государственной власти субъектов Российской Федерации".

Марченко Д.С.
студент 5 курса
кафедра «Информационной безопасности и телекоммуникационных систем»
Институт компьютерных технологий и информационной безопасности
Южный федеральный университет
Россия, г. Таганрог

КВАНТОВЫЕ ДЕНЬГИ БУДУЩЕГО

Аннотация. В данной статье освещена история возникновения квантовой криптографии. Приведена идея Визнера о защищенных деньгах с помощью квантовой криптографии.

Ключевые слова: квантовые деньги, оптическая ловушка, поляризация фотона.

История квантовой криптографии зародилась еще в 1960-е годы в США. В то самое время, когда студент Нью-Йоркского Колумбийского университета Стивен Визнер поведал своему бывшему однокурснику идею возможности применения квантовых состояний для защиты денежных купюр.

В 1969 году молодой аспирант закончил свою статью и попытался опубликовать её в журнале IEEE Transactions on Information Theory под названием «Conjugate coding», но все усилия были напрасны, так как в то время его суждения посчитали фантастическими и не отнеслись к ним с должной серьезностью. Только в 1983 г. статья вышла в свет в издании ACM Newsletter Sigact News и получила высокую оценку в научном сообществе.

Самое притягательное в задумке защиты банкнот квантовым контролем подлинности, что он базируется не на математической модели, чему присущи сложные вычисления и вполне известные злоумышленнику алгоритмы, а на физическом способе.

Смысл задумки заключается в том, чтобы на каждую купюру нанести несколько квантовых микрообъектов. Это могут быть несколько десятков оптических ловушек и фотоны, поляризованные под установленным углом.

Каждой банкноте присваивается серийный номер (СН), который также содержится в базе данных банка (БД) вместе с поляризацией фотона, как показанно на рисунке 1. Если купюра будет обращаться в банке, то не составит труда проверить в БД соответствие на купюре СН и поляризации фотонов с первого раза.

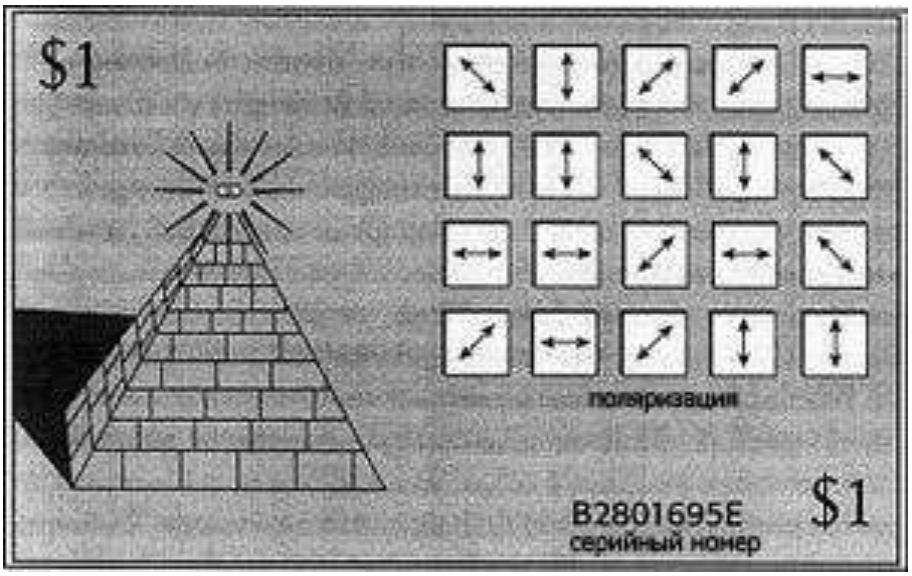

Рисунок 1 – квантовая купюра, показанная в статье Визнера

При попытке злоумышленника подделать купюры, либо сделать копию это легко будет заметно банку. Дело в том, что на каждое преступное деяние есть лишь 1 попытка. После несоответствия поляризаций фотон просто «исчезает», что ограничивает преступника в сведениях об этом фотоне. Поэтому банк определит злоумышленника при первой же ошибке в подделке банкноты.

Чтобы минимизировать «удачную попытку» преступника, высчитывается наивысшая вероятность допущения ошибки по формуле (5/6) n, где n - количество фотонов на купюре).

В предложенном методе защиты денег Визнера существует и немало недостатков, основные это: помехи и превышения полномочий банка, выпускающих данный вид купюр.

Помехи могут появиться в результате воздействия шума и небрежного обращения, так как квантовое ядро само по себе достаточно чувствительно, в следствии чего с течением времени код может немного измениться. Это послужило тому, что, сейчас, ученые вынуждены отказаться от 100% сходства и сойтись на 90% соответствии. Справедливо отметить, что это качественный результат, так как в нынешнее время преступникам удается подделать до 95% знаков на купюрах.

Что касается проблемы наделением власти банка-эмитента или его сотрудников, то этот вопрос, должен решиться внедрением технических новинок и принятием правовых норм, которые будут регулироваться законом.

Завершая статью хочется сказать, что в наше время технология «квантовых денег» активно развивается, так как фальшивомонетчикам предвещают большое будущее. В этих условиях физики продолжают разработку и изучение квантовых денежных средств, которые не поддавались бы подделке.

Использованные источники:
1. Stephen Wiesner, «Conjugate coding», Columbia University, New York, N.Y., Vol. 15 Issue 1, Winter-Spring 1983 Pages 78 – 88
2. Andrew Lutomirski, «Unexpected Problems For Quantum Money», December 23, 2009
3. Scott Aaronson, Edward Farhi, David Gosset, «Breaking and making quantum money: toward a new quantum cryptographic protocol», Tsinghua University, Beijing, China, January 5-7, 2010.

Марченко Д.С.
студент 5 курса
кафедра «Информационной безопасности и телекоммуникационных систем»
Институт компьютерных технологий и информационной безопасности
Южный федеральный университет
Россия, г. Таганрог

КВАНТОВАЯ КРИПТОГРАФИЯ: МЕТОД КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, СТАНЦИИ: «АЛИСА», «БОБ»

Аннотация

Данная статья позволяет рассмотреть метод квантового распределения ключей. Также подробно получить сведения о том, как работает система на базе станций «Алиса» и «Боб».

Ключевые слова: Метод квантового распределения ключа, станции: Алиса, Боб

Метод квантового распределения ключа (Quantum Key Distribution, QKD) — это способ передачи ключа шифрования по оптическому каналу при помощи одиночных фотонов. Попытка злоумышленником перехвата или измерения, интересующих его, параметров физических объектов, которые в данном случае являются переносчиками информации, в любом случае приведет к искажению других параметров. В результате, отправитель и получатель обнаруживают попытку получить несанкционированный доступ к информации.

В квантовой криптографии зафиксировали два основных направления развития систем распределения ключей. Первое направление зиждиться на кодировании квантового состояния одиночной частицы и основывается на принципе невозможности определить абсолютно надёжно два не ортогональных квантовых состояния.

Безопасность первого направления базируется на теореме о запрете клонирования неопределенного квантового состояния. С помощью целостности и линейности квантовой механики, нет никакой возможности создать клонируемую копию неизвестного квантового состояния без прямого воздействия на штатное состояние.