Quantum Cryptography: Opportunities and Challenges

David Nelson and Abhishek Parakh, *University of Nebraska at Omaha*

Quantum cryptography promises to do what classical cryptography can never achieve: provide a perfectly secure means to communicate over public channels. However, physical implementations of quantum cryptographic schemes suffer from numerous roadblocks from difficulty in implementing single-photon emitters to ensuring that signal-to-noise ratio is low enough to enable detection of an eavesdropper. In this paper, we discuss the current state of quantum cryptography and the challenges it faces. We will detail the most popular protocols and latest attacks against them. Then, we take a step back and discuss whether the current drive towards implementing single-photon emitters is justified or an entirely new method may be worthy of investigation. Finally, we discuss some of the benefits that threshold cryptography can provide in making non-ideal implementations of quantum cryptography secure.