Department of Electrical and Computer Engineering

TEXAS TECH UNIVERSITY
Edward E. Whitacre Jr.
College *of* Engineering

Fall 2025 Seminar Series

Seminar Title: ***Restricted Eavesdropping Analysis of Quantum Cryptography***

Time: 3:00-3:50 PM, Monday, Nov. 3, 2025

Location: ECE 101

Speaker:
Ziwen Pan
Computer Science Department, TTU

Abstract:
Quantum computing is a fast-developing field, posing critical threats to the modern cryptography system. Thus, research in quantum cryptography is of great importance for near-term applications. However, traditional security analysis of quantum cryptography assumes that the eavesdropper is omnipotent, with her "abilities" only limited by the laws of quantum physics. This is unrealistic since the eavesdropper will be subject to certain reasonable limitations, same as the communication parties. In this seminar Ziwen will introduce his work on "Restricted Eavesdropping Analysis of Quantum Cryptography", which extended traditional quantum cryptography analysis to analyze a more realistic scenario where the eavesdropper is with a limited power collection ability. Such a restricted-eavesdropping scenario is highly applicable to wireless links such as microwave or free space optics ones. The talk will start with the theory model of a quantum wiretap channel to establish lower bounds and upper bounds based on Hashing Inequality and Relative Entropy of Entanglement. Applications to realistic channel conditions will also be introduced where the eavesdropping and defense strategies from both sides are investigated. Analytical and numerical conclusions will be discussed during the seminar.

Speaker Bio:
Dr. Ziwen Pan is currently an assistant professor at Computer Science department at Texas Tech University. He obtained his Ph.D. degree at the Electrical & Computer Engineering department from the University of Arizona in 2022. His major research work focuses on quantum communication/cryptography, including security analysis of generic quantum cryptography schemes and protocol designs for quantum key distributions. He has also worked on other topics such as entanglement-assisted communication and quantum simulation.