# Quantum Cryptography – Security at Birth

*Paul Wang*
*TSYS Endowed Chair in Cybersecurity*
*Columbus State University, USA*

The need for secure communication has grown tremendously in the past few decades, and as computing power becomes cheaper, the value of more secure alternatives to traditional methods of encrypting information has similarly increased.

Quantum cryptography offers the possibility of theoretically perfect security based on the principles of quantum mechanics, ensuring that the presence of an eavesdropper will be detected before any sensitive information is transmitted. However, the commercial relevant technology is still under development and in an immature state. The protocols used to implement secure communications with quantum hardware may still to be improved.

While physical experiments will always be necessary, simulations based on robust models can provide the opportunity to study many different communications protocols and hardware configurations, leading to new methods of implementing quantum cryptography and suggesting the most promising paths to pursue in the development of new hardware.

This paper discusses Quantum Cryptography foundation, followed by introducing different protocols and tools in quantum crypto simulation. The crypto key distribution, the use of quantum crypto technology in detecting and preventing eavesdropper, and an application of quantum crypto system - DARPA Quantum Network are discussed in detail.