

Министерство образования Российской Федерации  
Санкт-Петербургский государственный технический университет

Радиофизический факультет

Допустить работу к защите

Кафедра радиофизики

Зав. кафедрой

В. М. Николаев

## **ДИПЛОМНАЯ РАБОТА**

**Система квантовой передачи криптографического ключа:  
автоматическая компенсация набега фазы в интерферометре**

Направление: 654200 – РАДИОТЕХНИКА

Специальность: 201500 – БЫТОВАЯ РАДИОЭЛЕКТРОННАЯ АППАРАТУРА

Выполнил студент гр. 6091/2

Брылевский А. В.

Руководитель, к.т.н, доц.

Купцов В.Д.

Консультанты: проф.  
аспирант (PhD)

Dag R. Hjelme (NTNU)  
Макаров В. В. (NTNU)

Санкт-Петербург  
2002

## Реферат

### **Система квантовой передачи криптографического ключа: автоматическая компенсация набега фазы в интерферометре**

**Цель дипломной работы** состояла в разработке методики автоматической компенсации случайного набега фазы в интерферометре системы квантовой передачи криптографического ключа, проведении соответствующих расчётов, а также в сборке, настройке и тестировании всей системы.

**Научная новизна** результатов работы заключается в том, что разработана новая методика компенсации фазового набега, не требующая применения дополнительных дорогостоящих компонентов, упрощающая систему в целом и повышающая общую надёжность установки.

**Практическая значимость** результатов работы заключается в том, что они могут быть применены при построении квантовых криптографических систем передачи закрытой информации, использующих принцип фазового кодирования.

Во **введении** описывается текущее положение в мире в области криптографии, показывается значимость криптографии в целом и необходимость создания новых видов криптографических систем (квантовых).

В **первой главе** описываются достоинства и недостатки классических криптосистем, обозначается место квантовой криптографии, описываются принципы квантовой передачи ключа, протокол BB84, а также проводится описание принципов работы основных разновидностей квантовых криптографических систем.

Во **второй главе** проводится описание экспериментальной установки, объясняется порядок её работы и практические особенности построения.

В **третьей главе** описывается разработанная методика автоматической компенсации набега фазы в интерферометре, разделённая на два этапа.

В **четвёртой главе** обсуждаются полученные результаты и проводится сравнение разработанной методики автоматической подстройки фазы с исследованиями других научных групп, работающих в данной области.

В **заключении** сформулированы основные результаты и выводы работы.

В **приложении** приведены расчёты, необходимые для проведения второго этапа автоматической подстройки фазы.

## Оглавление

Введение .....	4
Глава 1. Обзор текущего положения дел в области криптографических систем. Квантовая криптография. ....	5
§ 1.1. Классические системы криптозащиты .....	5
§ 1.2. Шифр Вернама.....	5
§ 1.3. Криптография с публичным ключом .....	7
§ 1.4. Краткая история появления систем квантовой криптографии .....	9
§ 1.5. Протокол BB84 .....	11
§ 1.6. Различные виды систем квантовой криптографии .....	15
1.6.1. Системы с поляризационным кодированием .....	15
1.6.2. Системы с фазовым кодированием.....	18
1.6.3. Системы "Plug and Play" .....	24
Глава 2. Экспериментальная установка .....	28
Глава 3. Подстройка фазы в интерферометре .....	35
§ 3.1. Алгоритм подстройки фазы.....	36
Глава 4. Полученные результаты.....	40
Заключение.....	46
Благодарности.....	47
Литература .....	48
Приложение .....	50

## Введение

В настоящее время во всём мире уделяется повышенное внимание к системам кодирования и передачи конфиденциальной информации. Во многих областях коммуникации – правительственной, дипломатической, военной, деловой, банковской сферах требуется обмениваться сообщениями таким образом, чтобы содержание этих сообщений не стало известным нежелательным людям или организациям. Обе составные части дисциплины криптологии – криптография, занимающаяся вопросами защищённой передачи информации, и криптоанализ, задачей которого является взлом (расшифровка) закодированных сообщений, – активно изучаются и проводится разработка новых методик в этих областях. На текущий момент в основе наиболее распространённых криптографических систем положен принцип защиты, заключающийся в трудности проведения работ по взлому сообщений, требующих больших вычислительных мощностей, но не исключающий полностью возможность расшифровки. Данный диплом посвящён новому направлению в области криптографии – квантовым криптографическим системам, задачей которых является 100% конфиденциальная передача сообщений. В отличие от большинства классических криптосистем, защищённость которых основывается на недоказанных математических предположениях, защищённость квантовых криптографических систем опирается на фундаментальные законы квантовой механики, что при надлежащей реализации таких систем делает принципиально невозможным чтение передаваемых сообщений третьими лицами.

Исследование, которому посвящена данная дипломная работа, проводилось в Норвежском университете науки и технологии (NTNU, г. Тронхейм) и финансировалось Норвежским советом по исследованиям (NFR) по проекту номер 119376/431.

# Глава 1. Обзор текущего положения дел в области криптографических систем. Квантовая криптография.

## § 1.1. Классические системы криптозащиты

Все современные криптографические системы делятся на два основных класса: симметричные и несимметричные. Симметричные, или системы с секретным ключом, представляют собой такие системы, в которых Алиса и Боб (принятые в научной литературе условные имена для передающей и принимающей сторон соответственно) владеют некоей информацией – ключом, который не должен быть известен Еве (условное имя для обозначения подслушивающей стороны). Ключ применяется каждый раз для кодирования и декодирования передаваемой информации.

В противоположность симметричным системам, асимметричные, или системы с открытым (публичным) ключом, имеют дело с парами ключей. Один из них (публичный ключ) используется для кодирования, в то время как другой (секретный ключ) используется для декодирования сообщений.

## § 1.2. Шифр Вернама

Шифр Вернама, предложенный Гилбертом Вернамом из АТ&Т в 1926 году, принадлежит к категории симметричных криптосистем. В схеме Вернама Алиса кодирует сообщение – последовательность бит, представленную двоичным числом  $m_1$ , используя случайным образом сгенерированный ключ  $k$ . Она попросту складывает каждый бит сообщения с соответствующим битом ключа для получения зашифрованного текста ( $s = m_1 \oplus k$ , где  $\oplus$  обозначает двоичное сложение по модулю 2). Этот текст затем посылается Бобу, который декодирует сообщение, вычитая биты ключа ( $s - k = m_1 \oplus k - k = m_1$ ).

Из-за того, что биты шифрованного текста настолько же случайны, насколько случаен ключ, они не содержат никакой информации. Поэтому защищённость этой криптосистемы доказуема по теории информации Шеннона. Более того, это единственная на сегодня криптосистема, защищённость которой строго доказуема. Абсолютная защищённость такой системы имеет место лишь при следующих условиях [2]:

1. Ключ абсолютно случаен
2. Его длина равна длине самого сообщения
3. Ключ "одноразовый" - он используется только единожды для передачи одного сообщения.

Попытки использовать один и тот же ключ много раз приводит к возникновению определённой структуры в шифрованном тексте, и Ева может этим воспользоваться. Например, если Ева перехватила два различных сообщения, зашифрованных одним и тем же ключом, она может получить сумму исходных текстов:  $s_1 \oplus s_2 = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2$  (где мы использовали свойство коммутативности  $\oplus$ ).

Очевидно, что главным недостатком такой системы является необходимость Алисе и Бобу располагать одним и тем же большим объёмом случайных данных для использования в качестве ключей. При интенсивном обмене сообщениями эти данные рано или поздно будут израсходованы, и опять возникнет проблема доставки ключа. Самый надёжный способ – личная встреча Алисы с Бобом, но в силу ряда причин такая встреча может быть невозможной. В связи с этим были предприняты попытки создать систему, в которой не было бы необходимости в секретной доставке ключа. Это привело к изобретению новых, "асимметричных" криптографических систем.

### § 1.3. Криптография с публичным ключом

Принцип криптографии с публичным ключом был впервые предложен в 1976 году Витфилдом Диффи и Мартином Хеллманом из Стенфордского университета в США. Идея заключалась в использовании двух разных ключей – одного для кодирования, а другого для декодирования сообщений. Кодирующий ключ не должен быть скрытым от потенциального противника – более того, он должен быть распространён как можно шире, чтобы любой желающий мог посылать сообщения Бобу. Таким образом, этот ключ является "публичным". В противоположность ему, декодирующий ключ должен держаться Бобом в секрете, так как только с помощью этого ключа возможно декодирование. Эти два ключа должны быть связаны между собой некоей "односторонней" функцией, которая позволила бы без труда вычислить публичный ключ из секретного, но не позволяла бы произвести обратную процедуру. Несмотря на то, что этот принцип был изобретён в 1976 году, никто в то время не знал подобной функции, которая бы удовлетворяла этому требованию. Однако в 1978 году Рональду Райвесту, Ади Шамиру и Леонарду Адельману удалось найти такую функцию, которая затем была применена в алгоритме, известном как RSA (Rivest, Shamir, Adleman). [1]

Защищённость криптографических систем с публичным ключом основана на сложности вычислений. Односторонняя функция должна позволять быстро вычислять  $f(x)$ , но должна сделать трудным вычисление  $x$  из  $f(x)$ . В контексте сложности вычислений "трудный" означает, что время вычисления растёт экспоненциально числу бит на входе, тогда как "простой" означает, что оно растёт полиномиально [2]. Интуитивно ясно, что не составит особого труда перемножить, например,  $67 \times 71$ , но нахождение простых чисел, при перемножении которых получится 4757, займёт гораздо больше времени. Защищённость алгоритма RSA основана на факторизации больших целых чисел.

На сегодня RSA считается достаточно защищённым для большинства применений современной криптографии. Наиболее популярная бесплатно распространяемая криптографическая программа PGP (Pretty Good Privacy) основана на принципе RSA. Разработанная в 1991 году Филиппом Циммерманом, PGP быстро стала популярной среди пользователей сети Интернет. Сейчас большинство банковских транзакций, система электронной покупки, коммерческие и некоммерческие системы криптографической защиты используют принципы RSA.

Таким образом, криптосистемы с публичным ключом преодолевают основной недостаток симметричных криптосистем – отпадает необходимость в обмене секретными ключами. Однако, RSA присущ серьёзный недостаток: никто ещё не доказал её защищённость. Это подразумевает, что мы не можем утверждать, что алгоритма быстрой факторизации не существует. И это ещё не всё. В 1985 году Дэвид Дойч описал принцип квантового компьютера – такого компьютера, который на качественном уровне отличается от общепринятых вычислительных систем. По словам Дойча, квантовый компьютер будет обладать вычислительной мощностью, намного превосходящей все мыслимые сегодняшние и будущие компьютерные системы. Более того, в 1994 году Питер Шор из AT&T описал алгоритм, с помощью которого квантовый компьютер сможет легко факторизовать гигантское число [22] – как раз то, что надо для взлома шифра RSA. К сожалению, Шор не смог продемонстрировать работу своего алгоритма, поскольку на тот момент квантовых компьютеров не существовало.

На сегодня никто не знает, как сконструировать квантовый компьютер. В то же время, никто не может доказать, что построение квантового компьютера вообще невозможно. Более того, мы не можем быть полностью уверены, что такой компьютер не построен в какой-нибудь секретной военной лаборатории, оставаясь скрытым от глаз

научной общественности. В истории криптологии существует достаточное количество подобных примеров – взять хотя бы алгоритм RSA. Лишь в 1997 году, когда он уже получил достаточное распространение, стало известно, что криптосистема с публичным ключом была изобретена ещё в 1969 году Джеймсом Эллисом из британского GCHQ (Government Communications Headquarters, штаба правительственных коммуникаций).

Итак, мы не можем быть абсолютно уверены в достаточной степени защищённости систем с публичным ключом. На сегодня шифр Вернама остаётся единственной системой, защищённость которой доказана. И опять мы сталкиваемся с проблемой доставки ключа. И эта проблема может быть успешно решена при помощи систем квантовой передачи ключа.

#### **§ 1.4. Краткая история появления систем квантовой криптографии**

Квантовая криптография была изобретена Чарльзом Беннеттом и Гиллсом Brassardом в 1984 году [16]. Предшественником этого изобретения была концепция "квантовых денег", которые невозможно подделать, предложенная Стивеном Визнером [17]. Идея заключалась в помещении в купюру нескольких фотонов, поляризованных в двух неортогональных базисах. В соответствии с принципом неопределённости Гейзенберга, существуют несовместимые между собой квантовые состояния, в том смысле, что измерение одного их свойства делает случайным значение другого. Итак, чтобы подделать купюру, фальшивомонетчик должен измерить состояния всех фотонов, "находящихся" в ней, и затем воспроизвести их в поддельной купюре. Однако, он не знает исходных базисов, в которых были закодированы фотоны (эта информация хранится в секрете банком, выпустившим купюру), так что измеряя одно свойство фотона (скажем, его вертикальную/горизонтальную поляризацию), он приводит в случайное состояние другое его свойство (левую/правую круговую поляризацию).

Очевидно, что такое измерение приведёт примерно к 50 % ошибок. В то же время, банк знает правильные базисы для каждого фотона, и таким образом способен получить полную информацию о квантовой системе. Он сверяет измеренные данные со своими записями, сделанными при производстве данной конкретной купюры (идентифицируя её по номеру), и выносит решение, подделка это или нет. [1]

Идея квантовых денег была блестящей, но она была также совершенно неспособной к воплощению: невозможно сохранить фотон в "ловушке" на достаточно долгое время. По этой причине статья Визнера была отвергнута несколькими научными журналами подряд.

Однако, Беннетт и Brassard восприняли эту идею по-иному: вместо того, чтобы хранить информацию, поляризованные фотоны могут передавать её по квантовому каналу. Как правило, квантовый канал представляет собой оптическое волокно – стандартное одномодовое волокно, используемое во множестве классических систем передачи данных. Отличие состоит в том, что данные по квантовому каналу передаются импульсами света, которые настолько слабые, что вероятность появления фотона в каждом из них значительно меньше единицы.

Итак, задача квантовой криптографической системы заключается в передаче *случайной последовательности бит*, которая затем может быть использована в качестве ключа для кодирования и декодирования сообщений с использованием шифра Вернама.

## § 1.5. Протокол BB84

Протокол BB84 был предложен Беннеттом и Brassардом в 1984 году (отсюда его название). При передаче ключа по этому протоколу Алиса посылает случайную последовательность поляризованных фотонов Бобу. Боб выбирает случайно и независимо для каждого фотона (и независимо от выбора Алисы, так как он неизвестен Бобу на данный момент) базис, линейный или круговой, в котором он производит измерение поляризации фотона. После приёма определённого количества фотонов Боб по открытому каналу связи сообщает Алисе, какой базис он использовал для измерения поляризации каждого фотона, и Алиса, опять же по открытому каналу, сообщает ему, в каких случаях он измерял поляризацию фотона в том базисе, в котором этот фотон был поляризован Алисой. Затем стороны отбрасывают результаты, полученные Бобом при измерениях в неправильных базисах; также отбрасываются случаи, в которых детектор Боба вообще не смог зарегистрировать фотон. Поляризации оставшихся фотонов интерпретируются как бит 0 для горизонтальной и левой круговой поляризаций и как бит 1 для вертикальной и правой круговой поляризаций. Результирующая последовательность бит является "сырым" ключом. [3]

Рис. 1 наглядно иллюстрирует шаги, описанные выше.

1.	↻	↓	↺	↔	↓	↓	↔	↔	↺	↻	↓	↺	↻	↻	↓
2.	+	○	○	+	+	○	○	+	○	+	○	○	○	○	+
3.	↓		↺		↓	↻	↻	↔		↓	↺	↺		↻	↓
4.	+		○		+	○	○	+		+	○	○		○	+
5.			✓		✓			✓				✓		✓	✓
6.			↺		↓			↔				↺		↻	↓
7.			1		1			0				1		0	1

Рис. 1. Иллюстрация передачи ключа по базовому протоколу.

1. Алиса посылает случайную последовательность фотонов, имеющих горизонтальную, вертикальную, левую круговую и правую круговую поляризации;
2. Боб измеряет поляризацию фотонов, выбирая базис по случайному закону;
3. Боб фиксирует полученные результаты измерений (некоторые фотоны могут быть не приняты вообще);
4. Боб сообщает Алисе, какие базисы он использовал для каждого принятого фотона;
5. Алиса сообщает ему, какие базисы были правильными;
6. Алиса и Боб отбрасывают данные, полученные при измерениях в неправильных базисах;
7. Полученные данные интерпретируются как двоичная последовательность в соответствии с условленной схемой (горизонтальная = левая круговая поляризация = 0 и вертикальная = правая круговая = 1).

Следующим шагом следует тест на наличие факта подслушивания. Алиса и Боб выбирают случайное подмножество бит "сырого" ключа и сравнивают его, передавая по открытому каналу. Очевидно, что Ева в результате подслушивания при передаче последовательности поляризованных фотонов может получить правильные сведения о поляризации не более чем половины фотонов, поскольку ей неизвестны ни базисы, используемые при передаче Алисой, ни базисы, используемые при приёме Бобом.

Если Алиса и Боб не найдут расхождений в своих данных, и если Ева не имеет возможности изменять по своему усмотрению информацию, передаваемую по открытому каналу, стороны могут заключить, что в оставшейся части ключа существует достаточно малое количество ошибок

(или их не существует вовсе) и лишь малая часть ключа (или вообще никакая) известна потенциальной Еве.

На самом деле, с "сырым" ключом необходимо произвести более сложные операции. Реальные однофотонные детекторы имеют некий шум. Поэтому данные Алисы и Боба будут различаться даже при отсутствии факта подслушивания. Следовательно, необходимо применять коррекцию ошибок.

Когда передача ключа завершена, Алисе и Бобу необходимо получить строго идентичные последовательности, которые можно будет использовать в качестве ключа, путём переговоров по незащищённому каналу. Так как мы предполагаем, что Ева перехватывает содержание всех сообщений, передаваемых по открытому каналу связи, эти "переговоры" должны производиться таким образом, чтобы сообщать Еве как можно меньше информации о ключе. Эффективным способом для согласования последовательностей Алисы и Боба является их "перемешивание" для более равномерного распределения ошибок и разбиение на блоки размером  $k$  – таким, при котором вероятность появления блоков с более чем одной ошибкой пренебрежимо мала. Для каждого такого блока стороны производят проверку чётности. Блоки с совпадающей чётностью признаются правильными, а оставшиеся делятся на несколько более мелких блоков, и проверка чётности производится над каждым таким блоком, до тех пор, пока ошибка не будет найдена и исправлена. Если из-за неверного начального предположения относительно количества ошибок начальный размер блока был слишком большим или слишком маленьким, этот факт станет очевидным, и процедура может быть повторена с блоками более подходящего размера. Чтобы исключить утечку информации о ключе при проведении коррекции ошибок, Алиса и Боб должны отбрасывать последний бит каждого блока, сведения о чётности которого они передали по открытому каналу.

Даже с оптимальным размером блока некоторые ошибки могут остаться незамеченными, когда в каком-либо блоке их количество окажется чётным [3]. Для их исключения перемешивание последовательности бит, разбиение её на блоки и сравнение их чётности производится ещё несколько раз, каждый раз с увеличением размера блоков, до тех пор, пока Алиса и Боб не придут к выводу, что вероятность ошибки в полученной последовательности пренебрежимо мала.

В результате всех этих действий Алиса и Боб получают идентичные последовательности бит, которые и являются ключом, с помощью которого они получают возможность кодировать и декодировать секретную информацию и обмениваться ей по незащищённому от прослушивания каналу связи. Разумеется, все действия, начиная от передачи последовательности фотонов и кончая кодированием, передачей и декодированием зашифрованных полученным ключом сообщений должны осуществляться в автоматическом порядке под управлением персонального компьютера.

## § 1.6. Различные виды систем квантовой криптографии

Существует несколько основных типов систем квантовой передачи ключа. Два основных типа – это системы с поляризационным кодированием и с фазовым кодированием. Исторически системы с поляризационным кодированием появились раньше, поэтому рассмотрим их в первую очередь.

### 1.6.1. Системы с поляризационным кодированием

Типичная схема квантовой криптографической установки с поляризационным кодированием по протоколу BB84 с четырьмя состояниями показана на рис. 2.

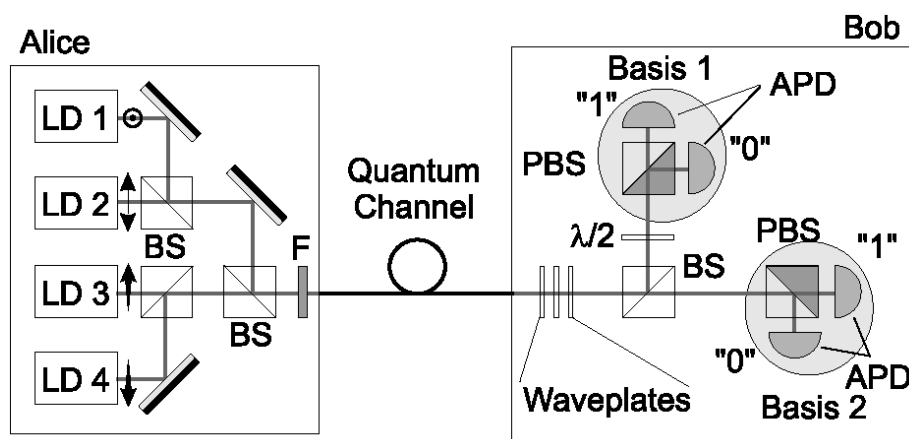


Рис. 2. Типичная схема квантовой криптографической установки с поляризационным кодированием (LD: лазерный диод, BS: ответвитель, F: фильтр нейтральной плотности, PBS: поляризационный ответвитель,  $\lambda/2$ : полуволновая пластинка, APD: лавинный фотодиод).

Часть, принадлежащая Алисе, состоит из четырёх лазерных диодов. Они излучают короткие импульсы света (1 нс), состоящие из фотонов, поляризованных на  $-45^\circ$ ,  $0^\circ$ ,  $+45^\circ$  и  $90^\circ$ . Для передачи одного бита

включается один из диодов. Затем импульсы ослабляются набором фильтров для уменьшения среднего количества фотонов, приходящихся на один импульс света, до величины, меньшей единицы. После этого они вводятся в волокно и покидают Алису. Крайне важным является сохранение поляризации фотонов по пути к Бобу, чтобы дать ему возможность получить информацию, закодированную Алисой. [2]

Дисперсия поляризационных мод может деполяризовать фотоны, при условии что задержка, которую она вносит между этими поляризационными модами, больше времени когерентности. Это вносит ограничение на типы лазеров, используемых Алисой.

Когда импульсы достигают Боба, они извлекаются из волокна и проходят через набор волновых пластинок, используемых для восстановления исходных поляризационных состояний путём компенсации трансформаций, внесённых волокном. Затем импульсы достигают ответвителя, осуществляющего выбор базиса. Переданные фотоны анализируются в базисе вертикальной/горизонтальной поляризации при помощи поляризационного ответвителя и двух счётчиков фотонов. Поляризация отражённых фотонов поворачивается волновой пластинкой на  $45^\circ$  (с  $-45^\circ$  до  $0^\circ$ ). После этого фотоны анализируются вторым набором из поляризационного ответвителя и счётчиков фотонов. Таким образом происходят измерения в диагональном базисе.

Для наглядной иллюстрации проследим путь фотона, поляризованного на  $+45^\circ$ . После того, как он покидает Алису, его поляризация случайным образом преобразуется в волокне. У Боба поляризационный контроллер должен быть установлен таким образом, чтобы вернуть поляризацию обратно к  $+45^\circ$ . Если фотон выберет выход ответвителя, соответствующий базису горизонтальной/вертикальной поляризации, у него будут равные шансы попасть в один из детекторов, что приведёт к случайному результату. С другой стороны, если он выберет

диагональный базис, его поляризация будет повернута на  $90^\circ$ . Тогда поляризационный ответитель отразит его с единичной вероятностью, что приведёт к определённому результату.

Вместо использования четырёх лазеров Алисой и двух поляризационных ответителей Бобом, возможно также применение активных поляризационных модуляторов, таких как ячейки Поக்கельса [4]. Для каждого импульса света модулятор активируется по случайному закону, приводя поляризацию в одно из четырёх состояний, в то время как принимающая сторона в случайном порядке вращает поляризацию половины принимаемых импульсов на  $45^\circ$ .

Антон Мюллер и его коллеги из Женевского университета использовали подобную систему для проведения экспериментов в области квантовой криптографии [9]. Они передавали ключ на расстояние 1100 метров, используя фотоны диапазона 800 нм. Для увеличения максимальной дистанции передачи они повторили эксперимент с фотонами 1300 нм [10, 11] и передавали ключ на 23 километра. Интересной особенностью данного эксперимента было использование в качестве квантового канала, связывающего Алису с Бобом, стандартного телекоммуникационного кабеля, который использовался компанией Swisscom для передачи телефонных переговоров. Это был первый случай, когда эксперимент по квантовой криптографии был проведён не в стенах физической лаборатории.

Эти два эксперимента показали, что изменения поляризации, вносимые оптическим волокном, были нестабильны во времени. Несмотря на то, что они стабилизировались на некоторое время (порядка нескольких минут), в какой-то момент поляризация резко менялась. Это означает, что реальная квантовая криптографическая система требует создания механизма активной компенсации поляризационных изменений. Несмотря на наличие принципиальной возможности создания такого механизма, очевидно, что его практическая реализация весьма затруднена. Джеймс

Френсон разработал систему автоматической подстройки поляризации [12], но не стал заниматься её дальнейшим совершенствованием. Существуют и другие способы автоматического контроля поляризации, разработанные для когерентных волоконно-оптических систем связи [18]. Интересно заметить, что замена стандартного волокна волокном с сохранением поляризации не решает проблему. Причина в том, что несмотря на название, эти волокна не сохраняют различные состояния поляризации.

Из-за всего этого поляризационное кодирование не представляется лучшим выбором при построении волоконно-оптических систем квантовой криптографии. Тем не менее, ситуация в корне отличается в случае систем передачи ключа в открытом пространстве, которые на сегодня составляют отдельный активно развивающийся класс подобных систем.

### **1.6.2. Системы с фазовым кодированием**

Нестабильность поляризации в системах с поляризационным кодированием сильно затрудняет (хотя и не делает невозможным) их создание. В поиске выхода был разработан другой тип квантовых криптографических систем. Идея кодирования бит фазой фотонов была впервые упомянута Беннеттом в статье, где он описывал протокол с использованием двух состояний [3]. Получение квантовых состояний и последующий их анализ производятся интерферометрами, которые могут быть реализованы одномодовыми компонентами волоконной оптики [2]. На рис. 3 показана волоконно-оптическая версия интерферометра Маха-Цендера.

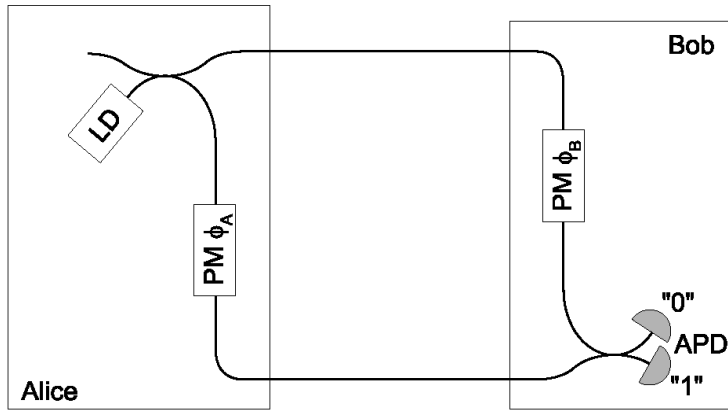


Рис. 3. Интерферометр Маха-Цендера (LD: лазерный диод, PM: фазовый модулятор, APD: лавинный фотодиод).

Интерферометр выполнен из двух волоконно-оптических разветвителей, соединённых между собой, и двух фазовых модуляторов – по одному в каждом плече. В такую систему можно ввести свет, используя классический непрерывный источник, и наблюдать интенсивность света на выходах. В случае, если длина когерентности света лазера больше разности длин плеч интерферометра, мы можем получить интерференционную картину. Принимая во внимание фазовый сдвиг  $\pi/2$ , происходящий при отражении на разветвителе, действия фазовых модуляторов ( $\varphi_A$  и  $\varphi_B$ ) и разность длин плеч ( $\Delta L$ ), интенсивность света на выходе "0" определяется следующим образом:

$$I_0 = \bar{I} \cdot \cos^2\left(\frac{\varphi_A - \varphi_B + k\Delta L}{2}\right),$$

где  $k$  – волновое число, а  $I$  – интенсивность источника.

Если разность фаз составляет  $\pi/2 + n\pi$ , где  $n$  – целое число, получается деструктивная интерференция. Поэтому интенсивность света, регистрируемого на выходе "0", достигает минимума и весь свет идёт на выход "1". Когда разность фаз составляет  $n\pi$ , ситуация обратная – на выходе "0" наблюдается конструктивная интерференция, в то время как интенсивность на выходе "1" достигает минимума. В промежуточных случаях свет может быть зарегистрирован на обоих выходах. Данное устройство работает как оптический переключатель. Необходимо

отметить, что крайне важным является сохранение постоянной и малой разности длин плеч для получения устойчивой интерференции.

Описанное выше поведение этого интерферометра справедливо для классического света. Тем не менее, интерферометр работает точно так же и в случае одиночных фотонов. Вероятность зарегистрировать фотон на одном из выходов будет изменяться с изменением фазы. Несмотря на то, что фотон ведёт себя как частица при регистрации, он распространяется через интерферометр как волна [6]. Интерферометр Маха-Цендера – это волоконно-оптический вариант эксперимента Юнга со щелями, в котором плечи интерферометра аналогичны апертурам. Такой интерферометр вместе с однофотонным источником и подсчитывающими фотоны детекторами может быть использован в квантовой криптографии. Установка Алисы в таком случае будет содержать источник, первый разветвитель и первый фазовый модулятор, а установка Боба будет состоять из второго модулятора, разветвителя и детекторов.

Рассмотрим применение к такой схеме протокола BB84 с четырьмя состояниями. Алиса может осуществлять один из четырёх фазовых сдвигов ( $0, \pi/2, \pi, 3\pi/2$ ). Она сопоставляет  $0$  и  $\pi/2$  биту  $0$  и  $3\pi/2$  - биту  $1$ . В свою очередь, Боб производит выбор базиса, в случайном порядке сдвигая фазу на  $0$  или  $\pi/2$ , и присваивает детектору, подсоединённому к выходу "0" значение бита  $0$ , и детектору, подсоединённому к выходу "1" значение бита  $1$ . Когда разности фаз равны  $0$  или  $\pi$ , Алиса и Боб используют совместимые базисы и получают вполне определённый результат. В таких случаях Алиса может определить, в какой из детекторов Боба попадёт фотон, и следовательно она может определить значение бита. Со своей стороны, Боб может заключить, какую фазу выбирала Алиса при передаче каждого фотона. В случае же, когда разность фаз принимает значения  $\pi/2$  или  $3\pi/2$ , стороны используют несовместимые базисы, и фотон случайным образом выбирает один из детекторов Боба. Все возможные комбинации сведены в таблицу 1.

Таблица 1. Иллюстрация протокола BB84 с четырьмя состояниями для фазового кодирования.

Alice		Bob		
Bit value	$\varphi_A$	$\varphi_B$	$\varphi_A - \varphi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	$\pi$	0	$\pi$	1
1	$\pi$	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	$\pi$	1

Для такой системы крайне важно сохранять стабильной разность длин плеч интерферометра в течение сеанса передачи ключа. Эта разность не должна изменяться более чем на долю длины волны фотонов. Изменения длины одного из плеч приведёт к дрейфу фазы и выразится в ошибках в передаваемом ключе. Несмотря на то, что данная схема прекрасно работает на оптическом столе, не представляется возможным сохранение длин плеч в случае, когда Алиса и Боб отделены друг от друга более чем на несколько метров. Беннетт показал, как обойти эту проблему [3]. Он предложил использовать два несбалансированных интерферометра Маха-Цендера, соединённых последовательно оптическим волокном (см. рис. 4).

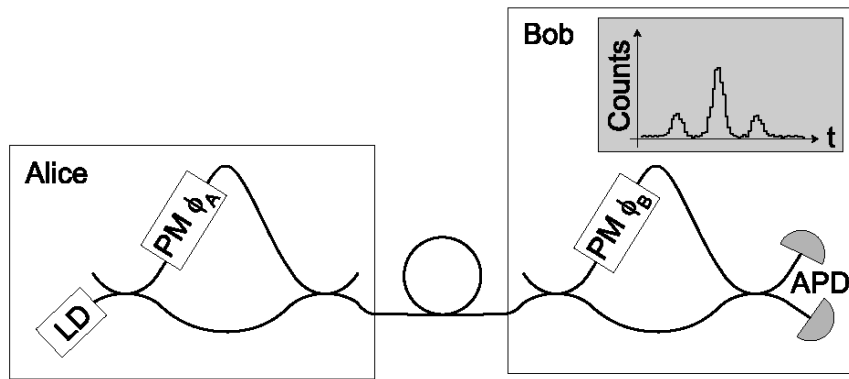


Рис. 4. Система для квантовой криптографии с двумя интерферометрами Маха-Цендера (LD: лазерный диод, PM: фазовый модулятор, APD: лавинный фотодиод).

Регистрируя количество отсчётов во времени, Боб получает три пика. Первый пик соответствует случаям, когда фотоны прошли по коротким плечам в интерферометрах Алисы и Боба, третий – случаям, когда они прошли по длинным плечам. Наконец, центральный пик соответствует фотонам, прошедшим через короткое плечо у Алисы и через длинное у Боба и наоборот. Такие фотоны интерферируют между собой. Для того, чтобы отделить проинтерферировавшие фотоны (то есть центральный пик) от остальных, используется временное "окно". Результат интерференции будет зависеть от состояния фазовых модуляторов Алисы и Боба.

Преимущество этой установки заключается в том, что обе "половинки" фотона проходят по одному и тому же волокну [2]. Следовательно, они проходят пути равной длины в той части системы, которая является наиболее чувствительной к изменениям состояния окружающей среды, при условии, что эти изменения более медленные, чем временные разделения, определяемые несбалансированностью интерферометра ( $\approx 5$  нс в установке Беннетта). Чтобы получить хорошую видимость интерференционной картины, и следовательно низкий процент

ошибок, несбалансированности в интерферометрах должны быть равными в пределах долей времени когерентности фотонов. Это подразумевает, что разности ходов должны совпадать в пределах нескольких миллиметров, что не представляет большой проблемы. Помимо этого, несбалансированность должна быть выбрана таким образом, чтобы дать возможность чётко разделить интерферирующий пик от неинтерферирующих. Следовательно, она должна превышать длину импульса и дрожание фазы детекторов фотонов. На практике, второе условие наиболее важное. Предполагая дрожание фазы порядка 500 пс, несбалансированность по крайней мере в 1,5 нс позволяет пикам не накладываться друг на друга.

Основная трудность, предоставляемая данной системой, состоит в том, что несбалансированности интерферометров Алисы и Боба должны быть стабильными в пределах доли длины волны фотонов во время передачи ключа для сохранения правильных фазовых отношений [8]. Это подразумевает, что интерферометры должны находиться в термостабилизированных контейнерах. Кроме того, реальная система потребует наличия активной системы компенсации дрейфа фазы. Наконец, в каждом интерферометре изменения поляризации, вызванные коротким плечом, должны совпадать с таковыми у длинного плеча. Для этого необходимо применение поляризационных контроллеров. Тем не менее, поляризационные изменения в коротких оптических волокнах, температура которых остаётся стабильной, и которые не испытывают механических напряжений, остаются достаточно стабильными, поэтому подстройка поляризационных контроллеров не должна быть частой.

Пол Тэпстер и Джон Рарити, работавшие с Полем Таунсендом, первыми продемонстрировали работу подобной системы на катушке волокна длиной в 10 км в 1993 году [19]. Позже Таунсенд усовершенствовал интерферометр установкой поляризующего ответвителя для подавления неинтерферирующих фотонов [13]. В таком случае, в

добавок к проблеме стабилизации интерферометров, опять становится необходимой подстройка поляризации фотонов у Боба. В своих последующих экспериментах он продолжил исследования в области систем квантовой криптографии с фазовым кодированием и увеличил максимальную дистанцию передачи [5, 14]. Он также протестировал возможность мультиплексирования квантового канала с традиционной передачей сообщений по одному и тому же волокну с использованием двух различных длин волн [15]. Ричард Хагис и его коллеги из Национальной лаборатории из Лос-Аламоса также экспериментировали с подобными интерферометрами [7].

### 1.6.3. Системы "Plug and Play"

Описание систем с фазовым кодированием было бы неполным без описания одной из их модификаций – схем "Plug and Play" ("Включил и работай"). Предыдущие системы требовали создания механизма автоматической компенсации флуктуаций, возникающих в квантовом канале. Подход, выработанный в 1989 году Мартинелли позволяет автоматически и в пассивном режиме компенсировать все поляризационные флуктуации в оптическом волокне [21]. Предложенная им схема показана на рис. 5.

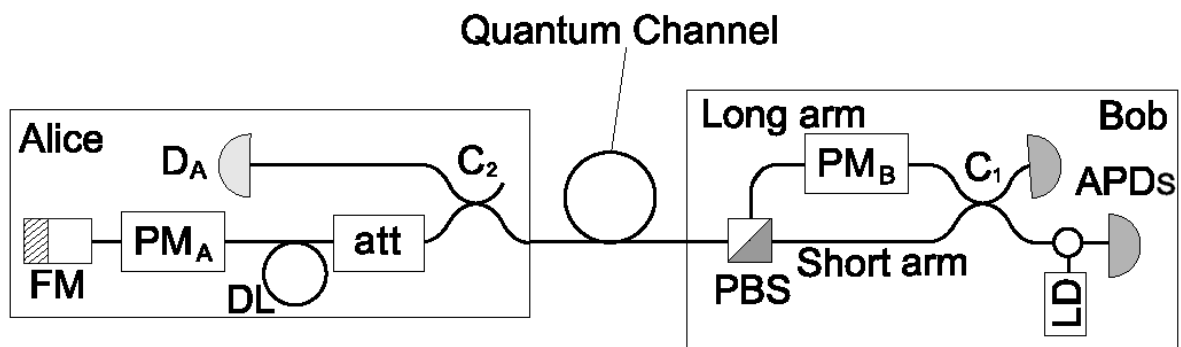


Рис. 5. Система "Plug and Play" (LD: лазерный диод, APD: лавинный фотодиод, С – волоконно-оптический разветвитель, РМ – фазовый модулятор, PBS: поляризационный ответвитель, DL – оптическая линия задержки, att – аттенюатор, FM – зеркало Фарадея, D<sub>A</sub>- классический детектор).

В данной схеме импульсы, которые излучаются Бобом, могут проходить через короткое плечо у Боба, отражаться от зеркала Фарадея у Алисы и возвращаться уже через длинное плечо у Боба, либо наоборот – проходить через длинное плечо, отражаться и проходить через короткое на обратном пути. Эти два типа импульсов интерферируют на разветвителе С<sub>1</sub>. Теперь опишем работу этой схемы подробнее. Короткий яркий импульс света вводится в систему через циркулятор. Этот импульс разделяется на разветвителе. Одна из половинок импульса, назовём её Р<sub>1</sub>, проходит через короткое плечо установки Боба напрямую к поляризационному ответвителю. Преобразование поляризации в этом плече установлено таким, что свет беспрепятственно попадает в линию. Вторая половинка, Р<sub>2</sub>, проходит к поляризационному ответвителю через длинное плечо. Преобразование поляризации установлено таким, что свет отражается в линию. Фазовый модулятор, присутствующий в длинном плече, на данном этапе остаётся неактивным, так что он не вносит фазового сдвига. Р<sub>1</sub> и Р<sub>2</sub> отстоят друг от друга на время порядка 200 нс. Обе половинки импульса достигают Алисы. Р<sub>1</sub> проходит через разветвитель С<sub>2</sub>. Половина попадает на классический детектор для получения сигнала синхронизации, а другая половина проходит через аттенюатор и оптическую линию задержки – состоящую попросту из катушки с волокном, чья роль будет объяснена чуть позже. Наконец, свет проходит через фазовый модулятор и отражается от зеркала Фарадея. Р<sub>2</sub> следует тем же путём. Алиса активизирует свой фазовый модулятор, чтобы сдвинуть по фазе только Р<sub>1</sub>,

кодируя при этом значение бита точно так же, как в традиционной схеме с фазовым кодированием. Атенюатор подобран таким образом, что когда импульсы покидают Алису, они содержат менее одного фотона на импульс. Когда они достигают поляризационного ответвителя после прохождения обратно через линию, благодаря зеркалу Фарадея их поляризация в точности ортогональна исходной. Поэтому  $P_1$  отражается в длинное плечо, вместо того, чтобы пройти в короткое. В этот момент Боб активирует свой модулятор для внесения фазового сдвига, осуществляя таким образом выбор базиса. Аналогичным образом  $P_2$  проходит в короткое плечо. Оба импульса достигают разветвителя и интерферируют на нём. Результат интерференции регистрируется одним из детекторов.

Поскольку по своей сути такая система является двунаправленной, повышенное внимание должно уделяться рэлеевскому обратному рассеянию. Свет, проходящий через волокно, рассеивается на его неоднородностях. Малая доля (порядка 1%) этого света идёт в обратном направлении. Когда частота повторения достаточно велика, импульсы, идущие к Алисе и обратно, пересекутся между собой в какой-то точке. Однако их интенсивности очень сильно различаются – импульсы, идущие к Алисе, имеют в тысячи раз большую интенсивность, чем импульсы, идущие от неё. Фотоны, вызванные обратным рассеянием, могут вызвать ложные отсчёты в детекторах Боба. Эту проблему можно обойти, построив систему таким образом, чтобы импульсы, идущие к Бобу и от него, не могли присутствовать в линии одновременно. Они излучаются в виде цепочек и хранятся Алисой в её линии задержки. Боб ждёт до тех пор, пока все импульсы цепочки не достигнут его, и только после этого посылает следующую цепочку. Несмотря на то, что такой подход полностью решает проблему ошибок, вызванных рэлеевским обратным рассеянием, он имеет недостаток, выражающийся в уменьшении эффективной частоты повторения. Линия задержки длиной в половину канала передачи приводит к уменьшению скорости передачи примерно втрое.

Главным же недостатком систем "Plug and Play" по отношению к другим системам является уязвимость по отношению к атакам типа "Троянский конь" [20]. В самом деле, Ева может послать свой сканирующий импульс для выяснения текущего состояния фазового модулятора Алисы и получить его обратно из-за сильного отражения, вызванного зеркалом на конце установки. Для предотвращения подобных видов атак Алиса устанавливает у себя аттенюатор для уменьшения количества света, проходящего через систему (однако очевидно, что при внесении слишком сильного ослабления система сама окажется неработоспособной). Кроме того, она должна отслеживать интенсивность принимаемого света при помощи классического детектора, чтобы отследить факт возможной атаки. В дополнение ко всему, системы "Plug and Play" не могут работать с настоящими однофотонными источниками, и следовательно, не будут выигрывать от продвижений в области создания таких источников.

## Глава 2. Экспериментальная установка

Экспериментальная установка, которая является предметом рассмотрения в данной дипломной работе, построена по схеме с фазовым кодированием для работы по протоколу BB84. Для удобства можно условно разделить её на две основные части – оптическую и электронную. Оптическая часть, представляющая собой интерферометр Маха-Цендера, проиллюстрирована на рис. 6.

Импульс света с длиной волны 1300 нм излучается полупроводниковым лазером (Fujitsu FLD3F6CX). Он проходит через поляризатор, вводится в волокно с сохранением поляризации и разделяется надвое на регулируемом волоконно-оптическом разветвителе. Половина импульса проходит через короткое плечо, а другая половина – через длинное, в котором установлен фазовый модулятор. Это плечо также содержит переменную линию задержки для точной подстройки длины плеча. Затем импульсы проходят через поляризационный ответвитель Алисы и попадают в линию, которая представлена стандартным одномодовым волокном. У Боба свет проходит через контроллер поляризации, необходимый для компенсации статических изменений поляризации, произошедших в линии, и разделяется на поляризационном ответвителе Боба, таким образом, что импульс, прошедший в длинном плече у Алисы, попадает в короткое плечо у Боба, и наоборот. Импульс света, попавший в длинное плечо у Боба, проходит через его фазовый модулятор. Наконец, импульсы интерферируют на волоконно-оптическом разветвителе Боба. Результат этой интерференции зависит от относительной фазы импульсов, которая контролируется фазовыми модуляторами Алисы и Боба. "Единицы" и "нули" идут на разные выходы разветвителя. Вместо того, чтобы использовать для них два отдельных детектора, мы задерживаем "нули" оптической линией задержки.

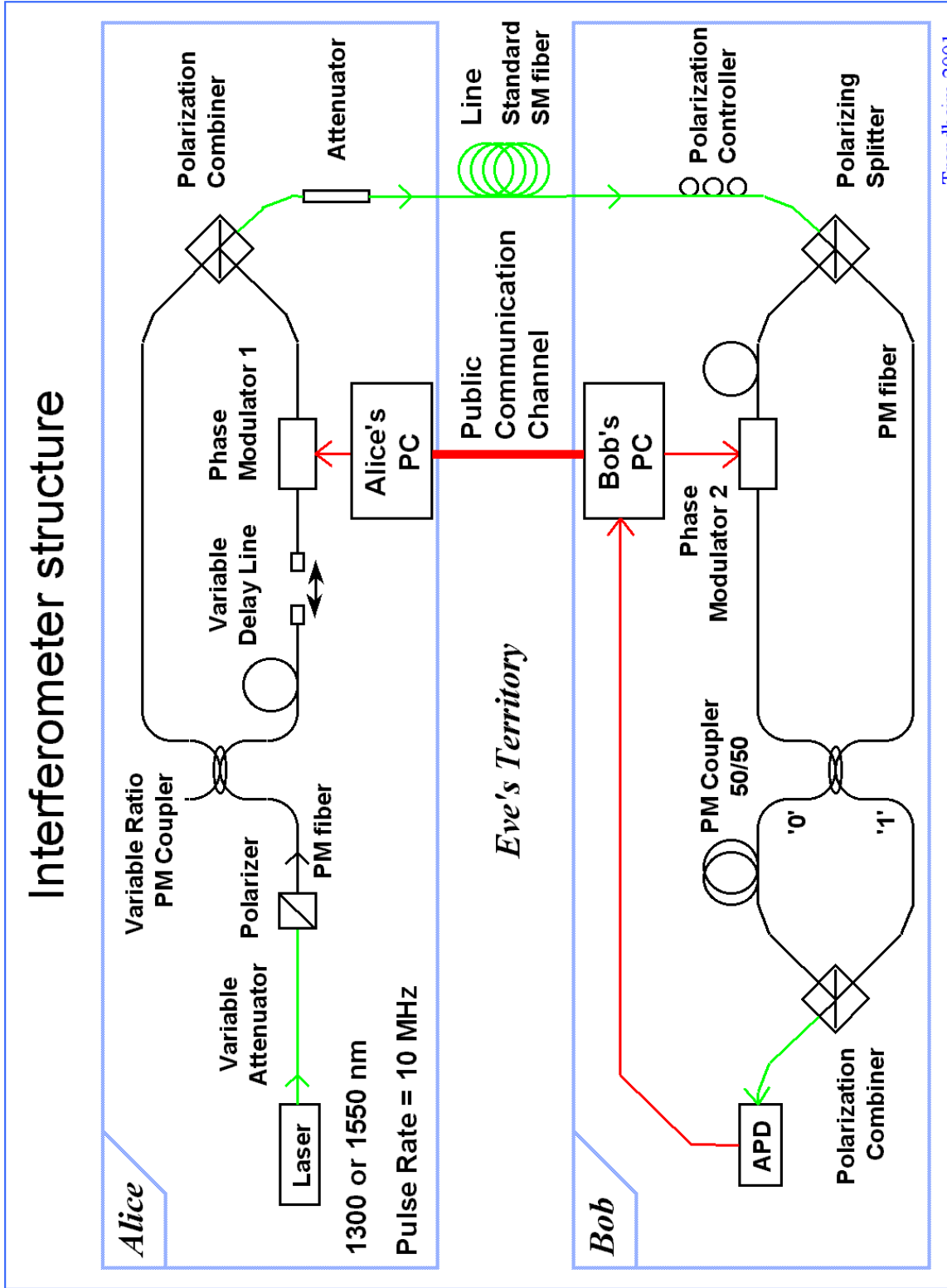


Рис. 6. Оптическая часть квантовой криптографической установки

Таким образом, импульсы света, соответствующие единицам и нулям, после прохождения поляризационного ответвителя регистрируются одним и тем же детектором, но достигают его в разное время. Для импульсов выделяются временные интервалы, и в зависимости от того, в каком из этих интервалов лавинным фотодиодом был зарегистрирован импульс, он интерпретируется как единица или ноль. Главная тактовая частота установки – 20 МГц, что означает работу детектора на этой частоте. Соответственно, при использовании двух отдельных детекторов их рабочая частота могла бы быть вдвое меньше.

Используемый в качестве детектора лавинный фотодиод (марки ФД-312Л, охлаждаемый жидким азотом) работает в так называемом режиме Гейгера. В этом режиме напряжение смещения фотодиода большую часть времени держится чуть ниже напряжения пробоя, так что возникновение лавины в таких условиях невозможно. Когда приходит сигнал синхронизации, стробирующий импульс складывается с постоянным напряжением смещения, поднимая напряжение на фотодиоде выше напряжения пробоя. В это время фотон, пришедший на фотодиод, может вызвать лавину. По сравнению с другими режимами работы ЛФД, режим Гейгера характеризуется гораздо более низкой вероятностью темновых отсчётов, так как большую часть времени, без стробирующего импульса, возникновение лавины невозможно. Однако, данный режим накладывает достаточно жёсткие ограничения на точность синхронизации, потому что стробирующий импульс должен прийти на ЛФД точно в тот момент времени, когда ожидается приход фотона. Мы должны сохранять импульс достаточной длины (1-2 нс) для более уверенной регистрации фотонов. Однако слишком широкие импульсы будут выражаться в увеличении вероятности темновых отсчётов. Эксперимент показывает низкую вероятность темновых отсчётов (порядка  $10^{-4}$ ), что является достаточным для передачи ключа на средние дистанции. Этот показатель может быть улучшен при наличии лавинного фотодиода с лучшими характеристиками.

Плечи интерферометра выполнены из оптических волокон с сохранением поляризации (Fujikura Panda PM 1300 nm), в то время как волокна между лазером и поляризатором Алисы и также между поляризационным ответвителем Боба и детектором (и, разумеется, сама линия передачи) не должны быть волокнами с сохранением поляризации.

Электронная часть установки показана на рис. 7.

Имеется два персональных компьютера, названные Алиса и Боб, которые соединены по стандартной сети 10 Мбит/сек в качестве открытого канала. В обоих компьютерах установлены карты цифро-аналогового преобразования National Instruments NI 5411 для управления напряжениями на фазовых модуляторах. у Боба также установлена цифровая карта ввода/вывода DIO D32HS, которая используется для сбора данных детектора. Один из выходов этой карты также используется для подачи сигнала, запускающего всю систему ("trigger"). Из-за того, что карты NI 5411 имеют максимальное выходное напряжение +/- 5 В, а фазовые модуляторы имеют полуволновое напряжение 8,3 В, были изготовлены два усилителя, помещённых в Box1 и Box2 (для Алисы и Боба соответственно). Box1 и Box2 также содержат схемы регулировки фазы для упрощения синхронизации карт. Сбор данных с лавинного фотодиода производится с помощью Box3 (бокс сбора данных), который содержит цифровые логические схемы и 512 КБ буферной памяти для записи данных с фотодетектора и временного их хранения перед загрузкой в компьютер Боба. Это выполнено по той причине, что обычные персональные компьютеры не могут обрабатывать данные, поступающие от детектора на скорости 20 МГц, в режиме реального времени. После заполнения буферной памяти её содержимое читается побайтно при помощи карты ввода-вывода DIO D32HS. Обработка данных в реальном времени может стать возможной при наличии специализированного контроллера.

QKD setup: electrical interconnections diagram

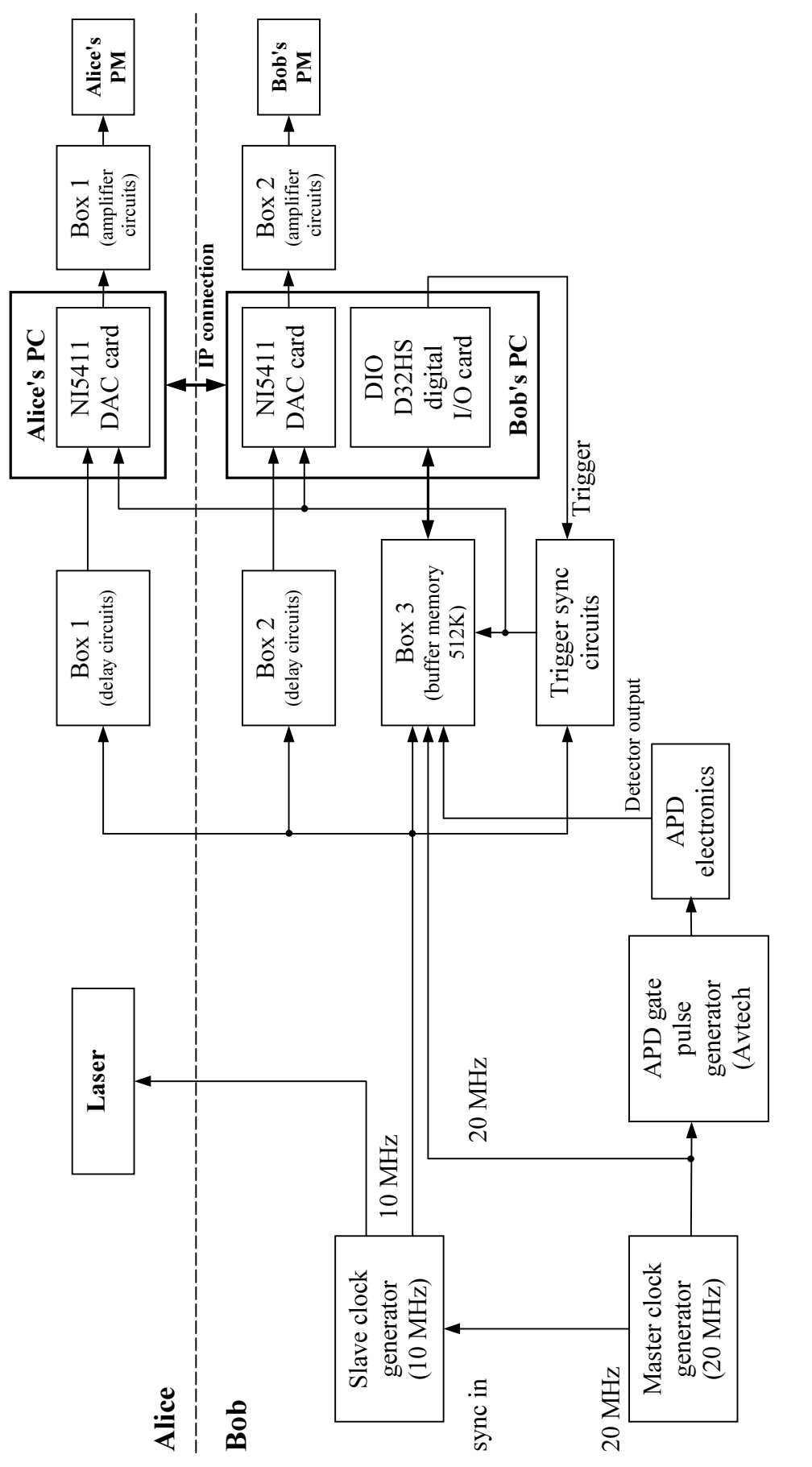


Рис. 7. Электронная часть квантовой криптографической установки

Вся система синхронизируется от главного тактового генератора с частотой 20 МГц (SRS DS345). Он обладает кварцевым генератором частоты, которая является достаточно стабильной для нормальной работы установки. От главного генератора синхронизируются фотодетектор и Vox3. Главный тактовый генератор также синхронизирует вспомогательный генератор частотой 10 МГц (HP 8008A), от которого синхронизируются лазер, карты цифроаналогового преобразования Алисы и Боба (сигнал предварительно проходит через схемы подстройки фазы в Vox1 и Vox2) и Vox3 (10-мегагерцовый сигнал необходим ему для различения временных интервалов "0" и "1").

При работе с картами NI 5411 возникла проблема синхронизации. На входы карт поступают сигнал синхронизации 10 МГц и сигнал запуска, который является статическим TTL-сигналом, посылаемым цифровой картой ввода-вывода Боба для запуска всей системы (для начала генерации напряжений на фазовых модуляторах и одновременного начала сбора данных детектора в буферную память Vox3). Карты NI 5411 не могли синхронизироваться в абсолютной фазе – начальные фазы сигналов, которые они выдавали, изменялись от запуска к запуску. После долгих поисков проблема была решена путём жёсткой привязки сигнала запуска к ближайшему 10-мегагерцовому синхронизирующему импульсу при помощи микросхемы триггера ("trigger sync circuits" на рис. 7). На самом деле, в соответствии с инструкцией к картам, в данной конфигурации они и не должны были синхронизироваться в абсолютной фазе друг с другом. В данном случае они заработали, но проявился недокументированный "побочный эффект" – частота выдаваемых картами сигналов стала вчетверо большей, чем в режиме внутренней синхронизации. Эта проблема была решена на программном уровне путём передачи каждого отсчёта 4 раза подряд.

С точки зрения охраны труда данная экспериментальная установка опасности не представляет. В ней нет высоких напряжений; работа установки не сопряжена с возникновением опасных электромагнитных излучений. Полупроводниковый лазер, задействованный в эксперименте, излучает менее 100 фотонов на импульс (импульсы следуют с частотой 10 МГц), что заведомо меньше любых норм безопасности. В дополнение ко всему, лазер излучает свет непосредственно в волокно, т.е. выходом лазера является оптический разъём, таким образом при отключении лазера от линии свет, выходящий из него, не является коллимированным.

### Глава 3. Подстройка фазы в интерферометре

Вероятность появления ошибки в "сыром" ключе зависит от точности установки фазы импульса света. Существуют две возможные причины неправильной установки фазы – ошибка в установке напряжений на фазовых модуляторах и несовпадение фазы между двумя плечами интерферометра. Допустим, что ошибки в установке напряжений на модуляторах Алисы и Боба легко могут быть сведены до пренебрежимо малого уровня. Проблемой остаётся дрейф фазы в интерферометре. Эксперименты показывают, что относительная фаза между двумя плечами интерферометра медленно меняется (со скоростью порядка  $360^\circ$  за несколько минут [5]), и измерения на нашей установке подтверждают этот результат. Чтобы не допустить слишком быстрый дрейф фазы, в установке используется ряд конструктивных решений для снижения влияния на неё условий окружающей среды. Интерферометры Алисы и Боба смонтированы на массивных металлических основаниях и накрыты термоизоляцией; они расположены на виброизолированном столе. Эти меры, однако, не могут полностью исключить дрейф фазы. Для нормальной работы установки необходимо подстраивать фазу каждый раз перед циклом передачи ключа. Для того, чтобы количество ошибок в "сыром" ключе не превысило 11%, что является максимально допустимым количеством, которое может быть исправлено известными алгоритмами коррекции ошибок при извлечении ключа, ошибка в установке фазы должна быть менее  $10^\circ$ .

### § 3.1. Алгоритм подстройки фазы

Существует два варианта подстройки фазы – ручная и автоматическая. В нашем случае, ручная подстройка будет бесполезной даже в эксперименте, потому что фаза уходит слишком быстро, чтобы на это успевал реагировать оператор, поэтому мы должны выбрать автоматическую подстройку. Нашей задачей было сделать так, чтобы алгоритм автоматической подстройки фазы работал прямо в однофотонном режиме, т.е. без увеличения количества света, проходящего через установку, по сравнению с режимом передачи ключа. Такой выбор был сделан из-за того, что он не потребует применения дополнительных дорогостоящих оптических компонентов (переменного аттенюатора), упростив таким образом всю систему и сделав её более надёжной.

Разработанный алгоритм можно разделить на два основных этапа:

#### **Этап 1:** грубая подстройка фазы

Алиса устанавливает свой фазовый модулятор в состояние "1" (0 В) и передаёт фотоны как обычно. Боб устанавливает напряжение на своём модуляторе так, чтобы за малое количество шагов (скажем, 20) перекрыть весь диапазон фазы от  $0^\circ$  до  $360^\circ$ . На каждом шаге он подсчитывает количества фотонов, пришедших на детектор как "единицы" и "нули". На каком-то шаге будет зарегистрировано минимальное количество "нулей" и максимальное количество "единиц". Напряжение на фазовом модуляторе Боба на этом шаге (и фаза, соответствующая этому напряжению) должно быть подано при передаче ключа в качестве постоянного смещения на этот модулятор, тогда набег фазы будет скомпенсирован и система сможет нормально функционировать. Однако эта фаза является грубым приближением к необходимому значению и используется только для обеспечения последующего уточнения на втором этапе. Назовём её  $\varphi_0$ .

Зависимость числа отсчётов детектора во временных интервалах "1" и "0" от  $\varphi$  показана на рис. 8.

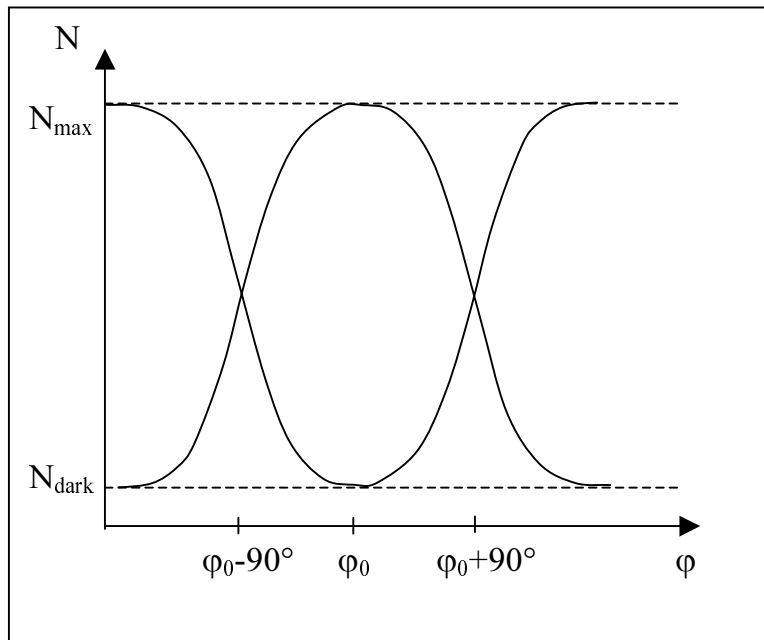


Рис. 8.  $\varphi$  - фаза,  $N$  – число отсчётов, зарегистрированное за некий фиксированный отрезок времени.

Минимальное число отсчётов ограничено количеством темновых отсчётов,  $N_{\text{dark}}$ , в то время как максимальное число отсчётов составляет  $N_{\text{max}}$ .

Как мы видим, если Боб "сканирует" фазу в диапазоне  $0^\circ \dots 360^\circ$ , на одном из шагов он окажется вблизи одного из максимумов  $N_1(\varphi)$  и одновременно вблизи соответствующего минимума  $N_0(\varphi)$ . Однако, это не позволит нам определить фазу с требуемой точностью в несколько градусов, так как даже если Боб разделит интервал в  $360^\circ$  на 360 шагов, из-за статистических флуктуаций в  $N$  потребуется слишком много времени для подсчёта  $N$  с необходимой точностью на каждом из 360-ти шагов. За это время фаза успеет уйти, и мы получим устаревшие результаты. Чтобы за одно и то же время получить максимальную точность измерения фазы,

мы должны считать фотоны в тех точках на этих кривых, в которых производная максимальна, то есть когда минимальному  $\Delta\varphi$  соответствует максимальное  $\Delta N$ . Этими точками являются  $\varphi_0+90^\circ$  и  $\varphi_0-90^\circ$ .

Этап 1 был предназначен для грубой оценки положения точек  $\varphi_0+90^\circ$  и  $\varphi_0-90^\circ$ . Полученная информация используется на втором этапе.

### Этап 2: точная подстройка фазы

Алиса продолжает посылать фотоны аналогично первому этапу, в то время как Боб устанавливает свой фазовый модулятор поочередно в состояния  $\varphi_0+90^\circ$  и  $\varphi_0-90^\circ$  и через некоторое время получает 4 величины – количества фотонов, зарегистрированных на обоих временных интервалах ("1" и "0") с фазовым модулятором в состояниях  $\varphi_0+90^\circ$  и  $\varphi_0-90^\circ$ .

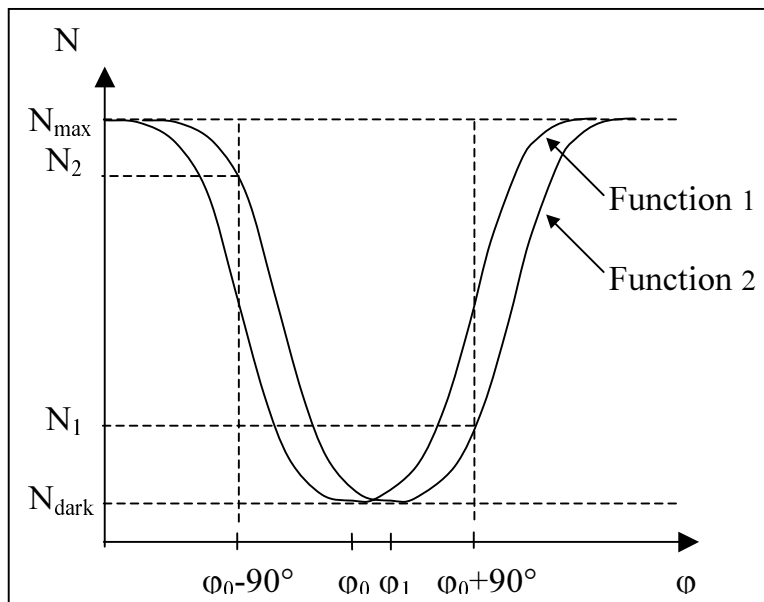


Рис. 9. Подстройка фазы, второй этап.

На рис. 9 функция 1 является нашим предположением о зависимости  $N(\varphi)$  после выполнения первого этапа. Функция 2 – действительная зависимость  $N(\varphi)$ , которая нам пока неизвестна.

$$\text{Функция 1: } N = (N_{\max} - N_{\text{dark}}) \sin^2\left(\frac{\varphi - \varphi_0}{360^\circ} \pi\right) + N_{\text{dark}}$$

$$\text{Функция 2: } N = (N_{\max} - N_{\text{dark}}) \sin^2\left(\frac{\varphi - \Delta\varphi - \varphi_0}{360^\circ} \pi\right) + N_{\text{dark}}$$

$$\Delta\varphi = \varphi_1 - \varphi_0$$

$N_{\text{dark}}$  может быть принято равным нулю либо оценено заранее на первом этапе;

$N_{\max}$  может быть принято равным  $N_1 + N_2$  либо оценено заранее на первом этапе.

$$\begin{aligned} \Delta\varphi = & \frac{45^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) + \right. \\ & \left. + \arccos\left(2 \frac{N_{\text{dark}} - N_4}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_3}{N_{\max} - N_{\text{dark}}} + 1\right) \right) \end{aligned}$$

(подробный вывод этого выражения приведён в приложении).

После получения  $\Delta\varphi$  мы складываем его значение с  $\varphi_0$ , которое было измерено на первом этапе. Затем, зная полуволновое напряжение фазового модулятора Боба, можно с лёгкостью вычислить соответствующее напряжение, которое необходимо приложить к нему в качестве постоянного напряжения смещения для выполнения последующего этапа передачи ключа. Передача ключа должна быть осуществлена незамедлительно после проведения процедуры подстройки фазы, иначе фаза успеет уйти.

Управление всей системой и осуществление автоматической подстройки фазы происходит при помощи программы, написанной в LabVIEW, со вставками на языке С в тех местах, где требуется повышенное быстродействие (например, для ускорения процедуры считывания информации из буферной памяти Вох3). LabVIEW – графический язык, то есть он не имеет текста программы как такового. Программа представлена в виде блок-схемы (примеры приведены в приложении).

## Глава 4. Полученные результаты

Программа на LabVIEW выводит результаты своих вычислений в графическом виде. На рис. 10 представлены результаты подсчёта фотонов на первом этапе процедуры автоматической подстройки фазы.

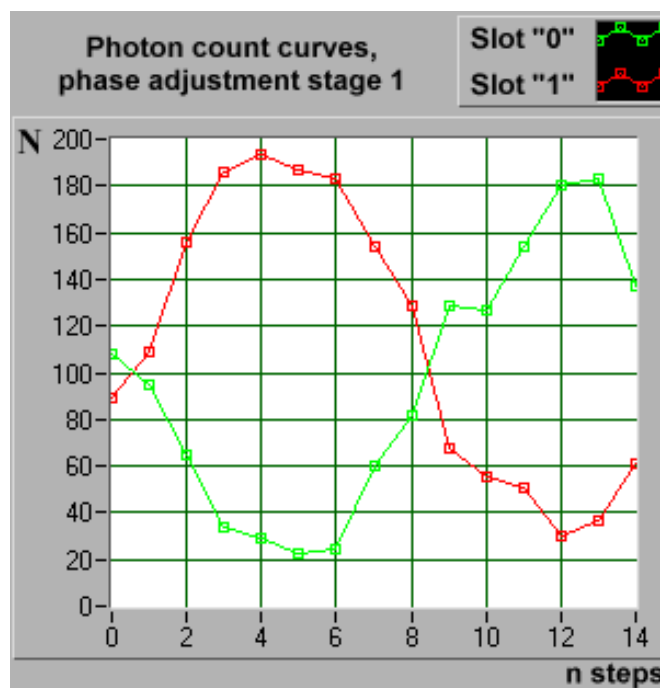


Рис. 10. Число срабатываний детектора для каждого шага напряжения на фазовом модуляторе Боба (всего - 15 шагов).

На рис. 10 представлены зависимости числа отсчётов от номера шага напряжения на фазовом модуляторе Боба для временных интервалов "0" и "1". Кривые по виду несколько отличаются от идеальных синусоид – это обусловлено малым количеством отсчётов, собираемых на каждом шаге. Несмотря на это, шаг с наименьшим количеством отсчётов хорошо виден – это всё, что нам требуется на первом этапе.

Графики итогового напряжения смещения для фазового модулятора Боба представлены на рис. 11.

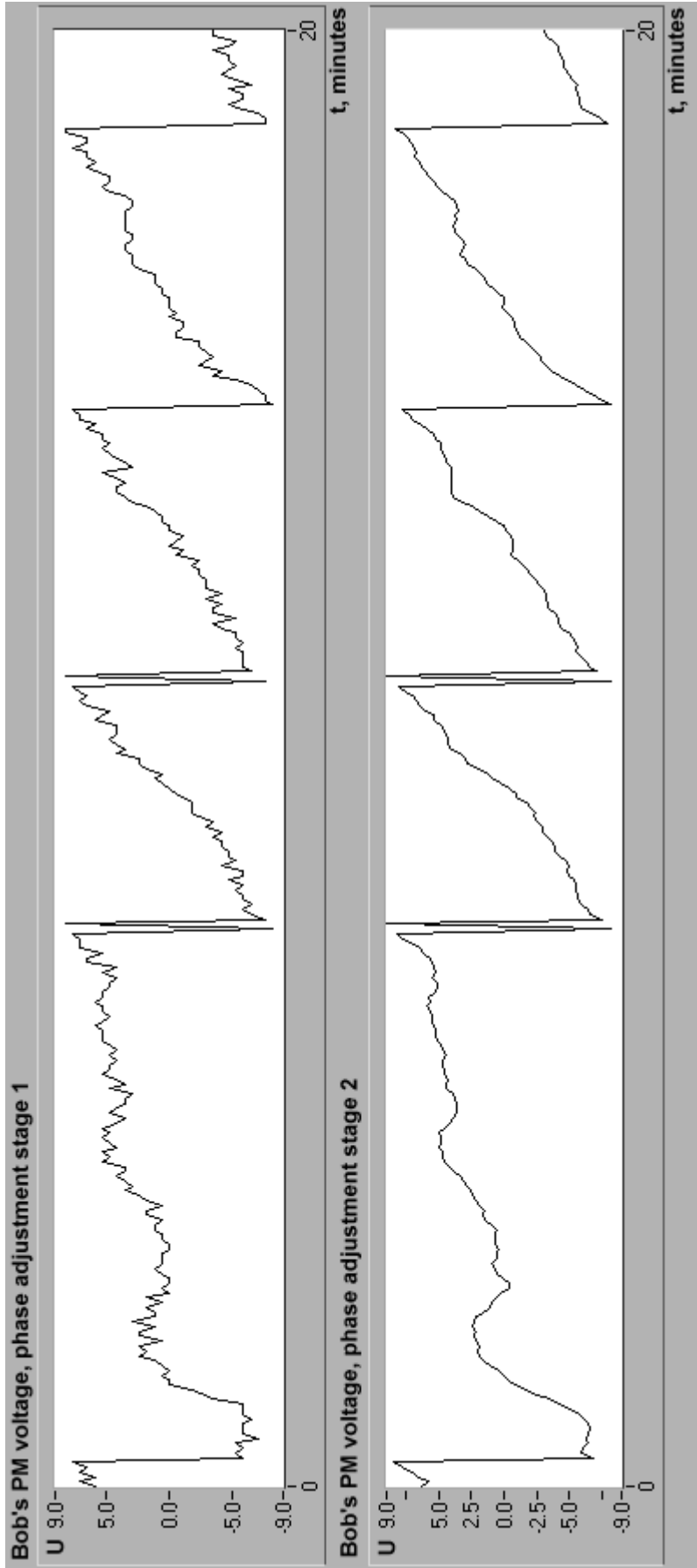


Рис. 11. Графики итогового напряжения смещения для фазового модулятора Боба (вверху – предварительные результаты, полученные на первом этапе, внизу – окончательные результаты, полученные на втором этапе).

Рис. 11 иллюстрирует результат работы алгоритма автоматической подстройки фазы - то напряжение, которое должно подаваться на фазовый модулятор Боба в качестве постоянного смещения при передаче ключа для того, чтобы система могла нормально функционировать в условиях дрейфа фазы. Ось ординат можно проградуировать и в градусах, которым соответствует напряжение фазового модулятора. Когда фаза проходит через  $360^\circ$ , происходит скачок (график шёл бы без скачков, если бы был нарисован на поверхности цилиндра).

График снимался в течение 20-ти минут; было снято подряд 300 значений напряжения, то есть каждый раз оба этапа подстройки фазы занимали в сумме 4 секунды. Это связано, в первую очередь, с медлительностью LabVIEW. Программа, полностью написанная, скажем, на C и со вставкой на ассемблере, отвечающей за сбор данных из Vох3, работала бы как минимум на порядок быстрее. Ещё сильнее ускорить процесс могла бы предварительная обработка данных с детектора прямо внутри Vох3 – на данный момент содержимое его буферной памяти (512 КБ) читается побайтно, что при необходимости чтения всего содержимого требует 524288 циклов ввода-вывода и занимает значительную часть времени. Если принять во внимание, что вероятность отсчёта детектора в реальных условиях (линия длиной 20 км, эффективность детектора 10 %) составляет порядка  $5 \cdot 10^{-4}$ , то при выводе из Vох3 информации лишь о тех случаях, когда детектор сработал, можно уменьшить количество циклов примерно в 2000 раз.

Как мы видим, фаза медленно дрейфует со скоростью, не превышающей  $360^\circ$  за несколько минут. Скорость изменения фазы изменяется случайным образом; иногда фаза начинает бежать в обратном направлении. "Шумный" вид верхнего графика объясняется ограниченным количеством шагов и ограниченным количеством отсчётов на каждом из этих шагов на первом этапе. Нижний график выглядит гораздо более

гладким, потому что  $\Delta\varphi$ , получаемая в результате выполнения второго этапа, компенсирует неточности первого этапа. Остаточный шум на нижнем графике может быть обусловлен относительно высокочастотной составляющей фазового дрейфа – это подтверждается тем фактом, что даже значительное увеличение числа отсчётов, собираемых на втором этапе, не приводит к дальнейшему сглаживанию кривой.

Другие научные группы, работающие с системами квантовой передачи ключа на основе фазового кодирования, разработали различные подходы к проблеме компенсации дрейфа фазы в своих интерферометрах. Вольфганг Титтель и его коллеги [23] для достижения стабильности фазы применили активную термостабилизацию своей установки. Интерферометры Алисы и Боба помещены в отрезки медных труб (длина отрезков – 40 см, диаметр – 2 см), трубы заткнуты с обоих концов и заполнены внутри песком. На трубы намотана проволока нагревателя, а внутри каждой трубы помещён термодатчик. Трубы уложены в контейнеры с поролоном внутри. Температура поддерживается на уровне 30 °С в соответствии с сигналами термодатчиков. В эксперименте они постепенно (в течение нескольких часов) поднимали температуру одного из интерферометров на 0,5 °С, при этом интерференционная картина прошла через четыре полных периода [23]. После фиксирования температуры на определённой точке фаза была достаточно стабильной, и было решено не разрабатывать дополнительных методик подстройки фазы.

Идея активной термостабилизации довольно проста и очевидна, однако она имеет свои недостатки. Главный из них – в том, что такая система является довольно инерционной (для подстройки фазы необходимо время порядка нескольких часов). Таким образом, хотя система в определённой степени ограждена от температурных воздействий, любое механическое возмущение выведет её из состояния

равновесия, и для компенсации такого возмущения потребуется время порядка нескольких часов. Представленная же в данной дипломной работе методика позволяет компенсировать возмущения (механические, температурные) за время порядка нескольких секунд. Следует отметить, что работа нашей системы была бы сильно затруднена в условиях быстрых изменений температуры, поэтому применяется термоизоляция интерферометра поролоном, однако применение активной термостабилизации не требуется.

Научная группа во главе с Полом Таунсендом для подстройки фазы применила пьезоэлектрический преобразователь для регулировки длины одного из плеч в интерферометре у Алисы [5]. Процедура подстройки фазы производилась следующим образом: Алиса и Боб отключали свои фазовые модуляторы, и Алиса переключала свой переменный аттенюатор в состояние с низким ослаблением для увеличения числа фотонов в импульсе. Затем она задействовала свой пьезоэлектрический преобразователь и регулировала с его помощью длину одного из плеч интерферометра, в то время как Боб следил за срабатываниями детекторов на выходах "0" и "1". В тот момент, когда число срабатываний детектора на выходе "1" достигало минимума, Боб посылал Алисе сигнал, по которому Алиса переключала свой переменный аттенюатор в состояние с высоким ослаблением и начинала передачу ключа. По результатам эксперимента [5], скорость дрейфа фазы составляла порядка 0,6 рад/мин, то есть фаза проходила  $360^\circ$  за время порядка 10,5 мин. В нашей установке скорость дрейфа фазы менялась с течением времени, но как правило не превышала 1 рад/мин.

Недостаток подхода Таунсенда вполне очевиден – он требует введения сразу двух дополнительных компонентов (пьезоэлектрического преобразователя и переменного аттенюатора). Наша система не требует

введения данных компонентов, таким образом мы повышаем её надёжность, одновременно уменьшая стоимость системы.

В настоящее время Таунсенд и его коллеги испытывают новый вариант квантовой криптографической установки [24]. В новой установке половинки интерферометра Маха-Цендера у Алисы и Боба изготовлены с помощью технологии интегральной оптики, поэтому они имеют небольшие размеры и их термостабилизация осуществляется элементами Пельтье. Ситуация аналогична случаю с установкой [23], то есть кроме активной термостабилизации никаких других мер по компенсации дрейфа фазы не предпринимается – отличие состоит лишь в том, что система [24] из-за меньших размеров менее инерционна.

## Заключение

Системы квантовой передачи ключа – это новое поколение криптографических систем, призванное обеспечить конфиденциальность передаваемой информации, недостижимую для классических криптосистем.

Целями данной дипломной работы являлись разработка методики автоматической компенсации дрейфа фазы в интерферометре квантовой криптографической системы, сборка и настройка этой системы и испытания данной методики в действии. Автоматическая компенсация дрейфа фазы, наряду с пассивными мерами (тепло- и виброизоляции) является необходимой для нормальной работы системы при передаче криптографического ключа. Применение разработанной методики автоматической подстройки фазы позволяет работать на квантовом уровне, то есть без увеличения количества света, проходящего через систему, по сравнению с режимом передачи ключа, что исключает необходимость использования дополнительных дорогостоящих компонентов (в первую очередь – переменного волоконно-оптического аттенюатора), тем самым упрощая всю систему и повышая её надёжность. Нормальная работа алгоритма автоматической подстройки фазы свидетельствует о том, что и оптическая, и электронная части системы квантовой передачи ключа настроены и функционируют должным образом. Разработанная методика компенсации дрейфа фазы является более перспективной по сравнению с методиками, разработанными другими научными группами. Следует отметить, что эксперименты, проведённые в рамках данной дипломной работы, не включали в себя непосредственно передачу ключа. На данный момент на кафедре физической электроники в NTNU происходит окончательная доводка программного обеспечения, отвечающего за передачу ключа, и соответствующие эксперименты будут проведены в первом полугодии 2002 г.

## Благодарности

Я благодарен своему научному руководителю, доценту кафедры радиофизики СПбГТУ Купцову В. Д.; профессору NTNU Дагу Йельме (Dag R. Hjelme) за руководство над проектом в Норвегии; аспиранту (PhD) Макарову В. В. с кафедры физической электроники в NTNU за неоценимую помощь в сборке установки и настройке её оптической части; сотруднице SINTEF Астрид Дирсетт (Astrid Dyrseth) за помощь в программировании на LabVIEW; а также всем тем, кто принимал участие в проекте до меня.

## Литература

- [1] Simon Singh. The Code Book. Fourth Estate, London, 1999.
- [2] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden. Quantum Cryptography, submitted to *Reviews of Modern Physics*, January 19, 2001.
- [3] Charles H. Bennett et al. Experimental Quantum Cryptography, *Journal of Cryptology*, no. 5, 1992.
- [4] Charles H. Bennett, Gilles Brassard, Artur K. Ekert. Quantum Cryptography, *Scientific American*, October 1992.
- [5] Christophe Marand, Paul D. Townsend. Quantum key distribution over distances as long as 30 km, *Optic Letters*, Vol. 20, No. 16, 1995.
- [6] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons. Quantum Cryptography over Underground Optical Fibers, *Lecture Notes in Computer Science* 1109, 1996.
- [7] R. J. Hughes, G. L. Morgan, C. G. Peterson. Practical quantum key distribution over a 48-km optical fiber network, *Journal of Modern Optics*, 47, 2000.
- [8] Wolfgang Tittel, Gregoire Ribordy and Nicolas Gisin. Quantum Cryptography, *Physics World*, March 1998.
- [9] A. Muller, J. Breguet and N. Gisin. Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km. *Europhysics Letters*, 23, 1993.
- [10] A. Muller, H. Zbinden and N. Gisin. Underwater quantum coding, *Nature* 378, 1995
- [11] A. Muller, H. Zbinden and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre, *Europhysics Letters*, 33, 1996.
- [12] J. D. Franson and B.C. Jacobs. Operational system for Quantum cryptography, *Elect. Letters*, 31, 1995.
- [13] Paul D. Townsend. Secure key distribution system based on Quantum cryptography, *Elect. Letters*, 30, 1994.
- [14] Paul D. Townsend. Quantum Cryptography in Optical Fiber Networks, *Optical Fiber Technology*, 4, 1998.

- [15] Paul D. Townsend. Simultaneous Quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM, *Elect. Letters*, 33, 1997.
- [16] Bennett, C. H., and Brassard, G., Quantum cryptography: Public key distribution and coin tossing. 1984, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179.
- [17] Wiesner, S., Conjugate coding, manuscript written *circa* 1970, unpublished until it appeared in *Sigact news*, Vol. 15, no. 1, 1983, pp. 78-88.
- [18] See, for example, Okoshi, T., Polarization-State Control Schemes for Heterodyne or Homodyne Optical Fiber Communications. *Journal of Lightwave Technology*, Vol. LT-3, no. 6, 1985, pp. 1232-1237.
- [19] Townsend, P. D., Rarity, J. G., and Tapster, P. R., Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters*, Vol. 29, no. 7, 1993, pp. 634-635.
- [20] Vakhitov, A., Makarov, V., and Hjelm, D. R., Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 2001, Vol. 48, no. 13, pp. 2023-2038
- [21] Martinelli M., A universal compensator for polarization changes induced by birefringence on a retracting beam. *Opt. Commun.*, 1989, vol. 72, pp. 341-344
- [22] Shor, P. W., Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35<sup>th</sup> Symposium on Foundations of Computer Science*, Los Alamitos, edited by Shafi Goldwasser (IEEE Computer Society Press), 1994, pp. 124-134
- [23] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time Bell states. *Phys. Rev. Lett.* Vol. 84, Number 20 (2000).
- [24] EQUIS Project. WP4 - Integrated Mach-Zehnder / Michelson interferometer (P. Townsend and G. Bonfrate from Corning Research, and four more persons from Heriot-Watt University).  
<http://www.phy.hw.ac.uk/resrev/EQUIS/>

## Приложение

Вычисление поправочного коэффициента для второго этапа подстройки фазы.

$$N_1 = (N_{\max} - N_{\text{dark}}) \sin\left(\frac{\Delta\varphi + 90^\circ}{360^\circ} \pi\right) + N_{\text{dark}}$$

$$N_2 = (N_{\max} - N_{\text{dark}}) \sin\left(\frac{\Delta\varphi - 90^\circ}{360^\circ} \pi\right) + N_{\text{dark}}$$

Вычисление  $\Delta\varphi$ :

$$\sin^2\left(\frac{\Delta\varphi_a + 90^\circ}{360^\circ} \pi\right) = \frac{N_1 - N_{\text{dark}}}{N_{\max} - N_{\text{dark}}}$$

$$1 - \cos\left(\frac{\Delta\varphi_a + 90^\circ}{180^\circ} \pi\right) = 2 \frac{N_1 - N_{\text{dark}}}{N_{\max} - N_{\text{dark}}}$$

$$\frac{\Delta\varphi_a + 90^\circ}{180^\circ} \pi = \arccos\left(2 \frac{N_1 - N_{\text{dark}}}{N_{\max} - N_{\text{dark}}} + 1\right)$$

$$\Delta\varphi_a = \frac{180^\circ}{\pi} \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - 90^\circ$$

Аналогичные вычисления с использованием  $N_2$  дают второе значение  $\Delta\varphi$ :

$$\Delta\varphi_b = \frac{180^\circ}{\pi} \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) + 90^\circ$$

$\Delta\varphi$  может быть вычислена усреднением  $\Delta\varphi_a$  и  $\Delta\varphi_b$ :

$$\Delta\varphi = \frac{\Delta\varphi_a + \Delta\varphi_b}{2}$$

$$\Delta\varphi = \frac{90^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) \right)$$

Поскольку мы имеем два временных интервала ("0" и "1"), аналогичные результаты будут получены для второго интервала:

$$\Delta\varphi = \frac{90^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_4}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_3}{N_{\max} - N_{\text{dark}}} + 1\right) \right)$$

Путём усреднения получаем окончательное значение  $\Delta\varphi$ :

$$\Delta\varphi = \frac{45^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) + \arccos\left(2 \frac{N_{\text{dark}} - N_4}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_3}{N_{\max} - N_{\text{dark}}} + 1\right) \right)$$