**Quantum Entanglement**

**Definition:**

* A quantum phenomenon where two or more particles share a linked quantum state.
* Measuring one particle’s property instantly determines the other’s property, regardless of distance.

**Key Features:**

* **Non-locality:** Changes in one particle affect the other instantly (“spooky action at a distance” – Einstein).
* **Indivisible State:** The system is described by a combined wavefunction that cannot be split into separate states.
* **Example State:**

∣ψ⟩=∣01⟩+∣10⟩2|\psi\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}∣ψ⟩=2​∣01⟩+∣10⟩​

* **Bell States:** Special maximally entangled two-qubit states used in quantum information science.

**Experimental Verification:**

* Alain Aspect’s 1982 experiment showed violations of Bell’s inequalities, confirming entanglement.

**Applications:**

* **Quantum teleportation** – transferring quantum states.
* **Quantum cryptography** – secure communication using entangled particles.
* **Quantum computing** – enables faster algorithms through correlated qubits.

**Significance:**

* Proves that quantum systems can act as a single entity over large distances.
* Essential for the development of future quantum technologies.

**Application of QFT – Shor’s Algorithm for Integer Factorization**

One of the most famous and impactful applications of the Quantum Fourier Transform (QFT) is in Shor’s algorithm, which is used to factor large integers efficiently. Classical algorithms for factoring large numbers require exponential time, but Shor’s algorithm, using QFT, can solve the problem in polynomial time.

The key step in Shor’s algorithm is period finding. Given an integer NNN to be factored, the algorithm picks a random integer aaa (coprime to NNN) and studies the function:

f(x)=ax (mod N)f(x) = a^x \ (\text{mod} \ N)f(x)=ax (mod N)

This function is periodic, and its period rrr is used to determine the factors of NNN. The QFT is applied to the quantum state encoding f(x)f(x)f(x), which transforms the state into the frequency domain. In this representation, the period rrr appears as peaks in the probability distribution when the state is measured.

Once rrr is found, the algorithm uses the relationship between rrr and NNN to compute non-trivial factors of NNN. This is significant because RSA encryption – widely used in internet security – relies on the difficulty of factoring large numbers. QFT’s role in making period finding exponentially faster is what enables Shor’s algorithm to potentially break RSA.

Thus, the Quantum Fourier Transform acts as the mathematical engine behind Shor’s algorithm, providing the speed-up necessary for solving a problem that is otherwise intractable for classical computers, and making it a cornerstone of quantum algorithms with major implications for cryptography and cybersecurity.