Chapter 14
Enhancing Quantum Random Number Generators, Cryptographic Security, and Machine Learning–Based Cryptoanalysis

U. Jayalatsumi
https://orcid.org/0000-0001-5642-0010
Dr. M.G.R. Educational and Research Institute, India

T. Godhavari
Dr. M.G.R. Educational and Research Institute, India

Borra Keerthana
Dr. M.G.R. Educational and Research Institute, India

R. Rahul
Dr. M.G.R. Educational and Research Institute, India

B. Swapna
https://orcid.org/0000-0002-7186-2842
Dr. M.G.R. Educational and Research Institute, India

ABSTRACT

Randomness is essential in cryptography for key generation and secure information exchange, ensuring confidentiality and protection. Quantum Random Number Generators (QRNGs) leverage quantum mechanics to produce truly random numbers, offering a major advantage over Pseudo Random Number Generators (PRNGs), which are slower and less secure due to their deterministic nature. Quantum computing boosts QRNG efficiency, making them ideal for cryptographic applications, such as secure key exchange and encrypted communication. QRNGs generate stronger encryption systems by utilizing quantum phenomena like Bloch sphere rotations. The integration of machine learning (ML) with QRNGs

DOI: 10.4018/979-8-3693-8332-2.ch014

further enhances their effectiveness, optimizing random sequences for improved speed and security. This combination of QRNGs and ML provides a powerful approach to cryptography, ensuring more secure communication channels and better protection against potential attacks.

1. INTRODUCTION

Over the years, computers have become smaller and faster due to the shrinking size of their electronic components. This miniaturization has allowed more powerful processors to fit into smaller devices, following a trend known as Moore's Law. However, this process of making transistors—the tiny switches that control the flow of electricity in a computer—smaller is reaching a physical limit. As these transistors approach the size of just a few atoms, they start to behave according to the rules of quantum mechanics, rather than classical physics, which creates new challenges for the future of computing (Marsaglia, 2002 & Rodriguez-Henriquez, 2007).

Electricity is simply the movement of electrons through a material, and transistors control this flow by either allowing electrons to pass through or blocking them. In classical computing, this control forms the basis of how computers process information using binary code—1s and 0s (Stipčević, 2004 & 2007). But when transistors become extremely small, strange quantum effects start to occur. One such effect is quantum tunneling, where electrons can pass through barriers even when, in theory, they shouldn't be able to (Kumar, V at al., 2020). This can cause transistors to malfunction because the electrons can unexpectedly appear on the other side of the barrier, making it difficult to maintain reliable on/off states, which are essential for traditional computing (Kumar, V. V et al., 2002).

Quantum mechanics, the branch of science that studies the behavior of particles at extremely small scales, reveals that particles like electrons do not behave in predictable ways. For example, a particle can be in more than one state at the same time, a phenomenon known as superposition. This means that instead of being either a 0 or a 1, as in classical computing, a quantum particle can be both at the same time until it is observed. This property is the foundation for qubits, the quantum version of bits in classical computers, which allows quantum computers to perform many calculations at once, vastly increasing their potential power (Lydersen et. al., 2010 & 2011).

Another important concept in quantum mechanics is entanglement, where particles become connected in such a way that the state of one particle is directly linked to the state of another, even if they are far apart. This means that measuring the state of one particle will instantly determine the state of the other, no matter the distance between them. This phenomenon, which Albert Einstein called “spooky action at a distance,” defies the usual understanding of how particles interact but offers exciting possibilities for quantum communication and computation.

As we approach the physical limits of how small transistors can get, researchers are looking toward quantum computing as the next big leap in technology. Quantum computers use the principles of superposition and entanglement to process information in ways that classical computers cannot, allowing them to solve complex problems much faster. Quantum computing could lead to breakthroughs in fields such as cryptography, medicine, and materials science, solving problems that would take traditional computers far too long to calculate (Ritter, 2002).

However, building quantum computers is incredibly difficult. Quantum systems are very sensitive to their surroundings, and any small disturbance can cause them to lose their quantum properties, a problem known as decoherence (Gottesman, 2004 & Jennewein, 2000). Scientists are working to overcome these