПТОГРАФИЧЕСКОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ С ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ ОДНОФОТОННЫХ ИМПУЛЬСОВ

Хайров И.Е., Румянцев К.Е.,
Серогодский Д.И., Носков С.В., Котегов М.Г.
Таганрогский государственный радиотехнический университет

Проблема защиты информации от несанкционированного доступа является актуальной в связи с широким распространением компьютерных и телекоммуникационных систем. Изучением методов шифровки занимается криптография. В последнее время в этой области идёт активная работа над принципиально новым методом защищенного распределения ключевой информации – квантовой криптографии.

Задача квантовой криптографии заключается в передаче случайных последовательностей бит, которая затем может быть использована в качестве ключа для кодирования и декодирования сообщений.

Квантовая криптография опирается на фундаментальную неопределенность поведения квантовой системы – невозможно одновременно достоверно измерить координаты и импульс частицы, а так же два не ортогональных состояния поляризации фотона. Это фундаментальное свойство природы в физике известно как принцип неопределенности Гейзенберга.

В квантовой криптографии разработано несколько протоколов. Наиболее распространённым и используемым в практических приложениях является протокол BB84. В данном протоколе для кодирования однофотонных импульсов используется модуляция оптического излучения по поляризации или по относительной фазе. Системы с фазовым кодированием наиболее предпочтительны в ВОЛС, а система с поляризационным кодированием наиболее распространены в открытых системах связи (атмосферных, космических) и в ВОЛС с использованием волокон специальных конструкций. К ним относятся волокна с сохранением поляризации, например, с сердцевиной в виде спирали.

В данной работе рассматривается протокол BB84 с кодированием по поляризации. Особенность данного протокола является то, что на передаче используется четыре неортогональных состояния поляризации (0°, 45°, 90° или 135°).

Идея квантовой криптографии с поляризационным кодированием заключается в следующем. Поток горизонтально поляризованных фотонов полностью проходит через горизонтальный анализатор. Если поворачивать анализатор вокруг своей оси, то поток пропускаемых фотонов будет уменьшаться до тех пор, пока при повороте на 90° ни один фотон не сможет пройти анализатор. При повороте фильтра на 45° он пропустит горизонтально поляризованный фотон с вероятностью 50%.

Таким образом, измерить поляризацию света можно лишь тогда, когда заранее известно, в каком базисе он был поляризован. Если известно, что свет поляризован либо вертикально, либо горизонтально, то пропустив его через горизонтальный фильтр, мы узнаем по результату, была ли поляризация 0 или 90°. Если поляризация была диагональной, а анализатор установлен горизонтально, то по результату невозможно сказать, был ли свет поляризован на 45° или 135°.

В связи с этим, при непосредственном вмешательстве в сеанс "квантовой связи" возникает большое количество ошибок, что достоверно выявляется легальными пользователями.

Основной принцип генерации квантового ключа на основе протокола BB84 [1] заключается в том, что передающая сторона подготавливает однофотонные состояния с линейной поляризацией в двух не ортогональных друг другу базисах. Один – назовем его вертикально-горизонтальным – с поляризацией фотонов 0° и 90°. Второй – назовем его диагональным – с поляризацией 45° и 135°. Передающая и приемная стороны договариваются о коде каждой поляризации в двоичном представлении, например, фотоны с поляризацией 0° и 45° обозначают цифру "0", а фотоны с поляризацией 90° и 135° обозначают цифру "1". Во время передачи осуществляется посылка последовательности фотонов, поляризация которых выбрана случайным образом, и может составлять 0°, 45°, 90° и 135°. Приемник регистрирует пришедшие фотоны, и для каждого из них случайным образом выбирает базис измерения. Далее после осуществления нескольких процедур усиления секретности формируется секретный ключ известный только двум пользователям. Таким образом, зашифрованную этим ключом информацию смогут расшифровать только легальные пользователи.

В заключении необходимо отметить то, что данные системы реализованы в практических приложениях. В начале июня 2004 года в Кембридже (штат Массачусетс, США) была запущена в эксплуатацию первая в мире компьютерная сеть с квантовой криптографией. Система Quantum Net (Qnet) в настоящее время состоит из шести серверов, которые способны взаимодействовать с обычными узлами Всемирной паутины и пользователями Интернета.

Предполагается, что квантовые криптосистемы заинтересуют военные организации и коммерческие