MagiQ Technologies

The Quantum Information Processing Company

Quantum Cryptography in the Real World

Ray Bassler
CTO
BCANetwork, LLC

Simple Fact

A couple thousand dollars worth of equipment, some packet-sniffer software, and a little homework can garner unfettered access to all data and voice communications on an optical network segment today with little risk of being detected.

Why is this important?

- Over 180 million miles of optical fibers exist worldwide
- All critical communications infrastructures rely on fiber optic networks
  - Voice, data, video, transactions, wireless, Internet, financial, TV, Satellite up/down links, etc.
- Corporations require confidential communications and data exchange in order to compete effectively in global marketplace
- Individuals expect privacy of their conversations and sensitive personal information
- Modern economies rely on the reliability and integrity of communications networks
- Fiber optics have been portrayed as a more secure method of transmitting data

Fiber optics networks are in fact quite *vulnerable and insecure*

QKD

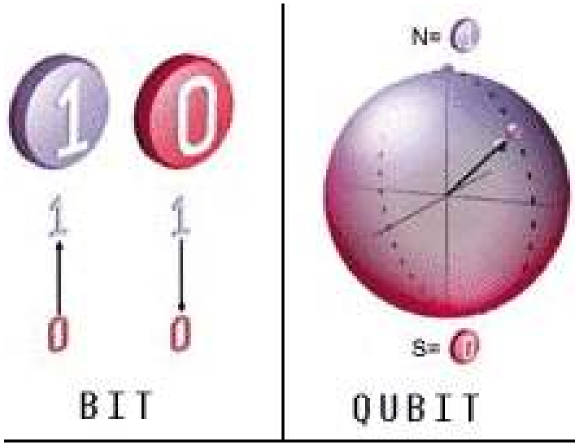
Original IDEA

“The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this “quantum noise,” quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.”

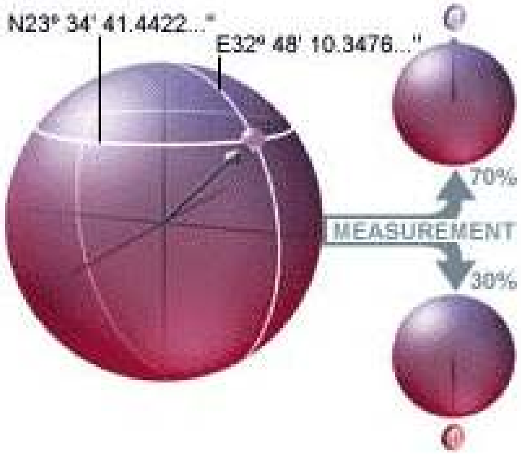
Stephen Wiesner 1970

Conception of a qubit

Unlike the classical bit, the qubit can be in the superposition of ones and zeros



Measurement of the qubit in arbitrary state gives probabilistic answer



Examples of a qubit systems

- Photon polarization
- Single-photon Mach-Zehnder interferometer
- Two-level atom
- Spin ½ system
- Josephson junction
- etc

Ekert protocol

The protocol use entanglement as a method for key exchange between distant parties

$$|\Psi^{-}\rangle = \rightarrow - \rightarrow (|\ \rangle\,|\ \rangle\ \ |\ \rangle\,|\ \rangle)$$

This state is the maximally entangled state of two qubits. The state is spherically symmetric, so and the choice of direction does not matter. The state can be produced for example by spontaneous parametric down conversion with Type II phase synchronism.

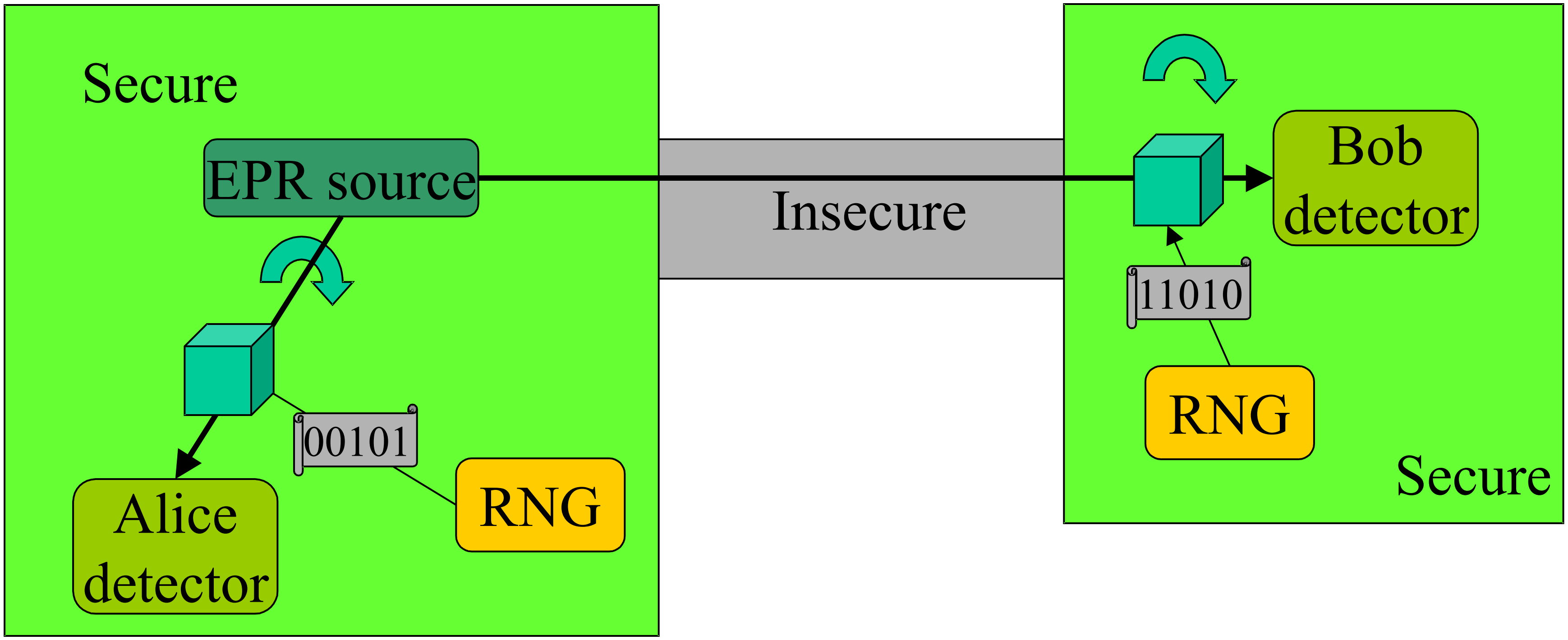
Basic idea: efficient eavesdropping
is equivalent to existence of local hidden variables!

Bell inequality in CHSH form

$S = -2\sqrt{2}$ Quantum theory $S \leq 2$ LHV theory

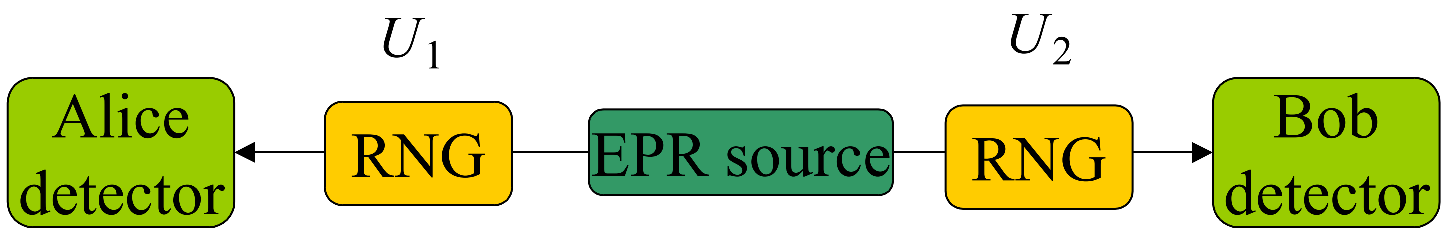
Bennett-Brassard- Mermin protocol

Modification of Ekert protocol made by BBM in 1992



Equivalence of different schemes

E91 or BBM92



U_1

U_2

Alice detector

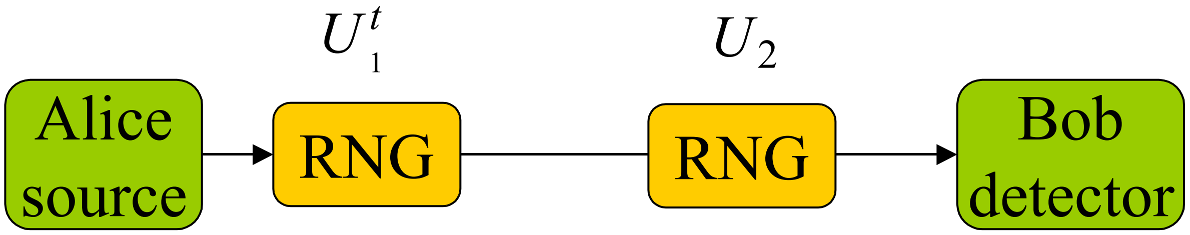
RNG

EPR source

RNG

Bob detector

$U_1 \text{ Ä } U_2 \text{F}^{(+)} = \mathbf{1} \text{ Ä } U_2 U_1^t \text{F}^{(+)}$ Klyshko, 1992



U_1^t

U_2

Alice source

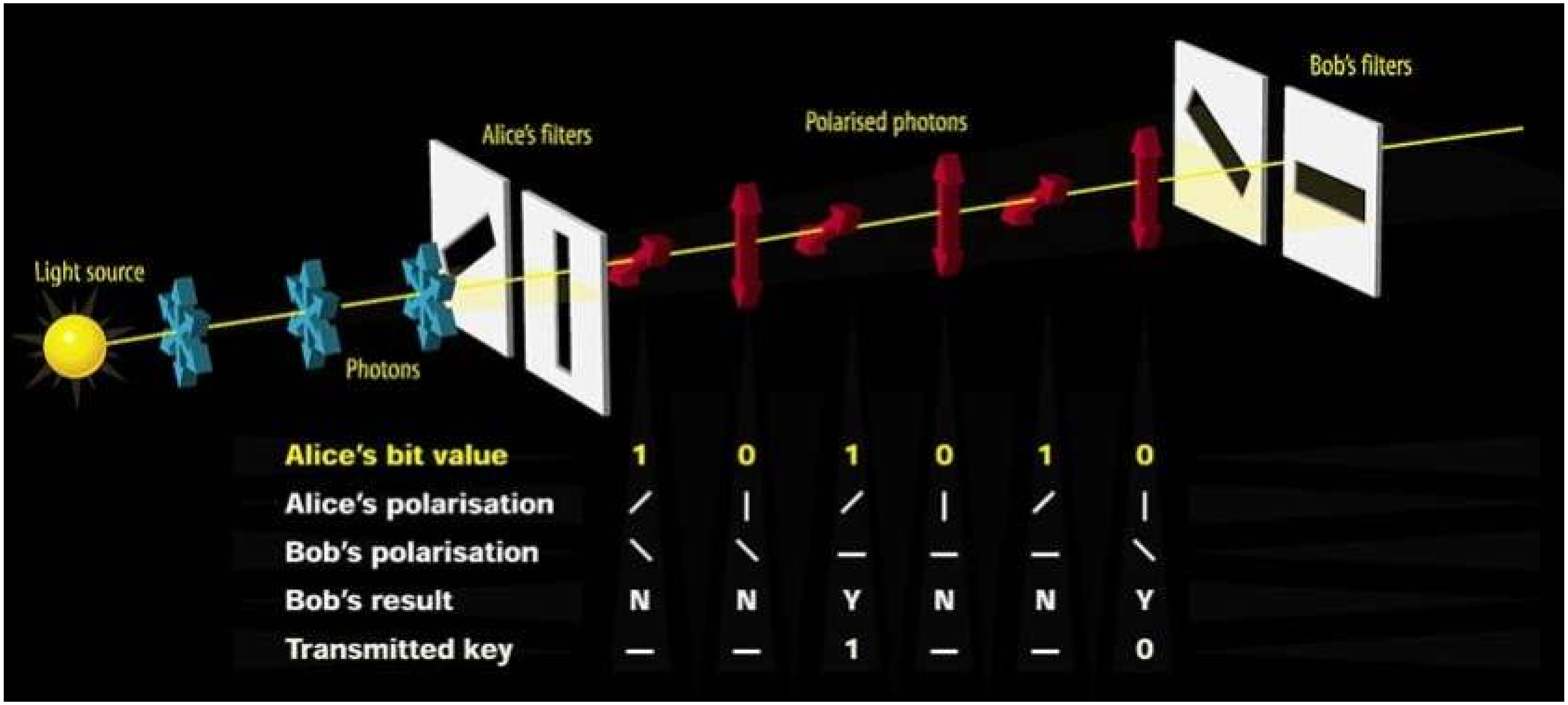
RNG

RNG

Bob detector

BB84

BB84 protocol



Alice's bit value	1	0	1	0	1	0
Alice's polarisation	/	|	/	|	/	|
Bob's polarisation	\	\	—	—	—	\
Bob's result	N	N	Y	N	N	Y
Transmitted key	—	—	1	—	—	0

Quantum Key Distribution

- Absolute security based on fundamental laws of quantum physics, rather than computational assumptions or difficulty
- Enables two organizations who share a small amount of authentication information to communicate in absolute security in the presence of an eavesdropper
- Any eavesdropping attack will always be caught

Intrusion alert!

Eve

Intrusion alert!

Quantum Key Distribution

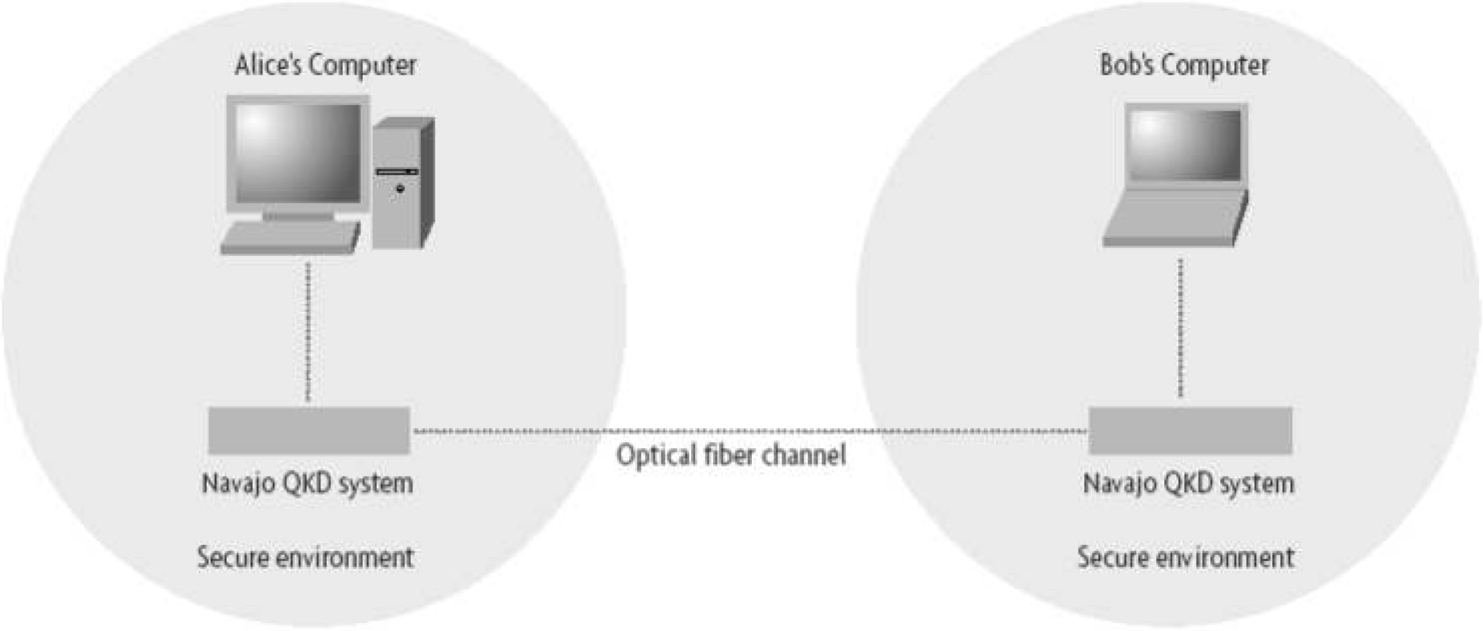


FIGURE 1: SCHEMATIC OF QUANTUM COMMUNICATION SYSTEM

Quantum Key Distribution: Polarization Bases

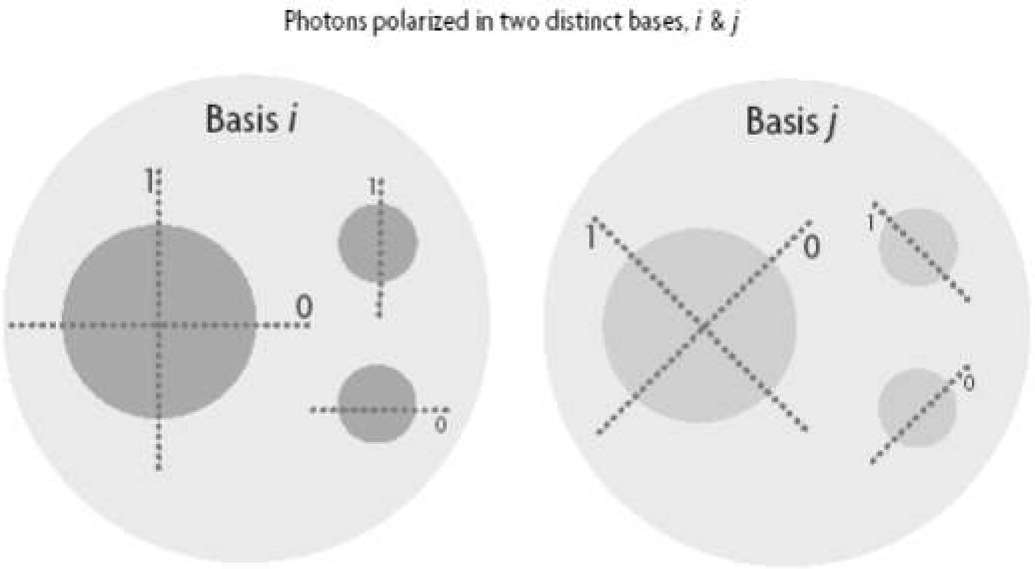


FIGURE 2: POLARIZATION BASES USED TO ENCRYPT PHOTONS IN QKD SYSTEMS

Quantum Key Distribution

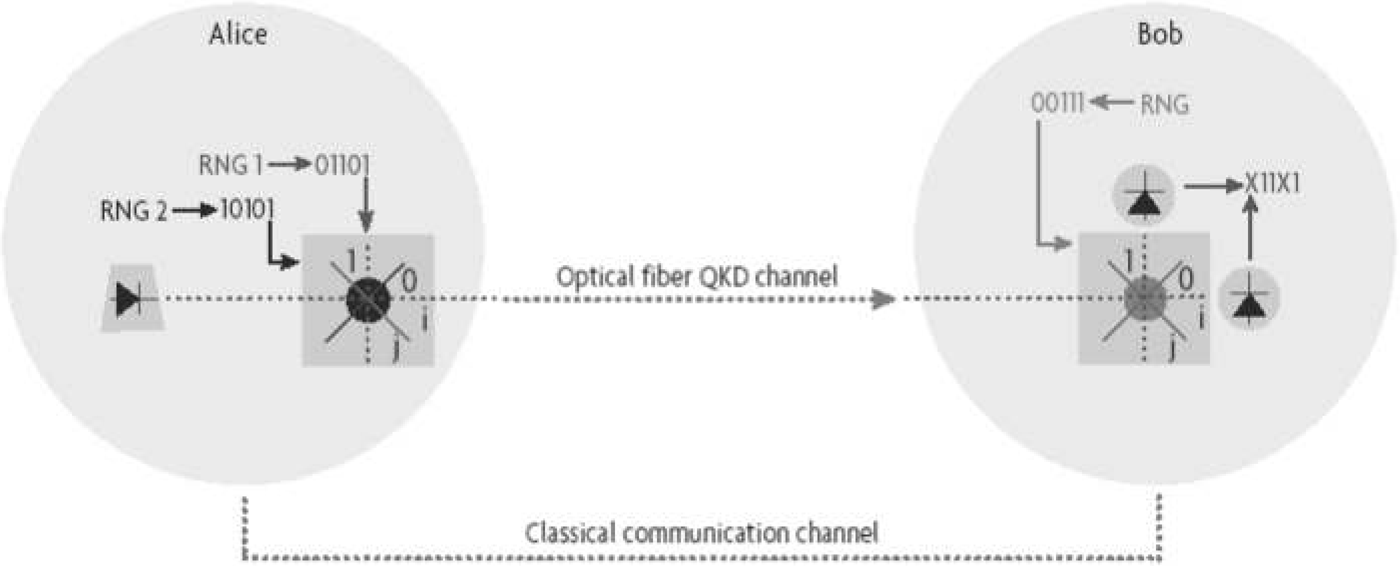
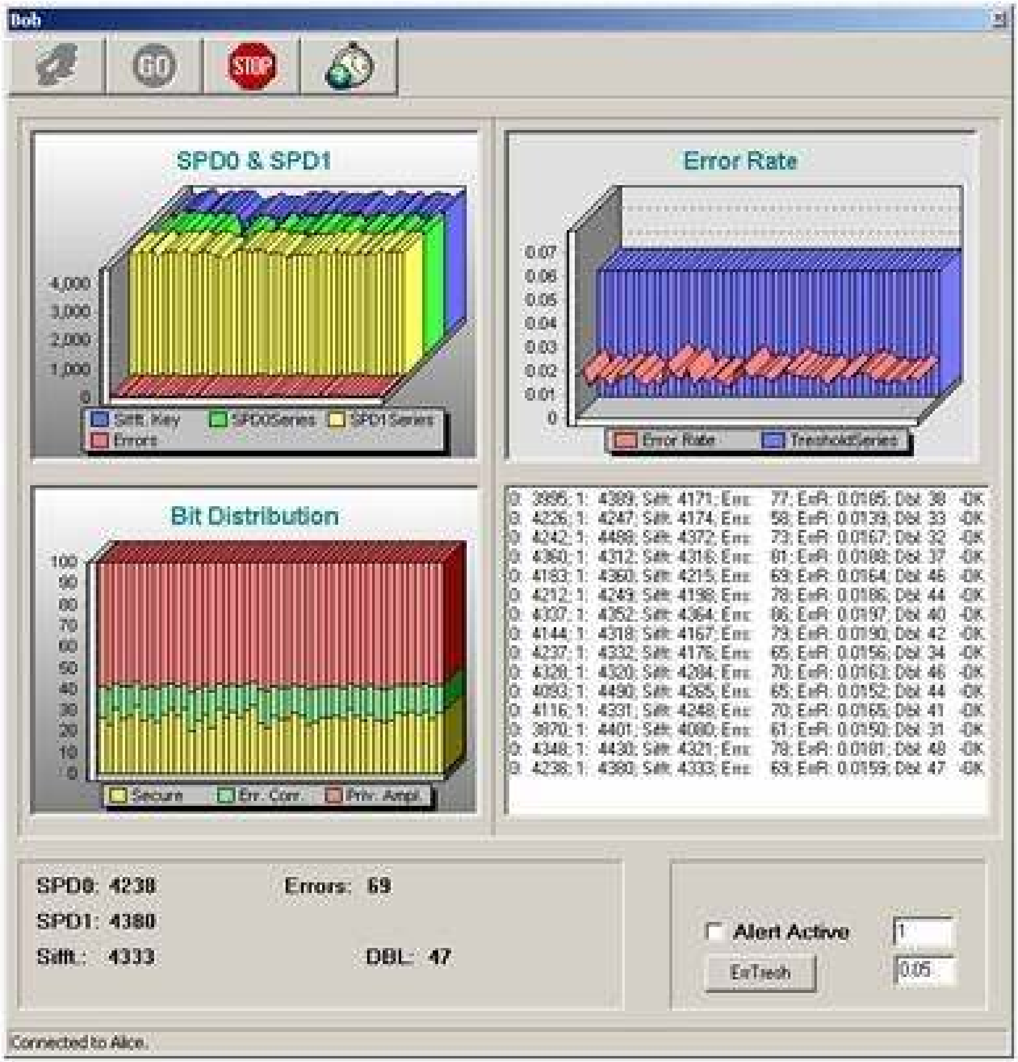


FIGURE 3: SCHEMATIC OF QUANTUM KEY DISTRIBUTION SYSTEM

QKD: Steady State



```
0: 3995; 1: 4389; Sift: 4171; Errs:  77; ErR: 0.0185; Dbl: 38  -OK
0: 4226; 1: 4247; Sift: 4174; Errs:  58; ErR: 0.0139; Dbl: 33  -OK
0: 4242; 1: 4488; Sift: 4372; Errs:  73; ErR: 0.0167; Dbl: 32  -OK
0: 4380; 1: 4312; Sift: 4316; Errs:  81; ErR: 0.0188; Dbl: 37  -OK
0: 4183; 1: 4360; Sift: 4215; Errs:  69; ErR: 0.0164; Dbl: 46  -OK
0: 4212; 1: 4249; Sift: 4198; Errs:  78; ErR: 0.0186; Dbl: 44  -OK
0: 4307; 1: 4352; Sift: 4364; Errs:  86; ErR: 0.0197; Dbl: 40  -OK
0: 4144; 1: 4318; Sift: 4167; Errs:  79; ErR: 0.0190; Dbl: 42  -OK
0: 4237; 1: 4332; Sift: 4176; Errs:  65; ErR: 0.0156; Dbl: 34  -OK
0: 4328; 1: 4320; Sift: 4284; Errs:  70; ErR: 0.0163; Dbl: 46  -OK
0: 4093; 1: 4490; Sift: 4265; Errs:  65; ErR: 0.0152; Dbl: 44  -OK
0: 4116; 1: 4331; Sift: 4248; Errs:  70; ErR: 0.0165; Dbl: 41  -OK
0: 3870; 1: 4401; Sift: 4080; Errs:  61; ErR: 0.0150; Dbl: 31  -OK
0: 4348; 1: 4430; Sift: 4321; Errs:  78; ErR: 0.0181; Dbl: 48  -OK
0: 4238; 1: 4380; Sift: 4333; Errs:  69; ErR: 0.0159; Dbl: 47  -OK
```

SPD0: 4238 Errors: 69

SPD1: 4380

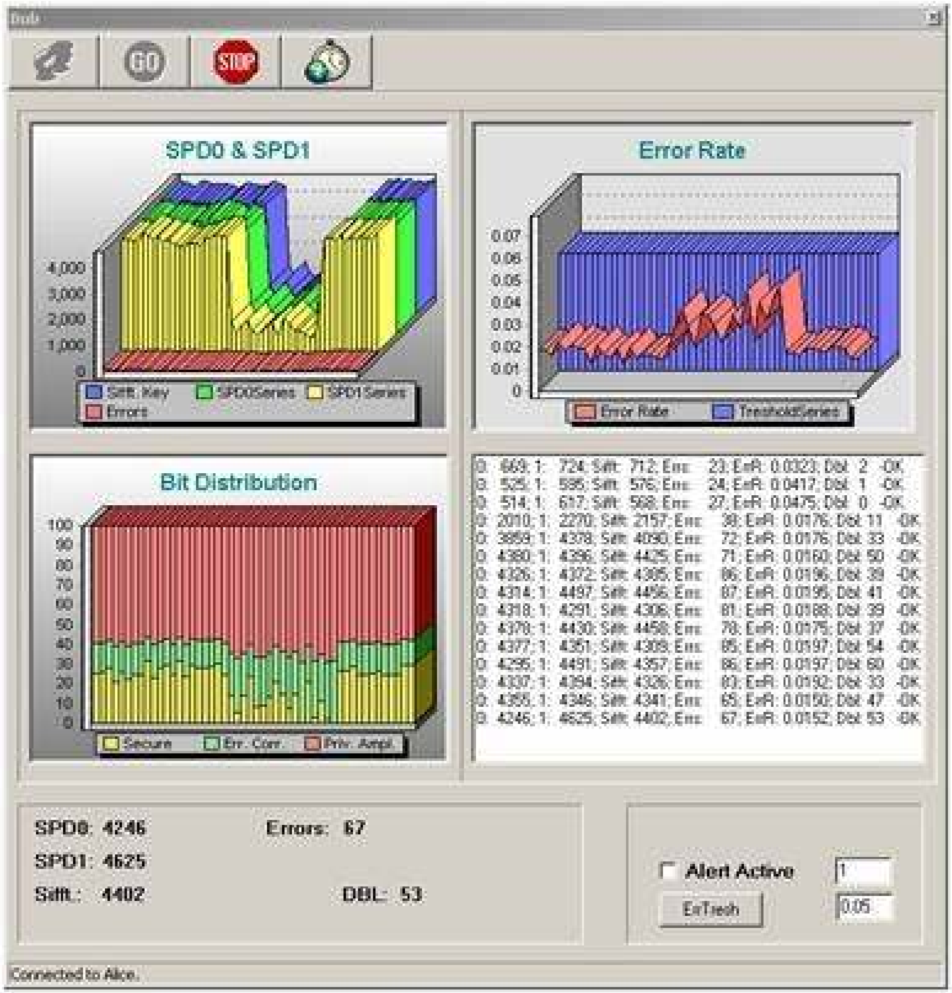
Sift.: 4333 DBL: 47

☐ Alert Active 1

0.05

Connected to Alice.

QKD: Compromise Detected



```
0:  669; 1:  724; Sifft:  712; Errs:   23; ErR: 0.0323; Dbl:  2  -OK
0:  525; 1:  595; Sifft:  576; Errs:   24; ErR: 0.0417; Dbl:  1  -OK
0:  514; 1:  617; Sifft:  568; Errs:   27; ErR: 0.0475; Dbl:  0  -OK
0: 2010; 1: 2270; Sifft: 2157; Errs:   38; ErR: 0.0176; Dbl: 11  -OK
0: 3859; 1: 4378; Sifft: 4090; Errs:   72; ErR: 0.0176; Dbl: 33  -OK
0: 4380; 1: 4396; Sifft: 4425; Errs:   71; ErR: 0.0160; Dbl: 50  -OK
0: 4326; 1: 4372; Sifft: 4385; Errs:   86; ErR: 0.0196; Dbl: 39  -OK
0: 4314; 1: 4497; Sifft: 4456; Errs:   87; ErR: 0.0195; Dbl: 41  -OK
0: 4318; 1: 4291; Sifft: 4306; Errs:   81; ErR: 0.0188; Dbl: 39  -OK
0: 4378; 1: 4430; Sifft: 4458; Errs:   78; ErR: 0.0175; Dbl: 37  -OK
0: 4377; 1: 4351; Sifft: 4309; Errs:   85; ErR: 0.0197; Dbl: 54  -OK
0: 4295; 1: 4491; Sifft: 4357; Errs:   86; ErR: 0.0197; Dbl: 60  -OK
0: 4337; 1: 4394; Sifft: 4326; Errs:   83; ErR: 0.0192; Dbl: 33  -OK
0: 4355; 1: 4346; Sifft: 4341; Errs:   65; ErR: 0.0150; Dbl: 47  -OK
0: 4246; 1: 4625; Sifft: 4402; Errs:   67; ErR: 0.0152; Dbl: 53  -OK
```

SPD0: 4246 Errors: 67

SPD1: 4625

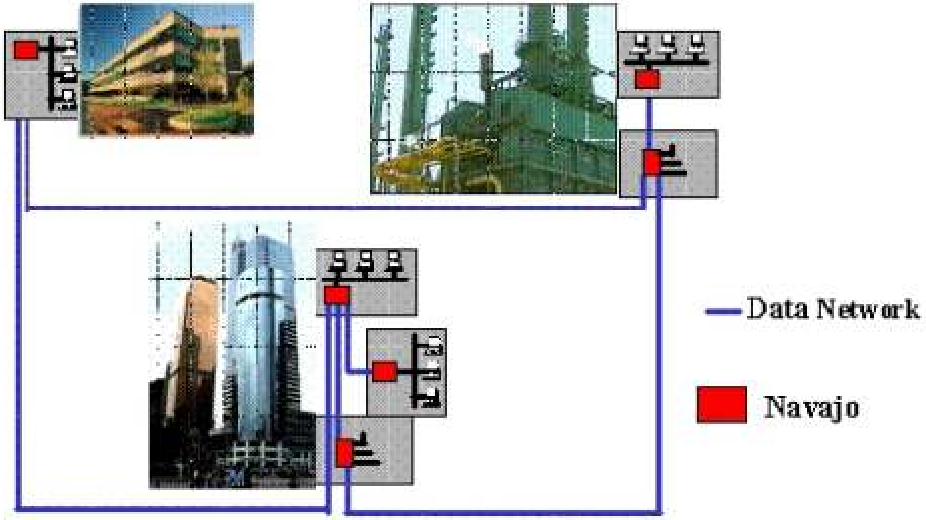
Sifft.: 4402 DBL: 53

□ Alert Active 1

ErrTresh 0.05

Connected to Alice.

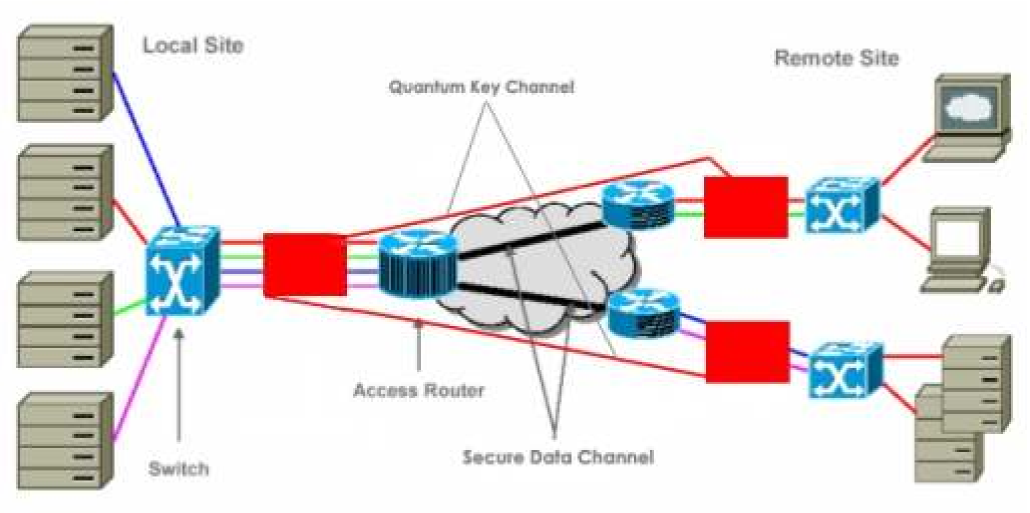
Navajo Enterprise Deployment



Case Study

- Industry: R&D intensive manufacturing company
- Network topology: private network in same metro area
- Security concern: trade secrets, intellectual property, and business plans
- MagiQ answer: lock down point to point data links with Navajo

Navajo Deployment: Enterprise

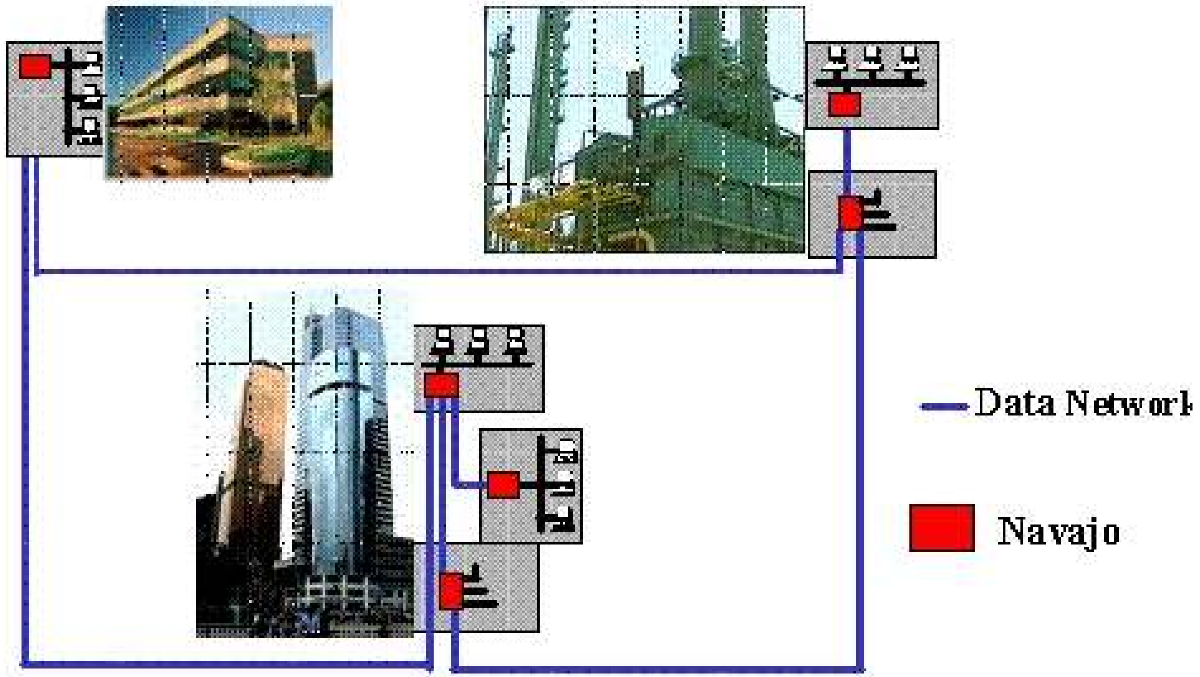


🟥 - Navajo

Case Study

- Industry: Carrier providing Financial Services customer with private network
- Network topology: private network in metro area
- Security concern: security of funds transfer and other transaction based data
- MagiQ answer: Lock down critical data channels with Navajo while locking down overall network with MagiQ VPN and classical products

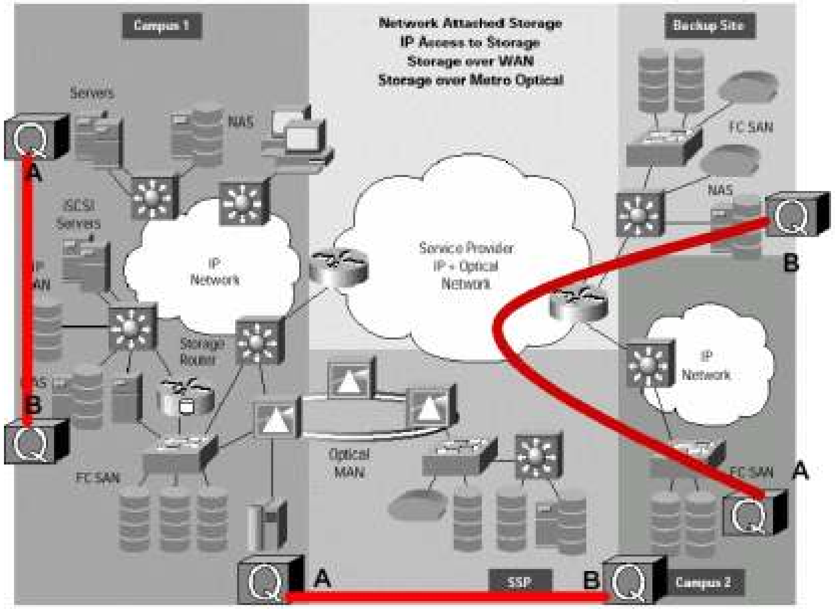
Navajo Carrier Deployment



Case Study

- Industry: carrier providing voice and data to many customers
- Network topology: central office to customer premise Security concern: internal or external threats to confidential customer data and access to the network command channel
- MagiQ answer: Lock down critical nodes with Navajo while locking down overall network with MagiQ VPN and classical products

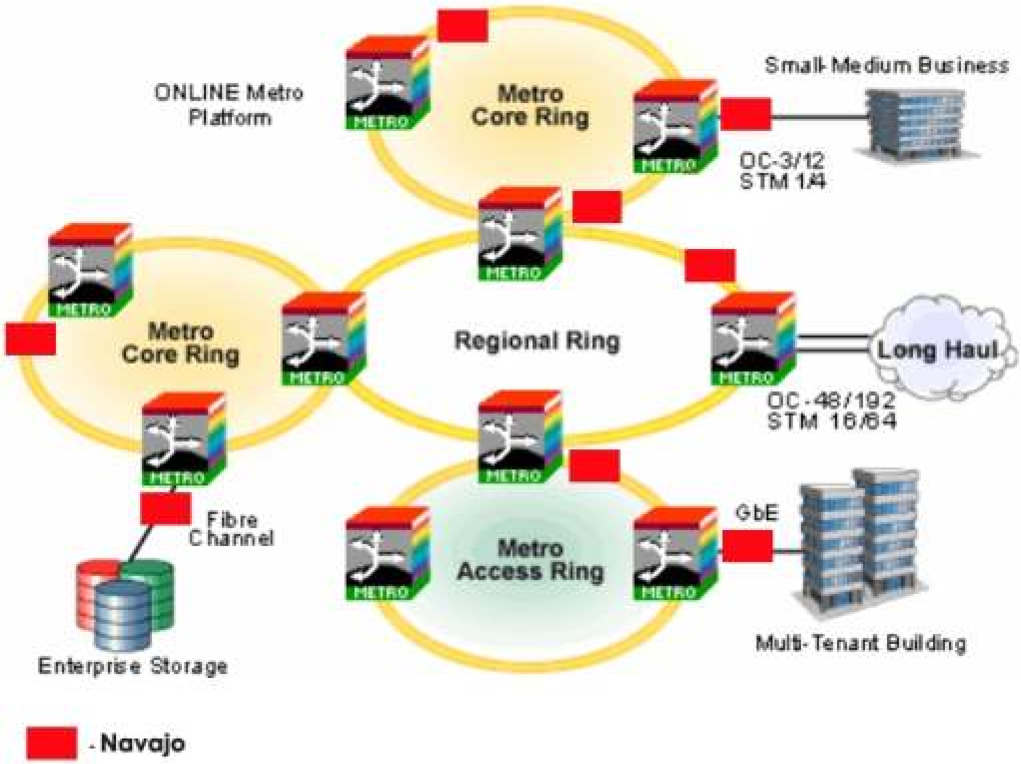
Navajo Deployment: SAN



Case Study

- Industry: High Tech company
- Network topology: Storage Area Network across many campuses
- Security concern: internal or external threats to confidential trade secrets, patents, and product plans
- MagiQ answer: Lock down critical nodes with Navajo while locking down overall network with MagiQ VPN and classical products

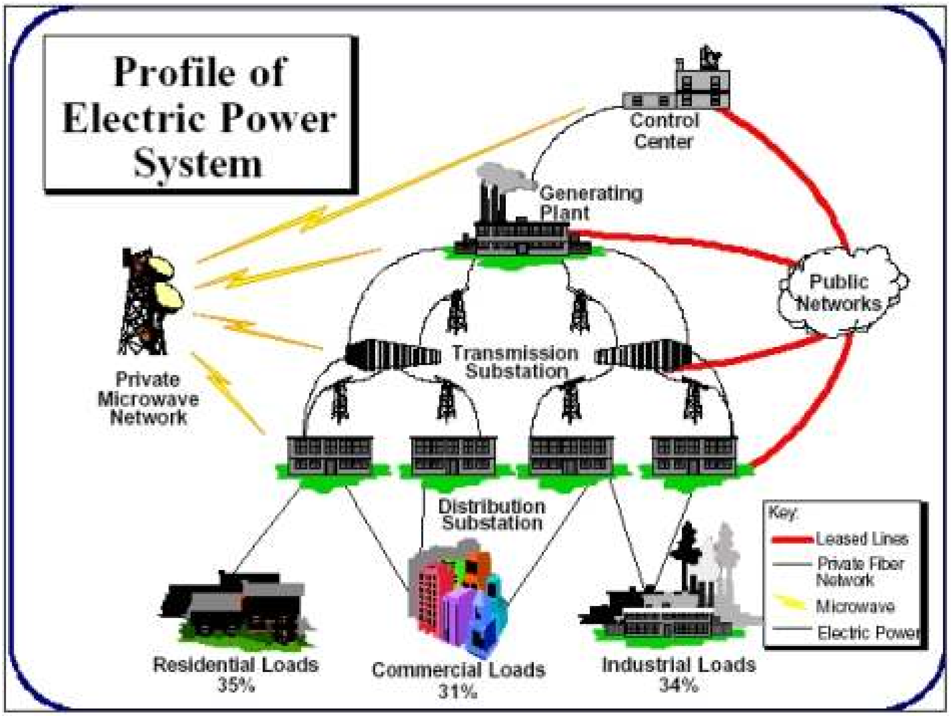
Navajo Deployment: Metro Ring



Case Study

- Industry: carrier providing voice and data to many customers
- Network topology: Metro Area Network
- Security concern: internal or external threats to confidential customer data and access to the network command channel
- MagiQ answer: Lock down critical nodes with Navajo while locking down overall network with MagiQ VPN and classical products

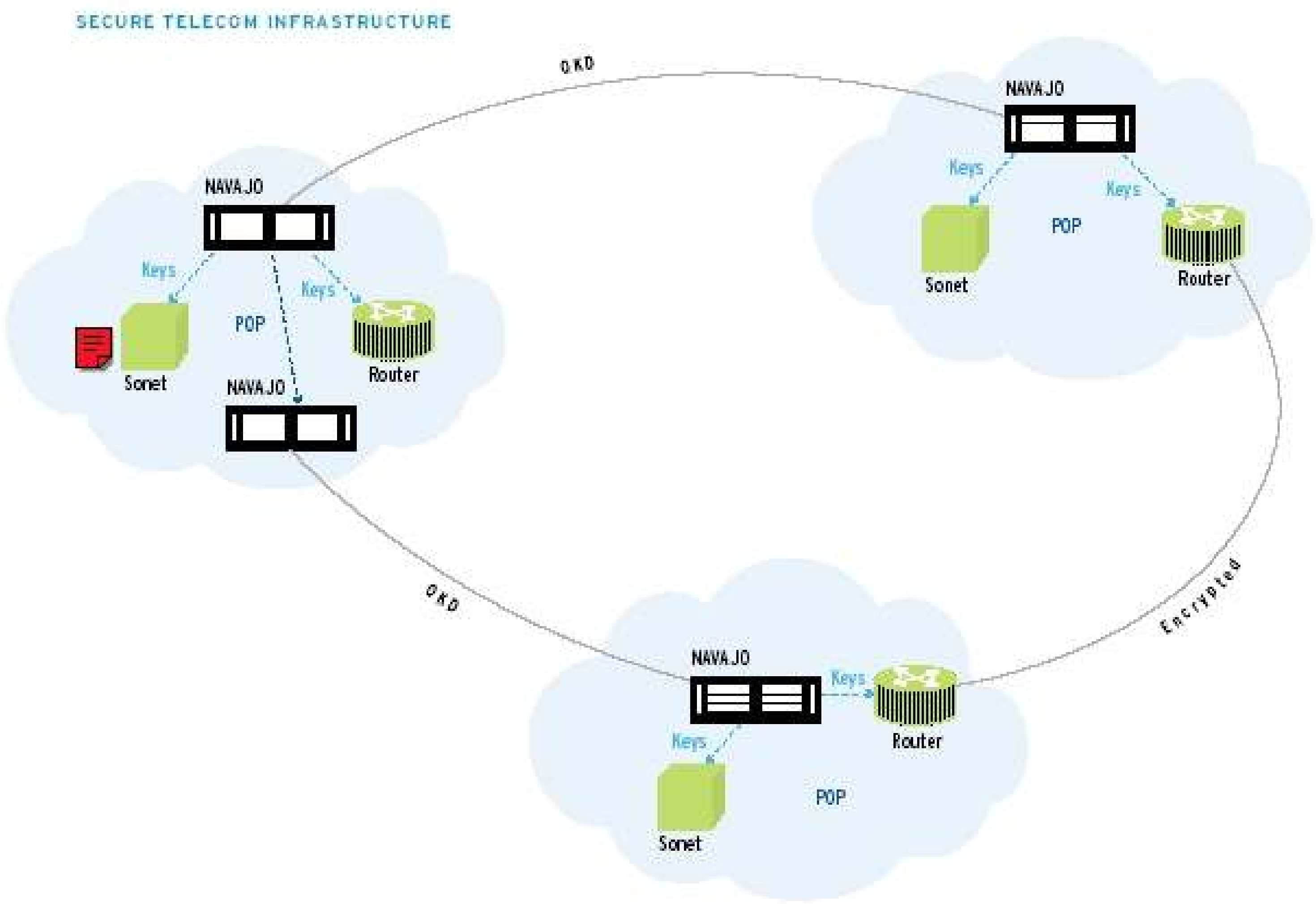
Navajo Deployment: Homeland Defense



Case Study

- Industry: Large power grid provider
- Network topology: large public and private network in large regional area
- Security concern: Terrorist or malicious hacking into the command and control channel interfaces
- MagiQ answer: Lock down critical command nodes with Navajo while locking down overall network with MagiQ VPN and classical products

Secure Network Configuration



MagiQ Technologies

The Quantum Information Processing Company