

Pseudorandom Generations in a Quantum Computing Setting

Danny Castonguay , Jean-Raymond Simard.

Abstract: As quantum computers may become a reality in the near future, it is interesting to test classical theory in the quantum setting. We will introduce basic notions of quantum computing by exploring the following fundamental concepts: qubits, Q-gates, Q-circuits, Q-algorithms. Then, we will do a brief overview of an article from Hastad, Impagliazzo, Levin and Luby, "A pseudo-random generator from any one-way function". In conclusion, we will present the reduction in two different quantum settings, and see if the result holds.