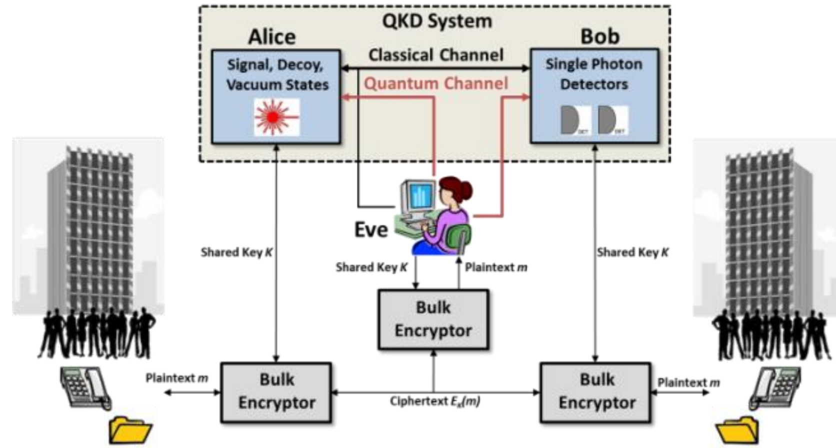
Modeling Quantum Optical Components, Pulses & Fiber Channels Using OMNeT++



Quantum Key Distribution (QKD) System

Ryan D. L. Engle, MS
Douglas D. Hodson, PhD

OMNeT++ Community Summit 2015
IBM Research - Zurich, Switzerland
September 3-4, 2015

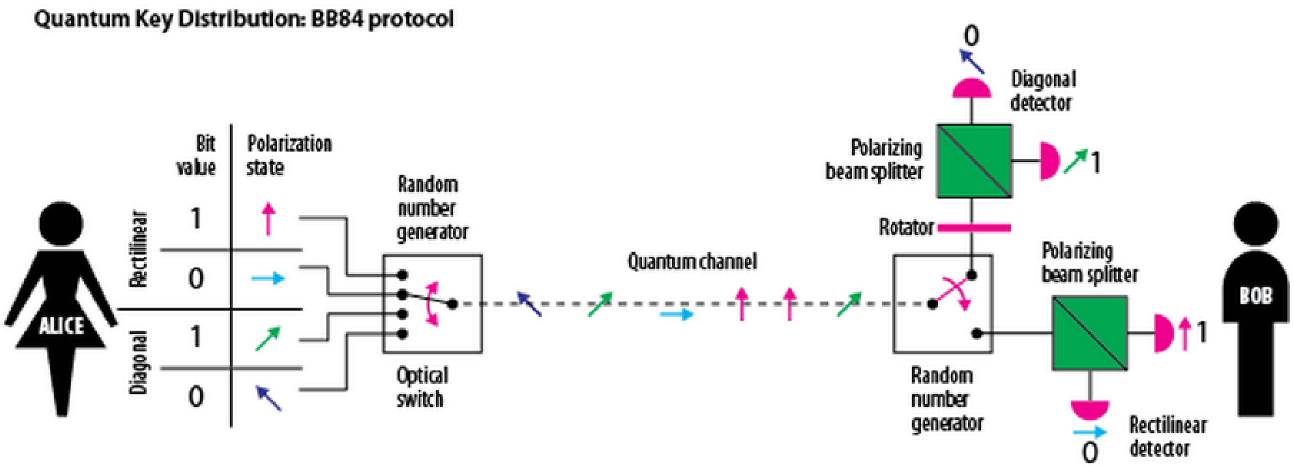
Research Team Members:
Dr. Michael R. Grimaila
Dr. Douglas D. Hodson
Maj Logan O. Mailloux
Capt Ryan D. L. Engle
Dr. Colin V. McLaughlin
Dr. Gerald Baumgartner

Overview

- Motivation: Quantum Key Distribution (QKD)
- Framework Packages & Organization
- Optical Pulses
- Optical Components
- Fiber Channels
- Testing
- Simulation Studies
- Publications

QKD System Operation / Protocol

The AFIT of Today is the Air Force of Tomorrow.

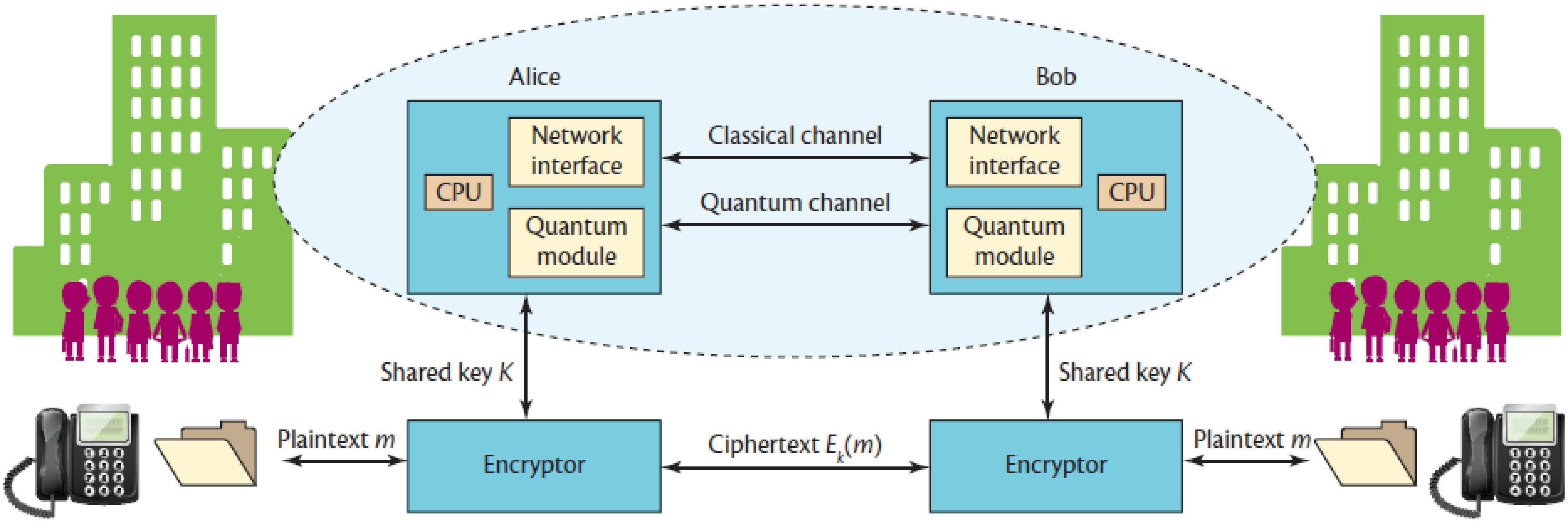


Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

- Innovative technology which **exploits the laws of quantum mechanics** to generate and distribute unconditionally secure cryptographic keys
- Unique in its ability to **detect the presence of an eavesdropper** attempting to subvert the distribution of key material
- Protocol **assumes certain idealities** with regard to pulse generation and detection

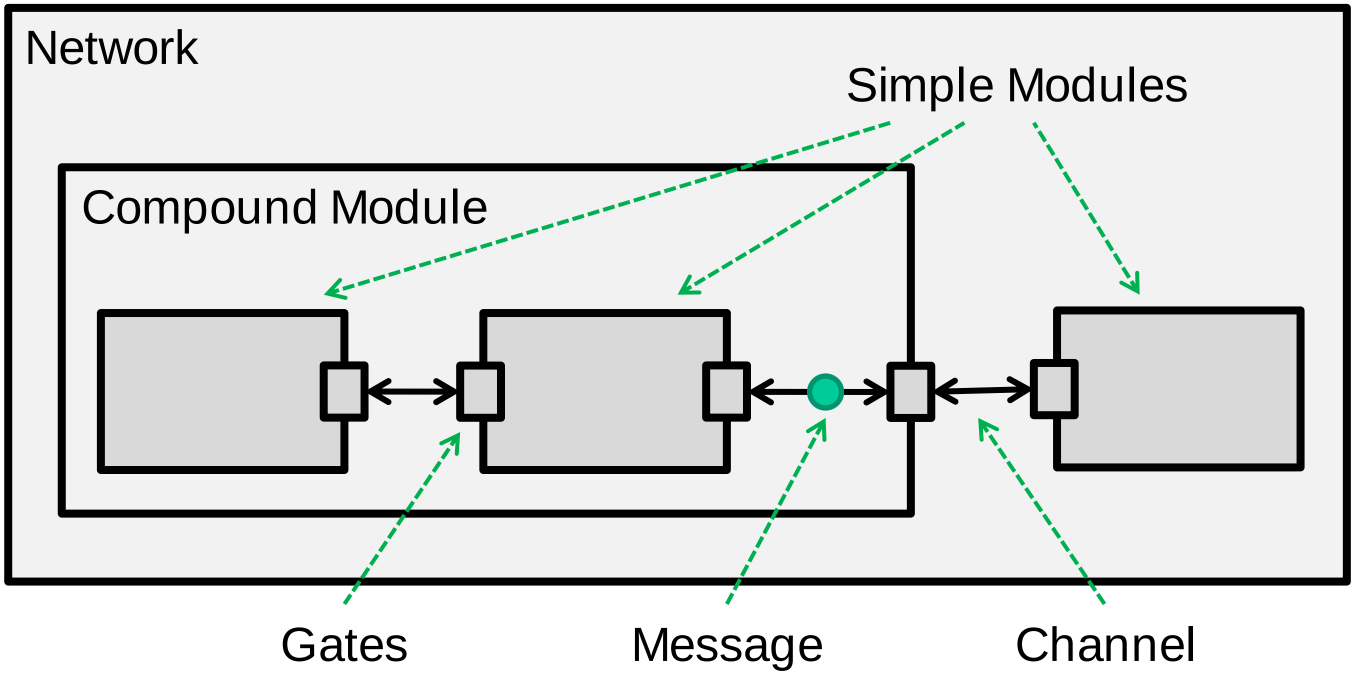
System Architecture

The AFIT of Today is the Air Force of Tomorrow.



- Motivation: simulate various system designs/architectures to understand the effects of ‘non-idealities’ on security and system performance
- Need to model: optical components (laser, beamsplitters, fiber channels, etc.), optical pulses, detectors
- System architecture easy to describe as a hierarchy of modules/components
- Created a framework to model these types of components (i.e., ‘qkdX’ framework)

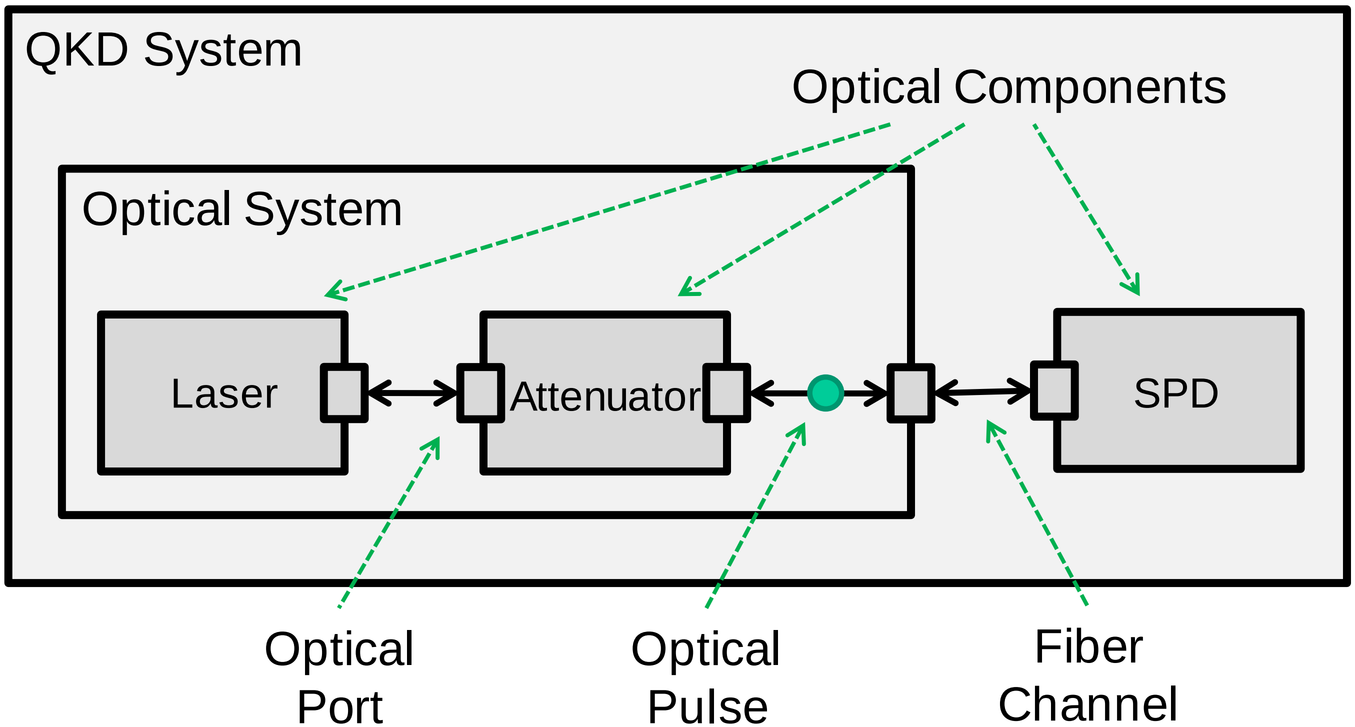
OMNeT++ Modeling Concepts



- Simple modules define behavior
- Compound modules are used to assemble a hierarchy
  - A network defines the system of interest (no gates)
- Gates define interface points – data (messages) flows through channels

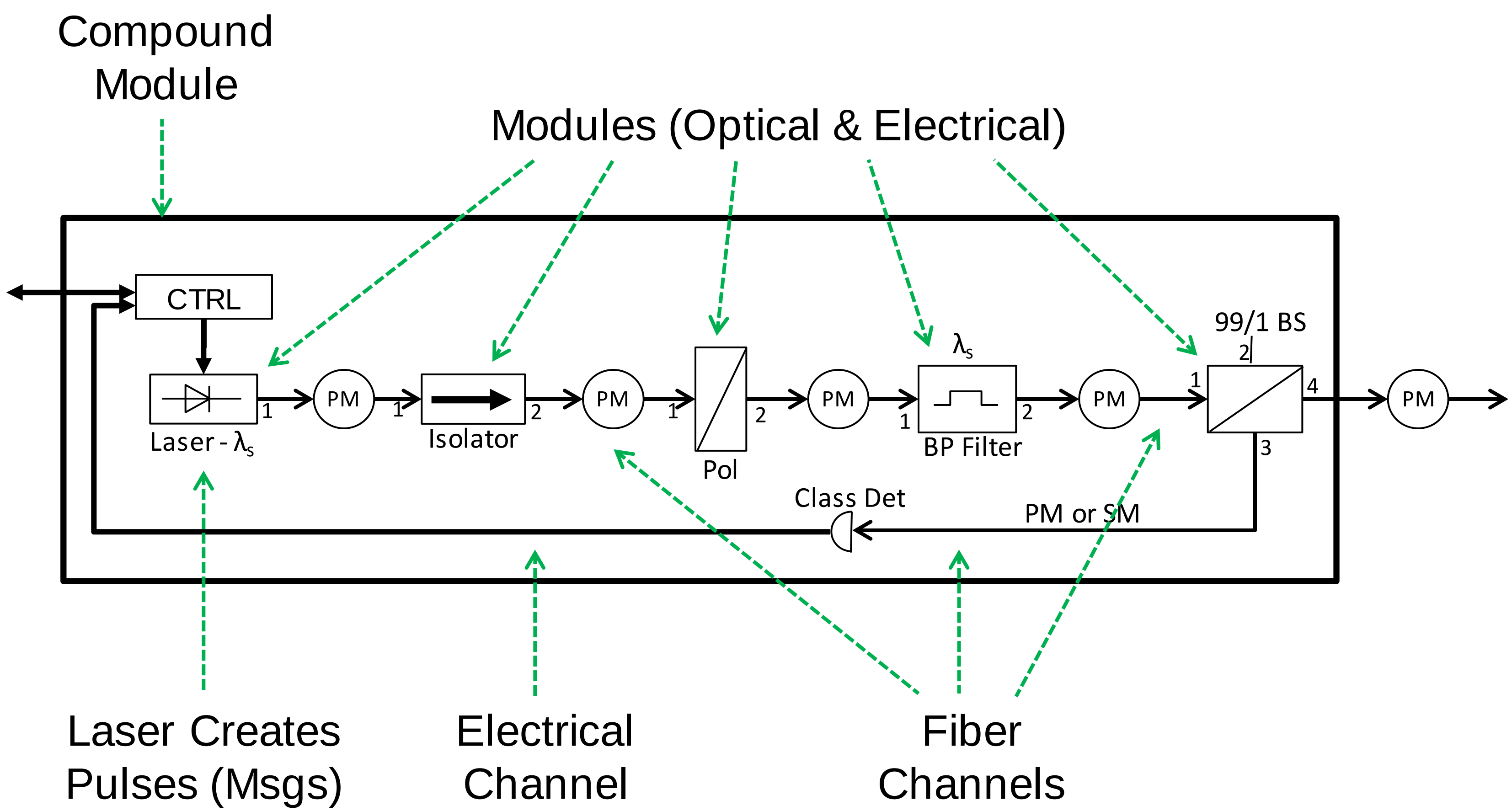
qkdX Modeling Concepts

The AFIT of Today is the Air Force of Tomorrow.



qkdX Classical Pulse Generator

The AFIT of Today is the Air Force of Tomorrow.

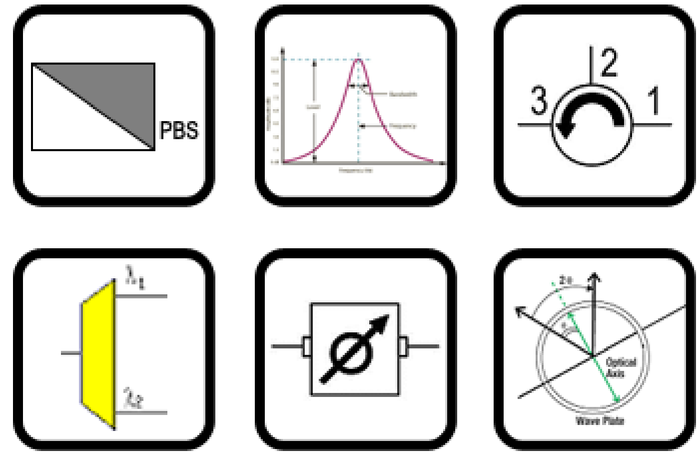


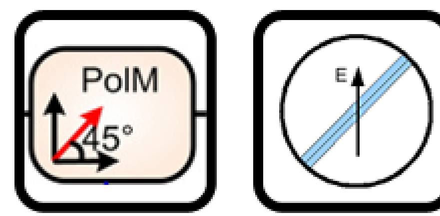
Modeled components must account for mathematics, state, data flow and timing

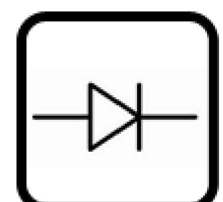
qkdX Components

Each component has multiple attributes:

- Type
- Active or Passive
- Number connections
- Type of connections
  - Input / Output / Bidirectional
  - Optical, Electrical, or Environmental
- Temporal behavior (OMNeT++)
- Functional behavior (C++)
- Component aging
- Failure modes (degraded/damaged)
- Parameterization depends upon abstraction

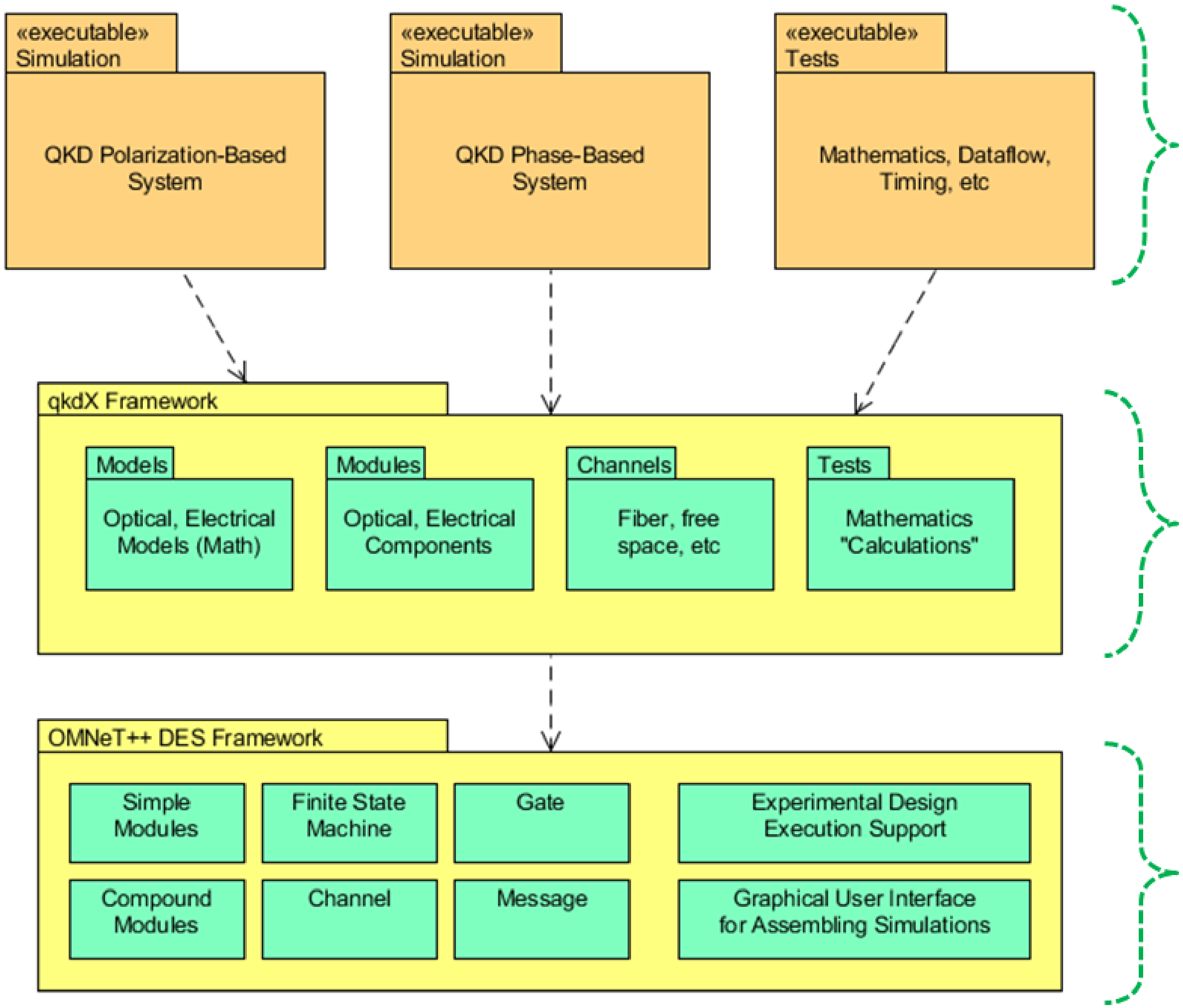






Package Relationships

The AFIT of Today is the Air Force of Tomorrow.

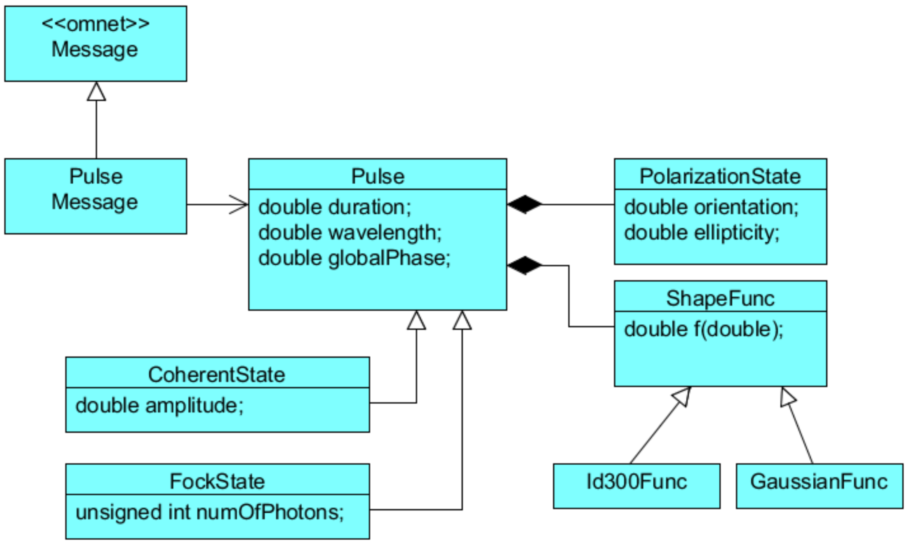


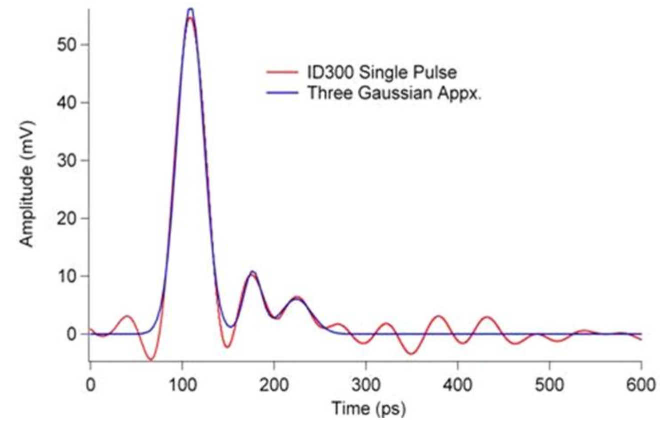
Simulation Products
Unique "applications" or system architectures

qkdX Framework
Defines system models and components common to many different architectures. Defines system abstractions to support different levels of fidelity/detail.

DES Framework (C++)
Provides fundamental infrastructure to build and interconnect system components

Optical Pulse Representation



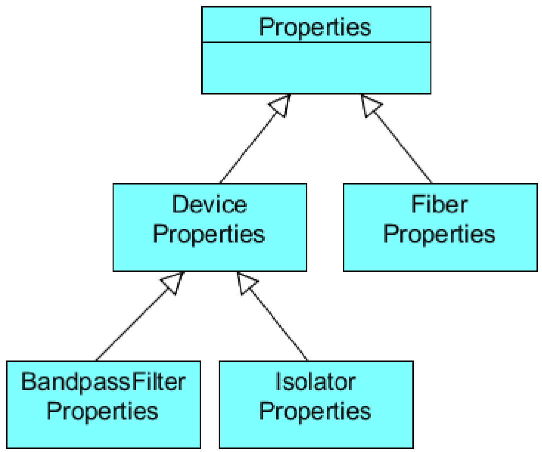


Example Pulse Representation

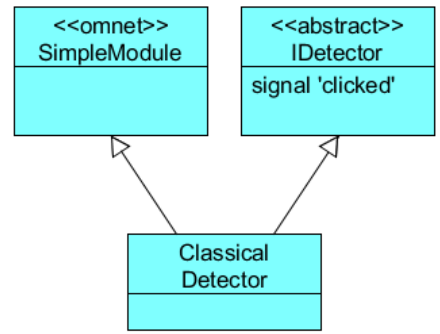
- Pulses encoded as messages
- Custom pulse message class created to manage pointer to actual pulse object
  - A variety of pulse objects have been created
  - The shape of pulses are described by functor-like objects

Optical Components

The AFIT of Today is the Air Force of Tomorrow.



Properties

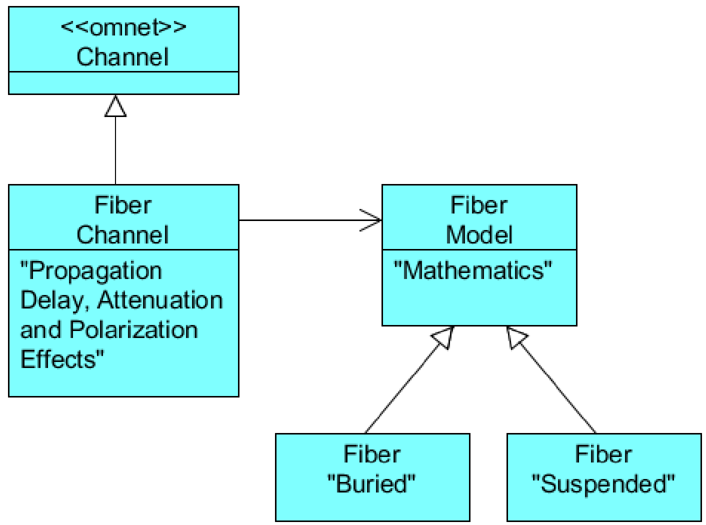


Interfaces

- Optical components are structured as simple modules
  - Need to account for mathematics (pulse transformations), component state (e.g., damaged), dataflow (physical path pulse traverses and reflections), and timing (propagation delay)
- Much of the code structured so that simple modules facilitate data flow and timing
  - State of components represented by different types (i.e., properties)
- Interfaces (mostly abstract classes) are defined to represent types (and support a public API)
  - Simple modules are viewed as a structuring concept (i.e., not as a 'type')

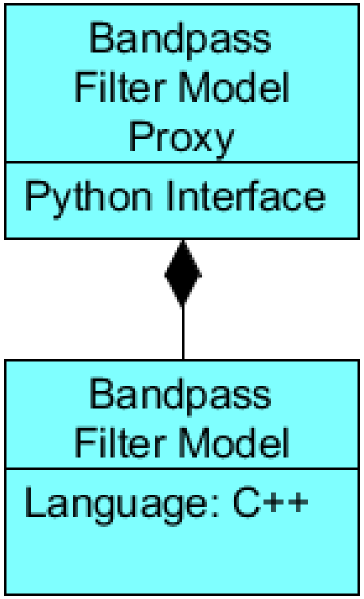
Fiber Channel

The AFIT of Today is the Air Force of Tomorrow.



- Fiber channels are implemented as a custom Channel
  - They add 'behavior' to the flow of pulses between components (e.g., attenuation, delay, polarization drift effects, etc.)
  - They include optional 'smarts' to delete pulses below a certain energy level (prevent infinite reflections between components)

Testing

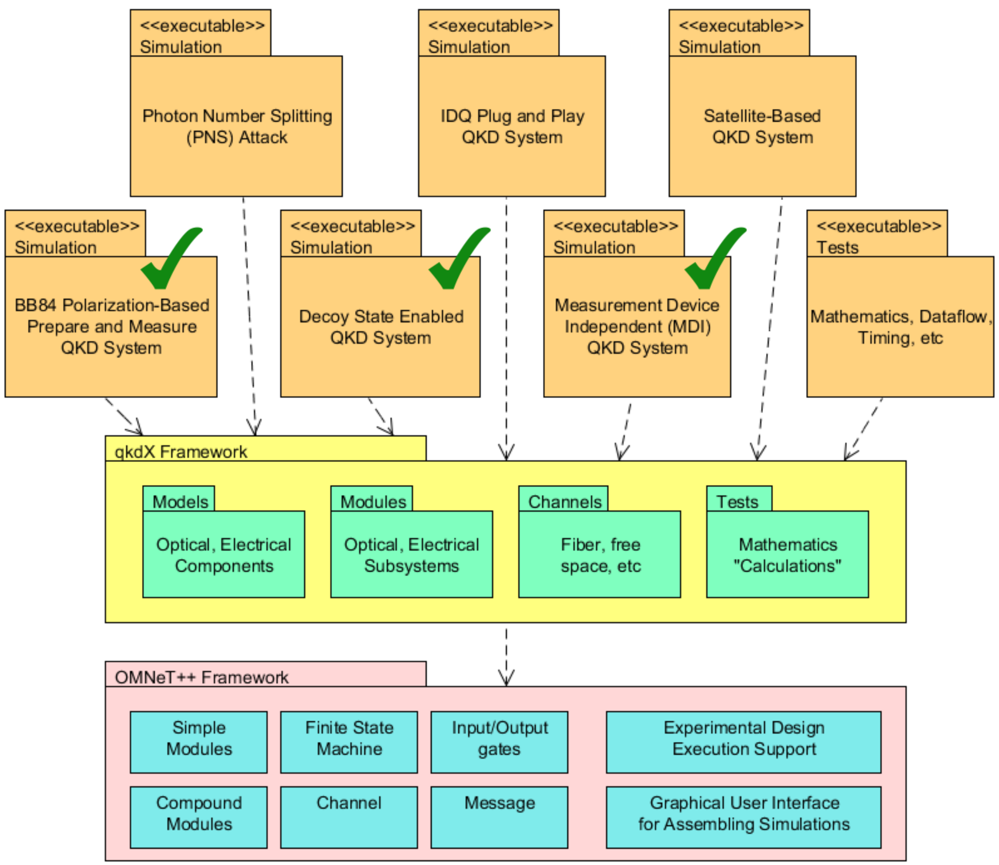


- Mathematics (pulse transformations)
- Component state (e.g., damaged)
- Dataflow (physical path pulse traverses)
- Timing (propagation delay)

- The mathematical calculations/transformations associated with component models does not require reside with simple modules
  - They are simple math functions that can be compiled separately into a library and called from Python
    - SWIG tool was used to generate proxy information
  - Python made it easier to 'script' extensive test cases to ensure this aspect of code is implemented correctly

Example Simulation Studies

The AFIT of Today is the Air Force of Tomorrow.



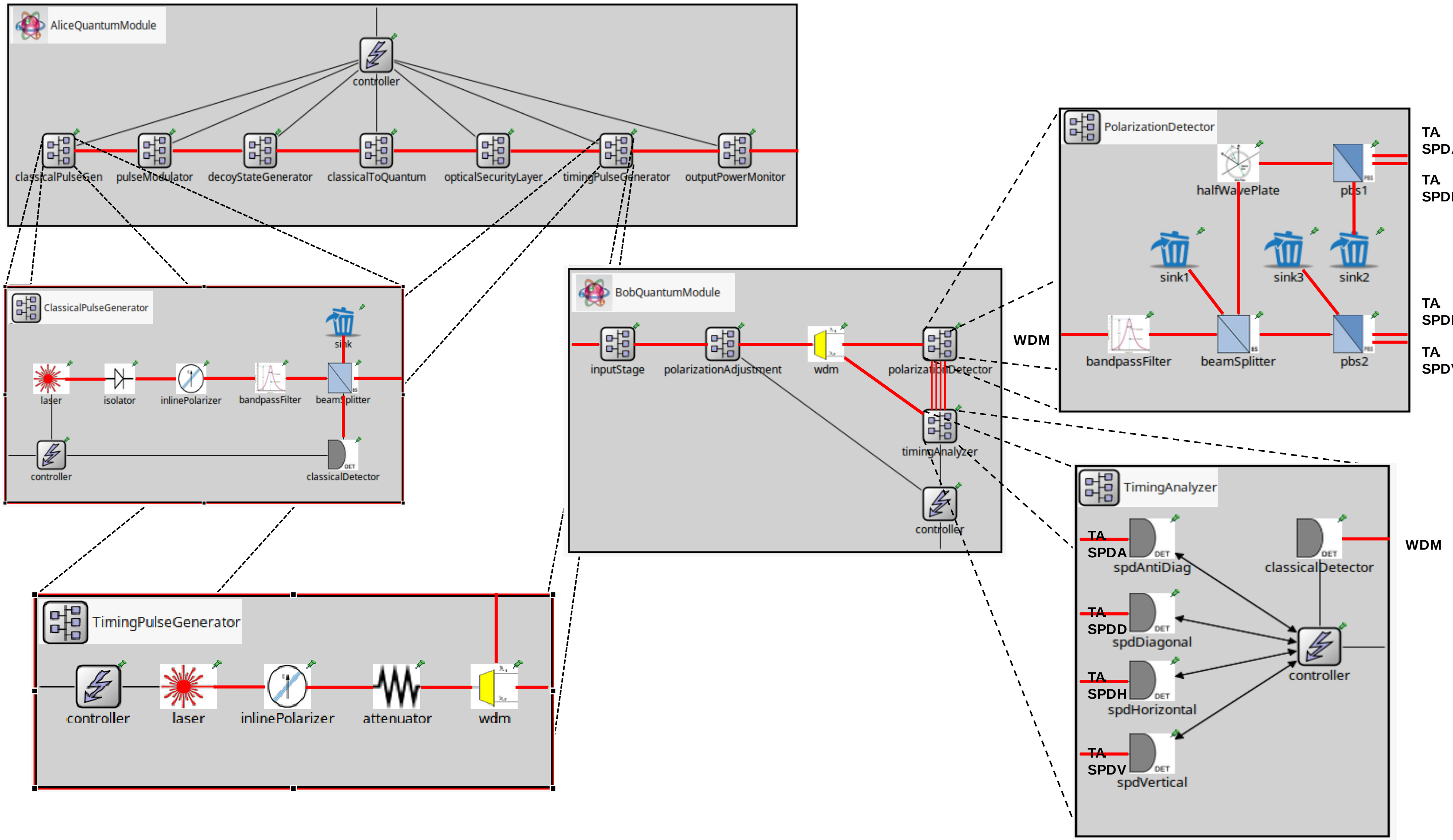
The variety and diversity of products have grown to support a number of Master and PhD thesis students resulting in a number of publications (provided at the end)

Examples:

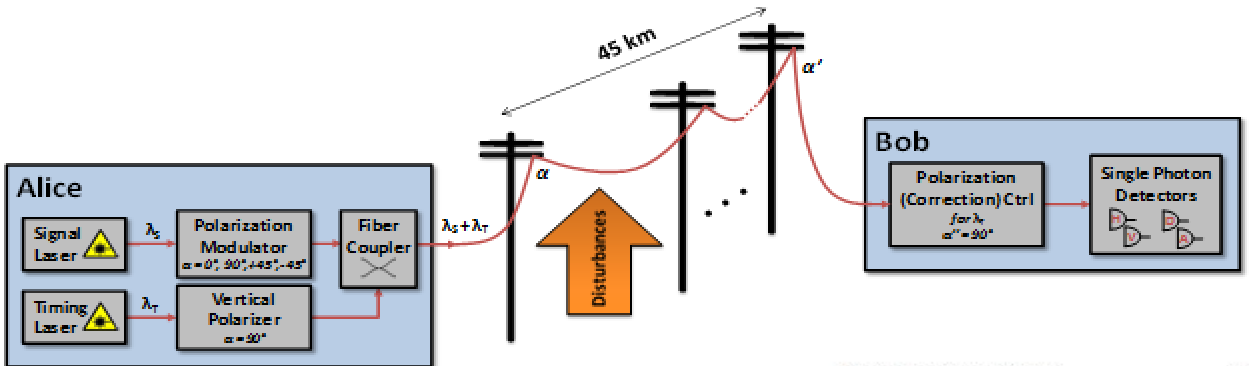
- Development of a BB84 reference architecture
- Decoy state enabled system designs
- Measurement device independent systems

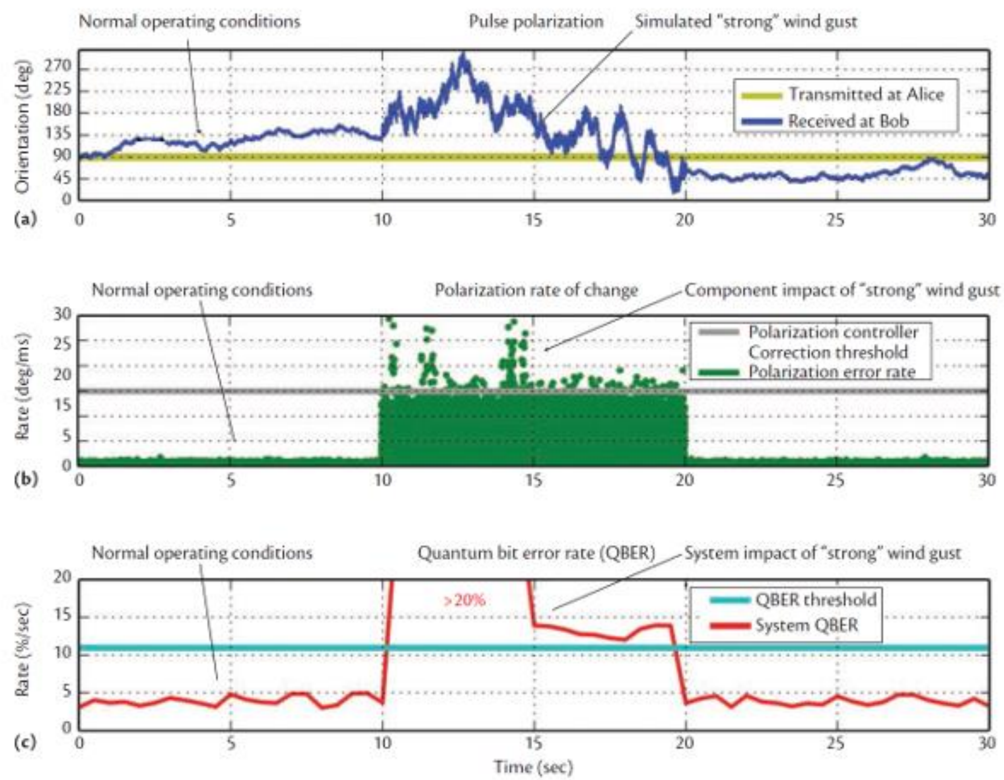
BB84 Reference Architecture

The AFIT of Today is the Air Force of Tomorrow.

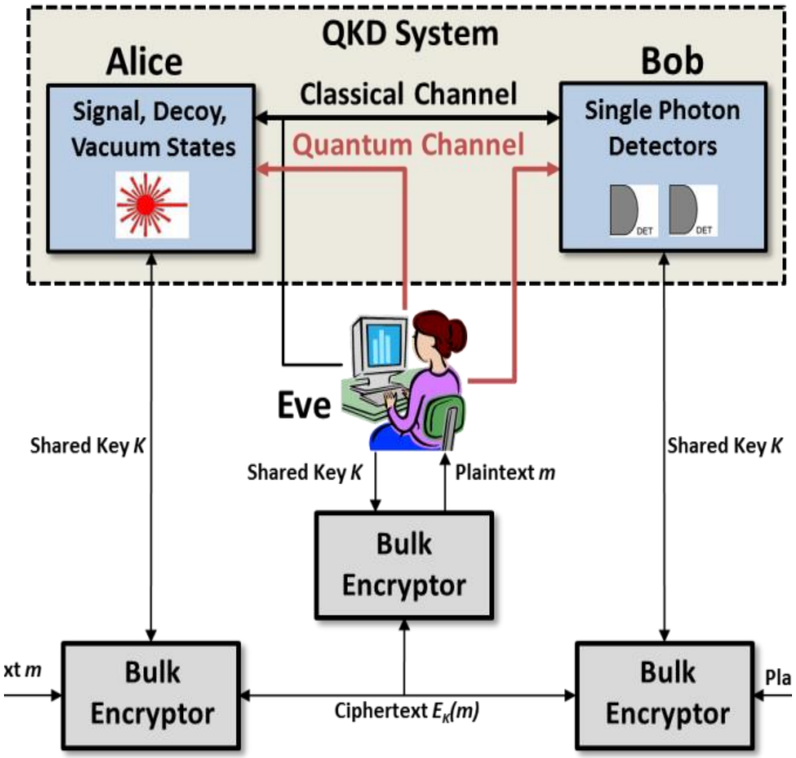


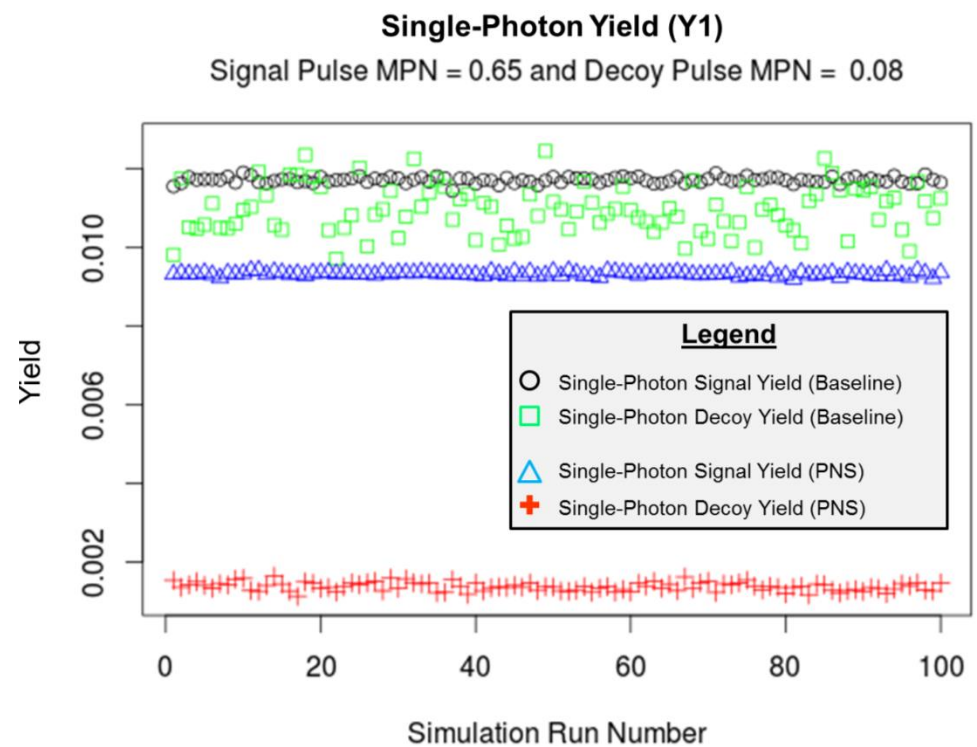
Polarization Drift





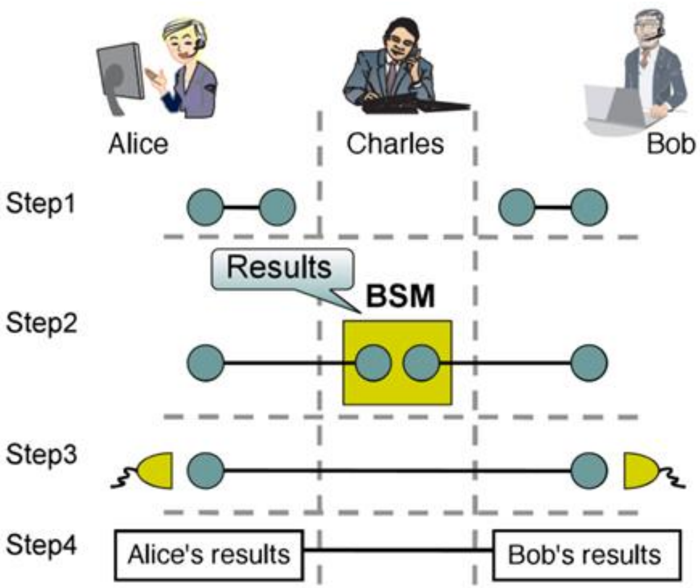
Decoy State Enabled QKD



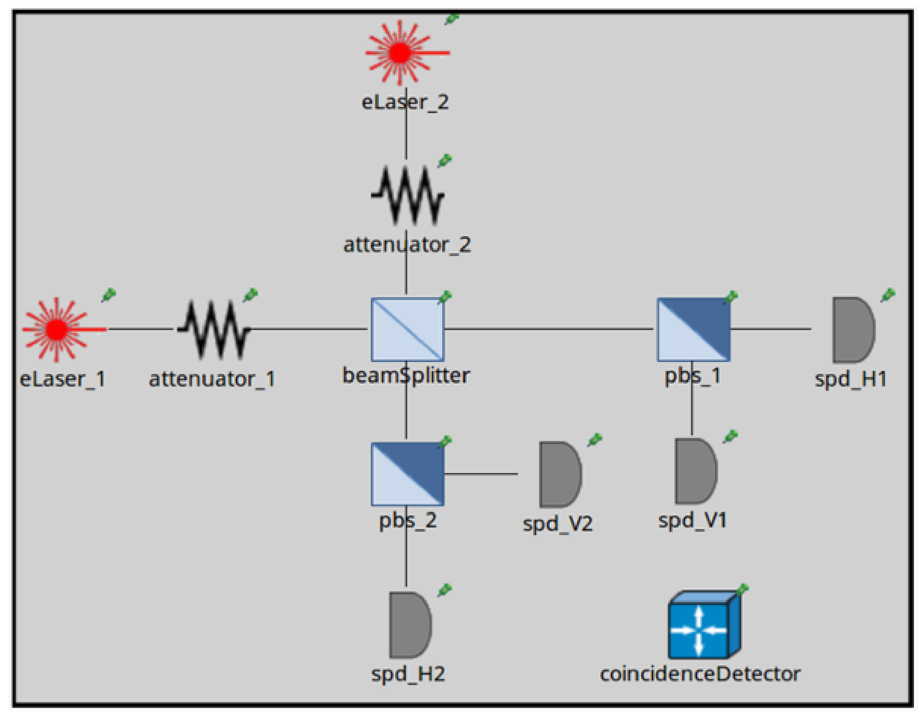


Measurement Device Independent QKD

The AFIT of Today is the Air Force of Tomorrow.



F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Measurement-device-independent quantum cryptography," IEEE Journal of Selected Topics in Quantum Electronics, 2014.



Publications

The AFIT of Today is the Air Force of Tomorrow.

- **Archival Journals**
- Mailloux, L.O., Hodson, D.D., Grimaila, M.R., Colombi, J.M., McLaughlin, C.V., and Baumgartner, G.B., "Test and Evaluation of Complex Cybersecurity Systems: A Case Study in Using Modeling and Simulation to More Efficiently Understand, Test, and Evaluate the Security of Quantum Key Distribution Systems," *ITEA Journal*. Submitted June, 2015.
- Mailloux, L.O., Engle, R.D., Grimaila, M.R., Hodson, D.D., Colombi, J.M., and McLaughlin, C.V., "Modeling Decoy State Enabled Quantum Key Distribution Systems," The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Accepted for Publication April, 2015.
- Mailloux, L.O., Grimaila, M.R., Colombi, J.M., Hodson, D.D., McLaughlin, C., and Baumgartner, G., "Quantum Key Distribution: Evaluation of the Decoy State Protocol," *IEEE Communications Magazine*, Submitted March, 2015.
- Engle, R.D., Grimaila, M.R., Mailloux, L.O., Hodson, D.D., McLaughlin, C., and Baumgartner, G., "Developing a Decoy State Enabled Quantum Key Distribution System Model," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Submitted February, 2015.
- Mailloux, L.O., Grimaila, M.R., Hodson, D.D., Baumgartner, G., and McLaughlin, C., "Performance Evaluations of Quantum Key Distribution System Architectures," IEEE Security and Privacy, January/February 2015, pp. 30-40. DOI: 10.1109/MSP.2015.11
- Mailloux, L.O., Morris, J.D., Grimaila, M.R., Hodson, D.D., Jacques, D.R., Colombi, J.M., McLaughlin, C.V., and Holes, J.A. "A Modeling Framework for Studying Quantum Key Distribution System Implementation Non-Idealities," *IEEE Access*, January, 2015. DOI: 10.1109/ACCESS.2015.2399101
- Sorensen, N.T., Grimaila, M.R., "Discrete Event Simulation of the Quantum Channel within a Quantum Key Distribution System," The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, February, 2015. DOI: 10.1177/1548512915569743
- Mailloux, L.O., Grimaila, M.R., Hodson, D.D., Colombi, J.M., "A Practical Assessment of Security Design Patterns," *The Information System Security Association (ISSA) Journal, 11*(9), September 2014, pp. 29-35.
- Morris, J.D., Grimaila, M.R., Hodson, D., McLaughlin, C., and Jacques, D., "Using the Discrete Event System Specification to Model Quantum Key Distribution System Components," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, October 17, 2014, pp. 1-24, , DOI: 10.1177/1548512914554404
- Morris, J.D., Hodson, D.D., Grimaila, M.R., Jacques, D.R., and Baumgartner, G., "Towards the Modeling and Simulation of Quantum Key Distribution Systems," *International Journal of Emerging Technology and Advanced Engineering*, Vol. 4, No. 2, February 2014, pp. 11-22.
- Grimaila, M.R., Morris, J., Hodson, D., "Quantum Key Distribution: A Revolutionary Security Technology," *The Information System Security Association (ISSA) Journal*, 10(6), June 2012, pp. 20-27.
- **Theses/Dissertations**
- Mailloux, L.O. (Scheduled August 2015) A performance and security analysis of practical decoy state enabled quantum key distribution systems (PhD Dissertation, Air Force Institute of Technology).
- Cernera, R.C. (Summer 2015) A System-Level Throughput Model for Quantum Key Distribution (Master's thesis, Air Force Institute of Technology).
- Engle, R.D. (2015) *Modeling, simulation, and analysis of a decoy state enabled quantum key distribution system.* (Master's thesis, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA615556).
- Morris, J.D. (2014) Conceptual modeling of a quantum key distribution simulation framework using the discrete event system specification (PhD Dissertation, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA609513)
- Harper, C.A. (2012) *Security standards and best practice considerations for quantum key distribution (qkd)* (Master's thesis, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA558003)
- Johnson, J.S. (2012) *An analysis of error reconciliation protocols for use in quantum key distribution* (Master's thesis, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA557404)
- Sorensen, N.T. (2012). *Quantum channel modeling for discrete event simulation of quantum key distribution* (Master's thesis, Air Force Institute of Technology). Limited Distribution.
- Thomas, A.C. (2012). *Empirical analysis of optical attenuator performance in quantum key distribution systems using a particle model* (Master's thesis, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA557492)
- Calver, T.I. (2011) An empirical analysis of the cascade secret key reconciliation protocol for quantum key distribution (Master's thesis, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA549804)
- Lustic, K.C (2011). Performance analysis and optimization of the winnow secret key reconciliation protocol (Master's thesis, Air Force Institute of Technology). Available from Defense Technical Information Center. (ADA544630)

Questions?

This work was supported by the Laboratory for Telecommunication Sciences [grant number 5743400-304-6448] and in part by a grant of computer time from the DoD High Performance Computing Modernization Program at the Air Force Research Laboratory, Wright-Patterson AFB, OH.