Абеуов Д.Р., Карагандинский университет имени академика Е.А. Букетова, физико-технический факультет, гр. ФПК-406, студент
Төлеген Н.Т., Карагандинский университет имени академика Е.А. Букетова, физико-технический факультет, гр. ФПК-206, студент
(Научный руководитель – ассоциированный профессор Аймуханов А.К.)

ИССЛЕДОВАНИЕ ГЕНЕРАЦИИ КВАНТОВОГО КЛЮЧА В ОДНОФОТОННЫХ СИСТЕМАХ СВЯЗИ

В настоящее время системы коммуникации имеют критические значения, что повышает потребность в разработке безопасных методов доставки информации. Алгоритм шифрования с помощью секретных ключей позволяет безопасно обмениваться информацией через открытый канал при наличии потенциального перехватчика. Современная криптография не только практикует, но и изучает методы безопасной связи между двумя удаленными пользователями при возможном риске утечки информации. Протоколы криптографических методов демонстрируют неидентифицируемые сообщения, которые могут быть прочитаны только отправителем и получателем, обеспечивая что зашифрованное сообщение, отправленное по публичному каналу будут недоступны для третьих лиц [1].

В настоящей работе представлен эксперимент по изучению протокола квантовой криптографии BB84. Для проведений исследований была собрано экспериментальная установка на базе источника света, приемника оптического излучения и системы поляризаторов (рисунок 1).

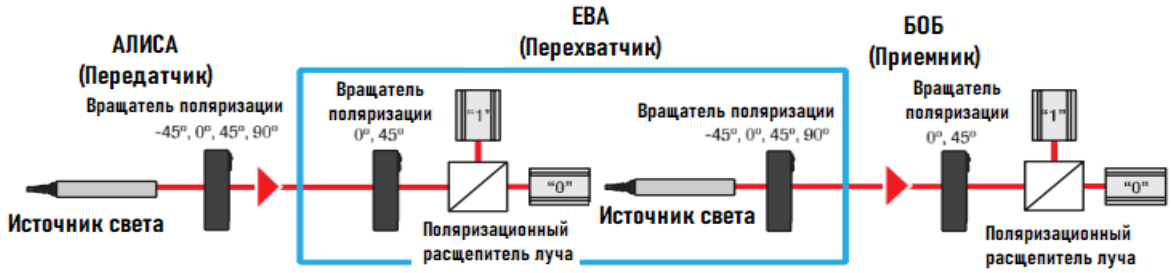

Рисунок 1 – Схема экспериментального криптографа

Протокол BB84 функционирует путем определения двух базисов, каждый из которых включает две поляризации света: базис + состоит из поляризаций 0° и 90°, а базис x - из поляризаций -45° и 45°. В этой схеме любой базис используется для представления двоичного 0 (0° или - 45°) и двоичной 1 (90° или 45°) (таблица 1) [2].

Таблица 1 – Указание для выбора между битом и базисом поляризационного вращателя

λ/2	Базис	Бит
90°	+	0
	+	1
45°	x	0
-45°	x	1

Рассмотрим работу публичного обмена информацией без перехватчика. Алиса посылает случайный бит в случайном базисе, а Боб определяет его в случайном базисе. Затем они обмениваются базисами по общедоступному каналу. Если каждый из них использовал свой базис, измерение отбрасывается; если базис одинаков, оба уже сгенерировали ключевой бит. Поскольку публичный обмен содержит только базис, бит неизвестен другим (таблица 2,3).

Таблица 2 – Измерительный протокол для генерации ключей - Алисы

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Базис (+ или x)	+	+	x	+	+	x	x	x	+	x	x	+	+	x	x	+	+	x
Бит (0 или 1)	0	1	0	1	0	0	1	0	1	0	1	0	0	1	0	0	1	1

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Базис (+ или x)	x	x	+	+	+	x	x	x	+	+	x	x	x	+	x	+	x	+
Бит (0 или 1)	0	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	0

Таблица 3 – Измерительный протокол для генерации ключей - Боба

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Базис (+ или x)	+	+	x	+	x	x	+	+	x	+	x	+	+	x	x	+	x	x
Бит (0 или 1)	0	1	0	1	1	0	1	1	1	0	1	0	0	1	0	0	1	1

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Базис (+ или x)	+	+	+	x	+	x	x	x	+	x	x	+	+	x	x	+	x	x
Бит (0 или 1)	1	1	0	1	1	0	1	1	0	1	0	0	0	1	0	1	0	1

Обмениваясь битами и базисами Алиса и Боб сгенерировали ключ: 01010 10010 01010 11001. После, с помощью Алисы зашифровываем слово (таблица 4) используя только что сгенерированный ключ, надо отметить что во время шифрования используется метод двоичного сложения.

Таблица 4 – Зашифровка слова

Слово	S					T					O					P				
Бит данных	1	0	0	1	0	1	0	0	1	1	0	1	1	1	0	0	1	1	1	1
+																				
Сгенерированный ключ	0	1	0	1	0	1	0	0	1	0	0	1	0	1	0	1	1	0	0	1
Зашифрованное письмо	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	0	0	1

Затем к установке добавляем Ева, и эксперимент проводим следующим образом. Алиса посылает бит, Ева пытается его перехватить, а затем Ева посылает бит Бобу в той базе, которую она выбрала для своего измерения. В конце эксперимента Алиса и Боб сравнивают свои базы

посредством публичного обмена, а также несколько тестовых битов. Если они обнаружат, что примерно 25% тестовых битов теперь неверны (из-за ошибок в битах, посланных Евой), они узнают о присутствии подслушивающего устройства. Мы посылали 52 бита, из них 28 базисов совпали (таблица 5.1, 5.2).

Таблица 5.1 – Точность 52 бита для эксперимента и моделирования - с Евой

x	+	+	x	+	+	x	+	x	+	x	x	+	+	+	x	+	+	x	x	+	x	+	+	+	x	x	x
1	0	1	1	0	1	1	0	1	1	1	0	0	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1
x	+	+	x	+	+	x	+	x	+	x	x	+	+	+	x	+	+	x	x	+	x	+	+	+	x	x	x
0	1	1	1	1	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	1	0	1	1	0	0	0	1

Таблица 5.2 – Итоги точности эксперимента и моделирования - с Евой

Подходящие базисы	28
Соответствующие биты	18
Несоответствующие биты	10
Вероятность присутствия подслушивающего устройства	34,6%

Измерения для 32 битов без подслушивающего устройства показали точность примерно 50% совпадения битов от общего количества отправленных битов. Это соответствует теории, согласно которой Алиса и Боб создают надежный ключ для шифрования.

Измерения для различных последовательностей битов с подслушивающим устройством показали точность примерно 35% совпадения битов от общего числа отправленных битов. Как объяснялось ранее, такая точность предупреждает Алису и Боба о том, что в системе присутствует подслушивающее устройство, поэтому им необходимо создать новый ключ.

Литература:

1. Yuval Bloom, Ilai Fields, Alona Maslennikov and Georgi Gary Rozenman. Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation // Physics 2022

2. ThorLabs, Quantum Cryptography Demonstration Kit // 2020

Амангельдина А.А., Карагандинский университет имени академика Е.А. Букетова, биолого-географический факультет, гр. МБТ-61, магистрант
(*Научный руководитель – к.б.н., ассоциированный профессор Тлеукенова С.У.)*

ВЛИЯНИЕ КРИОПРОТЕКТОРОВ НА ЖИЗНЕСПОСОБНОСТЬ СЕМЕННОГО МАТЕРИАЛА *VERBASCUM SONGARICUM*

Сохранение биоразнообразия генофонда растений важнейшая проблема, с которой сейчас может сталкнуться человечество [1]. Так сохранение биоразнообразия это один из механизмов стабильности жизни на Земле

В настоящее время лекарственные и дикие виды растений являются традиционным источником генетического материала. Следует отметить, что рост городов и сельскохозугодий, вырубки лесов, а также бедственное состоянием экологии эти факторы начинают постепенно вытесняться виды растений [2]. Множество растений находится на грани вымирания и исчезновения, в следствии чего их необходимо сохранить. Казахстан имеет большой запас хозяйственно ценных растений. Поэтому это делает их оптимальными для использования в промышленности. Казахстан характеризуется богатейшим генофондом флоры, а также уникальным запасом полезных растений. Дикие растения, обладающие лечебными свойствами, и значительная часть из них подходят для изучения химического состава и биологической