МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра оптики и биофотоники

Применение квантовых технологий для защиты информации

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента магистратуры 2 курса 2223 группы
направления 03.04.02 «Физика»,
профиль «Квантовые технологии»
института физики

Петровой Марии Тимофеевны

Научный руководитель,
доцент, к.ф.-м.н. _____ П.А. Дьяченко
должность, уч. степень, уч. звание — инициалы, фамилия

Зав. кафедрой,
д.ф.-м.н., профессор _____ В.В. Тучин
должность, уч. степень, уч. звание — инициалы, фамилия

Саратов 2023

Введение. С появлением письменности как средства передачи информации возникла концепция канала утечки информации. Отправлялись письма, гонцы и дипломаты. Большое внимание уделялось войнам, определенным государственным проблемам. Другими словами, пока информация не приносит вреда, нет необходимости ее защищать. Так было в античности, в средние века, в эпоху Возрождения и т.д., и так продолжается до сих пор.

Развитие технологий передачи информации прогрессировало, сейчас у нас есть телефоны, компьютеры, различные современные устройства для хранения информации и другие современные способы передачи информации, но по сути проблемы, существовавшие ранее, все еще существуют.

В течение нескольких лет криптографы экспериментировали с методами шифрования/дешифрования, чтобы создать эффективные и надежные методы защиты связи между двумя или более легитимными субъектами. Из-за огромного объема данных, которыми обмениваются через Интернет, классическая криптография может не обеспечить достаточной защиты. Поэтому ученые ищут более надежную систему, основанную на законах физики. Квантовая система - это следующее решение для криптографии, где квантовая криптография обладает силой квантовой механики. Возможности квантовой криптографии были впервые представлены Визнером и Беннетом в 1979 году. Квантовая криптография использует физические теории для создания секретного ключа, который может быть совместно использован общающимися сторонами.

Цель работы – изучение механизмов и процессов, которые используются для создания секретного ключа в квантовой системе с помощью протоколов QKD, таких как протокол BB84, протокол SARG04, протокол B92, протокол Coherent-One-Way (Когерентный односторонний) (COW), протокол KMB09, протокол EPR, протокол S09, протокол Differential-Phase-Shift (Дифференциально-фазовый сдвиг) (DPS). Несмотря на то, что в мире квантовой криптографии было объявлено о многих интересных протоколах

QKD, эти протоколы QKD определяют наиболее применимые и известные протоколы.

Задачами работы являются:

1) проведение обзора и анализа литературы на тему «Применение квантовых технологий для защиты информации»;

2) ознакомление с принципом квантового распределения ключей;

3) Проведение сканирования угла фазовой пластинки HWP_{B2} в диапазоне от 0º до 200º, при этом измерение количества единичных отсчетов в детекторе;

4) Определение средней частоты фотоотсчетов, вызванных входным состоянием света, и частоты шумовых отсчетов, угола при котором частоты фототсчетов в детекторах D_{B-} и D_{B+} выравниваются;

5) Реализация протоколов BB84 и SARG04;

6) Определен процент ошибок в результате обработки сгенерированного ключа;

7) проведение анализа результатов измерений и расчёт их погрешности.

Дипломная работа занимает 74 страницы, имеет 16 рисунков и 4 таблицы.

Литературный обзор составлен по 86 информационным источникам.

В первой, обзорной по характеру, главе определяется понятие классической криптографии.

Во второй главе излагается история возникновения квантовой криптографии, а также описан принцип квантового распределения ключей.

В третьей главе подробно описано квантовые протоколы передачи данных.

В четвертной главе проведено практическое сравнение реализации квантовых протоколов BB84 и SARG04.

Этому направлению уделяется пристальное внимание во всём мире, в том числе в нашей стране. Доказательством этому – национальная программа «Цифровая экономика Российской Федерации», согласно которой квантовая криптография вместе с квантовыми вычислениями выделена в отдельное направление развития и отнесена к сквозным технологиям.

Основное содержание работы

Квантовая криптография использует принципы квантовой физики для безопасной обработки информации. Ярким примером является безопасная связь, т.е. задача передачи конфиденциальных сообщений из одного места в другое. Криптографическое требование здесь заключается в том, чтобы передаваемые сообщения оставались недоступными для кого-либо, кроме назначенных получателей, даже если канал связи не заслуживает доверия. В классической криптографии это обычно может быть гарантировано только при условии вычислительной сложности, например, когда факторизация больших целых чисел невыполнима. В отличие от этого, безопасность квантовой криптографии полностью зависит от законов квантовой механики.

Квантовая криптография основана на фундаментальных и неизменных принципах квантовой механики. Фактически, квантовая криптография опирается на два столпа квантовой механики 20-го века - принцип неопределенности Гейзенберга и принцип поляризации фотонов. Согласно принципу неопределенности Гейзенберга, невозможно измерить квантовое состояние любой системы, не нарушив эту систему. Таким образом, поляризация фотона или частицы света может быть известна только в тот момент, когда она измеряется. Этот принцип играет важную роль в пресечении попыток подслушивания в криптосистеме, основанной на квантовой криптографии. Во-вторых, принцип поляризации фотонов описывает, как фотоны света могут быть ориентированы или поляризованы в определенных направлениях. Более того, фотонный фильтр с правильной поляризацией может обнаружить только поляризованный фотон, иначе фотон будет уничтожен.

Практическое сравнение реализации квантовых протоколов BB84 и SARG04.

Схема экспериментальной установки приведена на рисунке 12 В качестве источника используется ослабленный непрерывный лазер с длиной волны излучения 810 нм. Действия Отправителя имитируются с помощью фазовой плстинки HWP_{B1}, а действия Получателя – с помощью фазовой пластинки

HWP_{B2}. Четвертьволновые пластинки QWP_{B1} и QWP_{B2} в данной задаче не используются. Дополнительные потери в оптическую схему вносятся нейтральным фильтром NF, которые устанавливаются между фазовыми пластинками Отправителя и Получателя.

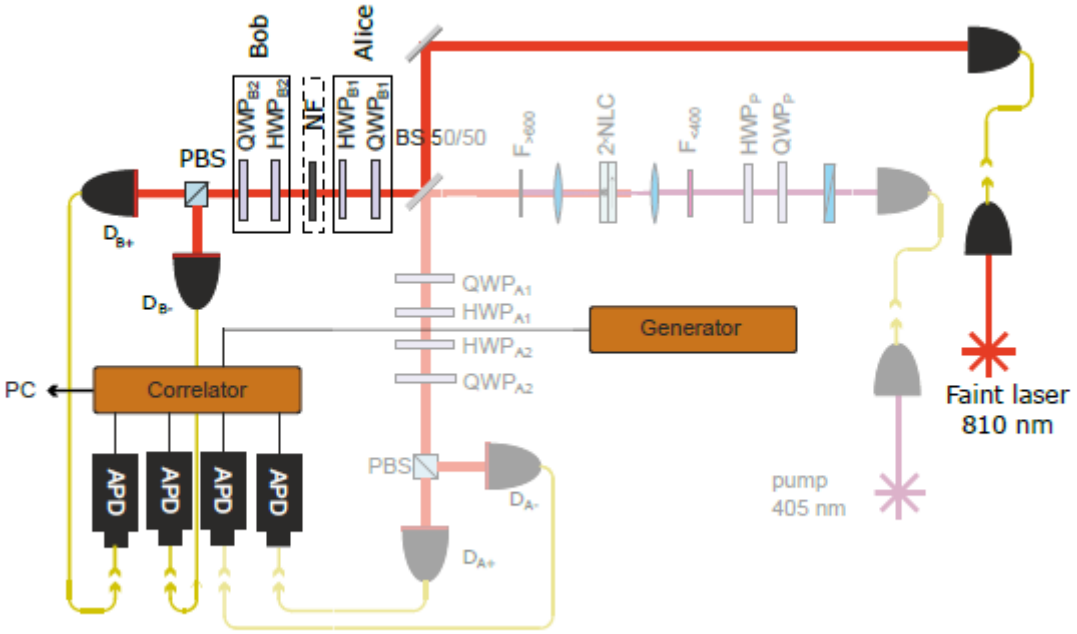


Рисунок 12. Экспериментальная установка.

Частота единичных отсчетов используемых детекторов D_{B-} и D_{B+} много больше 1. Для реализации однофотонного режима в канал 2 коррелятора подается сигнал с генератора импульсов с частотой 10 кГц. Затем регистрируются совпадения сигналов детекторов с сигналом генератора, а в настройках коллерятора устанавливается ограничение максимального суммарного числа совпадений равным 1.

В связи с этим, сначала на старт схемы совпадений приходит сигнал с генератора, затем с одного из детекторов поступает один отсчет, число совпадений становится равным 1, и измерения останавливаются. (В этом случае не может быть зарегистрировано 0 отсчетов в обоих детекторах.

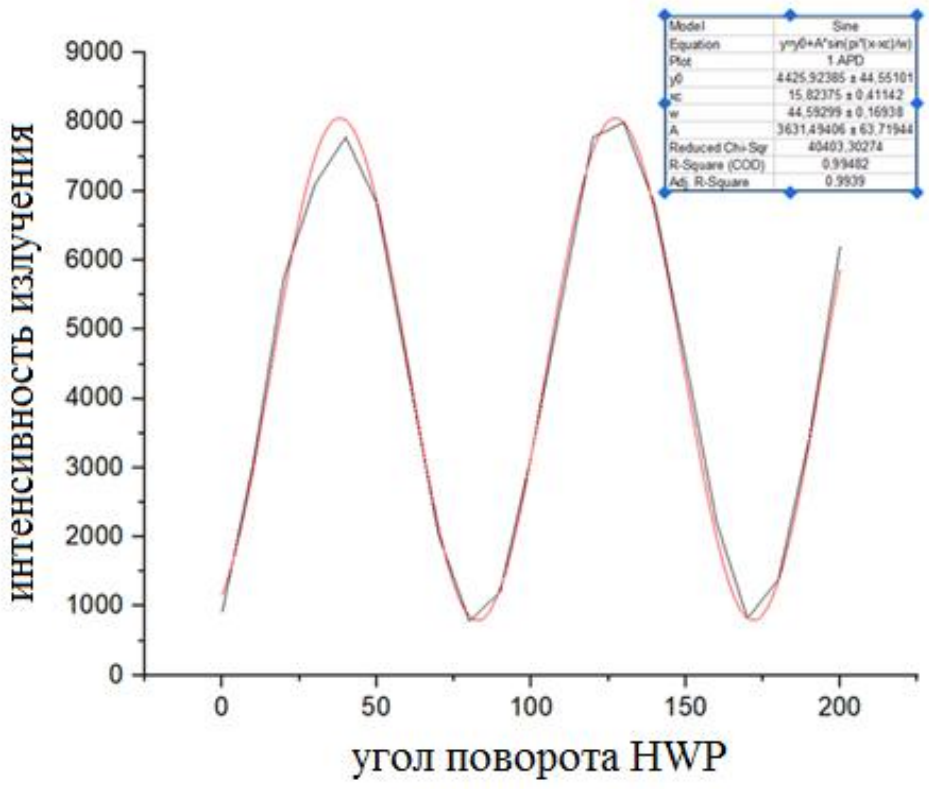
Ход работы:

1. Калибровка установки

Все фазовые пластинки установлены под углом 0º.

Время накопления 1с. Проведено сканирование угла фазовой пластинки HWP_{B2} в диапазоне от 0º до 200º, при этом измерено количество единичных отсчетов в детекторе.

Проследили изменения интенсивности в каналах 1 и 2 в зависимости от угла поворота пластины.



Интенсивность в каналах 1 и 2 в зависимости от угла поворота пластины.

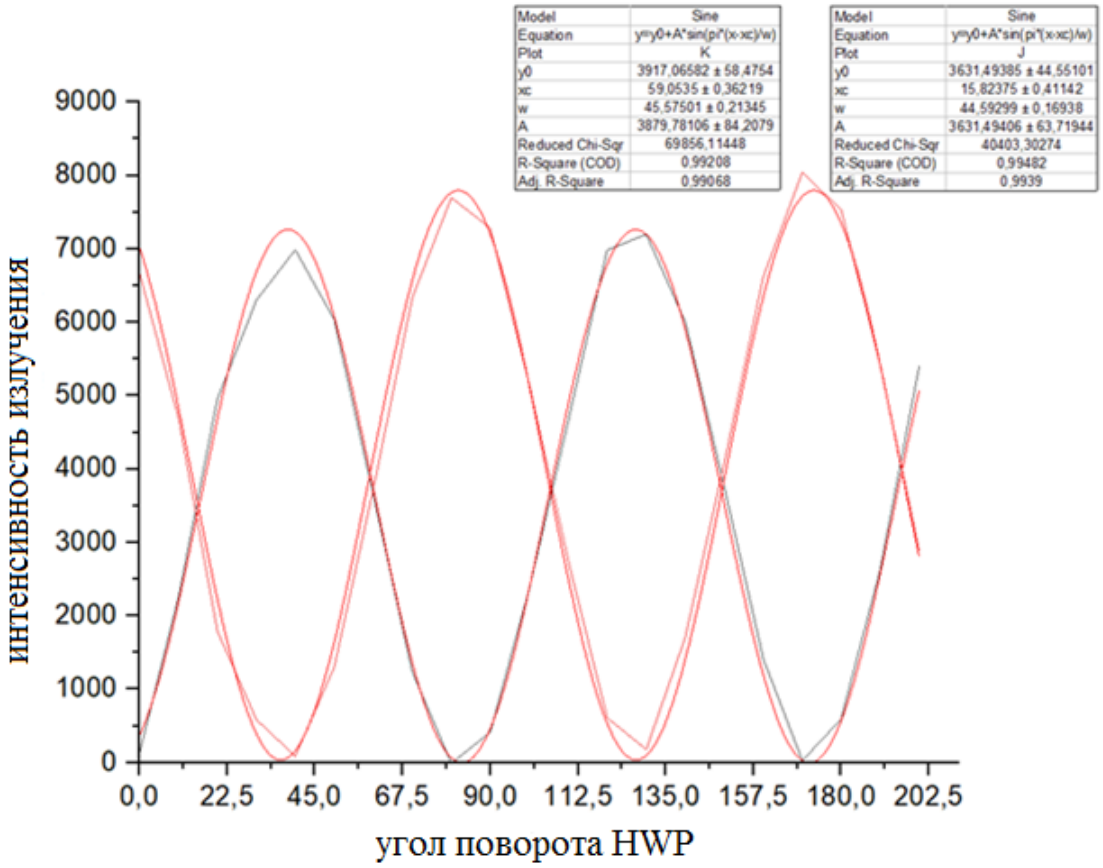


График аппроксимируемый синусоидой

По графику определена средняя частота фотоотсчетов = 794,4, вызванных входным состоянием света, и частота шумовых отсчетов =8039,57.

Угол при котором частоты фототсчетов в детекторах D_{B-} и D_{B+} выравниваются =17

1. Статистика когерентного состояния

   В настройках коррелятора установлено ограничение по максимальному числу единичных отсчетов в канале генератора, равное 1. Тогда на каждый импульс генератора программа выдает количество фотонов, зарегистрированных каждым из детекторов. Все пластинки установлены под углом 0°.

   Вывод пороговой величины коэффициента пропускания T

$$P(n) = \frac{\mu^n}{n!} e^{-\mu}$$

$$\frac{P(n>1)}{P(n\geq 1)} > T$$

Учитывая что

$$P(n \geq 1) = 1 - P(1) - P(0)$$

$$P(n > 1) = 1 - P(0)$$

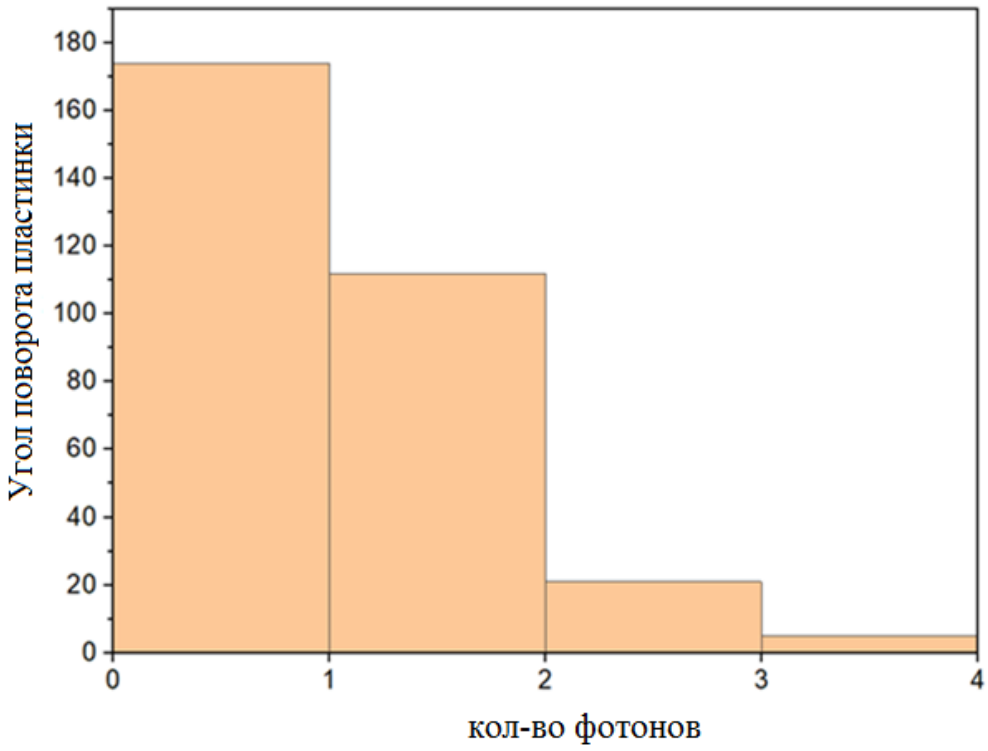
и $e^{-\mu} = 1 - \mu$

тогда

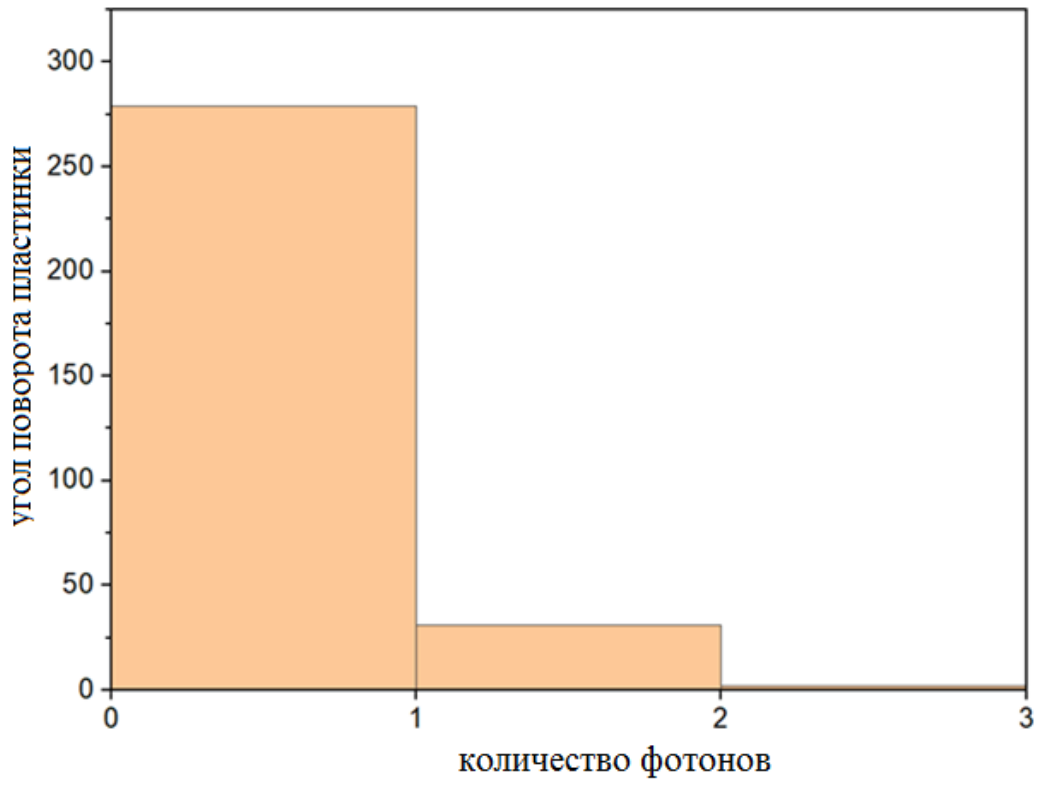
$$\frac{1 - \mu e^{-\mu} - e^{-\mu}}{1 - e^{-\mu}} = \frac{1 - (1 - \mu)\mu - (1 - \mu)}{1 - (1 - \mu)} = \mu$$

$\mu > T$

Построила гистограммы для каждого канала:



Гистограмма сигнальных фотонов



Гистограмма шумовых фотонов

Состояние	Дисперсия	Среднее число фотонов
Сигнальное	0,480573419078241	0,541666666666667
Шум	0,112777228130926	0,112179487179487

Реализация протоколов КРК

В данном упражнении учитываются только те входные импульсы, при которых был получен фотоотсчет в одном из детекторов.

1. BB84

	A	B	C	D	E	F	G
1	Abasis	Abit	AHWP	Bbasis	Bbit	BHWP	Процент ошибок
2	1	1	22,5	1	0	22,5	4,545454545455
3	1	1	22,5	1	1	22,5	
4	1	0	-22,5	1	0	22,5	
5	0	1	0	0	1	0	
6	1	0	-22,5	1	0	22,5	
7	1	1	22,5	1	1	22,5	
8	1	1	22,5	1	1	22,5	
9	1	0	-22,5	1	0	22,5	
10	0	1	0	0	1	0	
11	1	1	22,5	1	1	22,5	
12	0	0	45	0	0	0	
13	1	1	22,5	1	1	22,5	
14	0	1	0	0	1	0	
15	1	0	-22,5	1	0	22,5	
16	1	1	22,5	1	1	22,5	
17	0	1	0	0	1	0	
18	0	1	0	0	1	0	
19	1	0	-22,5	1	0	22,5	
20	0	0	45	0	0	0	
21	1	0	-22,5	1	0	22,5	
22	0	0	45	0	0	0	
23	1	1	22,5	1	1	22,5	

Где стобцы A,B,C – значения отправителя, а столбцы D,E,F – значения получателья.

В результате обработки ключа было отброшено 23/51 сгенерированного ключа. Из оставшегося процент ошибок составляет: 0,05.

2. SARG04

	A	B	C	D	E	F	G
1	Abit	AHWP	BHWP	Bbit	ОШИБКИ	Процент ошибок	
2	0	-22,5	0	1	1	28,125	
3	0	-22,5	0	1	2		
4	1	22,5	22,5	1			
5	0	-22,5	22,5	0			
6	0	45	22,5	1	3		
7	1	0	0	1			
8	0	-22,5	22,5	0			
9	0	45	22,5	1	4		
10	1	22,5	22,5	1			
11	1	22,5	22,5	1			
12	0	-22,5	0	1	5		
13	0	-22,5	22,5	0			
14	1	22,5	0	0	6		
15	1	0	0	1			
16	1	22,5	22,5	1			
17	0	-22,5	0	1	7		
18	0	45	0	0			
19	1	22,5	22,5	1			
20	1	0	22,5	0	8		
21	1	0	0	1			
22	0	-22,5	22,5	0			
23	1	22,5	22,5	1			
24	1	0	0	1			
25	1	0	0	1			
26	0	-22,5	22,5	0			
27	0	45	0	0			
28	0	-22,5	22,5	0			
29	1	0	0	1			
30	0	-22,5	0	1	9		
31	0	45	0	0			
32	1	22,5	22,5	1			

Где стобцы A,B, – значения отправителя, а столбцы C, D – значения получателя.

В результате обработки ключа было отброшено 32/51 сгенерированного ключа. Из оставшегося процент ошибок составляет: 0,28.

Вывод:

Генерация секретного ключа для SARG04 протокола шифрования оказалась не секретная. Анализ ключа по BB84 привел к меньшему количеству ошибок, чем в SARG04. Генерация секретного ключа BB84 эффективней, но в нем проще Злоумышленнику оказаться не замеченной при атаке с расщеплением фотонов.

Заключение. Передача и хранение данных в современных реалиях, где данные чрезвычайно важны, должны быть настолько безопасными, насколько это возможно. Эти две традиционные процедуры симметричных ключей и методы открытого доступа (включая RSA, El Gamal, ECC и DSA) находятся под реальной угрозой со стороны квантовых компьютеров (3DES, AES). Создается впечатление, что мы все ближе подходим к созданию полностью целенаправленного всемирного квантового компьютера, который сможет использовать влиятельные квантовые алгоритмы. Результатом этого технологического развития является полный крах современных безопасных методов открытого ключа, таких как RSA и криптосистемы с эллиптическими кривыми.

Исследования в сфере квантовых технологий все еще продолжаются, чтобы разработать усовершенствованные протоколы и повысить безопасность уже существующих. Но до сих пор все разработанные протоколы являются вариантами протокола BB84. Возможно, будут разрабатываться все новые и новые протоколы, которые будут предоставлять более безопасные и надежные варианты. Появление методов криптографии, не подверженных влиянию квантовых вычислений, является решением этой угрозы.