МФТИ

Защита информации

Безопасная подводная связь на квантовом уровне

Петросян Акоб

14 декабря 2021 г.

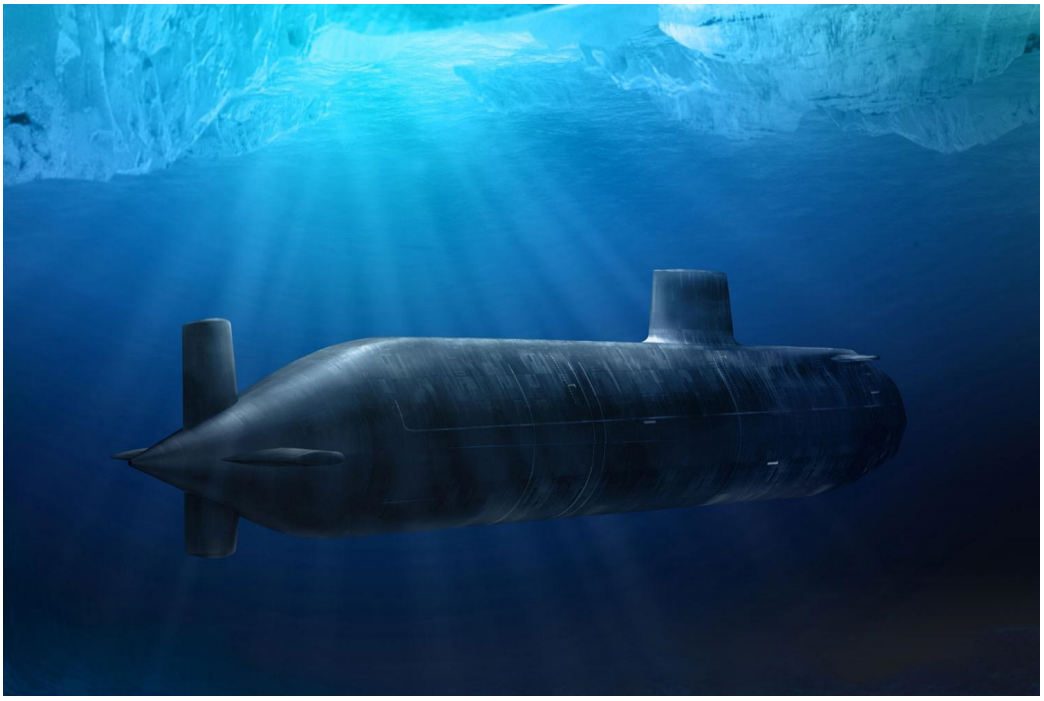

Рис. 1: Подводная лодка класса Astute Королевского флота является ударной подводной лодкой с ядерной установкой.

В этой обзороной статье рассмотрим некоторые из основных способов коммуникации подводных лодок. Изучим технологию квантового распределения ключей, которая позволяет подводным лодкам безопасно общаться как на глубине, так и на скорости.

Проблемы подводной связи

Подводная связь ограничена глубиной, на которой суда могут обмениваться информацией, и скоростью, с которой они могут делать это через воду.

Однако в последнее время исследователи добились впечатляющих успехов в решении этой дилеммы, используя технику под названием квантовое распределение ключей (КРК, *английский: QKD*).

КРК обещает гарантировать безопасную связь на основе принципов квантовой механики, не жертвуя скоростью и не заставляя подводную лодку подниматься ближе к поверхности.

Чтобы подводная лодка сохранила все свои тактические преимущества, она должна оставаться погруженной в смешанный слой, глуби-

на которого составляет от 60 до 100 метров, ниже которого гидролокаторы не могут их обнаружить. Подводная связь в настоящее время осуществляется под водой с использованием радиоволн ОНЧ(VLF) или КНЧ(ELF), потому что только очень низкие или крайне низкие частоты могут проникать в воду на этих глубинах.

Однако использование КНЧ и ОНЧ имеет ряд недостатков. Пункты передачи должны быть очень большими, а это означает, что подводная лодка должна буксировать громоздкие антенные кабели, плюс обычно она должна быть ориентирована на определенную ориентацию и снижать скорость для получения оптимального приема.

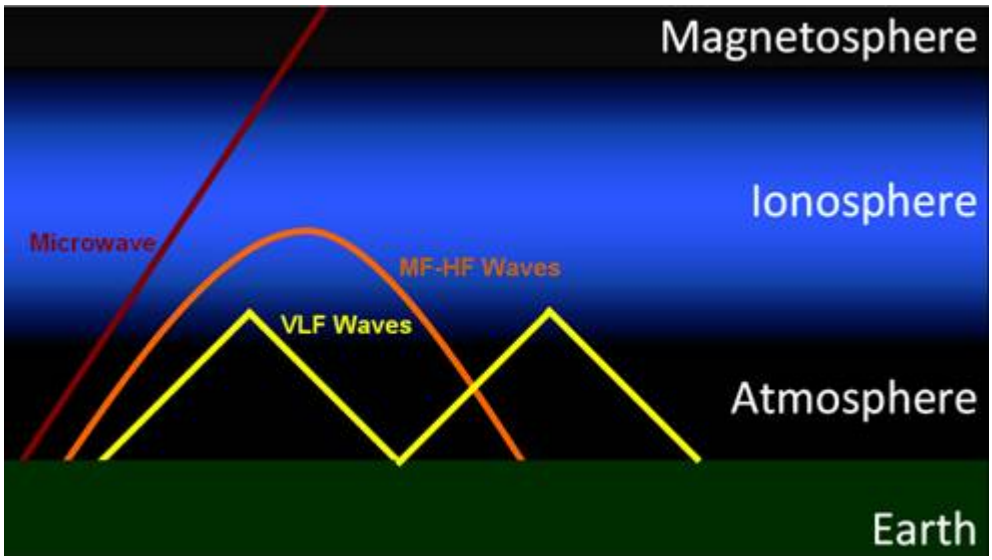

Рис. 2: ОНЧ волны

Частоты ОНЧ и КНЧ предлагают только очень низкую полосу пропускания: ОНЧ поддерживает несколько сотен бит в секунду, а КНЧ - всего несколько бит в минуту. Это предотвращает передачу сложных данных, таких как видео. Однако использование КНЧ и ОНЧ имеет ряд недостатков. Пункты передачи должны быть очень большими, а это означает, что подводная лодка должна буксировать громоздкие антенные кабели, плюс обычно она должна быть ориентирована на определенную ориентацию и снижать скорость для получения оптимального приема.

Частоты ОНЧ и КНЧ предлагают только очень низкую полосу пропускания: ОНЧ поддерживает несколько сотен бит в секунду, а КНЧ

- всего несколько бит в минуту. Это предотвращает передачу сложных данных, таких как видео.

Одним из возможных решений является осуществление оптической связи с помощью лазера, концепция, которая существует с 1980-х годов, когда проводились эксперименты, демонстрирующие возможность поддержания оптического канала между подводной лодкой и воздушной платформой.

Группа Quantum Technologies из компании ITT Exelis, специализирующейся на оборонных технологиях, рассматривает возможность сделать еще один шаг вперед, исследуя возможность лазерной оптической связи между подводной лодкой и спутником или бортовой платформой, защищенной с помощью квантовой информации.

Работа ITT Exelis для правительства США включает исследования по широкому кругу вопросов квантовой информации, включая разработку квантовых алгоритмов, квантовых датчиков и новых решений для систем квантовой связи.

Квантовое распределение ключей(QKD)

Квантовое распределение ключей - это безопасный метод связи, реализующий криптографический протокол, включающий компоненты квантовой механики, который позволяет двум сторонам создать общий случайный секретный ключ, известный только им, который затем может использоваться для шифрования и дешифрования сообщений.

Единицей квантовой информации является кубит, который представляет собой квантовое состояние фотона. Это может быть ноль, единица или любая суперпозиция нуля и единицы.

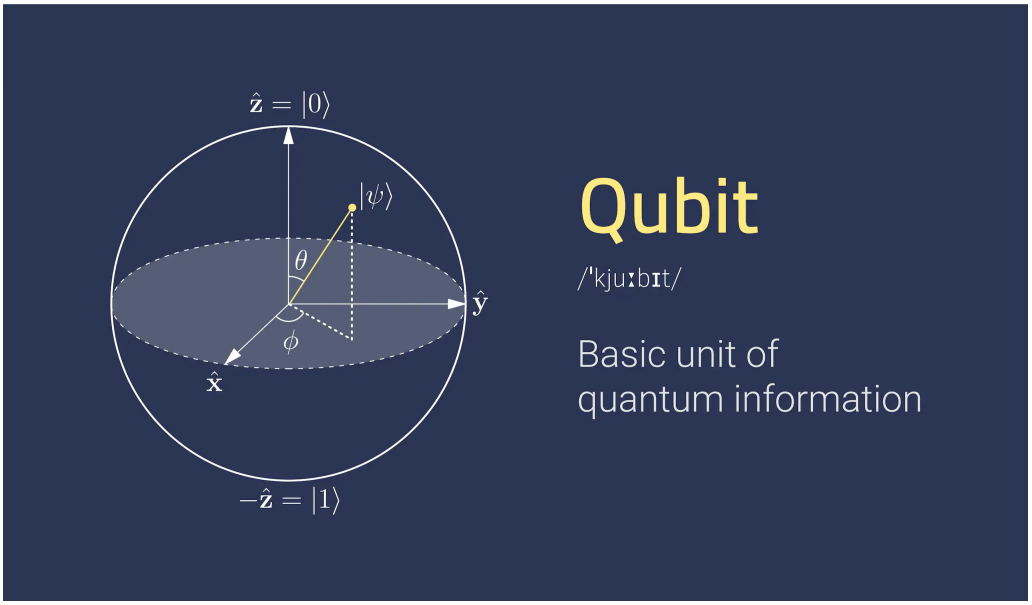

Рис. 3: кубит

Понятно, что кубит содержит в себе больше информации, чем классический бит.

Важным и уникальным свойством квантового распределения ключей является способность двух взаимодействующих пользователей обнаруживать присутствие любой третьей стороны, пытающейся получить информацию о ключе. Это является следствием фундаментального аспекта квантовой механики: процесс измерения квантовой системы в целом нарушает ее. Третья сторона, пытающаяся подслушать ключ, должна каким-то образом измерить его, тем самым создавая обнаруживаемые аномалии. Используя квантовые суперпозиции или квантовую запутанность и передавая информацию в квантовых состоянияхможет быть реализована система связи, обнаруживающая подслушивание.

Безопасность шифрования, использующего квантовое распределение ключей, опирается на основы квантовой механики, в отличие от традиционной криптографии с открытым ключом , которая опирается на вычислительную сложность определенных математических функций и не может предоставить никаких математических доказательств фактической сложности обращения используются односторонние функции. QKD обладает доказанной безопасностью, основанной на теории информации, и прямой секретностью .

Главный недостаток квантового распределения ключей заключается в том, что оно обычно зависит от наличия аутентифицированного клас-

сического канала связи. В современной криптографии наличие аутентифицированного классического канала означает, что либо уже произведен обмен симметричным ключом достаточной длины, либо открытые ключи достаточного уровня безопасности.

Квантовое распределение ключей используется только для создания и распространения ключа, а не для передачи каких-либо данных сообщения. Затем этот ключ можно использовать с любым выбранным алгоритмом шифрования для шифрования (и дешифрования) сообщения, которое затем может быть передано по стандартному каналу связи.

Итак, как мы поняли, квантовая связь включает в себя кодирование информации в квантовых состояниях (кубитах). Обычно для этих квантовых состояний используются фотоны. Квантовое распределение ключей использует определенные свойства этих квантовых состояний для обеспечения своей безопасности. Существует несколько различных подходов к квантовому распределению ключей, но их можно разделить на две основные категории в зависимости от того, какое свойство они используют.

- **Протоколы на основе измерений**
  В отличие от классической физики, акт измерения является неотъемлемой частью квантовой механики. В общем, измерение неизвестного квантового состояния каким-то образом меняет это состояние. Это является следствием квантовой неопределенности и может быть использовано для обнаружения любого перехвата связи (что обязательно включает измерение) и, что более важно, для вычисления количества перехваченной информации.

- **Протоколы на основе запутывания**
  Квантовые состояния двух (или более) отдельных объектов могут быть связаны вместе таким образом, что они должны описываться комбинированным квантовым состоянием, а не как отдельные объекты. Это называется запутыванием и означает, что, например, измерение одного объекта влияет на другой. Если запутанная пара объектов используется совместно двумя сторонами, любой, кто перехватывает любой из них, изменяет систему в целом, показывая присутствие третьей стороны (и объем полученной информации).

Оптическая связь

Технология КРК уже существует и коммерчески доступна, но в настоящее время она осуществляется через оптическое волокно, а не через

фотоны, свободно перемещающиеся через воздух или воду.

Совсем недавно на Канарских островах был проведен эксперимент, где впервые установили базу КРК на расстоянии 144 км, показав, что возможно иметь эту квантовую связь в свободном пространстве.

Помимо проблем, связанных с передачей фотонов через воду и свободный воздух, исследователям необходимо установить лазерную связь между передатчиком и приемником на спутниковой или бортовой платформе.

В настоящее время этим занимается команда QinetiQ North America, которая разрабатывает специализированную систему отслеживания.

Как только оптическая связь между подводной лодкой и спутником установлена, работа исследователей ITT Exelis берет верх, исследуя, как включить протокол КРК для защиты связи. Это делается с помощью фотодатчика, работающего в так называемом режиме Гейгера, что фактически означает, что он считает фотоны, приходящие с определенной поляризацией.

ПО сути, для передачи квантовой информации нужно что-то, что поляризует фотоны, поэтому квантовое состояние будет в заданном базисе, и иметь фильтр, который обнаруживает это в передатчике и приемнике.

Использовать обычные лазеры нельзя, поскольку нам нужны специальные фотонные лазеры, которые похожи на очень разбавленный лазер. Они посылают по одному фотону за раз, и каждый фотон имеет четко определенное квантовое состояние.

Технико-экономические обоснования

На следующем этапе программы военно-морская исследовательская лаборатория США проведет серию экспериментов, чтобы установить, насколько хорошо сохраняется квантовое состояние фотона при его прохождении через воду, чтобы проверить точность теоретического технико-экономического обоснования ITT Exelis.

Если эксперименты подтвердят теоретическую модель и исследования перейдут к следующему этапу, экспериментальный прототип может быть создан в течение пяти лет. Однако на столь радикальный новый подход влияет ряд факторов.

«Это не только научно-технический вопрос, но также связан с уровнем финансирования и политикой», - заявил Ланзагорта.

Однако, если власть имущие все же доведут дело до конца, выгоды могут быть существенными. Предлагаемая система потенциально могла бы обеспечить совершенно безопасную передачу, высочайший доступный

уровень безопасности, со скоростью до 170 кбайт в секунду, что примерно в 600 раз больше пропускной способности, чем способны нынешние системы ОНЧ, легко справляясь со сложными данными, такими как видео.

Кроме того, не было бы потери эксплуатационной эффективности или скрытности для самой подводной лодки, поскольку в принципе ей не нужно было бы замедляться, оставаться на глубине менее 100 м или менять ориентацию для обмена данными.

Однако весь успех зависит от того, как путешествие в воде влияет на фотон. Самая большая проблема состоит в том, чтобы увидеть, как лучше всего послать импульсы одиночных фотонов таким образом, чтобы квантовое состояние было защищено, даже если оно проходит через воду. Нужно найти способ выполнить своего рода кодирование, такое как кодирование с исправлением ошибок, которое защищает квантовое состояние фотона, чтобы мы могли иметь больший диапазон операци.

Литература

1. Stanford VLF Group: *What is ELF/VLF Research?*
2. Naval technology (30.01.2020): *Deep secret – secure submarine communication on a quantum level*
3. Wikipedia[electronic resource] (14.12.2021): Quantum entanglement
4. Wikipedia[electronic resource] (14.12.2021): Сверхдлинные волны
5. Wikipedia[electronic resource] (14.12.2021): Quantum key distribution