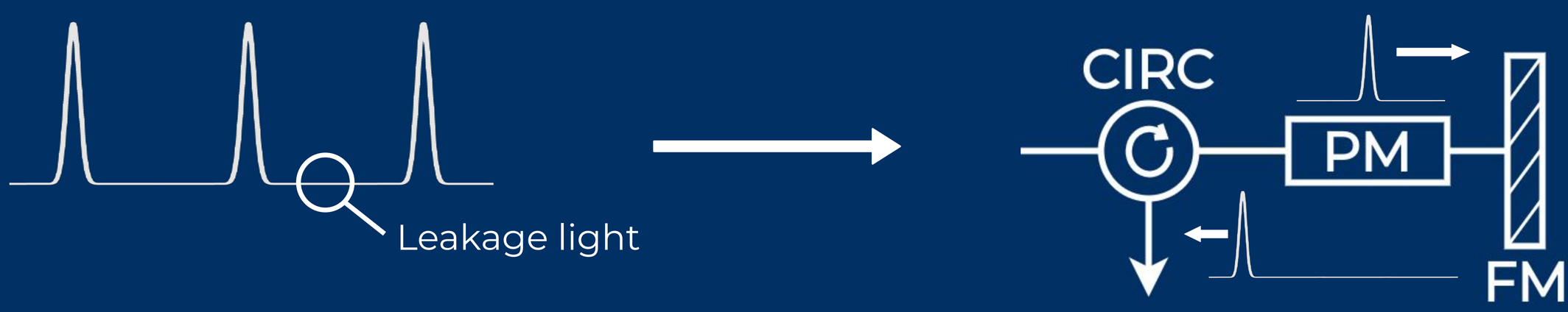
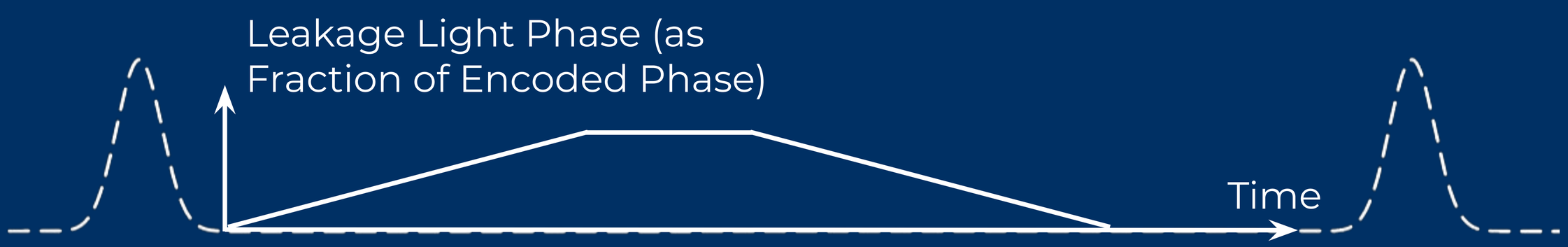
Incorporating passive time-dependent information leakage into QKD security proofs?

Although quantum key distribution (QKD) promises unconditional security [1], practical encoded signals from the source deviate from the theoretical requirements. Hence, these signals are often a source of passive information leakage. In practice, different experimental setups require different quantum optical models to describe this passive information leakage and how it varies in time (/frequency/etc.) across optical pulses. Previous work on side channels focused on active attacks by an adversary and specific models for passive side channels. [2] We demonstrate that a recently developed numerical security proof technique using semidefinite programming [4] can easily incorporate *any* arbitrary time varying model.

CASE EXAMPLE - NOVEL passive source side channel when using a Faraday mirror for stable bit (phase) modulation [5].



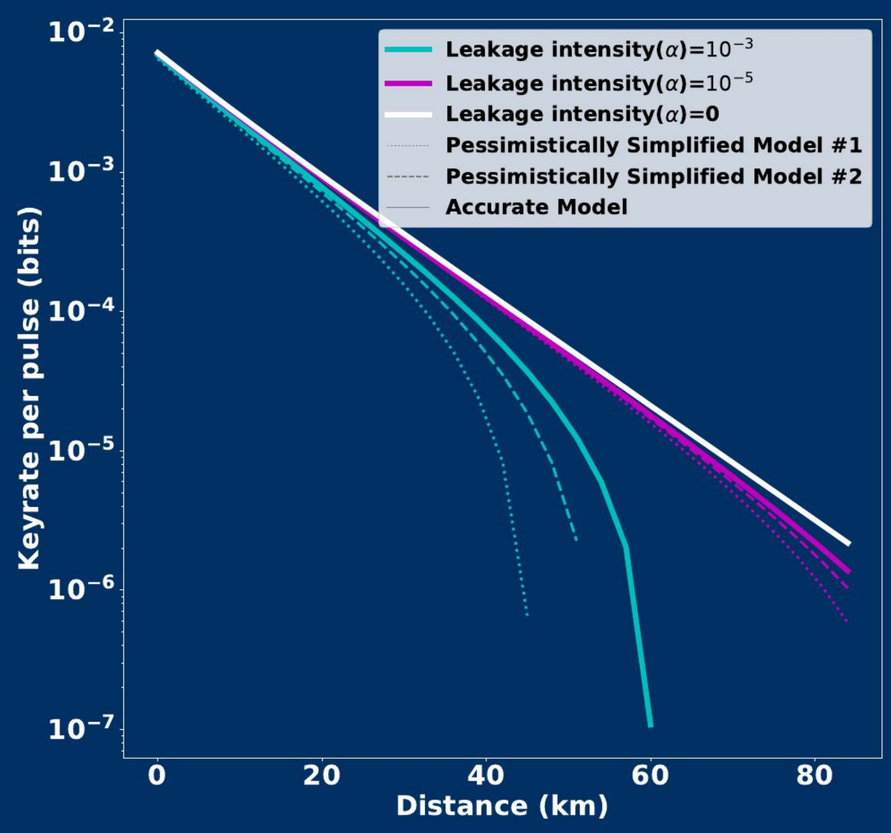
As an optical pulse experiences voltage induced bit/phase modulation, counter-propagating leakage light within the PM also gets modulated.



SECURITY ANALYSIS - Secure key rate improves noticeably when time dependence is fully incorporated (rather than making pessimistic simplifications)

Proof technique [4] (applied to decoy state MDI QKD):

- ➢ Express phase error rate in terms of inner products of Eve's states (unknowns)
- ➢ Constrain inner products of Eve's states by inner products of transmitted states (using unitary evolution postulate)
- ➢ Constrain inner products of Eve's states using decoy state detection statistics
- ➢ Perform a numerical optimization (semidefinite programming) with respect to inner products of Eve's states to obtain phase error rate



Key Rate Results when using Decoy State MDI QKD

References
[1] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. 92, 025002 (2020).
[2] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Physical Review A 73, 022320 (2006).
[3] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A 90, 052314 (2014).
[4] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, Phys. Rev. A 99, 062332 (2019).
[5] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. 112, 190503 (2014).

Amita Gnanapandithan[1], Eli Bourassa[2], Li Qian[1,3], Hoi-Kwong Lo[1,2,3,4]
1) Department of Electrical and Computer Engineering, University of Toronto. 2) Department of Physics, University of Toronto. 3) Center for Quantum Information and Quantum Control, University of Toronto. 4) Department of Physics, University of Hong Kong, Hong Kong