КВАНТОВАЯ КРИПТОГРАФИЯ: ПЕРЕДАЧА КВАНТОВОГО КЛЮЧА

ПРОБЛЕМЫ И РЕШЕНИЯ

Н. Слепов
nslepov@online.ru

Криптография – это искусство изобретения кодов и шифров. Как искусство оно было известно еще со времен Цезаря. Криптография была востребована всегда – сильным мира того и сего всегда было что прятать от глаз и ушей простого народа, но особенно интенсивно она развивалась во время мировых войн. Достаточно вспомнить разработку Германией шифровальной машины "Энигма" и героические усилия английских специалистов по разработке метода дешифрации ее кода, которые способствовали становлению и развитию вычислительных машин. Современная криптография получила мощный импульс для своего совершенствования благодаря быстрому развитию персональных компьютеров и сети Интернет, способствовавших, благодаря возможности использовать защищенные механизмы электронной подписи, развитию бизнеса.

Новая эра криптографии началась с идеи о возможности разработки квантового компьютера, которая сначала повергла специалистов в шок, когда они поняли, что такой компьютер в считанные секунды сможет взломать любой шифр, а потом стала мощным стимулом для тех же специалистов в разработке противоядия – квантовой криптографии. Предложенный ниже обзор преследует цель – дать, если получится, возможность рядовым читателям разобраться, что же дает квантовая криптография и как она решает проблемы защиты нас от взломщиков.

Классическая криптография стала наукой тогда, когда наряду с эвристикой положила в основу *криптоанализ* – искусство разработки процедур, ведущих к дешифрации кодов. Комбинация криптографии и криптоанализа привела к *криптологии* – науке о шифрации и дешифрации сообщений.

Шифрование – это процесс перевода исходного (открытого) текста m в зашифрованный текст C – *шифрограмму* с помощью *функции шифрации* E – процедуры, применяемой к специальному ключу k (или двум ключам) и тексту m: C = E(k, m).

Если традиционная криптография веками использовала для функции шифрации процедуры *перестановки* и *подстановки (замены)* символов/слов, то современная криптография основана на использовании техники сверточных алгоритмов для достижения гарантированной безопасности. Используемой процедурой здесь является операция сложения по модулю 2 ($\oplus$) поточных бит/букв (для *поточных шифров*) или блока бит/букв (для *блочных шифров*). Тогда для поточных шифров имеем: $C_i = m_i \oplus k_i$ при шифрации и $m_i = C_i \oplus k_i$ при дешифрации.

Обмен шифрованными сообщениями происходит обычно между двумя сторонами: передающей – A и принимающей – B. В научной литературе по криптосистемам их ласково называют Алисой (A) и Бобом (B). Допускается также, что сообщение, передаваемое со стороны A к B, может быть перехвачено *оператором перехвата сообщений* (eavesdropper), роль которого играет грехоподобная Ева (E).

Все криптографические системы делятся на два класса: *симметричные* и *несимметричные*.

Симметричные криптосистемы, или *системы с секретным ключом* (private key), – это такие системы, в которых один секретный ключ применяется как для шифрации, так и дешифрации передаваемой информации. В этом случае Алиса и Боб владеют некой секретной информацией – ключом, который не должен быть известен Еве.

Абсолютная защищенность симметричной системы имеет место при следующих условиях [1]:

- Ключ абсолютно случаен;
- Длина ключа равна длине самого сообщения (что предопределяет использование потоковой техники генерации ключа);
- Ключ, как правило, одноразовый, т.е. используется только один раз для передачи одного сообщения или в одном сеансе связи (более подробно см. ниже).

Одной из основных проблем симметричных криптосистем является передача или распределение секретного ключа между пользователями. Попытки использовать один и тот же ключ много раз (хотя и допустимые) приводят к возникновению определенной структуры в шифрованном тексте, и Ева может этим воспользоваться для дешифрации сообщений. Недостатком такой системы является необходимость Алисе и Бобу располагать большим набором случайных двоичных последовательностей для использования их в качестве ключей. При интенсивном обмене сообщениями эти наборы рано или поздно будут израсходованы, и опять возникнет проблема передачи ключа. Самый надежный способ – личная встреча Алисы с Бобом, но в силу ряда причин такая встреча может оказаться невозможной.

Принято считать, что вычисления, состоящие из 2^{80} шагов, сегодня трудноосуществимы, поэтому предполагается, что секретный ключ должен иметь длину, по крайней мере, 80 бит. Сейчас секрет-

ные ключи имеют длину 128/192/256 бит, т.е. требуют анализа $2^{128/192/256}$ вариантов перебора, что делает отгадку (раскрытие) кода трудноразрешимой задачей. Однако прогресс в росте быстродействия процессоров заставляет и дальше увеличивать длину ключа. Не имея этого ключа, оператор перехвата сообщений наблюдает лишь случайную последовательность бит.

В свете проблем доставки в симметричных криптографических системах были предприняты попытки создания систем, которые не нуждались бы в доставке секретного ключа. Они привели к созданию несимметричных криптографических систем.

Несимметричные криптосистемы, или *системы с открытым ключом* (public key), – это такие системы, которые имеют дело с парами ключей. Один из них (открытый ключ) используется для шифрации, в то время как другой (секретный ключ) – для дешифрации сообщений. Если кто-то шлет вам сообщение, то он шифрует его, используя ваш открытый ключ, а вы, дешифруя его, используете ваш секретный ключ. Главное в том, насколько хорошо сформирована функция шифрации/дешифрации и как соотносятся между собой открытые и секретные ключи.

Эти два ключа должны быть связаны между собой некой "односторонней" функцией, которая позволила бы без труда вычислить открытый ключ, используя секретный, но не позволяла бы произвести обратную процедуру. Этот принцип был предложен в 1976 году, но только в 1978 году Р.Райвесту, А.Шамиру и Л.Эдльману удалось найти такую функцию, которая была применена в алгоритме, известном как RSA (Rivest, Shamir, Adleman) [1]. Алгоритм RSA считается достаточно защищенным для многих применений современной криптографии. Сейчас большинство банковских транзакций, системы электронной покупки, коммерческие и некоммерческие системы криптографической защиты используют принципы RSA.

Криптосистемы с открытым ключом, казалось бы, преодолели основной недостаток симметричных криптосистем – необходимость в обмене секретными ключами. Однако никто еще не доказал полную защищенность алгоритма RSA. В 1985 году Дэвид Дойч описал принцип *квантового компьютера*, который будет обладать вычислительной мощностью, намного превосходящей все нынешние и будущие компьютерные системы. В 1994 году Питер Шор описал алгоритм, с помощью которого такой компьютер сможет легко взломать шифр RSA [2], хотя и не смог продемонстрировать его работу, поскольку на тот момент квантовых компьютеров не существовало.

Несмотря на то, что сегодня никто вроде не знает, как сконструировать квантовый компьютер, в то же время никто не может доказать, что его построение невозможно или что он уже не построен в какой-то секретной лаборатории. Это значит, что нет абсолютной уверенности в достаточной степени защищенности систем с открытым ключом.

Мы не будем рассматривать несимметричные системы – они слишком хорошо известны. Что касается симметричных систем, то мы сосредоточимся только на проблемах распределения/передачи секретных ключей в симметричных криптосистемах, учитывая, что они могут быть успешно решены уже сегодня.

РАСПРЕДЕЛЕНИЕ/ПЕРЕДАЧА КЛЮЧЕЙ

Различают два типа секретных ключей для симметричных систем: *долговременные*, используемые многократно и длительное время, и *кратковременные* (сеансовые), используемые на один сеанс или не более одного дня. Для передачи или распределения таких ключей между пользователями существует несколько решений [1, 3]:

- *физическое распределение* – передача долговременного ключа с помощью курьера;
- *распределение с помощью протоколов* с секретным ключом – передача сеансовых ключей пользователям в режиме реального времени с помощью *центра доверия*, пользующегося специальными протоколами обмена ключей;
- *распределение с помощью протоколов* с открытым ключом – передача сеансовых ключей пользователям в режиме реального времени с помощью центра доверия, использующего криптосистемы с открытым ключом (наиболее распространенное приложение техники шифрования с открытым ключом);
- *квантовое распределение ключей* – передача квантовых ключей с использованием квантовых свойств частиц (фотонов) в соответствии с процедурами *квантовой криптографии*.

Первые три способа передачи секретных ключей традиционны и хорошо известны [1], поэтому мы остановимся на последнем способе, который имеет наибольшую перспективу. Однако для этого нужно кратко описать квантовые криптосистемы, чтобы понимать особенности их работы и возможности решения поставленной задачи.

ВВЕДЕНИЕ В КВАНТОВУЮ КРИПТОГРАФИЮ

Первым толчком в развитии квантовой криптографии была идея выпуска "квантовых денег", предложенная С.Визнером (Wiesner) в 1970. Она была, по сути, отвергнута, но позднее опубликована в 1983 году [3]. Идея заключалась в размещении внутри купюры нескольких фотонов, поляризованных в двух сопряженных ортогональных состояниях поляризации. Согласно принципу неопределенности Гейзенберга, существуют сопряженные квантовые состояния, которые не могут быть измерены одновременно. Фальшивомонетчику, чтобы подделать купюру, нужно измерить состояния всех фотонов в ней, а потом воспроизвести их в фальшивой купюре. Однако он не может этого сделать (согласно принципу неопределенности), с одной стороны, и не может получить эту информацию от банка, который хранит эту информацию, зависящую от номера банкноты, в секрете, с другой стороны.

Квантово-механические принципы

Основными принципами квантовой механики, положенными в основу квантовой криптографии, являются [4]:

- *Невозможность различить абсолютно надежно два неортогональных квантовых состояния;*
- *Запрет на клонирование.* Благодаря унитарности и линейности квантовой механики невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние. Таким образом, факт "прослушивания" квантового канала уже приводит к ошибкам передачи, обнаружение которых доступно легальным пользователям.
- *Наличие перепутанных/запутанных квантовых состояний.* Две квантово-механические системы могут находиться в состоянии взаимной корреляции, например благодаря явлению двухфотонной корреляции при интерференции. Это приводит к тому, что измерение выбранной величины в одной из систем влияет на результат измерения этой же величины в другой системе. Такой эффект может быть объяснен возникновением перепутанных квантовых состояний [5]. Это значит, что измерение, проведенное на одной из двух систем, может дать с равной вероятностью $|0\rangle$ или $|1\rangle$, тогда как состояние другой системы будет противоположным (т.е. $|1\rangle$ или $|0\rangle$), и наоборот. Эти состояния используются в оптических тестах неравенств Белла в связи с уточнением полученных "черновых вариантов" квантовых ключей (raw key) [5].

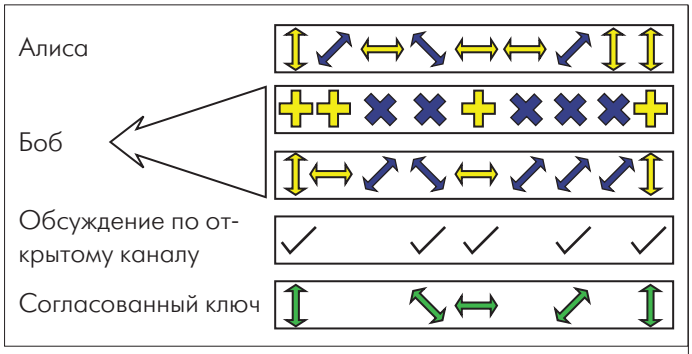

Рис.1. Формирование квантового ключа по протоколу BB84

- *Причинность и суперпозиция*. Причинность, исходно не являющаяся ингредиентом нерелятивистской квантовой механики, может быть, тем не менее, использована для квантовой криптографии вместе с принципом суперпозиции: если две системы, состояния которых образуют некую суперпозицию, разделены во времени, не будучи связаны причинностью, то нельзя определить суперпозиционное состояние, проводя измерения на каждой из систем последовательно.

ОСНОВЫ КВАНТОВОЙ КРИПТОГРАФИИ

Идея квантовых денег была нереализуема, так как требовала сохранять фотон в "ловушке" (купюре) достаточно долгое время. Однако эта идея подтолкнула Ч.Беннетта и Г.Брассара (C.Bennett и G.Brassard) к изобретению квантовой криптографии в 1984 году [6]. Беннетт и Брассар предложили не хранить информацию о поляризации фотонов, а передавать ее по квантовому каналу, сформированному, например, с помощью стандартного одномодового волокна, используемого в системах передачи данных.

Задача квантовой криптосистемы (которая относится к классу симметричных криптосистем) заключается в генерации и передаче *последовательности случайно поляризованных фотонов* (ПСПФ), используемой в формировании ключа для шифрации и дешифрации сообщений путем манипуляции четырьмя состояниями поляризации фотонов (генерируемых двухуровневой физической системой), представляющими два сопряженных ортогональных базиса A и B: $|0_A\rangle$, $|1_A\rangle$ и $|0_B\rangle = (1/\sqrt{2})/(|0_A\rangle + |1_A\rangle)$, $|1_B\rangle = (1/\sqrt{2})/(|0_A\rangle - |1_A\rangle)$.

Здесь состояния $|0_A\rangle$ и $|1_A\rangle$ используются для кодирования значений "0" и "1" в базисе A, а $|0_B\rangle$ и $|1_B\rangle$ – для кодирования тех же значений в базисе B. Эти состояния можно представить с помощью поляризационных состояний фотона. Например, $|0_A\rangle$ и $|1_A\rangle$ можно сопоставить с горизонтальным (0°) и вертикальным (90°) направлениями линейной поляризации фотона (базис "+", помечен желтым цветом на рис.1), а $|0_B\rangle$ и $|1_B\rangle$ – сопоставить с двумя диагональными (ортогональными) направлениями линейной поляризации, направленными под углами 45° и 135° (или -45°) (базис "×" помечен синим цветом на рис.1). Два состояния, принадлежащие к одному и тому же базису, являются ортогональными, то есть их можно надежно различить при измерении в том же базисе, тогда как измерение в другом (неправильном) базисе, например, в базисе (0°, 45°) даст абсолютно случайный результат (с вероятностью 50% это может быть "1" или "0").

Протокол BB84

Протокол BB84 был предложен Беннеттом и Брассаром в 1984 году. По этому протоколу осуществляются следующие действия, описанные ниже и иллюстрируемые пятью группами рисунков (1–5 сверху вниз) на рис. 1:

1. Алиса посылает последовательность фотонов, имеющих случайную (0°, 45°, 90°, 135°) поляризацию;
2. Боб измеряет поляризацию фотонов, выбирая базис "+" (0°, 90° – линейная поляризация) или "×" (45°, 135° – диагональная линейная поляризация) по случайному закону;
3. Боб фиксирует полученные результаты измерений, сохраняя их в секрете (отдельные фотоны могут быть не приняты вовсе – потеряны или "стерты");
4. Боб сообщает затем Алисе по открытому каналу, какие базисы ("+" или "×") он использовал для каждого принятого фотона (но не полученные им результаты), а Алиса сообщает ему, какие базисы из использованных были правильными (данные, полученные при измерениях в неправильных базисах, отбрасываются);
5. Оставшиеся данные интерпретируются в соответствии с условленной схемой (0° и 45° декодируются как "0", а 90° и 135° – как "1") как двоичная последовательность (11001).

Полученная последовательность бит является "черновым вариантом" ключа, подлежащим уточнению [7] (см. краткое описание этой процедуры ниже применительно к протоколу B92).

Протокол B92

B92 был предложен Беннеттом в 1992 году [8], который показал, что для кодирования "0" и "1" могут быть использованы не четыре, как в протоколе BB84, а любые два неортогональных поляризованных состояния $|\psi_0\rangle$ ("0") и $|\psi_1\rangle$ ("1"), произведение которых лежит в интервале (0,1): $0 < \|\langle\psi_0|\psi_1\rangle\|^2 < 1$. Для кодирования состояния "0" Алиса может использовать линейную поляризацию 90° (V), а для "1" – диагональную линейную поляризацию, повернутую на угол 45° [см. рис. 2]. Стандартный вариант реализации предполагает, что Боб при измерении будет декодировать как "1" состояние с линейной (горизонтальной) поляризацией 0° (H) и как "0" – состояние с диагональной линейной поляризацией, повернутой на угол 135° (-45°). Могут быть выбраны и другие варианты.

Идея такого упрощения основана на том, что если измерение, которое могло бы (согласно принципу неопределенности) различить два неортогональных квантовых состояния, нельзя осуществить, то невозможно с уверенностью идентифицировать конкретный бит. Более того, любая попытка изучения этого бита приведет к заметной модификации его состояния.

Этапы реализации передачи, приема и декодирования бит квантового ключа показаны на рис. 2.

1. Алиса, согласовав с Бобом процедуру сравнения при декодировании, посылает Бобу сгенерированную последовательность ПСПФ;
2. Боб применяет к ней случайным образом один из двух ортогональных базисов "+" или "×" (как и в протоколе BB84), вычисляя возможные значения посланных бит. Таких значений может быть в принципе три – "1", "0" и "?". Последний вариант означает, что с вероятностью 50% результат может быть "1" или "0". Кроме

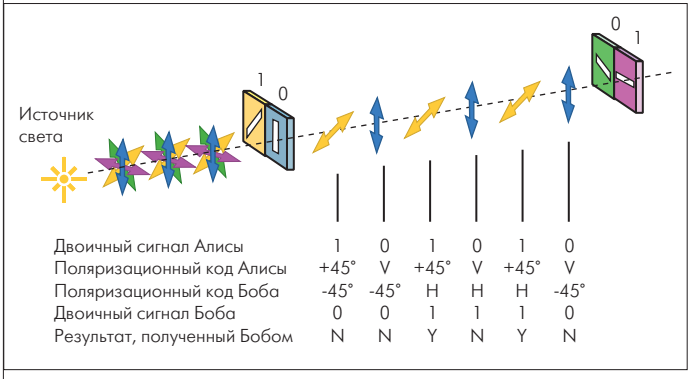

Рис.2. Формирование квантового ключа по протоколу B92

этого, в канале могут произойти стирания, когда Боб ничего не фиксирует в принятом битовом интервале;

3. После приема Бобом последовательности бит и отбрасывания неопределенных позиций остается N заведомо определенных позиций, которые и принимаются за "черновой вариант" ключа.

Уточнение чернового варианта ключа

При последующем уточнении чернового варианта ключа путем обмена определенными данными по открытому каналу Алиса и Боб могут либо получить *вариант ключа, годный для совместного использования* (shared key) (в отсутствие подслушивания примерно половина полученных ими данных может быть абсолютно коррелированной), либо отбросить черновой ключ и повторить процедуру генерации и передачи квантового ключа. Открытым каналом связи может быть любой канал связи или Интернет, на котором реализован, например, стандартный алгоритм RSA с открытым ключом. Уточнение может состоять из следующих четырех этапов (более подробно см. [9]).

- *Оценка ошибки* – Алиса объявляет подмножество из K позиций чернового варианта ключа длиной N и соответствующие им значения бит. Боб также посылает ей биты, полученные в этих же позициях. Оба (Алиса и Боб) вычисляют по ним ошибку наблюдений **e** на длине подмножества K и одобряют результат передачи квантового ключа, если $\mathbf{e} \le \mathbf{e}_{макс}$ (установленного Алисой в процессе конфигурации протокола B92), или нет – в противном случае, после чего процесс передачи повторяется снова. В случае одобрения объявленное подмножество из K бит удаляется из чернового варианта ключа, и одобренный ключ длиной N–K подвергается процедуре согласования.
- *Согласование* – Алиса и Боб осуществляют процедуру согласования одобренного ключа с использованием итеративного алгоритма коррекции ошибок на основе контроля четности (например, в [9] используется специальный алгоритм CASCADE). Учитывая, что процедура согласования позволяет, с одной стороны, сохранить больше бит в итоговой реализации квантового ключа, а с другой стороны, существенно замедляет процесс, а значит, и скорость передачи секретного ключа, нужно подходить к ее реализации гибко, отдавая предпочтение или итоговой длине (при дорогом квантовом канале), или скорости передачи ключа. Если для согласованного ключа оценка ошибки $\mathbf{e} > \mathbf{e}_{макс}$, то процесс передачи должен повториться снова, если нет, то согласованный ключ подвергается процедуре подтверждения правильности.
- *Подтверждение правильности* – Алиса выбирает L (например, 10) случайных подмножеств $X_1 \ldots X_L$ и объявляет X_i вместе с показателем четности бит в них. Боб сравнивает объявленные Алисой четности бит и сообщает ей, где они у него совпадают. Если некоторые биты четности не совпадают, то процесс передачи должен повториться снова; если все биты совпадают, то мы получаем *подтвержденный согласованный ключ*, который уже может рассматриваться как *ключ, годный для совместного использования* с вероятностью $1-2^L$. Учитывая, что это все-таки не полностью секретный ключ, он может быть подвергнут процедуре усиления секретности.
- *Усиление секретности* – Алиса объявляет Бобу описание случайно выбранной хэш-функции **f** из некоторого класса F, которая потом может быть применена к подтвержденному согласованному ключу для получения итогового *полностью случайного ключа* $X_f = f(X_A) = f(X_B)$, где X_A и X_B частично секретные подпоследовательности в $\{0,1\}^{N-K}$, полученные после подтверждения правильности согласованного ключа. Эта процедура позволяет, в принципе, получить *статистически секретный ключ*.

В результате Алиса и Боб получают идентичные последовательности, которые и являются секретным ключом, с помощью которого они смогут шифровать и дешифровать секретную информацию и обмениваться ею, используя незащищенный от прослушивания канал связи. Разумеется, все действия, начиная от передачи ПСПФ и кончая ее дешифрацией с помощью секретного ключа, должны осуществляться автоматически под управлением компьютера.

То, что черновой вариант ключа требует такой серьезной проверки, неудивительно. Импульсы реальной последовательности, генерируемой передатчиком, могут быть неоднофотонными, а сами однофотонные приемники могут иметь большой уровень шума спонтанной эмиссии. Поэтому данные Алисы и Боба будут различаться даже при отсутствии факта подслушивания. Если же такой факт возможен, то очевидно, что Ева в результате подслушивания может получить правильные сведения о поляризации не более чем половины фотонов, поскольку ей не известны все базисы, используемые Алисой и Бобом. Если в данных Алисы и Боба нет расхождений в результате серии указанных проверок, то можно заключить, что оставшаяся часть ключа содержит мало ошибок (если они вообще есть), а Еве известна лишь малая часть ключа.

СИСТЕМЫ С КВАНТОВОЙ ПЕРЕДАЧЕЙ КЛЮЧА

Существует несколько типов *систем квантовой передачи ключа*. Основные из них – это *системы с поляризационным кодированием* и *с фазовым кодированием*. Первый тип систем появился раньше, и мы рассмотрим его в первую очередь.

Системы с поляризационным кодированием

Схема одной из первых лабораторных квантовых криптосистем с поляризационным кодированием по протоколу BB84 с четырьмя состояниями поляризации (0°, 45°, 90°, 135°), так, как она была реализована авторами – Беннетом и Брассаром в 1988 году, показана на рис.3. [10]. В ней свет зеленого светоизлучающего диода (СИД) формируется диафрагмой в точечный источник, который с помощью конденсорной линзы преобразуется в коллимированный пучок, дополнительно формируемый апертурным экраном и фильтром. Этот пучок горизонтально поляризуется линейным поляризатором. Угол (плоскость) поляризации может затем дискретно меняться с помощью двух активных поляризационных модуляторов, типа ячейки Поккельса (см., например, в [11]). Для каждого светового импульса модуляторы, активированные по случайному закону, формируют в фотоне (переносимом импульсом) одно из четырех описанных выше состояний поляризации.

В качестве квантового канала передачи используется свободное пространство (длина канала – 30 см – ограничена, очевидно, размерами оптической скамьи). Принимающая сторона случайным образом дополнительно вращает (или же нет) поляризацию принимаемых импульсов на 45° благодаря еще одной ячейке Поккельса,

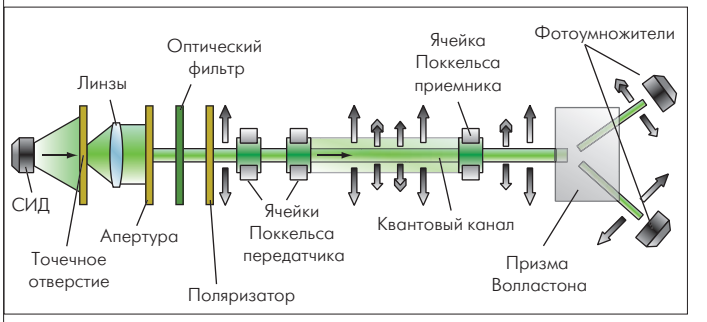

Рис.3. Схема квантовой криптосистемы Беннета и Брассара с ячейками Поккельса в качестве поляризаторов

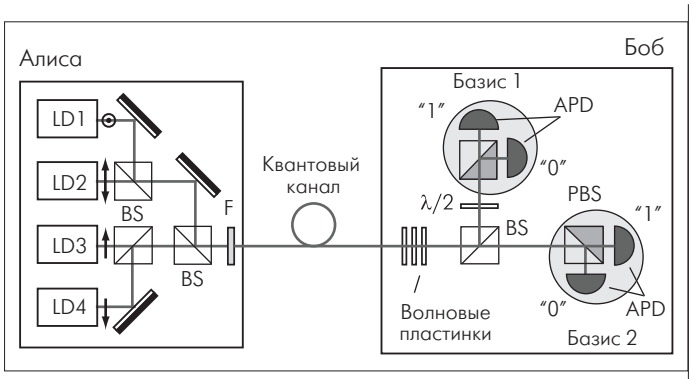

Рис. 4. Схема квантовой криптосистемы с поляризационным кодированием

давая возможность формировать базисы "+" и "×". С выхода ячейки Поккельса луч попадает на призму Волластона – двулучепреломляющую призму, используемую для разделения ортогональных линейно-поляризованных сигналов, при этом (рассматривая вариант обработки в базисе "+") горизонтально поляризованный луч дешифруется правым (нижним) приемником-фотоумножителем, а вертикально поляризованный луч дешифруется левым (верхним) приемником-фотоумножителем.

Другой пример квантовой криптосистемы с поляризационным кодированием по протоколу BB84 приведен на рис. 4. Система, впервые вынесенная за рамки лаборатории, состояла из двух блоков, связанных оптоволоконным (ОВ), а не воздушным пространственным каналом.

Блок на стороне Алисы состоит из четырех лазерных диодов (LD), излучающих короткие (1 нс) световые импульсы, фотоны которых могут быть поляризованы в базисе "+" (90° и 0°) и в базисе "×" (-45°, 45°). Для передачи одного бита включается один из диодов. Импульсы от LD ослабляются фильтром F для уменьшения количества фотонов, приходящихся на один импульс, до величины порядка единицы. После этого они вводятся в волокно квантового канала и передаются на приемный блок Боба.

Основным требованием, накладываемым на квантовый канал, является сохранение поляризации фотонов на всем пути следования к блоку Боба, чтобы Боб имел возможность получить информацию, кодируемую Алисой, в неискаженном виде. *Поляризационная модовая дисперсия* (ПМД) может изменить поляризацию фотонов, если вносимая ей задержка больше времени когерентности, что накладывает ограничение на используемые типы лазеров.

На стороне Боба импульсы проходят через ряд волновых пластинок (имитирующих контроллер поляризации), используемых для восстановления исходных поляризационных состояний путем компенсации изменений, вносимых волокном. Затем луч света расщепляется с помощью расщепителя BS и подается на два *поляризационных расщепителя* (PBS), формирующих два типа базиса: "×" (1) и "+" (2).

Принятые фотоны анализируются в двух PBS: в нижнем – с базисом 2 ("+"), использующим прямой луч, прошедший через BS, при помощи двух счетчиков фотонов (APD); в верхнем – с базисом 1 ("×"), использующим луч, отраженный от BS вверх, при помощи двух аналогичных счетчиков фотонов (APD). Поляризация отраженных вверх фотонов поворачивается волновой пластинкой (λ/2) на 45° (с -45° до 0° и с 45° до 90°), реализуя, таким образом, измерения в диагональном базисе.

А.Мюллер и др. [12] использовали подобную криптосистему для проведения экспериментов в области квантовой криптографии. Им удалось передать квантовый ключ на расстояние 1100 метров, используя фотоны с длиной волны 800 нм. Для увеличения длины передачи они использовали фотоны с длиной волны 1300 нм [13] и достигли 23-километровой дистанции передачи ключа. В качестве квантового канала использовался стандартный оптоволоконный кабель.

Эти эксперименты показали, что изменения поляризации, вносимые оптическим волокном, нестабильны. Причем поляризация может резко меняться, хотя и может иметь короткие периоды стабильности (порядка нескольких минут). Это значит, что квантовая криптографическая система требует создания механизма стабилизации или активной компенсации таких изменений. Такие механизмы стабилизации и способы автоматического контроля поляризации существуют [14], но они малоэффективны и пока не используются. Замечено также, что использование вместо стандартного ОВ волокна с сохранением поляризации не решает проблему, хотя и позволяет увеличивать длину участка с контролируемой поляризацией.

Системы с фазовым кодированием

Идея кодирования бит, используя фазу оптического излучения, была впервые высказана Беннеттом в статье [7]. Формирование квантовых состояний и их анализ может в этом случае проводиться интерферометрами, которые легко реализуются на базе компонентов волоконной оптики.

Понятие фазы оптического излучения (благодаря корпускулярно-волновому дуализму) справедливо не только для светового луча (т.е. волны в классической оптике), но и для одиночных фотонов (т.е. частиц, в квантовой оптике), поведение которых (расщепление, сложение и интерференция) интерпретируется, однако, как волновое.

Для этих целей может быть использован интерферометр Маха-Цендера вместе с однофотонным источником излучения и детекторами фотонов. Блок на стороне Алисы тогда будет содержать источник, разветвитель и фазовый модулятор РМφ_A, а блок на стороне Боба будет состоять из фазового модулятора РМφ_B, разветвителя и детекторов APD, вероятность регистрации фотона на одном из выходов которых ("0" или "1") будет меняться с изменением фазы. На рис. 5 показана схема криптосистемы с использованием двух ОВ-интерферометров Маха-Цендера (Алисы – А и Боба – В), соединенных ОВ-кабелем [15].

Как видно из рисунка, передатчик Алисы посылает поток одиночных фотонов длиной волны 1550 нм в виде сильно ослабленных

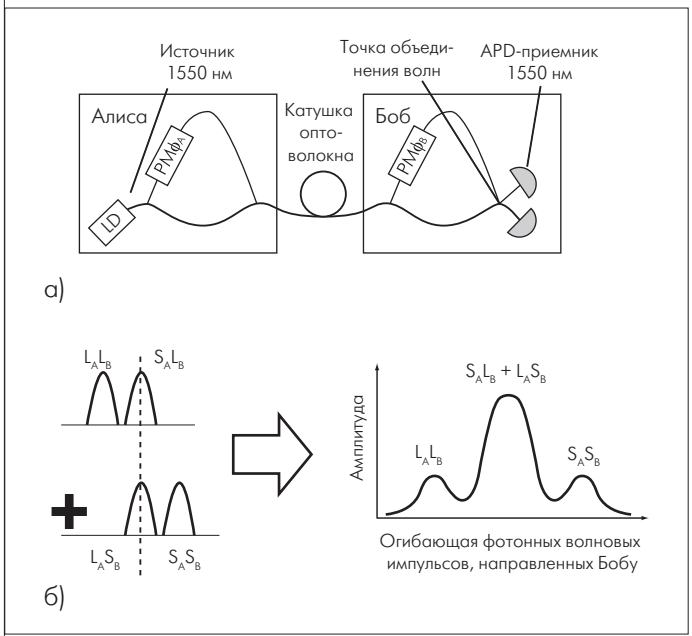

Рис.5. Схема квантовой криптосистемы с двумя интерферометрами Маха-Цендера

лазерных импульсов (формируя так называемое звено слабой когерентности). Каждый из этих фотонов проходит через интерферометр Маха-Цендера, который случайно модулируется с помощью РМφ_A, устанавливаясь на одну из четырех фаз (вариант, соответствующий использованию протокола BB84), действующую на интервале прохождения импульса. Тем самым модулируется "фаза" волнового образа фотона, выбранная на основе используемого базиса ("+","×") и значения ("0","1"), важных при самоинтерференции на выходе интерферометра.

Приемник на стороне Боба содержит другой похожий интерферометр, случайно модулируемый с помощью РМφ_B для установления одной из двух фаз, требуемой для установления нужного базиса. Фотон, пройдя интерферометр Боба, восстанавливает, интерферируя на выходном разветвителе, свое состояние, попадая на один из детекторов ("0" или "1") APD. Для синхронизации работы детекторов Алиса посылает (используя WDM-мультиплексор, не показанный на рис. 5) в то же волокно мощные импульсы с длиной волны 1300 нм для синхронизации и стробирования диодов APD.

На рис. 5 показан механизм прохождения фотонов от источников у Алисы до детекторов APD у Боба (без учета факта использования модуляции). На рис. 5а показаны несбалансированные интерферометры Маха-Цендера, плечи которых исходно разные: нижние (короткие) имеют длину S_A и S_B, а верхние (длинные) – длину L_A и L_B. Это значит, что плечи имеют разную временную задержку на распространение волнового импульса. Фотон, рассматриваемый как волна, расщепляется на два одинаковых луча первым разветвителем (50/50) у Алисы. Нижний проходит путь S_A, а верхний – L_A до выходного разветвителя, где лучи объединяются, образуя дипульс L_AS_A, который, пройдя квантовый ОВ-канал, доходит до входного разветвителя (50/50) интерферометра Боба. Затем он снова расщепляется на два одинаковых луча. Нижний проходит путь S_B, а верхний – L_B до выходного разветвителя Боба, где они образуют два дипульса: нижний L_AS_B/S_AS_B и верхний – L_AL_B/S_AL_B. Объединение их показано на рис.5б. Оно приводит (при условии идентичности/настроенности обоих интерферометров) к формированию волны с тремя пиками: большим центральным ($S_AL_B+L_AS_B$) и двумя боковыми (L_AL_B и S_AS_B).

Для описания действия модуляции в данной системе вспомним законы отражения/преломления:

- Фаза луча, отраженного от границы раздела двух сред (с показателем преломления n_1 и n_2), сдвигается на $\pi/2$, если $n_2 > n_1$, и не изменяется, если $n_2 < n_1$;
- Фаза луча, преломленного на границе раздела двух сред (если луч существует), не изменяется.

На рис. 6 показано [15], что центральный пик в фотонном импульсе содержит *интервал когерентности* (рис. 6а), внутри которого одновременно присутствуют волновые образы двух различных путей: S_AL_B и L_AS_B, фазы которых, в общем случае, сдвинуты относительно друг друга на некоторую величину Δ (рис. 6б). Эти два волновых образа взаимодействуют (интерферируют) при объединении на выходе интерферометра в точке разветвления у Боба (на рис. 6в показана граница раздела сред в этой точке). Применяя законы отражения/преломления и предполагая, что ниже этой границы раздела среда более плотная, получим, что отраженная верхняя и преломленная нижняя волны окажутся в противофазе и уничтожат друг друга (это называют иногда *деструктивной интерференцией*), что фиксируется с помощью APD как "0" (т.е. фотон не фиксируется), а отраженная нижняя и преломленная верхняя волны окажутся в фазе и усилят друг друга (это называют иногда *конструктивной интерференцией*), что фиксируется APD как "1" (т.е. фотон не фиксируется).

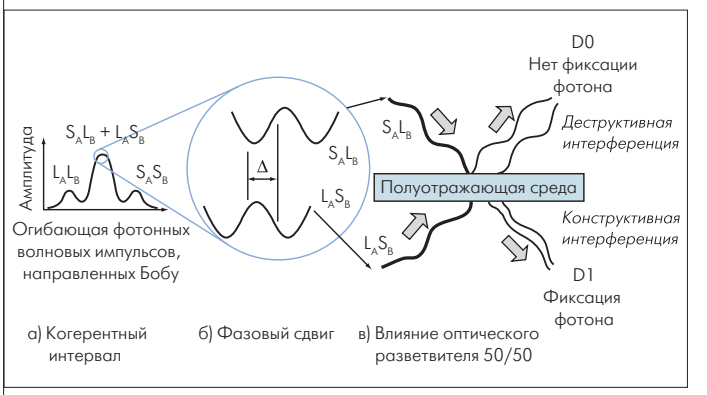

Рис.6. Механизм выбора "0" и "1" с помощью APD и интерферометра на стороне Боба

Настройка правильности срабатывания APD осуществляется путем подстройки фазового сдвига Δ от импульса к импульсу, что и делает Алиса путем установки нужной величины сдвига фазы для фазосдвигающей схемы своего РМφ_A для каждого передаваемого импульса.

Рассмотрим такую схему кодирования для протокола BB84 с четырьмя состояниями. Алиса кодирует "0" и "1" для одного фотона в любом из двух случайно выбранных неортогональных базисов (обозначим их как 0 и 1). Так она может представить значение бита "0" фазовым сдвигом 0° (в базисе 0) или $\pi/2$ (в базисе 1), а значение "1" – фазовым сдвигом π (в базисе 0) или $3\pi/2$ (в базисе 1). Итак, Алиса может формировать один из четырех фазовых сдвигов ($0, \pi/2, \pi, 3\pi/2$) путем выбора четырех кодовых комбинаций в пространстве состояний "бит-базис": (00, 01, 10, 11). Это можно осуществить, подавая четыре различных напряжения (условно: 0, 1, 2, 3) на электрооптическое фазосдвигающее устройство.

Боб выбирает базис, сдвигая в случайном порядке фазу на 0 или $\pi/2$, и присваивает APD, подсоединенному к выходу "0", значение 0, а APD, подсоединенному к выходу "1" – значение 1. Когда разности фаз равны 0 или π, Алиса и Боб используют совместимые базисы и получают определенный результат. В этих случаях Алиса может определить, в какой из детекторов Боба попадет фотон и какое значение 0 или 1 получено. Боб также может заключить, какую фазу выбирала Алиса при передаче каждого фотона. Если же разность фаз равна $\pi/2$ или $3\pi/2$, то Алиса и Боб используют несовместимые базисы, и фотон случайным образом выбирает один из детекторов Боба. Все возможные комбинации сведены в таблицу.

Основная трудность реализации данной системы в том, что несбалансированность интерферометров Алисы и Боба должна быть стабильной в пределах долей длин волны фотонов во время передачи ключа для сохранения нужных фазовых соотношений. Это значит,

что интерферометры должны быть в термостабилизированных контейнерах, а системе нужно обеспечить компенсацию дрейфа фазы. Кроме того, изменения поляризации в коротком и длинном плечах в каждом интерферометре должны совпадать, т.е. требуется использовать контроллеры поляризации.

Состояния для фазового кодирования/декодирования протокола BB84

Алиса			Боб		
Бит	φ_A	Бит + базис	φ_B	φ_A-φ_B	Бит
0	0	00	0	0	0
0	0	00	$\pi/2$	$3\pi/2$	? (0/1)
0	$\pi/2$	01	0	$\pi/2$	? (0/1)
0	$\pi/2$	01	$\pi/2$	0	0
1	π	10	0	π	1
1	π	10	$\pi/2$	$\pi/2$	? (0/1)
1	$3\pi/2$	11	0	$3\pi/2$	? (0/1)
1	$3\pi/2$	11	$\pi/2$	π	1

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Анализируя описанное выше, можно понять основные проблемы квантовой криптографии и передачи квантового ключа. О некоторых мы уже упоминали. Эти проблемы грубо можно разделить на два класса: методологические и технологические. К методологическим проблемам можно отнести проблему секретности, подслушивания, возможности перехвата и дешифрации сообщений. Этот класс проблем, ввиду его специфичности, требует отдельного углубленного исследования, поэтому мы его не будем здесь рассматривать. Желающие кратко войти в курс этого класса проблем могут обратиться к обзору в работе [16].

Технологические проблемы и перспективы роста длины передачи определяются, с одной стороны, типом используемого кодирования, а с другой – теми сложностями процедуры уточнения, которые мы отмечали выше и которые неизбежно влияют на допустимую точность и надежность формирования итогового секретного квантового ключа.

Проблемы систем с поляризационным кодированием, как отмечено выше, кроются в среде передачи. Если она сохраняет поляризацию на длине L неизменной, то может использоваться для квантового канала передачи. Такой средой является свободное пространство, однако при ее использовании длина передачи L ограничивается обычно 1 км (и меньше при дожде и тумане) ввиду большого затухания сигнала в атмосфере, хотя известны и системы рекордной длины – 10 км при хорошей погоде [17]. Использование ОВ в качестве среды передачи также ограничено, но не затуханием сигнала, а случайным изменением состояния поляризации волокна, которое имеет место даже в специальных волокнах, сохраняющих состояние поляризации, хотя достигнутые результаты (23 км) и выглядят обнадеживающе [13].

Изложенное говорит о том, что поляризационное кодирование не оптимально при построении криптосистем с квантовым ОВ-каналом, хотя оно и эффективно для криптосистем с каналом связи в открытом пространстве.

Использование фазового кодирования выглядит более перспективным, так как снимает ограничения, накладываемые изменением поляризации, на использование стандартного ОВ. Успехи в этом направлении Таунсенда и др., разработавших систему на ОВ длиной в 10 км в 1993 году [18], были позже подкреплены увеличением дальности передачи этой системы до 30 км [19]. Результаты по дальности передачи с использованием ОВ-канала постоянно растут. Так, в работе [20] сообщалось об успешной передаче ключа на расстояние 67 км, а компания MagiQ сообщила [21] о создании первой коммерческой квантовой криптосистемы, позволяющей обмениваться секретными ключами уже на расстоянии до 120 км. Но и это не было пределом. Сегодня рекордная дальность передачи установлена компанией NEC, которая успешно передала ключ по квантовому ОВ-каналу на 150 км [22], побив свой же рекорд (100 км), установленный за год до этого, за счет оптимизации параметров оптических детекторов и интерферометров.

Технологические проблемы и перспективы роста скорости передачи ключа. Указанная выше дальность и скорость соответствует факту передачи не итогового секретного ключа, а одного фотона, зафиксированного APD в результате интерференции на выходе разветвителя Боба. Фактическая же скорость передачи может быть гораздо ниже благодаря необходимости уточнить первоначально полученную последовательность. Так, те же авторы сообщили в работе [23], что достигнутая ими скорость передачи составила 100 кбит/с при установленной длине передачи 40 км.

Главной причиной низких скоростей, кроме уже упомянутых, являются большие потери в системах QKD. Типичной величиной потерь считается 30 дБ [24]. В этом смысле за последнее десятилетие наиболее эффективным и коммерчески жизнеспособным зарекомендовал себя протокол B92. При его использовании ослабление сигнала может достигать 99,7% (при теоретическом минимуме в 50%). Используя этот протокол, криптосистема с оптимальным уровнем ослабления сигнала в 98,75% способна передавать ключ со скоростью до 1 Мбит/с, что, по крайней мере, на порядок выше возможностей существующих систем другого типа.

Специалисты видят выход из положения в использовании техники стробирования APD, открывающей APD в нужный момент времени, однако до недавнего времени синхронизирующие стробы передавались асинхронно (перед переданным импульсом или пакетом импульсов). В работе [24] предложено применять синхронную технику стробирования, используя параллельный канал передачи данных на другой несущей. Им может быть, например, синхронный поток импульсов гигабитного Ethernet (в кодировке 8B/10B), передаваемый на скорости 1,25 Гбит/с. Такой вариант стробирования позволяет существенно увеличить фактическую скорость передачи (теоретически до скорости синхропотока), а также увеличить и дальность передачи за счет увеличения отношения сигнал/шум детектора фотонов.

В заключение нужно отметить, что при передаче квантового ключа в криптосистеме приходится преодолевать значительные трудности, вызванные нюансами, которые здесь не освещены за недостатком места и определенной направленностью статьи. К ним относятся проблемы создания надежного источника одиночных фотонов, равно как и однофотонного приемника; проблемы принципиального уменьшения уровня шумов приемников (не только путем использования их глубокого охлаждения); проблемы компенсации многочисленных изменений состояния поляризации фотона или изменения фазы его эквивалентной волны за счет случайных изменений поляризации и фазы в ОВ, наличия ПМД и других эффектов.

Важно то, что все это уже работает, имеются промышленные системы квантовой криптографии, которые начинают внедряться в жизнь, делая, казалось бы, жизнь бизнеса (и нашу в свете заверений о происках террористов) более безопасной. Нельзя, однако, не отметить, что существуют и альтернативные (скептические) точки зрения на возможности и, главное, на необходимость квантовых систем; желающих отправляем к работе [25].

ЛИТЕРАТУРА

1. Смарт Н. Криптография. / Пер. с англ. под ред. С.К.Ландо. – М.: Техносфера, 2005.

2. **Shor P.W.** Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos, ed. by Sh.Goldwasser (IEEE Computer Society Press), 1994, p.124–134.
3. **Gisin N.** et al. Quantum Cryptography. – Reviews of Modern Physics, 74, p.145–195 (2002).
4. **Bruss D., Luetkenhaus N.** Quantum Key Distribution: From Principles to Practicalities. – arXiv:quant-ph/9901061 v2 (1999).
5. **Скалли М.О., Зубайри М.С.** Квантовая оптика. / Пер. с англ. под ред. В.В.Самарцева. – М.: Физматлит, 2003. – 512с.
6. **Bennett C.H., Brassard G.** Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, – 1984, p.175–179.
7. **Bennett C.H.** et al. Experimental Quantum Cryptography. – Journal of Cryptography, 1992, No.5.
8. **Bennett C.H.** Quantum Cryptography Using Any Two Nonorthogonal States. – Phys. Rev. Letters, Vol.68, 3121 (1992).
9. Implementation of the B92 QKD protocol. – www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92prot.html
10. **Nazarian Sh.** CS556: Quantum Cryptography. – http://poisson.usc.edu/~shahin/QC
11. **Слепов Н.Н.** Современные технологии цифровых оптоволоконных сетей связи. – 2-е изд. исправл. – М.: Радио и связь, 2003. – 468с.
12. **Muller A.** et al. Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km. – Europhysics Letters, 1993, 23.
13. **Muller A.** et al. Quantum cryptography over 23 km in installed under-lake telecom fibre. – Europhysics Letters, 1996, 33.
14. **Okoshi T.** Polarization-State Control Schemes for Heterodyne or Homodyne Optical Fiber Communications. – Journal of Lightwave Technology, Vol. LT-3, 1985, No.6, p.1232–1237.
15. **Elliott Ch.** et al. Quantum cryptography in practice. – BBN Technologies. Preprint, May 1, 2003.
16. **Вахитов А.В.** Оценка защищенности практической квантово-криптографической системы на основе волоконно-оптических линий связи от несанкционированного доступа. – Магистерская диссертация. СПб. ГТУ, 2000. – 50с.
17. **Hughes R.**, et al. Practical free-space quantum key distribution over 10 km in daylight and at night. – New J. Phys. 4, July 2002, 43.
18. **Townsend P.D.**, et al. Single photon interference in 10 km long optical fibre interferometer. – Electronics Letters 1993, Vol.29, No.7, 1993, p.634–635.
19. **Marand C.** et al. Quantum Key Distribution over Distances as Long as 30 km. – Optical Letters, 1995, Vol.20, No.16, p.1695.
20. **Stucki D.** et al. Quantum key distribution over 67 km with a plug & play system. – New J. Phys. 4, July 2002, 41.
21. First Commercial Quantum Cryptography System, 3.11.2003. – www.magiqtech.com (magiq_navajo_launch.pdf)
22. **Tomita A.** et al. Recent Progress in Quantum Key Transmission. – NEC J. of Advanced Tech., Vol.2, No.1, p.84–91.
23. **Tanaka A.** et al. – 30th ECOC, Stockholm, Sweden (Sep. 5–9, 2004), Tu4.5.3.
24. **Bienfang J.C.** et al. Quantum key distribution with 1.25 Gbps clock synchronization. – Optic Express, Vol.12, No.9, p.2011.
25. **Берд К.** Квантовая криптонеопределенность. – www.computerra.ru/print/xterra/37181/