

Quantum security for optical networking

Alexei Trifonov
MagiQ Technologies, Inc.

Caltech quantum and classical security workshop

Outline

- QKD has good chances to become a commercially successful technology
- Currently up to 100 km of absolutely secure communication is possible
- The limitations of fiber-optics point-to-point QKD are mainly the source and the detector
- There is no working solution for quantum repeater – analog for optical amplifier
- Single/entangled photon source – the good and the bad.



NEC Empowered by Innovation

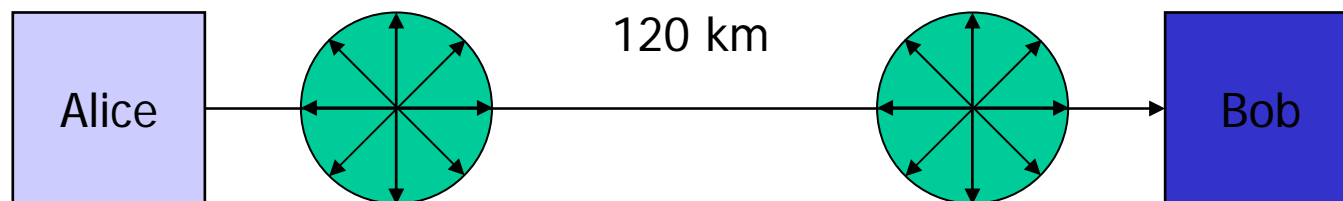
MagiQ Corporate Background

- Founded in July 1999
- Headquartered in NYC with R&D Laboratories in Somerville, Mass.
- Seed Funding to Date
 - Angels Include:
 - Jeff Bezos, Amazon.com founder and CEO
 - Robert Gelfond, MagiQ founder and CEO
 - Walter Riley, Guaranteed Overnight Delivery (G.O.D.) chairman
- Dual Business Strategy
 - MagiQ is developing and is selling commercial quantum information devices
 - MagiQ is simultaneously building a portfolio of valuable intellectual property for future products
- QPN – Quantum Private Network
 - MagiQ first commercial quantum device
 - Secure Network VPN appliance with Quantum Key Distribution and encryption

What are the main challenges now?

- Two main parameters – distance and key generation rate
- For commercial application distance must cover up to 120 km (more than 25 dB loss budget) – 100 km current spec
- Rate is not very important parameter so far, unless one-time-pad encryption is used (not for commercial use!!). In commercial application we are looking for 1Gb/sec and higher data rate so 256 bit AES encryption is going to be used.
- The main security parameter is the ratio of the data rate vs. key flipping rate. 256 bit/sec is considered to be secure key refresh rate for the 1 Gb/sec data capacity.
- Cascading
- Integration into the network – key management, remote control, etc
- Physical security etc.

QKD fiber optical link



Loss=0.2dB/km
Chromatic dispersion -17ps/nm/km
(SMF-28)
PMD=0.1ps km^{1/2}

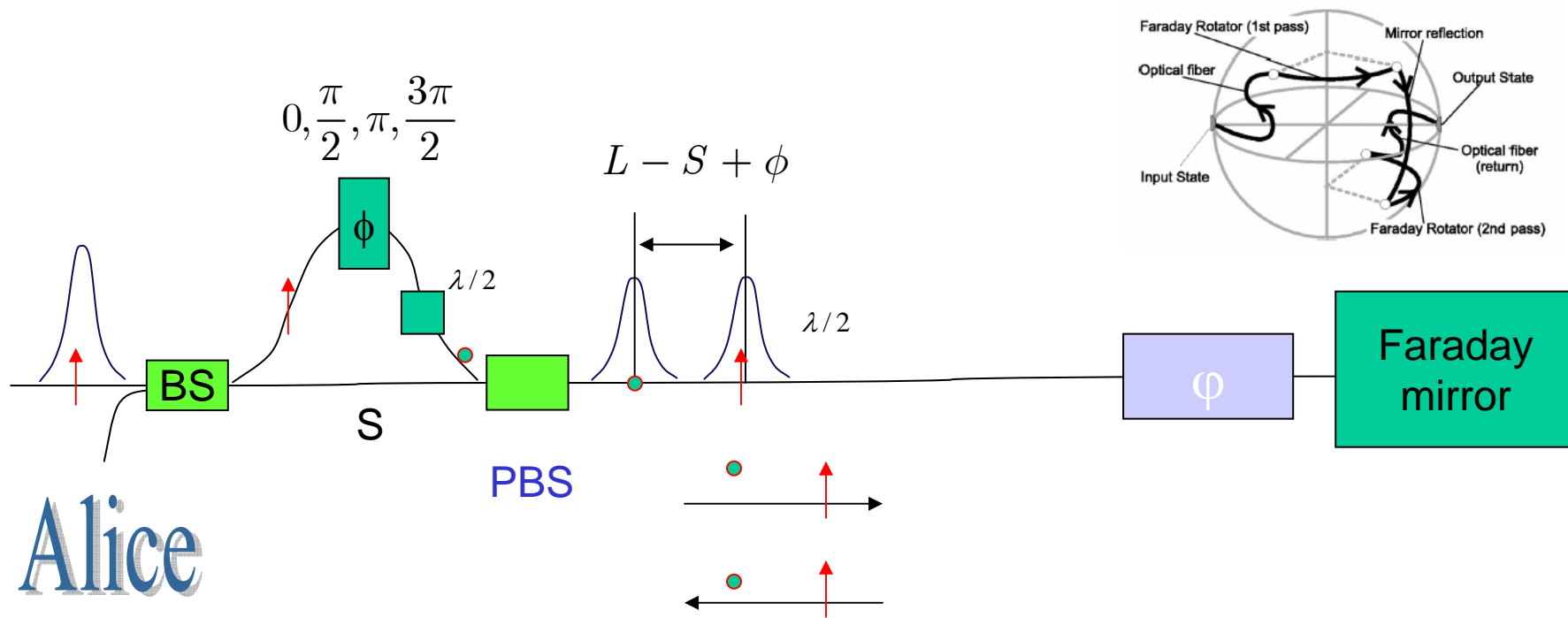
1 photon or less

>25dB of attenuation

QBER=1-10%

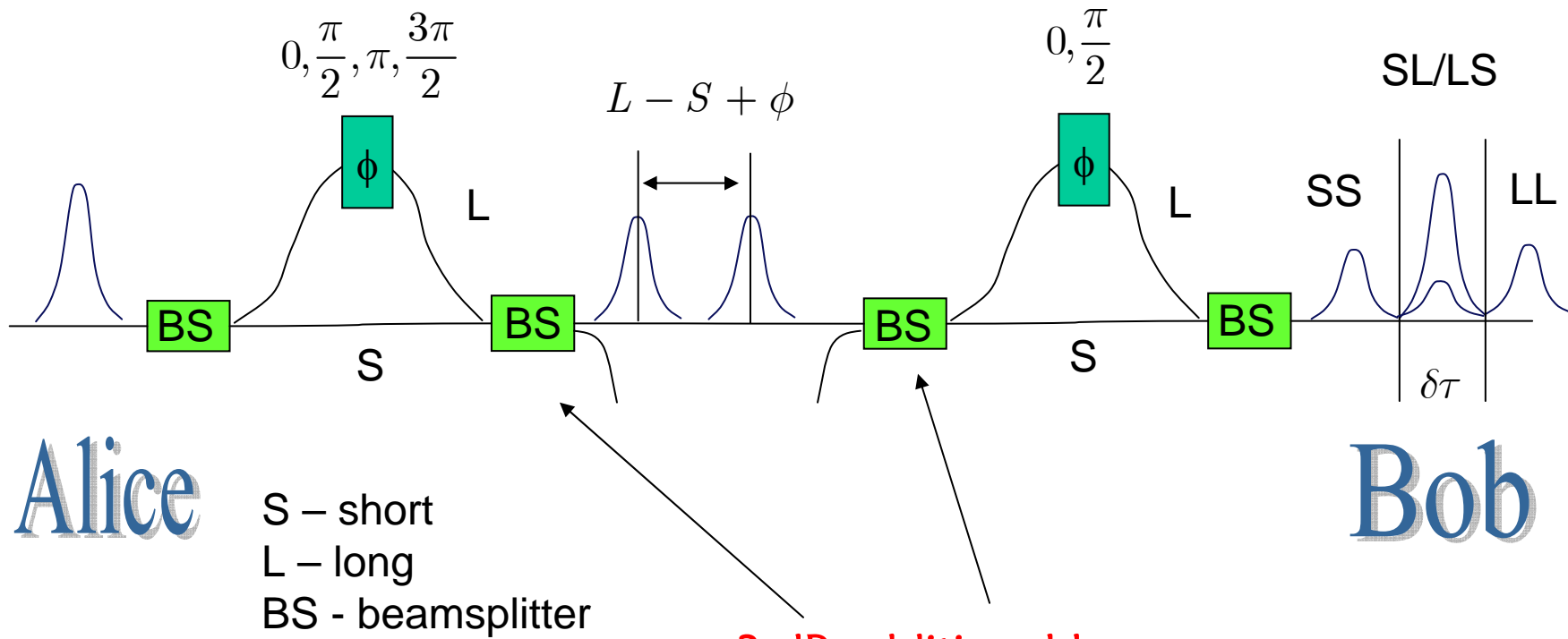
Very stringent requirement on QE/DC ratio – 10^{-5} or better! DC= 10^{-5} - 10^{-7}
QE=10%

Plug-and-Play scheme



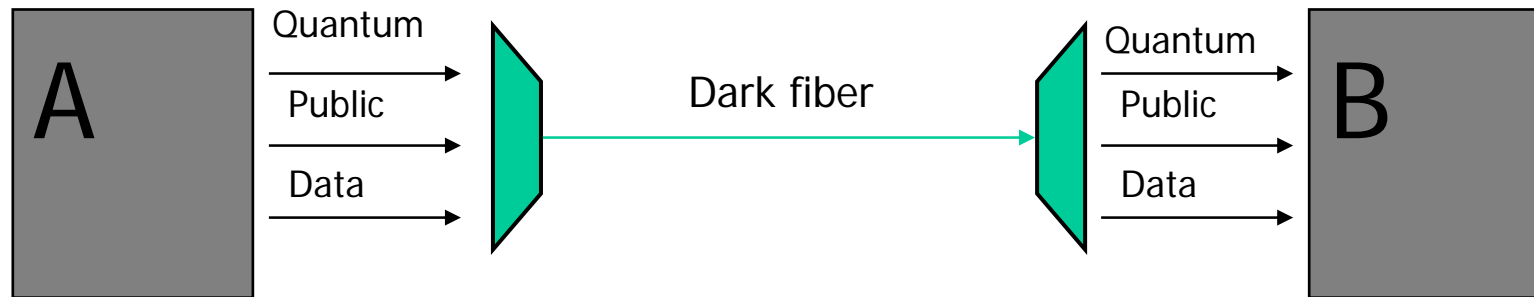
Releygh backscattering problem, security loophole,
 But – stable and easy to maintain.

MZ time-bin interferometer



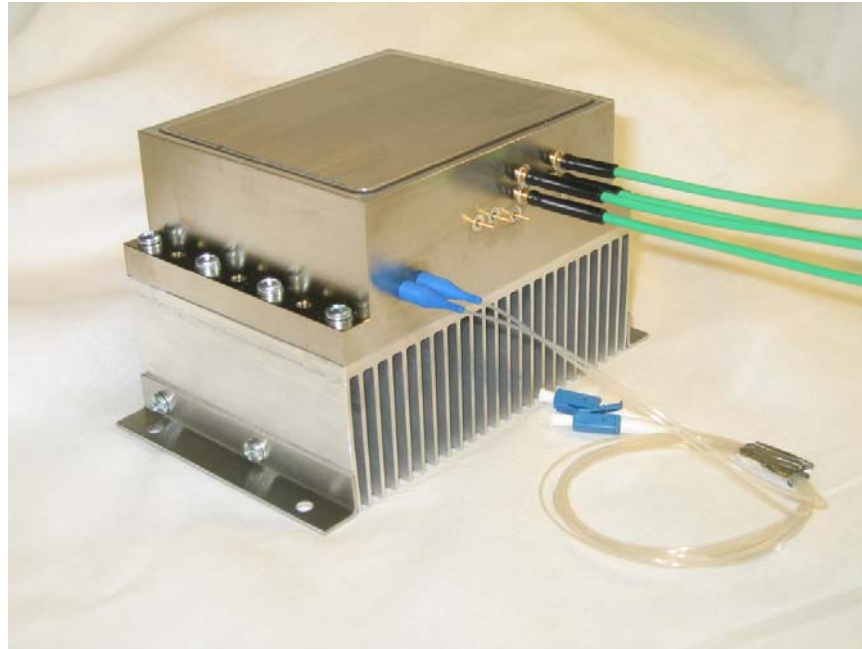
3 dB additional loss
 + stabilization problem – Plug and Pray

QKD channel - multiplexing



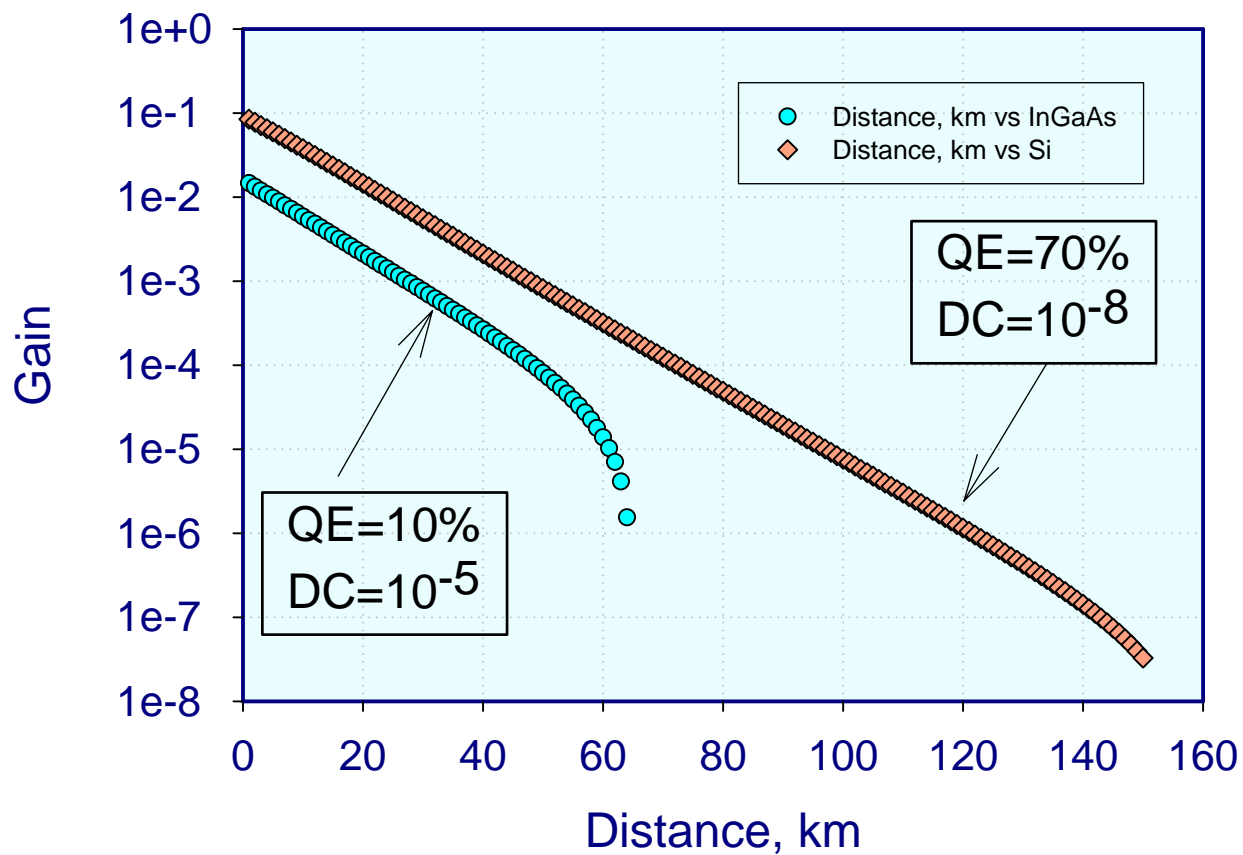
- **Public channel** used for all the data and timing information exchange necessary to run the QKD protocols
- **Data channel** is used to transfer the encrypted data for the user
- **Dedicated dark fiber** is preferable (if not compulsory) for long distance quantum communication
- **Raman scattering** can prevent of multiplexing all the channels in one fiber! (see *APL* (2005) 86(1), 11103)

Single photon counting module



Dark counts/sec:	3000
Quantum Efficiency:	10%
Temperature:	-60 C
Time resolution:	600 ps
Wavelength range:	1100-1600nm (aprox)

Performance of WCP QKD vs. detector spec
for realistic InGaAs detector and hypothetical case
of Si-APD spec

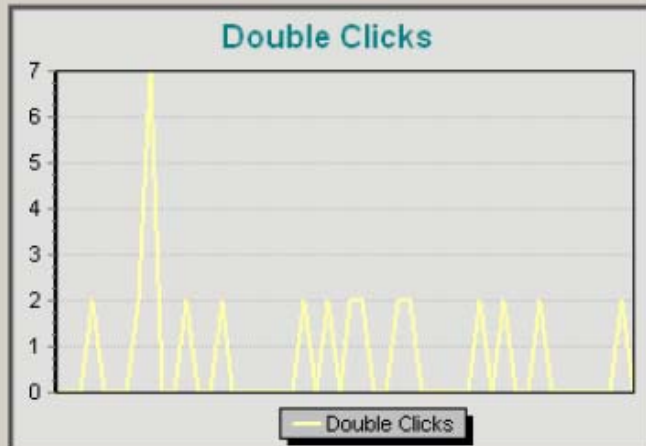
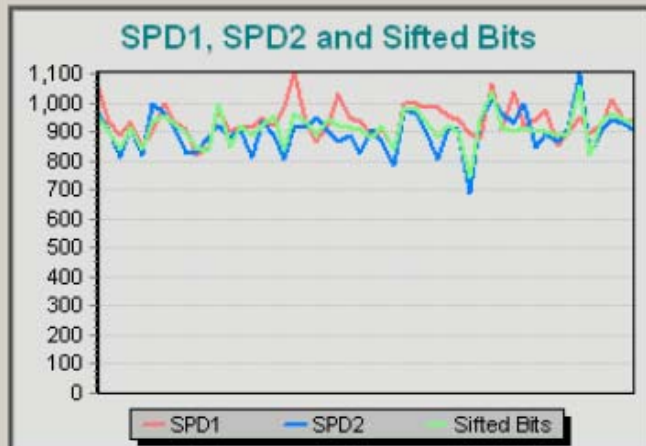


System test – QPN 5505

- System was tested with 75 km of optical fiber
- 24 hours/7days test was performed
- Major parameters:
 - Fiber loss – 18 dB
 - Fiber – SMS-28
 - Laser pulse repetition rate – 600 kHz
 - Average photon number launched – 0.05/pulse
- Results:
 - Error rate - 1-2%
 - Average key rate – 1.7 bits/sec - 574 keys (256 bits) per day!
Or a key every 3 minutes
 - Perfect stability



QKD



Data	Values	Thresholds	Log
SPD1:	936	<input type="text" value="100"/>	
SPD2:	912	<input type="text" value="100"/>	
Error Rate:	5.6076 %	<input type="text" value="10"/>	<input type="checkbox"/>
Key Rate:	367 bits/sec	<input type="text"/>	
Keys:	37	<input type="text" value="Empty"/>	<input type="text" value="Full"/>



Tunnels

The following Tunnels are installed:

#	Alias	State	Bob->Alice	Alice->Bob
1	Data Tunnel One	Active	219.06 Mbps	219.06 Mbps
2	Data Tunnel Two	Active		
3				
4				
5				
6				
7				
8				

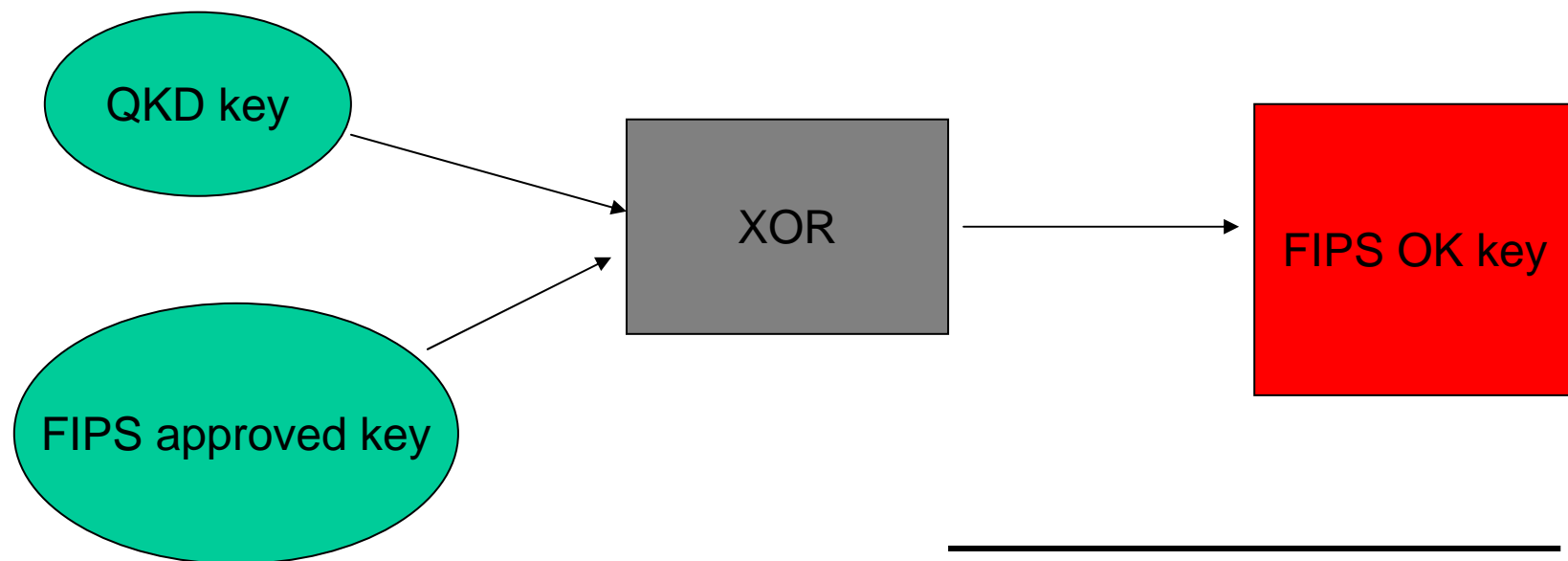
Properties Create Delete Activate Deactivate Stop Stats

Mbps

— Alice->Bob — Bob->Alice

FIPS certification ?

- There are no standards for QKD ☹️
- There are standards for CKD 😊
- Solution:



QPN 7505 main features

- Major upgrade of QPN 5505
- Up to 100km
- Only one fiber needed for everything but client data; multiplexing of QKD and client data under 25 kilometers)
- Modular architecture supports upwards migration to true carrier class
- Ethernet based backplane, to support carrier class chassis design
- IPsec Gateway: Wire-speed secure tunnel for the client data (up to 8 1 Gbps tunnels).
- 2 to 8 1-Gigabit User Data Ports
- Leveraging Cavium high end IPSEC encryption engine
- Supports a variety of network configurations:
 - Dedicated link virtual LAN.
 - Dedicated link enterprise intranet.
 - Enterprise extranet VPN.
 - Carrier network.
 - Cascaded QPN.
 - Storage area network.



Test results

- Up to 100 km
- Up to 200 km for two cascaded systems
- 24 hours/7days test
- Good Stability Results
- Available now
- Current Test sites: Defense, OEM, and Major Telcos
- Organizations interested in a free test drive of the QPN 7505 should apply at www.magiqtech.com