Университет ИТМО
Физико-технический мегафакультет
Физический факультет

УНИВЕРСИТЕТ ИТМО

Группа М3304 К работе допущен
Студент Васильков Д.А, Лавренов Д.А. Работа выполнена
Преподаватель Шоев В.И. Отчет принят

Рабочий протокол и отчет по лабораторной работе №5.06
“Квантовая криптография”

1) Цель работы

1. Изучение основных принципов квантовой связи
2. Создание зашифрованного сообщения
3. Обнаружение перехватчика

2) Объект исследования

1. Импульсный источник света

3) Рабочие формулы и исходные данные

Alice		***Bob***		
State	Basis, Bit	Chosen Basis	State	Measured Bit
$\|0°\rangle$	$+, 0$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
		$\times$	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
$\|90°\rangle$	$+, 1$	$+$	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	1
		$\times$	$\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
$\|45°\rangle$	$\times, 1$	$+$	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
		$\times$	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	1
$\|-45°\rangle$	$\times, 0$	$+$	$\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
		$\times$	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	0

Alice		Eve			Bob		
Basis, Bit	State	Basis	State	State Sent	Basis	State	Measured Bit
+, 0	$\|0°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	$\|0°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
					×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
		×	$\hat{M}_\times \|0°\rangle = \frac{\|45°\rangle}{\sqrt{2}} - \frac{\|-45°\rangle}{\sqrt{2}}$	$\|45°\rangle$ or $\|-45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ or $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1 0 or 1
					×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$ or $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	1 0
+, 1	$\|90°\rangle$	+	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	$\|90°\rangle$	+	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	1
					×	$\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
		×	$\hat{M}_\times \|90°\rangle = \frac{\|45°\rangle}{\sqrt{2}} + \frac{\|-45°\rangle}{\sqrt{2}}$	$\|45°\rangle$ or $\|-45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ or $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1 0 or 1
					×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$ or $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	1 0
×, 1	$\|45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} - \frac{\|90°\rangle}{\sqrt{2}}$	$\|0°\rangle$ or $\|90°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$ or $\hat{M}_+ \|90°\rangle = -\|90°\rangle$	0 1
					×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ or $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1 0 or 1
		×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	$\|45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
					×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	1
×, 0	$\|-45°\rangle$	+	$\hat{M}_+ \|-45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} + \frac{\|90°\rangle}{\sqrt{2}}$	$\|0°\rangle$ or $\|90°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$ or $\hat{M}_+ \|90°\rangle = -\|90°\rangle$	0 1
					×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ or $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1 0 or 1
		×	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	$\|-45°\rangle$	+	$\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
					×	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	0

4) Измерительные приборы

№ п/п	Наименование	Тип прибора	Используемый диапазон	Погрешность прибора
1	Детекторы сигнала	Электронный	"0"и "1"	–

5) Схема установки.

Установка состоит из: Алиса, Боб, Ева – представляют из себя три отдельные оптические плиты со следующими элементами. Алиса – лазер с блоком управления, полуволновая пластинка. Боб – полуволновая пластинка, светоделительный куб, два сенсора с блоком управления. Ева – полуволновая пластинка, светоделительный куб, два сенсора и лазер с полуволновой пластинкой.

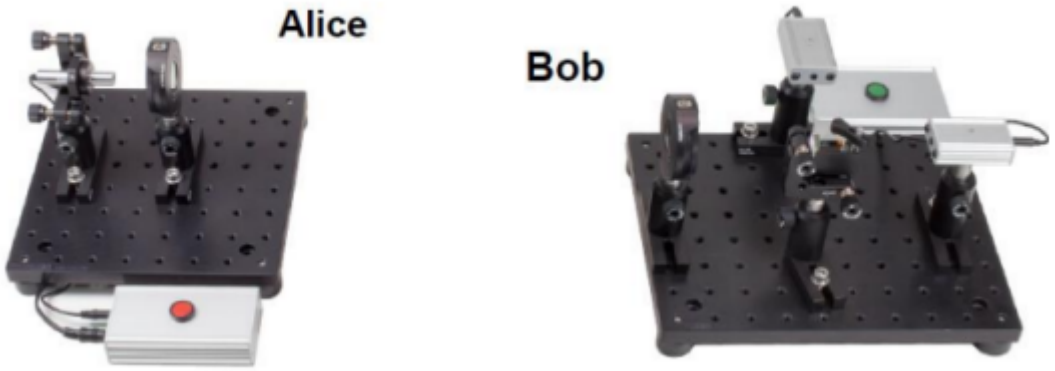

Рис. 1. Алиса и Боб

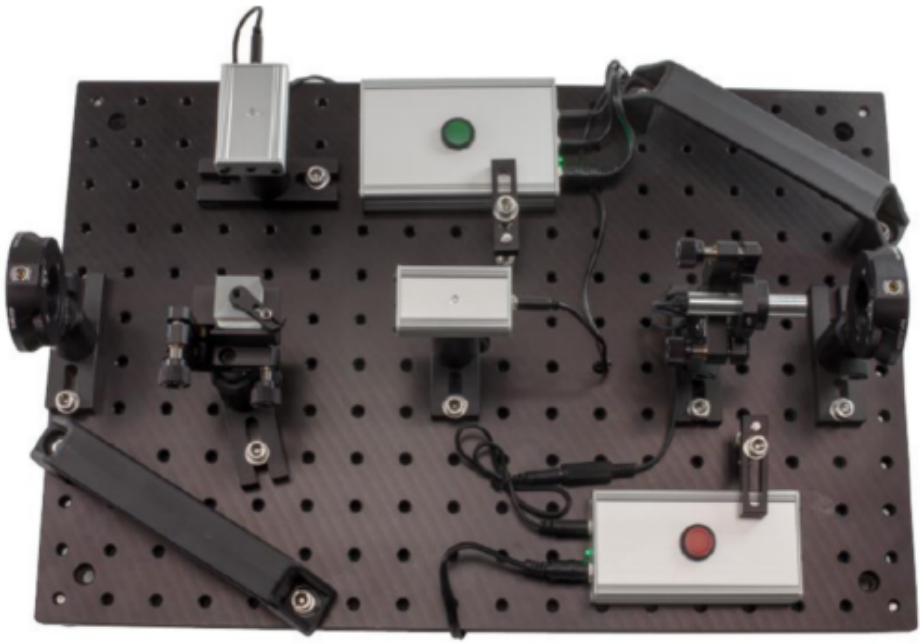

Рис. 2. Ева

Рис 3. Полуволновая пластинка

Рис. 4. Блок управления источником излучения

Рис. 5. Детектор сигнала

6) Результаты прямых измерений и их обработки (таблицы, примеры расчетов).

Alice	№	Basis	Bit	Bob	№	Basis	Bit
	1	X	1		1	+	0
	2	X	0		2	X	1
	3	+	0		3	X	0
	4	+	1		4	X	0
	5	X	1		5	+	0
	6	+	0		6	+	0
	7	+	0		7	+	0
	8	X	1		8	+	0
	9	X	1		9	X	0
	10	+	1		10	X	0
	11	X	1		11	X	0
	12	+	0		12	+	0
	13	X	0		13	+	0
	14	X	1		14	X	0
	15	+	0		15	X	0
	16	X	0		16	X	1
	17	X	0		17	X	1
	18	X	1		18	X	0
	19	+	1		19	X	0
	20	+	1		20	X	1

	21	+	1		21	+	1
	22	X	1		22	+	1
	23	+	1		23	+	1
	24	+	0		24	X	1
	25	X	0		25	X	1
	26	+	0		26	X	0
	27	+	0		27	+	0
	28	X	1		28	+	1
	29	+	0		29	X	0
	30	X	0		30	X	1
	31	+	0		31	X	0
	32	+	1		32	+	1
	33	X	1		33	+	0
	34	+	1		34	+	1
	35	+	0		35	X	1
	36	X	0		36	X	1
	37	X	1		37	+	1
	38	X	1		38	+	0
	39	X	1		39	+	0
	40	+	1		40	X	0
	41	X	1		41	X	0
	42	+	1		42	X	0
	43	X	1		43	+	1
	44	+	0		44	+	0
	45	X	0		45	X	1
	46	+	0		46	+	0
	47	+	1		47	+	1
	48	+	1		48	X	0
	49	X	1		49	X	0
	50	+	0		50	X	0
	51	+	0		51	+	0
	52	X	1		52	+	1

Таб. 1. Создания ключа длинной 20 бит

C	0	0	0	1	0										
L	0	1	0	1	1										
N	0	1	1	0	1										
Mes	0	0	0	1	0	0	1	0	1	1	0	1	1	0	1
XOR															
Key	1	0	0	0	0	0	0	1	1	0	1	1	1	1	0
Req	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1
Basis	+														
Bob	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1
Key	1	0	0	0	0	0	0	1	1	0	1	1	1	1	0
Mes	0	0	0	1	0	0	1	0	1	1	0	1	1	0	1

Таб. 2. Кодировка 3-х буквенного слова

Alice	№	Basis	Bit	Eva	№	Basis	Bit	Bob	№	Basis	Bit
	1	+	1		1	+	1		1	X	1
	2	+	0		2	X	0		2	X	1
	3	X	1		3	X	0		3	+	0
	4	+	1		4	X	0		4	+	0
	5	X	1		5	X	0		5	+	0
	6	+	1		6	X	1		6	+	1
	7	X	1		7	X	0		7	X	1
	8	+	0		8	X	1		8	X	0
	9	X	1		9	X	0		9	+	0
	10	+	1		10	+	1		10	+	1
	11	X	1		11	+	0		11	+	1
	12	+	1		12	+	1		12	+	1
	13	X	1		13	+	0		13	X	0
	14	+	1		14	+	1		14	X	1
	15	X	1		15	+	1		15	+	1
	16	X	0		16	X	1		16	+	0
	17	+	0		17	X	1		17	+	0
	18	+	0		18	+	0		18	X	0
	19	X	1		19	+	0		19	X	0
	20	X	1		20	X	0		20	+	0

21	+	1		21	X	0		21	+	0
22	X	0		22	X	1		22	X	0
23	+	0		23	X	1		23	+	0
24	X	1		24	X	0		24	+	0
25	+	1		25	+	1		25	+	1
26	X	1		26	+	0		26	+	0

Таб. 3. Введение в установку Евы и обнаружение перехватчика Алисой и Бобом

7) **Расчет результатов косвенных измерений (таблицы, примеры расчетов).**

Совпавшие базисы - 12

Несовпавшие биты в этих базисах - 4

%Ошибок = (100/12)*4=33.3%

8) **Окончательные результаты.**

%Ошибок = 33.3% > 25%

9) **Выводы и анализ результатов работы.**

В первой части лабораторной работы мы создали ключ с помощью методов квантовой криптографии и использовали его для передачи зашифрованного сообщения. Во второй части мы смогли перехватить сигнал Алисы при помощи Евы и передали его Бобу. Процент ошибок был выше 25%, что указывало на наличие перехватчика.

① Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
Basis	X	X	+	+	X	+	+	X	X	+	X	+	X	X	+	X	X	X	+	+	+	X	+	+	X	+	X	+	+	X	+	+	X	+	+	X	X	X	X	+	X	+	X	+	X	+
Bit	1	0	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	1	1	0	0	1	1	1	1	1	1	1	0	0	0

47	48	49	50	51	52
+	+	X	+	+	X
1	1	1	0	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
Bas.	+	X	X	X	+	+	+	+	X	X	+	+	X	X	X	X	X	X	X	X	+	+	+	X	X	X	+	+	X	X	X	+	+	+	X	X	+	+	+	X	X	X	+	+	X	+
Bit	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	1	1	1	1	0	0	1	0	1	0	1	0	1	1	1	1	1	0	0	0	0	0	1	1	0

1 0 0 0 0 0 0 1 1 0 1 1 1 1 0

47	48	49	50	51	52
+	X	X	X	+	+
1	0	0	0	0	1

1 0 0 0 1

(2)

C	00010
L	01011
N	01101

00010 | 01011 | 01101

Xor

key → 10000 00110 11110

10010 01101 10011

Bas. − +

Bob	10010	01101	10011
key	10000	00110	11110
	00010	01011	01101

③ Alice

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
+	+	x	+	x	+	x	+	x	+	x	+	x	+	x	x	+	+	x	x	+	x	+	x	+	x
1	0	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	1	1	1

Eve

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
+	x	x	x	x	x	x	x	x	+	+	+	+	+	+	x	x	+	+	x	x	x	x	x	+	+
1	0	0	0	0	1	0	1	0	1	0	1	0	1	1	1	1	0	0	0	0	1	1	0	1	0

Bob

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
x	x	+	+	+	+	x	x	+	+	+	+	x	x	+	+	+	x	x	+	+	x	+	+	+	+
1	1	0	0	0	1	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0