
SCTE®
CABLE-TEC EXPO®
FAST FORWARD 2021
ATLANTA, GA
OCTOBER 11-14
SCTE
a subsidiary of CableLabs®
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®

SCTE
a subsidiary of CableLabs

Security & Privacy

Hitchhiker's Guide to QKD

Vaibhav Garg

Sr. Director
Cybersecurity Research & Public Policy

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

SCTE CABLE-TEC EXPO FAST FORWARD 2021
VIRTUAL EXPERIENCE
OCTOBER 11-14

QUANTUM WHO?

COMCAST

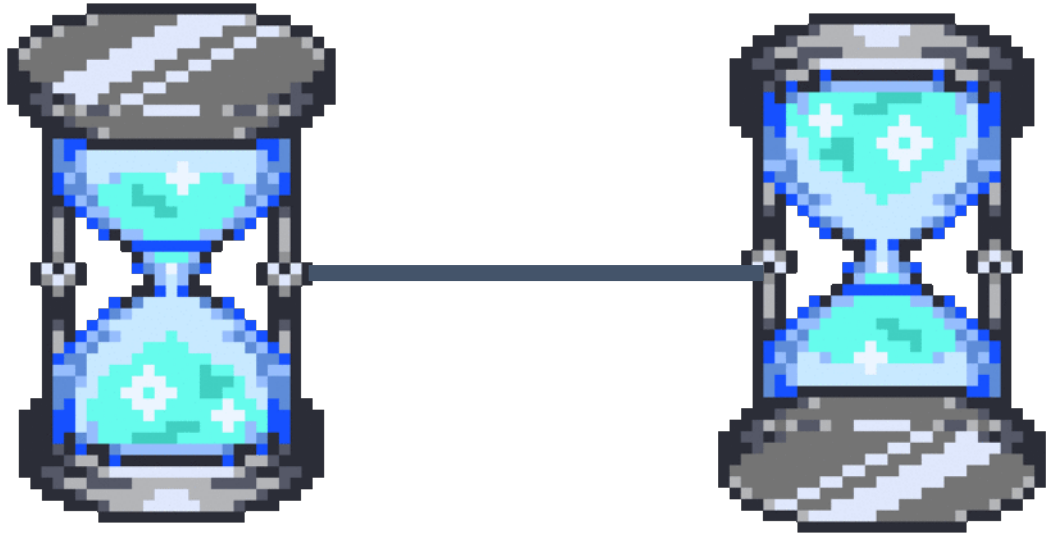
WHAT IS QUANTUM?

Is it a 0, is it a 1, it is Superposition!

In classical computing we operate over bits, which are either 0 or 1. Quantum technologies operates over **qubits**, which are in a superposition of 0 and 1, i.e. they are simultaneously 0, 1, and anything in between. This is known as **superposition** and remains true so long as the qubits are not observed (or measured). Once a qubit is measured it collapses to a classical state of either 0 or 1.

Entanglement

In addition to superposition, quantum particles have a second property called entanglement that leads to 'spooky' action at a distance. Essentially, when two entangled particles are separated by arbitrary large distance they stay in the same state. So if they are in the state of super-position they remain so. If one of them is observed and thus collapses to either 0 or 1, the other is similarly impacted.



WHAT IS QKD?

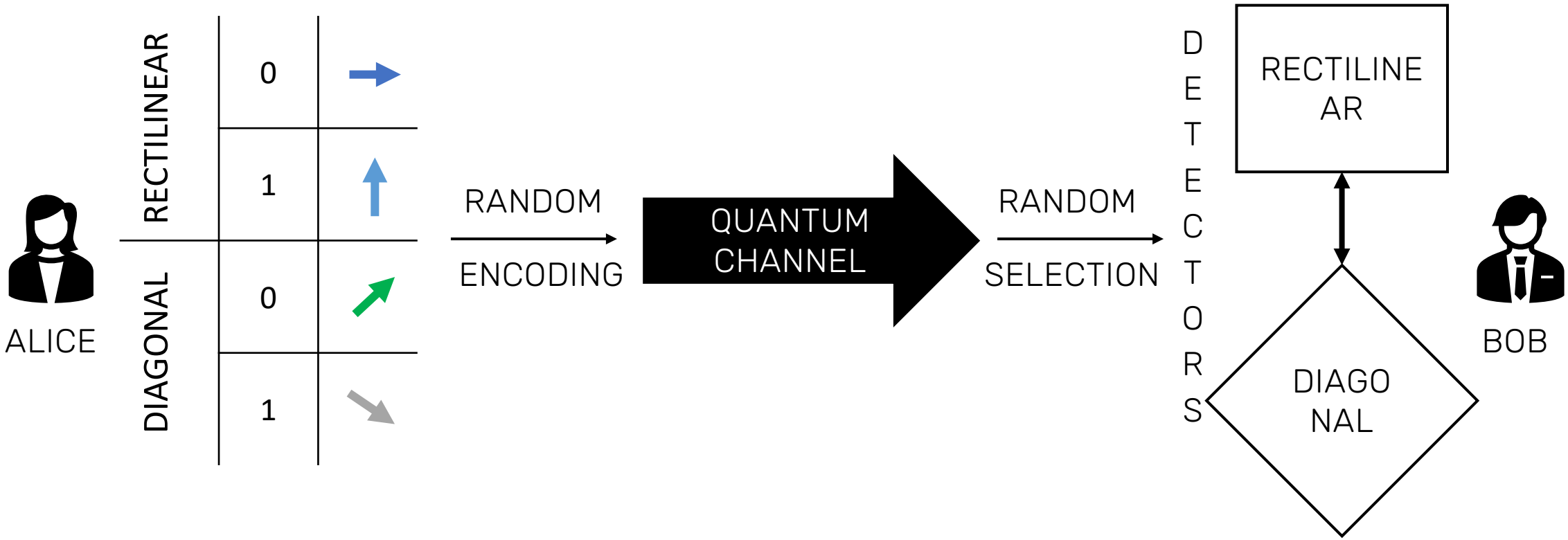
A Basic System

QKD is a system that uses quantum superposition and entanglement as a way to distribute keys over an arbitrary distance. Because entangled particles collapse under observation to a classical state, it is impossible to eavesdrop on the quantum channel without being detected. QKD is expensive; costs are driven by light detectors. Fiber implementations are limited to hundreds of kilometers, while air implementations are limited by line of sight. Over air implementations may be hampered by environmental conditions such as rain.

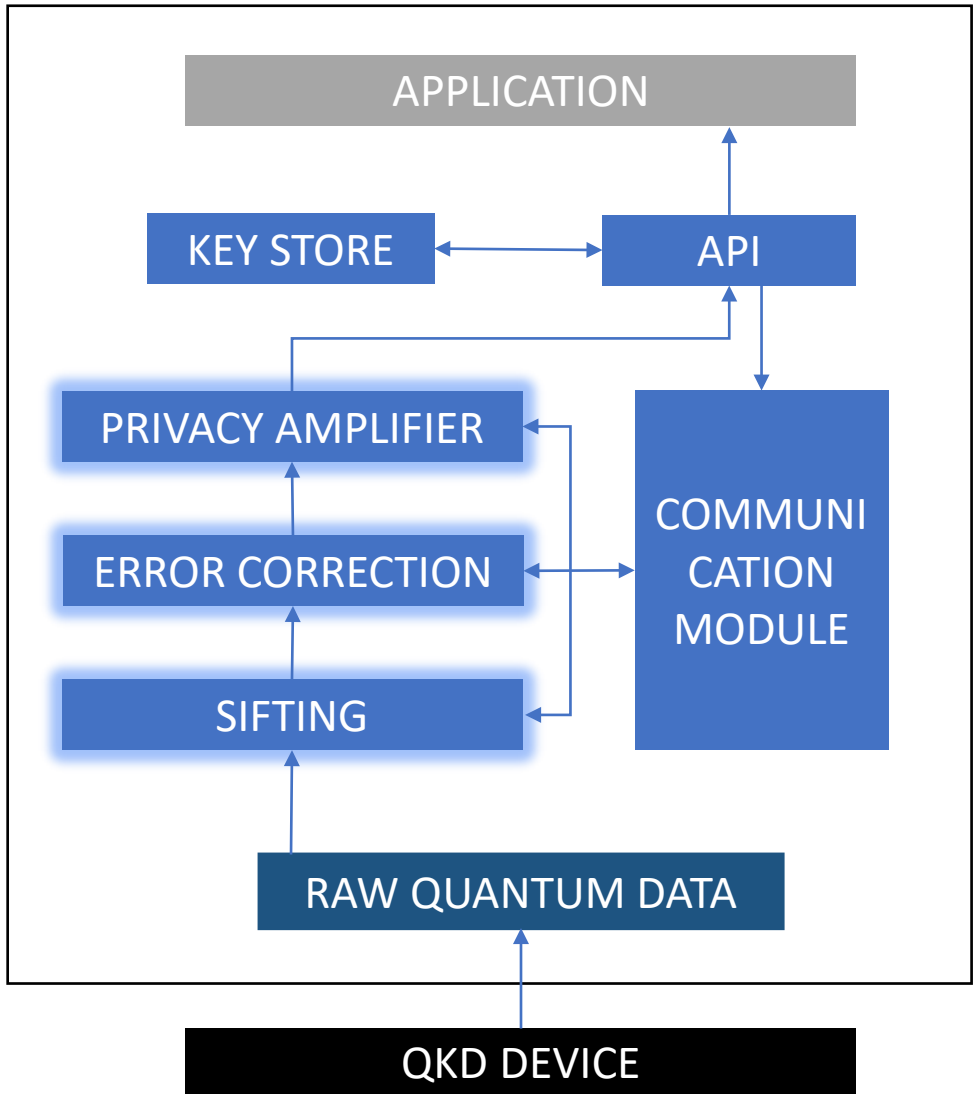
- Single Photon
- Entangled Photon
- Weak Laser Pulse

- Air
- Fiber

- Visible SPAD
- IR SPAD
- Superconducting Detector



Alice Transmission	0	1	1	0	1	1
Alice Basis	R	D	R	D	R	D
Bob Basis	R	R	D	D	D	D
Bob Detection	0	0	1	0	1	1
Final key	0	-	-	0	-	1



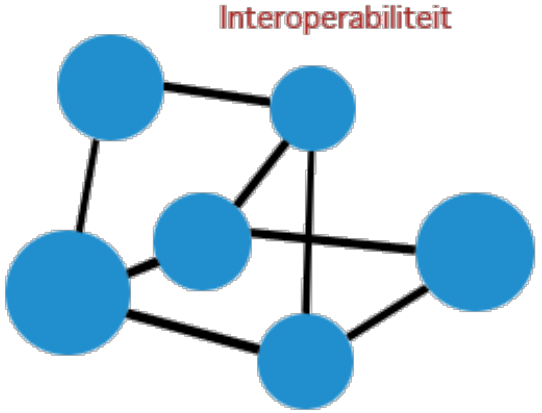
Common Post-Processing

Sifting: Keeps the data that contribute to the key or for statistic gathering. When enough information is gathered to compromise a block, parameter estimation is run to obtain an upper bound.

Error Correction: A portion of each block is sacrificed to get an estimate on the amount of noise and used to correct the errors in the rest of the block so that they each have an identical key block.

Privacy Amplification: Shrinks the corrected key block to a smaller size, in accordance with the quantum left-over hash lemma to obtain a key.

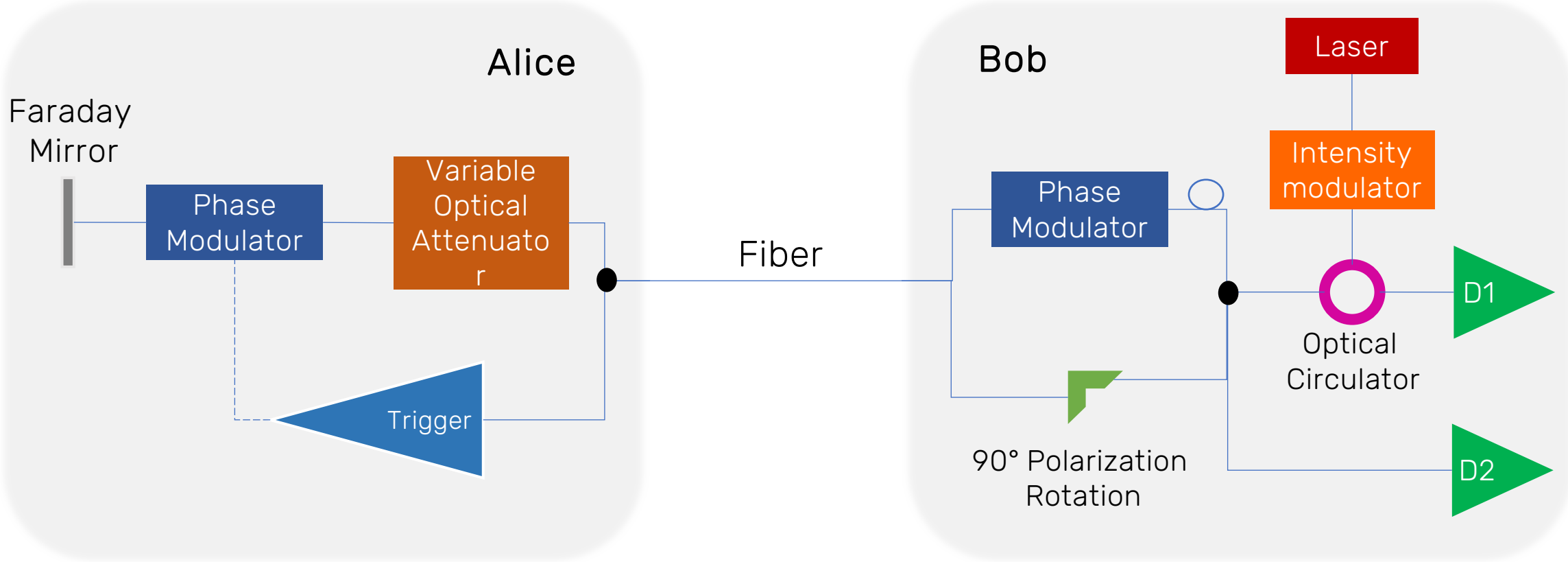
CHALLENGES SOLVED



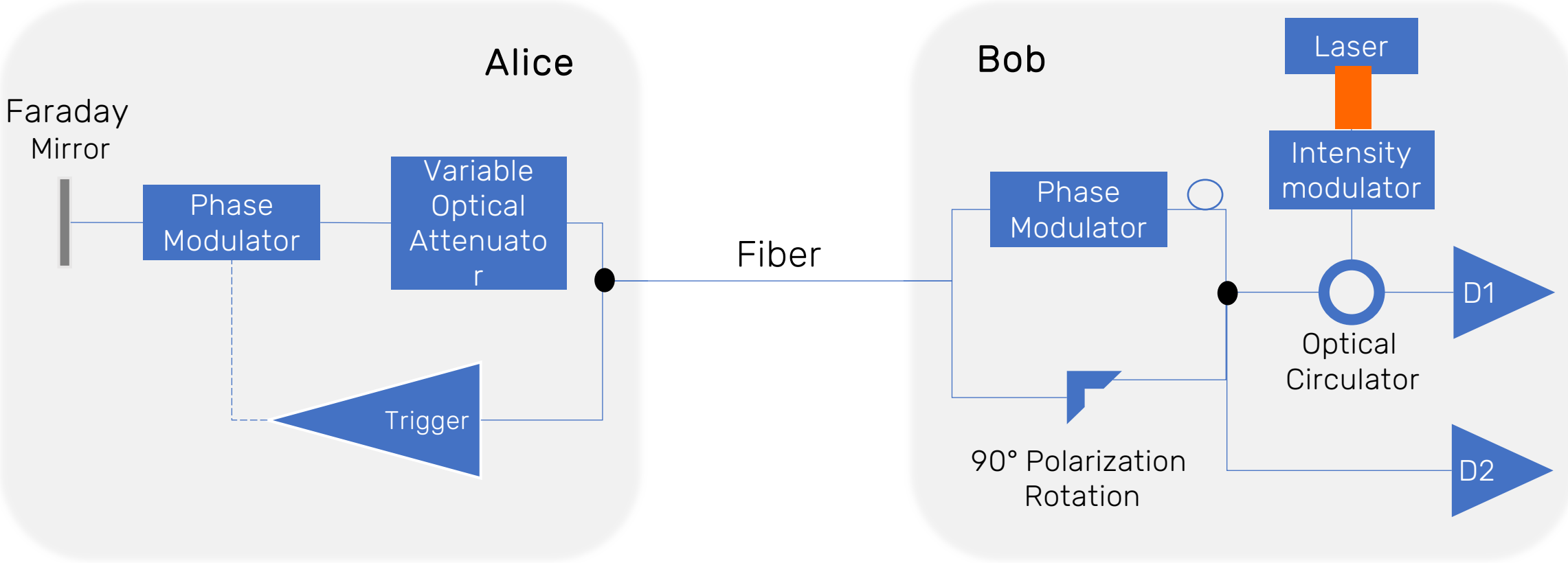
COMCAST

ONGOING INNOVATIONS

Auto-Compensated Fiber MZD QKD System

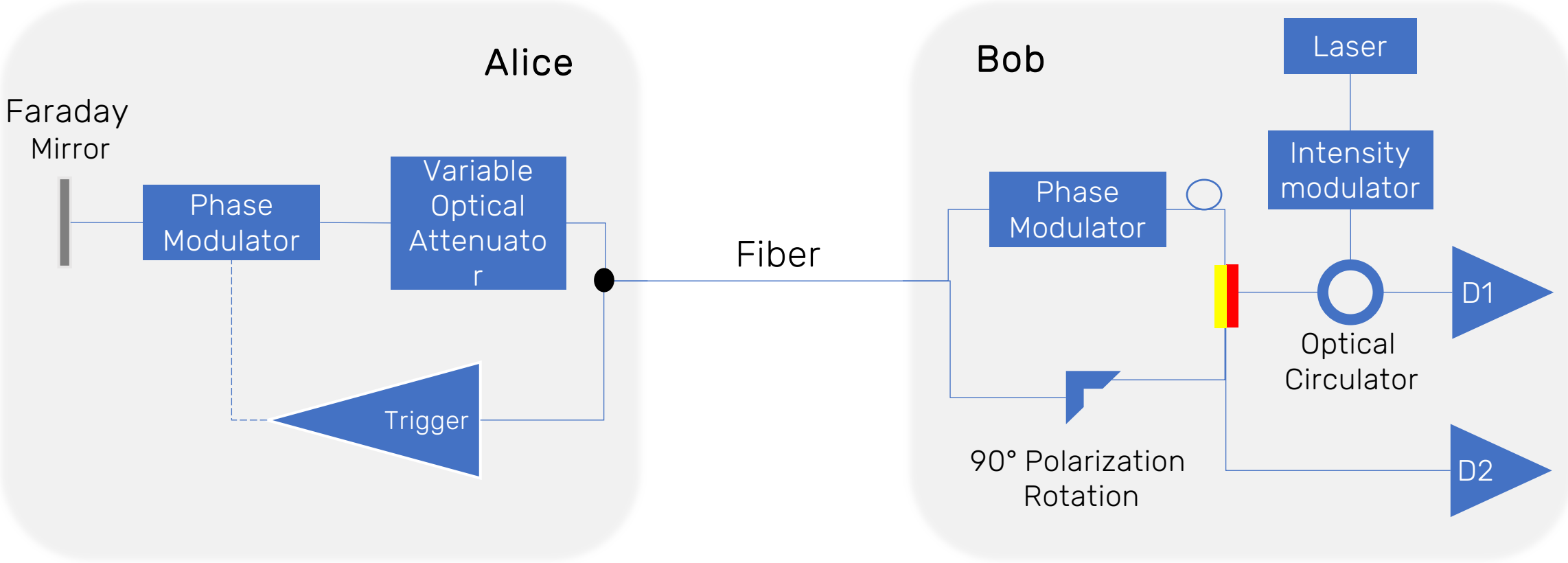


Auto-Compensated Fiber MZD QKD System

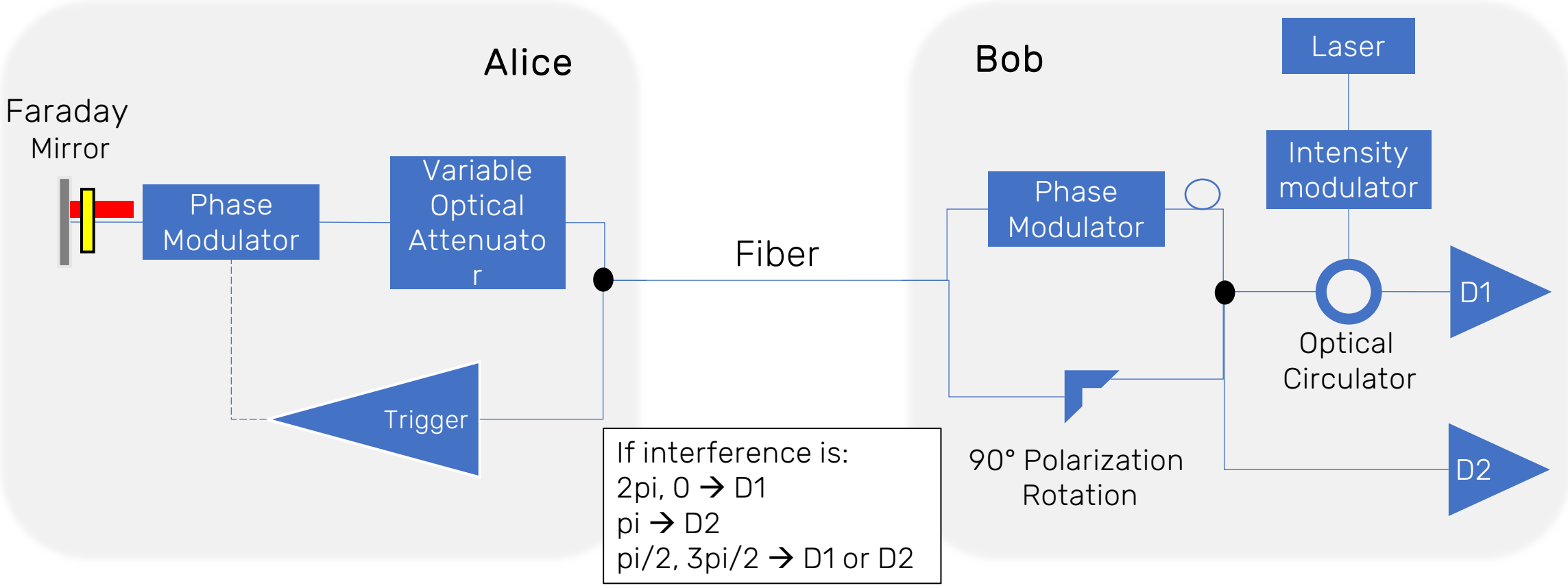


14

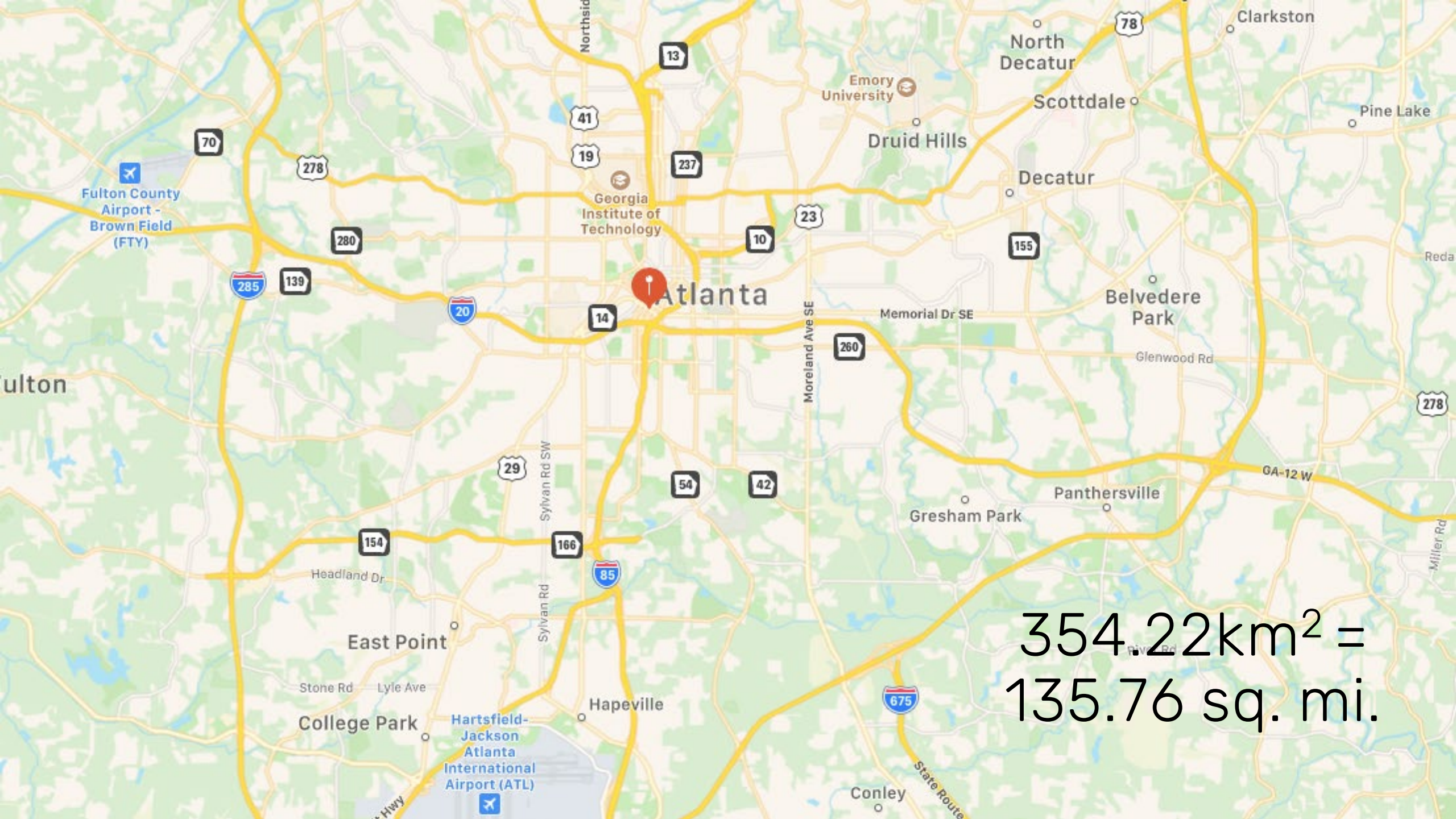
Auto-Compensated Fiber MZD QKD System



Auto-Compensated Fiber MZD QKD System



BUT DISTANCE!


354.22km² =
135.76 sq. mi.
Atlanta
Georgia Institute of Technology
Emory University
North Decatur
Clarkston
Scottdale
Druid Hills
Decatur
Pine Lake
Belvedere Park
Memorial Dr SE
Moreland Ave SE
Glenwood Rd
Panthersville
Gresham Park
GA-12 W
Fulton County Airport - Brown Field (FTY)
East Point
College Park
Hapeville
Hartsfield-Jackson Atlanta International Airport (ATL)
Conley
Headland Dr
Sylvan Rd SW
Sylvan Rd
Stone Rd
Lyle Ave
Miller Rd
70
278
280
285
139
20
14
13
41
19
237
10
23
155
260
29
54
42
154
166
85
675
78

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs

Thank You!

Vaibhav Garg

Sr. Director, Cybersecurity Research & Public Policy
Comcast Cable
Vaibhav_garg@comcast.com

2021 Fall
Technical Forum
SCTE • NCTA • CABLELABS

COMCAST