SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF DESIGN AND ENGINEERING
Website: https://cde.nus.edu.sg/ece

Area: Microwave & Radio Frequency

Host: Assoc Prof Charles Lim Ci Wen

TOPIC	**:**	**Improved Coherent One-Way Quantum Key Distribution For High-Loss Channels**
SPEAKER	**:**	**Mr Lavie Emilien Claude** **Graduate Student, ECE Dept, NUS**
DATE	**:**	**Wednesday, 20 April 2022**
TIME	**:**	**4.00PM to 5.00PM**
WEBINAR	**:**	**Join Zoom Meeting** **https://nus-sg.zoom.us/meeting/register/tZMlcOiuqDIjHt3a4M4uretQ-mFPoSS8vS5Q**

ABSTRACT

The coherent one-way (COW) quantum key distribution (QKD) is a highly practical system that has been widely deployed in many industry sectors. However, despite its simplicity and widespread use, the security of COW-QKD is still an open problem. This is largely due to its unique security feature based on inter-signal phase distribution, which makes it very difficult to analyze using standard security proof techniques. In this talk, we will review the current understanding of COW-QKD and highlight a new security analysis based on the universal squashing framework proposed in Ref.[1] and numerical methods. The proposed protocol is the same as the original protocol, except for (1) an additional vacuum tail signal that is needed to keep the protocol in the IID setting and (2) a balanced beam-splitter is used to decide passively the measurement basis. Remarkably, we show that by further modifying the intensity of the test signal, the proposed protocol can achieve quadratic scaling (in terms of the channel transmittance). We also analysed another modification proposed recently in Ref.[2]: if a fourth signal state composed of vacuum pulses only is sent, then the overall performance is significantly improved and a quadratic scaling is also achievable. These results match the recent upper bounds found for the original protocol in Ref.[3] and the secret key rate of coherent-state Bennett-Brassard 1984 QKD. Our findings therefore suggest that production-grade COW-QKD systems in deployment today could still be deployed in high loss optical networks with basic software and hardware modifications.

BIOGRAPHY

Emilien Lavie received his M.Eng. degree in 2018 from Telecom ParisTech (France) in Communication Engineering. He is currently pursuing the PhD degree with the Department of Electrical and Computer Engineering, National University of Singapore. His research interests include design and security analysis of quantum cryptography protocols for secure communication.