The Quantum Information Processing Company

Bob Gelfond, CEO

QIP Impact

"Quantum information is a radical departure in information technology, more fundamentally different from current technology than the digital computer is from the abacus."

- William D. Phillips, NIST 1997 Nobel Laureate in Physics

"In the nineteenth century, life was transformed by the conscious application of classical mechanics, in the form of Newton's equations (and, later, thermodynamics) to the engines of the industrial revolution. In [the 20th] century, a similar transformation has been wrought by electromagnetism, in generating and distributing electric power and communicating words and pictures across the world at the speed of light, in what should be seen as the conscious application of Maxwell's equation. It is easy to predict that in the twenty-first century it will be quantum mechanics that influences all our lives."

- Prof. Michael Berry, Bristol University

Leverage Point Between Private and Public Sectors

- MagiQ is leveraging past research and ongoing research funding ($100m/year in the US)
- Technologies from QIP are over 20 years old and ready to be commercialized
  - BB-84 protocol has been through the necessary vetting process in academic and government labs
- MagiQ has built infrastructure to commercialize QIP related technologies
- Sweet spot for developing and acquiring intellectual property

Multiplies Impact of Private Investment in MagiQ

MagiQ Corporate Background

- **Founded in July 1999**
- **Headquartered in NYC with R&D Laboratories in Somerville, Mass.**
- **Successful and Senior Management Team with broad background.**
- **Awards**
  - ***Scientific American* "Business Leader" in computing as part of the Scientific American 50**
  - **IEEE Spectrum's "Top Ten Companies to Watch for Next 10 Years"**
  - **World Economic Forum (Davos) Technology Pioneer**
- **Dual Business Strategy**
  - **MagiQ is developing and is selling commercial quantum information devices with 70% gross margins.**
  - **MagiQ is simultaneously building a broad portfolio of intellectual property - 50 patents pending/issued.**
- **QPN™ – Quantum Private Network**
  - **MagiQ launched first commercial quantum device in 2003.**
  - **Standards based VPN appliance with Quantum Key Distribution**
  - **Next generation QPN 7505 will be commercially available in November**
    - **Multi gigabit data plane**
    - **Remote monitoring, management, and alarming**
    - **Multiplex quantum keys and data on same fiber**

MagiQ is the Leader in a New and Profitable Category.

Financing

- Substantial angel-only funding to date.
- Angels Include:
  - Jeff Bezos, Amazon.com founder and CEO
  - Robert Gelfond, MagiQ founder and CEO
  - Neal Goldman, President of Goldman Capital Management
  - Walter Riley, Chairman and founder, Global Overnight Delivery (G.O.D.)
  - Joseph Flom, Partner, Skadden, Arps, Slate, Meagher & Flom
  - Other highly successful Wall St. professionals and technology entrepreneurs.
- Could accelerate revenue and profits by investing in additional engineering, sales, and marketing resources
- Open to discussions on a larger scale institutional round
  - Strategic
  - Private Equity
  - Venture Capital

Sustainable Business Model That Can Be Accelerated

MagiQ's Milestones

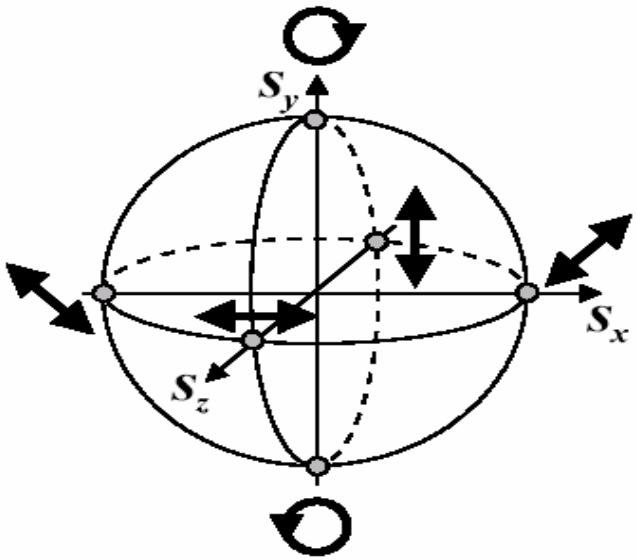
- QPN has been sold and shipped to Europe, Asia, and North America – both commercial and government sales.
- We have sold systems to organizations that test and recommend technologies to the branches of the military
- Distribution agreements in place for Europe, Japan and Israel
- RSA audited our security architecture, and found significant advantages compared to PKI and other key management approaches.
- Partnered with Cavium for GB/sec encryption chips that interface standard IPSec to quantum keys
- Involved in OEM discussions with top tier VPN and transport gear makers
- Analyst coverage of quantum crypto by IDC and Frost & Sullivan
- Demoed QPN at Bank of England event March 2005
- Interoperability with major VPN appliance
- Ongoing QPN 7505 field tests with major telecoms (including AT&T) and telecom equipment makers

Track Record of Successful Execution

Quantum Key Distribution: QPN

What Is a Qubit?

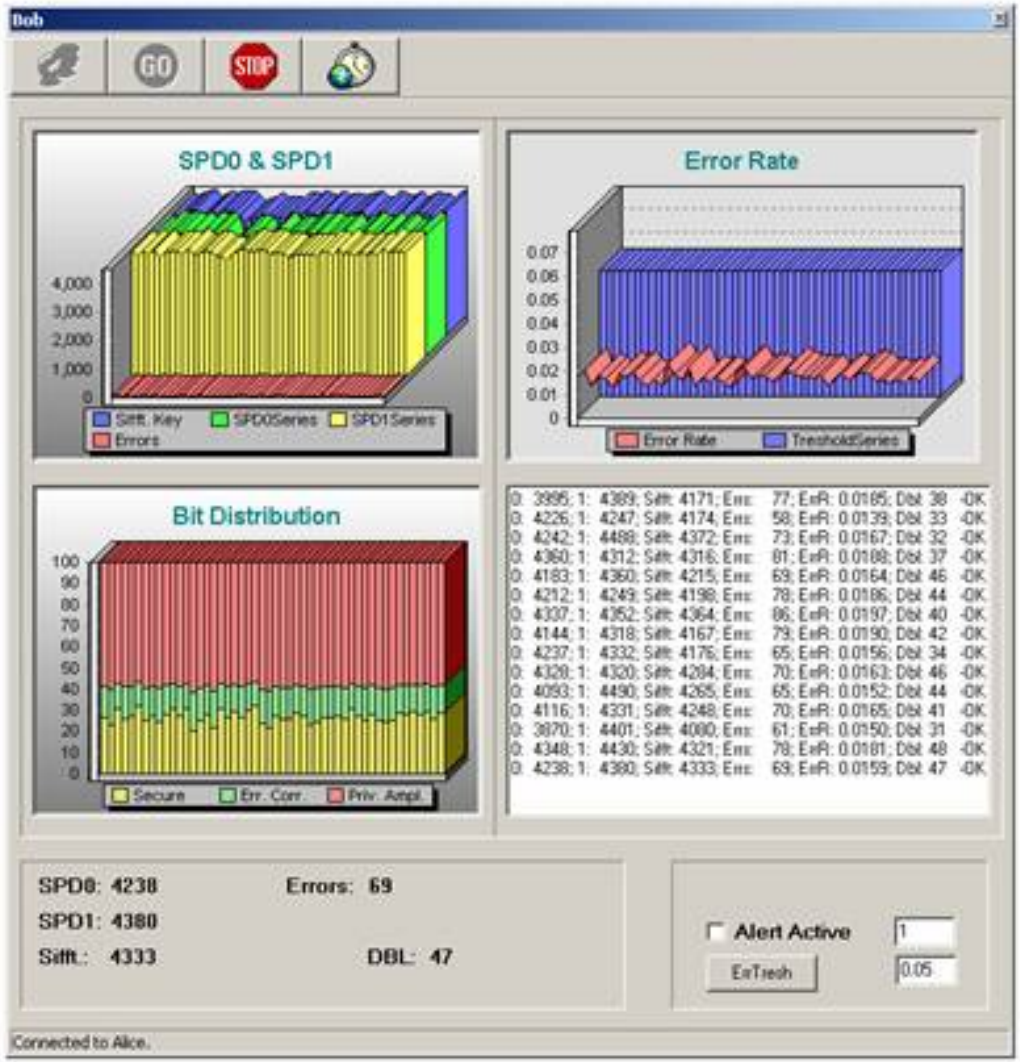
- Exploiting quantum information.



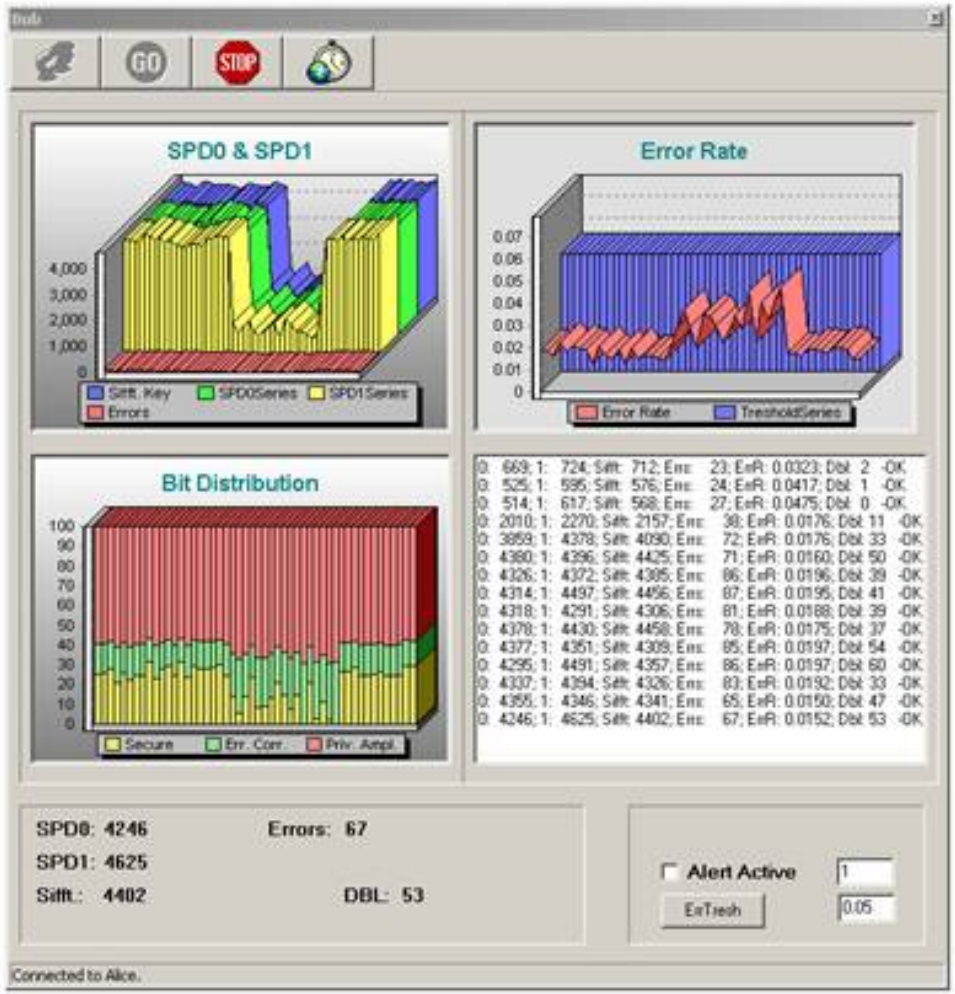
Quantum Bit (Qubit).

- Qubits are in a superposition of 1 and 0.
- N qubits can store 2^n numbers.
- Classical bits represent 1 or 0.

QPN: Steady State



QPN: Compromise Detected



Why QPN Is Needed *Now*?

QPN Key Market Drivers

- The heightened awareness of security vulnerabilities
- Compliance with regulatory requirements in the United States, European Union, and Japan
- The return on investment for QPN by avoiding breaches in security
- Long-term protection of secrets
- Increased deployment of fat optical pipes carrying critical voice and data

Market Ripe for Evolution of Security Functionality

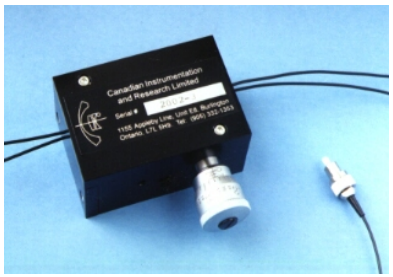
Why QPN is Needed Now

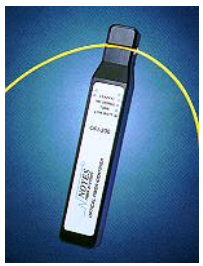
- On average keys are changed infrequently making brute force attacks much easier
- Reduces human element of alternatives like PKI
- Trusted Courier and Current VPN products are subject to key access attacks
  - Social engineering
  - Internal threats
    - Disgruntled employee
    - Contractor who is conducting corporate or economic espionage
  - SSL, PKI
    - Server or PC storing keys can be compromised
    - Relies on Trustworthiness of the Certificate Authority (CA)
  - External threats
    - Tapping is ubiquitous, easy and inexpensive
    - Carrier and Campus fiber networks are wide open to tapping of data
- Boeing was tapped by AirBus (2002).
- US businesses lose over $500B/year in sales because of economic espionage (US Government).

Threat Profile is Growing

Tools for Security Breach

- Optical taps
  - May be easily created using common maintenance equipment that can be purchased legally and cheaply worldwide
  - Allow unfettered access to all voice and data communications transiting an optical fiber
  - Are not detectable in today's optical networks
- Packet-Sniffers filter out specific packets based on header and store and analyze the data

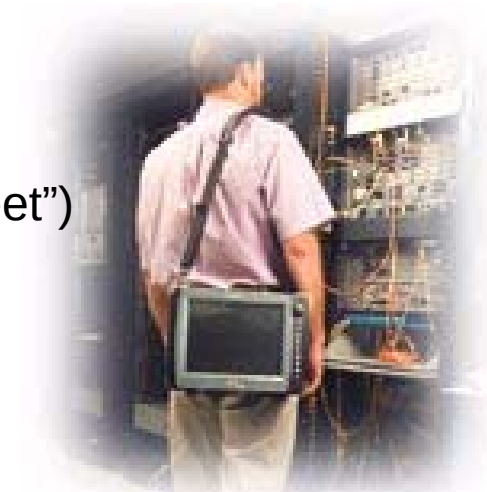


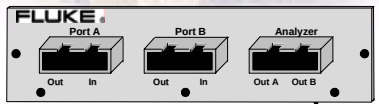


Opportunities for Security Breach

Carrier Equipment Locations

- Central Office
- Co-located leased space
- Carrier Hotels (“60 Hudson Street”)
- Commercial Office Buildings
- Office Building Wiring Closets
- Outside Plant Equipment Huts
- Personnel access





Network Access Concerns

- Undetectable Fiber Taps
- Fiber Cross Connects Patch Panel
- Network Probes
- Out of Band Management Network
- Monitoring Access Ports
- Local DTE Access Ports

Why QPN is Needed Now

Evolving Threats to Cryptographic Security

- Advancements in mathematical methods, cryptanalysis attacks, and increases in computational power can weaken security methods that are currently in use
- Keys are continualy getting larger to try to maintain same level of security
- Even without quantum computers improvements in hardware can present threats such as Bernstein's circuit for factoring large numbers

Cryptanalysis - Study of methods for obtaining the meaning of encrypted information without access to the secret information

- PKI
  - Diffie-Hellman (1976) weakened by discovery of a computational way to find discrete logarithms (Coppersmith 1983).
  - The security of the RSA algorithms, rests in the difficulty of factorizing large integers.
    - RSA 576 bit key factored in 2003, now recommends use of 2048 bit keys
- Cryptographic Hash Functions
  - MD5 (1991), collisions discovered (1996, 2004), recommend replacements
    - Still in use in many programs today
  - SHA-0 replaced by SHA-1 (1995) by NSA & NIST
  - SHA-1 cracked February 2005
- Encryption algorithm –
  - DES (1976) no longer recommended for use
  - NIST now recommends use of 3DES or AES (2001)
  - Many banking and financial funds software still using DES imbedded in software
    - Replace costs and time needed to move systems away from DES are high
  - XLS Attack- Courtois and Pieprzyk (2002) thought to pose a threat to AES encryption algorithm

Stops the Battle Between the Code Makers and the Code Breakers

QPN Market Segmentation

		Application Types		
Market Segments		Disaster Recovery	Enterprise Network	Metro Area Network
	Service Providers (Communications Infrastructure)	H	H	H
	Financial Services	H	H	H
	Military/Government	H	H	H
	Homeland Security (Power Grid, Nuclear Power Plants, Airports, Dams, Law Enforcement)	H	H	H
	IP Intensive Industries (Aeronautics, Pharmaceutical, Bio Tech, High Tech)	M	H	M
	Health Care/Insurance	M	M	M
	Manufacturing	M	M	L
	Entertainment	M	M	L
	Legal	L	M	L

H – High M- Medium L-Low

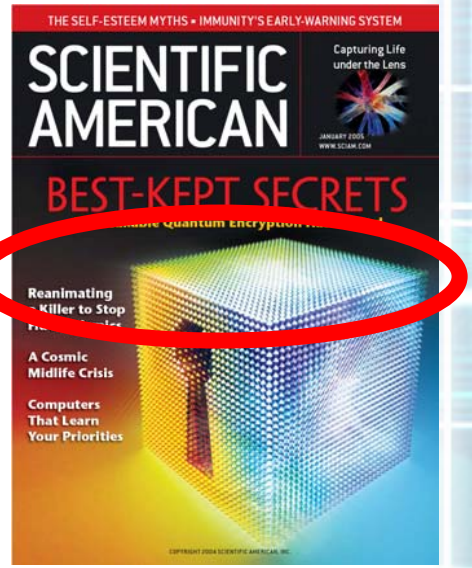
QPN Benefits: Best Return on Investment

- Competitive advantage gained by deploying QPN
- Reduced costs by thwarting theft of financial transactions or intellectual property
- Protection of company reputation and goodwill
- Increased assurance based on the best of breed security technology
- Audit and regulatory compliance
- Ongoing and reliable security for sensitive, trusted, or regulated information
- Cost effective security deployment
- Lowest total cost of ownership

Turn Security into a Profit Center

Market Pull for QPN

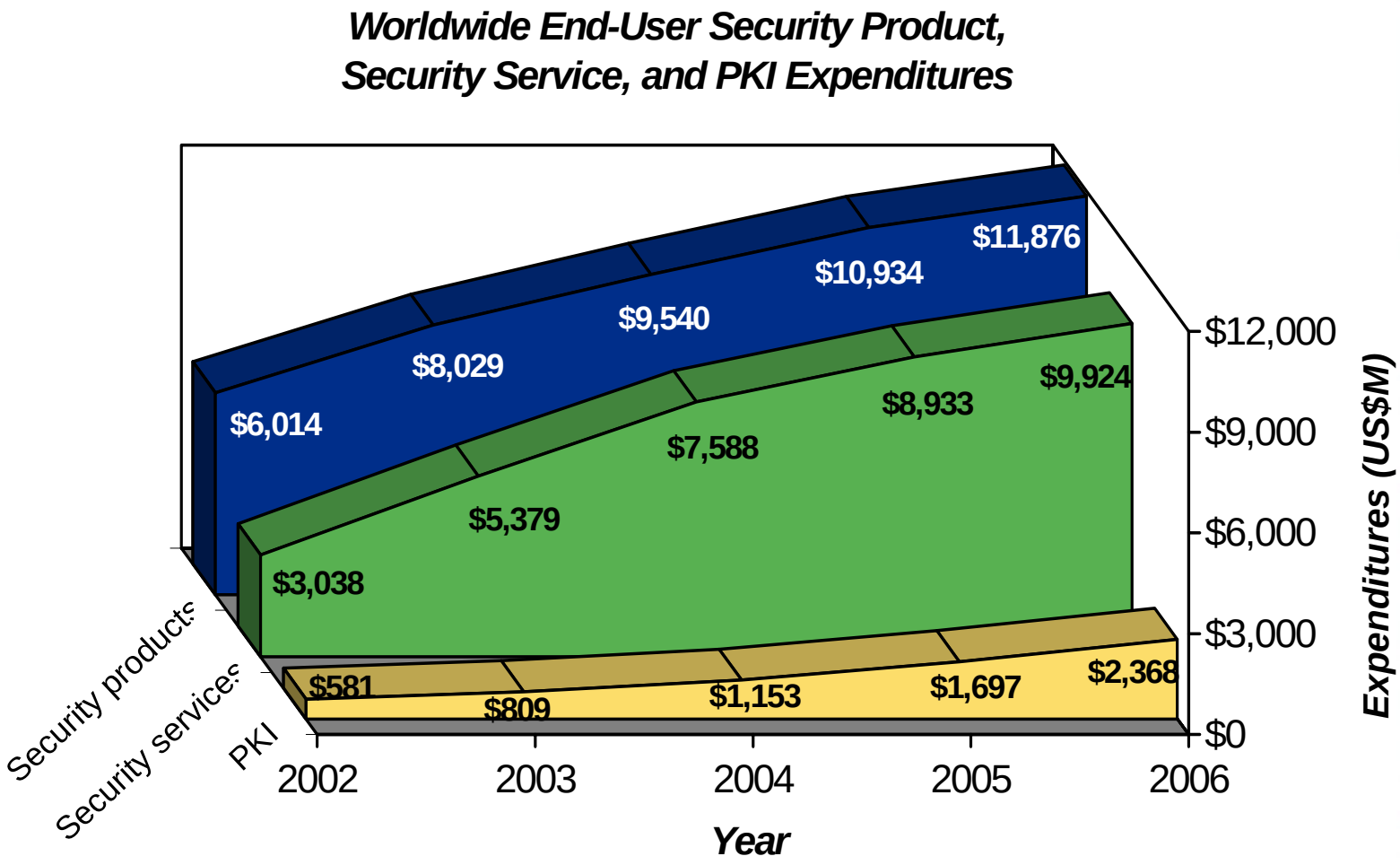
- MagiQ's QPN has been covered in:
  - Scientific American (named an SA50 as the Business Leader in Computing)
  - IEEE Spectrum (named one of Top 10 Tech Cos. for the Next 10 Years)
  - Economist
  - Wall St. Journal
  - Nikkei
  - New York Times
  - Associated Press
  - Major Broadcast Outlets
  - All relevant trade publications in optics, networking, security, and high tech
  - Recent survey of 30 CSOs indicated that they had all seen multiple sources of coverage on quantum cryptography



QPN Has Captured People's Imagination.

Market Size and Competition

Security Product/Service & PKI Forecast



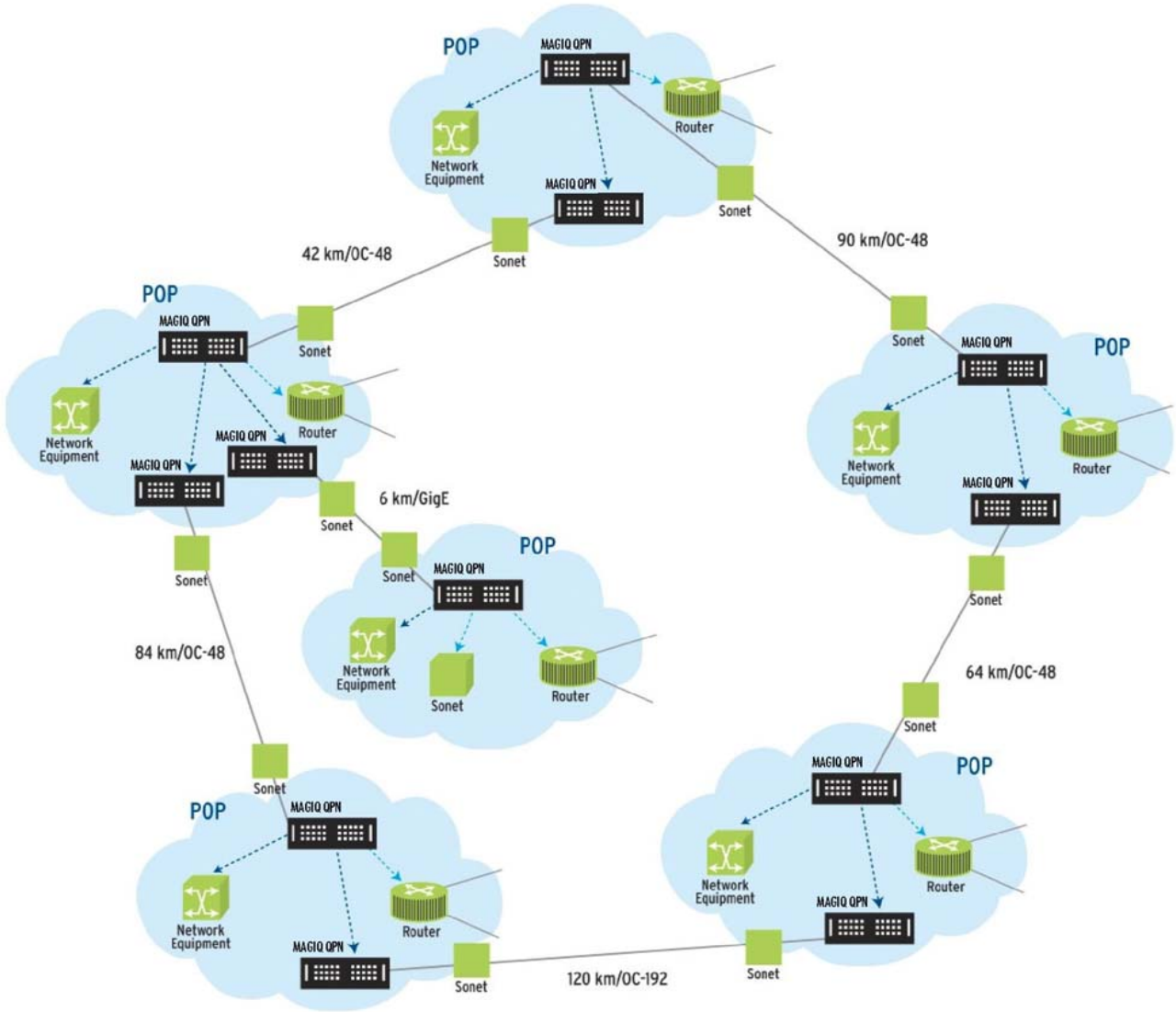
Primary Competition

- Startups
  - id Quantique, Switzerland
  - SmartQuantum, France
  - Optemax, Maryland
- Commercial Research Houses
  - BBN, MA
  - QinetiQ, UK
- Japanese companies are testing the market, all of these look likely to produce commercial systems:
  - NTT recently announced plans to deliver a commercial system by mid-2007.
  - NEC
  - Mitsubishi
  - Toshiba
  - Fujitsu
- D-Wave Systems - Vancouver, Canada
  - Working only on superconducting qubits for quantum computation
- US companies are doing blue sky research
  - IBM
  - HP
  - Bell Labs

Any of these commercial QKD systems will likely need to license MagiQ's IP

QPN Deployment Case Studies

Secure Telecom Network



NEON Footprint