Введение в квантовую криптографию

Содержание

1. Введение

Базовой задачей криптографии является шифрование данных и аутентификация отправителя. Отправитель должен произвести некоторое преобразование сообщения, возможно используя дополнительные данные, называемые ключом, таким образом, чтобы получатель смог по принятому им сообщению определить, было ли сообщение изменено.

Классический подход состоит в том, что ключ, использующийся как для шифровки, так и для расшифровки сообщения, должен быть известен только отправителю и получателю. Такие системы называются криптосистемами с закрытым ключом. Надежность процедуры шифрования доказана только для метода «одноразовых блокнотов», предложенного в 1917 году Гильбертом Вернамом (Gilbert Vernam). Идея его состоит в том, что оба участника обмениваются набором общих секретных ключей, каждый из которых используется для шифрования только одного сообщения. Ключи генерируются случайно и никакой информации не несут. Процесс шифровки состоит в том, что каждый символ исходного сообщения «складывается» с соответствующим символом ключа (так что ключ должен быть достаточно длинным, а сообщение — достаточно коротким). В «докомпьютерное» время ключи хранили в блокнотах с отрывными листами (отсюда и название метода). Каждый лист блокнота уничтожался после использования.

В применении к системам телекоммуникаций возникает проблема обеспечения секретности во время обмена ключами, поскольку ключ должен быть доставлен получателю сообщения заранее и с соблюдением строгой секретности. Иначе говоря, конфиденциально обменяться сообщениями позволяют ключи, но как обменяться самими ключами с обеспечением секретности? Сформулированную таким образом проблему называют проблемой распространения ключа.

1.1. Симметричное шифрование

Если используется постоянный закрытый ключ, то расшифровка сообщения зависит от вычислительной мощности системы и времени. В США, например, для шифрования используется стандарт DES (Data Encryption Standard), разработанный в 1977 году. Он основан на 56-битном ключе, при помощи которого можно закодировать 64 бит информации. На этом стандарте основывается защита банковских транзакций, паролей Unix-систем и других секретных данных. Поскольку длина ключа меньше, чем длина кодируемого сообщения, то механизм защиты не является абсолютно надежным. Если попытаться угадать ключ методом проб и ошибок, нужно перебрать 256 всевозможных значений. И хотя этот объем вычислений очень велик, в настоящее время уже имеются данные о возможности взлома подобных систем. Рекордное время составляет 22 часа 15 минут при распределенной обработке информации в компьютерной сети (www.rsasecurity.com/rsalabs/challenges/).

1.2. Асимметричное шифрование

Теория шифрования с использованием открытого ключа была создана Уэтфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman) в 1976 г. В этой системе получатель имеет общедоступный код для шифрования и закрытый код для расшифровки сообщений. Криптосистемы с открытым ключом основываются на так называемых односторонних функциях: по некоторому x легко вычислить функцию f(x), но зная f(x) трудно вычислить x.

Первый алгоритм, основанный на теории Диффи-Хеллмана, был предложен Роном Райвестом (Ron Rivest), Эди Шамиром (Adi Shamir) и Леонардом Эдлманом (Leonard Adleman) в 1977 г (RSA-алгоритм). Он основан на разложении простого числа на множители. Известно,

что вычислить произведение двух простых чисел легко. В то же время, обратная задача – разложение числа на простые множители, достаточно трудоемка, поскольку время вычислений экспоненциально возрастает при увеличении количества битов в исходном числе. Хотя в настоящее время не опубликованы быстрые алгоритмы решения задачи разложения числа на простые множители, нельзя утверждать, что они не существуют вовсе. Кроме того, вычислительная мощность компьютерных систем постоянно возрастает, поэтому сложность задачи не означает ее неразрешимость. Так, компания RSA, основанная вышеперечисленными авторами алгоритма, предлагает всем желающим разложить на простые множители представленные ею числа. Один из последних отчетов компании посвящен разложению числа, состоящего из 155 цифр. Эта задача требует 35,7 процессорных года, что примерно эквивалентно 8000 MIPS-лет3; в реальном времени потребовалось 3,7 месяца благодаря распределенной обработке информации в компьютерной сети.

Таким образом, на настоящий момент единственно надежным методом шифрования является метод «одноразового блокнота», поскольку доказана его безусловная секретность, то есть секретность по отношению к шпиону, который обладает неограниченными временем и вычислительной мощностью. На пути к достижению такого уровня секретности, стоит проблема распространения ключа: отправитель и получатель должны обменяться ключом, сохранив его в полном секрете. Задача безопасной пересылки ключей может быть решена с помощью квантовой рассылки ключей QKD (Quantum Key Distribution).

1.3. Основные понятия квантовой криптографии

Состояние квантового объекта может быть определено измерением. Однако сразу после выполнения этого измерения квантовый объект неизбежно переходит в другое состояние, причем предсказать это состояние невозможно. Следовательно, если в качестве носителей информации использовать квантовые частицы, то попытка перехватить сообщение приведет к изменению состояния частиц, что позволит обнаружить нарушение секретности передачи. Кроме того, невозможно получить полную информацию о квантовом объекте, и, следовательно, невозможно его скопировать. Таким образом, можно перечислить основные свойства квантовых систем:

1. Невозможно произвести измерение квантовой системы, не нарушив ее
2. Невозможно определить одновременно позицию и момент частицы со сколь угодно высокой точностью
3. Невозможно одновременно измерить поляризацию фотона в вертикально-горизонтальном и в диагональном базисах
4. Невозможно дублировать неизмеренное квантовое состояние

Отсюда следует, что из-за ограниченности возможностей по измерению квантовых система, использовать квантовые способы передачи данных в целом невыгодно, однако задействовать квантовый канал для согласования или распространения ключа между отправителем (далее Алиса) и получателем (далее Боб), размер которого обычно значительно меньше размера блока данных, нуждающегося в шифровании, представляется разумным из-за следующих свойств квантовых систем: при перехвате ключа третьим лицом (далее Ева), неизбежна подмена пересылаемых квантов. Из-за невозможности точно измерить позицию и момент кванта, часть подмененных Евой квантов будет отличаться от посланных Алисой. Следовательно, если после получения Бобом всей последовательности квантов он сравнит по открытому каналу какую-то ее подпоследовательность с отправленными Алисой, то, при слишком частом вмешательстве Евы, сравниваемые последовательности будут сильно отличаться.

2. Протоколы квантового распространения ключа

2.1. Протокол BB84

Идея использовать квантовые объекты для защиты информации от подделки и несанкционированного доступа впервые была высказана Стефаном Вейснером (Stephen Weisner) в 1970 г. Спустя 10 лет Беннет и Брассард, которые были знакомы с работой Вейснера, предложили использовать квантовые объекты для передачи секретного ключа. В 1984 г. они опубликовали статью, в которой описывался протокол квантового распространения ключа BB84.

Носителями информации в протоколе BB84 являются фотоны, поляризованные под углами 0, 45, 90, 135 градусов. В соответствии с законами квантовой физики, с помощью измерения можно различить лишь два ортогональных состояния: если известно, что фотон поляризован либо вертикально, либо горизонтально, то путем измерения, можно установить — как именно; то же самое можно утверждать относительно поляризации под углами 45 и 135 градусов. Однако с достоверностью отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45º, невозможно.

Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа. Отправитель кодирует отправляемые данные, задавая определенные квантовые состояния, получатель регистрирует эти состояния. Затем получатель и отправитель совместно обсуждают результаты наблюдений. В конечном итоге со сколь угодно высокой достоверностью можно быть уверенным, что переданная и принятая кодовые последовательности тождественны. Обсуждение результатов касается ошибок, внесенных шумами или злоумышленником, и ни в малейшей мере не раскрывает содержимого переданного сообщения. Может обсуждаться четность сообщения, но не отдельные биты. Открытый канал связи не обязан быть конфиденциальным, только аутентифицированным.

Чтобы обменяться ключом, Алиса и Боб предпринимают следующие действия:

1. Алиса посылает Бобу бит A_i, задавая определенное квантовые состояние - поляризацию в 0, 45, 90, 135 градусов. Отсчет углов можно вести от направления "вертикально вверх" по часовой стрелке.
2. Боб располагает двумя анализаторами: один распознает вертикально-горизонтальную поляризацию, другой — диагональную. Для каждого фотона Боб случайно выбирает один из анализаторов и записывает тип анализатора и результат измерений. Полученный, т.н. «сырой», ключ $B_i = A_i$ с вероятностью $P = 75\%$. То есть он содержит ~ 25% ошибок.
3. По общедоступному каналу связи Боб сообщает Алисе, какие анализаторы использовались, но не сообщает, какие результаты были получены.
4. Алиса по общедоступному каналу связи сообщает Бобу, какие анализаторы он выбрал правильно. Те фотоны, для которых Боб неверно выбрал анализатор, отбрасываются.
5. Для обнаружения перехвата Алиса и Боб выбирают случайный участок ключа и сравнивают его по общедоступному каналу связи. Если процент ошибок велик, то он может быть отнесен на счет Евы, и процедура повторяется сначала.

В качестве источника света может использоваться светоизлучающий диод или лазер. В качестве проводника используют либо пространство, либо оптические кабели.

2.2. Пример шифрования по протоколу BB84

Условные обозначения:

Обозначение	Поляризация фотонов	Кодируемый бит
|	Вертикальная	0
—	Горизонтальная	1
/	Под угром 45,	0
\	Под углом 135	1

Эти правила могут с легкостью быть заменены на противоположные (лишь бы Алиса и Боб договорились между собой), однако в таблицах приняты именно эти обозначения.

Обозначение анализатора	Поляризация фотонов
+	Прямоугольный
x	Диагональный

Последовательность фотонов Алисы	|	/	/	—	\	|	|	—	—
Последовательность анализаторов Боба	+	x	+	+	x	x	x	+	x
Результаты измерений Боба	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	да	да		да	да			да	
Ключ	0	0		1	1			1	

Если бы Ева производила перехват информации при помощи оборудования, подобного оборудованию Боба, то примерно в 50 процентах случаев она выберет неверный анализатор, не сможет определить состояние полученного ею фотона, и отправит фотон Бобу в состоянии, выбранном наугад. При этом в половине случаев она выберет неверную поляризацию и, таким образом, примерно в 25 процентах случаев результаты измерений Боба могут отличаться от результатов Алисы. Это довольно заметно и быстро обнаруживаемо. Однако, если Ева перехватывает только 10% информации, тогда уровень ошибок будет 2.5%, что менее заметно.

2.3. Снижение уровня ошибок и увеличение секретности ключа

Вносимые ошибки могут быть обнаружены и устранены с помощью подсчета четности, так что сравнивается четность в блоках из нескольких бит, при этом после проверки один бит из каждого блока отбрасывается. Беннет в 1991 году предложил следующий протокол.

1. Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.
2. Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).
3. Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга о полученных результатах. Последний бит каждого блока удаляется.
4. Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.
5. Чтобы исключить кратные ошибки, которые могут быть не замечены, операции пунктов 1-4 повторяются для большего значения k.
6. Для того чтобы определить, остались или нет необнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки:
   - Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.
   - Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.
   - Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.
7. Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2^{-m}.

Увеличение секретности ключа также может быть произведено без дополнительного обмена данными по открытому каналу. Например, при наличии у Алисы последовательности отправленных битов A_i, и последовательности принятых битов B_i у Боба оба могут произвести следующие преобразования:

$$A'_i = A_{2i} \; xor \; A_{2i+1},$$
$$B'_i = B_{2i} \; xor \; B_{2i+1}$$

что обеспечивает секретность ключа от Евы, даже если она смогла перехватить и скопировать каждый второй пересылаемый фотон.

2.4. Протокол Экерта

Если Алиса и Боб не собираются использовать полученный ими ключ сразу, то перед ними возникает новая проблема, — как сохранить ключ в секрете? В 1991 г. Артур Экерт (Artur Ekert) предложил протокол, позволяющий решить обе эти проблемы — распространения и хранения ключа. Протокол Экерта основан на эффекте EPR (Einstein-Podolsky-Rosen). Эффект EPR возникает, когда сферически симметричный атом излучает два фотона в противоположных направлениях в сторону двух наблюдателей. Фотоны излучаются с неопределенной поляризацией, но в силу симметрии их поляризации всегда противоположны. Такие состояния двух фотонов называются сцепленными.

На основе эффекта EPR Экерт предложил криптосхему, которая гарантирует безопасность пересылки и хранения ключа. Отправитель генерирует некоторое количество EPR фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При этом, если эффективность регистрации близка к единице, при получении отправителем значения поляризации 1, его партнер зарегистрирует значение 0 и наоборот. Ясно, что таким образом партнеры всякий раз, когда требуется, могут получить идентичные псевдослучайные кодовые последовательности. Практически реализация данной схемы проблематична из-за низкой эффективности регистрации и измерения поляризации одиночного фотона.

Неэффективность регистрации является платой за секретность. Следует учитывать, что при работе в однофотонном режиме возникают чисто квантовые эффекты. При горизонтальной поляризации и использовании вертикального поляризатора результат очевиден - фотон не будет зарегистрирован. При 45^0 поляризации фотона и вертикальном поляризаторе вероятность регистрации 50%. Трудность также состоит в том, что в настоящее время не все сцепленные состояния поддаются измерению, не говоря уже о создании идеально отражающих емкостей для хранения фотонов.

2.5. Практическая реализация протокола BB84

Схема реализация однонаправленного канала с квантовым шифрованием показана на рис. .1. Передающая сторона находится слева, а принимающая - справа. Ячейки Покеля служат для импульсной вариации поляризации потока квантов передатчиком и для анализа импульсов поляризации приемником. Передатчик может формировать одно из четырех состояний поляризации (0, 45, 90 и 135 градусов). Собственно передаваемые данные поступают в виде управляющих сигналов на эти ячейки. В качестве канала передачи данных может использоваться оптическое волокно. В качестве первичного источника света можно использовать и лазер.

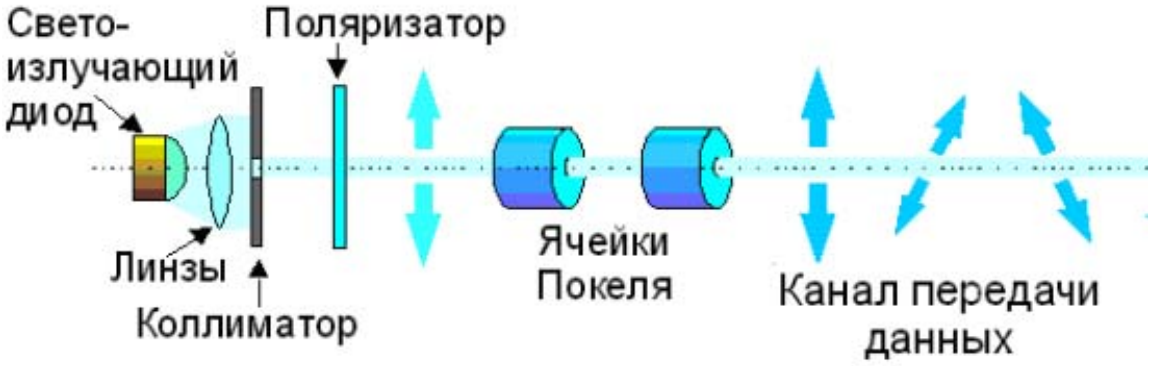

Рис.1. Схема передающей стороны

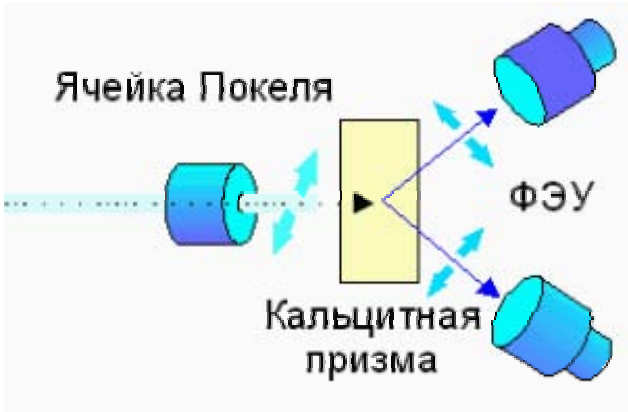

Рис.2. Схема принимающей стороны

На принимающей стороне после ячейки Покеля ставится кальцитовая призма, которая расщепляет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации. При формировании передаваемых импульсов квантов приходится решать проблему их интенсивности. Если квантов в импульсе 1000, есть вероятность того, что 100 квантов по пути будет отведено злоумышленником на свой приемник. Анализируя позднее открытые переговоры между передающей и принимающей стороной, он может получить нужную ему информацию. В идеале число квантов в импульсе должно быть около одного. Здесь любая попытка отвода части квантов злоумышленником приведет к существенному росту числа ошибок у принимающей стороны. В этом случае принятые данные должны быть отброшены и попытка передачи повторена. Но, делая канал более устойчивым к перехвату, мы в этом случае сталкиваемся с проблемой "темнового" шума (выдача сигнала в отсутствии фотонов на входе) приемника (ведь мы вынуждены повышать его чувствительность). Для того чтобы обеспечить надежную транспортировку данных логическому нулю и единице могут соответствовать определенные последовательности состояний, допускающие коррекцию одинарных и даже кратных ошибок.

2.6. Протокол B92

Протокол B92 также используется в качестве носителей фотоны, однако, поляризованные только в двух состояниях. Такие состояния поляризации более удобны для передачи данных на большие расстояния по оптическим кабелям.

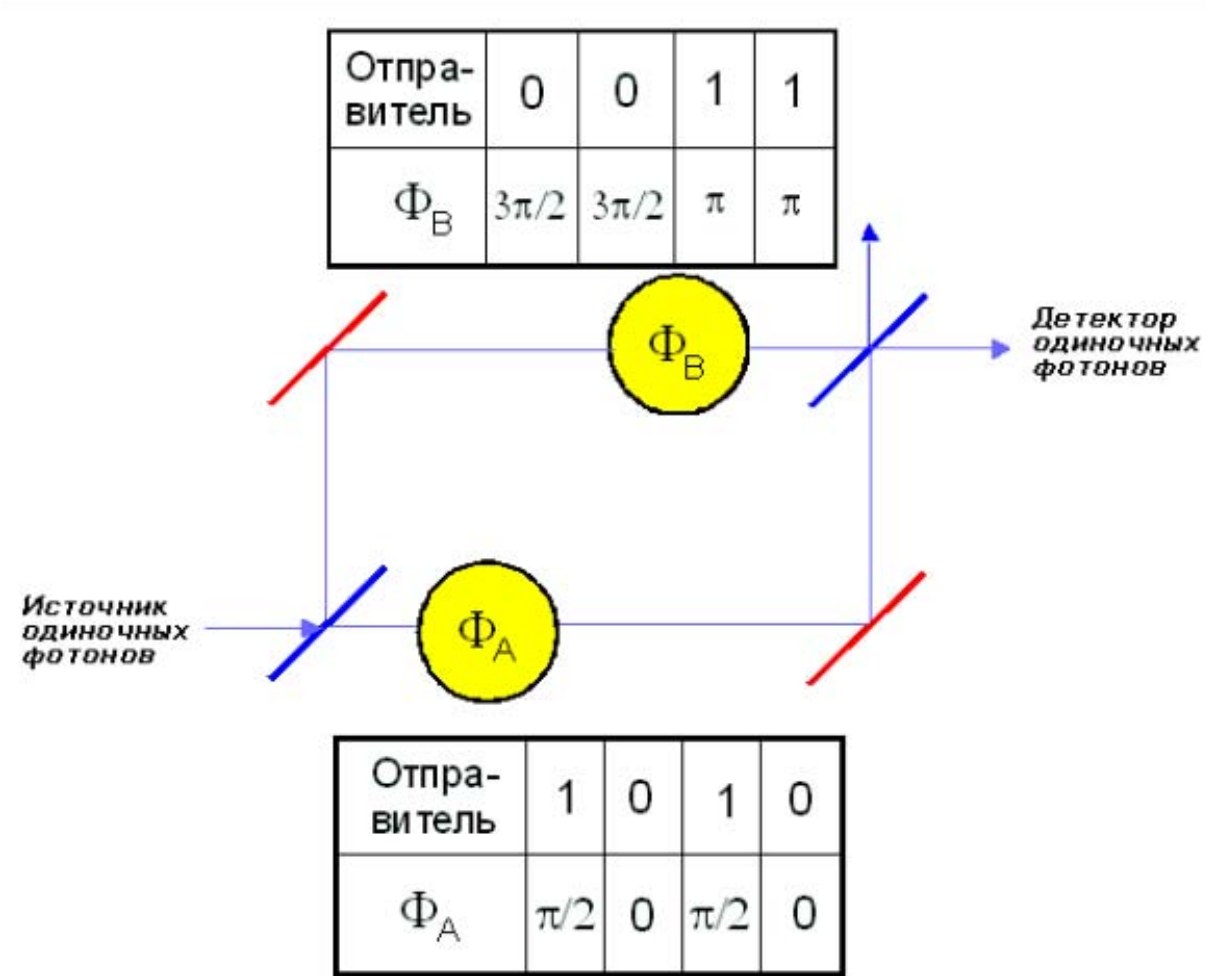

Рис. 3. Реализация алгоритма B92

В алгоритме B92 приемник и передатчик создают систему, базирующуюся на интерферометрах Маха-Цендера. Отправитель определяет углы фазового сдвига, соответствующие логическому нулю и единице ($F_A = p/2$), а приемник задает свои фазовые сдвиги для логического нуля ($F_B = 3p/2$) и единицы ($F_B = p$). В данном контексте изменение фазы $2p$ соответствует изменению длины пути на одну длину волны используемого излучения.

Хотя фотоны ведут себя при детектировании как частицы, они распространяются как волны. Вероятность того, что фотон, посланный отправителем, будет детектирован получателем равна

$$P_d = \cos^2\left(\frac{F_A - F_B}{2}\right)$$

и характеризует интерференцию амплитуд волн, распространяющихся по верхнему и нижнему путям (см. рис. 3).

Вероятность регистрации будет варьироваться от 1 (при нулевой разности фаз) до нуля. Здесь предполагается, что отправитель и получатель используют фазовые сдвиги $(F_{A,}F_B) = (0,3p/2)$ для нулевых бит и $(F_{A,}F_B) = (p/2, p)$ для единичных битов (для алгоритма BB84 используются другие предположения).

Для регистрации одиночных фотонов, помимо ФЭУ, могут использоваться твердотельные лавинные фотодиоды (германиевые и InGaAs). Для понижения уровня шума их следует охлаждать. Эффективность регистрации одиночных фотонов лежит в диапазоне 10-40%. При этом следует учитывать также довольно высокое поглощение света оптическим волокном (~0,3-3ДБ/км). Схема интерферометра с двумя волокнами достаточно нестабильна из-за разных свойств транспортных волокон и может успешно работать только при малых расстояниях. Лучших характеристик можно достичь, мультиплексируя оба пути фотонов в одно волокно (см. рис. 4).

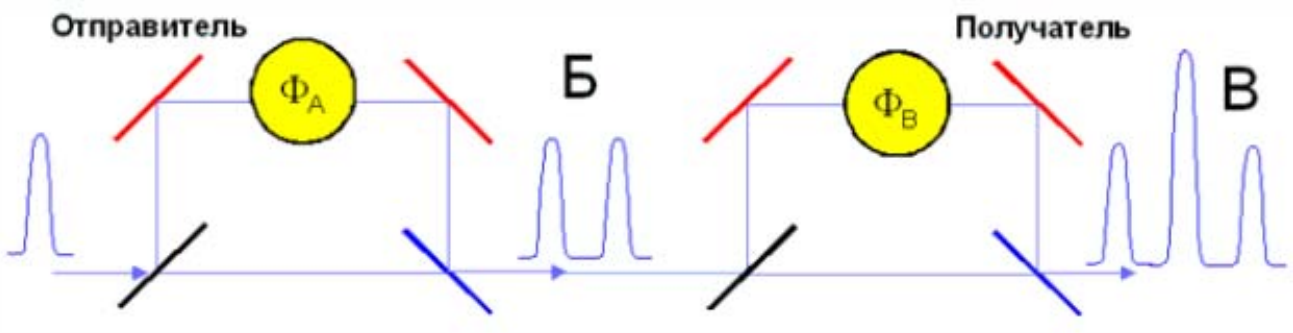

Рис. 4. Интерферометр с одним транспортным волокном

В этом варианте отправитель и получатель имеют идентичные неравноплечие интерферометры Маха-Цендера (красным цветом отмечены зеркала). Разность фаз длинного и короткого путей DT много больше времени когерентности светового источника. По этой причине интерференции в пределах малых интерферометров не происходит (Б). Но на выходе интерферометра получателя она возможна (В). Вероятность того, что фотонные амплитуды сложатся (центральный пик выходного сигнала интерферометра В) равна

$$P = \frac{1}{8}\left(1 + \cos\left(F_A - F_B\right)\right)$$

Разветвители пучка (полупрозрачные зеркала) могут быть заменены на оптоволоконные объединители (coupler). Практические измерения для транспортного кабеля длиной 14 км показали эффективность генерации бита ключа на уровне 2,2 10^{-3} при частоте ошибок около 1,2%.

3. Технологические аспекты

3.1. Практические проблемы квантовой криптографии

При создании практических криптосистем, основанных на квантовом распространении ключа приходится сталкиваться со следующими проблемами:

- Низкая скорость передачи
- Небольшие расстояния
- Невозможность создания квантовых повторителей
- Интенсивность импульсов квантов
- Атаки злоумышленников на квантовый канал

При формировании передаваемых импульсов квантов приходится решать проблему их интенсивности. В теоретической части мы исходим из предположения, что сообщение передается и принимается импульсами по одному кванту. На практике такого результата добиться не удается - источник с ненулевой вероятностью излучит больше одного фотона. Если квантов в импульсе 1000, есть вероятность того, что 100 квантов по пути будет отведено злоумышленником на свой приемник. Анализируя позднее открытые переговоры между передающей и принимающей стороной, он может получить нужную ему информацию. В идеале число квантов в импульсе должно быть около одного. Здесь любая попытка отвода части квантов злоумышленником приведет к существенному росту числа ошибок у принимающей стороны. В этом случае принятые данные должны быть отброшены и попытка передачи повторена. Но, делая канал более устойчивым к перехвату, мы в этом случае сталкиваемся с проблемой "темнового" шума (выдача сигнала в отсутствии фотонов на входе) приемника (ведь мы вынуждены повышать его чувствительность).

Атаки на квантовую передачу классифицируются следующим образом:

- Некогерентные (индивидуальные)
- Когерентные (массовые)
    - Совместные
    - Коллективные

3.2. Практические успехи

Практические работы в области квантовой криптографии ведут такие компании как IBM, Mitsubishi, Toshiba, лаборатории GAP-Optique, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт (Caltech), MagiQ, холдинг QinetiQ.

Организация	**Исследователи**	**Достигнутые результаты**
IBM	Чарльз Беннетт, Жиль Броссард	
Gap-Optique	Николас Гисин	67 км
Mitsubishi		87 км, 7.2 бит/с
Toshiba Research Europe		100 км

Создана также коммерческая квантовая криптосистема id 3000 Clavis Quantum Key Distribution System, поддерживающая:

- Безопасный обмен ключами на расстоянии до 100 км
- Поддержку протокола BB84
- Встроенный протокол просеивания ключа
- Протокол шифрования и передачи файлов
- Битрейт = 1500 бит/с