МФТИ

Защита информации

Безопасная подводная связь на квантовом уровне

Петросян Акоб

19 декабря 2021 г.

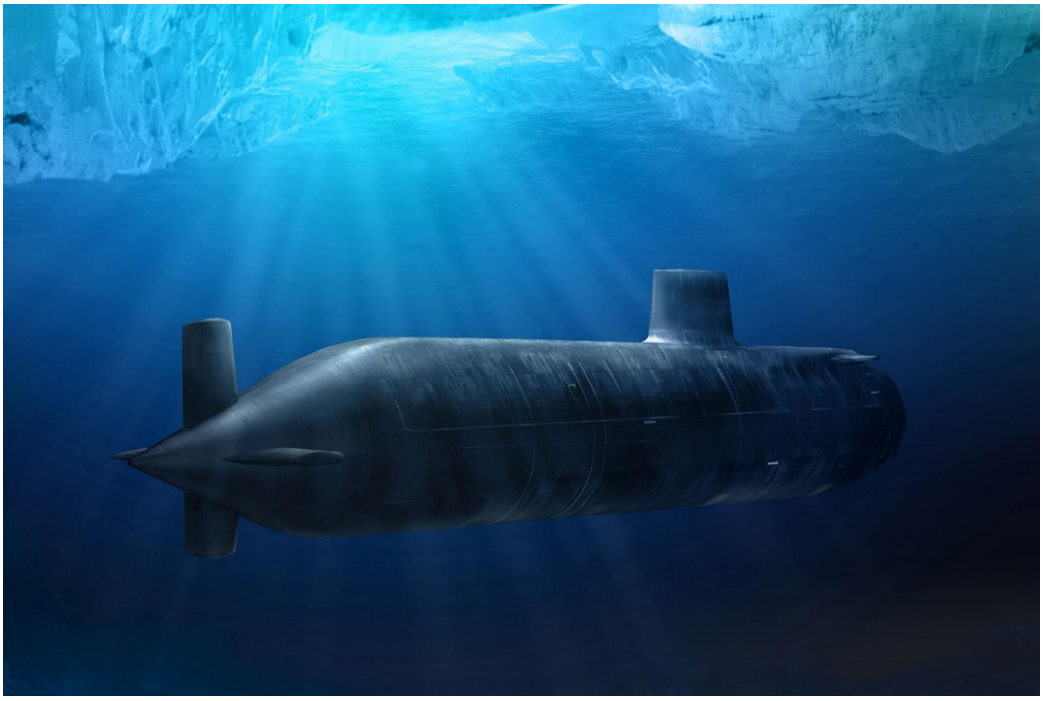

Рис. 1: Подводная лодка класса Astute Королевского флота является ударной подводной лодкой с ядерной установкой.

В этой обзорной 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

Чтобы оставаться не замеченной от гидролокаторов подводная лодка должна находиться на глубине от 60 до 100 метров. Но поддерживать подводную связь между подлодками или подлодками и базой довольно затруднительно, так как обычные радиоволны очень быстро поглощаются уже на глубине несколько десятков метров. Поэтому вместо "обычных"радиоволн используются волны с очень низкими или крайне низкими частотами(далее ОНЧ и КНЧ). Это волны, которые хорошо проникают вглубь воды, отражаются от ионосферы Земли и слабо поглощаются земной поверхностью.

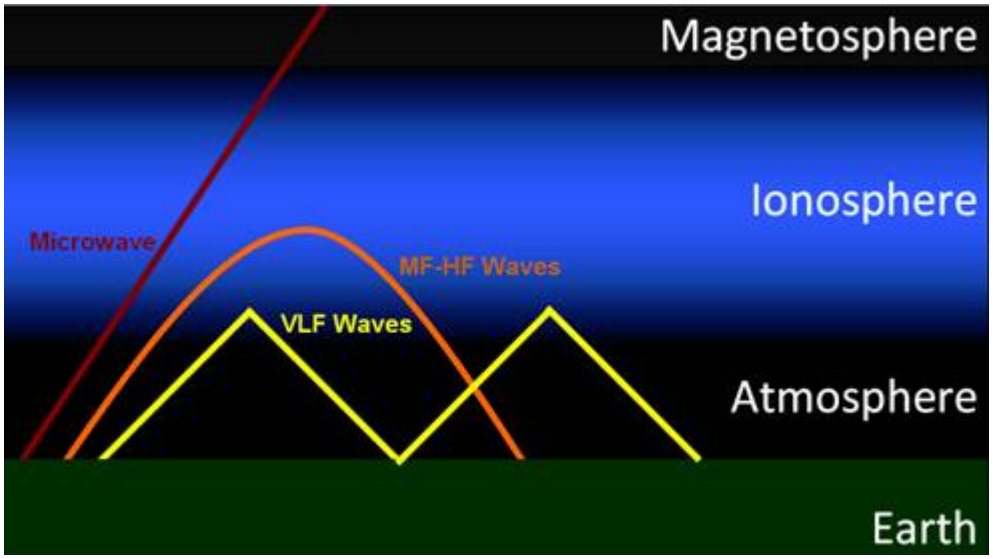

Рис. 2: ОНЧ волны

Слабости такого подхода состоят в том, что чаще всего лодке надо буксировать огромные кабели-антены над водой, которых легко заметить с самолётов. Да и двигаться лодка может только с очень низкой скоростью, в определенном направлении.

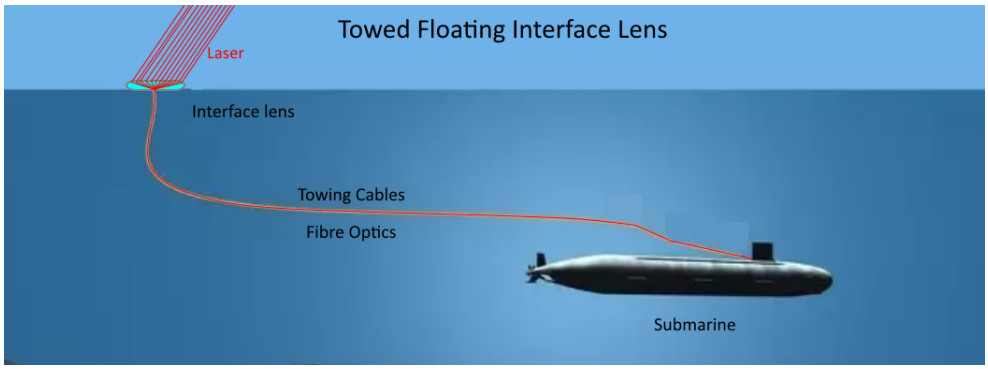

Рис. 3: ОНЧ волны

Хвастаться скоростью передачи такой метод тоже не может, так как ОНЧ и КНЧ предлагают только очень низкую полосу пропускания: ОНЧ поддерживает несколько сотен бит в секунду, а КНЧ - всего несколько бит в минуту.

Учитывая все эти недостатки, исследователи предлагают использовать технику под названием квантовое распределение ключей (КРК, *ан-*

глийский: QKD), с помощью которой сумели добиться впечатляющих успехов не жертвуя скоростью и не заставляя подводную лодку подниматься ближе к поверхности. При этом безопасность связи гарантируется принципами квантовой механики.

Что касается вида канала связи, ещё в 1980-х годах, были эксперименты, демонстрирующие способ поддержания оптического канала между подводной лодкой и воздушной платформой, используя оптическую связь с помощью лазера.

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.

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.

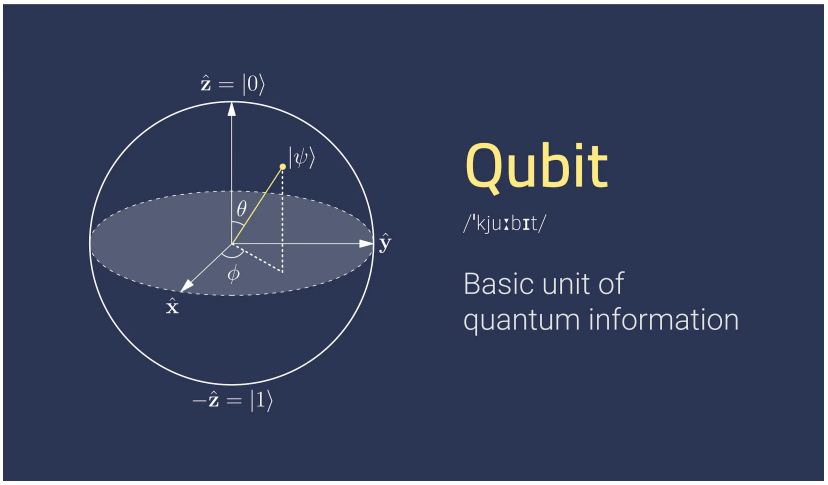

Рис. 4: кубит

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 состояниях, может быть реализована система связи, обнаруживающая подслушивание.

Традиционная криптография с открытым ключом , которая опирается на вычислительную сложность определенных математических функций и не может предоставить никаких математических доказательств фактической сложности обращения. В отличее от неё безопасность шифрования, использующего квантовое распределение ключей, опирается на основы квантовой механики и 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 классического 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.

Заключение

Проведя итоги, скажу, что технология КРК имеет хорошую перспективу и в будущем, когда будут решены перечисленные выше проблемы (оптическая связь, защита от искажения состояния кубитов), можно будет добиться впечатляющих результатов, а именно невидимости подводной лодки, защищенного канала связи и высокой скорости передачи.

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*