Квантовый параллелизм

Переходя к разговору о квантовой криптографии, можно отметить, что единицу квантовой информации называют кубит.

Если классический бит информации может находиться в двух состояниях: 0 и 1, то в противоположность ему квантовые биты одновременно находятся в суперпозиции своих состояний.

Они могут одновременно быть и 0, и 1 с некоторыми амплитудами альфа и бета. Они могут задаваться в произвольной точке, которая интерпретирует состояние квантового бита, и находится на сфере Блоха.

Можно сравнить кубит с летящей в воздухе монетой. Монета летит в воздухе и крутится, и вы не знаете, как она упадет — орлом или решкой. Но как только вы поймаете ее, она окажется в одном из двух состояний.

Похожая ситуация и с квантовым битом. Пока кубит участвует в процессе преобразований, вычислениях, он находится в произвольной позиции, точнее, одновременно в одном из базовых своих состояний: 0 или 1. Как только его измерят, то спроецируют на одно из базовых состояний. Такова особенность квантовой формации.

Благодаря тому, что квантовый бит может быть и 0, и 1, появляется понятие квантового параллелизма. Вычисляя некоторую функцию, аргумент которой задается квантовыми битами, аргументы одновременно принимают все свои возможные значения.

И вычисляя эту функцию на аргументах, вычисляются все аргументы сразу. Это и есть квантовый параллелизм, который во многих случаях обеспечивает преимущества квантовых вычислений.  
Классический пример и простая иллюстрация квантовых вычислений — это алгоритм Дойча-Йожи. Интерпретировать этот алгоритм можно следующим образом.

Как узнать, фальшивая монета или настоящая? Как это можно проверить? Мы смотрим на монету с одной стороны, переворачиваем на другую и видим, что она фальшивая или настоящая.

В квантовом случае мы можем создать суперпозицию состояния монеты, посмотреть на нее один раз и сразу узнать, фальшивая она или нет.

Настоящий значимый пример превосходства квантовых вычислений перед классическими обнаружили в 1994 году.

В этот год Питер Шор предложил эффективный алгоритм разложения числа на множители. Это стало бы возможным, если бы был создан квантовый компьютер и тогда можно было бы взламывать соответствующие протоколы.