ПЛИС — СКОРОСТНАЯ ОБРАБОТКА СИГНАЛА. УЧЕБНО-ИССЛЕДОВАТЕЛЬСКАЯ ГИБРИДНАЯ СХЕМА

ВАДИМ РОДИМИН
СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ГРУППЫ КВАНТОВЫХ КОММУНИКАЦИЙ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА

В ЧЕМ СИЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА?

Надо сказать несколько слов об ограничениях в квантовом распределении ключа. В том, что мы не можем подслушать, считать и перехватить квантовое состояние. Но ведь из-за этого мы не можем и усилить квантовое состояние.

В обычных телекоммуникационных каналах у нас идут какие-то импульсы, и их усиливают время от времени, чтобы они прошли тысячи километров. Мы усилитель использовать не можем, в частности из-за того, что невозможно клонировать импульс. И это слабость, потому что мы ограничены по длине передачи квантового ключа. В принципе, импульсы идут, достаточно слабые, причем не все доходят до адресата. И даже с этим можно работать, часто отправляя эти импульсы, и самая малая часть все же будет доходить. Но чем дальше, тем больше и больше шансов не дойти до конца. Квантовая криптография заканчивается.

КАК ЖЕ МОЖНО ЕЕ УСИЛИТЬ?

Например, использовать квантовые повторители, которые, правда, пока еще не сделаны и существуют только в лабораториях. Квантовые повторители телепортируют квантовое состояние. Передачу по оптоволокну можно еще больше удлинить при помощи обычных детекторов одиночных фотонов. Но тут уже свои издержки: у каждого детектора есть свой шум, который изредка «кликает» даже когда фотона нет.

Тем не менее, мы можем попытаться обойти все это. Например, сделать линию связи с доверенными серверами. Каждый сервер передает информацию на определенном расстоянии другому серверу, тот — третьему и т. д. Таким сквозным образом можно передать один и тот же ключ.

Но ведь нам нужно передавать ключ достаточно быстро. В этом случае лучше всего использовать алгоритм одноразовых блокнотов.

КАК ЖЕ РАСПРЕДЕЛЯТЬ КВАНТОВЫЙ КЛЮЧ?

Распределение квантового ключа нормально заработало только последние 10 лет. Почему? Вот какой нюанс: нам нужно быстро обрабатывать оптические и электрические сигналы, увеличивать частоту этих сигналов, потому что нам важно, чтобы ключ генерировался быстро. А технологии доросли до такой скорости обработки сигналов только в последнее десятилетие. Эта технология называется обработкой сигналов на уровне ПЛИС.

ПЛИС (FPGA) — программируемые логические интегральные схемы, позволяющие контролировать процессы в режиме реального времени.

КАК РАБОТАЕТ ПЛИС?

Представим обычный компьютер, где есть операционная система, работающая с использованием процессора. Эта ОС работает не в реальном времени, поэтому для скоростной обработки сигналов она не годится. ПЛИС по виду такой же, как процессор, но только его можно сделать под свою задачу. В ПЛИСЕ миллиарды логических элементов, из которых можно написать программу для его прошивки. Задачи будут выполняться одновременно. И квантовая криптография — именно то самое, для чего идеально может использоваться ПЛИС.

Мы в нашей группе разработали установку для учебных целей и прототипирования идей, связанных с квантовой криптографией и не только. Эта установка представляет собой материнскую плату, на которой есть ПЛИС, занимающийся как раз обработкой сигналов. Материнская плата соединена с компьютером, в который вставлена плата National Instruments, которую можно программировать с помощью языка LabVIEW. Мы использовали нашу установку для реализации многих идей.

Вообще, квантовая криптография – довольно обширная область, которая вобрала в себя много знаний из электроники, математики, физики. Поэтому, если вы хотите понять ее хорошо, то читайте много дополнительного материала.