Министерство образования Российской Федерации

Санкт-Петербургский Государственный Политехнический Университет

Радиофизический факультет
Кафедра радиофизики

Допустить работу к защите
Зав. кафедрой д.ф.-м.н.
профессор

_____

Черепанов А.С.

Дипломный проект

Тема: **СИСТЕМЫ КВАНТОВОЙ КРИПТОГРАФИИ (QUANTUM CRYPTOGRAPHY SYSTEMS)**

Специальность: 201500 – «Бытовая радиоэлектронная аппаратура»

Выполнил студент гр. 6091/2: _____ Чижов М.Н.

Руководитель работы, к.ф.-м.н., доцент: _____ Медведев А.В.

Консультанты по работе:
аспирант _____ Анисимов А.А.

аспирант (NTNU) _____ Макаров В.В.

Консультант по
охране труда, к.т.н. доцент: _____ Малышев В.П.

Санкт-Петербург
2004

Содержание (Table of Contents)

Данный диплом состоит из двух частей. Работа над первой частью велась в лаборатории кафедры, ее тема: «Методы стабилизации низких температур с помощью элементов Пельтье». В ней описывается создание системы охлаждения фотодетектора, который используется в системах квантовой криптографии.

Вторая часть диплома была написана по результатам работы, которая проводилась во время моего пребывания (январь 2004 – июль 2004) в Норвежском университете науки и технологии (NTNU, г. Тронхейм) и финансировалась Норвежским государственным образовательным заемным фондом (State Educational Loan Fund). Тема этой части: «Эксперимент по квантовой передаче ключа» («Quantum Key Distribution experiment»). В ней описывается установка для квантовой передачи ключа с фазовым кодированием, ее программное обеспечение и результаты проведенных экспериментов. Эта часть приведена на английском языке.

1. Введение

Непрерывное совершенствование технологии производства радиоматериалов и принципов конструирования аппаратуры привело к тому, что параметры значительного числа радиоустройств, предназначенных для работы в обычном интервале температур, приблизились к теоретически достижимому пределу. Это означает, что возможности, определяемые свойствами веществ, из которых изготовлены компоненты радиоаппаратуры, при комнатных температурах во многом уже исчерпаны. Использование низких температур позволяет преодолеть это препятствие и открывает новые пути в разработке радиоэлектронных систем.

В последние годы по всему миру активно разрабатываются системы квантовой криптографии. В лаборатории кафедры ведутся работы по созданию фотодетекторов для систем квантовой криптографии. Требование высокой чувствительности, вплоть до регистрации единичных фотонов, и низкого уровня ложных срабатываний приводит к необходимости использования в качестве чувствительного элемента лавинного фотодиода, охлажденного до низких температур. Так как характеристики фотодиода сильно зависят от температуры, ее необходимо стабилизировать с высокой точностью. Типовые значения рабочих температур фотодиодов -50…-80 ^{o}C при точности ее поддержания не хуже десятых долей градуса.

При исследовании экспериментальных моделей фотодетекторов необходимо также изменение температуры, что повышает требования к оптимизации переходных процессов, возникающих в системе регулирования. Все это в сочетании с высокой точностью поддержания температуры вплоть до предельно низких значений, требует тщательного расчета и экспериментальной проработки не только электронной части системы охлаждения, но и конструкции устройства.

Таким образом, целью данной работы является:

- создание автономной и компактной системы охлаждения фотодиодов до температуры -50…-60 ^{o}C;
- разработка системы автоматического регулирования (САР) для поддержания заданной температуры фотодиодов с точностью до 0.1 ^{o}C.

В NTNU ведутся работы по созданию квантовой криптографической системы передачи ключа с фазовым кодированием. Эта работа требует не только настройки оптических компонентов, но и написания программного обеспечения. В мою задачу входило создание программы для осуществления передачи ключа между двумя объектами и вычисления процента ошибки (QBER (Quantum Bit Error Rate)), а также реализация блокировки сопровождающего импульса сигнала (afterpulse blocking) на программном уровне. Необходимо было получить значение QBER<11%.

Также в дипломе рассмотрены принципы криптографии, приведено сравнение классических и квантовых криптосистем, и объяснено преимущество квантовых систем с фазовым кодированием.

2. Обзор литературы

2.1 Методы стабилизации низких температур с помощью элементов Пельтье

2.1.1 Методы охлаждения

По способу получения холода циклы криогенных установок подразделяются на три группы, каждая из которых включает ряд типов в зависимости от процесса охлаждения.

1. Циклы для термомеханической системы, в которой рабочим веществом является газ или жидкость.
2. Циклы с использованием рабочего вещества в твердом состоянии.
3. Прочие циклы. К этой группе можно отнести циклы, основанные на использовании особых свойств такого рабочего вещества как изотопы гелия.

Сжатие газа является необходимым и важнейшим процессом холодильного цикла при использовании газообразных рабочих тел. Процессы сжатия реализуются в компрессорных машинах и могут протекать по-разному в машинах различных типов. Анализ экспериментальных данных существующих рефрижераторов, работающих по циклам Джоуля-Томсона, Клода, обратному циклу Стирлинга, Мак Магона-Джиффорда, показывает принципиальную трудность при конструировании всех криогенных газовых установок: уменьшение КПД и уменьшение холодопроизводительности при микроминиатюризации конструкции.

Электронные охладители любого типа отличаются от газовых машинных охладителей отсутствием механических подвижных деталей, объемных полостей и т. д. Поэтому размерный фактор, ограничивающий создание газовых микрокриогенных установок минимальной холодопроизводительности, в электронных – не является ограничением. Электронные методы охлаждения принципиально отличаются от всех

известных тем, что при их использовании электрическая энергия непосредственно создает тепловой поток без применения какого-либо движущегося жидкого или газообразного рабочего тела. Поэтому электронные охладители не нуждаются в обслуживании и ремонте и могут работать длительное время, позволяя в принципе объединить электронный микроохладитель с электронной схемой в одной конструкции.

Существуют два электронных метода получения криогенных температур: с отсутствием переноса носителей заряда и с использованием явлений переноса [1,2]. К последнему относится термоэлектрический метод (эффект Пельтье).

Требование автономности фотодетектора и малых его габаритов не позволяет использовать для достижения низких температур сжиженные газы и компрессорные холодильники. Таким образом, наиболее подходящими для использования в таких системах являются термоэлектрические модули, работающие на основе эффекта Пельтье. Эти модули серийно выпускаются промышленностью, надежны и находят широкое применение в различных устройствах.

2.1.2 Эффект Пельтье

В основе метода термоэлектрического охлаждения лежит эффект Пельтье (1834 г.), который заключается в выделении (или поглощении) теплоты $\boldsymbol{Q}$ в месте контакта двух различных проводников, включенных в электрическую цепь, при прохождении через нее электрического тока. Рабочей средой в такой электрической цепи из двух разнородных проводников является электронный газ, который переносит энергию от холодного контакта к теплому. Эффект Пельтье у металлов невелик, тогда как у полупроводников он во много раз выше; особенно значителен он в парах разнородных полупроводников дырочного (p) и электронного (n) типа. Схема термоэлемента, состоящего из двух последовательно соединенных полупроводниковых ветвей **A** и **B**, приведена на рис.1. При прохождении

тока поглощается теплота Q_x при температуре T_x на холодном конце элемента и выделяется теплота Q_o при температуре T_o на теплом конце. Количество теплоты прямо пропорционально току, проходящему через термопару:

$Q = П \cdot I$, где $П$ – коэффициент Пельтье.

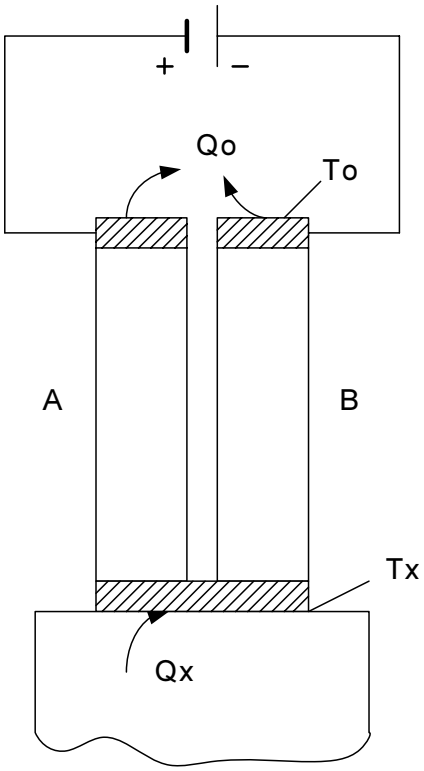


Рис.1 Схема термоэлемента, состоящего из пары полупроводников

Коэффициент $П$ можно выразить через коэффициент a термо-ЭДС; термо-ЭДС $E = a \cdot T$, здесь T – температура спая. Причем, $П = a \cdot T$. Полную термо-ЭДС пары проводников **A** и **B** определяют как разность их абсолютных значений для каждого проводника; при этом $a = a_A - a_B$. Таким образом, теплота, поглощаемая в единицу времени на холодном конце, т.е. холодопроизводительность элемента (при отсутствии потерь), Вт

$Q_{ox} = (a_A - a_B) \cdot I \cdot T_x$.

Увеличение силы тока приводит к росту Q_{ox} , но одновременно увеличиваются и потери за счет джоулевой теплоты:

$Q_{Дж} = ½ \cdot I^2 \cdot R$.

Другой источник потерь обусловлен теплопроводностью ветвей элемента

$Q_T = K \cdot (T_o - T_x)$, где $K = \sum \frac{\lambda}{l} \cdot f$ (λ - коэффициент теплопроводности; l и f – соответственно длина и площадь поперечного сечения каждой ветви термоэлемента).

Уравнение теплового баланса для контакта, находящегося в холодной зоне, при отсутствии теплопритока из окружающей среды запишем в виде

$$(a_A - a_B) \cdot I \cdot T_x = Q_x + \tfrac{1}{2} \cdot I^2 \cdot R + K \cdot (T_o - T_x) ,$$

где Q_x – полезный эффект охлаждения, обеспечиваемый термоэлементом.

Минимально возможную температуру можно T_x достичь при $Q_x = 0$, тогда соответствующая разность температур равна

$$T_o - T_x = \{(a_A - a_B) \cdot I \cdot T_x - \tfrac{1}{2} \cdot I^2 \cdot R\} / K .$$

Поэтому, если термоэлемент используется для охлаждения, то для эффективной работы необходимо обеспечить беспрепятственное рассеивание мощности на горячем спае [1].

Отсюда можно найти оптимальную силу тока I_{opt} , соответствующую наибольшей разности температур.

$$I_{opt} = \{(a_A - a_B) \cdot T_x\} / R .$$

Для производства термоэлектрических модулей используется сплав теллура и висмута с добавками селена и сурьмы. Слитки выращенного материала нарезаются на прямоугольные ветки с квадратным сечением. Последовательно соединенные две ветки разной проводимости образуют термоэлектрическую пару (рис.2). Для изготовления термоэлектрического модуля термоэлектрические пары соединяются последовательно по току (параллельно по тепловому потоку) между двух керамических пластин. Внутренняя структура модуля Пельтье представлена на рис.3 [3].

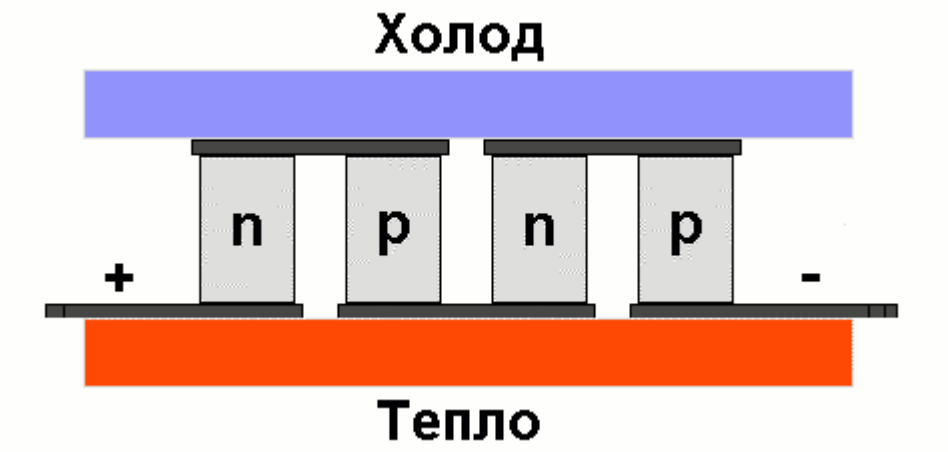


Рис.2 Модуль Пельтье на полупроводниках p- и n типа

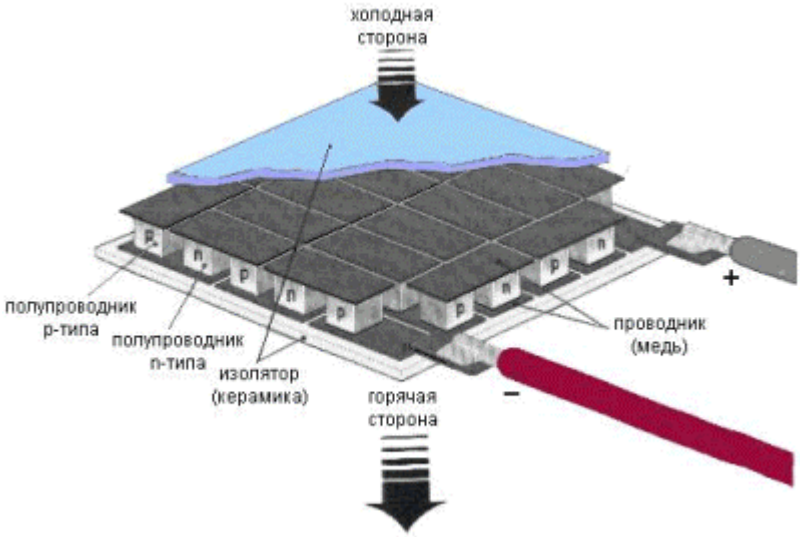


Рис.3 Структура модуля Пельтье

Увеличения эффективности и температурного перепада можно достичь при использовании многокаскадных схем. В каскадной термобатарее несколько элементов последовательно охлаждают друг друга; полезный эффект создается на нижнем первом каскаде. Холодный конец второго каскада отводит теплоту от первого и, в свою очередь охлаждается верхним третьим каскадом, передающим в окружающую среду теплоту. Термоэлементы в зоне контакта электроизолированы один от другого. С увеличением числа ступеней отвода теплоты холодильный коэффициент существенно возрастает [1].

2.1.3 Особенности применения модулей Пельтье

Охлаждающие устройства на основе термоэлектрических модулей выполняют те же функции, что и традиционные компрессионные или абсорбционные агрегаты холодильников, работающие на основе хладагентов. Однако использование термоэлектрических модулей, представляющих собой, по сути, твердотельные тепловые насосы, имеет ряд преимуществ:

· отсутствие в блоке охлаждения движущихся частей и рабочей жидкости;

· бесшумность работы;

· малый размер и вес охлаждающей системы, возможность построения микроминиатюрных охладителей;

· высокая надежность термоэлектрического модуля;

· легкость управления и возможность прецизионной регулировки температуры;

· низкая стоимость при высокой эффективности работы;

· возможность работы в любом положении.

Указанные преимущества делают термоэлектрические модули очень популярными, что подтверждается постоянным ростом спроса на них во всем мире и возникновением новых областей их использования. Однако если приведенные выше факторы не являются доминирующими, то термоэлектричество нельзя рассматривать как единственный способ решения всех проблем охлаждения, и при выборе принципа охлаждения для данной конкретной задачи следует руководствоваться сравнением различных принципов по критерию "эффективность/стоимость" [3].

Кроме перечисленных преимуществ, модули Пельтье обладают и специфическими свойствами, которые необходимо учитывать при их эксплуатации:

- Модули Пельтье, выделяющие в процессе работы большое количество тепла, требуют наличия в составе кулера соответствующих радиаторов и вентиляторов, способных эффективно отводить избыточное тепло.

При этом термоэлектрические модули отличаются относительно низким коэффициентом полезного действия, и сами являются источниками тепла. Использование данных модулей в составе средств охлаждения электронных компонентов вызывает значительный рост температуры внутри блока, что нередко требует дополнительных мер и средств для снижения температуры внутри корпуса. В противном случае повышенная температура создает трудности для работы не только охлаждаемых элементов и их систем охлаждения, но и остальным компонентам прибора. Также необходимо отметить, что модули Пельтье являются сравнительно мощной дополнительной нагрузкой для блока питания.

- Модуль Пельтье, в случае его выхода из строя, изолирует охлаждаемый элемент от радиатора. Это приводит к быстрому нарушению теплового режима защищаемого элемента, особенно в том случае, когда он сам является источником тепла (например, при охлаждении микросхемы процессора).
- Низкие температуры, возникающие в процессе работы холодильников Пельтье, способствуют конденсации влаги из воздуха.

2.1.4 Теплоизоляция

Теория теплообмена – это наука о процессах переноса теплоты в пространстве с неоднородным распределением температур. К особому случаю теплопроводности в криогенных системах относится перенос теплоты в различных видах тепловой изоляции. Перенос теплоты теплопроводностью является характерным для таких видов теплоизоляции, как пенопласты, газонаполненные порошковые и волокнистые материалы, вакуумированные порошковые и волокнистые материалы, многослойные изоляции. Обычная теплоизоляция имеет зернистую, волокнистую или ячеистую структуру и находится под атмосферным давлением, в отличие от вакуумной. Перечисленные изоляции расположены в порядке улучшения их

свойств и увеличения цены. В дополнение к эффективности выбор изоляции для каждого конкретного случая определяется как компромисс между ценой, технологичностью, весом, прочностью и др.

Материалы, имеющие теплопроводность λ при t = 50…100 ^{o}C меньше 0.25 Вт/(м·К), называются теплоизоляторами. Некоторые теплоизолирующие материалы используются в их естественном состоянии (пробка, опилки, слюда), другие получают искусственно (минеральная вата, стеклянная вата). Хорошие теплоизоляторы получают при добавлении пенообразующих веществ к различным химикатам. Такие материалы называются пенопластами. Например, пенопласты К-40 и ПУ-101 имеют теплопроводность 0.046 и 0.057 Вт/(м·К) соответственно [4].

Механизм передачи теплоты через такую дисперсную среду, как теплоизоляция носит сложный характер и определяется рядом составляющих, а именно теплопроводностью твердых частиц, контактным теплообменом в местах касания частиц или слоев, конвекцией и теплопроводностью газа, излучением между частицами.

Итак, как уже было сказано получаемые в процессе работы модулей Пельтье, низкие температуры способствуют конденсации влаги из воздуха. Это приводит к необходимости тщательно изолировать охлаждаемый объект. Учитывая стоимость, легкость в обработке и теплопроводность в качестве теплоизолятора был выбран пенопласт.

2.1.5 Измерение температуры

Измерение температуры вещества основано на изменении физических свойств тела, находящегося в тепловом контакте с контролируемым веществом, в зависимости от изменения температуры.

Для измерения температуры необходимо преобразовать градусы Цельсия (Кельвина) в другую, более удобную для контроля физическую величину. Устройство, выполняющее такое преобразование, называется датчиком

температуры. Основное назначение датчиков – служить воспринимающими элементами приборов контроля и автоматического регулирования.

Наибольшее применение имеют датчики, использующие такие физические явления, как тепловое расширение, изменение электрической проводимости вещества и появление контактной термо-ЭДС.

Учитывая необходимость автоматического регулирования температуры, а также компактные размеры холодильника использование ртутных и манометрических термометров не представляется возможным.

Применение термоэлектрических датчиков (термопар) для измерения температуры основано на возникновении термо-ЭДС в электрически соединенных разнородных проводниках при условии разности температур между точками их соединения. Один спай разнородных проводников называется горячим или рабочим концом, а другой холодным или свободным концом. Величина термо-ЭДС развиваемая термопарой, зависит от материала электродов и от разницы температур рабочего и свободного спаев. Поэтому при измерении температуры необходимо свободный спай поддерживать при постоянной температуре.

Следующий способ состоит в применении полупроводниковых термометров сопротивления (термисторов). Он основан на использовании изменения их электрического сопротивления в зависимости от температуры. Эта зависимость выражается экспоненциальным законом, что создает трудности при их использовании в качестве датчиков температуры.

Такой проблемы не возникает у полупроводниковых диодов. Зависимость сопротивления их переходов от температуры позволяет с успехом применять их в качестве датчиков температуры. Из-за нелинейности вольт-амперной характеристики диодов для измерения температуры используют линейную характеристику изменения напряжения на диоде в зависимости от его температуры при постоянном значении тока, протекающего в прямом направлении через переход. Постоянство тока достигается последовательным включением диода и большого активного сопротивления в цепь с

источником постоянного напряжения. Ток, протекающий через диод, устанавливают порядка 1-2 мА, так как большой ток приводит к ошибке измерения температуры вследствие внутреннего разогрева диода [5].

Также можно использовать платиновый термометр сопротивления. Но он стоит дороже.

Таким образом, в нашем случае было решено производить измерение температуры при помощи полупроводникового диода.

2.1.6 Автоматическое регулирование

Работа любой технологической установки, агрегата или технологического объекта характеризуется различными физическими величинами, например температурой, давлением, расходом вещества и т. п. Для обеспечения оптимального режима их работы эти физические величины должны с определенной точностью поддерживаться на заданном уровне или изменяться по определенному закону. Эта задача может быть успешно решена с помощью использования автоматического регулирования.

Комплекс технических средств (устройств), присоединяемых к регулируемому объекту и обеспечивающих автоматическое поддержание заданного значения его регулируемой величины или автоматическое изменение ее по заданному закону, называют *автоматическим регулятором.*

В общем случае совокупность управляемого объекта и автоматического управляющего устройства, определенным образом взаимодействующих между собой, называют *автоматической системой*. Автоматическая система с замкнутой цепью воздействия, в которой управляющее (регулирующее) воздействие вырабатывается в результате сравнения истинного значения управляемой (регулируемой) величины с заданным (предписанным) ее значением, называется *системой автоматического регулирования (САР)*.

По функциональному назначению при разработке систем автоматического регулирования наиболее широко применяются следующие элементы.

Первичные измерительные устройства (ИУ) *(датчики)* – элементы, измеряющие значение регулируемой величины и преобразующие их в эквивалентные значения сигнала, как правило, другой физической природы, более удобной для последующей передачи и использования.

Устройства, формирующие закон регулирования (УФЗР) (ф*ункциональные преобразователи)* – это преобразователи, которые при поступлении на вход сигнала формируют на выходе изменение сигнала во времени по определенному закону.

Усилительные устройства (УУ) – это устройства, предназначенные для усиления в случае необходимости поступающих сигналов.

Сравнивающие устройства (СУ) – элементы, сравнивающие значения двух (или нескольких) сигналов. Выходной сигнал этих элементов равен разности поступающих на их вход сигналов.

Задающие устройства (ЗУ) – элементы, с помощью которых оператор устанавливает заданное значение регулируемой величины.

Регулирующие органы (РО) – устройства, непосредственно воздействующие на объект регулирования для поддержания заданного значения регулируемой величины или изменения ее по заданному закону.

Исполнительные механизмы (ИМ) – устройства, воздействующие на регулирующий орган и изменяющие его состояние в сторону ликвидации отклонения регулируемой величины от заданного значения или закона ее изменения.

Объект регулирования (ОР) – объект, являющийся составным элементом системы автоматического регулирования.

На рис.4 в общем виде представлена функциональная структурная схема САР [6].

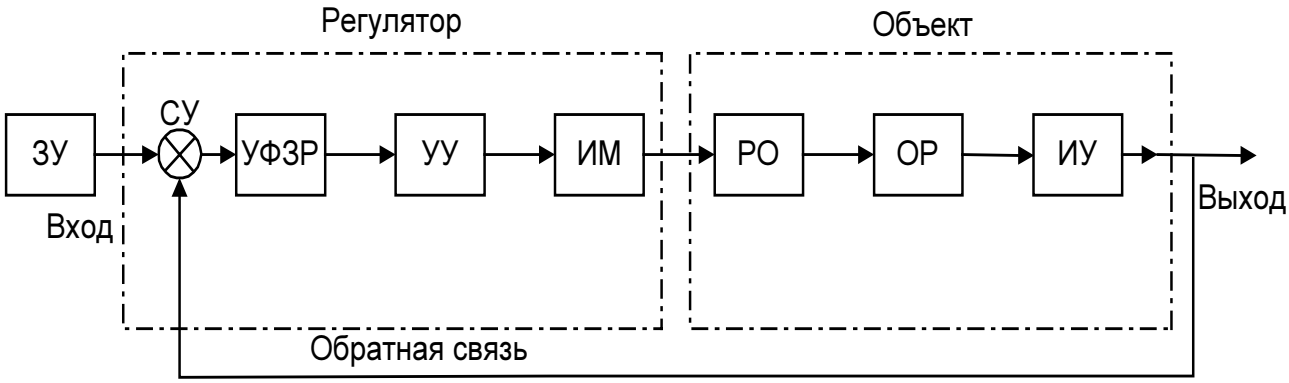


Рис.4 Типовая структурная схема САР

2.1.7 Виды САР

Наиболее распространенными задачами, которые решают системы автоматического регулирования, являются стабилизация, выполнение заданной программы и слежение.

Системы, поддерживающие постоянное значение управляемой величины при изменяющихся возмущающих воздействиях называются *стабилизирующими системами*.

Системы, изменяющие управляемую величину по заранее заданной программе, называются *программными системами*.

Системы, управляемая величина которых воспроизводит изменяющееся задающее воздействие, называются *следящими системами*.

В ряде случаев сама система в процессе управления должна производить поиск такого требуемого значения, которое необходимо в данный момент времени выдерживать, чтобы режим работы управляемого объекта был оптимальным по определенному параметру. Такие системы называются *экстремальными.*

В тех случаях, когда закон изменения параметров объекта во времени заранее хорошо известен, можно рассчитать, как и когда нужно менять параметры управляющего устройства, чтобы качество работы автоматической системы в целом оставалось неизменно хорошим. Если же составление такой программы оказывается невозможным вследствие

незнания истинного закона изменения хотя бы некоторых параметров объекта, то прибегают к построению *самонастраивающейся системы*.

Для решения поставленной перед нами задачи применяется *стабилизирующая* система регулирования.

Теперь рассмотрим классификацию автоматических систем по характеру внутренних динамических процессов. Основными признаками такого деления являются:

- непрерывность или дискретность (прерывистость) динамических процессов во времени;
- линейность или нелинейность уравнений, описывающих динамику процессов управления.

Применительно к поставленной задаче нас будут интересовать *непрерывные линейные системы* автоматического регулирования.

Системой непрерывного действия или непрерывной системой называется такая система, в каждом из звеньев которой непрерывному изменению входной величины во времени соответствует непрерывное изменение выходной величины. При этом закон изменения выходной величины во времени может быть произвольным, в зависимости от формы изменения входной величины и от вида уравнения динамики звена.

Линейной системой называется такая система, поведение всех звеньев которой вполне описывается линейными уравнениями (алгебраическими и дифференциальными или разностными). Для этого прежде всего необходимо, чтобы статические характеристики всех звеньев системы были линейными [7].

2.1.8 Устойчивость САР

Устойчивость является одним из главных требований, предъявляемых к автоматическим системам.

Основным назначением САР в нашем случае является поддержание заданного постоянного значения регулируемого параметра (температуры).

При отклонении в данный момент времени регулируемого параметра от заданного значения, что может произойти или в результате появления возмущающих воздействий на систему, или при изменении заданного значения регулируемой величины, автоматический регулятор воздействует на систему таким образом, чтобы ликвидировать это отклонение. В системе возникает переходный процесс, определяемый ее динамическими свойствами.

Если после окончания переходного процесса система снова приходит в первоначальное или другое равновесное состояние, то такую систему называют *устойчивой*.

Если при тех же условиях в системе или возникают колебания со все возрастающей амплитудой, или происходит монотонное увеличение отклонения регулируемой величины от ее заданного равновесного значения, то систему называют *неустойчивой* [6].

2.1.9 Качество процессов регулирования

Устойчивость является необходимым, но не достаточным условием работоспособности САР, поскольку в устойчивой системе могут возникать очень медленно затухающие, длительные переходные процессы, и ее применение будет ограничено. Возникает необходимость количественно оценить качество процессов регулирования при устойчивой работе системы. Оно, как правило, оценивается по переходной функции системы. Основными показателями качества являются время регулирования, перерегулирование, колебательность и установившаяся ошибка. Для нас главное значение имеет установившаяся ошибка, а также время регулирования не должно быть слишком большим.

Одним из методов улучшения точности систем автоматического регулирования является повышение порядка астатизма.

Относительно задающего воздействия систему принято называть *статической*, если при любом постоянном задающем воздействии

установившаяся ошибка регулирования не равна нулю. Если же при любом постоянном задающем воздействии установившаяся ошибка регулирования равна нулю, то такую систему называют *астатической*.

Так, астатическая система первого порядка без установившейся ошибки отрабатывает постоянные задающие воздействия, но имеет установившуюся ошибку при задающем воздействии, изменяющемся с постоянной скоростью. Астатическая система второго порядка без установившейся ошибки отрабатывает как постоянные задающие воздействия, так и задающие воздействия, изменяющиеся с постоянной скоростью, но имеет установившуюся ошибку при изменении задающего воздействия с постоянным ускорением [8, 9].

2.2 Quantum key distribution experiment: cryptography overview

2.2.1 Abstract

This report describes tests of fiber-optic quantum key distribution (QKD) system. Phase coding, BB84 protocol, active phase tracking in the interferometer and software-based afterpulse blocking for APD single-photon detector were implemented. Although the best recorded quantum bit error rate (QBER) was 4%, the system was unstable and QBER fluctuated in the 4% to 13% range during the experiments. Replacement of defective electronic and optical parts is necessary before a better QKD demonstration can be made. A detailed description of the set-up and software is included. This report also reviews the principles of cryptography, compares classical cryptosystems and QKD systems, and explains the advantages of using phase-coding QKD set-up.

2.2.2 Introduction

Cryptography is the art of devising codes and ciphers, and cryptanalysis is the art of breaking them. Cryptology is the combination of the two.

Cryptography has a long history of military and diplomatic applications, dating back to the Babylonians. Even then people tried to find a way to exchange

messages in absolute secrecy. Nowadays, cryptography is becoming increasingly important in commercial applications for electronic business. Sensitive data such as credit card numbers and personal identification numbers (PINs) are routinely transmitted in encrypted form.

The best-known application of cryptography is secure communication.

2.2.3 Classical Cryptography

Cryptography is the art of hiding information in a string of bits that are meaningless to any unauthorized person. To achieve this goal, an algorithm is used to combine a message with some additional information – known as the "key" – to produce a cryptogram. This process is called "encryption". For a cryptosystem to be secure, it should be impossible to unlock the cryptogram without the key.

Usually the party that encrypts and transmits messages is called Alice, and the party that receives it is called Bob. There is also Eve – an unauthorized eavesdropper.

Cryptosystems come in two main classes – depending on whether the key is shared in secret or in public.

In asymmetrical systems Alice and Bob use different keys (public key for encryption and private key for decryption). They are also known as "public-key cryptosystems" and were proposed in 1976 by Whitfield Diffie and Martin Hellman [10]. Bob chooses a private key and keeps it secret. Then he computes a public key from it and openly publishes this key. Alice uses it to encrypt her message. She transmits her encrypted message to Bob, who decrypts it with the private key [11].

One such cryptosystem is RSA, which was proposed by Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman in 1977, and therefore has this name [12]. With RSA Bob generates his public key by multiplying two very large prime numbers.Anyone with the public key can send secret messages, but only Bob who knows the private key can read them. To decode you need the two large prime

numbers Bob used to create the public key in the first place. These two numbers – which Bob keeps hidden from everyone, even Alice – constitute his private key.

If Eve intercepts Alice's message, she can't read it, because she doesn't have Bob's private key. Eve's only hope of breaking the code is to work backwards, trying to deduce the private key from the public key. But Bob's primes are so large that Eve needs decades to figure them out [13].

But there are drawbacks with the RSA system. There is no guarantee that the factorisation algorithm doesn't exist. If it exists Eve could factorise numbers quickly. The second drawback is if a quantum computer is constructed in the future, the security of much of the conventional cryptography can be questioned, because recent work in quantum computation shows that quantum computers can factorise faster than classical computers [14].

Symmetrical ciphers (secret key cryptosystems) require the use of a single key for both encryption and decryption. Such a "one-time pad" system was proposed by Gilbert Vernam in 1917 and published in 1926 [15]. In this scheme Alice encrypts a message using a randomly generated key and then simply adds each bit of the message to the corresponding bit of the key. The scrambled text is then sent to Bob who decrypts the message by subtracting the same key. The problem with this system is that it is essential for Alice and Bob to possess a common secret key, which must be at least as long as the message itself. They can also only use the key for a single encryption – hence the name "one-time pad". Furthermore, the key has to be transmitted in some trusted ways, such as a courier, or through a personal meeting between Alice and Bob [11].

The most popular standard symmetric algorithm of data encoding is DES (Data Encryption Standard). The algorithm is developed by IBM, and in 1976 it was recommended by the National Bureau of Standards (NBS), the predecessor to today's National Institute of Standards and Technology (NIST), to usage in open sectors of economy. The essence of this algorithm consists in the following (Fig.5).

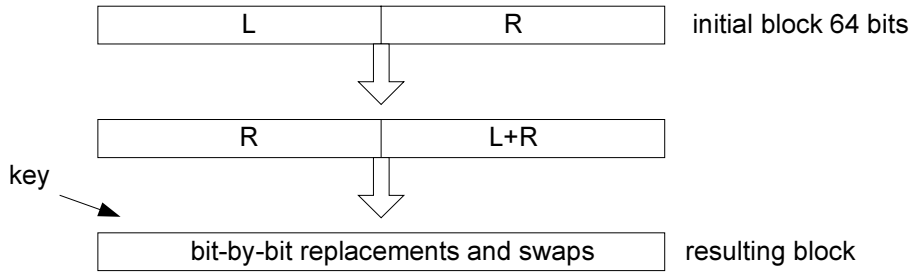


Fig.5. DES coding algorithm

The data are encrypted block by block. Before encoding any form of a data representation will be transformed in a numerical form. The block of the data by a size of 64 bits comes to an input of the coding function. Then it is bisected on left (L) and right (R) parts. At the first stage the right part of the initial block is located on a place of the left part of the resulting block. The right part of the resulting block is calculated as the modulo 2 sum (operation XOR) of the left and right parts of the initial block. Then on the basis of a random sequence under the defined scheme in the obtained result the bit-by-bit replacements and swaps are fulfilled. A DES key consists of 64 binary digits ("O"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte.

There have been several criticisms directed at DES, including its inadequate 56-bit key length and an alleged trapdoor inserted by the NBS [16]. Despite these gripes and further claims of attacks, DES has withstood the test of time, until recently: in January 1999, a cobbled-together network of 100,000 PCs cracked a DES-encoded message in slightly less than 24 hours. Therefore application of its strengthened variant called Triple-DES begins, which includes triple encoding with usage of two different keys. But it is necessary to pay for it in productivity – Triple-DES requires three times more time, than usual.

Triple-DES is DES, used three times on one block of the data, using different keys, except that the second operation passes in the return order in the decryption

mode. Basic disadvantage Triple-DES is that it provides rather small productivity of applications. The standard Triple-DES, which has more cycles of encoding, than for DES (in fact, it means triple application of DES algorithms to the initial text with usage of two or three different keys — with length of 112 or 168 bits), supports three times smaller speed.

One more weak place for DES and Triple-DES is the application of blocks of length 64 bits. For support of efficiency and safety it is desirable to use blocks of greater length.

Because of these disadvantages Triple-DES could not become the candidate for long-term application. In 2001 NIST has released the standard AES (Advanced Encryption Standard), known as FIPS 197 [17, 18]. It provides block encryption of length 128 bits and application of keys by a size 128, 192 and 256 bits.

Similar, that the version AES with a key length of 128 bits is realised today most frequently. Such key size is sufficient for support of a level of safety necessary for the majority of applications, and requires less time for data processing, than at usage of longer keys. These days there are no known loopholes neither in AES, nor in Triple-DES, and the level of safety is directly proportional to a key length of encoding.

According to AES, the entry objects for processes of encryption and decryption are single 128-bit blocks of the data. This block will be transformed to a matrix by a size 4x4 byte, which is named as the array of states. It will be updated on each cycle of coding or decoding. At a completing stage of the process the matrix of states again will be transformed to linear string of 128 bits. The similarly 128-bit key is perceived as a square-law matrix, which size is measured in bytes. 10 linear keys are shaped from it, what needs 10 operation cycles. The typical cycle consists of four phases.

As in the majority block coding devices, the algorithm of decryption uses the extended key in the return order. However algorithm of decryption is not identical to algorithm of encoding.

So we can see that a fundamental problem exists. In principle, any classical private channel can be monitored passively, without the sender or receiver knowing that the eavesdropping has taken place. For example, a key carried by a trusted courier might have been read en route by a surreptitious high-resolution x-ray scan or another sophisticated imaging technique without the courier's knowledge. More generally, classical physics allows all physical properties of an object to be measured without disturbing those properties. So classical theory leaves open the possibility of passive eavesdropping [19].

And other problem exists – sometimes we want to keep a secret forever, but Eve can wait many years until we have more powerful computers, to break our code. So by using classical cryptosystems our message is not completely secret.

2.2.4.Quantum Cryptography

In contrast to classical, quantum cryptography (QC) is based on the fundamental postulate of quantum physics that "every measurement disturbs a system". So it is possible to design a quantum channel, that carries signals based on quantum phenomena in such a way that any try to monitor the channel disturbs the signal in some detectable way. The effect arises because in quantum theory, certain pairs of physical properties are complementary in the sense that measuring one property disturbs the other. This statement known as the Heisenberg uncertainty principle, named after its discoverer, the German physicist Werner Heisenberg.

Quantum cryptography allows two physically separated parties to create a random secret key without a courier's help. The key distribution problem can be partially solved using the idea of quantum key distribution (QKD).

Quantum cryptography began with the work by Stephen Wiesner called "Conjugate coding". This paper was written in about 1970, but was unpublished until 1983 [20]. At that time Charles Bennett and Gilles Brassard, who were familiar with Wiesner's ideas, produced the first and best-known QKD protocol,

usually called “BB84”. It was published in 1984 [21]. So for best understanding of QKD, it will be useful to describe this protocol.

Assume that two people wish to exchange a message securely. They are connected by a quantum channel and a classical public channel. If single photons are being used to carry the information, the quantum channel is usually an optical fibre. The public channel can be any communication link, such as a phone line or an Internet connection. We can also use an optical fibre for the public link. In this case both channels differ only in the intensity of the light pulses that code the bits: one photon per bit for the quantum channel, hundreds of photons per bit for the classical public channel.

When a photon is on the move, it vibrates and the angle of vibration is called its polarization. A polarizer is simply a filter that permits certain photons to pass through it with the same oscillation as before and lets others pass through in a changed state of oscillation or blocks them.

Alice has a polarizer that can transmit the photons in any one of the four states mentioned. In fact, she can choose either rectilinear (vertical and horizontal) or diagonal (upleft/rightdown ($+45^{o}$) and upright/leftdown (-45^{o})) polarization filters. She sends a series of photons down the quantum channel and swaps her polarization scheme between rectilinear and diagonal filters for the transmission of each single photon bit in a random manner. In doing so, the transmission can have one of two polarization states that represent a single bit, either 1 or 0, in either scheme she uses. Alice also records her choice.

Bob has two analysers. One analyser allows him to distinguish between horizontally and vertically polarized photons. The other allows him to distinguish between photons polarized at $+45^{o}$ and -45^{o}. Like Alice he selects each polarizer in a random manner. He also writes down which analyser he used and what it recorded. Bob must choose to measure each photon bit using either his rectilinear or diagonal polarizer: sometimes he will choose the correct polarizer and at other times he will choose the wrong one.

Suppose Bob uses a rectilinear polarizer to measure diagonal photons (±45^{o}). If he does this, then the photons will pass through in a changed state, there is 50% chance that he will find the photon in either the +45^{o} channel or the –45^{o} channel. Even if he finds out later that he chose the wrong analyser, he will have no way of finding out which polarization state Alice sent.

On Fig.6 you can see example of quantum key distribution, where photons polarized at horizontal and +45^{o} represent 0, and photons polarized at vertical and -45^{o} represent 1.

After exchanging enough photons Bob announces on the public channel the sequence of analysers he used, but not the results that he obtained. Alice compares this sequence with the list of bits that she originally sent, and tells Bob on the public channel on which occasions his analyser was compatible with the photon's polarization [11]. Alice and Bob then discard all the photon measurements where he used the wrong polarizer. Now they have a sequence of 0s and 1s that is on average, half the length of the original transmission. We can use these bits to generate a key, and send encrypted messages to one another.

To assess the secrecy of their communication, Alice and Bob select a random part of their key, and compare it over the public channel. Obviously, the disclosed bits cannot then be used for encryption any more. If their key had been intercepted by an eavesdropper, the correlation between the values of their bits will have been reduced. For example, if Eve has the same equipment as Bob and cuts the fibre and measures the signal, she will always get a random bit whenever she chooses the wrong analyser, i.e. in 50% of the cases. But having intercepted the signal, Eve still has to send a photon to Bob, to cover her tracks. Therefore in half of the cases in which Alice's and Bob's analysers match, Eve will have sent a photon that is incorrectly polarized. However, in half of these cases, the photon will accidentally leave Bob's analyser through the correct channel, in which case, Eve's presence goes undetected. The point is that if Eve had been listening in, one in four of

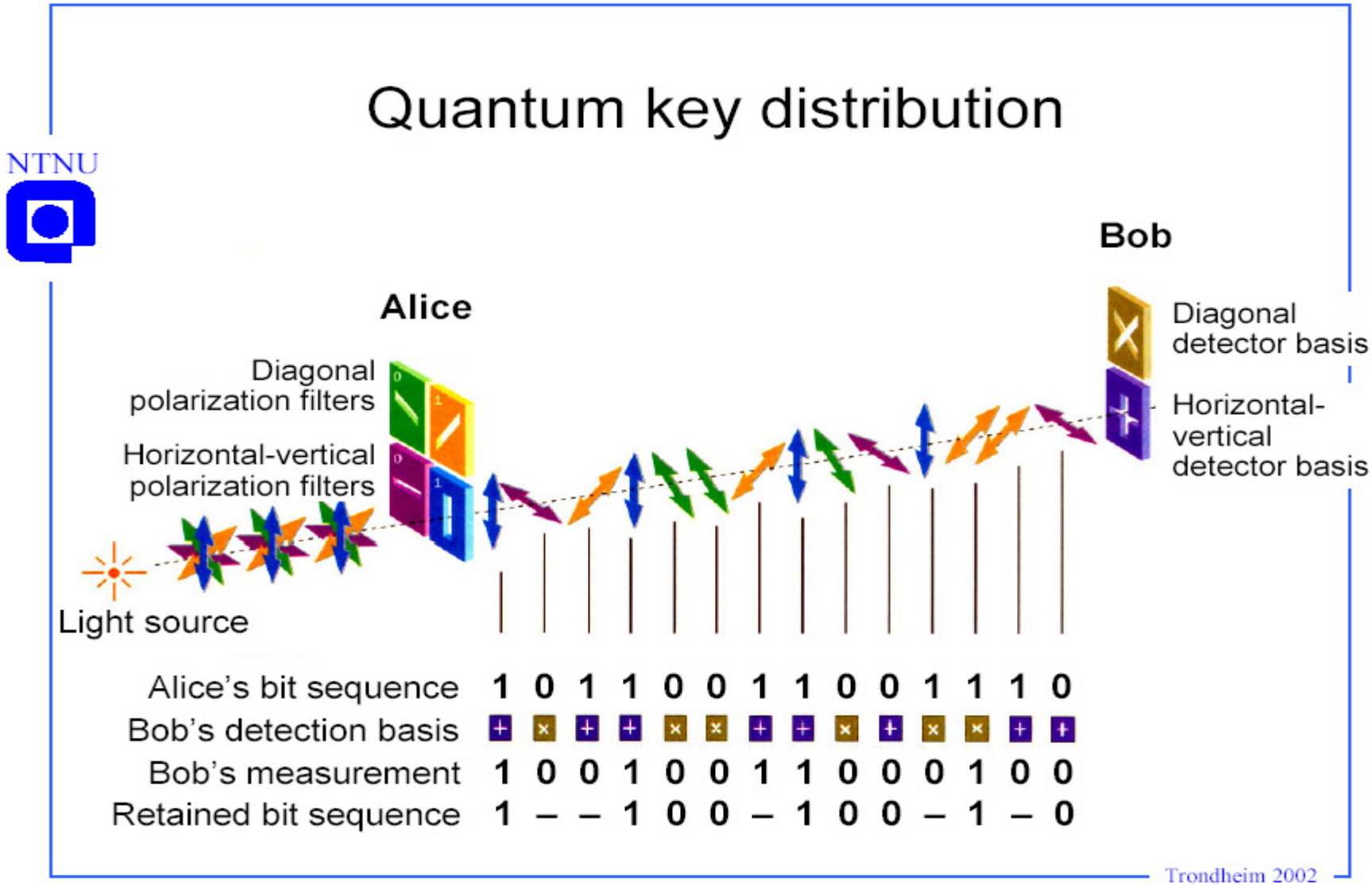


Fig.6. Encryption with polarized light, BB84 protocol (Reprinted from [11])

Alice's and Bob's bit values would disagree. In other words, her eavesdropping strategy could be easily detected [11].

If we have noise, which may occur randomly or may be introduced by eavesdropping, we should use an error correction procedure. When noise exists, the polarization observed by the receiver may not correspond to that emitted by the sender. In order to deal with this possibility, Alice and Bob must ensure that they possess the same string of bits, removing any discrepancies. In the Bennett protocol error correction is:

1) Alice and Bob agree on a random permutation of bit positions in their strings (to randomise the locations of errors).
2) The string is partitioned into blocks of size K (K is ideally chosen so that the probability of multiple errors per block is small).
3) For each block, Alice and Bob compute and publicly announce parities. The last bit of each block is then discarded (to avoid leaking any information to Eve).
4) For each block for which their calculated parities are different, Alice and Bob use a binary search with $log(K)$ iteration to locate and correct the error in the block.
5) To account for multiple errors that might remain undetected, steps 1-4 are repeated with increasing block sizes in an attempt to eliminate these errors.
6) To determine whether additional errors remain, Alice and Bob repeat a randomised check:
   - Alice and Bob agree publicly on a random assortment of half the bit positions in their bit strings.
   - Alice and Bob publicly compare parities (and discard a bit). If the strings differ, the parities will disagree with probability ½.
   - If there is disagreement, Alice and Bob use a binary search to find and eliminate it, as above.
7) If there is no disagreement after l iterations, Alice and Bob conclude that their strings agree with low probability of error (2^{-l}) [22].

In addition to error correction to reduce the amount of information that Eve may have obtained, Alice and Bob use a procedure known as “privacy amplification”, in which several bits are combined into one.

But there is a problem in using the polarization states of photons for distribution of a key, because we have the polarization transformation along the optical fibre. This means that a real fibre-based QC system would require active polarization adjustment. Even replacing standard fibres with polarization maintaining fibres doesn’t solve the problem [23].

There is an alternative scheme that is more suitable for long distances, based on differences in phase instead of differences in polarization of photons.

2.2.5 Phase coding QKD system

A phase coding QKD set-up was developed in 1993 by Paul Townsend and colleagues at British Telecom [24]. They also used BB84 protocol. In this scheme Alice and Bob use identical unbalanced Mach-Zehnder interferometers, in which one arm is longer than the other. Interferometers are connected in series by a single optical fibre, and both have a phase modulator (PM) in a short arm. Alice’s interferometer is combined with a single-photon source, while Bob’s one is combined with photon-counting detectors (Fig.7).

Pulses that go down the short arm in Alice’s interferometer and then the long arm in Bob’s interferometer, interfere with pulses that follow the long arm first and then the short one. When Alice sends her message, she randomly applies phase shifts of 0, $\pi/2$, π or $3\pi/2$ to her photons. Bob only has the option of applying a phase shift of $\pi/2$ or none at all. If Bob applies no phase shift, he can work out whether Alice’s photon has a phase shift 0 or π. On the other hand, if Bob applies a phase shift of $\pi/2$, he can distinguish between Alice’s choice of $\pi/2$ and $3\pi/2$. After the message has been sent, Alice and Bob compare their settings using the public channel. When the difference in phase is equal to 0 or π, Alice and Bob use compatible bases and they obtain a deterministic result. A secret key can therefore be established by interpreting phase shifts of 0 and $\pi/2$ as “0”, and π and $3\pi/2$ as

"1". When the phase difference equals π/2 or 3π/2, the bases are incompatible and the photon randomly chooses which port it takes at Bob's coupler. Incompatible measurements are discarded (Table 1) [11,23].

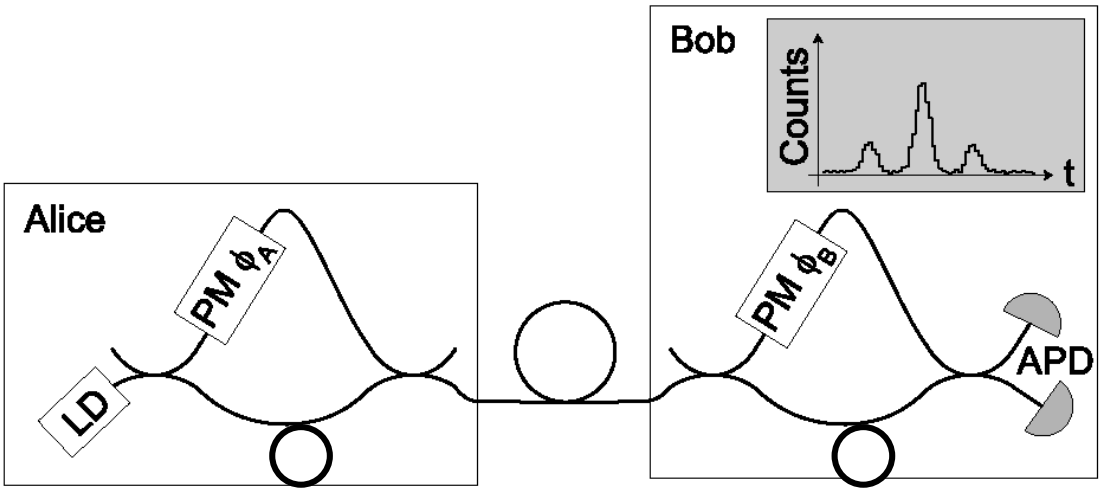


Fig.7. Double Mach-Zehnder implementation of an interferometric system for quantum cryptography (LD: laser diode, PM: phase modulator, APD: avalanche photodiode) (Reprinted from [23])

Alice		Bob		
Bit value	φ_A	φ_B	φ_A-φ_B	Bit value
0	0	0	0	0
0	0	π/2	3π/2	?
1	π	0	π	1
1	π	π/2	π/2	?
0	π/2	0	π/2	?
0	π/2	π/2	0	0
1	3π/2	0	3π/2	?
1	3π/2	π/2	π	1

Table 1. Implementation of the BB84 four-states protocol with phase encoding

After that Alice and Bob apply error correction and privacy amplification as in polarization encoding. This scheme requires a polarization control too, because two pulses in Bob's interferometer interfere perfectly only if they are in the same polarization state. But it is not so sensitive as the polarization encoding scheme. Another problem is that the arms in the two interferometers have to be adjusted so

that the differences in the path length are the same. These differences also have to be kept stable [11].

2.2.6 Experimental QKD

QKD is an active experimental field. The first working prototype, constructed in 1989 at IBM in Yorktown Heights, New York, transmitted quantum signals over 32 cm of open air (the results were published only in 1992 by Bennett, Bessette) [25]. Since then, tremendous progress has been made. Today, various groups have shown that quantum key distribution is possible, even outside the laboratory.

For example, Antonie Muller and co-workers at the University of Geneva have used polarization coding system to perform QC experiments over optical fibres (1993) [26]. They created a key over a distance of 1100 meters with photons at 800 nm. In order to increase the transmission distance, they repeated the experiment with photons at 1300 nm (1995) and created a key over a distance of 23 km [27]. An interesting feature of this experiment is that the quantum channel connecting Alice and Bob consisted of an optical fibre part of an installed cable used by the telecommunication company Swisscom for carrying phone conversations. It runs between the Swiss cities of Geneva and Nyon, under Lake Geneva. This was the first time QC was performed outside of a physics laboratory. These experiments had a strong impact on the interest of the wider public in the new field of quantum communication.

In 1993 Paul Tapset and John Rarity of DERA, the Defence Evaluation and Research Agency (Malvern, England), working with Paul Townsend, were the first to test the double Mach-Zehnder implementation of an interferometric system with phase coding over a fibre optic spool of 10 km [24].

In 1995 Christopher Marand and Paul Townsend improved the transmission distance up to 30 km [28]. It is useful to describe this set-up in detail because our set-up is similar to it. Since true single-photon states are difficult to generate in practice, they utilize instead the nonorthogonal phase states of weak coherent pulses in an interferometer. The experimental system shown in Fig.8 is based on a

Mach-Zehnder device in which the source is a 1.3-μm-wavelength semiconductor laser that generates 80-ps-duration pulses at a repetition rate of 1MHz. The laser output is strongly attenuated so that the average photon number of the pulse pairs entering the transmission fibre is ~0.1. This system is formally equivalent to a simple Mach-Zehnder interferometer with a phase modulator in each spatially separated arm. However, by use of time and polarization division to separate the individual paths in a single long-transmission fibre, the device can be many kilometres in length and yet still remain stable against environmental perturbations. Although polarization division alone would be sufficient to separate the two components, the addition of time division means that the error rate in the system is less sensitive to small changes in output polarization from the transmission fibre. Pulses leaving the interferometer are detected with a time correlated photon-counting set-up, which is based on a liquid-nitrogen-cooled germanium avalanche photodiode (APD). The device is operated in Geiger mode, with the above-breakdown bias gated on for ~100 ns (every 1μs) synchronously with the laser source. Coupling between the interferometer and the APD is provided by a low-loss polarization multiplexer, and pulses arriving from the 1 and 0 output ports are distinguished temporally by means of a fibre delay loop.

Both polarization and phase coding systems require active compensation of optical path fluctuations (such as polarization and interferometer phase shifts). But there is another so called plug & play auto-compensating set-up [23].

The first experiment on such a system was in early 1997 and a key was exchanged over a 23 km installed optical cable [29]. After that in 2002 D. Stucki, N. Gisin and co-workers with id Quantique SA company presented a fibre optical QKD system, which works at 1550 nm and is based on the plug & play set-up. They performed a key exchange over 67 km between Geneva and Lausanne [30].

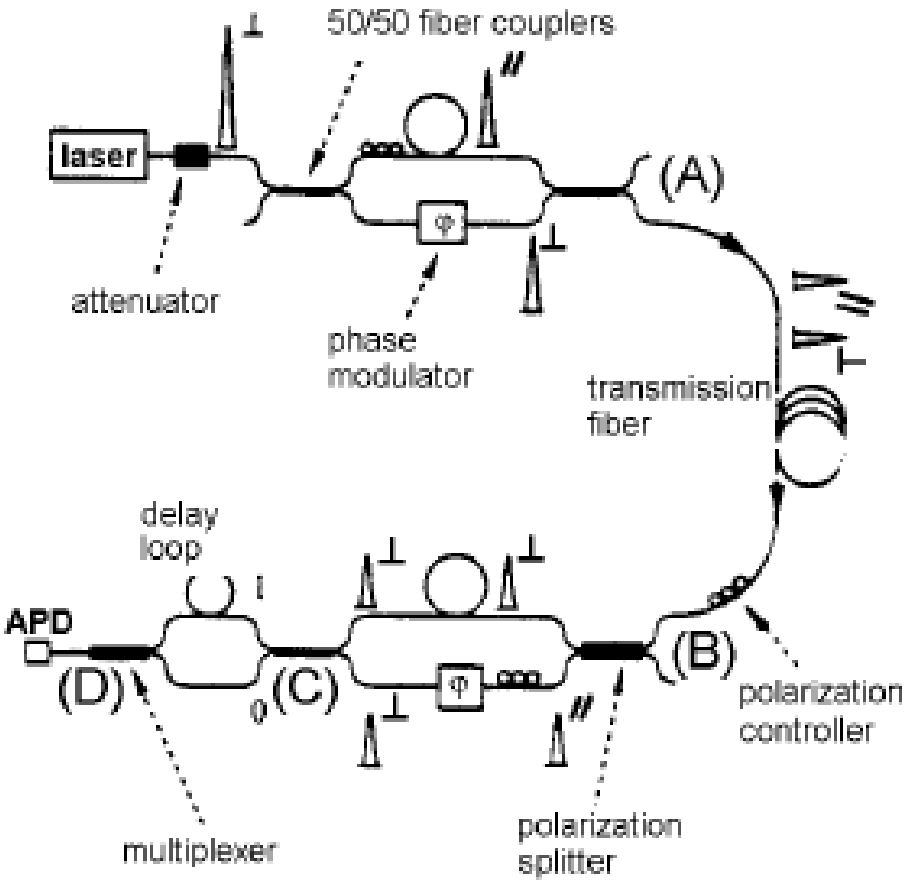


Fig.8. Marand-Townsend interferometric quantum key distribution scheme (Reprinted from [28])

There has also been progress in free-space cryptographic transmission, with the eventual goal of satellite-borne QKD. C. Kurtsiefer and co-workers have recently transmitted a secret key between two mountains separated by 23.4 km in south Germany [31]. This marks a step towards accomplishing key exchange with a near-Earth orbiting satellite and hence a global key distribution system.

3. Разработка охладителя

3.1 Выбор конструкции охладителя

В связи с тем, что нам необходимо получить достаточно низкие температуры, и при этом устройство должно быть компактным, было принято решение использовать элементы Пельтье. Эти элементы имеют свойство создавать разность температур между своими поверхностями под воздействием протекающего через них тока. Таким образом, мы можем изменять температуру внутри холодильника, меняя протекающий через элементы Пельтье ток. Их применение облегчит создание системы регулирования. Для достижения более низких температур была выбрана двухступенчатая схема охлаждения: «верхняя» ступень для охлаждения объекта и «нижняя» ступень для охлаждения «верхней» ступени. Но одних элементов Пельтье недостаточно, так как от «нижней» ступени необходимо отводить тепло. Это связано с их принципом работы: чем холоднее одна из поверхностей элемента, тем будет холоднее и другая.

Первоначально была реализована конструкция с отводом тепла от нижней ступени при помощи водяного охлаждения (рис.9). Вода проходит сквозь радиатор, отводящий тепло от «нижней» ступени.

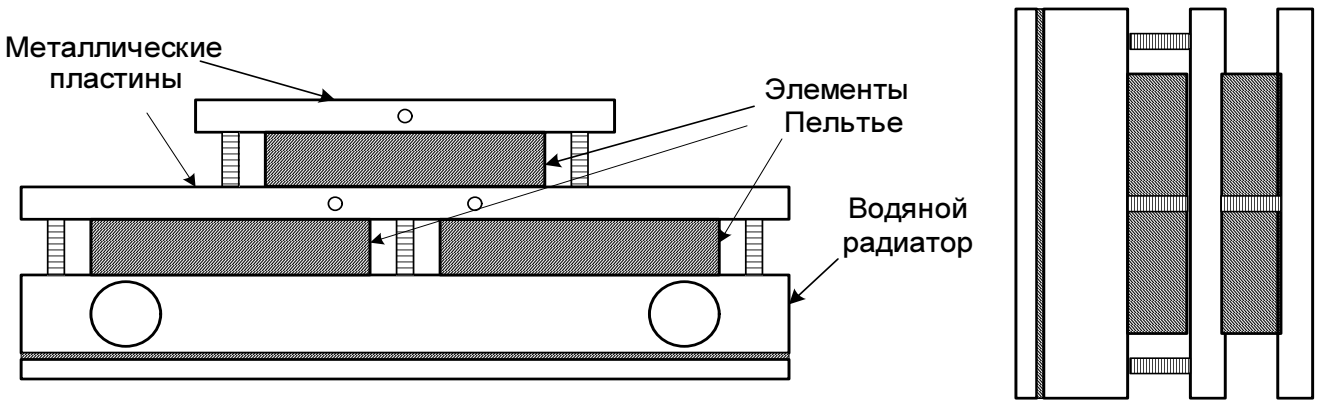


Рис.9 Система с водяным охлаждением

Внутри верхней металлической пластины находится охлаждаемый объект (фотодиод) и датчик температуры (полупроводниковый диод).

Для «нижней» ступени были использованы 2 модуля FROST-73 (I_{max}=6.2A, U_{max}=16.5В). Для «верхней» – 1 модуль TURBO-1,5 (I_{max}=3.1A, U_{max}=31.4В). Но эксперименты показали, что не удается полностью отвести тепло, выделяющееся на модулях при максимальных режимах. Это приводит к перегреву модулей и повышению температуры. Экспериментально полученные оптимальные значения токов и напряжений для обеспечения низких температур таковы: FROST-73 (I=5.4A, U=12.5В), TURBO-1,5 (I=1.5A, U=10В).

При таком способе отвода тепла от нижней ступени после теплоизоляции конструкции при помощи пенопласта внутри холодильника была получена температура –57 ^{o}C. Устройство получилось компактным: длина – 11 см, ширина – 6.5 см, высота – 5 см. Этот тип охлаждения является эффективным, но требует подключения к водопроводу, что не удовлетворяет требованию об автономности.

Поэтому для отвода тепла от «нижней» ступени было принято решение использовать воздушное охлаждение. В конструкцию такого типа входят 4 вентилятора, установленные на радиаторах, и 2-х ступенчатая система из элементов Пельтье (рис.10). Здесь внутри центральной пластины находится охлаждаемый объект и датчик температуры. Размеры холодильника: длина – 18 см, ширина – 8 см, высота – 20 см .

В воздушном варианте для нижней ступени были использованы 4 модуля FROST-73 (I_{max}=6.2A, U_{max}=16.5В). Для «верхней» – 2 двухступенчатых модуля BULLFINCH (I_{max}=8.8A, U_{max}=8.9В). Экспериментально полученные оптимальные значения рабочих режимов охладителя таковы: FROST-73 (I=4A, U=12.6В), BULLFINCH (I=5A, U=6.6В).

Детектор с воздушным охлаждением является автономным и удобным в эксплуатации, но он не дает таких низких значений температур как водяной. Так, после теплоизоляции было получено значение температуры –52 ^{o}C.

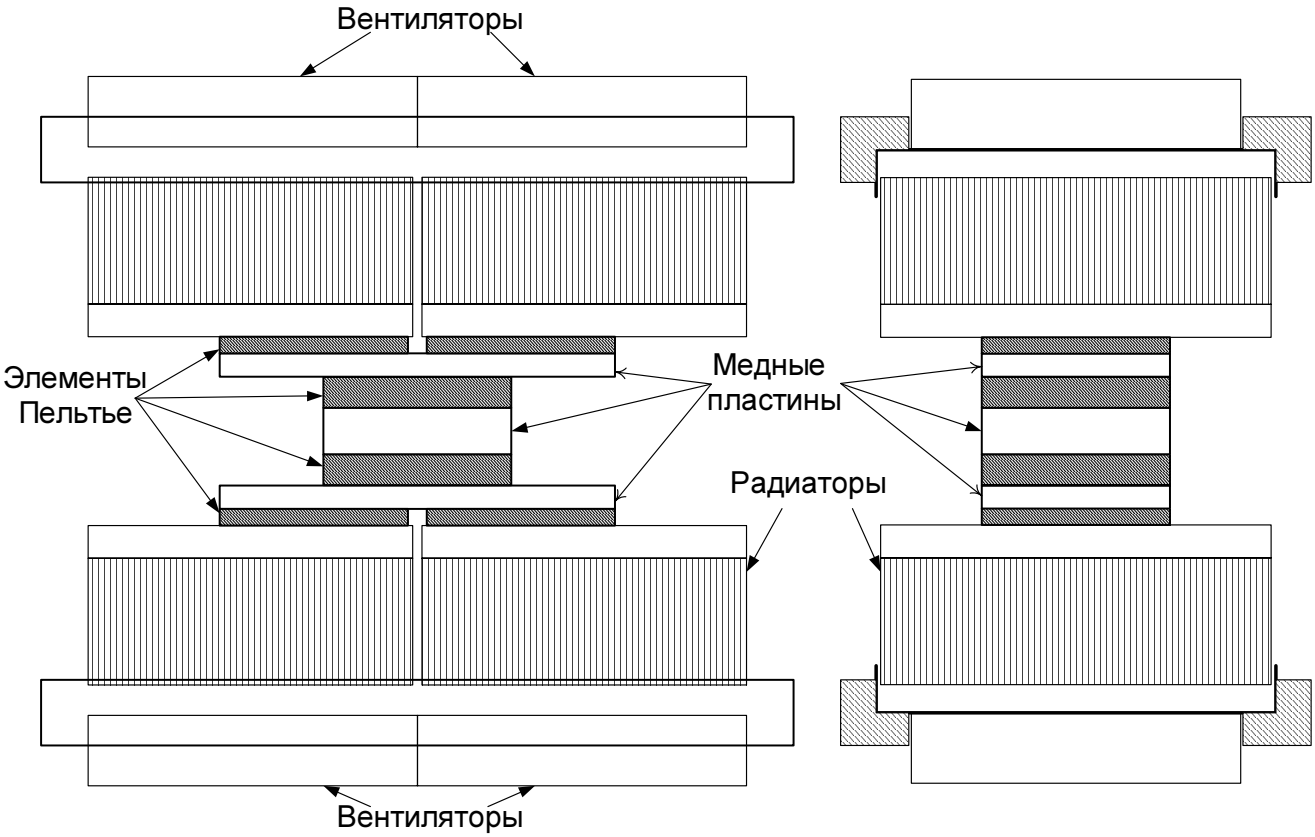


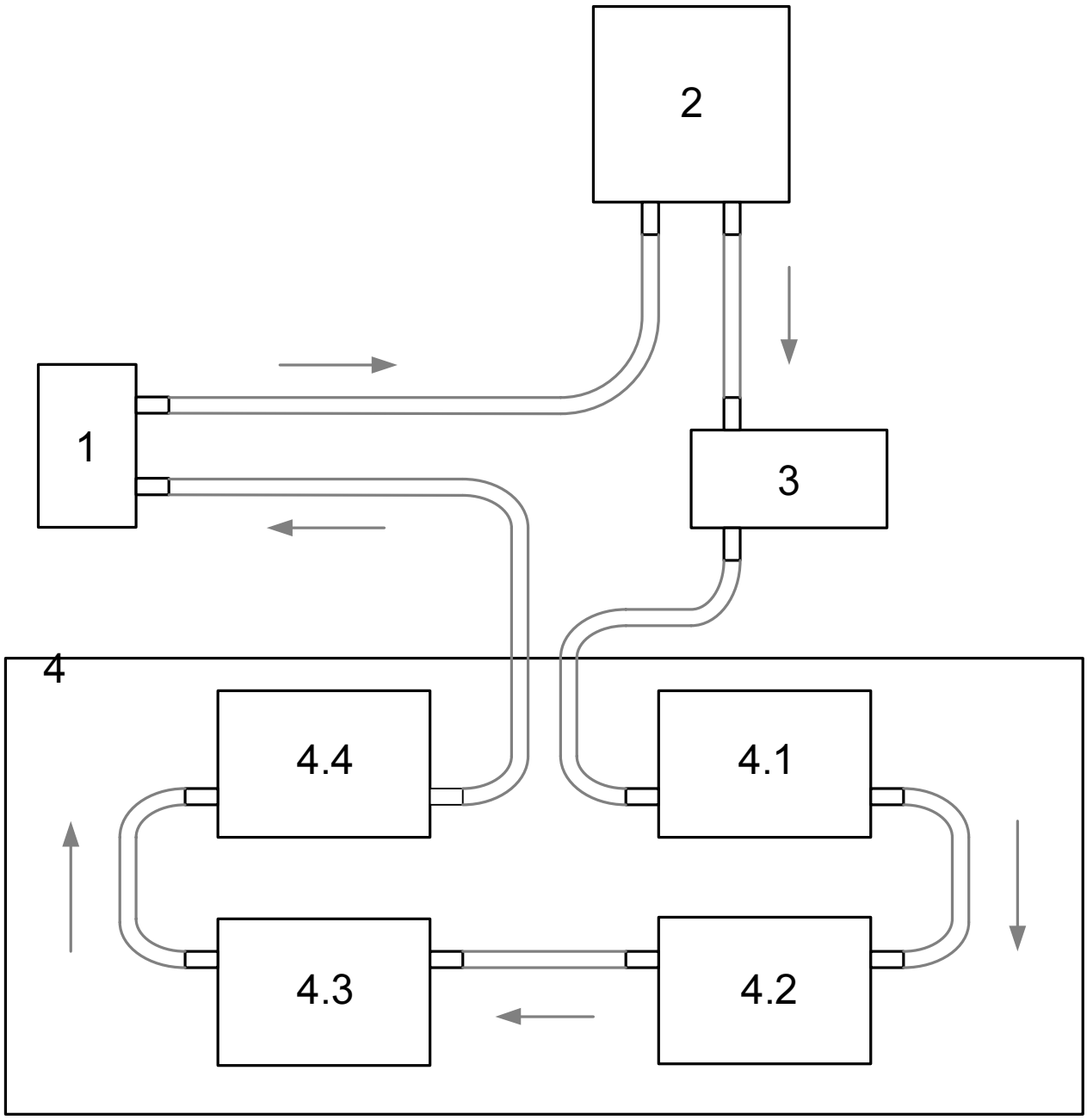
Рис.10 Система с воздушным охлаждением

Учитывая все плюсы и минусы воздушного и водяного охлаждения, было принято решение о целесообразности использования замкнутого контура водяного охлаждения. На рис.11 представлена блок схема такого варианта.

В контуре, вместо воды был использован тосол А40. Такая замена была вызвана тем, что в ходе экспериментов значение температуры охлаждающей жидкости опускалось ниже 0 ^{o}C. Стрелочками на рисунке показано направление движения тосола по соединительным трубкам.

Теперь перейдем к описанию отдельных блоков системы охлаждения.

Блок, предназначенный для охлаждения непосредственно фотодиода, состоит из металлической пластины (где находится фотодиод и датчик температуры), элемента Пельтье и водяного радиатора (рис.12).



1 – охладитель фотодиода (рис.12)

2 – расширительный бачок для тосола

3 – насос

4 – система охлаждения тосола (приложение 1)

4.1…4.4 – модули, состоящие из водяного радиатора, 2-х элементов Пельтье, воздушного радиатора и вентилятора (рис.13)

Рис.11 Контур водяного охлаждения

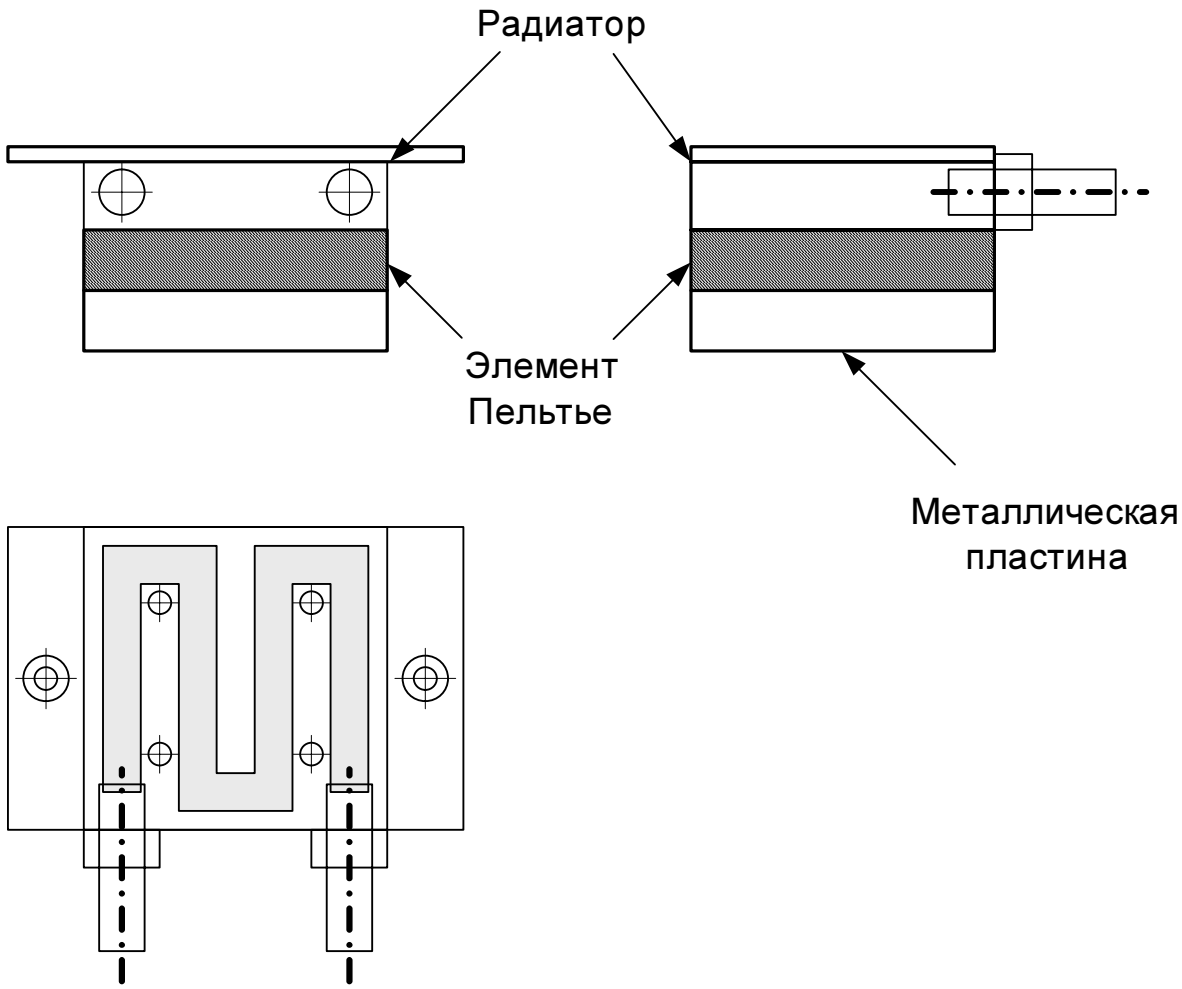


Рис.12 Блок охлаждения фотодиода

Элемент Пельтье охлаждает пластину, а тепло выделяющееся на нем отводится при помощи протекающего сквозь радиатор тосола. Для предотвращения контакта теплого воздуха и пластины, а также образования конденсата блок охлаждения тщательно теплоизолирован со всех сторон. В качестве теплоизолятора применялся пенопласт, толщина которого была определена используя программу компании «Криотерм». Также были теплоизолированы модули системы охлаждения тосола, расширительный бачок и соединительные трубки.

Система охлаждения тосола состоит из четырех одинаковых последовательно соединенных модулей. Каждый модуль (рис.13) состоит из водяного радиатора, 2-х элементов Пельтье, воздушного радиатора и вентилятора.

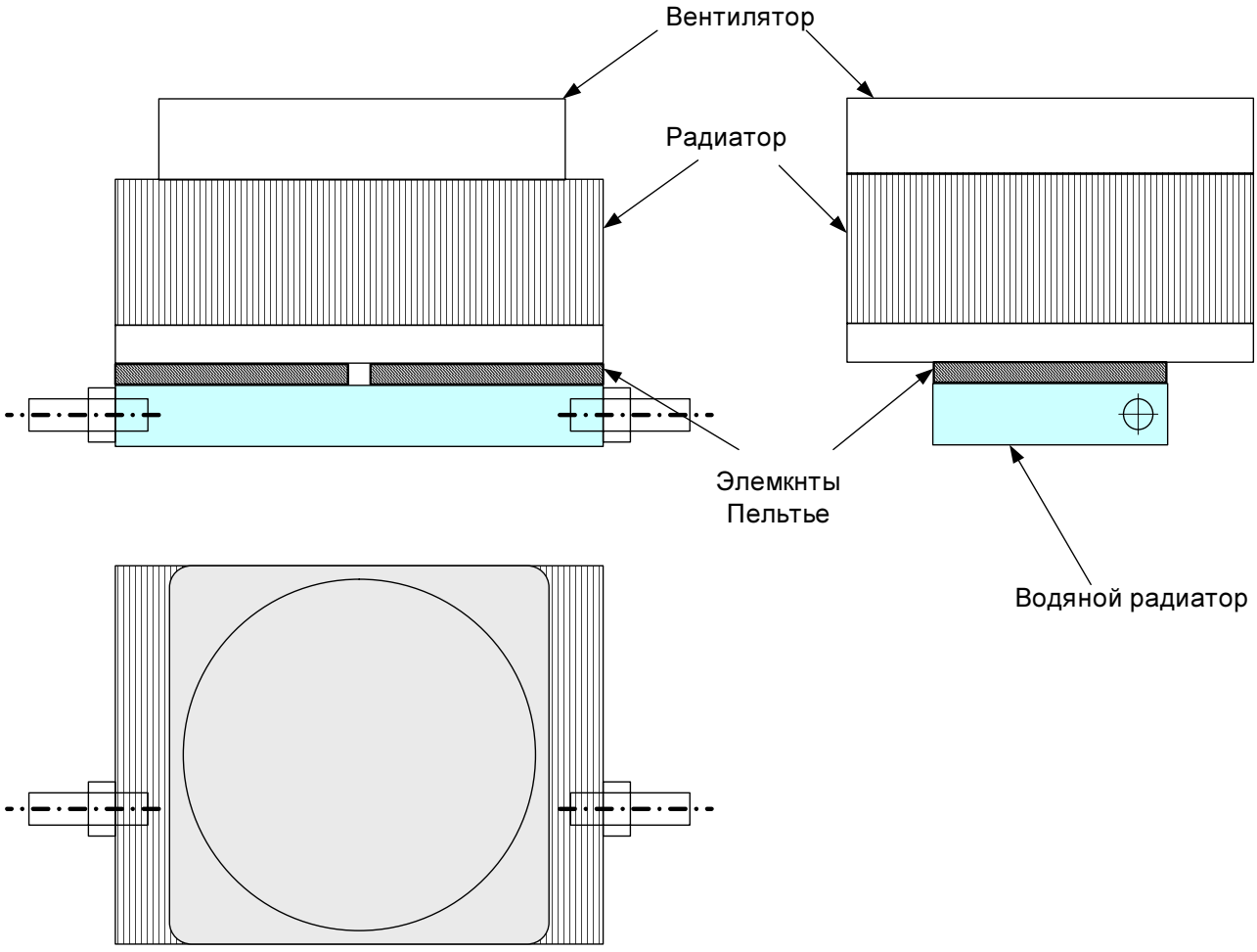


Рис.13 Модуль для охлаждения тосола

Тосол, протекая сквозь радиатор охлаждается элементами Пельтье, тепло от которых отводится посредством воздушного охлаждения. Для этого были использованы стандартные компьютерные радиаторы с вентилятором.

Конструкция радиаторов для охлаждения фотодиода и тосола приведена в приложении 1.

Учитывая, что вся конструкция охладителя находится в корпусе необходимо отводить избыточное тепло от охлаждающих модулей. Для этого внутри корпуса с помощью дополнительных вентиляторов создан воздушный

поток. Расположение модулей в системе охлаждения тосола и направления воздушных потоков внутри корпуса представлены в приложении 2. В частности на рисунке стрелками представлены направления движения нагнетаемого холодного и отводимого теплого воздуха.

3.2 Выбор типов элементов Пельтье

Для выбора термоэлектрических модулей была использована программа, предоставленная компанией «Криотерм». Она позволяет рассчитать холодопроизводительность и подобрать тип модулей.

Так, для задачи охлаждения тосола был выбран однокаскадный термоэлектрический модуль FROST-74. Его параметры:

- dTmax = 74 К - максимальная разность температур между сторонами модуля при определенной температуре горячей стороны (Th=300 K);
- Imax = 6.3 А - ток, при котором достигается разность температур dTmax;
- Umax = 16.7 В - напряжение, соответствующее току Imax и разности температур dTmax;
- Qmax = 65 Вт - холодопроизводительность при токе I=Imax и разности температур dT=0.

Для охлаждения фотодиода использовался двухкаскадный термоэлектрический модуль ТВ-2-(127-127)-1,15, параметры которого:

- dTmax = 84 К;
- Imax = 5.8 А;
- Umax = 15.4 В;
- Qmax = 34 Вт;

Но эксперименты показали, что не удается полностью отвести тепло, выделяющееся на модулях при максимальных режимах. Это приводит к перегреву модулей и повышению температуры. Экспериментально полученные оптимальные значения токов и напряжений для обеспечения низких температур таковы: FROST-74 (I=2.4A, U=7B), ТВ-2-(127-127)-1,15 (I=4.2A, U=11B). Зависимость температуры фотодиода от тока через модуль ТВ-2-(127-127)-1,15 при постоянной мощности на модулях FROST-74

представлена на графике (рис.14). При оптимальных значениях была достигнута температура –58 °С.

Всего было использовано 8 модулей FROST-74 и один модуль ТВ-2-(127-127)-1,15.

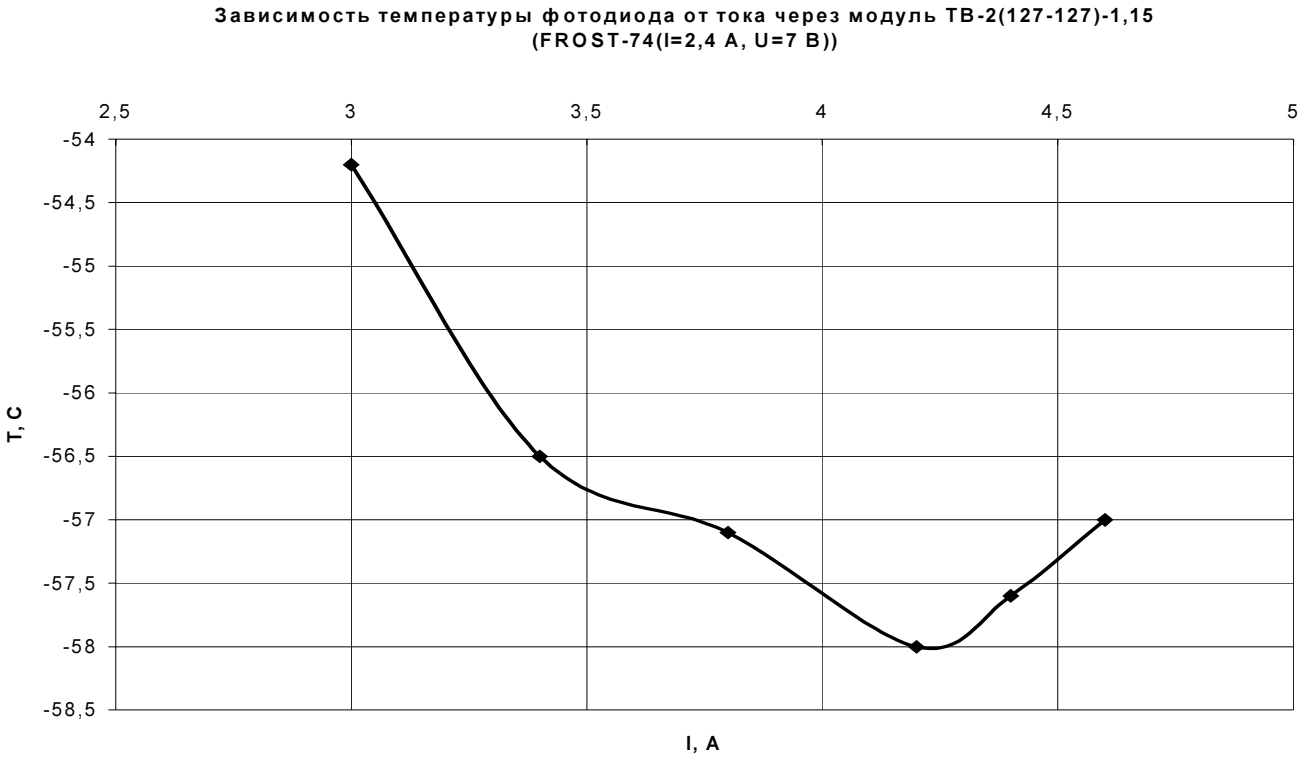


Рис.14

3.3 Измеритель температуры

Для определения температуры внутри холодильника использовался полупроводниковый диод КД521, через который протекал постоянный ток в 1 мА. Он был помещен внутрь металлической пластины (где находится фотодиод). Предварительно были проведены измерения температурной характеристики этого диода. Калибровка проводились с использованием платинового резистора, который был помещен внутрь теплоизолированной системы рядом с диодом. Градуировочная прямая диода показана на рис.15.

Измеритель состоит из полупроводникового диода КД521 и схемы усиления. Такая схема необходима, так как напряжение на диоде изменяется незначительно (так в рабочем диапазоне +20…-30 °С он меняется на 0.15 В).

На выходе измерителя мы получаем определенную характеристику зависимости напряжения от температуры (рис.16). Для удобства был выбран наклон 100 мВ/^{o}C и 0 ^{o}C соответствует напряжение 0 В. Это облегчает создание регулятора и удобно для визуального контроля температуры.

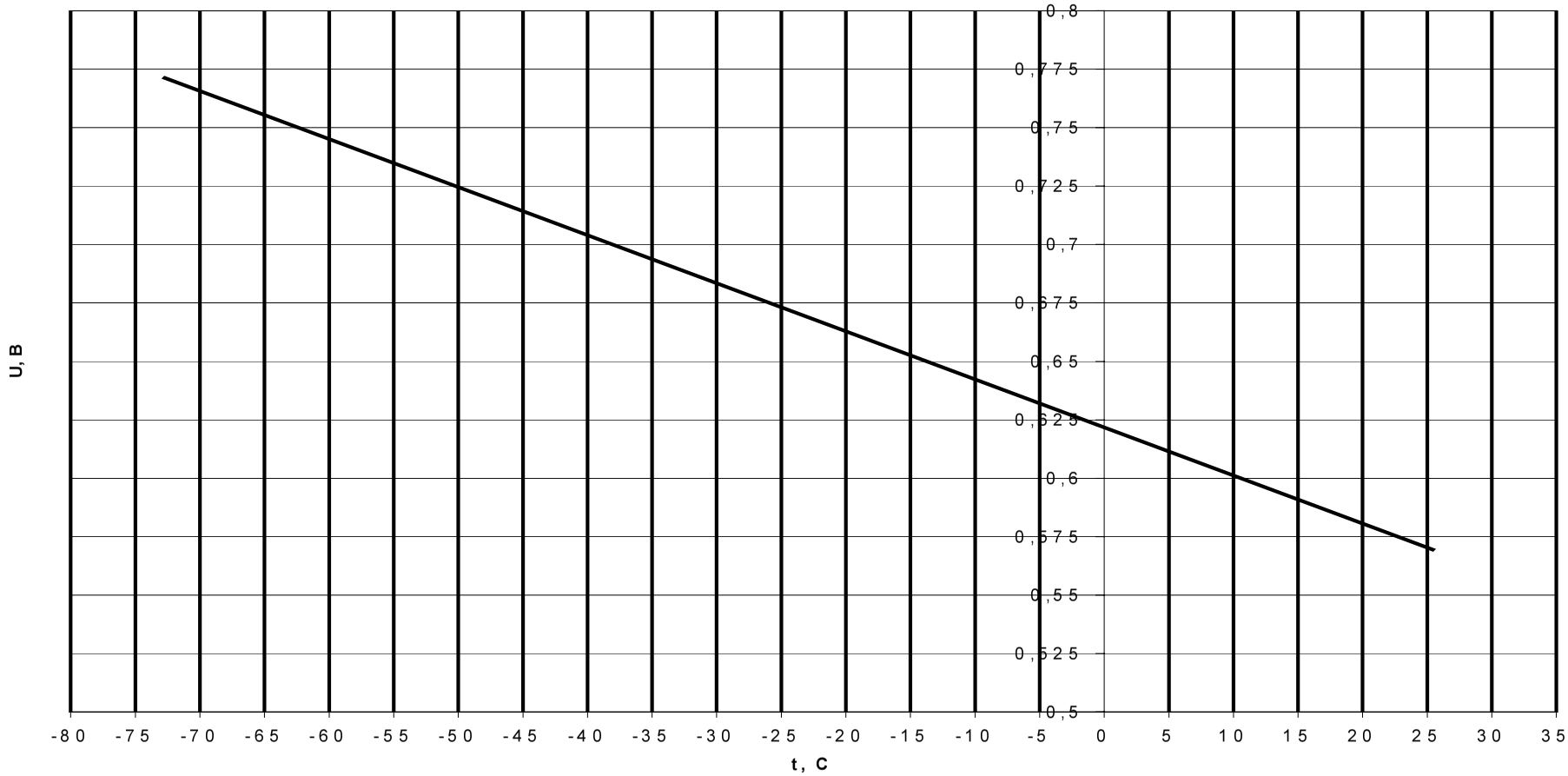


Рис.15 Калибровка диода

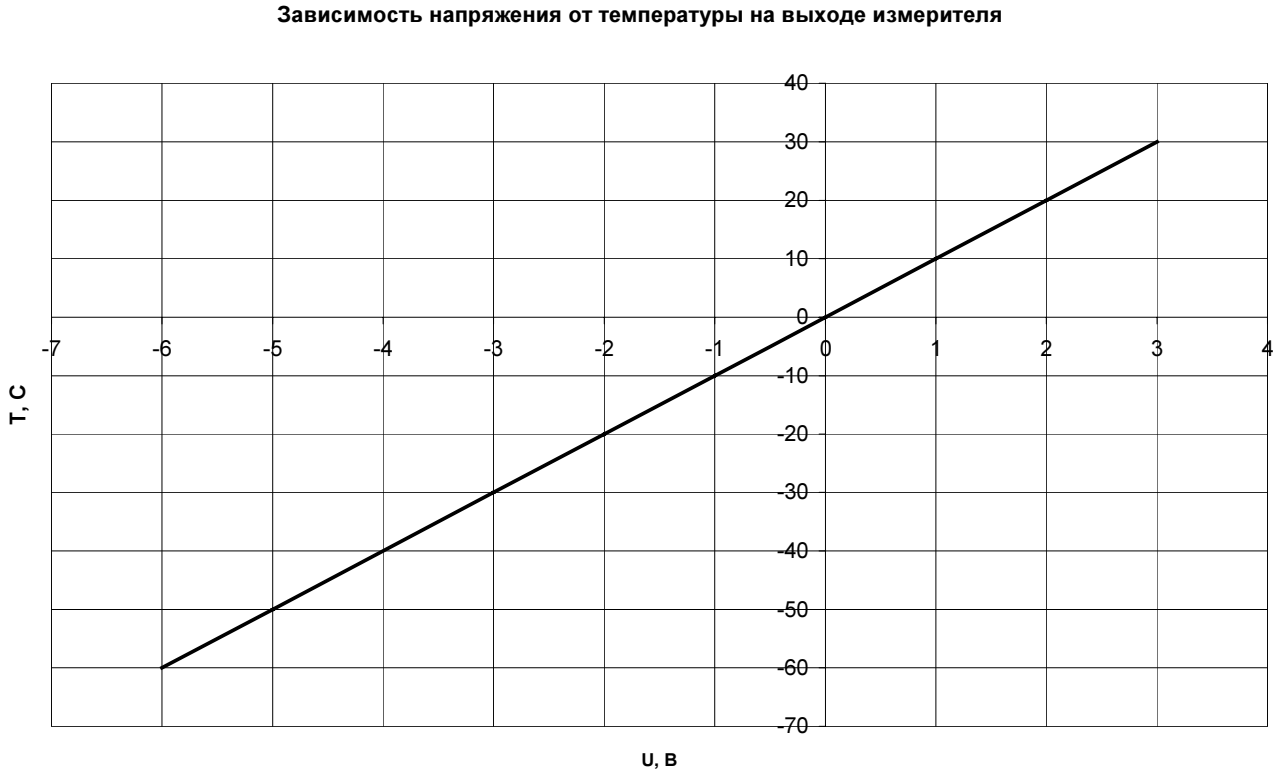


Рис.16

Принципиальная схема измерителя температуры приведена на рис.17.

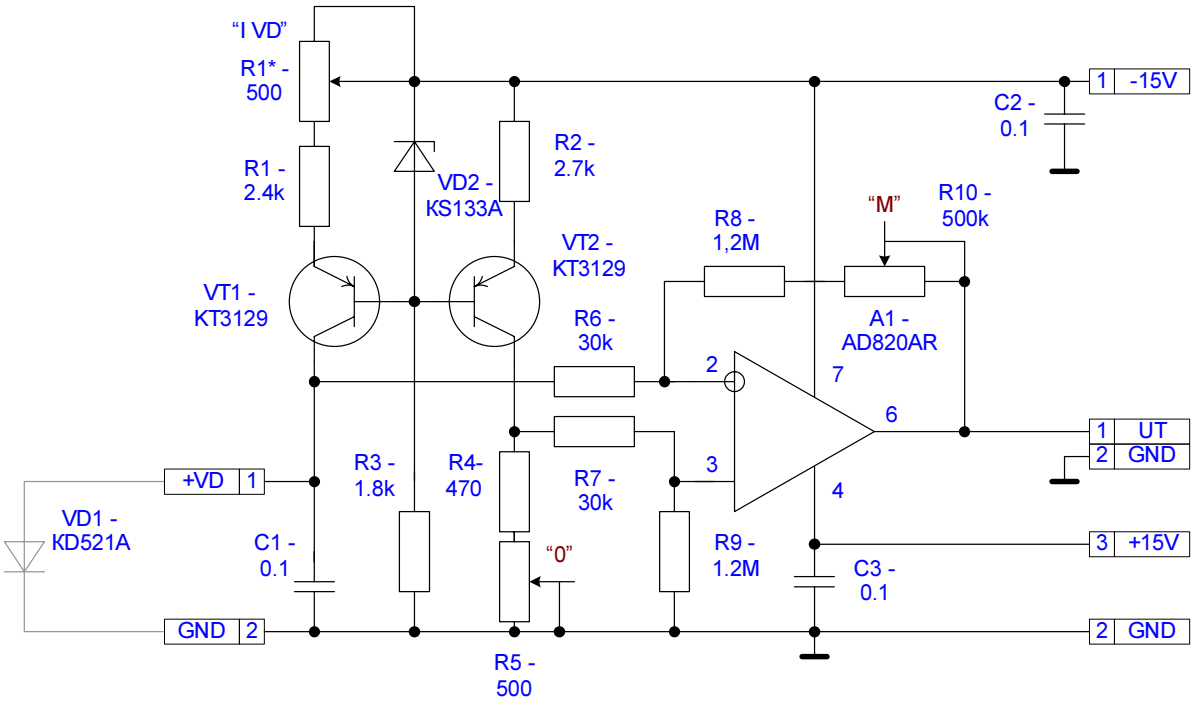


Рис. 17 Принципиальная схема измерителя температуры

4. Система автоматического регулирования температуры

4.1 Построение САР

Учитывая то, что нам необходимо поддерживать постоянное значение температуры внутри холодильника была реализована *стабилизирующая* система регулирования. И как уже было сказано выше, применительно к поставленной задаче нас будут интересовать *непрерывные линейные* САР.

Первоначально в системе был использован пропорциональный или П-регулятор. Но эксперименты показали, что точность поддержания им температуры оказалась неудовлетворительной. Недостаток П-регулятора вытекает непосредственно из принципа его функционирования. Этот регулятор представляет собой усилитель с большим коэффициентом усиления, на вход которого поступает сигнал рассогласования – разница между текущим значением регулируемой величины и заданным ее значением, - а выходной сигнал управляет объектом регулирования (в нашем случае меняется ток, протекающий через элемент Пельтье) (рис. 18). Нам необходимо, чтобы сигнал рассогласования был равен нулю, но в этом случае выходной сигнал тоже будет равен нулю. То есть, как только регулируемая величина достигнет заданного значения, охлаждение прекратится, объект начнет нагреваться, и это продолжится до тех пор, пока сигнал рассогласования не достигнет заданного значения, и все повторится заново. Такая система называется статической [32].

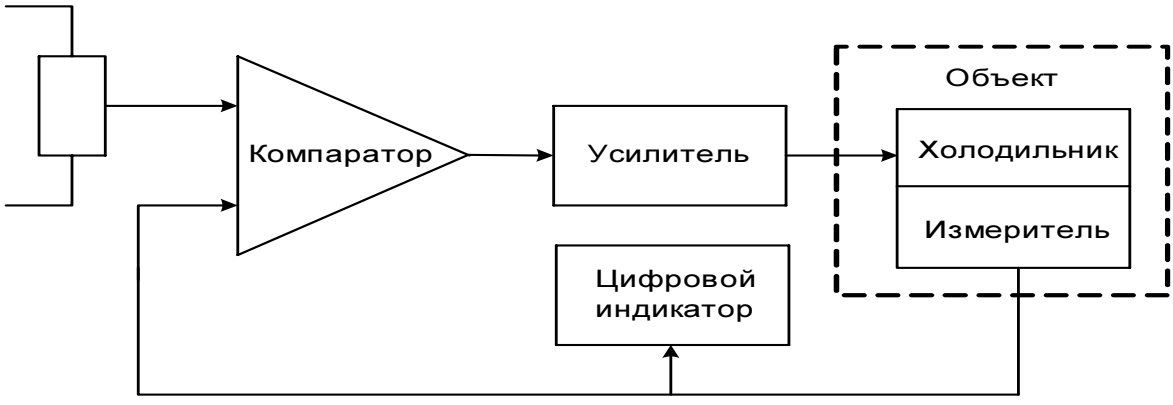


Рис.18 Схема с П-регулятором

Учитывая вышесказанное, было принято решение построить астатическую систему. Так как значение температуры будет изменяться редко, то нам будет достаточно применения астатической системы первого порядка. Для этой цели подходит пропорционально интегрирующий или ПИ-регулятор (рис. 19). Такой вариант предусматривает сложение сигналов рассогласования от усилителя и интегратора. Выходной сигнал представляет собой усиленную в определенное количество раз сумму сигнала рассогласования и интеграла от него. В итоге, даже при очень небольшом отклонении регулируемой величины от заданного значения, когда это рассогласование еще очень мало для того, чтобы заметно воздействовать на элемент Пельтье, оно, тем не менее, накапливается на конденсаторе интегратора до такой величины, которой хватит для ликвидации этого отклонения. Таким образом, благодаря интегрирующему звену в ПИ-регуляторе регулируемый параметр принципиально должен быть равен значению, выставленному на задающем устройстве, и малейшие его отклонения вверх или вниз, накапливаясь в интегрирующем звене, снова возвращают его к заданному значению.

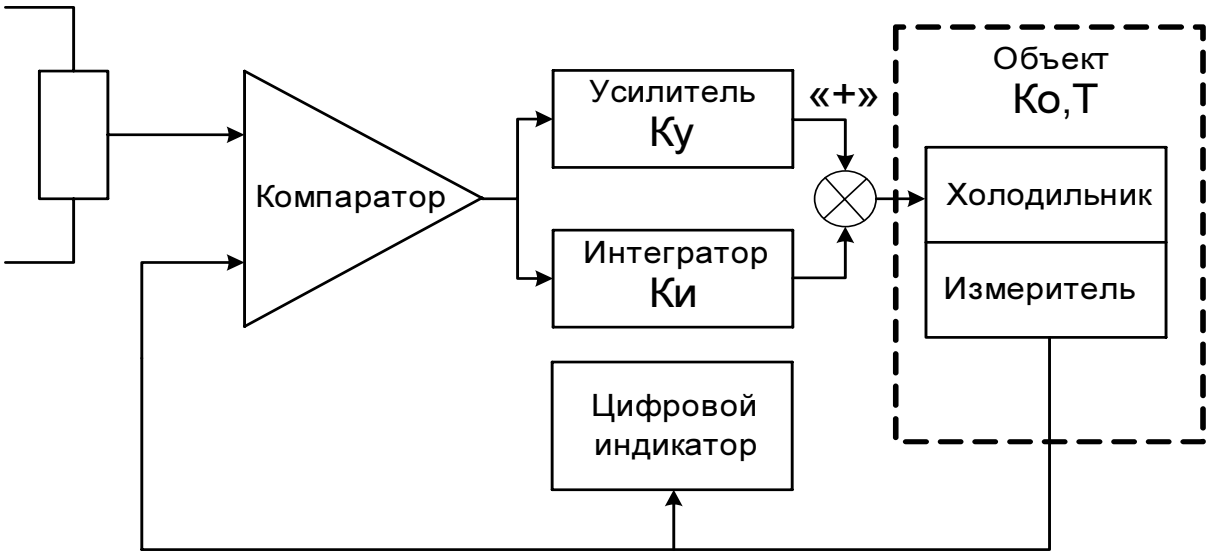


Рис.19 Схема с ПИ-регулятором

Для удобства составим блок-схему САР с использованием типовых звеньев: пропорциональное (усилитель с коэффициентом усиления $К_у$), интегрирующее (интегратор с коэффициентом передачи $К_и$ (либо постоянная интегрирования $Т_и=1/К_и$)), апериодическое (объект с коэффициентом передачи $К_о$ и постоянной времени Т). Апериодическое звено отражает инерционность объекта регулирования. Здесь необходимо заметить, что в понятие «объект» входит непосредственно холодильник, датчик и плата измерителя температуры, а также мощный выходной усилитель регулятора.

Рассмотрим уравнения звеньев и их передаточные функции:

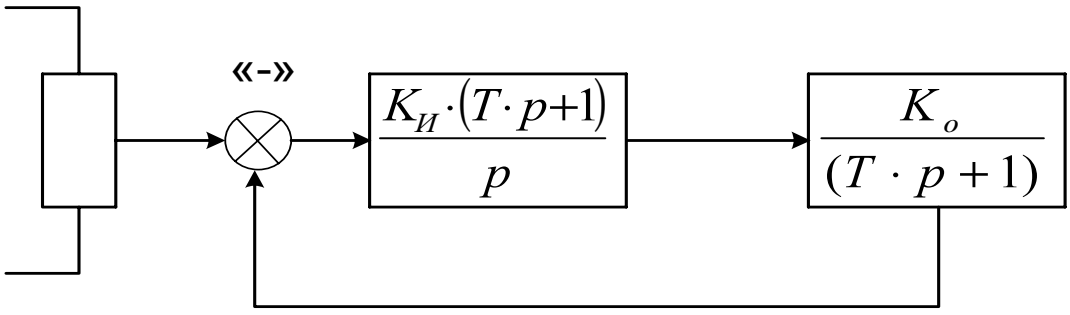
- усилитель $X_{вых} = K_y \cdot X_{вх}$, K_y ,
- интегратор $X_{вых} = K_И \int_0^t X_{вх} dt$, $K_И / p$,
- объект $T \cdot \frac{dX_{вых}}{dt} + X_{вых} = K_o \cdot X_{вх}$, $K_o / (T \cdot p + 1)$.

Учитывая необходимость получения нулевой ошибки регулирования, регулятор и объект, соединенные последовательно, должны представлять собой интегратор (рис.20). Отсюда мы можем получить передаточную функцию регулятора

$$\frac{K_И \cdot (T \cdot p + 1)}{p} , \text{ где } K_И = K_y / T .$$

Передаточная функция разомкнутой системы равна

$$W(p) = \frac{K_И \cdot (T \cdot p + 1)}{p} \cdot \frac{K_o}{(T \cdot p + 1)} = \frac{K_И \cdot K_o}{p}.$$



$$W(p) = (W_y(p) + W_И(p)) \cdot W_o(p) = \frac{K_И \cdot (T \cdot p + 1)}{p} \cdot \frac{K_o}{(T \cdot p + 1)} = \frac{K_И \cdot K_o}{p}$$

Рис. 20

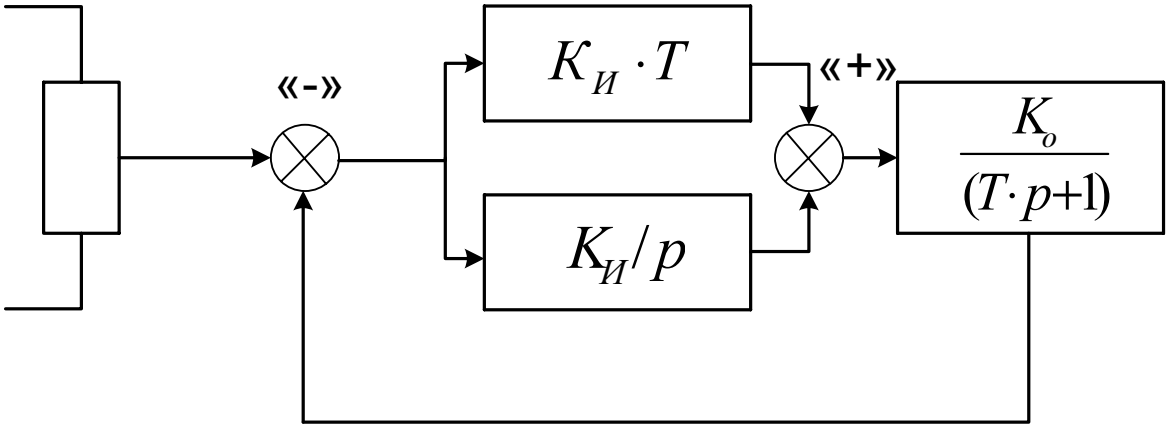
Передаточную функцию регулятора можно получить с помощью параллельного соединения пропорционального и интегрирующего звеньев

$$W_1(p) = \frac{K_И}{p} + K_y = \frac{K_И}{p} \cdot (T \cdot p + 1), \text{ где } T = \frac{K_y}{K_И} .$$

Окончательный вариант блок-схемы САР представлен на рис.21.

Основная передаточная функция замкнутой системы

$$\Phi(p) = \frac{X_{вых}(p)}{X_{вх}(p)} = \frac{W(p)}{1 + W(p)} = \frac{1}{\frac{1}{K_И \cdot K_o} \cdot p + 1} .$$



$$K_y = T \cdot K_И$$

Рис. 21

Характеристическое уравнение системы

$$\frac{1}{K_И \cdot K_o} \cdot p + 1 = 0.$$

Корень этого уравнения является вещественным и отрицательным, поэтому система устойчива. Причем такая система удовлетворяет критериям устойчивости Рауса и Гурвица.

4.2 Схема САР

На рис.22 приведена принципиальная схема регулятора температуры. На операционном усилителе (ОУ) А1 собрана схема дифференциального усилителя.

На входы А1 одновременно поступают напряжения от измерителя температуры и от ручки регулировки температуры (для этого используется потенциометр). Коэффициент усиления первого каскада выбирается из компромиссных соображений (в данном случае он равен единице). С одной стороны, его увеличение снижает чувствительность регулятора к смещениям и сдвигам во втором и третьем каскадах, и с этой точки зрения оно полезно. Но с другой стороны, его увеличение в определенное количество раз приводит к уменьшению во столько же раз постоянной времени интегратора $t_{инт}$. В самом деле, усиленный сигнал зарядит емкость интегратора до выбранного значения быстрее, чем не усиленный. А это приводит к необходимости использования в интеграторе резисторов и конденсаторов с большими номиналами. С выхода первого каскада сигнал рассогласования подается на интегратор и усилитель.

Интегратор выполнен на основе ОУ А2.2. Его постоянная времени

$$t_{инт} = R11 \cdot C1.$$

На основе ОУ А2.1 выполнен усилитель с коэффициентом усиления 2. К тому же на выходах интегратора и усилителя установлены подстроечные резисторы R13 и R15. С их помощью в процессе эксперимента производилась точная настройка $K_и$ и $K_у$.

Сигналы с выходов интегратора и усилителя подаются на третий каскад, выполненный на ОУ А3.1 и А3.2 по схеме дифференциальных усилителей. Там сигналы складываются и с разными знаками поступают на пары выходных транзисторов VT1-VT2 и VT3-VT4, которые конструктивно размещены на отдельном радиаторе. Транзисторы регулируют ток, протекающий через модуль Пельтье ТВ-2-(127-127)-1,15.

В приложении 3 приведена блок-схема электрического соединения плат и модулей устройства охлаждения в корпусе, а также схема питания водяного насоса и соединение элементов Пельтье для охлаждения воды.

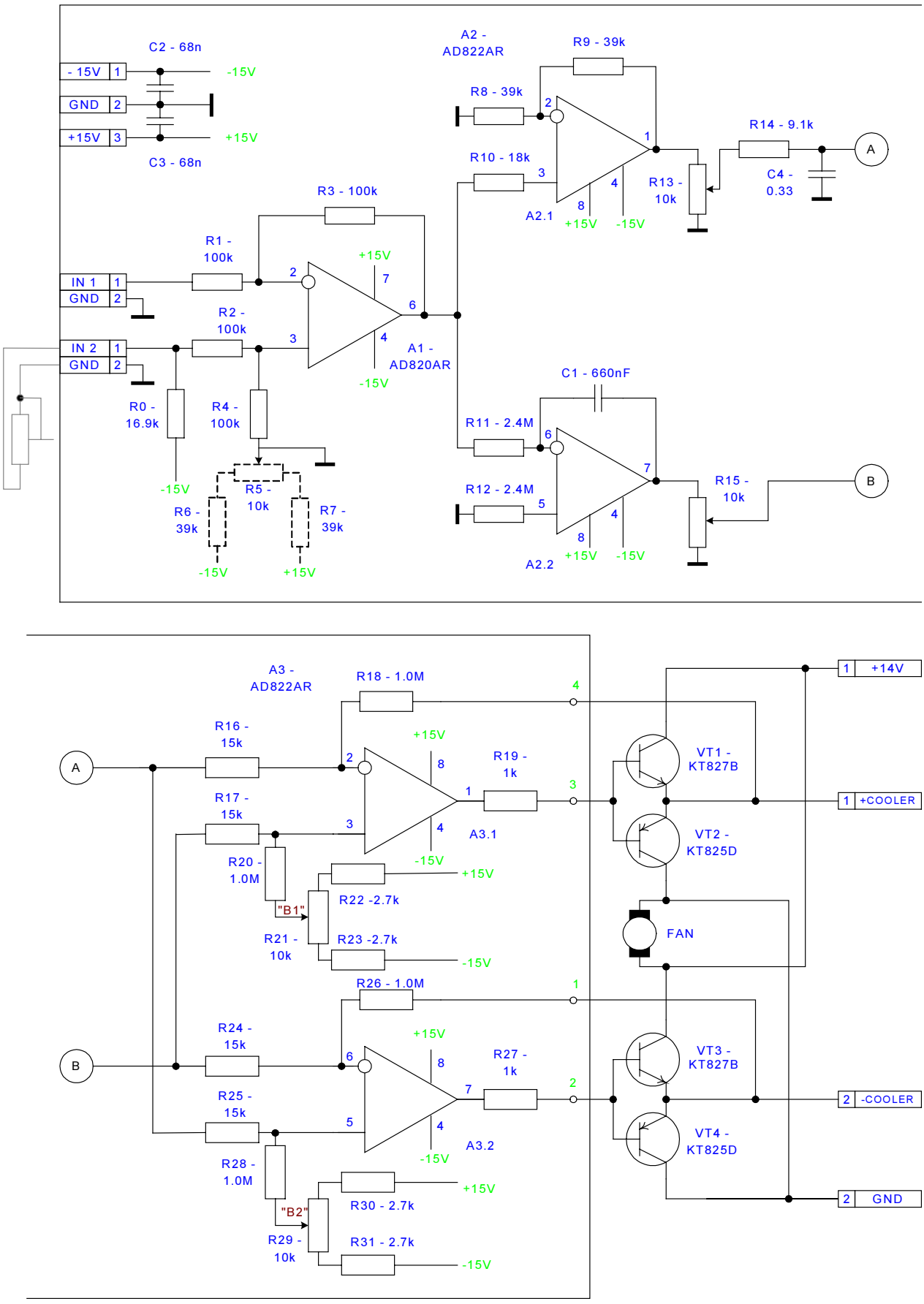


Рис.22 Принципиальная схема регулятора температуры

4.3 Выбор коэффициентов $К_и$ и $К_у$

Сначала были экспериментально определены коэффициент передачи K_o (рис.23) и постоянная времени T_o объекта.

$$K_o = \frac{dU_{ВЫХ}}{dU_{ВХ}} = \frac{5.14 - 3.03}{0.111 - 0.055} = 37.68$$

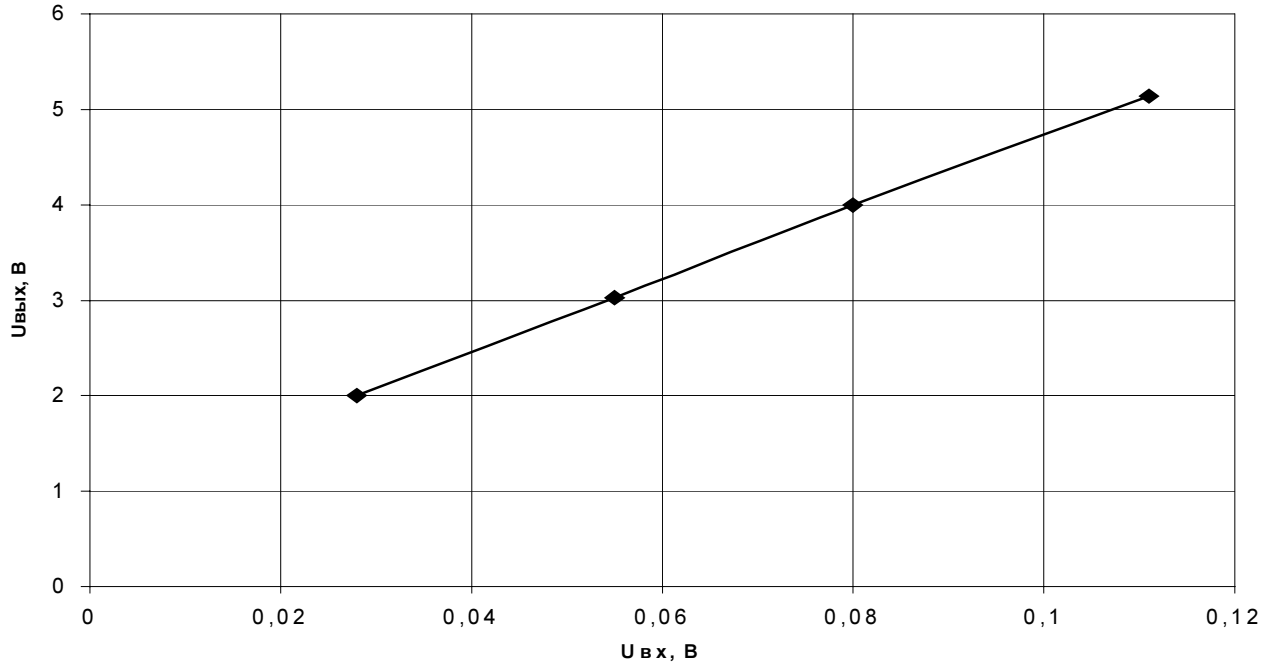


Рис.23 коэффициент передачи объекта K_o

На рис.24 представлена переходная характеристика объекта, снятая при помощи персонального компьютера и цифрового осциллографа. По этой характеристике была определена постоянная времени объекта, которая составила T_o = 160 с.

Параметры интегратора и усилителя ($T_И$ *и* K_y) определялись расчетным путем, исходя из значений коэффициента передачи K_o и постоянной времени T_o объекта ($T_u = 1/K_u$, $K_y = T \cdot K_u$, при $T=T_o$).

При $K_y = 1.1$ получим $K_u = K_y/T = 1.1/160 = 0.0069$.

Необходимое значение K_y устанавливалось при помощи подстроечного резистора R. Параметры интегратора были выбраны R=2.4 МОм, С=660 нФ ($t_{инт}$=1.59 с), и корректировались подстроечным резистором R.

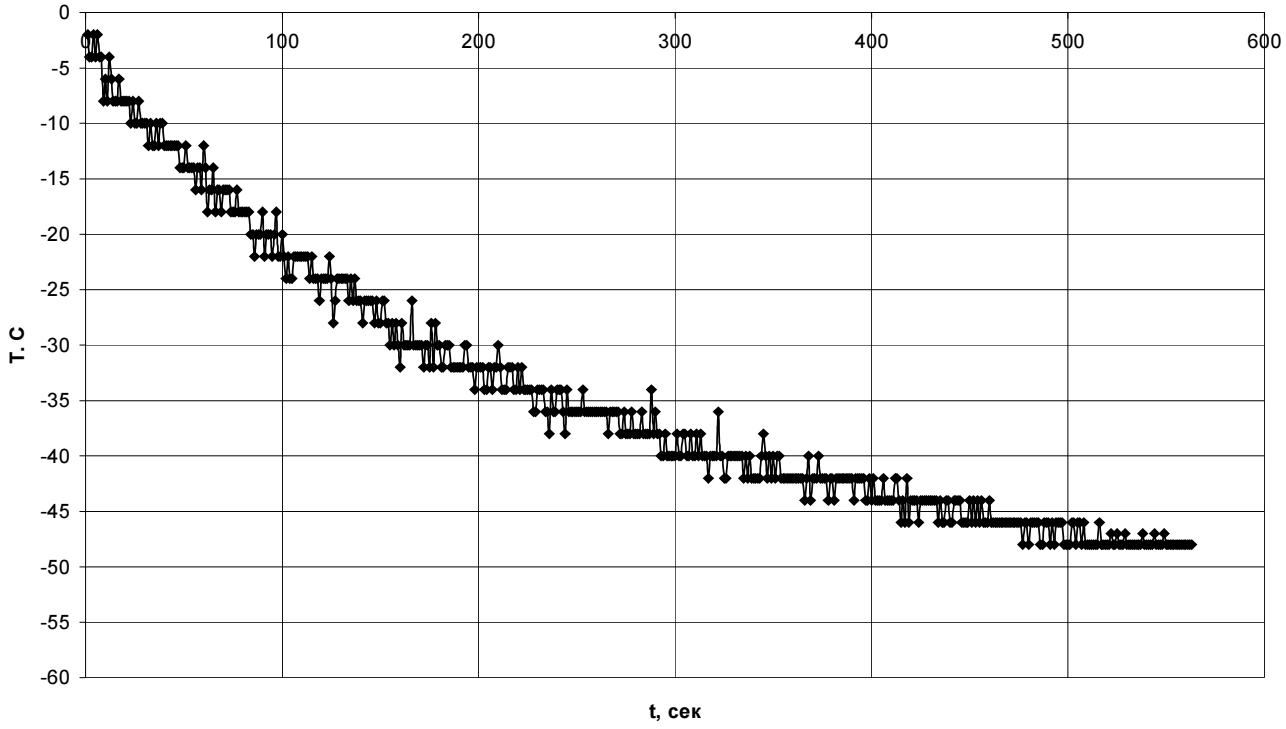


Рис.24 Переходная характеристика объекта

Регистрация данных во время эксперимента производилось при помощи аналого-цифрового преобразователя (АЦП), подключенного к персональному компьютеру. Далее они обрабатывались и строились зависимости переходных процессов от времени. По результатам анализа графиков корректировались значения T и K_y. Таким образом оказалось, что теоретически найденные значения T и K_y отличаются от тех, которые были установлены в результате экспериментов

$K_y = 1.1$, $K_u = 0.0184$, и $T = K_y/K_u = 60$ с.

Это можно объяснить тем, что теоретические расчеты предназначены для построения системы без перерегулирования. В построенной же нами системе коэффициент передачи интегратора K_u больше, что и вызывает перерегулирование. Плюсом такой системы является меньшее время установления температуры, что ниже будет подтверждено графиками.

К тому же стоит отметить, что скорости охлаждения и нагрева объекта различны. Нагрев происходит быстрее, чем охлаждение. Это оказывает неблагоприятное воздействие на скорость процесса установления температуры. В особенности различия в скорости влияют на установление промежуточных значений температуры, таких как 0…-30 ^{o}C (рис.25,26).

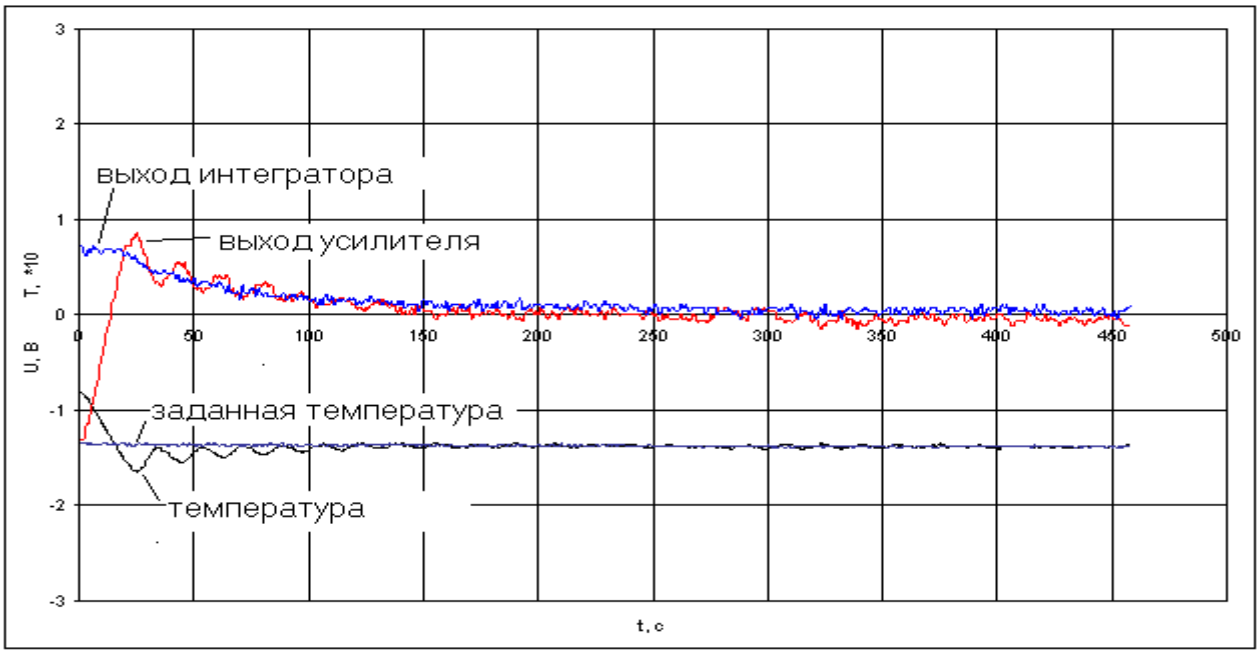


Рис.25

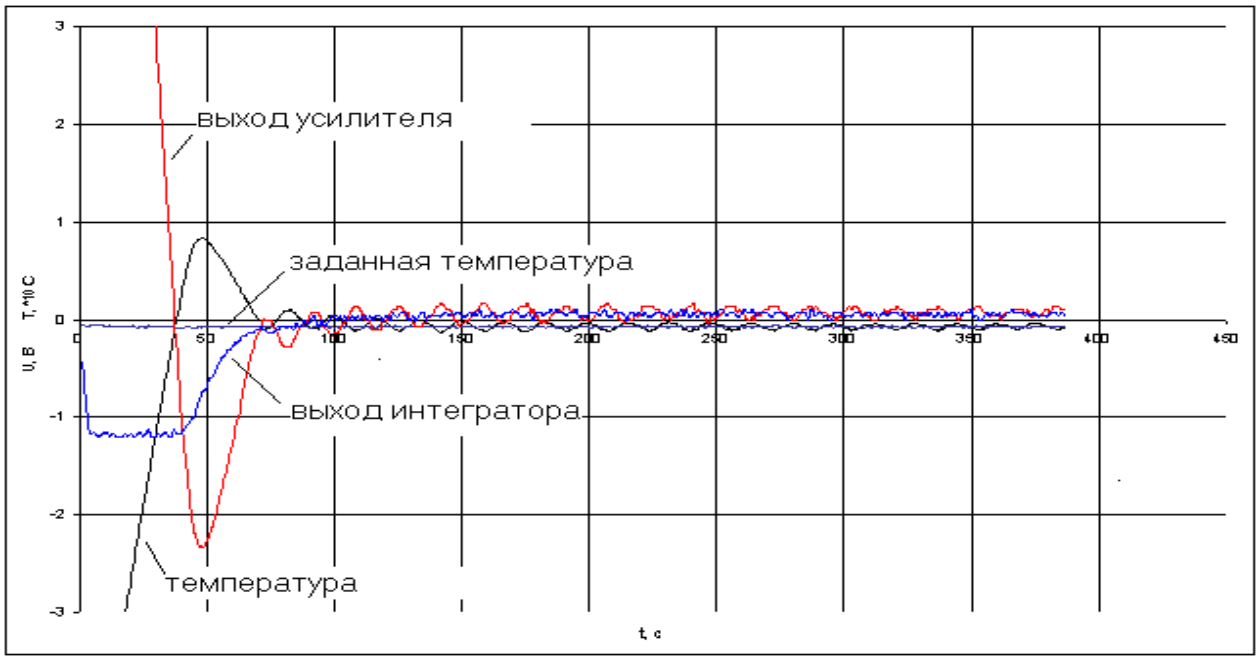


Рис.26

Установление температуры происходит с множеством переколебаний. Поэтому были проведены исследования переходных характеристик при изменении температуры. Результаты показали, что с помощью корректировки K_y и K_u это воздействие можно компенсировать и получить необходимую точность и время регулирования. Конечно, если далее усовершенствовать САР и делать ее цифровой или сопряженной с персональным компьютером, то будет целесообразнее установить различные постоянные времени для нагрева и охлаждения. В нашем же случае необходимый результат достигается и без этого.

Теперь проверим полученную САР на устойчивость.

Передаточная функция разомкнутой системы равна

$$W(p) = \frac{K_И \cdot (T \cdot p + 1)}{p} \cdot \frac{K_o}{(T_o \cdot p + 1)}.$$

Основная передаточная функция замкнутой системы

$$Ф(p) = \frac{X_{вых}(p)}{X_{вх}(p)} = \frac{W(p)}{1 + W(p)} = \frac{K_o \cdot K_И \cdot (T \cdot p + 1)}{T_o \cdot p^2 + (1 + K_o \cdot K_И \cdot T) \cdot p + K_o \cdot K_И}.$$

Характеристическое уравнение

$$T_o \cdot p^2 + (1 + K_o \cdot K_И \cdot T) \cdot p + K_o \cdot K_И = 0.$$

Найдем корни этого уравнения.

$$p_{1,2} = \frac{-1 - K_o \cdot K_y \pm \sqrt{K_o{}^2 \cdot K_y{}^2 + 2 \cdot K_o \cdot K_y + 1 - 4 \cdot T_o \cdot K_o \cdot K_И}}{2 \cdot T}$$

Подставив значения $К_у = 1.1$, $K_u = 0.0184,$ получим

$p_1 = -0.19$, $p_2 = -0.08$.

Корни вещественны и отрицательны, что говорит об устойчивости системы.

В итоге были выбраны оптимальные значения коэффициентов, при которых и точность, и время установления температуры были наилучшими. Создание такой системы позволило экспериментально изучить влияние параметров усилителя и интегратора на точность поддержания температуры и время ее установления, а также определить, как на них влияет наличие или

отсутствие перерегулирования. Так при большом коэффициенте передачи интегратора мы получим систему с перерегулированием и большим числом переколебаний (рис.27). При низком – систему без переколебаний (рис.28). В обоих случаях время установления температуры было велико. Как показали эксперименты, наилучшим оказался случай с одним переколебанием (рис.29). Ему соответствуют параметры САР $K_y = 1.1$, $K_u = 0.0184$, и $T = K_y/K_u = 60$ с. Он и был выбран в качестве окончательного варианта. Причем важную роль играет величина постоянной интегрирования интегратора T_u и, соответственно $T = K_y/K_u$. При $T_u << T_o$ (где T_o – постоянная времени объекта) значение температуры колеблется (рис.30), что вызвано слишком быстрым накоплением ошибки в интеграторе. Такой переходной процесс происходит при установленной емкости С=10 нФ, $K_y = 1.1$, $K_u = 1.24$ ($T_u = 0.8$ с, $T = 0.9$ с). При $T_u >> T_o$ система ведет себя подобно П-регулятору и существует установившаяся ошибка (рис.31). Это вызвано слишком маленьким значением K_u. Так, на приведенном графике С=50 мкФ, $K_y = 1.1$, $K_u = 0.00024$ ($T_u = 4166$ с, $T = 4509$ с). Ошибка составляет 0.5 °С.

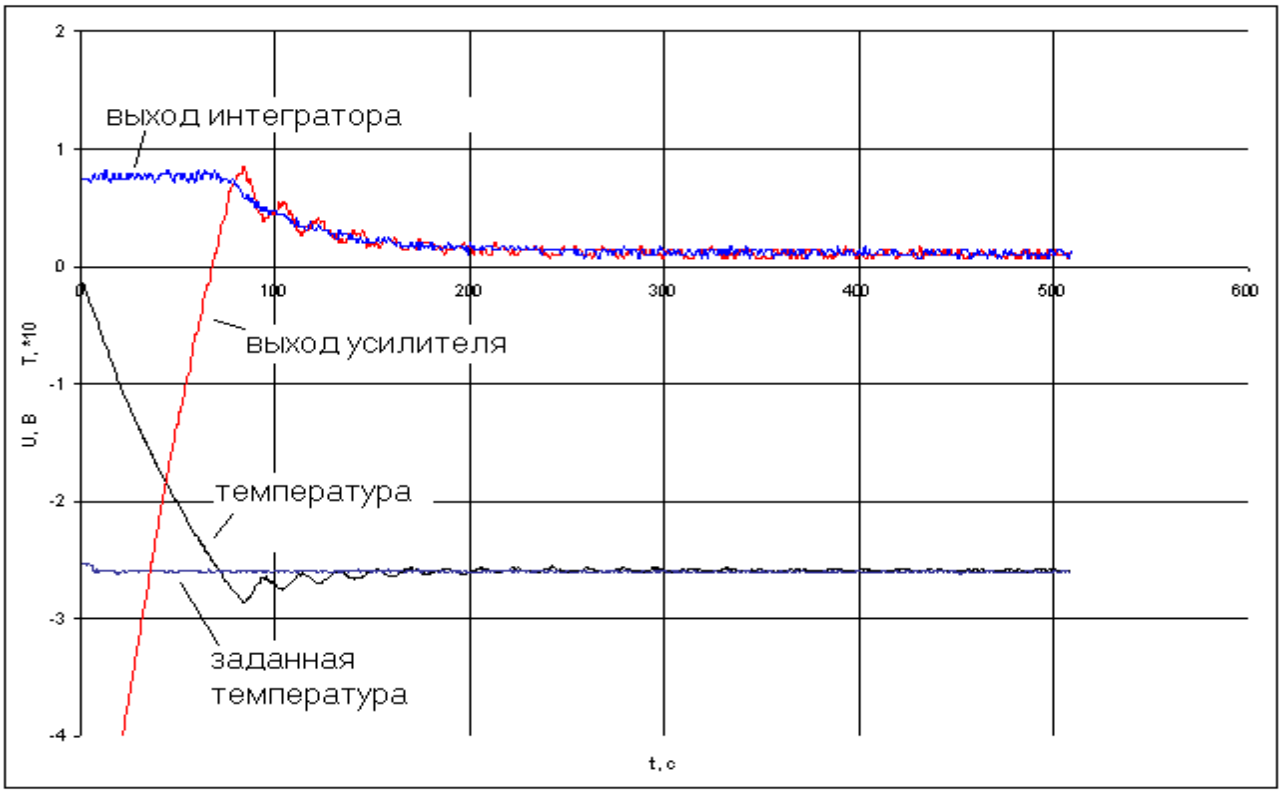


Рис.27

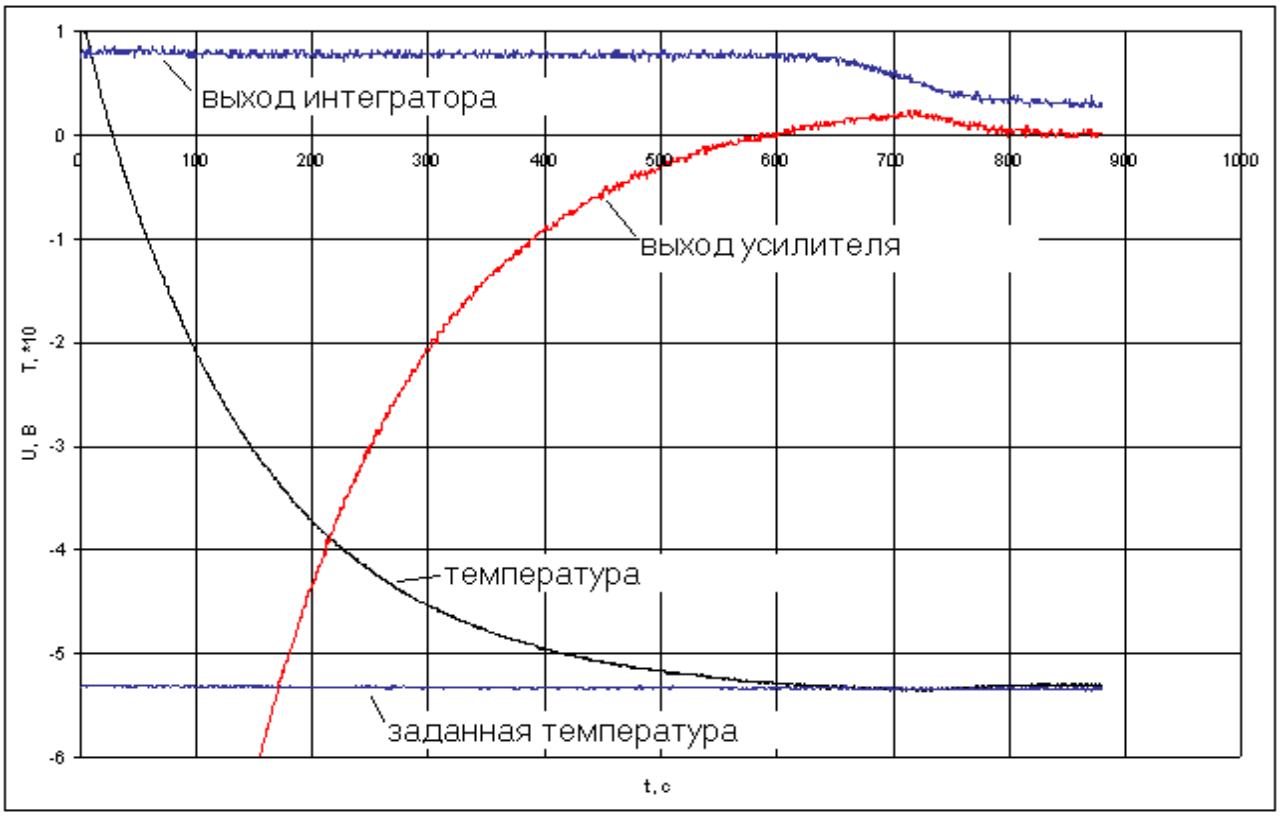

выход интегратора
выход усилителя
температура
заданная температура
U, В T, *10
t, c

Рис.28

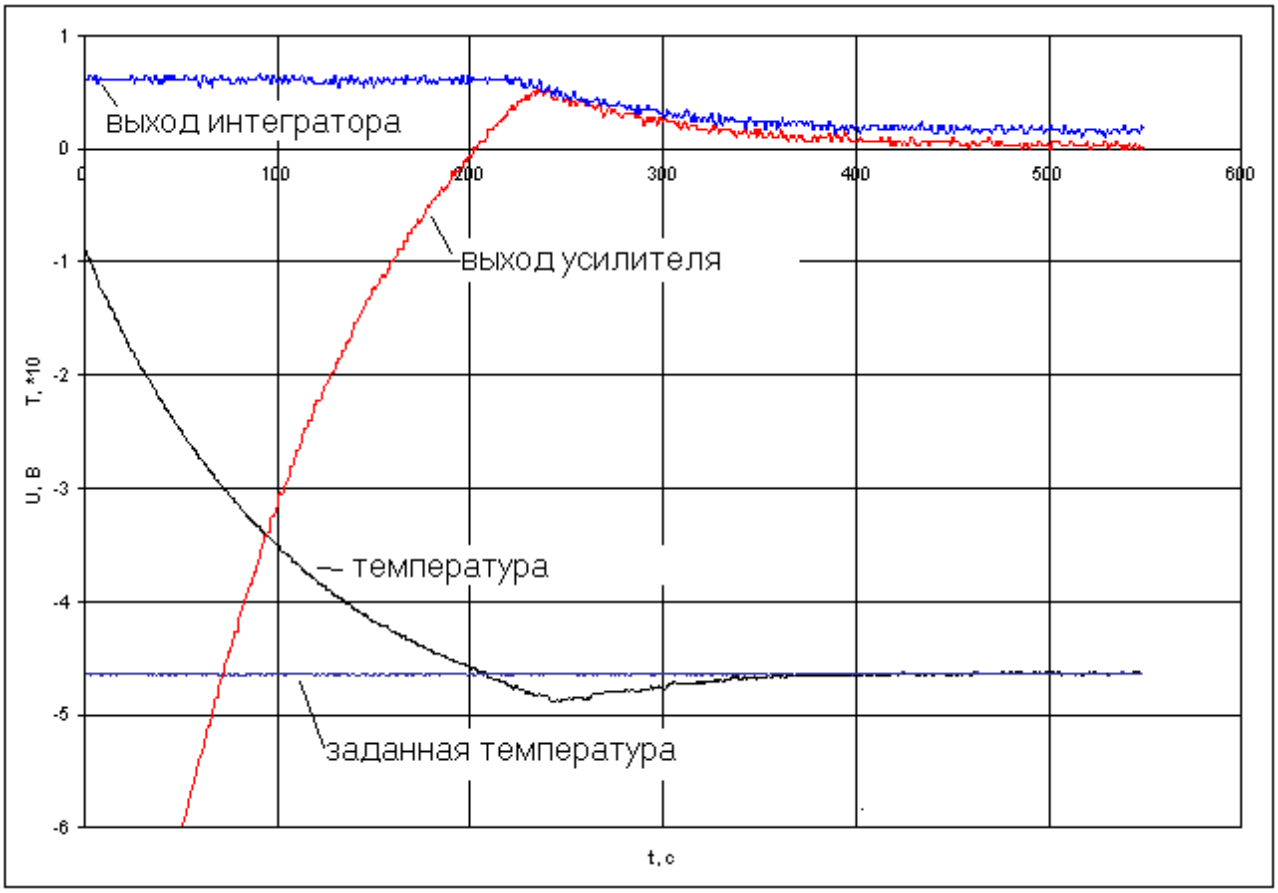

выход интегратора
выход усилителя
температура
заданная температура
U, В T, *10
t, c

Рис.29

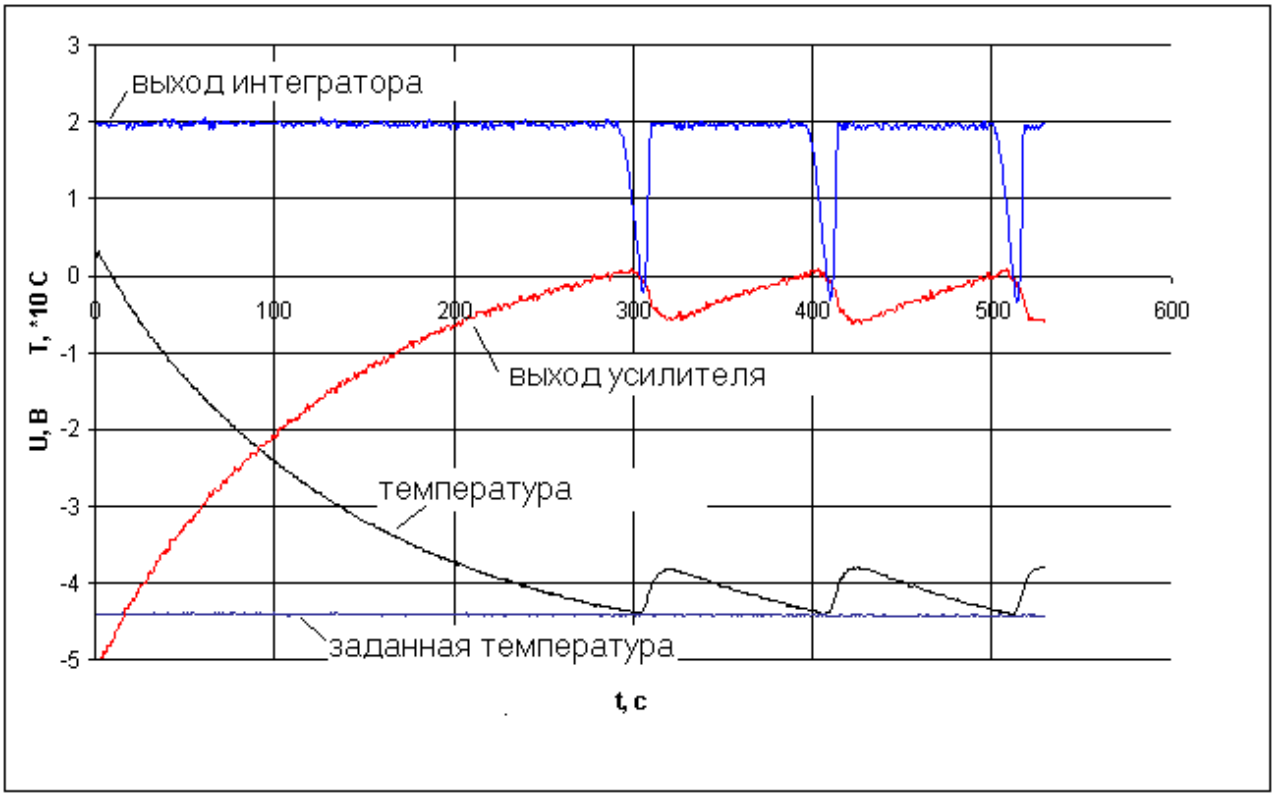

выход интегратора
выход усилителя
температура
заданная температура
U, В T, *10 C
t, c
3
2
1
0
-1
-2
-3
-4
-5
0
100
200
300
400
500
600

Рис.30

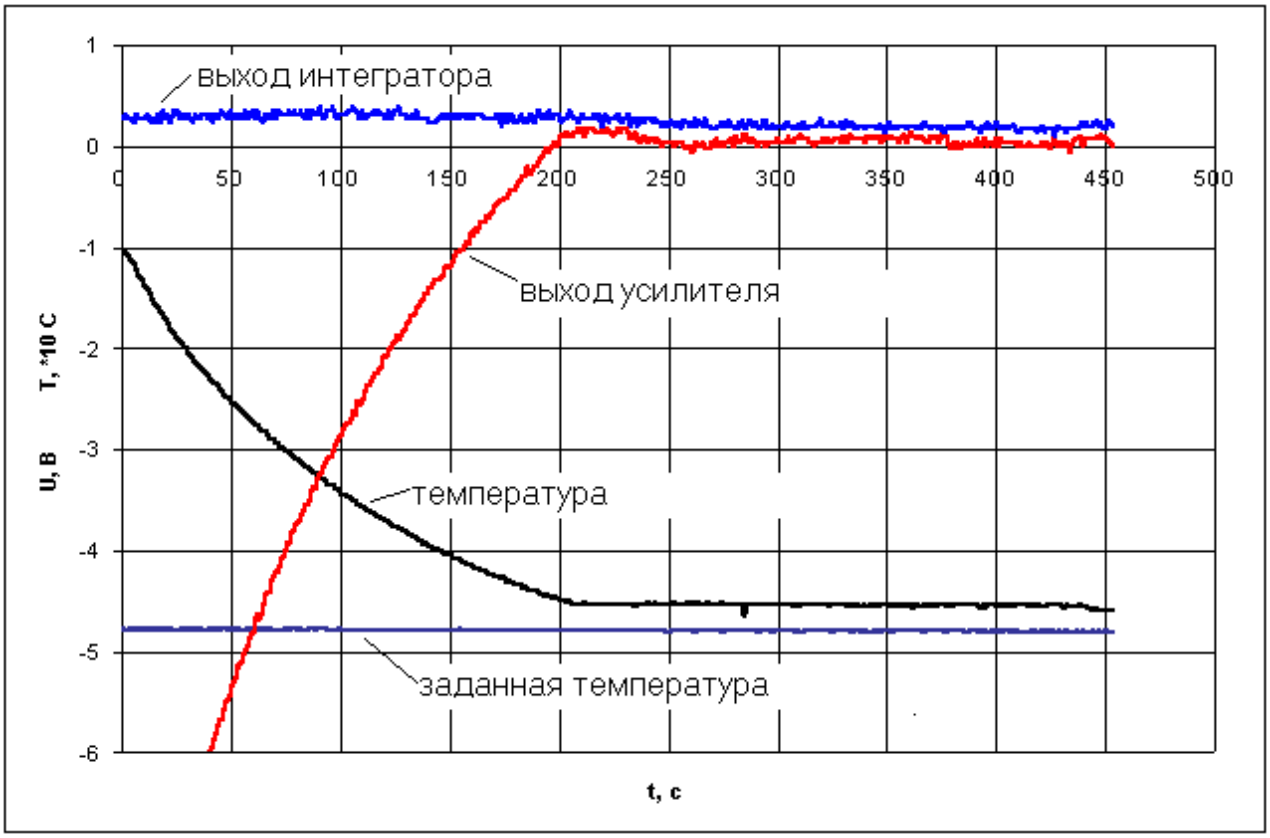

выход интегратора
выход усилителя
температура
заданная температура
U, В T, *10 C
t, c
1
0
-1
-2
-3
-4
-5
-6
0
50
100
150
200
250
300
350
400
450
500

Рис.31

На графиках кроме установившейся и заданной температуры приведены зависимости напряжений на выходах усилителя и интегратора системы автоматического регулирования.

Эти дополнительные зависимости использовались в ходе поиска оптимальных значений K_y и K_u, так как наглядно отражали процессы, происходящие в САР. Так, по скорости изменения значения сигнала на выходе интегратора можно судить о соответствии величины постоянной интегрирования процессу регулирования.

В приложении 4 приведена фотография прибора, а в приложении 5 – его внешний вид с открытой крышкой и вид передней и задней панелей.

5. QKD Experimental Set-up

In our laboratory at NTNU we utilize a phase coding based QKD set-up and BB84 protocol. Because, as it was said before, the polarization drift in QKD set-ups based on polarization coding makes them difficult to implement for the long distances.

This set-up is similar to the one, that was presented by Christopher Marand and Paul D. Townsend in their article "Quantum Key Distribution over distances as long as 30 km" in 1995 [28]. The set-up was built at our laboratory with the help of earlier students.

For a more detailed analysis it is better to explain the optical and electronic parts of the set-up separately [33].

5.1 Optical part of the set-up

The optical part of the QKD set-up is shown on Fig.32. It consists of a Mach-Zehnder interferometer, a laser and a single photon detector (SPD).

The light pulse is emitted by a 1300 nm semiconductor laser (Fujitsu FLD3F6CX, see Appendix 6). The QC experiment needs a single photon source. True single photon sources have been recently demonstrated, but not yet practical for commercial implementation [34, 35, 36]. Therefore an attenuated laser pulse was used. The output of this source has a probabilistic distribution based on the shape and the optical power in the pulse. Detailed description and calculations of the laser is included in [37].

The light pulse from the laser passes through a polarizer, then it is split by the variable ratio coupler and passes down the two separate arms of the interferometer. Here we have two pulses: one follows the short arm, the other follows the long one. In the long arm the pulse passes through Alice's phase modulator, which is used to add a phase shift of either $-3\pi/4$, $-\pi/4$, $\pi/4$ or $3\pi/4$. This arm also has a variable delay line for adjusting the differences between the lengths of the interferometer's arms. Then Alice's polarization combiner multiplexes the pulses

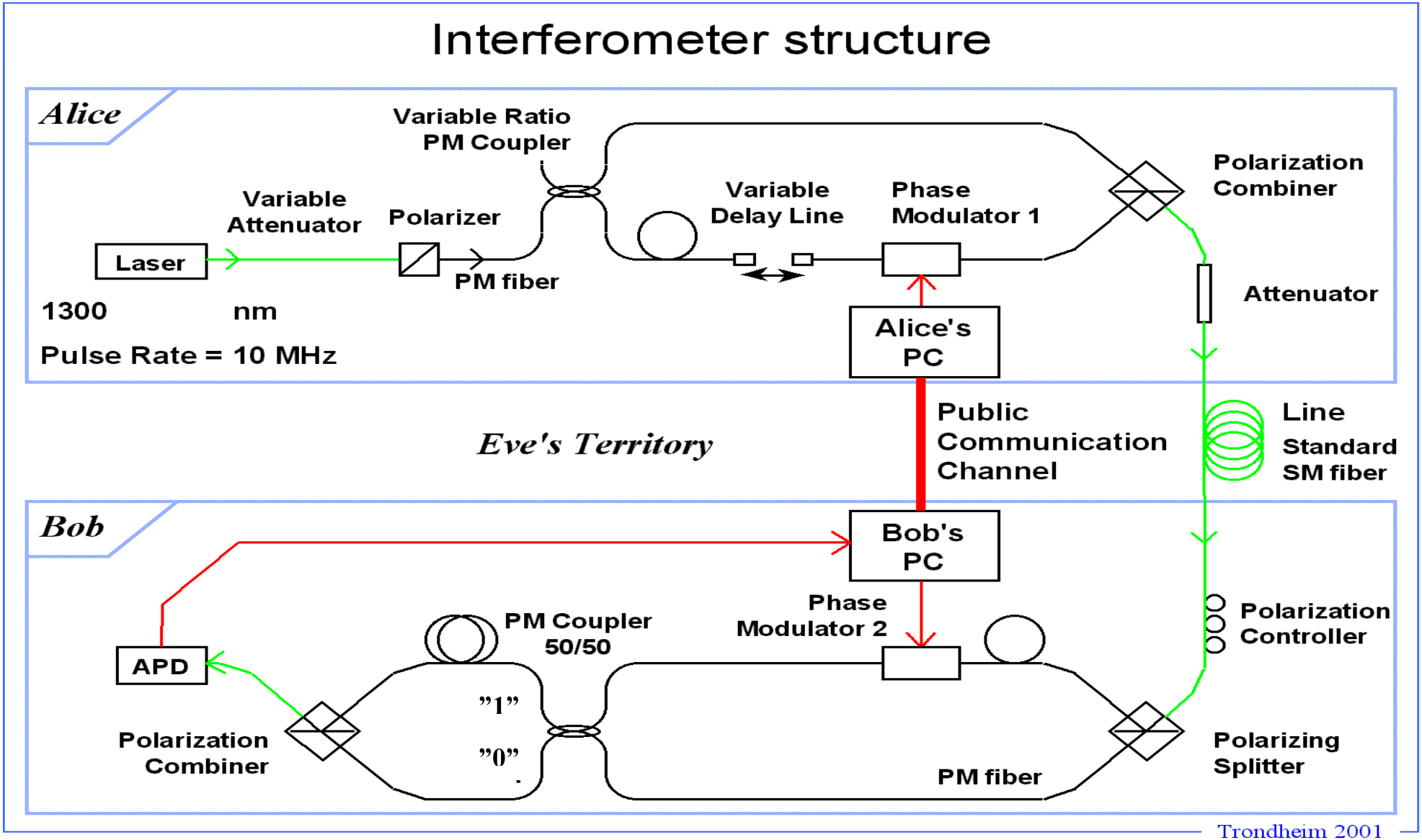


Fig. 32. Optical part of the QKD set-up

into a single-mode fibre and they pass through the variable attenuator and the transmission line (in our case Alice's and Bob's set-ups are connected through 5 m of standard single-mode fibre). Before Bob's polarising splitter, our pulses pass through a polarization controller. It is used to compensate for static polarization transformation the pulses receive in the transmission line. The polarizing splitter splits pulses in a such way, that the pulse that chose the short arm in Alice's interferometer goes into the long arm in Bob's, and vice versa. Bob can either apply a phase shift of $-\pi/4$ or $\pi/4$ on his phase modulator. After that the pulses interfere on Bob's coupler. The outcome of interference depends on the differences between the phases of the pulses. As you can see, if the difference is 0, then we detect "0"; if the difference is π, then we detect "1". In Table 2 you can find all possible combinations of the phase shifts we used to transmit the key. The other phase differences produce inconclusive results (50/50%), which are rejected at sifting. "1" and "0" go to the different outputs of the coupler and are time-multiplexed at the same detector. To use one detector to detect them, we delay "1" and they reach the SPD at different intervals of time. So if we use laser pulses with 10 MHz repetition rate, we should increase the detector-gating rate two times (20 MHz).

On both Alice's and Bob's sides we use travelling wave phase modulators made of lithium niobate (Alenia Marconi-made at Alice's side and Uniphase-made at Bob's side). Alice's PM has half-wave voltage of 3.50 V, Bob's one has half-wave voltage of 8.20 V. Here we should also mention that before passing to Bob's PM voltage is inverted, because Alice's and Bob's PM have different polarity.

The SPD is a Soviet-made FD312L germanium avalanche photodiode (APD) (Appendix 7). To detect single photons the APD must have a low dark current and it needs to be cooled in liquid nitrogen (LN_2) at about 77K. The APD is operated in Geiger mode (GM). GM operation is one of the basics in QC when utilising an APD. It increases the detector efficiency significantly and makes it possible to use commercially available APD's. In GM the APD bias voltage is kept below the

breakdown voltage and it is raised above it only for a short time (so called gate pulse), when a photon is expected to arrive. Without the gate pulse no avalanche can appear in the APD, so it decreases the dark count rates. During the gate pulse the voltage on the APD rises above the breakdown level and we can detect the photon. The gate pulse must come to the APD at the same time as the photon is expected to arrive, so it must be carefully synchronized. To detect the photon with high probability we use a pulse width of about 1-2 ns. But we can't make it longer, because it increases the dark count rates. We have dark count probability of about 10^{-4} [33]. The details of the APD characteristics are described in [37, 38].

Alice		Bob		
Bit value	φ_A	φ_B	φ_A-φ_B	Bit value
0	$-\pi/4$	$-\pi/4$	0	0
0	$-\pi/4$	$\pi/4$	$-\pi/2$	?
1	$3\pi/4$	$-\pi/4$	π	1
1	$3\pi/4$	$\pi/4$	$\pi/2$	?
0	$\pi/4$	$-\pi/4$	$\pi/2$	?
0	$\pi/4$	$\pi/4$	0	0
1	$-3\pi/4$	$-\pi/4$	$-\pi/2$	?
1	$-3\pi/4$	$\pi/4$	π	1

This table is equal to the Table 1 except the correction factor in 2nd and 3rd columns, because it is more convenient for us to use symmetrical meanings of the phase shifting.

Table 2. Implementation of the BB84 four-states protocol in our set-up

As in Paul Townsend's set-up (Fig.8) [28] we utilize time and polarization division to separate the individual paths in a single long-transmission fibre. Although polarization division alone would be sufficient to separate the two components, the addition of time division means that the error rate in the system is less sensitive to small changes in output polarization from the transmission fibre. But in contrast to Townsend's set-up the arms of our interferometer are made of polarization-maintaining fibre (Fujikura Panda PM 1300nm), so we needn't extra polarization controllers in the arms. Fibres between the laser and Alice's polarizer,

between Bob's polarization combiner and detector, and also the transmission line are made of standard single-mode fibre. In contrast to Townsend's scheme, where he used an attenuator right after the laser, we use it on the output of Alice's polarization combiner. This trick gives us an advantage against eavesdropping, because using a large pulse attack allows the eavesdropper to avoid inducing transmission errors that disclose her presence to the legal users. With the large pulse attack, settings of transmitting and/or receiving apparatus are interrogated by external high power light pulse. If Eve launches a bright light pulse into the transmission line towards Alice's or Bob's set-up (in our case the attenuator protects Alice's part), some part of the pulse will be reflected back from different optical components inside the set-up, because any real components have a non-zero reflection coefficient. On its way, the pulse can pass internal modulators and be modulated one or more times. Measuring characteristics of the reflected pulses, Eve can make some conclusions on the modulator's settings and then at least know transmission or detection bases. Placing the attenuator at the output of Alice's set-up will mean for Eve a significant increase in the level of the laser power she needs [39].

The optical part of the set-up is situated in two separate boxes: Alice's part (Fig.33) and Bob's part (Fig.34). The whole picture of the set-up you can see on Fig.35 (while Alice's and Bob's set-ups are located side-by-side in the same lab in our experiments, in the real use they would be separated by tens of kilometres). Also we have a cryostat for APD cooling. The size of each box is approximately 420 x 420 x 150 mm. The main difficulty associated with the scheme we use is that the imbalance between the two arms of the interferometer must be kept stable within a fraction of the wavelength, during a key exchange, to maintain the correct phase relations [23]. This means that the temperature of the boxes must be stabilized. Our boxes are filled in with custom-cut pieces of foam insulation. But it is not enough and we need an active system to compensate the phase drift in the interferometer. A special program [33] makes a phase adjustment (calculates appropriate voltage, which we apply to Bob's PM as the bias voltage for

subsequent key transmission cycle) to compensate this drift. It adjusts the phase before each cycle of key transmission.

5.2 Electronic part of the set-up

On Fig.36 you can see the electronic part of the set-up.

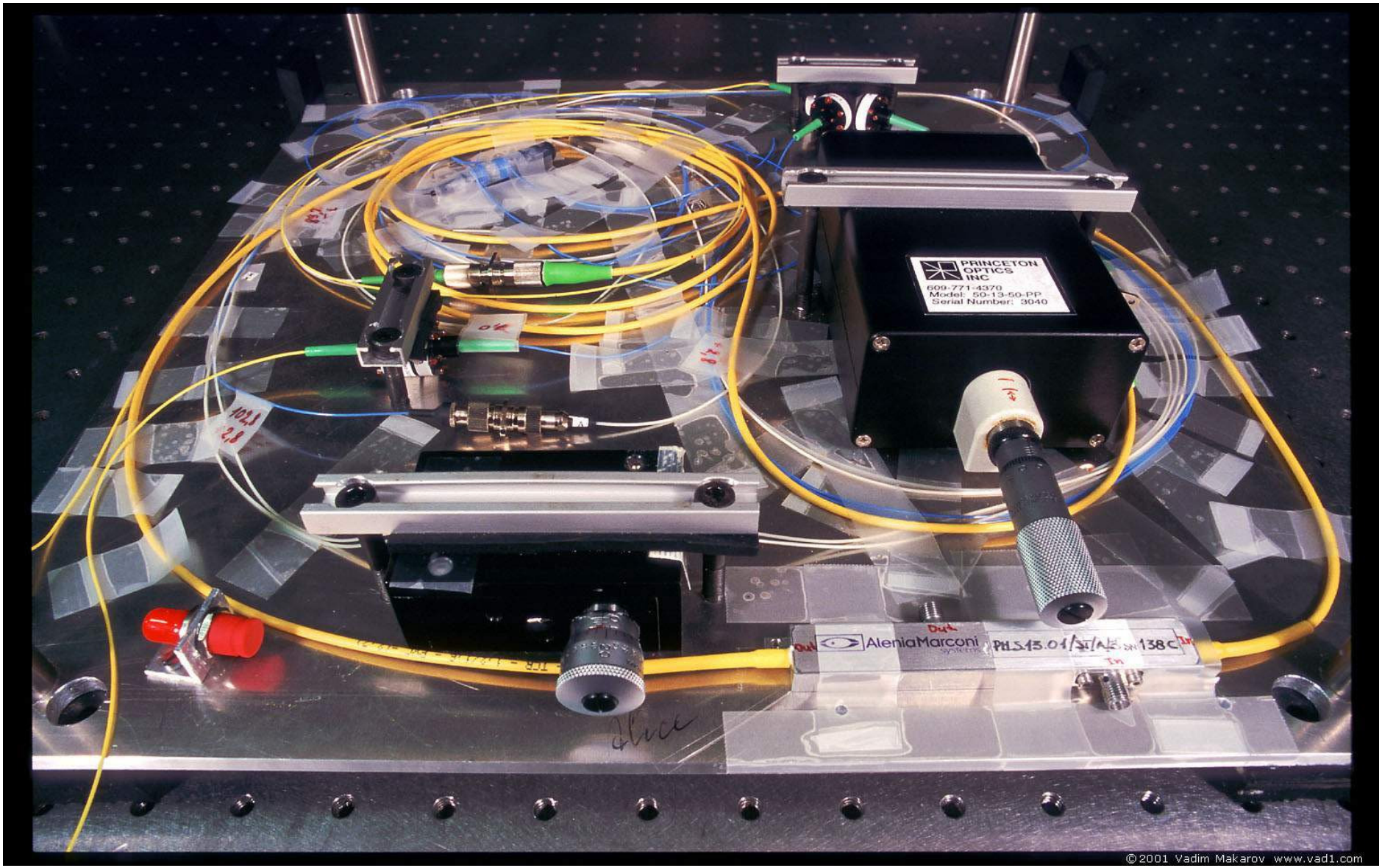


Fig. 33. Photo, Alice (uncovered, no thermo isolation installed)

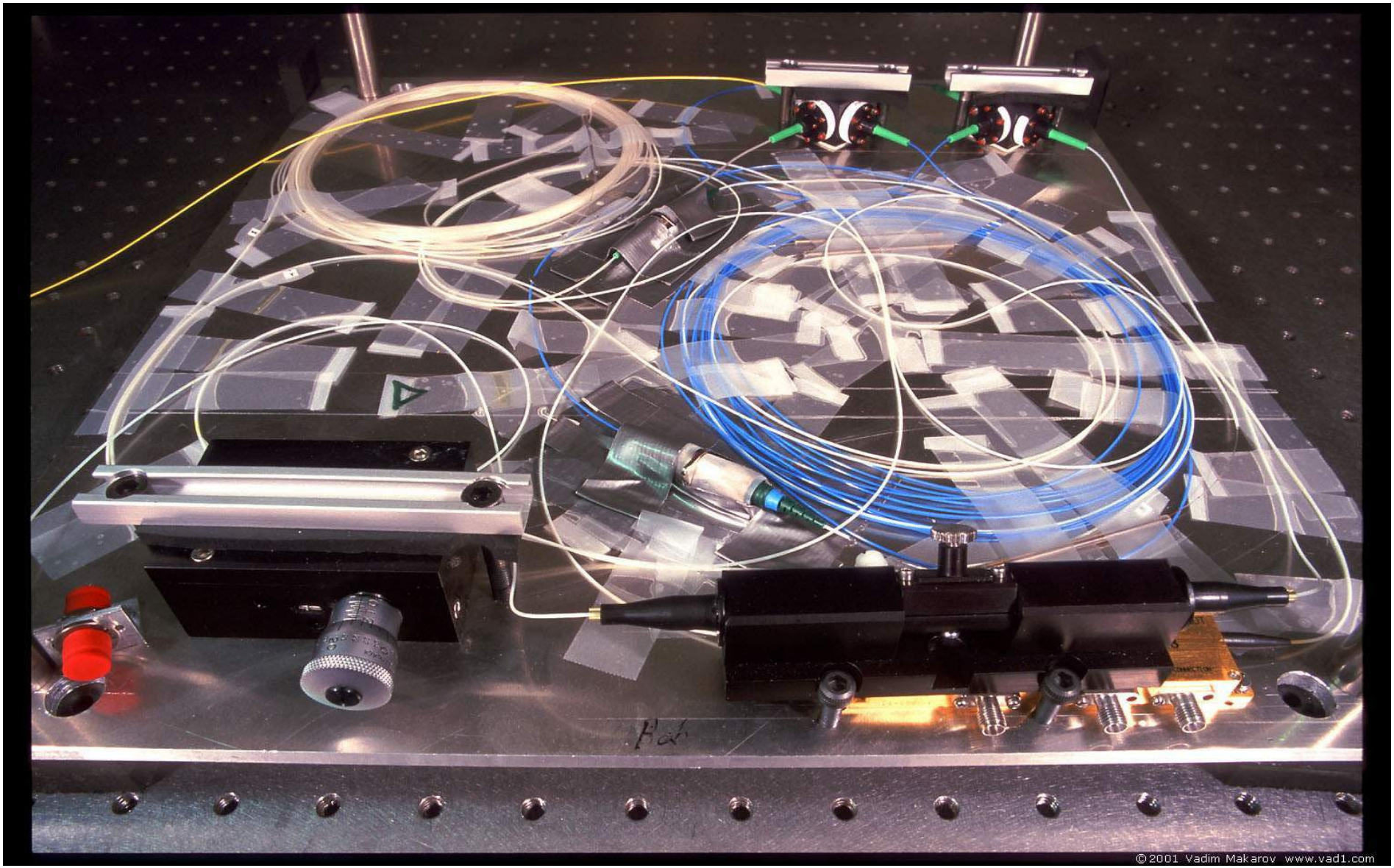


Fig. 34. Photo, Bob (uncovered, no thermo isolation installed)

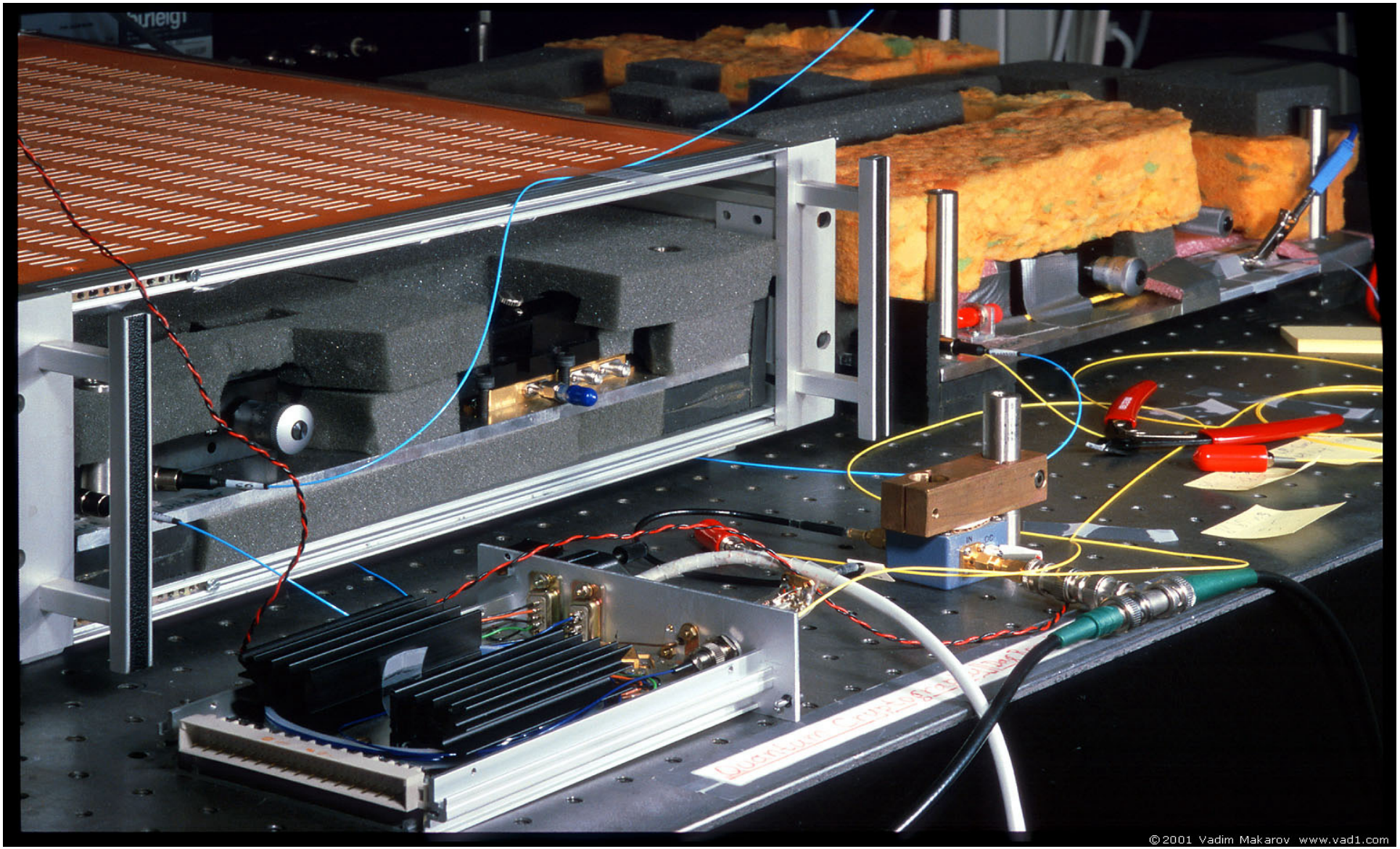


Fig.35. Photo Bob (left) and Alice (right), thermoisolation partially installed

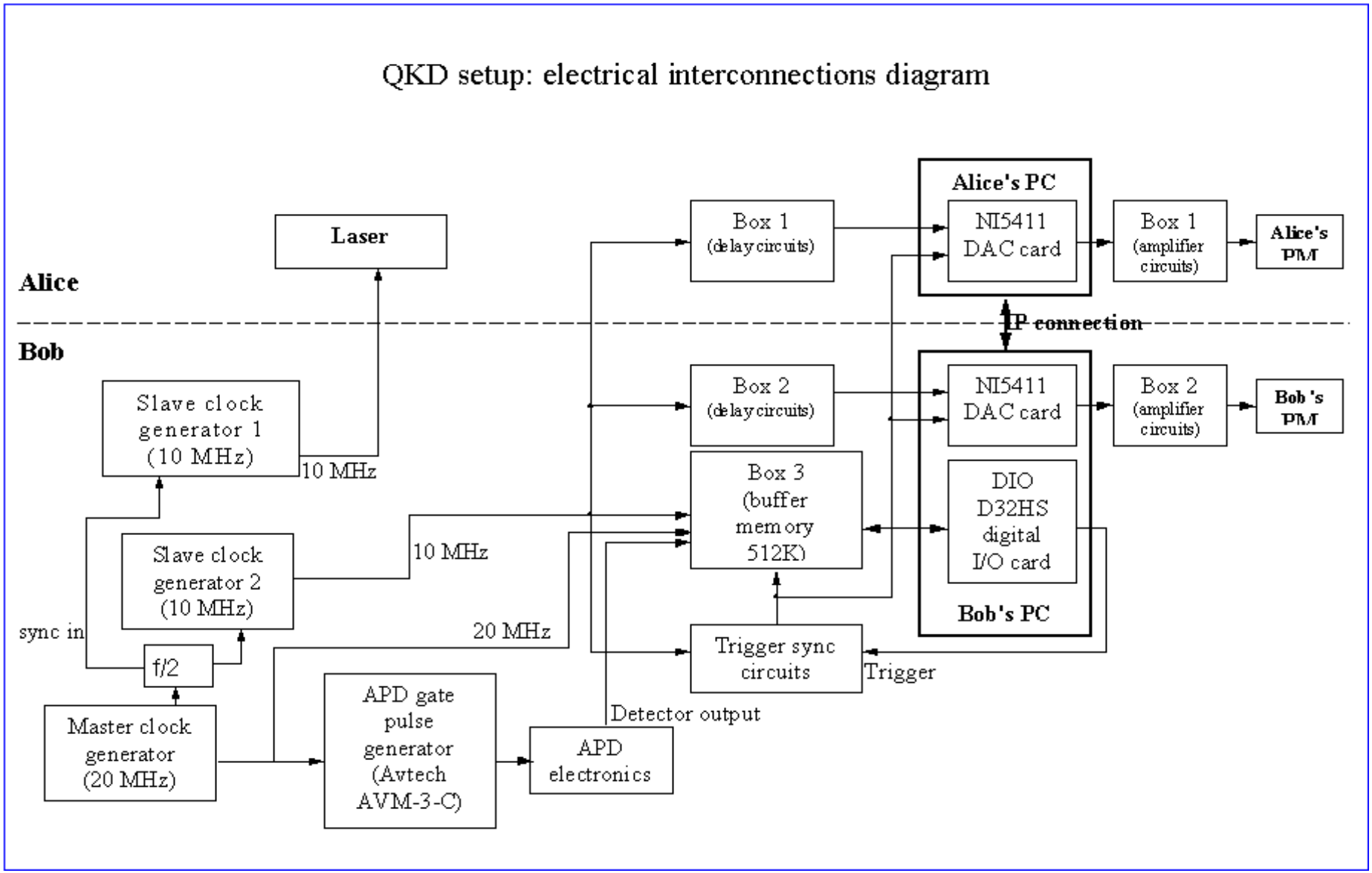


Fig. 36. Block diagram of the electronic part of the set-up

We have two PCs named Alice and Bob, which are connected via the Internet (10 Mbps LAN) used as a public channel. Both Alice and Bob have National Instruments NI 5411 cards, which are high-speed arbitrary waveform generators for driving their phase modulators; Bob also has a DIO D32HS digital I/O card, which is used for detector data acquisition. One of the outputs of this card is also used for generating the trigger signal, which starts the packet transmission in the whole system. Because the NI 5411 cards have a maximum output voltage of +/- 5 V, and our phase modulators have half-wave voltages of up to 8.2 V, there has been made two amplifiers placed in Box1 and Box2 (for Alice and Bob respectively). These boxes also contain adjustable phase shift circuits that help to synchronize the cards. The data acquisition from the APD is done by Box 3, which contains digital circuits and 512KB buffer memory with 20 MHz serial input to store APD data before loading it into Bob's PC (the memory can store up to 2097152 consecutive pairs of detection outcomes). This is made because general-purpose PCs cannot process this data in real time. The detector data is collected to the memory of Box 3 and then Bob's PC reads its contents byte-by-byte using the DIO D32HS card. Real-time data processing would be possible with a dedicated controller.

The whole system is synchronized from the 20 MHz master clock generator (SRS DS345). Its frequency is digitally synthesized and we can consider it to be stable enough. The master clock generator synchronizes two 10 MHz slave clock generators (E-H Research Laboratories inc. model EH129 and Datapulse101), the 20 MHz generator that produces gate pulses for the APD, and also Box 3, which uses it for synchronization during data acquisition. The 10 MHz clock is sent to the laser electronics, to Box 3 (to initiate synchronization) and to the PLL (Phase Locked Loop) inputs of Alice's and Bob's NI 5411 cards through phase delay circuits (Box 1 and 2) [33]. EH129 generator is used to send pulses to the laser electronics (it must be very stable and has small fall time (in our case it is 500 ps)). In our set-up we use narrow laser pulse with 100 ps FWHM. Because we have a lot of devices to synchronize from the master clock generator we had to build a special

distribution buffer for this purpose (Appendix 8). This buffer gives the amplitude of pulses we need for synchronization. It has 5 outputs (3 outputs are 20 MHz, 2 outputs are 10 MHz). We use 10 MHz outputs to synchronize the slave generators, because they can't synchronize from 20 MHz.

In Appendix 9 you can find a detailed scheme with all equipment we used. This scheme shows the exact lengths of the cables and all connections. Also Appendix 10 shows how we should synchronize our generators to get a good interference picture and implement a key transmission. That picture is a screenshot from the oscilloscope.

5.3 Software

Our set-up includes Alice's and Bob's PCs and needs software. Therefore this system is controlled by a program written in LabVIEW and partially in C++ for time-critical routines. All the important values are calculated with subsequent displaying.

Our program cycles through three parts. The first part is phase adjustment; it always runs. Also we have two parts which you can turn on or off depending on the needs of the experiment: a part measuring the delay of bit and a part performing QKD with calculation of the QBER (this last part will be described in Chapter 7). This program runs simultaneously on two computers (Alice's and Bob's), which synchronizes to each other through the IP-connection.

The first part of the program makes a phase adjustment in the interferometer, because the imbalance between the two arms of the interferometer must be kept stable within a fraction of the wavelength of the photons, during a key exchange, to maintain correct phase relations [40]. This program compensates a phase drift in the interferometer. The software realization of such phase tracking algorithm consists of two stages. During both stages Alice sets her phase modulator to 0V and transmits photons.

Stage 1 makes rough phase compensation. During this stage Bob sets his phase modulator voltage to scan the 0^o to 360^o range of phase in a small number of steps

(16 steps). During each step he is counting the number of photons in both “0” and “1” detector time slots. In one of the steps there will be a minimum number of photons counted in “0” time slot and in another it will be a minimum number counted in “1” time slot. At the result we have φ_o.

Stage 2 makes fine phase compensation. At the result of this stage we find $\Delta\varphi$ and add it to φ_o.

Then, knowing Bob’s modulator half-wave voltage, we simply calculate the appropriate voltage, that we apply to Bob’s PM as the bias voltage for subsequent key transmission cycle [33]. The phase compensation is good for few seconds; after that the actual phase in the interferometer drifts away too far. This is why the phase adjustment part of the program is run first in every cycle of the program.

The second, optional part of the program calculates and displays on the graph delays between the moment of passing the voltage to Alice’s and Bob’s PMs and coming of this modulated pulse to the APD. It is necessary to know these delays, because during the key transmission we should read from the memory (Box 3) only such data, which is a result of interference of the modulated pulses. We don’t use the data written to memory before this event. During this program, when we test Alice, she gives a half-wave voltage for her PM and after reading from the memory we can see when the modulated laser pulse reached the APD. The same is for Bob.

For better understanding of this part we describe the working sequence of the set-up that is repeated during every part of program:

1) Loading the values of voltages to Alice’s and Bob’s NI cards.
2) Initialization of the buffer memory at the Box 3.
3) Giving out of the start signal to the set-up (it simultaneously starts both Alice’s and Bob’s NI cards for giving out the voltages and the buffer memory for writing the data from the APD).
4) Wait 300 ms (during this time the buffer memory fills up, sharp value is 210 ms).

5) Reading the data from the memory and subsequent treatment (it can take up to 30 s and depends on the amount of the data we read from the memory).

6. Afterpulsing effect

We tried to make the set-up not only with 100% secrecy but also with high speed of the data transmission. But the result of this is appearing of problems, connected with single photon detection. Today a lot of QKD systems work with low frequency (about 1-1000 kHz), because the increasing of the frequency leads to the increasing of error probability during single photon detection. It is because the afterpulsing effect exists.

The basic feature with the APD is the internal amplification. In QC it is exactly that feature that makes it highly usable. Only one incident photon can actually cause an avalanche breakdown. Under ideal conditions almost every incident photon is absorbed, creating an electron-hole pair. Both carriers are accelerated under the influence of a strong electrical field.

An ideal single photon detector should produce an electronic logical signal when and only when a photon strikes it. Real detectors unfortunately differ from this simple picture. First, the detector sometime fails to record a photon. The probability for an impinging photon to be detected (also called detection efficiency (DE)) is lower than 100%. DE is the overall probability of registering a count if a photon arrives at the detector, and includes fibre coupling loss, APD optical coupling efficiency and intrinsic quantum efficiency, and the efficiency with which the signal processing electronics respond to photon signals from the APD. Second, the detector also has a non-zero probability to produce a count even though no photon is present. Such an event can stem from the thermal generation of a carrier in the sensitive area. In this case, it is known as a dark count. It can also arise from the release of a charge trapped in the junction in the course of a previous avalanche, in which case it is called an afterpulse.

In order to work well for QKD, a single-photon detector should have reasonably high detection efficiency, and low dark count and afterpulse probabilities [41].

In our set-up we use the APD that is operated in so-called Geiger mode. An impinging photon triggers an avalanche and generates thus a macroscopic current pulse, which is recorded with suitable electronic circuits. After it is detected, the avalanche must be quenched. This can be done with three different techniques. First, one can use passive quenching, where a large (typically 50 kΩ) resistor is connected in series with the APD and drops the bias voltage after the beginning of an avalanche. Next, it is also possible to use an active quenching circuit, which lowers the bias voltage and keeps it below the breakdown for a certain time interval as soon as an avalanche is sensed. Finally, when the arrival time of the photon on the junction is known, it is possible to use a so-called gated mode. The bias voltage is raised above the breakdown level only for a short period of time when a photon is expected. In comparison with passive and active quenching, the last method allows very low noise detection, but we have an error that is connected with afterpulsing.

Afterpulse probability is connected with dark counts. In avalanche detectors, dark counts arise from the injection into the junction of charge carriers by three different phenomena: thermal excitation, tunneling across the depletion zone, and emission by trapping centers. This last effect gives rise to afterpulses, where the reemission of a charge trapped during an avalanche takes place during a subsequent gate pulse and produces a count. It induces an overestimation of the count rates.

The two main parameters influencing the afterpulse fraction are the temperature, through the lifetime of trapped charges, and the time interval between two gate pulses. One can evaluate the importance of this effect by measuring the probability of recording a count during a gate pulse coming a certain time after a first avalanche, as a function of this delay. In practice, the voltage generator is triggered a first time, in coincidence with a strong laser pulse (n = 1000). An

avalanche is therefore generated with unit probability, filling up trapping centres. The voltage generator is then triggered a second time and a possible avalanche recorded. By subtracting the dark count rate, obtained in the same conditions but without the laser pulses, one gets a good estimation of the afterpulse probability.

The initial afterpulse probability, which corresponds to the situation of minimal delay between both gate pulses, depends on the gate voltage. This is no surprise, as the excess bias controls the charge flowing through the device, which influences in turn trap population. Moreover, this initial afterpulse probability decreases with increasing temperature (but this also leading to an increase of the dark count). This suggests that temperature doesn't only have an effect on the lifetime of traps, but also on their population by an avalanche [42].

In [38] described one of the methods for decreasing the afterpulsing effect. This method is realized at the electronics of the APD in our set-up. Decreasing the time interval between two gate pulses causes increasing the frequency of the QKD system and also increasing the afterpulsing effect error rate. To solve this problem it was made a scheme that block the appointed number of the gate pulses after coming the first avalanche, to give the APD time fore quenching. This method also increases the speed of the data transmission through the quantum channel.

Now we describe the essence of the method. The laser sends in average 0.1 photons per pulse and it means that only 1 photon will be send in 1 of 10 pulses, and absolutely unable to say in which one. Therefore we can increase the frequency and give the APD time for quenching. In this case we will have faster QKD system with almost the same afterpulsing effect probability as the system that works with the lower frequency.

During our experiments we didn't use this method. Instead of it afterpulses are controlled by software (it will be described in Chapter 7.3).

7. QKD experiment

This part describes an experiment showing the transmission of a key between two parties, usually called Alice and Bob. To do this we utilize phase coding based QKD set-up described in Chapter 5 and BB84 protocol. The main purpose of this experiment is to transmit the key through the quantum channel and calculate the Quantum Bit Error Rate (QBER). Value of the QBER must be less than 11% in order for the key extraction algorithm to be able to produce a secret key [43].

During this experiment we didn't actually extract the key, only did the sifting and measured the QBER, because on this stage we just needed to check the parameters of our set-up (and to know that we should improve the set-up, as the reader will see later).

The key transmission was realized under the computer control, using program written in LabVIEW and partially in C++. Routines written in C++ were used to provide fast treatment for big arrays of the detector data. The structure of software is described in Section 5.3; here we describe the part that performs QKD.

The transmission process begins with Alice. She generates a random sequence of voltages (4 different values) for her phase modulator which correspond to 4 phase shifts: $-3\pi/4$, $-\pi/4$, $\pi/4$ or $3\pi/4$. Such random sequence is 256 values in length and repeated a lot of times, until the memory (Box 3) is full. It is generated by the Random Number Instrument from Numeric Function Subpalette of LabVIEW program. And it is also generated anew in each cycle of the experiment. Bob does the same, but he generates 2 different values of voltage for his PM, which correspond to 2 phase shifts: $-\pi/4$ or $\pi/4$. Also we have the phase drift in the interferometer and a special program [33] makes a phase adjustment (calculates appropriate voltage, which we apply to Bob's PM as the bias voltage for subsequent key transmission cycle) to compensate this drift.

When the memory is full, the C++ subroutine reads the data from it byte by byte (FIFO memory type). If a byte is non-zero, the program splits it into bit pairs to distinguish in which bit (i.e. laser pulse) number and slot ("0" or "1") we

detected a photon. As we use the same detector to detect “0” and “1” we need to use 2 bits to write the result of interference. In each bit pair the first bit is non-zero if we detected “0”, and the second one is non-zero if we detected “1”. At the end of the program we have two arrays and an integer. One of the arrays contains the results of detection (0 or 1, or also another number (2) if we registered a double detection event (it is when we detect a photon simultaneously in both “0” and “1” slots)), another array contains the sequential numbers of the laser pulses with non-zero detection outcomes recorded in the first array. The integer represents the number of non-zero detection outcomes, i.e. the size of the arrays. After that, the LabVIEW program purges double detection event from the arrays. Then, it rejects the results that had been written to memory before the first laser pulse modulated by Alice reached the APD. Number of bits to skip measured in advance with the help of the second optional part in the cycle; see Section 5.3. After the program does sifting (for this purpose we use TCP/IP connection between Alice’s and Bob’s PC to transfer Alice’s modulator data to Bob’s PC where the processing is done). Finally, Bob compares the data he has detected with the calculated data he would have detected in the absence of errors, and calculates the QBER.

7.1 Calculation of the number of photons per pulse

For our experiments we need a very narrow laser pulse (in our case it has about 100ps FWHM). We choose the intensity of the laser pulse to get the right pulse shape and then use the variable attenuator to reduce the number of photons per pulse at the output of Alice.

The optical power at the output of Alice with the laser in the pulse mode is too small to measure the attenuation in Alice’s set-up directly. Therefore we need to put the laser in a continuous mod for this measurement. The results of measurement are:

$$P_{pulse\ \mathrm{mode}}(after\ the\ laser) = 1\ \mu W = P_p(l)$$
$$P_{contin.\ \mathrm{mode}}(after\ the\ laser) = 1.03\ \mathrm{m}W = P_c(l)$$
$$P_{contin.\ \mathrm{mode}}(after\ \mathrm{Alice}) = 7.9\ \mathrm{n}W = P_c(A)$$
$$\frac{P_c(l)}{P_c(A)} = 128607 \quad \Rightarrow \quad 51\ dB$$

Attenuation in Alice's optical setup is 51 dB.

(Current through the laser in the continuous mode was 23.6 mA)

Attenuation in Bob's part was earlier measured to be 4.2 dB.

These results were obtained without the attenuator at the output of Alice.

Now we can find the number of photons per pulse at the output of Alice and also at the input of the APD (knowing the latter, we can compare it with the results we obtain in the QKD experiment our program).

The energy of one photon is:

$$E_{ph}(\lambda = 1310\ nm) = h \cdot \upsilon = h \cdot \frac{c}{\lambda} = 1.517 \cdot 10^{-19}\ J$$
$$P_{pulse\ \mathrm{mode}}(after\ Alice) = \frac{P_p(l)}{128607} = \frac{1 \cdot 10^{-6}}{128607} \approx 7.8\ pW = P_p(A)$$
$$\text{Number of pulses per second } n = 10^7$$
$$\frac{\mathrm{P_p}(A)}{n} = \frac{7.8 \cdot 10^{-12}}{10^7} = 7.8 \cdot 10^{-19}\ J / pulse = E_{pulse}$$
$$N = \frac{E_{pulse}}{E_{ph}} \approx 5.1\ photons / pulse$$

N is big, because it was the first experiment and we needed to check and adjust the system in favorable conditions, and then to improve it.

7.2 First experimental results

In all our experiments we had to know delays between the moment of applying the voltage to Alice's and Bob's PMs and arrival of the laser pulse modulated by this voltage to the APD. The delays were measured: for Alice it is 20 pulses (it means that we need to ignore first 20 detected bits in the buffer memory in Box 3) and for Bob it is 19 pulses. These graphs (Fig. 37, Fig. 38) were displayed by the second part of the program. To measure this delay (for example Alice's) at the moment of starting the set-up Alice gives a half-wave voltage for her PM (Bob gives zero for his PM), in this case it has to be "1" after detection event. At the graph you can see the moment in which we have "1" written to the memory (this is delay). The same for Bob, except that gives a half-wave voltage for his PM and Alice dives zero for her one.

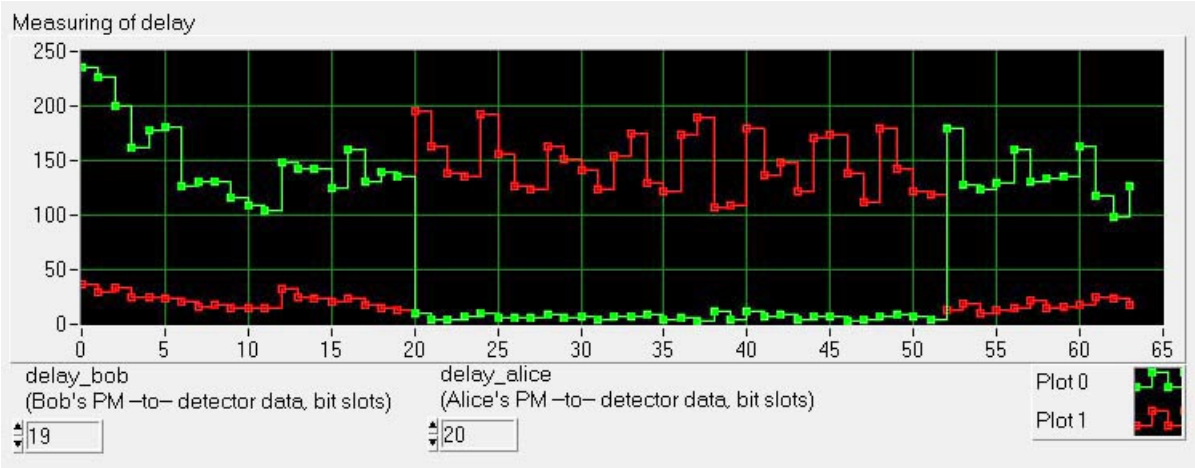


Fig. 37. Measurement of Alice's bit delay. The green curve (plot 0) represents the number of photons we detected in 0 time slot, and the red curve (plot 1) represents the number of photons we detected in 1 time slot

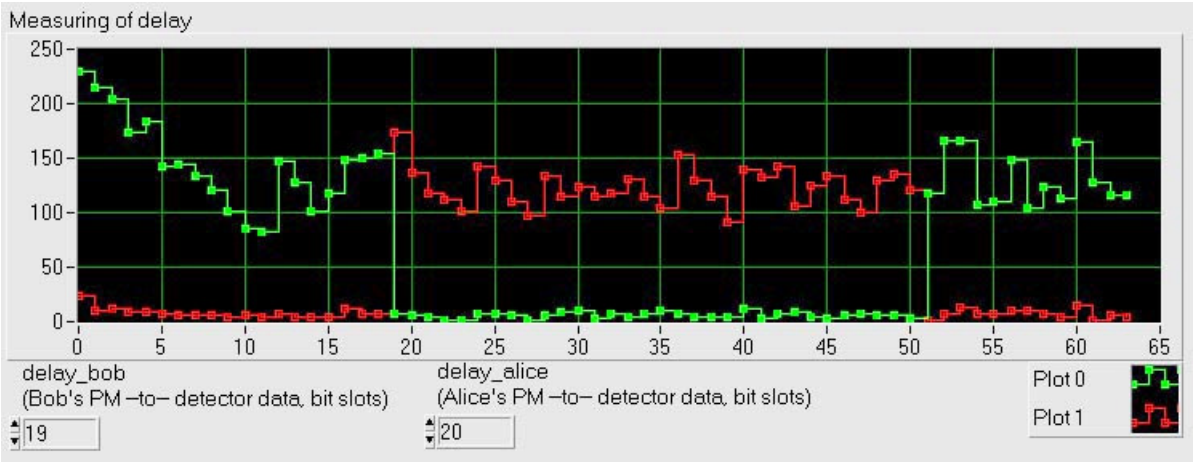


Fig. 38. Measurement of Bob's bit delay. The green curve (plot 0) represents the number of photons we detected in 0 time slot, and the red curve (plot 1) represents the number of photons we detected in 1 time slot

First experiments were made with a big number of photons per pulse (5.1 photons/pulse), because we had to adjust the system at first and used quite bright pulses. Here you can see the result of one of the first experiments, where we calculated QBER (Fig. 39, Fig. 40). On Fig. 39 you can see the graph of QBER (the best values are about 8 –9%; the last point on the graph is 7%) and the number of bits after sifting. The shape of the interference curves is presented on Fig. 40. Green curve is the number of photons we detected in 0 time slot, and red one – is the number of photons we detected in 1 time slot.

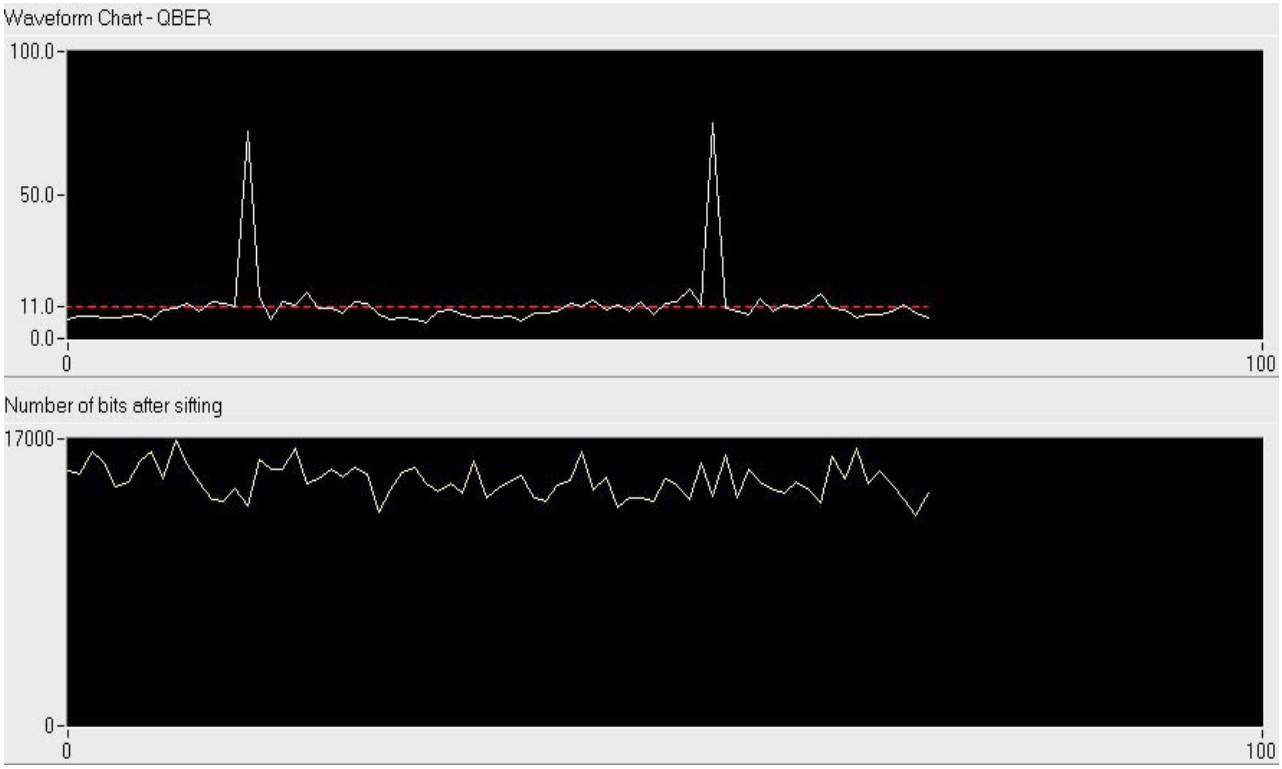


Fig. 39. QKD Experiment no. 1. QBER and the number of bits after sifting. Each point on the chart represents results of one QKD run

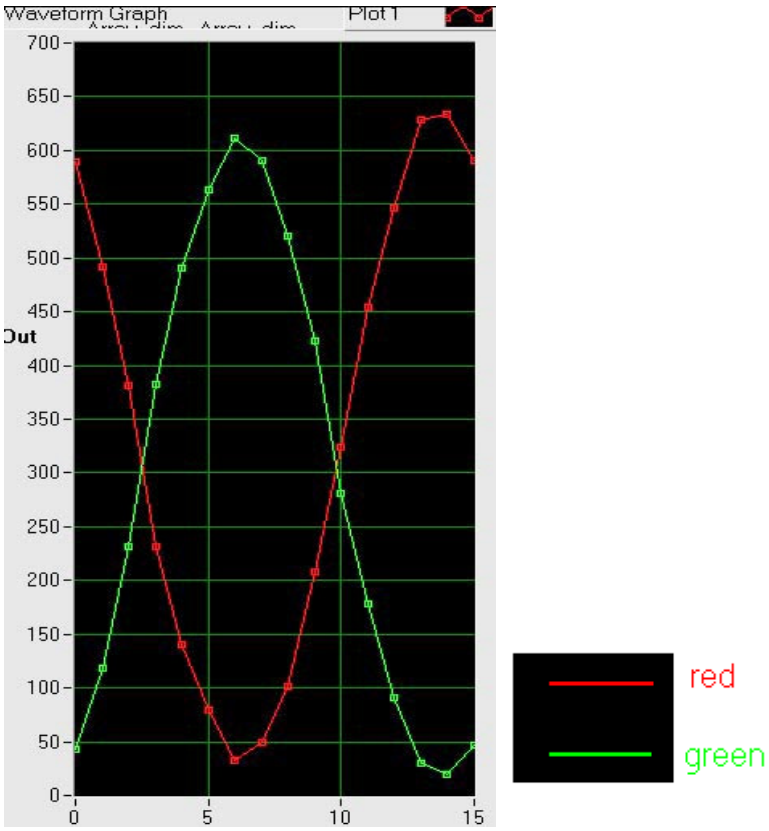


Fig. 40. QKD Experiment no. 1. Interference curves

Now we can explain conditions of the experiment and the data we have gotten.

Let's take for example one typical QKD run. Out of 512 KB buffer memory (2097152 bit pairs), we have read the first 209695 bit pairs. Number of non-zero detection outcomes was 30375. In 1100 of them we registered double detection event. Number of bits after sifting was 14778. The size of the raw key we transmitted was 14778 bits with QBER = 8%.

Sometimes you can see some peaks on QBER graph Fig. 39. It is problems with Alice's NI 5411 DAC card. It works unstable and sometimes gives too low voltage for her PM. Unfortunately we had no time to buy new card or repair this one. Also from QBER graph you can see that in some moments value of QBER is above the 11% line.

We have adjusted Alice's variable ratio coupler and obtained more results represented on the Fig. 41 and Fig. 42.

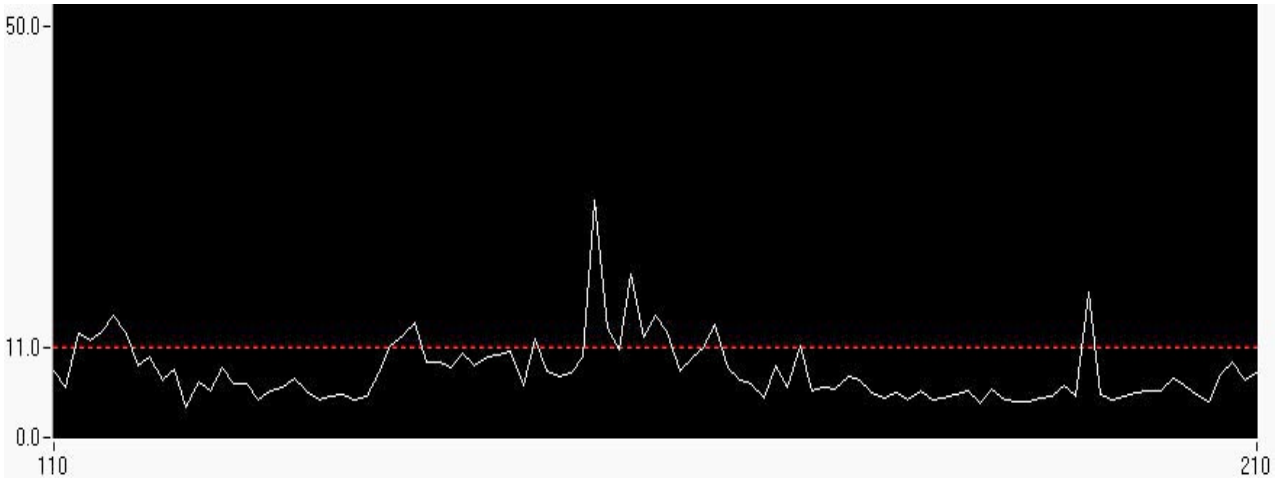


Fig. 41. QKD Experiment no. 2. QBER graph. Each point on the chart represents results of one QKD run

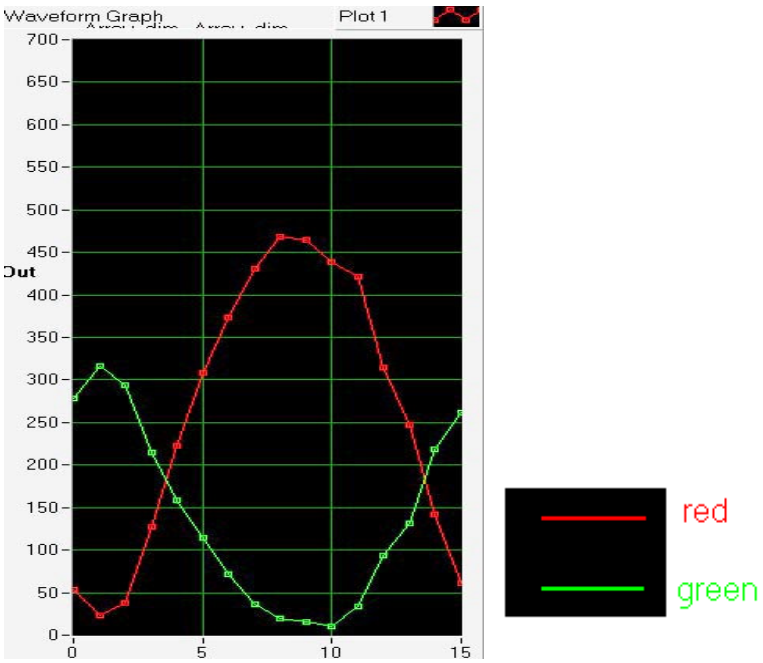


Fig. 42. QKD Experiment no. 2. Interference curves

From the result that is shown on Fig. 41 we can see that the set-up is still not stable, but there are some periods we have QBER = 4%. We have found the cause of this instability: we had unstable generator that gives pulses for the laser and also it has too big raise and fall times.

7.3 Results with the completed set-up

We have exchanged the generator and put the variable attenuator at the output of Alice to complete the set-up.

The attenuator has 2,5 dB attenuation (in its 0 position). Also, the length of the pathcord connecting Alice and Bob was increased to 5 m.

We made some experiments and they showed us that there is instability in optical part, because the results change from day to day. We suppose such instability is caused by Alice's coupler. Also attenuation inside Alice's part is too large (it has become larger some time ago, the variable delay line came out of alignment).

Thinking about instability we measured the attenuation once more and obtained another results:

$$P_{contin.\ mode}(after\ the\ laser) = 0.989\ \text{m}W = P_c(l)$$
$$P_{contin.\ mode}(after\ \text{Alice}) = 13.9\ \text{n}W = P_c(A)$$
$$P_{contin.\ mode}(after\ \text{Bob}) = 1.5\ \text{n}W = P_c(B)$$
$$\frac{P_c(l)}{P_c(A)} = 71151 \quad \Rightarrow \quad 48.5\ dB$$
$$48.5 + 2.5 = 51 dB \quad \text{(added the attenuator)}$$

The attenuation in the transmission line and Bob' part is:

$$\frac{P_c(A)}{P_c(B)} = \frac{13.9 \cdot 10^{-9}}{1.5 \cdot 10^{-9}} = 9.3 \qquad \Rightarrow \qquad 9.7\ \text{dB}$$

9.7-2.5=7.2 dB

The experiment under these conditions gave us results with QBER = 9 %. On Fig. 43 you can see the graph of QBER and the number of bits after sifting. The shape of the interference curves is presented on Fig. 44. Green curve is the number of photons we detected in 0 time slot, and red one – is the number of photons we detected in 1 time slot.

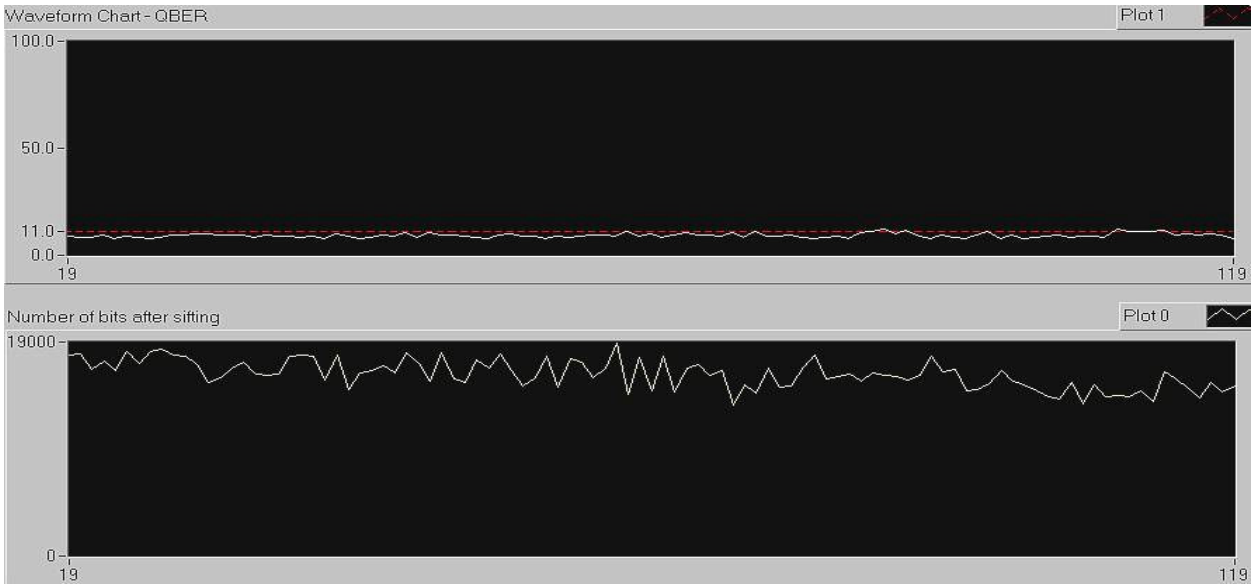


Fig. 43. QKD Experiment no. 3. QBER and the number of bits after sifting. Each point on the chart represents results of one QKD run

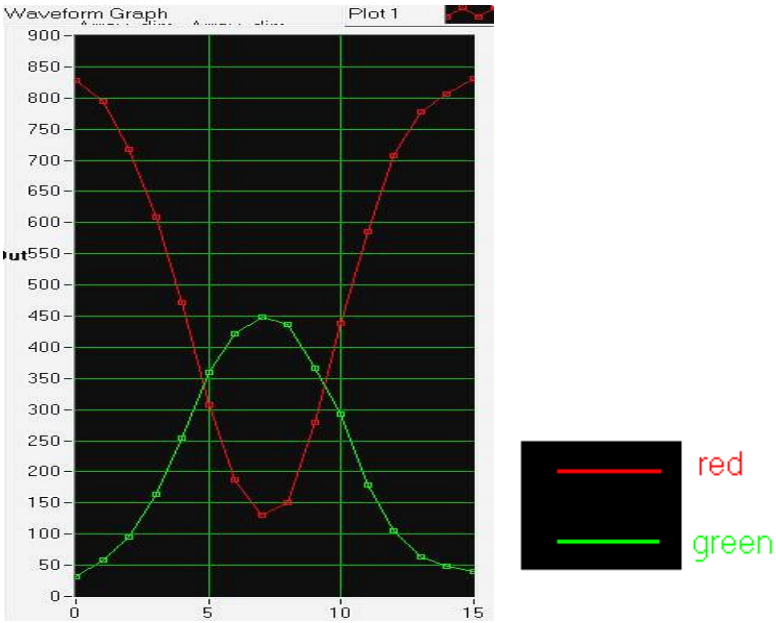


Fig. 44. QKD Experiment no. 3. Interference curves

On Fig.44 you can see that visibility of interference curves is bad. Therefore we adjusted Alice's coupler and obtained better results, which you can see on Fig. 45 and Fig. 46.

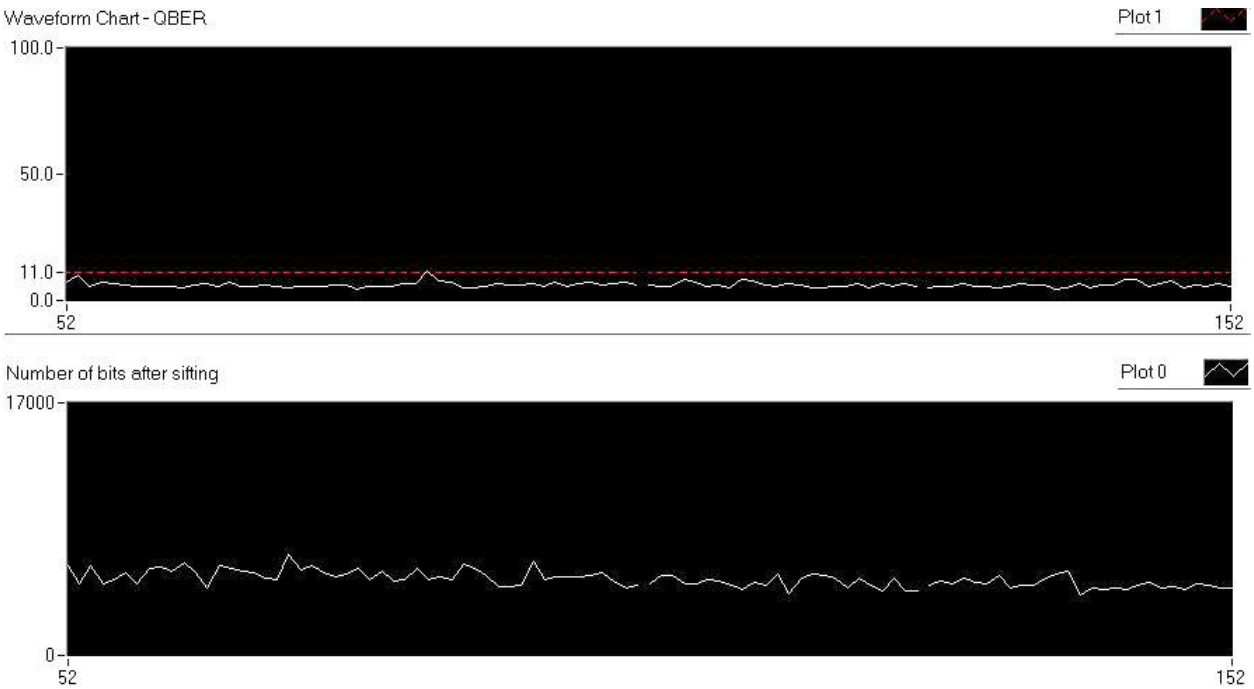


Fig. 45. QKD Experiment no. 4. QBER and the number of bits after sifting.Each point on the chart represents results of one QKD run.

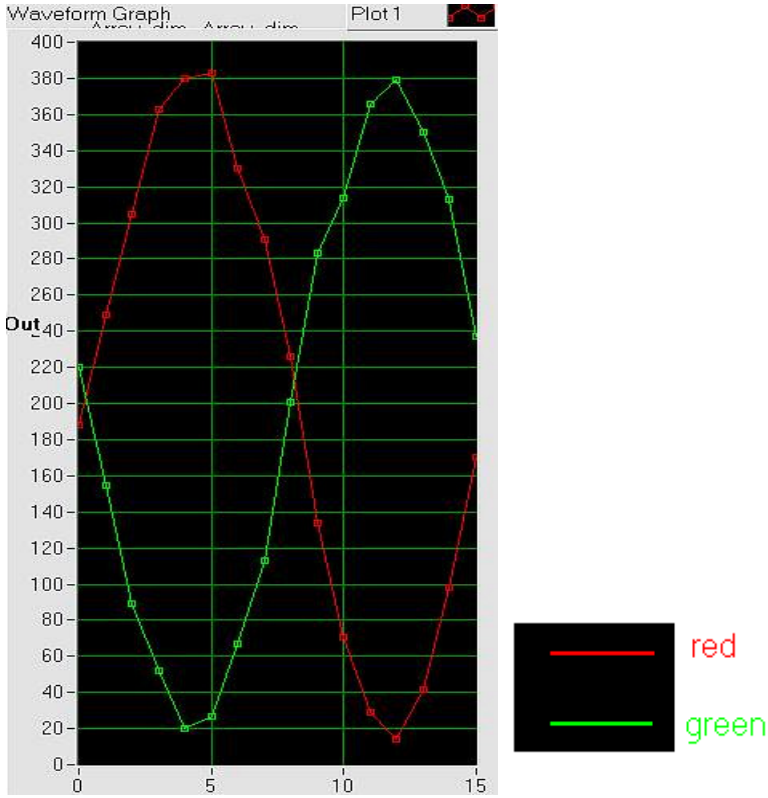


Fig. 46. QKD Experiment no. 4. Interference curves.

The best value of the QBER was 5.7 %. During this experiment the average power of the laser in the pulse mode was 1.35 μW ($P_{pulse} = 1.35\ \mu W$). It means that we had 7 photons per pulse at the output of Alice (after the attenuator). Knowing the attenuation of the transmission line and Bob's optical set-up we can calculate the number of photons per pulse at the input of the APD. Let's base the calculations on one typical QKD run. Out of 512 KB buffer memory, we have read the first 209695 bit pairs. Number of non-zero detection outcomes was 11199. In 185 of them we registered double detection event. Number of bits after sifting was 5225.

The number of photons per pulse on the input of the APD is:

$$N_{APD} = \frac{N_{AfterAlice}}{5.2} = \frac{7}{5.2} = 1.34 \text{ photons/pulse},$$

where 5.2 is the attenuation in the transmission line and Bob's optical set-up.

We detected 11199 pulses from 209695 that is 5.58 %. Therefore Quantum Efficiency of the APD is 4.1%.

After that we added afterpulse blocking to our treatment of the data. Afterpulse blocking has a software realization (LabVIEW). To make the program faster we put it before rejecting the results with double detection events, because afterpulsing effect usually causes many of double detection events. In our experiment we blocked 20 bit pairs after each detection event. But we couldn't check influence of the afterpulse blocking to the QBER, because the set-up was unstable and we had very bad visibility of the interference curves that time.

Also we measured dark count level, and realized that the QBER that is caused by the dark counts is only 0.1 %. The rest of the QBER is the result of non-ideal fringe visibility of the interference curves.

Here is the example of bad fringe visibility of the interference curves Fig. 47:

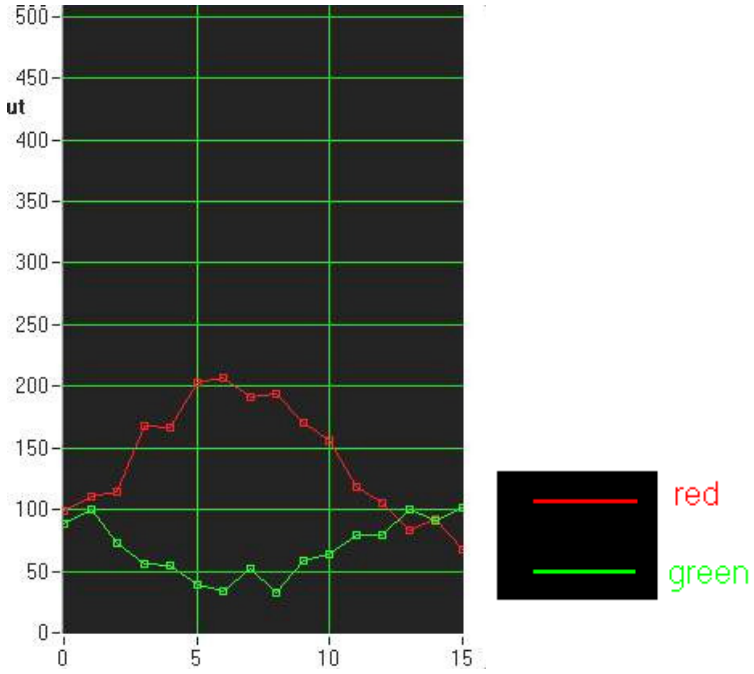


Fig. 47. Interference curves. Bad fringe visibility caused by instability in the experimental set-up

8. Conclusion

During the work the task of the transmitting the key for calculating the QBER was completed, the software was written. I always had to adjust the electronic and optical parts of the set-up, which were unstable. The results we obtain are non-ideal.

In our experiments we had QBER<11%, but the number of the phonons per pulse was quite large (5 photons/pulse). Therefore under these conditions we can't extract the key from the data. To do it we need to decrease the phonons per pulse down to 0.2 photons/pulse to provide secrecy. That means that we need to weaken the laser pulses at about 25 times. But in this case fringe visibility will be bad, and also we have the dark counts that can influence on the result with such weak pulses. To make the experiments with the key extraction we have to repair some components of the set-up.

In the future to make easy the further experiments it is necessary to replace or repair Alice's DAC card and some optical components (such as optical delay line), which gives a big attenuation in Alice's optical set-up.

This work makes it possible to demonstrate a well-working QKD in the future, after the necessary repairs to the equipment are done. In the further experiments key extraction can be implemented.

9. Acknowledgements

I'd like to thank all people I worked with, especially my supervisors: Professor Dag Roar Hjelme, Associate Professor Astrid Aksnes Dyrseth and PhD student Vadim Makarov. Also I thank Steinar Smistad for help with laboratory equipment, Geir Myrvågnes for providing the liquid nitrogen and Bendik Vignes for help with adjusting the set-up.

This research and my stay here in Trondheim were financed with support of the International Office at NTNU, which nominated me for financial support under the Quota Programme from the State Educational Loan Fund. I thank Bjørn Kolstad for his help in financing of my researches.

10. Охрана труда

В данном проекте разработана система охлаждения фотодиода с использованием элементов Пельтье с САР температуры. Этот прибор питается от сети переменного тока 220 В частотой 50 Гц. Поэтому существует опасность поражения электрическим током при работе с прибором или его настройке.

Электробезопасность

Проходя через организм человека электрический ток, оказывает термическое, электролитическое и биологическое действия.

Термическое – нагрев тканей человека.

Электролитическое – начинаются ионные процессы (разложение тканевых жидкостей).

Биологическое – раздражение и возбуждение тканей нервной системы.

Воздействие электрического тока на организм человека может явиться причиной электротравмы. Электротравма – это травма, вызванная воздействием электрического тока или электрической дуги.

Виды электрических травм:

- местные травмы;
- электрические удары (общие).

Местные электротравмы – четко выраженные местные повреждения тканей организма, вызванные действием тока или электрической дуги.

Виды местных электротравм:

1. Электрические ожоги (от тока или электрической дуги);
2. Электрические знаки (четко очерченные пятна серого или бледно-желтого цвета на поверхности кожи);

3. Металлизация кожи;
4. Электроофтальмия – воспаление наружных оболочек глаз – роговицы и конъюктивы (слизистой оболочки, покрывающей глазное яблоко), возникающее в результате воздействия мощного потока ультрафиолетовых лучей, которые энергично поглощаются клетками организма и вызывают в них химические изменения;
5. Механические повреждения (под действием тока мышцы сокращаются – могут порваться связки, вывихи, и т.д.).

Электрический удар – возбуждение живых тканей организма проходящим через них электрическим током, сопровождающееся непроизвольными судорожными сокращениями мышц.

В зависимости от исхода поражения электрические удары можно условно разделить на следующие четыре степени:

1. Судорожное сокращение мышц без потери сознания;
2. Судорожное сокращение мышц с потерей сознания, но с сохранившимся дыханием и работой сердца;
3. Потеря сознания и нарушение сердечной деятельности или дыхания (или того и другого вместе);
4. Клиническая смерть, т.е. отсутствие дыхания и кровообращения [44].

Характер воздействия электрического тока на человека и тяжесть поражения пострадавшего зависит от многих факторов.

Значение тока, проходящего через тело человека, является основным фактором. Сопротивление тела человека и прикладываемое напряжение влияют на исход поражения лишь в той мере, в которой они определяют величину тока.

Действие тока\Род тока	~50Гц мА	= мА
Ощущается начальное действие тока (пороговый ощутимый ток)	0.6÷1.5	5÷7
Непреодолимые судорожные сокращения мышц рук (пороговый неотпускающий ток)	10÷15	50÷80
Фибриляция сердца (через 1÷2 сек)	100÷5000	300÷5000
Остановка сердца минуя стадию фибриляции	>5000	>5000

Еще одним фактором является длительность протекания тока через тело человека. С ростом времени протекания тока уменьшается сопротивление тела человека (а значит, растет ток), накапливаются отрицательные последствия воздействия тока на организм.

Окружающая среда (влажность и температура воздуха, наличие заземленных металлических конструкций и полов, токопроводящей пыли и др.) оказывает дополнительное влияние на условия электробезопасности. Степень поражения электрическим током во многом зависит от плотности и площади контакта человека с токоведущими частями.

Согласно ГОСТ 12.1.038 – 92, установлены предельно допустимые значения токов, проходящих через человека при нормальном и аварийном режимах работы электроустановок.

Род тока	Норм. вел.	Продолжительность действия, сек.										
		0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	>1.0
~50 Гц	I_h,мА	500	250	165	125	100	85	70	65	55	50	6
=	I_h,мА	500	400	350	300	250	240	230	220	210	200	15

По напряжению электроустановки и сети подразделяют на две группы: напряжением до 1000 В и выше [45].

Работа в действующих электроустановках по мерам безопасности разбивают на 4 категории:

1. Выполняемые при полном снятии напряжения;
2. При частичном снятии напряжения;
3. Без снятия напряжения вблизи и на токоведущих частях;
4. Без снятия напряжения вдали от токоведущих частей, находящихся под напряжением.

По условиям электробезопасности прибор, разработанный в дипломном проекте, относится к категории установок, работающих с напряжением до 1000 В.

Прибор относится к 1 классу электроустановок, так как имеет рабочую изоляцию (в соответствии с ГОСТ 12.1.009 – 92) и место для заземления. Безопасность эксплуатации при нормальном режиме работы электроустановки обеспечивается следующими защитными мерами:

1. Применение изоляции;
2. Недоступность токоведущих частей;
3. Применение малых напряжений;
4. Изоляция электрических частей от земли.

Основными техническими способами защиты человека от поражения электрическим током являются:

- защитное заземление;
- зануление;
- защитное отключение.

Учитывая, что у нас используется 3-хфазная 4-хпроводная сеть с глухо-заземленной нейтралью, необходимо зануление.

Зануление – преднамеренное электрическое соединение с нулевым защитным проводником металлических токоведущих частей, которые могут оказаться под напряжением.

Нулевой защитный проводник – проводник, соединяющий зануленные части с глухо-заземленной нейтральной точкой.

Задача зануления – снижение опасности поражения людей током при замыкании на корпус путем уменьшения длительности аварийного режима.

Принцип действия зануления – превращение замыкания на корпус в однофазное короткое замыкание, способное обеспечить срабатывание защиты, и, тем самым, отключить поврежденную установку от питающей сети.

При коротком замыкании либо сгорает предохранитель, либо срабатывает автомат [44].

Расчет зануления

Расчет зануления имеет целью определить условия, при которых оно надежно выполняет возложенные на него задачи – быстро отключает поврежденную установку от сети и в то же время обеспечивает безопасность прикосновения человека к зануленному корпусу в аварийный период.

а) Расчет на отключающую способность

При замыкании фазы на зануленный корпус электроустановка автоматически отключится, если значение тока однофазного короткого замыкания I_k , удовлетворяет условию

$$I_k \geq kI_{ном}$$

$I_{ном}$ – номинальный ток плавкой вставки предохранителя,

k – коэффициент кратности тока.

Так как установка защищается плавкими предохранителями, принимаем k =3.

$$I_k = \frac{U_ф}{\frac{z_T}{3} + z_ф + z_{н.з.}}$$

$U_ф$ – фазное напряжение,

$z_T, z_ф, z_{н.з.}$ – полные сопротивления трансформатора, фазного проводника, нулевого защитного проводника соответственно.

Необходимо, чтобы $z_{н.з.} \le 2z_ф$.

В качестве нулевых защитных проводников рекомендуется применять голые или изолированные проводники, а также различные металлические конструкции зданий, подкрановые пути, стальные трубы электропроводок, трубопроводы и т. п.

Принимаем, что $\frac{z_T}{3} + z_ф + z_{н.з.} = 0.2$ Ом , поэтому получим

$$I_{ном} \le \frac{220}{3 \cdot 0.2} = 366 \text{ А}.$$

б) Расчет сопротивления заземления нейтрали

Сопротивление заземления нейтрали источника тока r_o , должно быть таким, чтобы в случае замыкания какой либо фазы на землю через сопротивление $r_{зм}$, напряжение, под которым окажется человек, прикоснувшийся к зануленному корпусу или к нулевому защитному проводу непосредственно, не превышало некоторого допустимого напряжения прикосновения $U_{пр.доп.}$:

$$U_k \alpha_1 \alpha_2 \le U_{пр.доп} ,$$

$U_k = I_з r_o$ - напряжение зануленного корпуса относительно земли,

$I_з$ - ток замыкания на землю.

Рассмотрим наиболее опасный случай:

- $\alpha_1 = 1$ - человек, касаясь зануленного корпуса, находится за пределами зоны растекания тока замыкания на землю;

- $\alpha_2 = 1$ - сопротивление растеканию ног человека незначительно по сравнению с сопротивлением тела человека;

- в сети отсутствуют повторные заземления нулевого защитного проводника.

Тогда

$$U_{пр.доп} \geq I_з r_о = U_ф \frac{r_о}{r_о + r_{зм}} ,$$

откуда

$$r_о \leq r_{зм} \frac{U_{пр.доп}}{U_ф - U_{пр.доп}} .$$

По условиям безопасности прикосновения к зануленным корпусам в период существования замыкания фазы на землю $r_{зм}$ и $U_{пр.доп}$ должны быть возможно меньшего значения. Поэтому принимаем $r_{зм}$ = 15 Ом.

Поскольку при замыкании фазы на землю установка автоматически, как правило, не отключится и зануленный корпус будет длительное время находиться под напряжением U_k принимаем длительно допустимое напряжение прикосновения $U_{пр.доп}$ = 42 В [44].

При этих условиях $r_о$ =3.54 Ом.

11. Заключение

В результате выполненной работы была собрана система охлаждения, позволяющая охладить фотодиод до –58 ^{o}C и с помощью системы автоматического регулирования устанавливать и стабилизировать ее с точностью 0.1 ^{o}C. Такое значение температуры в системе достигается с помощью использования элементов Пельтье и замкнутого контура водяного охлаждения.

В ходе проведенной работы были рассмотрены преимущества термоэлектрических модулей перед другими видами охлаждения, разработаны и собраны три различные по способу отвода тепла конструкции системы охлаждения. По результатам экспериментов была выбрана лучшая. При разработке охладителя были выбраны модели термоэлектрических модулей, количество их ступеней и мощность. Были проведены измерения параметров охладителя и найдены оптимальные рабочие режимы. Также были проанализированы способы измерения температуры и выбран теплоизолирующий материал.

Следующим этапом в работе были проведены теоретические расчеты САР температуры, сняты экспериментальные характеристики переходных процессов, по которым САР была настроена.

После настройки САР были произведены практические измерения и построены графики переходных процессов при изменении параметров системы регулирования.

В дальнейшем представляется целесообразным усовершенствовать САР и выполнить ее на микроконтроллере. Такое решение позволит легко установить различные постоянные времени для нагрева и охлаждения. Что должно сократить время установления температуры. Для удобства управления ее можно сделать сопряженной с персональным компьютером.

В результате работы по квантовой криптографии было написано соответствующее программное обеспечение и решена задача передачи

ключа с последующим вычислением QBER. Также была написана программа для блокировки сопровождающих импульсов сигнала, но в связи с нестабильностью работы установки результат ее работы было сложно оценить. В ходе работы также производилась настройка как электронной, так и оптической частей установки.

Значение QBER удовлетворяет поставленной задаче и в лучшем случае составляет 4%. Правда система работала нестабильно, и его значение флуктуировало от 4 до 13%. Такая работа была вызвана неидеальностью части оптических и электронных компонентов, которые для дальнейших усовершенствований установки будет необходимо заменить. Также стоит отметить, что во время экспериментов число фотонов в импульсе на входе в линию передачи было довольно большим (5 фотонов на импульс). Поэтому при таких условиях мы бы не смогли извлечь ключ. Чтобы это сделать, необходимо уменьшить число фотонов в импульсе до 0.2, что обеспечит секретность. Это означает, что мы должны ослабить лазерные импульсы в 25 раз, но в этом случае видность интерференционных кривых будет плохой. Таким образом, здесь также необходимо улучшить параметры установки.

При дальнейшей работе с этой установкой планируется осуществление извлечения секретного ключа и увеличение длины линии передачи между общающимися сторонами.

Список литературы (References)

1. Архаров А.М., Марфенина И.В., Микулин Е.И. «Теория и расчет криогенных систем». – Москва, Машиностроение, 1978 г.
2. Алфеев В.Н. «Полупроводники, сверхпроводники и параэлектрики в криоэлектронике». – Москва, Советское радио, 1979 г.
3. http://www.kryotherm.ru.
4. Мухачев Г.А., Щукин В.К. «Термодинамика и теплопередача». – Москва, Высшая школа, 1991 г.
5. Шорников Е.А. «Электронные приборы для контроля и автоматического регулирования температуры». – Москва - Ленинград, Энергия, 1964 г.
6. Клюев А.С. «Автоматическое регулирование». – Москва, Высшая школа, 1986 г.
7. Бесекерский В.А., Попов Е.П. «Теория систем автоматического управления». – Санкт-Петербург, Профессия, 2003 г.
8. Глинков Г.М. «Основы теории и элементы систем автоматического регулирования». – Москва, Металлургия, 1987 г.
9. Чинаев П.И. «Беседы по автоматике». – Киев, Техніка, 1973 г.
10. W. Diffie and M. Hellman, “New directions in cryptography”, IEEE Trans. Inf. Theory IT-22, 1967, pp. 644-654.
11. W. Tittel, G. Rribordy and N. Gisin, “Quantum Cryptography”, Physics World, Vol. 11, № 3, March 1998, pp. 41-45.
12. R.L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM 21, 1978, pp. 120-126.
13. C. Metz, “Special Report: Quantum Cryptography Arrives”, August 2002, http://www.pcmag.com/article2/0%2C1759%2C440474%2C00.asp.
14. P.W. Shor, “Proceedings of the 35th Annual Symposium on the Foundations of Computer Science”, IEEE Computer Society, Los Alamitos, CA, 1994, p. 124.

15. G. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications”, J. Am. Inst. Electr. Eng. 45, 1926, pp. 109-115.
16. The Federal Information Processing Standards Publication Series of the National Bureau of Standards (NBS), “Data encryption standard”, 1993, http://www.itl.nist.gov/fipspubs/fip46-2.htm
17. R. N. Srinivas, “AES: cryptography advances into the future”, 2000, http://www.javaworld.com/javaworld/jw-04-2000/jw-0428-aes_p.html
18. W.Stellings, “Safety and efficiency of the AES”, 2003, http://www.osp.ru/nets/2003/07/038_1.htm
19. C.H. Bennett, G. Brassard and A.K. Ekert, “Quantum Cryptography”, Scientific American, October 1992, pp. 26-33.
20. S. Wiesner, “Conjugate coding”, SIGACT News 15, 1983, pp. 78-88.
21. C.H. Bennett, and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, in Proceedings of IEEE International Conference on computers, Systems and Signal processing (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175-179.
22. J. Ford, “Quantum Cryptography Tutorial”, 1996, http://www.cs.dartmouth.edu/~jford/crypto.html.
23. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum Cryptography”, Reviews of Modern Physics, Vol. 74, № 1, January 2002, pp. 145-195.
24. P.D. Townsend, J.G. Rarity and P.R. Tapster, “Single photon interference in 10 km long optical fibre interferometer”, Electronics Letters, Vol. 29, № 7, April 1993.
25. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental Quantum Cryptography”, Journal of Cryptology, Vol. 5, 1992, pp.3-28.

26. A. Muller, J. Breguet and N. Gisin, “Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more 1 km”, Europhys. Lett. 23, 1993, pp. 383-388.
27. A. Muller, H. Zbinden and N. Gisin, “Quantum cryptography over 23 km in installed under-lake telecom fibre”, Europhys. Lett. 33, 1996, pp. 335-339.
28. C. Marand and P.D. Townsend, “Quantum key distribution over distances as long as 30 km”, Optics Letters, Vol. 20, № 16, August 1995, pp. 1695-1697.
29. H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller and W. Tittel, “Interferometry with Faraday mirrors for quantum cryptography”, Electron. Lett. 33, 1997, pp. 586-588.
30. D. Stucki, N. Gisin, O.Guinnard, G. Ribordy and H. Zbinden, “Quantum key distribution over 67 km with a plug&play system”, New Journal of Physics, Vol. 4, July 2002.
31. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinferter, P.M. Gorman, P.R. Tapster and J.G. Rarity, “ Quantum cryptography: A step towards global key distribution”, Nature, Vol. 419, October 2002.
32. Фрунзе А. «Практика создания ПИ-регуляторов». – Схемотехника №3, декабрь 2000 г., стр.2-7, http://www.dian.ru/.
33. A. Brylevski, Master thesis “Quantum key distribution: Real-time compensation of interferometer phase drift”, 2002, http://www.vad1.com/qcr/alexey.
34. A. Kuhn, M. Hennrich and G. Rempe, “Deterministic Single-Photon Source for Distributed Quantum Networking”, Physical Review Letters, Vol. 89, № 6, August 2002.
35. C.L. Foden, V.I. Talyanskii, G.J. Milburn, M.L. Leadbeater and M. Pepper, “High Frequency Acousto-electric Single Photon Source”, 2000, http://eprint.uq.edu.au/archive/00000253.

36. C. Santory, M. Pelton, G. Solomon, Y. Dale and Y. Yamamoto, “Triggered Single Photons from a Duantum Dot”, Physical Review Letters, Vol. 86, № 8, February 2001, pp. 1502-1505.
37. T. Nesheim, Master thesis “Single photon detection using avalanche photodiode”, 1999, http://www.vad1.com/qcr/torbjoern.
38. K. Vylegjanine, Master thesis “High-speed single photon detector for quantum cryptosystems”, 2000, http://www.vad1.com/qcr/kirill.
39. A. Vakhitov, V. Makarov and D.R. Hjelme, ”Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography”, Journal of Modern Optics, Vol. 48, № 13, 2001, pp. 2023-2038.
40. V. Makarov, A. Brylevski and D.R. Hjelme, “Real-time phase tracking in single-photon interferometers”, Applied Optics (to be published, 2004).
41. D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J.G. Rarity and T. Wall, “Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD’s”, June 2001, http://citebase.eprints.org/cgi-bin/citations?id=oai:arXiv.org:quant-ph/0106007.
42. G. Ribordy, J.D. Gautier, H. Zbinden and N. Gisin, “Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters”, Applied Optics, Vol. 37, № 12, 1998, pp. 2272-2277.
43. The threshold value of QBER is still being discussed. Most of the recent strict security analyses, howewer, put it at 11%. For review, see for example:

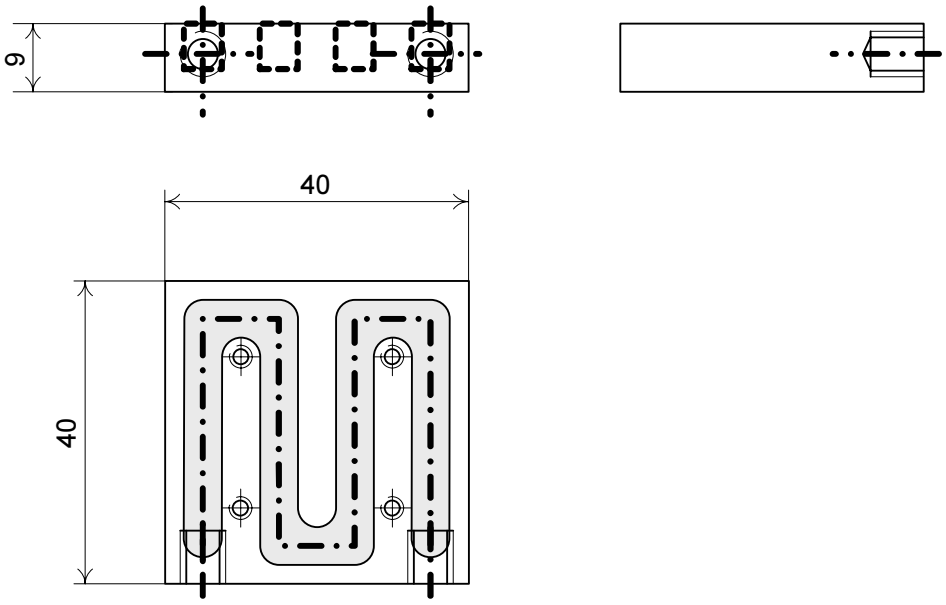
N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum Cryptography”, Reviews of Modern Physics, Vol. 74, № 1, January 2002, pp. 145-195.

M. Bourenanne, A. Karlsson, G. Bjork, N. Gisin and N.J. Cerf, ”Quantum key distribution using multilevel encoding: security analysis”, J. Phys. A: Math. Gen. **35** (2002) 10065–10076.
44. Долин П.А. «Основы техники безопасности в электроустановках». – Москва, Энергия, 1979 г.

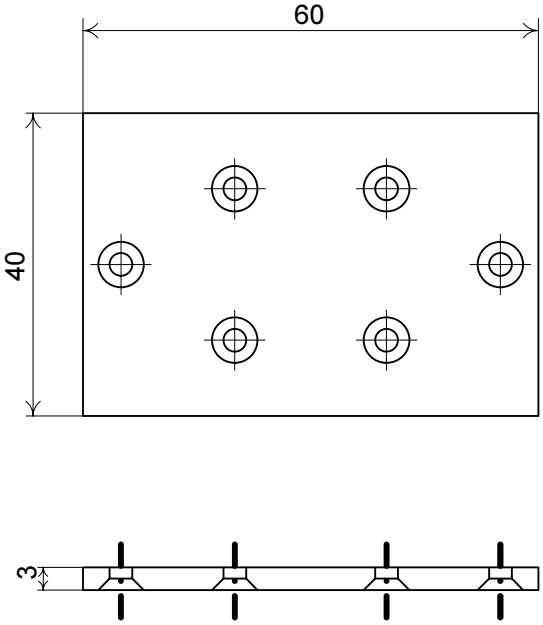
45. Малоян К.Р. «Безопасность жизнедеятельности. Учебное пособие». – Санкт-Петербург, изд-во СПбГТУ, 1994 г.
46. D. Bouwmeester, A. Ekert and A. Zeilinger, ”The physics of Quantum Information”, International, Springer 2000.

Приложение 1

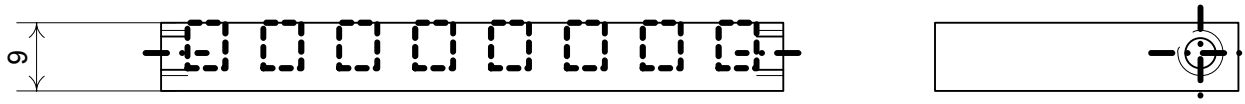
Радиатор для охлаждения фотодиода

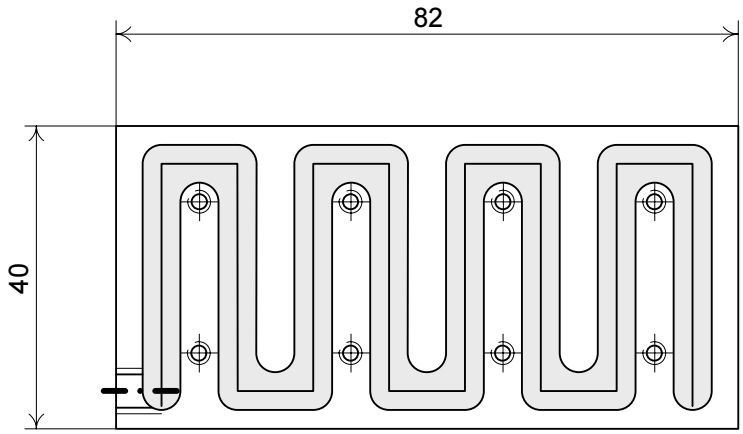


Крышка

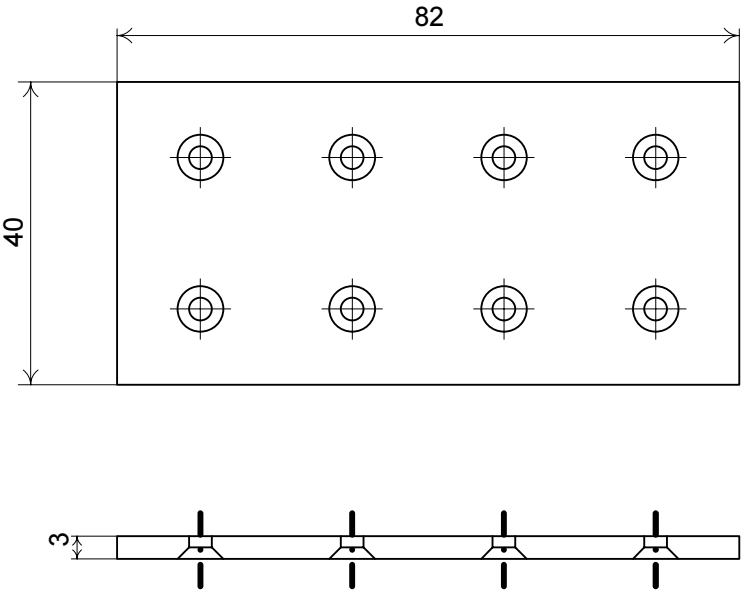


Радиатор для охлаждения воды

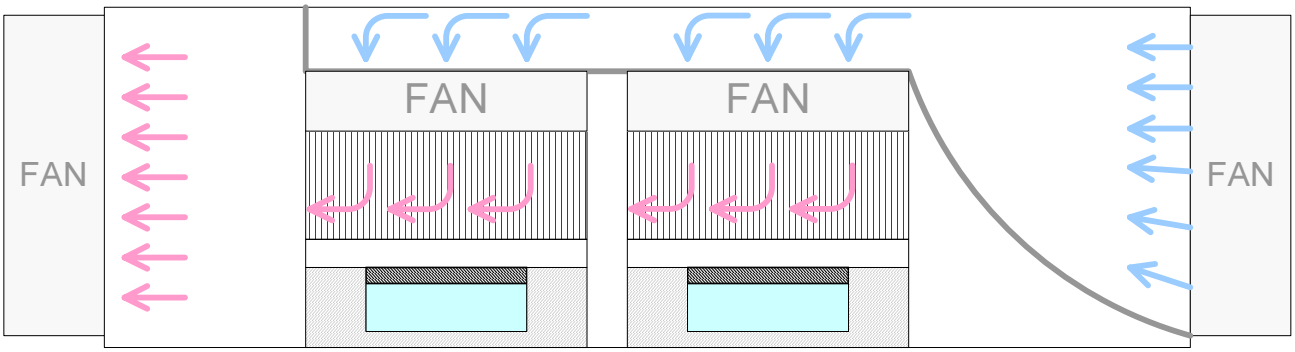


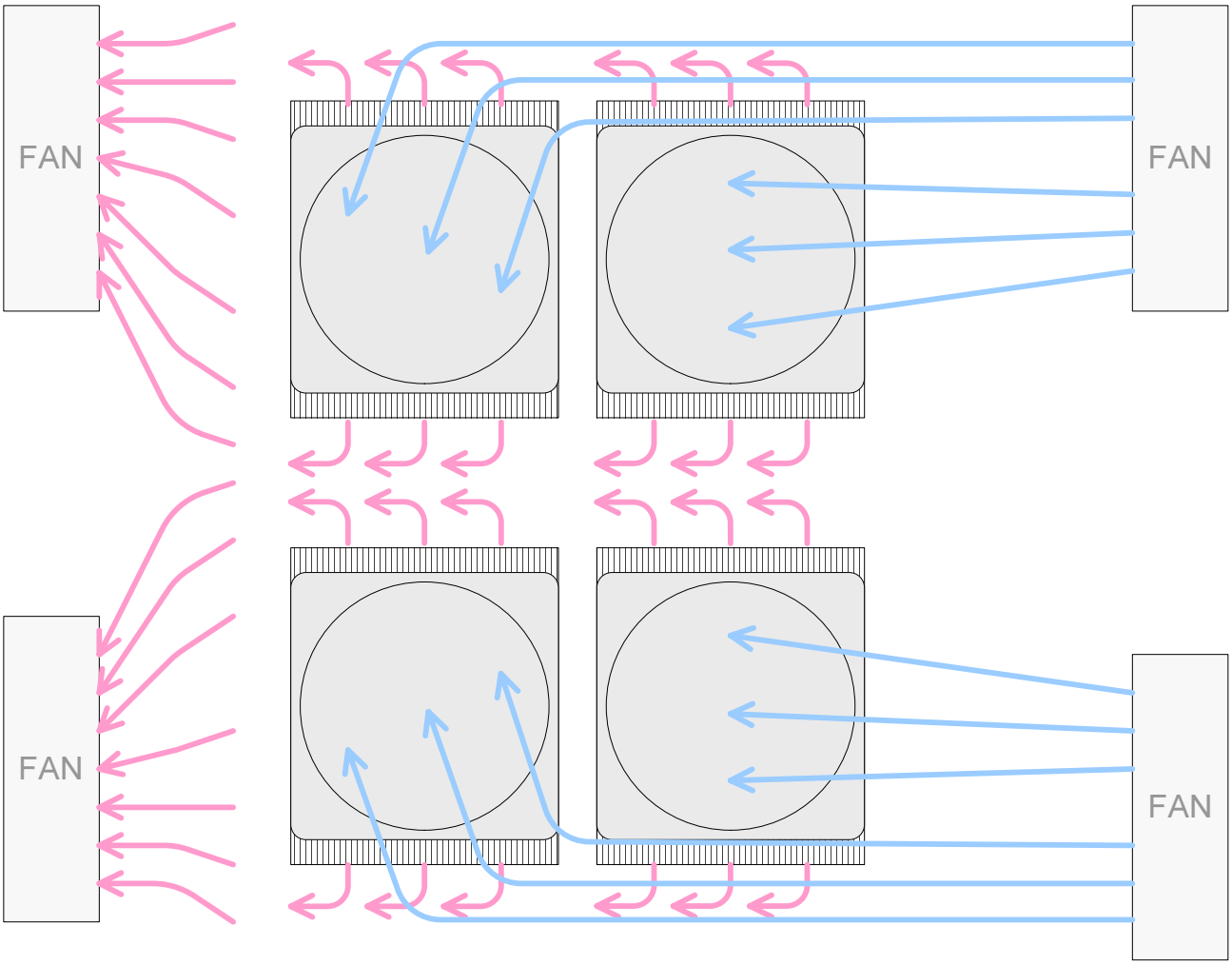


Крышка



Приложение 2





Приложение 3

Электрическое соединение плат и модулей в корпусе

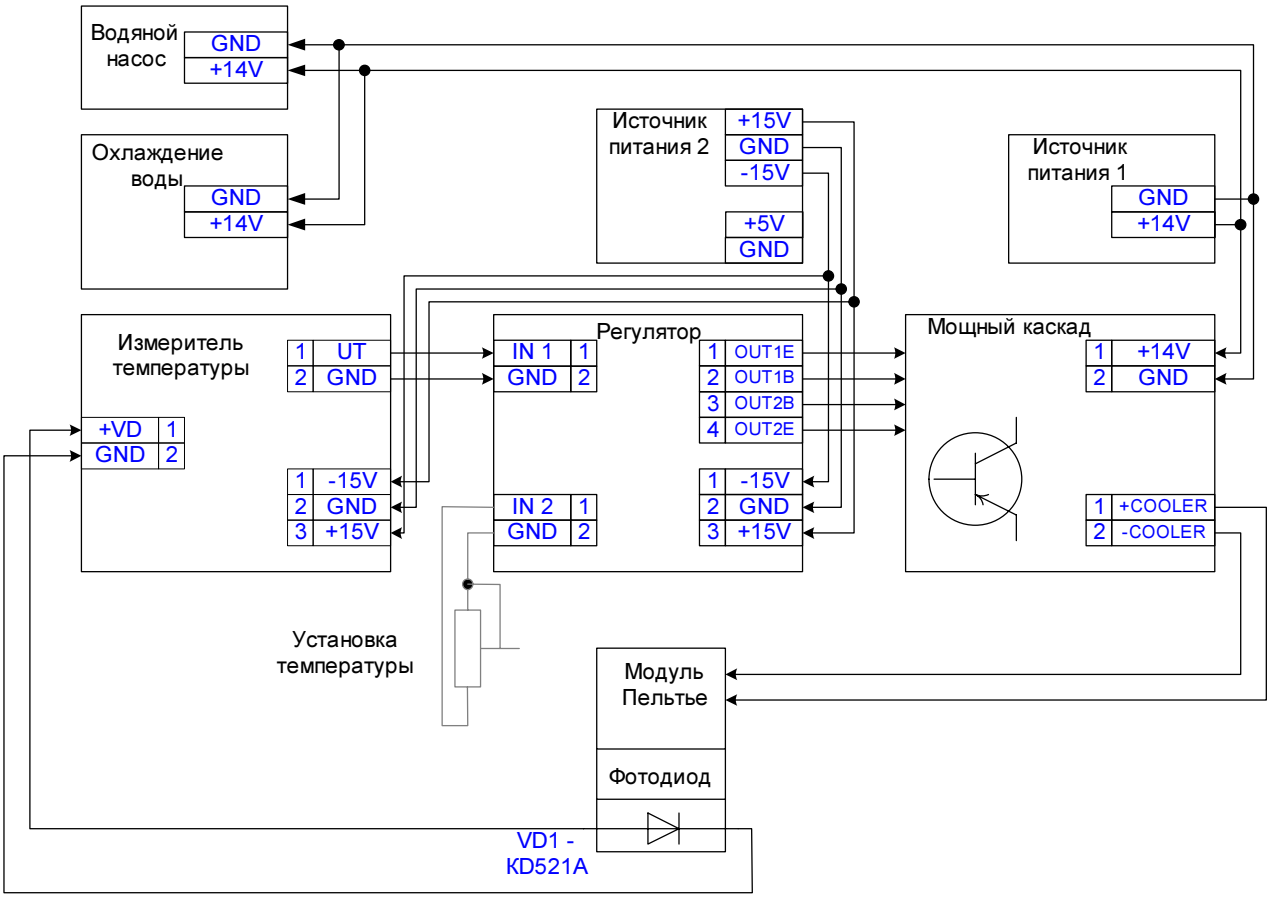


Схема подключения водяного насоса

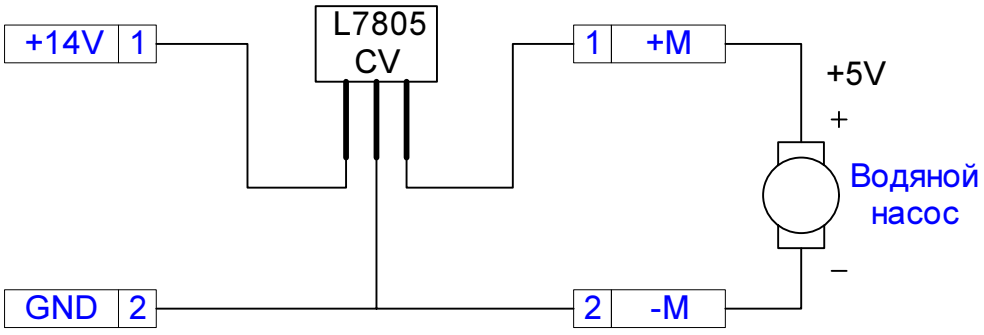
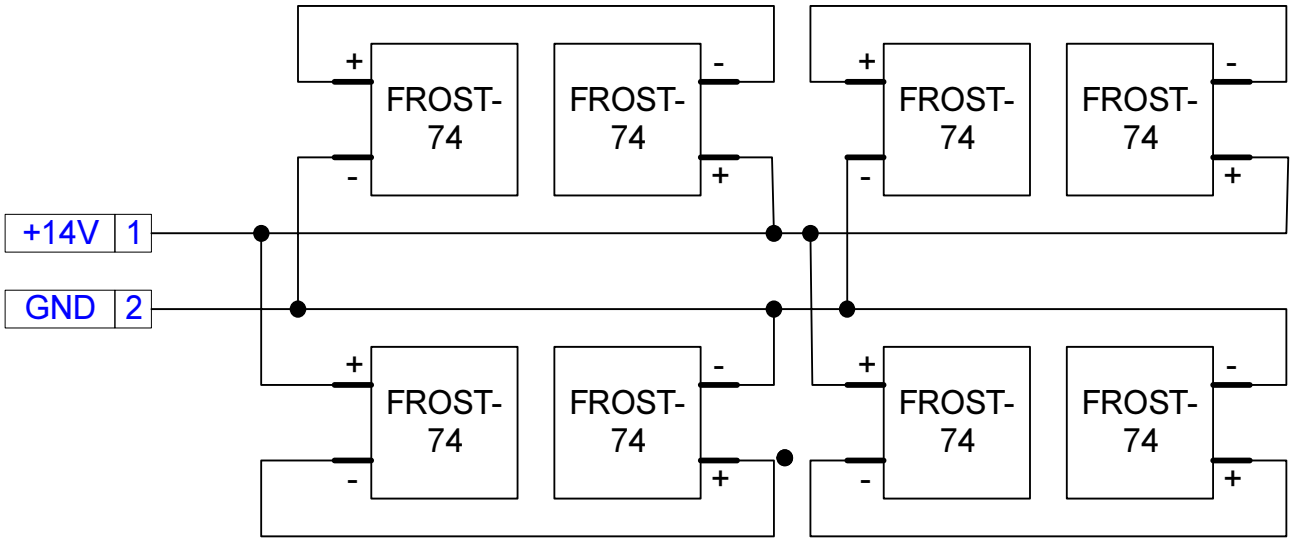


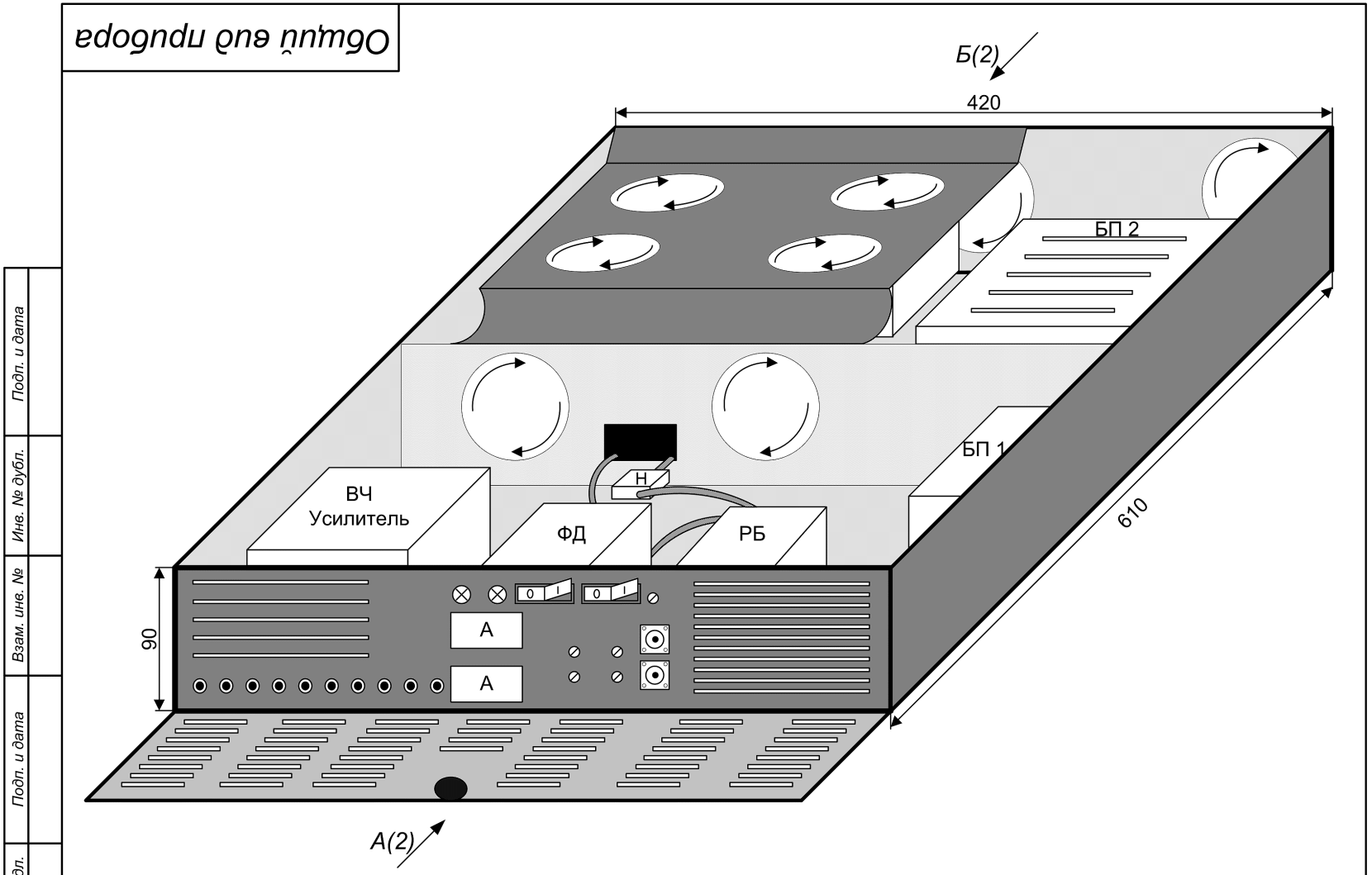
Схема соединения элементов Пельтье для охлаждения воды



Приложение 4

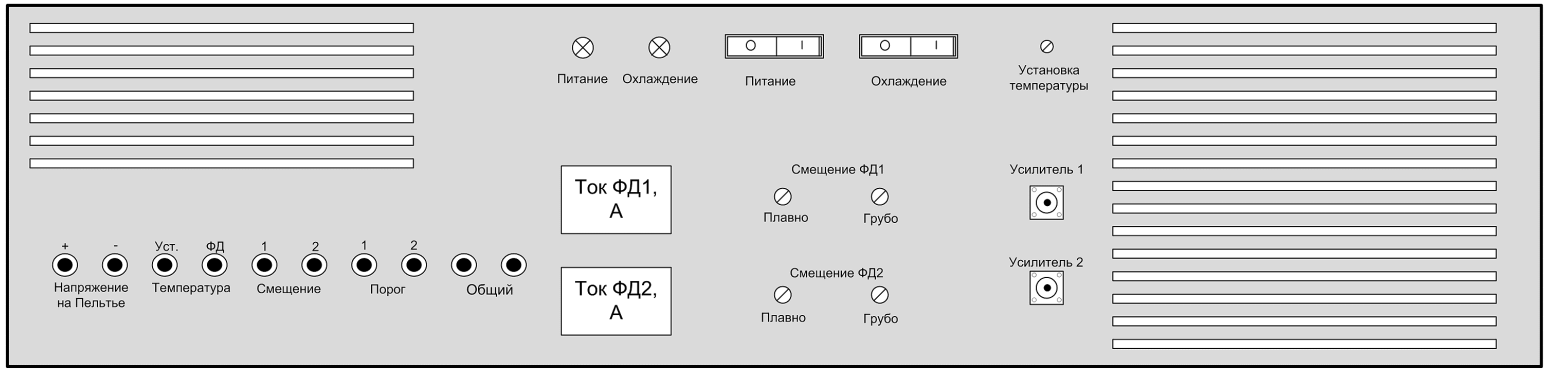
Фотография прибора

Приложение 5. Внешний вид прибора

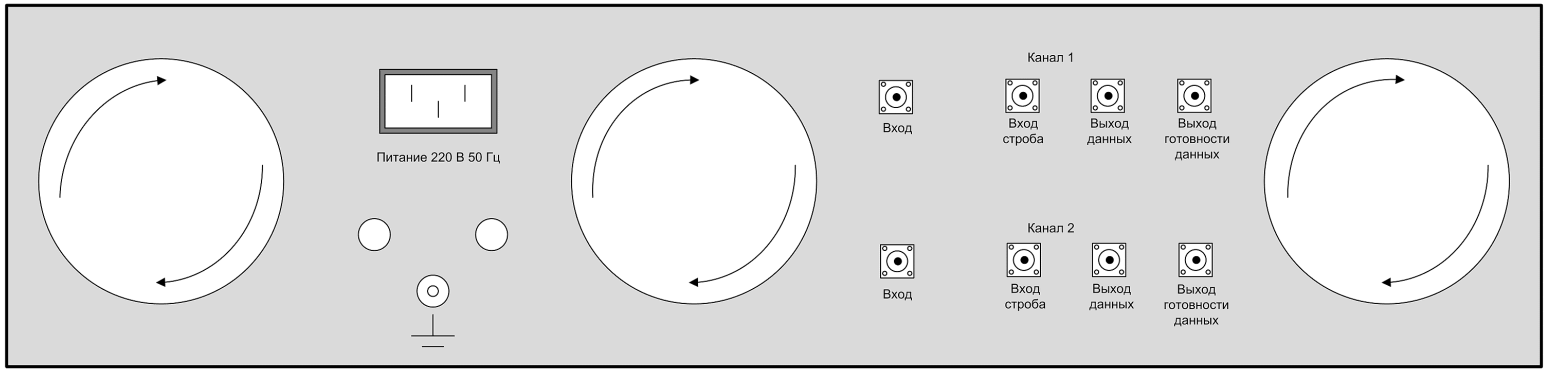


Общий вид прибора

А(1)



Б(1)



Изм.	Лист	№ докум.	Подп.	Дата	Общий вид прибора	Лист 2

Подп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Приложение 6 (Appendix 6)

Semiconductor laser Fujitsu FLD3F6CX

TEST DATA

FUJITSU LIMITED

1015 Kamikodanaka Nakaharaku Kawasaki 211 JAPAN
Cable "FUJITSU LIMITED KAWASAKI" Telephon : Kawasaki)044-777-1111
Telex(Kawasaki)(3842)122 telefax 044-755-3113

1. PRECAUTIONS FOR LASER DIODE

1-1. Safety Precautions

FLD3F6CX laser diode module emits invisible infrared electromagnetic radiation which is harmful to eyes. The radiation may by of sufficient intensity to cause instantaneous damage to the retina of the eye, if viewed at close range. In viewing the laser beam, an infrared-to-visible converter, such as fluorescent screen or TV camera with an image tube is recommended. A "Warning Label",an "Aperture Label" which depicts laser radiation and direction and a."Certification and Identification Label" are attached to the individual laser diode container (Figs. A,B and C).

Fig. A Warning Label

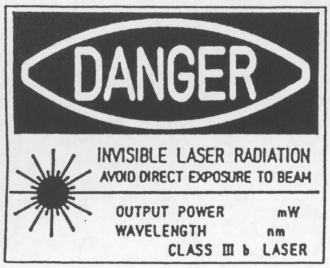
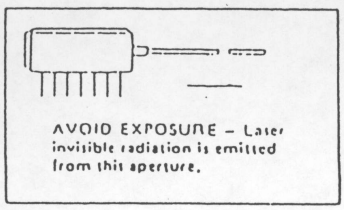


Fig. B Aperture Label



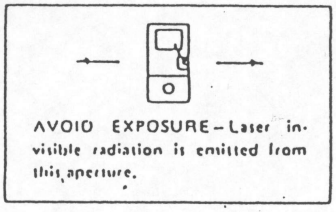
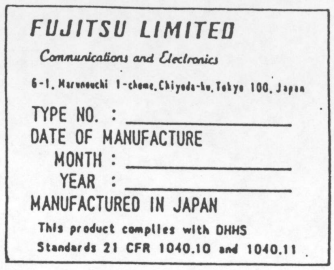


Fig. C Certification and Identification Label



1-2. Handling precautions

Thermal precautions

Operation of a laser diode at temperatures higher than specified (Top MAX.) will cause a rapid degradation. The device must be mounted onto a good heatsink such a copper or aluminum. The radiant area of the heatsink must be larger than 100 cm^2 .

The device may be soldered into a circuit only after proper mounting of the header to an appropriate heatsink. Soldering time should be less than 10 seconds at below 260 deg.C(Tc less than 250 deg.C).

Mechanical precautions

The attached fiber should be handled very carefully,do not twist nor exceed a pull force of gre-

ater than 500 g.f.(5N,case to fiber),or a bending radiusof less than 20 mm.

The device should be mounted onto a heatsink block having a surface flatness of less than 50 um using M2.0 screws with a torque less than 1.5 kg.f.cm.

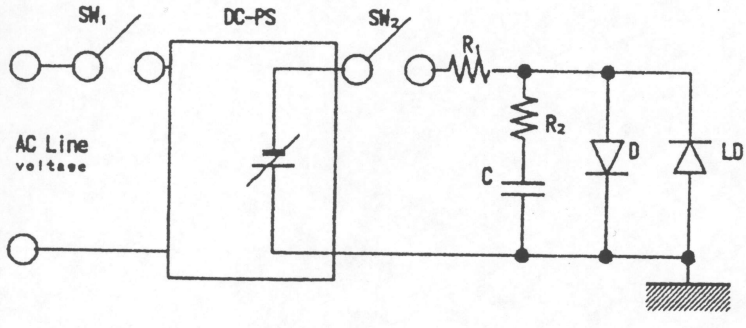
Electrical precautions

To protect the device against electrostatic damage during transportation,lead pins are shorted by electrically conductive material. In taking the device out of the case,appropriate handling precautions against electrostatic damage must be taken.

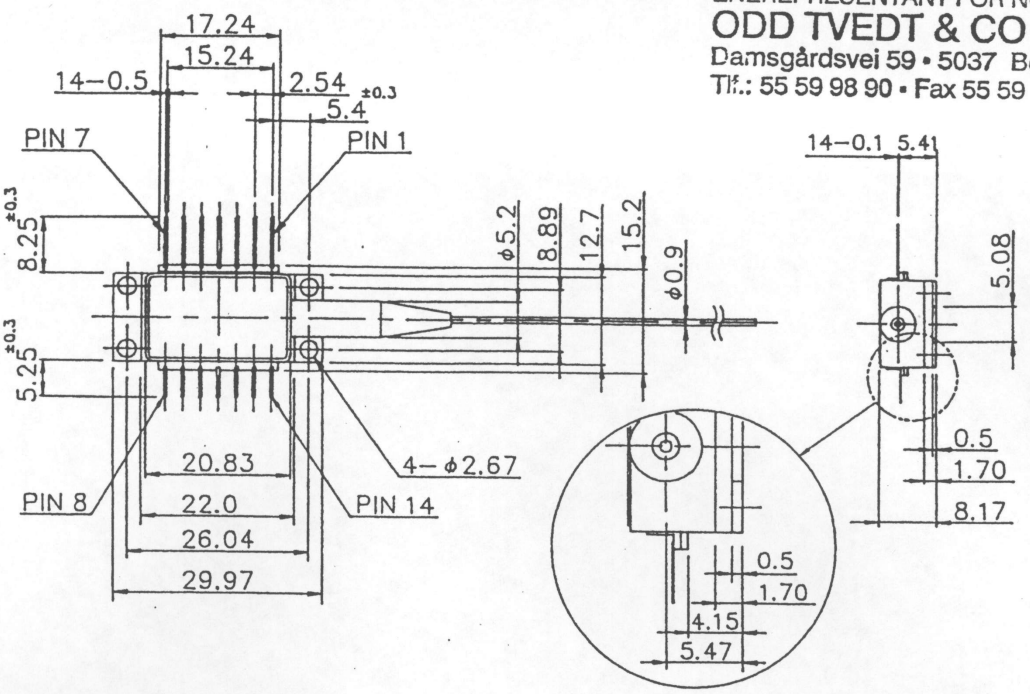
Surge current in the forward or reverse direction may damage the diode. Use of a regulated power supply,a 10 to 20 ohm current limiting resistor,and a negative surge absorbing diode is preferred (Fig.D). A constant current power supply is not recommended because it often generates destructive current surges when it is switched on or off. The current lebel must be at zero before switching the supply on or off.

Stability of the optical output power from the laser diode is affected by the fluctuations in case temperature and the driving current. Optical output power may increase over the absolute maximum ratings as the device junction temperature is reduced. To avoid damaging the device at lower temperature and to achieve stable operation,an automatic output power control (APC) circuit is recommended. This is easily obtained by using the monitoring beam feedback or current signal from the diode to control the driving current supply.

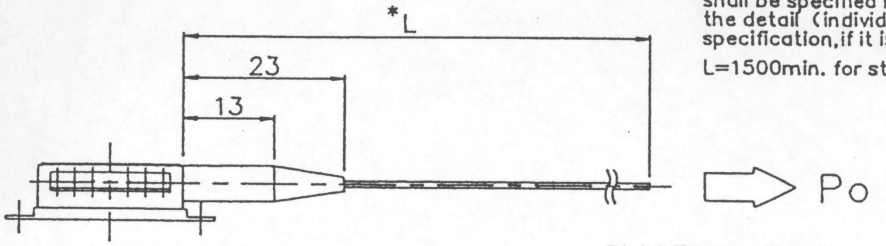
Fig. D Surge Protection Circuit



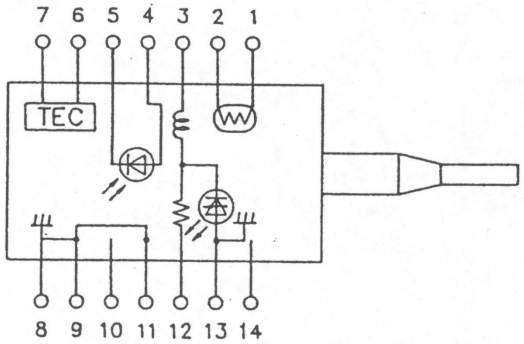
DC-PS : Constant voltage power supply (output adjustable)
SW_1 : Power switch
SW_2 : Output switch
R_1 : Resistor (Forward current limiter-20Ω)
R_2 : Resistor (Surge absorber-20Ω)
C : Capacitor (Surge absorber-1 μF)
D : Diode (Reverse voltage limiter-1S2070)



*Note) Pigtail length (L) shall be specified in the detail (individual) specification, if it is special.
L=1500min. for standard.



TOP VIEW



PIN DESIGNATIONS

1. TEMPERATURE MONITOR
2. TEMPERATURE MONITOR
3. LASER DC BIAS (−)
4. MONITOR (ANODE)
5. MONITOR (CATHODE)
6. TEHP (+)
7. TEHP (−)
8. GROUND
9. GROUND
10. N.C.
11. LASER GROUND
12. LASER MODULATION (−)
13. GROUND
14. N.C.

(Preliminary)

Non−limited dimensions tolerance shall be as follows.				
Length Diameter	0.2 ~ 0.5	~ 30	~ 120	~ 300
	±0.1	±0.2	±0.3	±0.5
Chamfer Radius	0.2 ~ 0.4	~ 1.0	~ 5.0	~ 10.0
	±0.1	±0.2	±0.3	±0.5

all dimensions in mm

EDIT.	DATE	DESIG	CHECK	DESCRIPTION
DESIG.	'93-09-27	K. aoki	CHECK	K. Komiya
APPR.	T. Kaneda			

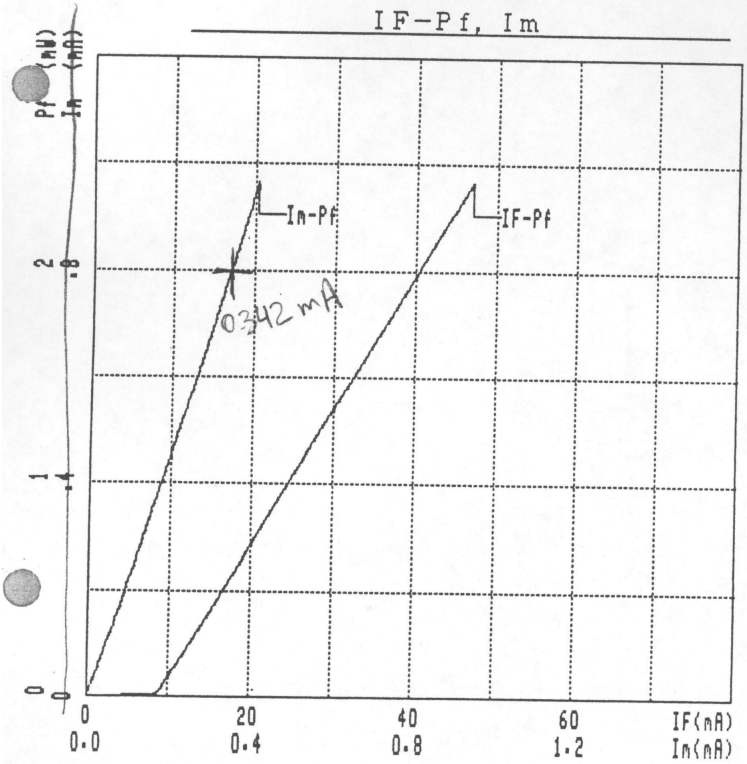
TITLE: CX PKG WO/CON.
DRAW.NO.: FLD−DR027
CUST.:
FUJITSU LIMITED
SHEET 1/1

ENEREPRESENTANT FOR NORGE
ODD TVEDT & CO A/S
Damsgårdsvei 59 • 5037 Bergen
Tlf.: 55 59 98 90 • Fax 55 59 96 0

Sample No . ES-1028 FLD3F6CX Date ; 97/06/18

Tested by ; A. Maki

Approved by ; T. Sasaoka



ITEM		CONDITIONS(25deg.C)	LIMIT	VALUE	UNIT
Threshold Current	Ith	CW	4~ 20	8.7	mA
Slope Efficiency	S	CW, Pf=2mW	0.05~0.083	0.063	W/A
Monitor Current	Im	CW, Pf=2mW	0.1~ 1.0	0.342	mA
Peak Wavelength	λp	Note.1	1290~ 1330	1309.3	nm
Thermistor Resistance	Rth	TLD=25 degC	9.5~ 10.5	10.3	KΩ

Note.1 Ipp=30mA, 2.5Gb/s, NRZ, PRBS, Ib=0.8Ith

CAUTION ! Use of control or adjustment or performance of procedures other than those specified herein may result in hazardous radiation exposure.

FUJITSU LIMITED

Приложение 7 (Appendix 7)

Soviet-made FD312L germanium avalanche photodiode (APD), data sheet.

УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

Указания по эксплуатации по ТУ3-3.2248-89

ХРАНЕНИЕ

Требования к хранению по ТУ3-3.2248-89

ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

Изготовитель гарантирует соответствие данного изделия требованиям технических условий ТУ3-3.2248-89 в течении минимальной наработки и срока сохраняемости при соблюдении потребителем режимов и условий эксплуатации, правил хранения и транспортирования, а также указаний по применению, монтажу и эксплуатации, установленных в ТУ.

Срок гарантии исчисляется с даты приемки изделия.

РЕКЛАМАЦИИ

При предъявлении рекламации изделие возвратить предприятию-изготовителю вместе с паспортом и с указанием следующих сведений:

время хранения ;

дата начала эксплуатации ;

дата выхода из строя ;

наработка ч;

основные данные режима эксплуатации ;

причины снятия с эксплуатации или хранения

Сведения заполнены

ОСОБЫЕ ОТМЕТКИ ПРИ ЭКСПЛУАТАЦИИ

ж Конкретный тип фотодиодов указать при поставке

жж На каждом изображении фотодиода указать полярность питающего напряжения.

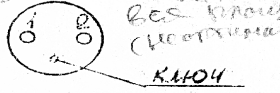
= APD3 Ge APD

ИЗДЕЛИЕ ТИПА ФД312(312Л)*

ТУ3-3.2248-89

ПАСПОРТ

Заводской № 1611 1752 Дата выпуска



Обозначение вывода	Наименование вывода
I	Вывод фотодиода "+"**
2	Вывод фотодиода "-"

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

электрические и фотоэлектрические параметры

Наименование параметра	Норма по ТУ ФД312Л	Норма по ТУ ФД312	Данные испытания	Примечание
1. Рабочее напряжение, В	≤ 40	≥ 8±0,5	32,34	
2. Токовая монохроматическая чувствительность, А/Вт, при температурах				
Т=(20±2)°С	≥ 5,0	≥ 0,5	5,5	
Т=(50±2)°С	≥ 3,0	≥ 0,4	4,0	
Т=минус(60±)°С	≥ 3,0	≥ 0,4	5,6	
3. Темновой ток, мкА, при температурах				
Т=(20±2)°С	–	≤ 0,4	должно быть 200 мкА	
Т=(50±2)°С	–	≤ 3,5		
Т=минус(60±3)°С	–	≤ 0,01		
4. Емкость фотодиода, пФ	≤ 3	≤ 5	1,99	
5. Время нарастания и спада фронта импульса, нс	≤ 2	≤ 3	0,6/1,2	

Измерения проводили

Сделан на з-де п/п приборов в г. Черновцы — по разработке моск. НПО «Орион»

Наработка и сохраняемость

Минимальная наработка для изделий ФД3I2,ФД3I2Л- I0000 ч.Минимальный срок сохраняемости I2 лет. При этом параметры-критерии годности по ТУ3-3.2248-89.

Допустимые режимы эксплуатации

Допустимые режимы эксплуатации по ТУ3-3.2248-89

Сведения о содержании драгоценных материалов

Изделие содержит: золото,серебро

Сведения о содержании цветных металлов

Цветных мателлов не содержится

КОМПЛЕКТ ПОСТАВКИ

Наименование	Обозначение	Количество	Примечание
Изделие ФД3I2,ФД3I2Л	3.368.292 ТУ	I	
Паспорт	3.368.292 ПС	I	
Инструкция по эксплуатации	3.368.292 ИЭ		Количество оговаривается в договоре на поставку
Тара индивидуальная	АДБ4.170.027	I	

СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие типа ФД3I2,ФД3I2Л заводской № 1БУ1752 соответствует техническим условиям ТУ3-3.2248-89 и признано годным для эксплуатации

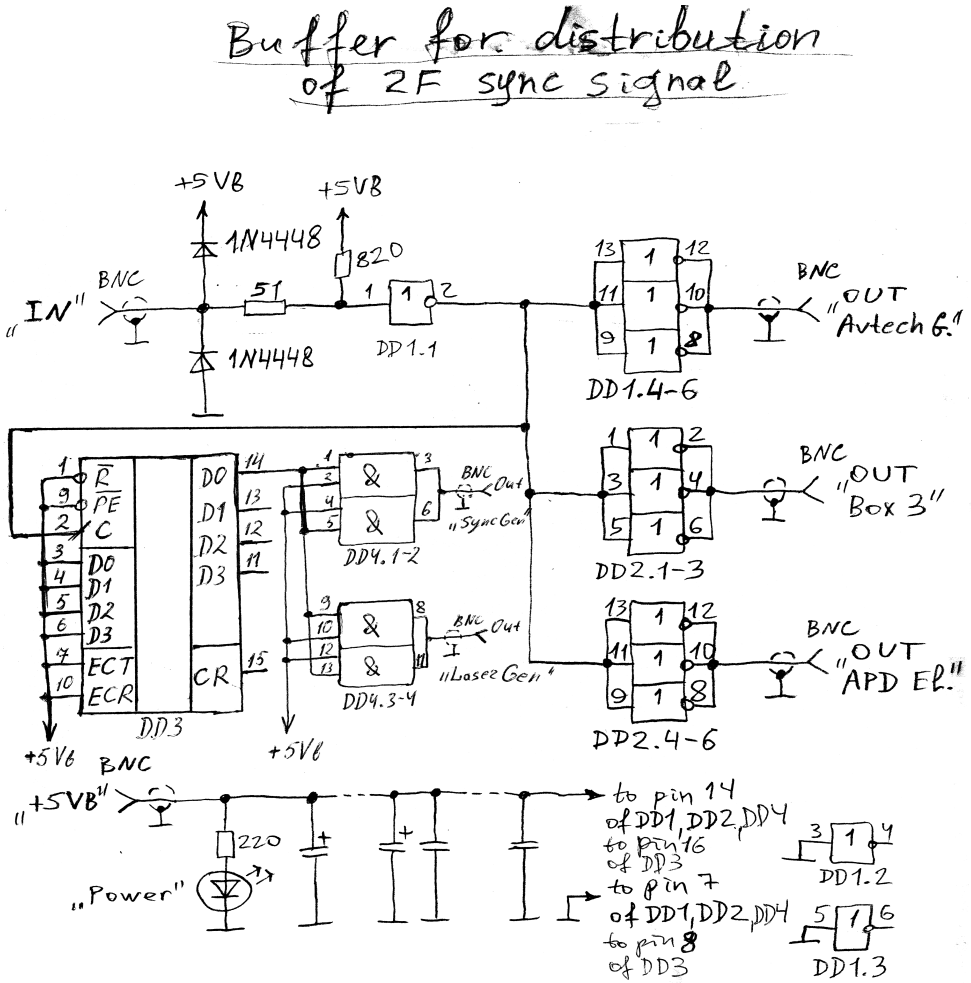
Дата приемки

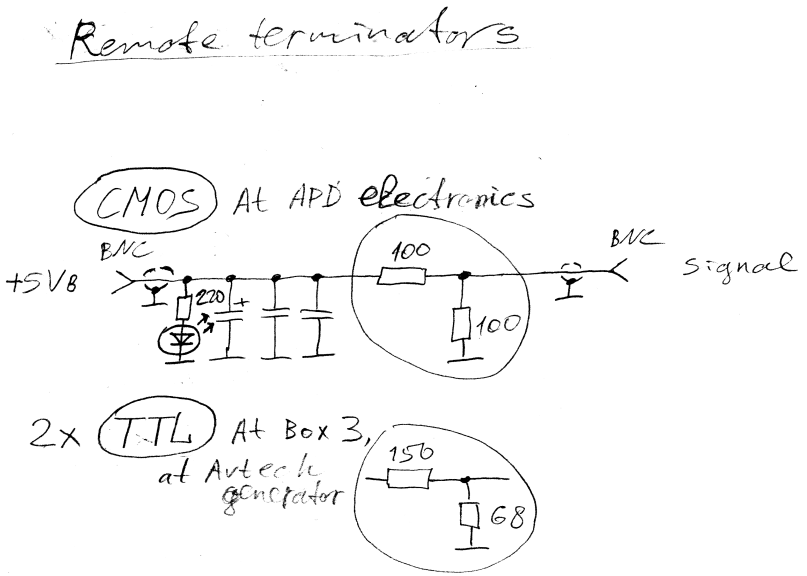
СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие типа ФД3I2,ФД3I2Л заводской № 1БУ1752 упаковано согласно техническим условиям ТУ3-3.2248-89.

Приложение 8 (Appendix 8)

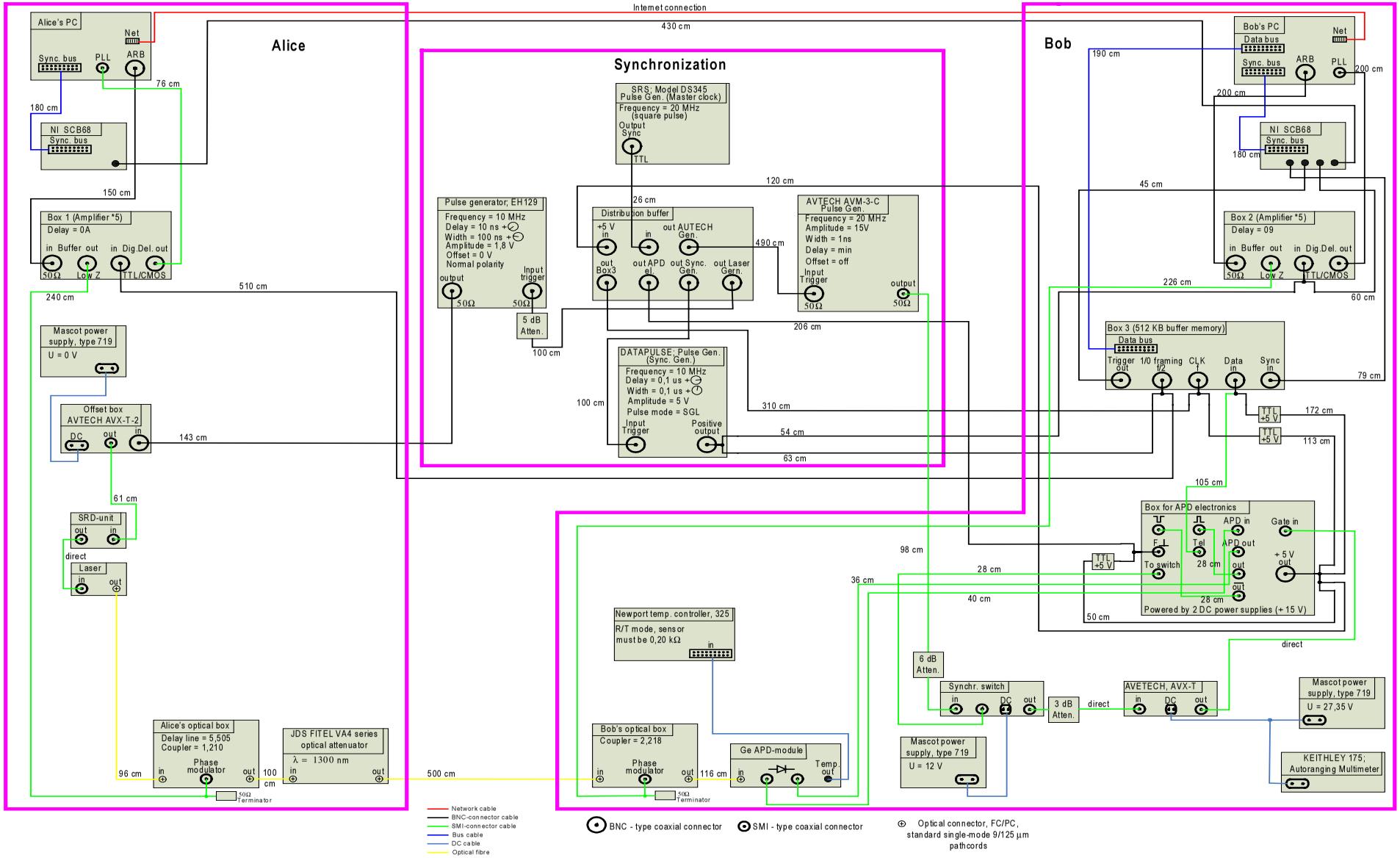
Schematic of the distribution buffer





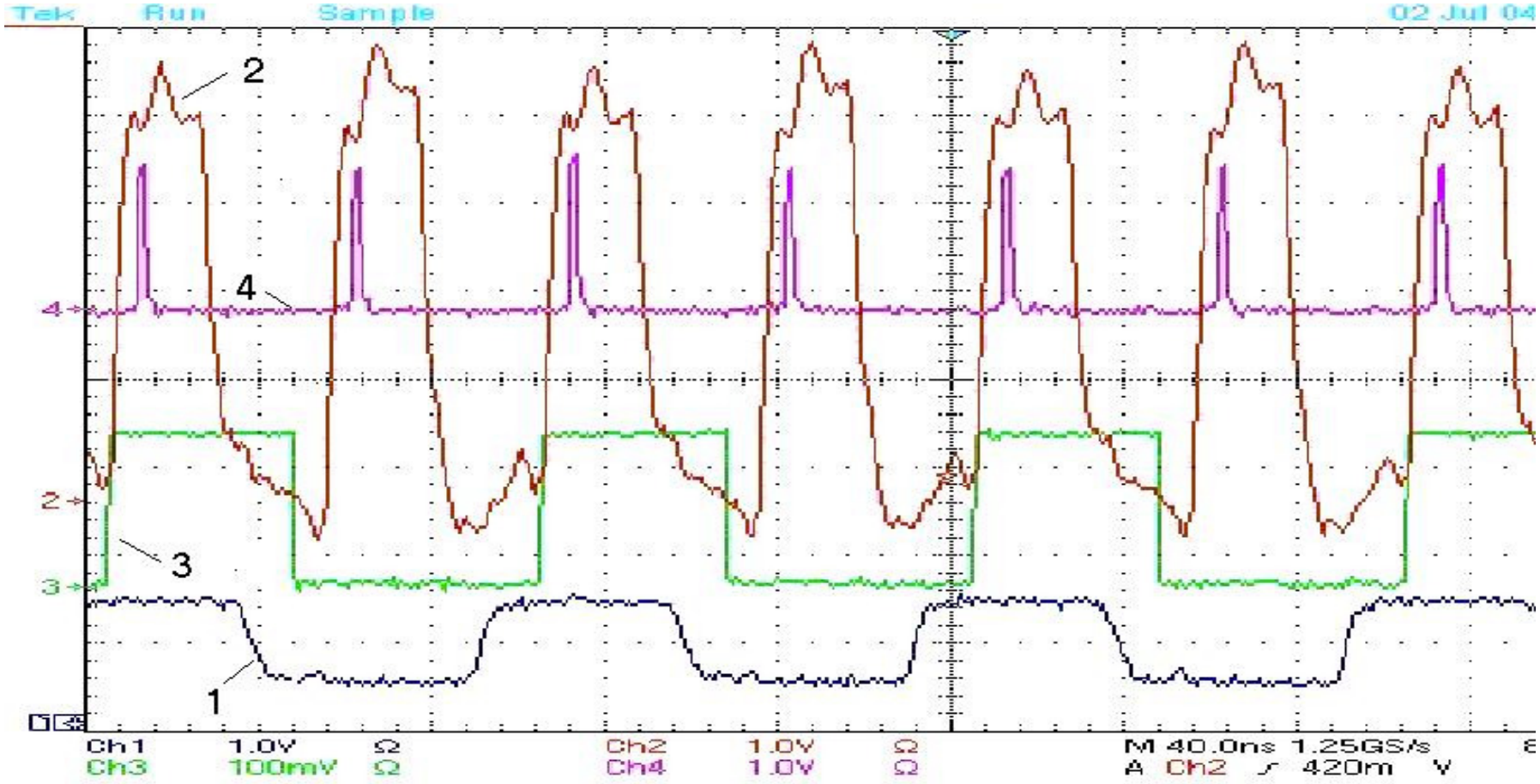
DD1, DD2 74AC04
DD3 74AC163
DD4 74AC08

Приложение 9 (Appendix 9). Quantum key distribution experiment. Interconnection diagram and equipment settings.



Приложение 10 (Appendix 10)

Synchronization of the generators



See legend on the next page.

Curves:

1 (Blue) – synchronization pulses 10 MHz; the output of Datapulse101 generator is connected to the oscilloscope using 1.12 m long cable and 9 dB attenuator;

2 (Red) – master clock generator signal 20 MHz; the signal was measured after the Distribution buffer at “Box 3 out” output, using 1.50 m long cable;

3 (Green) – pulses for the laser 10 MHz; the output of EH129 generator is connected to the oscilloscope using 1.12 m long cable and 20 dB attenuator;

4 (Magenta) – gate pulses 20 MHz; the output of AVTECH generator is connected to the oscilloscope using 1.20 m long cable and 18 dB attenuator;

This image was obtained using Tektronix TDS 7104 Digital Phosphor Oscilloscope.