Approved for public release

Practical Quantum Cryptography

G. Gilbert

28 March 2001

Seminar Presentation at Purdue University
Center for Education and Research in Information Assurance and Security

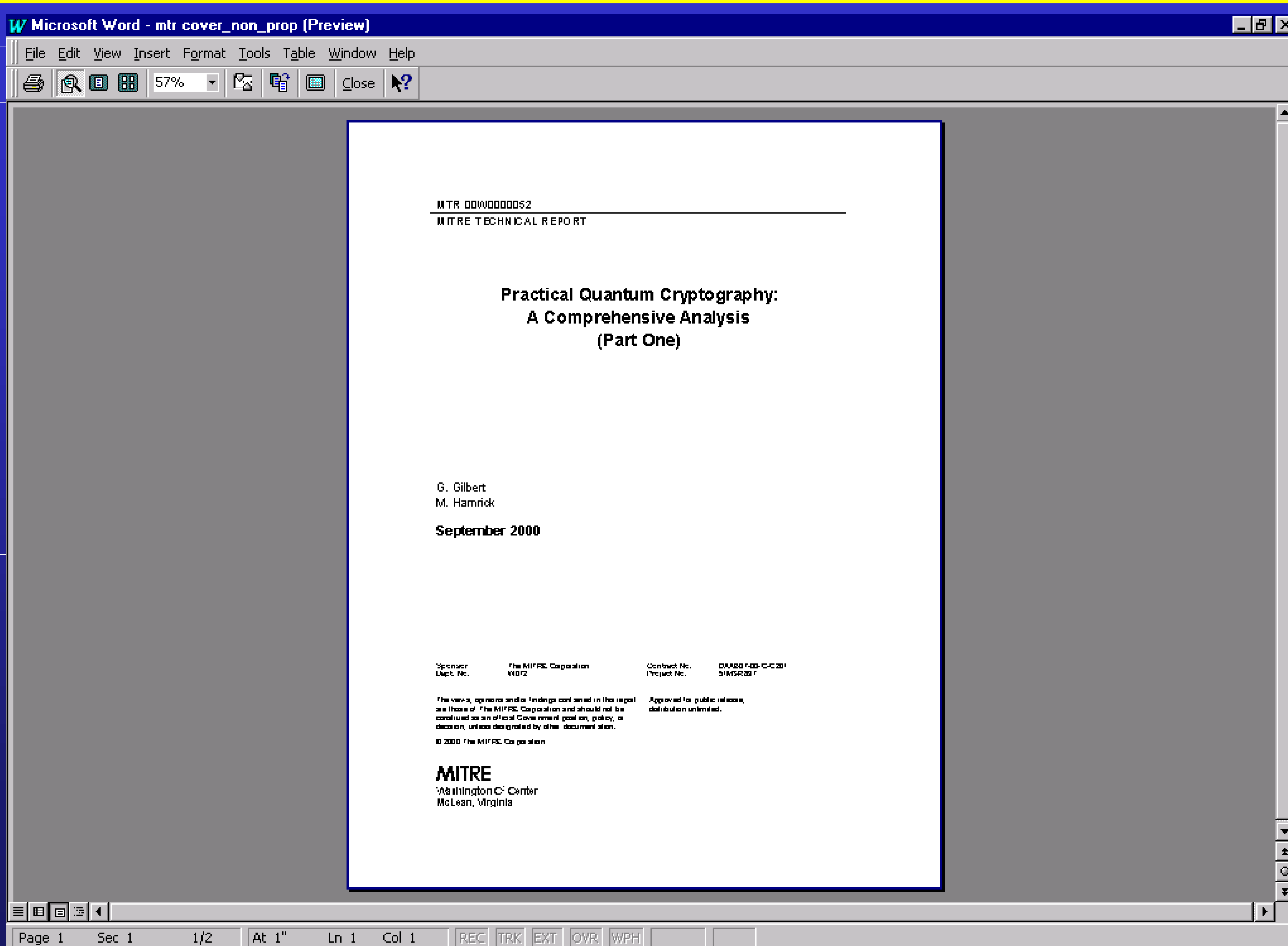
UNCLASSIFIED

MITRE

Principal Seminar Reference -

Approved for public release

http://xxx.lanl.gov/abs/quant-ph/0009027



MTR 00W0000052
MITRE TECHNICAL REPORT

Practical Quantum Cryptography:
A Comprehensive Analysis
(Part One)

G. Gilbert
M. Hamrick

September 2000

Sponsor	The MITRE Corporation	Contract No.	[illegible]
Dept. No.	W072	Project No.	[illegible]

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

Approved for public release; distribution unlimited.

MITRE
Washington C³ Center
McLean, Virginia

UNCLASSIFIED

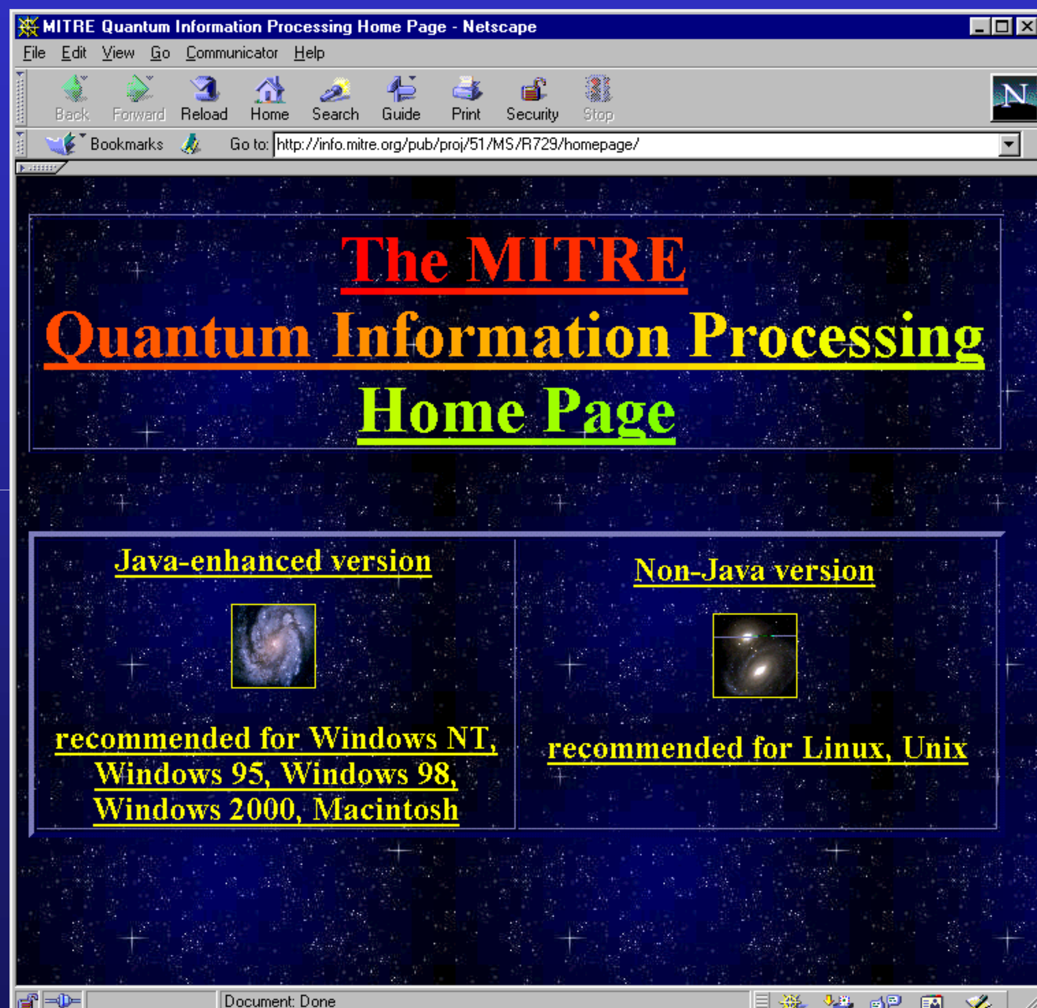
MITRE

Information on Quantum Information...

Approved for public release

MITRE Quantum Information Processing Website:

appearing soon at: **http://www.mitre.org/**



MITRE

The situation in a nutshell…(1)

1) <u>The Future</u> - Optical Communications Spanning the Globe
   - a) Ultra-Transparent Optical Fibers & All Optical Switching
   - b) Optical Links Connecting Spaceborne Assets

2) <u>An Important Element</u> - Quantum Cryptography
   - a) *Unconditional* Secrecy (even against Quantum Computers)
   - b) Los Alamos, MITRE and others: Working Prototypes already
   - c) <u>But</u>: Slow (5 Kbps)

3) MITRE - MSR (MITRE Sponsored Research) Project + IC funding
   - a) Objective: High-Speed (1 Gbps)
   - b) Theoretical Work: Detailed mathematical analyses
   - c) Experimental Work: Laboratory prototype demonstrations

The situation in a nutshell…(2)

- Improvements in algorithms and/or computing machinery

a) Moore's Law & Nanocomputing - "Slippery Slope" (Now & 10+ years)

b) Quantum Computers - "The Precipice" (10+ years ?)

First-Year Accomplishments - Theoretical (1)

- MITRE has obtained the first complete mathematical description of quantum cryptosystem operating characteristics
- MITRE has analyzed a practical system design which should be able to achieve high throughput
- Theoretical analysis demonstrates possibilities for a variety of specific applications of quantum cryptography

First-Year Accomplishments - Theoretical (2)

• We show that various practical high-speed quantum cryptosystems can work (multiplexing can increase these rates) -

30 cm transmit telescope

- •Free-space channel: Aircraft-LEO satellite link
  - •Secret throughput ~60 Mbps (> T3 link) — 0.6 meter receive telescope

- •Free-space channel: Earth (MSL)-LEO satellite link
  - •Secret throughput ~60 Mbps (>T3 link) — 1.6 meter receive telescope

- •Free-space channel: Earth (10000')-GEO satellite link
  - •Secret throughput ~240 Kbps (1/6th T1 link) — 10 meter receive telescope

- •Fiber-optic channel:
  - •Secret throughput ~115 Mbps (10 km link)
  - •Secret throughput ~30 Mbps (40 km link)

MITRE

High-Speed Quantum Cryptography

Approved for public release

- **Quantum key *distribution*:**
  - It is impossible to measure the state of a quantum bit without altering it; No passive eavesdropping possible due to the Heisenberg Indeterminacy Principle ⇒ unconditional secrecy
- **Vernam cipher ("one-time pad") *encryption*:**
  - Plaintext encrypted via XOR against Vernam cipher; As a result ciphertext is literally random ⇒ unconditional secrecy
- **High speed *transmission*:**
  - Generation of large Vernam ciphers ⇒ bulk encryption

•Quantum Key Distribution + Vernam cipher system = QUANTUM CRYPTOGRAPHY: most secure possible system consistent with the laws of physics

• Secure against even Quantum Computers

"Ideal" Quantum Key Distribution Protocol (BB84)

1) Alice sends: | | / – – \ – | – /

2) Bob sets: x + + x x x + x + +

3) Bob receives: / | – \ / \ – / – |

4) Bob tells Alice (publicly) what his settings were

5) Alice tells Bob (publicly) which settings were correct: 2,6,7,9

6) Alice and Bob keep those states correctly measured:

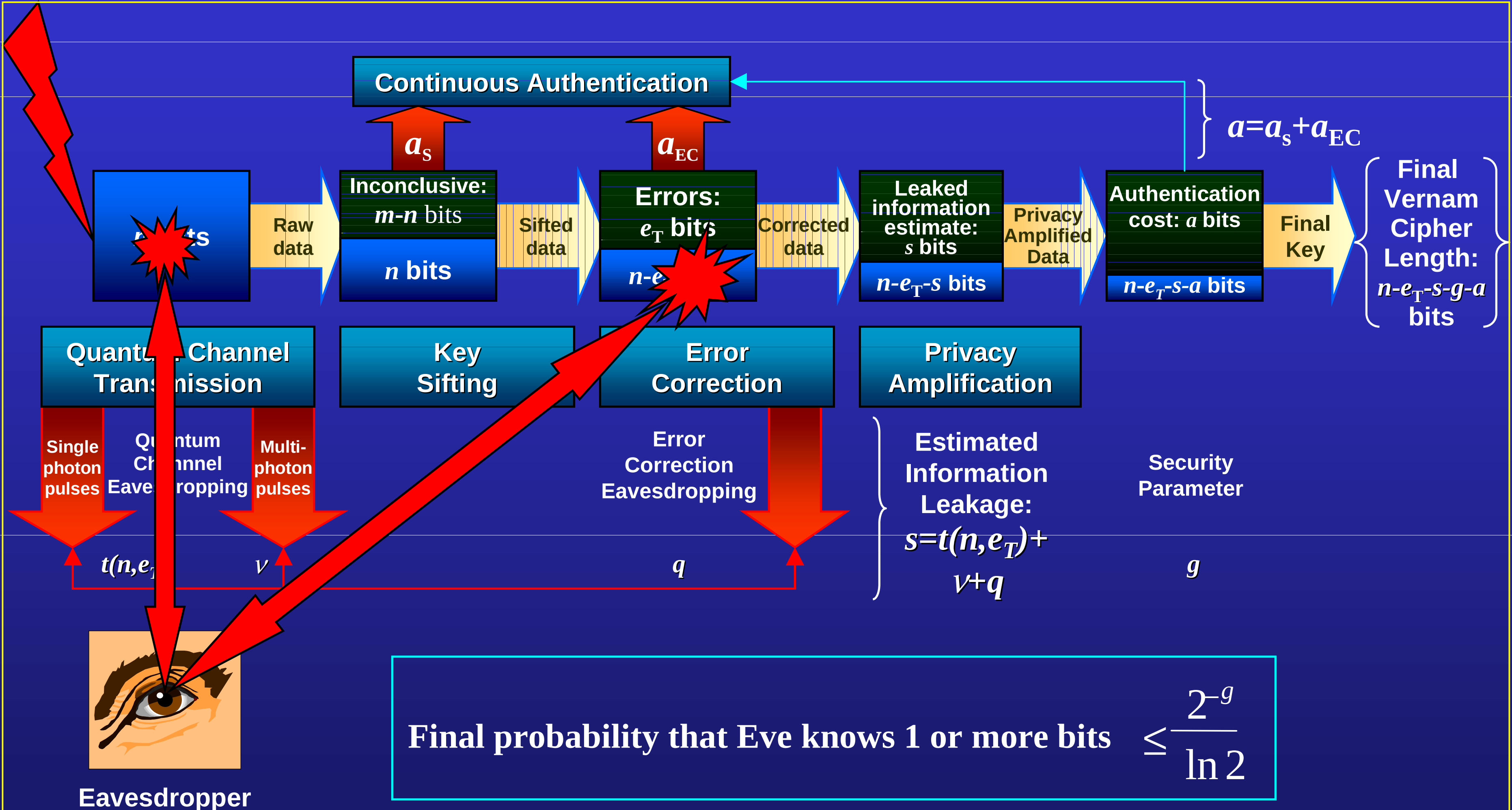
* | * * * \ – * – *

7) Using { | , \ } = 0 and { – , / } = 1 yields:

0 0 1 1 : the shared random key

MITRE

Practical Quantum Key Distribution Analysis



Final probability that Eve knows 1 or more bits $\leq \dfrac{2^{-g}}{\ln 2}$

e.g. if g=30 this probability is 10^{-9}

Adapted from Slutsky, et. Al, "Defense frontier analysis of quantum cryptographic systems," Applied Optics, Vol. 37, No 14, 10 May 1998.

MITRE

Physical Variables for Effective Secrecy Capacity

The effective secrecy capacity function is defined as:

$$S \equiv \frac{n - e_T - s - g - a}{m}$$

The effective secrecy rate function is defined as:

$$R \equiv \tau^{-1} S$$

m number of raw bits

n number of sifted bits

e_T number of sifted bits in error

s information content obtained by eavesdropper

g privacy amplification security parameter

a number of continuous authentication bits

τ bit cell period

Physical Parameters for Effective Secrecy Capacity

To calculate the secrecy capacity and rate we also need:

- α line attenuation
- η photon detector quantum efficiency
- r_c intrinsic error in quantum channel
- r_d dark count
- x Shannon limit exceedence
- μ mean photon number per pulse

Calculation of Number of Sifted Bits: *n*

Fundamental Approach:

(1) enumerate all dynamical events
(2) deduce associated absolute and conditional probabilities
(3) carry out the sums

$$n = m\Big\{\Big[\sum_{l,l',l''} P(l \text{ photons leave Alice})$$
$$\times P(l' \text{ photons reach Bob} \mid l \text{ photons leave Alice})$$
$$\times P(l'' \text{ photons detected} \mid l' \text{ photons reach Bob})$$
$$\times P(\text{no dark count event}) \times P(\text{basis compatibility})\Big]$$
$$+ P(\text{dark count event}) \times P(\text{basis compatibility})\Big\}$$

Calculation of Number of Sifted Bits: probabilities

The relevant absolute and conditional probabilities are:

$$P(l \text{ photons leave Alice}) = e^{-\mu} \frac{\mu^l}{l!}$$

$$P(l' \text{ photons reach Bob} \mid l \text{ photons leave Alice}) = \binom{l}{l'} \alpha^{l'} (1-\alpha)^{l-l'}$$

$$P(l'' \text{ photons detected} \mid l' \text{ photons reach Bob}) = \binom{l'}{l''} \eta^{l''} (1-\eta)^{l'-l''} \left(1-\delta_{0,l''}\right)$$

$$P(\text{no dark count event}) = 1 - r_d$$

$$P(\text{basis compatibility}) = \frac{1}{2}$$

Calculation of Effective Secrecy Capacity

mean photon number per pulse

number of sifted bits

$$n = \left[(1-r_d)\psi_{\ge 1}(\eta\mu\alpha) + r_d\right]\cdot\frac{m}{2} \approx \left[\psi_{\ge 1}(\eta\mu\alpha) + r_d\right]\cdot\frac{m}{2}$$

loss at detector

dark count

line attenuation

channel error

number of error bits

$$e_T = \left[\left(1-\frac{r_d}{2}\right)r_c\psi_{\ge 1}(\eta\mu\alpha) + \frac{r_d}{2}\right]\cdot\frac{m}{2} \approx \left[r_c\psi_{\ge 1}(\eta\mu\alpha) + \frac{r_d}{2}\right]\cdot\frac{m}{2}$$

mean photon number per pulse

Physical Variables for Effective Secrecy Capacity

The information obtained by eavesdropper is:

$$s = q + t + \nu$$

q information obtained via error-correction eavesdropping

t information obtained via single-photon pulses

ν information obtained via multi-photon pulses

We now determine in turn: *q*, *t* and ν:

3 Types of Individual Attacks on Multi-Photon Pulses

Direct Attack:

(1) Eve intercepts multi-photon pulse (3 or more photons)
(2) Eve measures and determines polarization of pulse
(3) Eve prepares and transmits *surrogate* pulse

Indirect Attack:

(1) Eve intercepts multi-photon pulse (2 or more photons)
(2) Eve retains *u* photons in quantum memory
(3) Eve allows *remnant* pulse to propagate to Bob
(4) Eve listens to public discussion and measures retained pulse

Combined Attack:

(1) Eve intercepts multi-photon pulse (5 or more photons)
(2) Eve performs direct attack against some of the pulse
(3) Eve performs indirect attack against some of the pulse

Calculation of Multi-photon Privacy Amplification:

Sample Calculation - Indirect Attack:

(1) Eve intercepts multi-photon pulse (2 or more photons)

(2) Eve retains *u* photons in quantum memory

(3) Eve allows *remnant* pulse to propagate to Bob

(4) Eve listens to public discussion and measures retained pulse

$$\nu_i^{(u)} = \frac{m}{2} \sum_{l,l',l'',l'''} P(l \ \text{photons leave Alice})$$

$$\times P(l' \ \text{photons reach Eve} \mid l \ \text{photons leave Alice})$$

$$\times P(l'' \ \text{photons reach Bob} \mid l' - u \ \text{photons pass Eve})$$

$$\times P(l''' \ \text{photons detected} \mid l'' \ \text{photons reach Bob})$$

Best Value for Privacy Amplification Function

The complete closed form expressions for the privacy amplification functions that guarantee secrecy against individual attacks are:

$$\nu^{max} = \frac{m}{2}\left[\psi_2(\mu)\eta + 1 - e^{-\mu}\left(\sqrt{2}\sinh\frac{\mu}{\sqrt{2}} + 2\cosh\frac{\mu}{\sqrt{2}} - 1\right)\right]$$

$$\eta > 1 - \frac{1}{\sqrt{2}}$$

$$\nu^{max} = \frac{m}{2}\left[\psi_2(\mu) + (1-\eta)^{-1}\left\{e^{-\eta\mu} - e^{-\mu}\left[1 + \mu(1-\eta)\right]\right\}\right]$$

$$\eta < 1 - \frac{1}{\sqrt[3]{2}}$$

$$\tilde{\nu} = \frac{2\nu}{m}$$

Calculation of Effective Secrecy Capacity

The complete closed form expressions for the effective secrecy capacity and rate functions are:

$$S = \frac{1}{2}\left[\psi_{\geq 1}(1 - fr_c) + \left(1 - \frac{f}{2}\right)r_d - \tilde{\nu}\right] - \frac{g+a}{m}$$

effective secrecy capacity

$$R = \tau^{-1}\left\{\frac{1}{2}\left[\psi_{\geq 1}(1 - fr_c) + \left(1 - \frac{f}{2}\right)r_d - \tilde{\nu}\right] - \frac{g+a}{m}\right\}$$

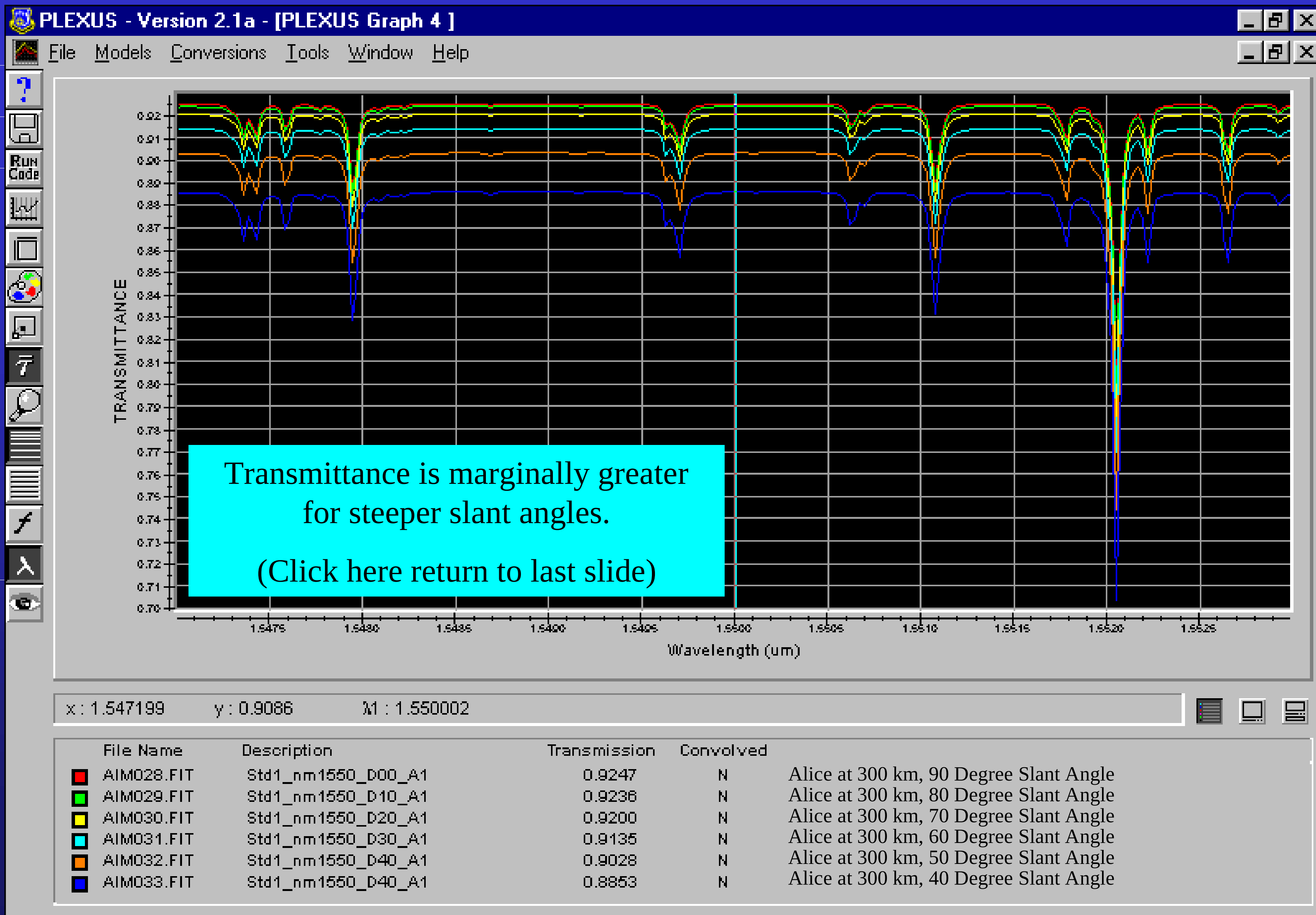
effective secrecy rate

Sources of Attenuation: Loss Budget

- **Atmospheric Transmission Losses: FASCODE**
  - Atmospheric absorption and scattering
- **Turbulence-Induced Losses: NUMERICAL MODELS**
  - Scintillation
  - Beam wander
  - Beam spread
  - Coherence loss
  - Pulse distortion and broadening (dispersion)
- **Geometrical Diffraction Loss: HAND CALCULATION**
- **Optics-Package Losses: COMPARATIVE ANALYSIS**

Atmospheric Transmission Loss due to Absorption and Scattering - Summary

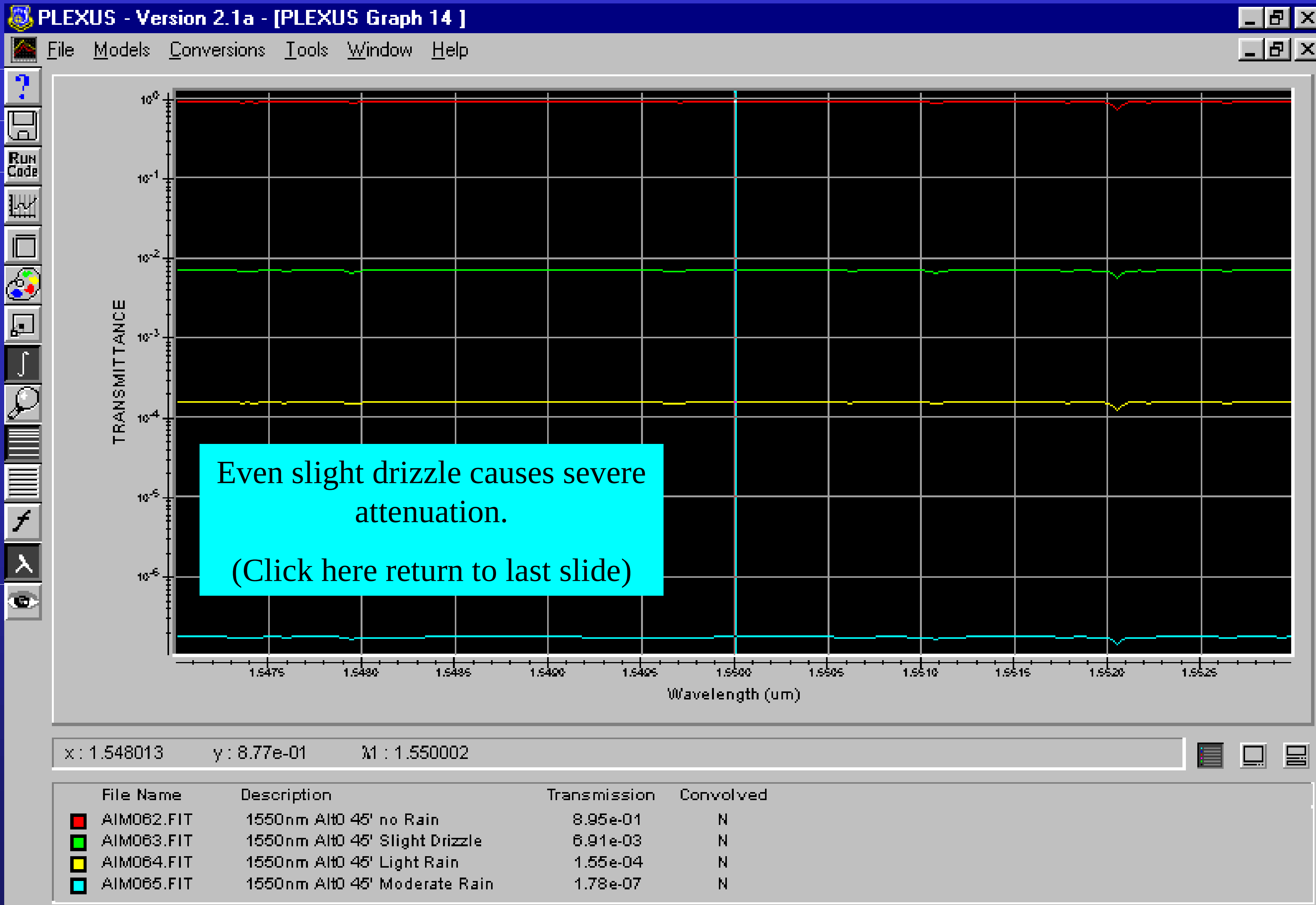
- Analysis using AFRL's PLEXUS system, which provides an interface to FASCODE
- Typical attenuation calculations for 1550 nm laser, 300 km to ground clear weather conditions on the order of 1 db
- Attenuation virtually disappears for 10 to 300 km communication
- Slight asymmetry in upwards and downwards transmittance
- Clouds and even light drizzle will severely attenuate beam



Transmittance as a Function of Slant Angle

Alice at 300km, Bob on Ground, 1550nm Laser

MITRE



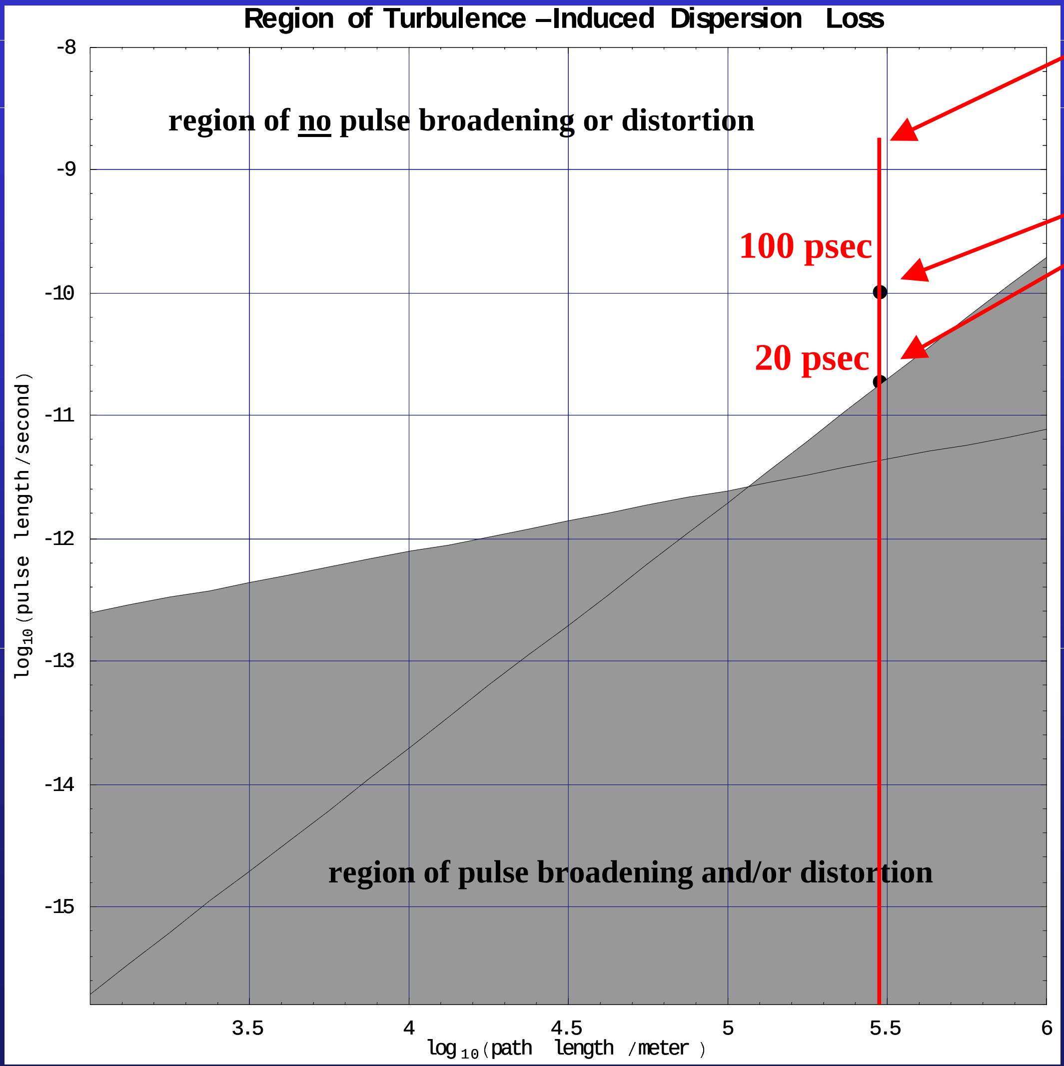
Transmittance in the Presence of Precipitation

Alice at 300km, Bob on Ground, 1550nm Laser

MITRE

Approved for public release

Turbulence-Induced Dispersion Loss Diagram



this line corresponds to 300 km path length

limits of pulse width for 10 GHz qubit source

Unshaded region is the solution to simultaneous inequalities that determine conditions for the spectrum of a short pulse in a turbulent medium to be equal to that of the incident pulse

graph calculated for qubits with wavelength λ = 1550 nm

UNCLASSIFIED

MITRE

Calculations for Diffraction and Turbulence Losses

- **Calculation of geometrical vacuum diffraction beam spread:**

$$\rho_d = \left[\frac{4L^2}{(kD_A)^2} + \left(\frac{D_A}{2} \right)^2 \right]^{1/2}$$

- **Calculation of transverse coherence length for turbulence:**

$$\rho_0 = \left[1.46k^2 \sec(\varphi) \int_0^L d\eta C_n^2(\eta) \left(1 - \frac{\eta}{L} \right)^{5/3} \right]^{-3/5}$$

- **Calculation of short-term beam broadening due to turbulence:**

$$\left\langle \rho_s^2 \right\rangle = \rho_d^2 + \frac{4L^2}{(k\rho_0)^2} \left[1 - 0.62 \left(\frac{\rho_0}{D_A} \right)^{1/3} \right]^{6/5}$$

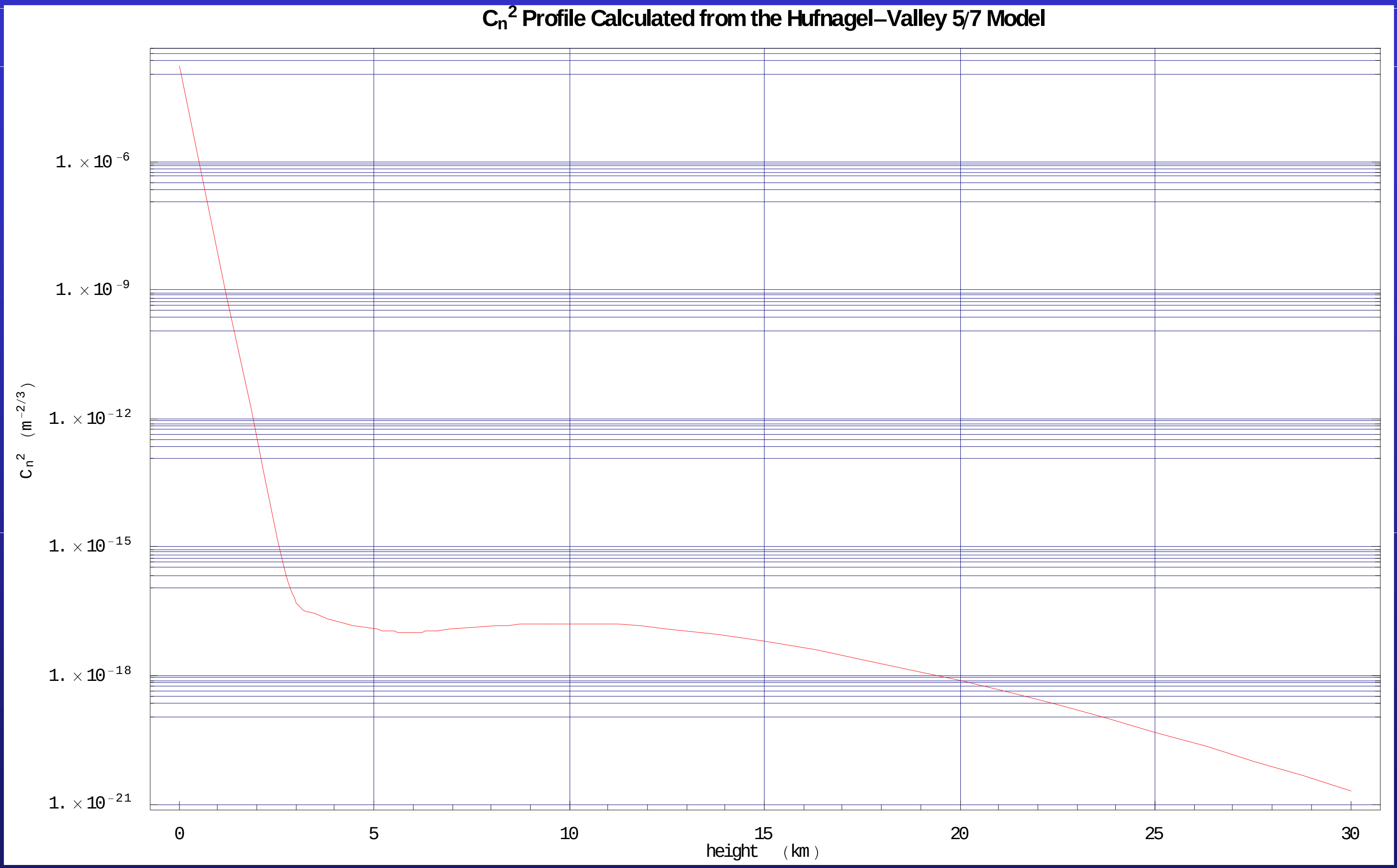
- **Calculation of scintillation due to turbulence:**

$$\sigma_I^2 = \frac{\left\langle \left(I - \langle I \rangle \right)^2 \right\rangle}{\langle I \rangle^2} \approx 4\sigma_\chi^2 \quad \Rightarrow \quad \sigma_\chi^2 = 0.56k^{7/6} \int_0^L dz C_n^2(z) z^{5/6}$$

UNCLASSIFIED

MITRE

Model for Refractive Index Structure Function



This empirically fitted model for C_n^2 characterizes the refractive index in the turbulent boundary layer

Beam Wander Correction

- Active closed-loop feedback at Alice and Bob reject beam wander (>30 dB rejection)
- Tracking beam from each terminal split to quad cell detectors for beam tilt correction
- Fast steering mirrors scans incoming tracking beam to correct for lower frequency wander (<100 Hz)
  - Source: MIT/LL GeoLITE program

Beam wander due to turbulence:

$$\left\langle \rho_c^2 \right\rangle = \frac{2.97 L^2}{k^2 \rho_0^{5/3} D_A^{1/3}}$$

Receiver Optics Package Efficiency Estimate

- Telescope efficiency: 90%
- Optical fiber component transmission efficiencies
  - Free-space to fiber collimator: 80%
  - Polarization beamsplitter: 80%
  - Wave division multiplexer: 90%
  - Optical filters: 95%
- Free space optical components efficiencies: ~95% each
- <u>Optical fiber implementation of ULTRA Bob: –3.8 dB</u>
- <u>Free space ULTRA Bob: –2.3 dB</u>
- Reported optics losses for demonstrated lasercom terminals range from –1.9 to –8 dB

References for Receiver Optics Losses

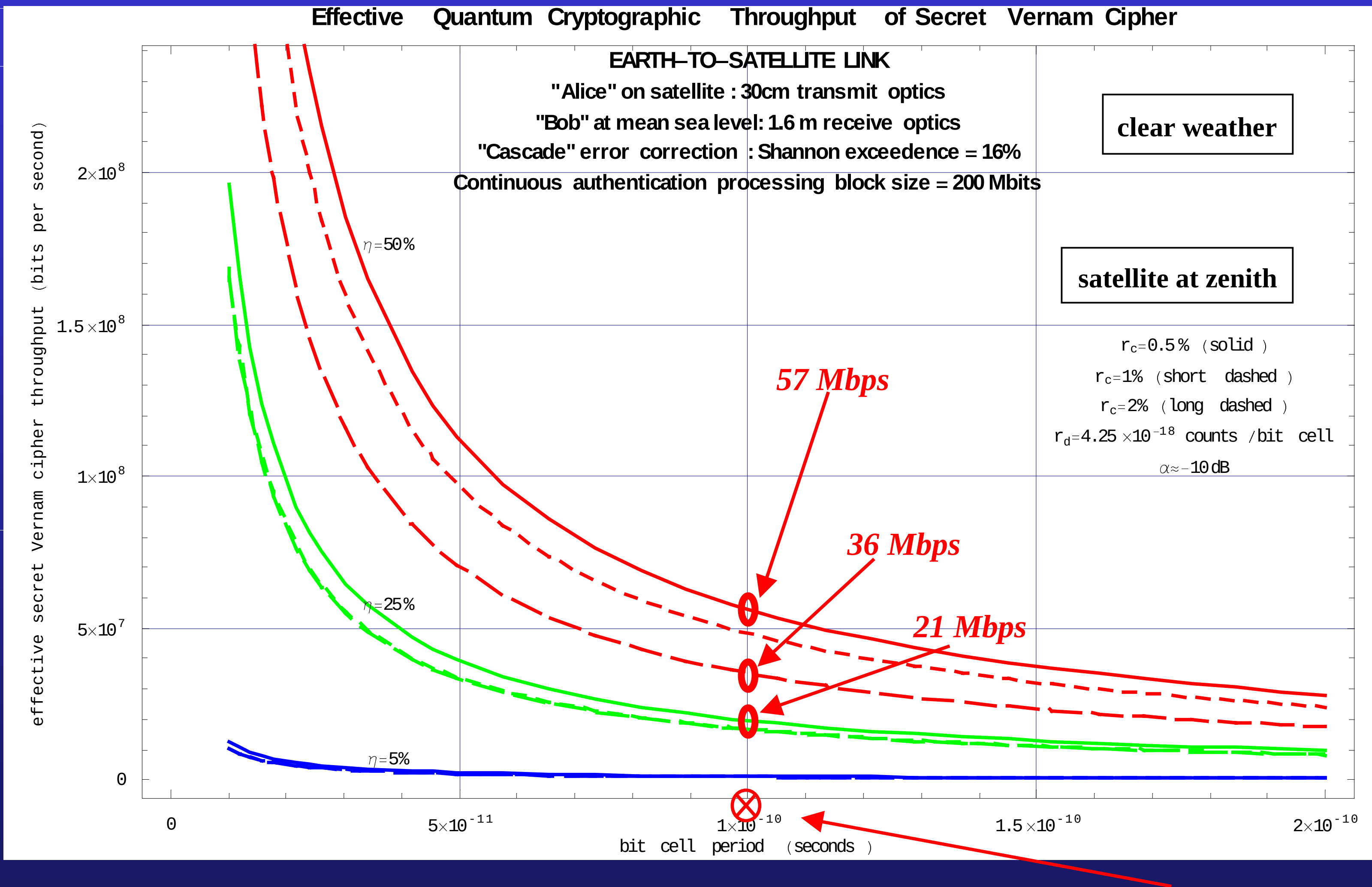
System	Atmospheric Attenuation (dB)	Optics Package Loss (dB)	Mission	Wavelength (nm)	Reference	Notes
JPL-OCD		-1.9	lab demo	840	SPIE vol. 3266 pp. 33-41	measured
AF Airborne ACT	-4.8	-3	air-to-air	810	SPIE vol. 3266 pp. 178-197	design; 500 km airborne demo at 40,000 ft alt.
JPL-OCD	-5		terrestrial point-to-point	780	SPIE vol. 3615 pp. 43-53	measured
JPL-OCD	-6		terrestrial point-to-point	840	SPIE vol. 3615 pp. 43-53	measured
JPL-DSO	-3.65	-3.36	deep space to ground	800	SPIE vol. 3615 pp. 154-169	design
JPL-OCDHRLF	-2		earth orbit to ground	1550	SPIE vol. 3615 pp. 185-191	design
JPL-X2000		-4	deep space to ground	550-1000	SPIE vol. 3615 pp. 206-211	design
JPL-GOLD	-3.14	-8.24	ground to GEO	514.5	SPIE vol. 2990 pp. 70-81	measured
JPL-GOLD	-2.19	-1.94	GEO to ground	830	SPIE vol. 2990 pp. 70-81	measured
CRL	-3	-6.5	GEO to ground	1550	SPIE vol. 2990 pp. 142-151	design
CRL ETS-VI	-3	-8.2	ground to GEO	514.5	SPIE vol. 2990 pp. 264-275	measured
CRL ETS-VI	-2	-4.4	GEO to ground	830	SPIE vol. 2990 pp. 264-275	measured
CRL LCE	-2	-7.2	GEO to ground	830	SPIE vol. 2990 pp. 264-275	estimated

Classical Processing & Public Discussion Phase

- Steps in the classical process
  - Sifting
  - Error correction
  - Privacy amplification
- Several associated costs
  - Authentication
  - Communications
  - Computation
    - Time: Processing requirements
    - Space: Memory requirements
  - Supply of random numbers
- We have obtained analytical results for authentication, communications, and processing costs

Approved for public release

Effective Secrecy Capacity: Earth-LEO Link

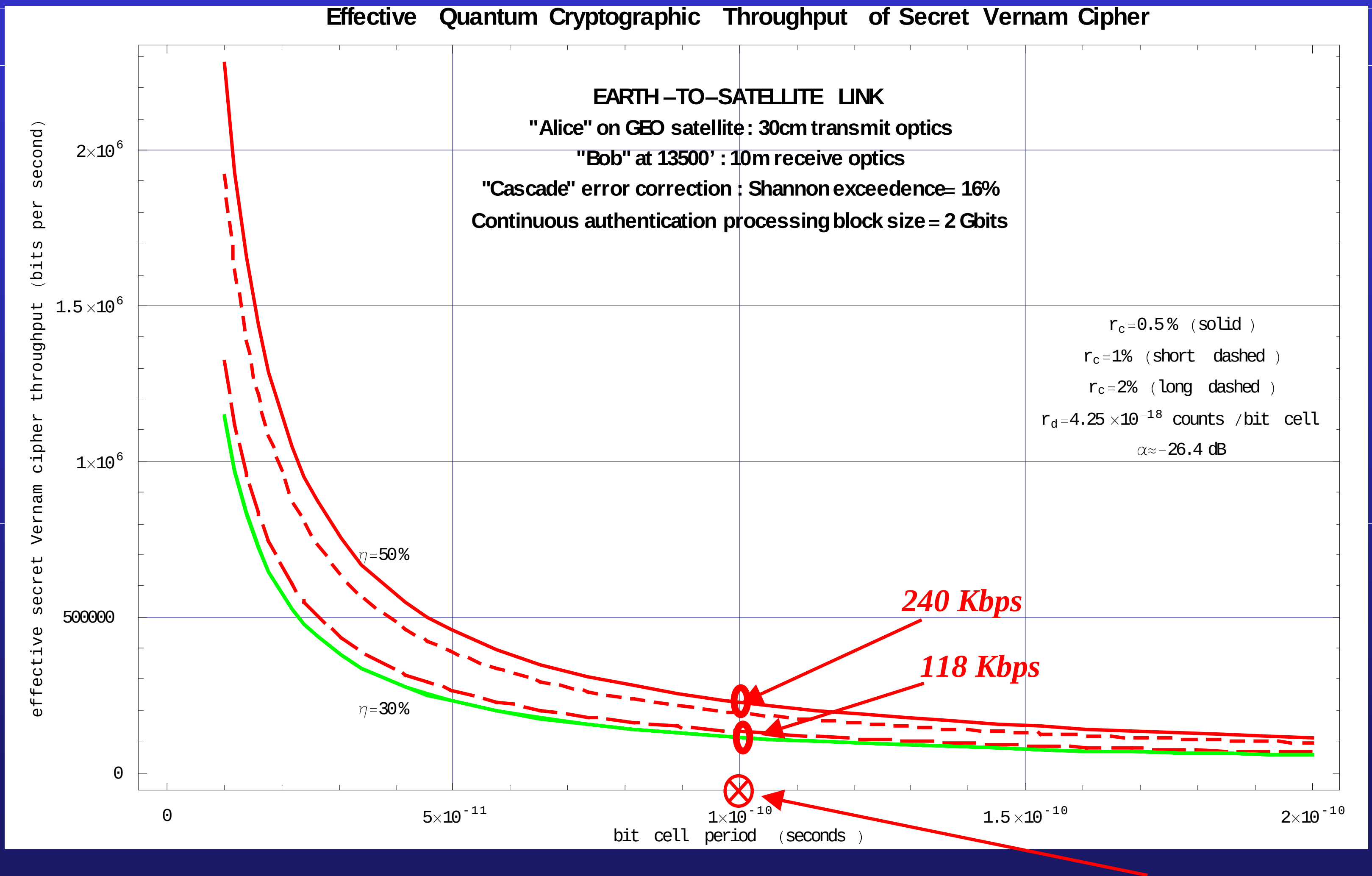


free-space quantum channel

UNCLASSIFIED

MITRE

Effective Secrecy Capacity: Earth-GEO Link

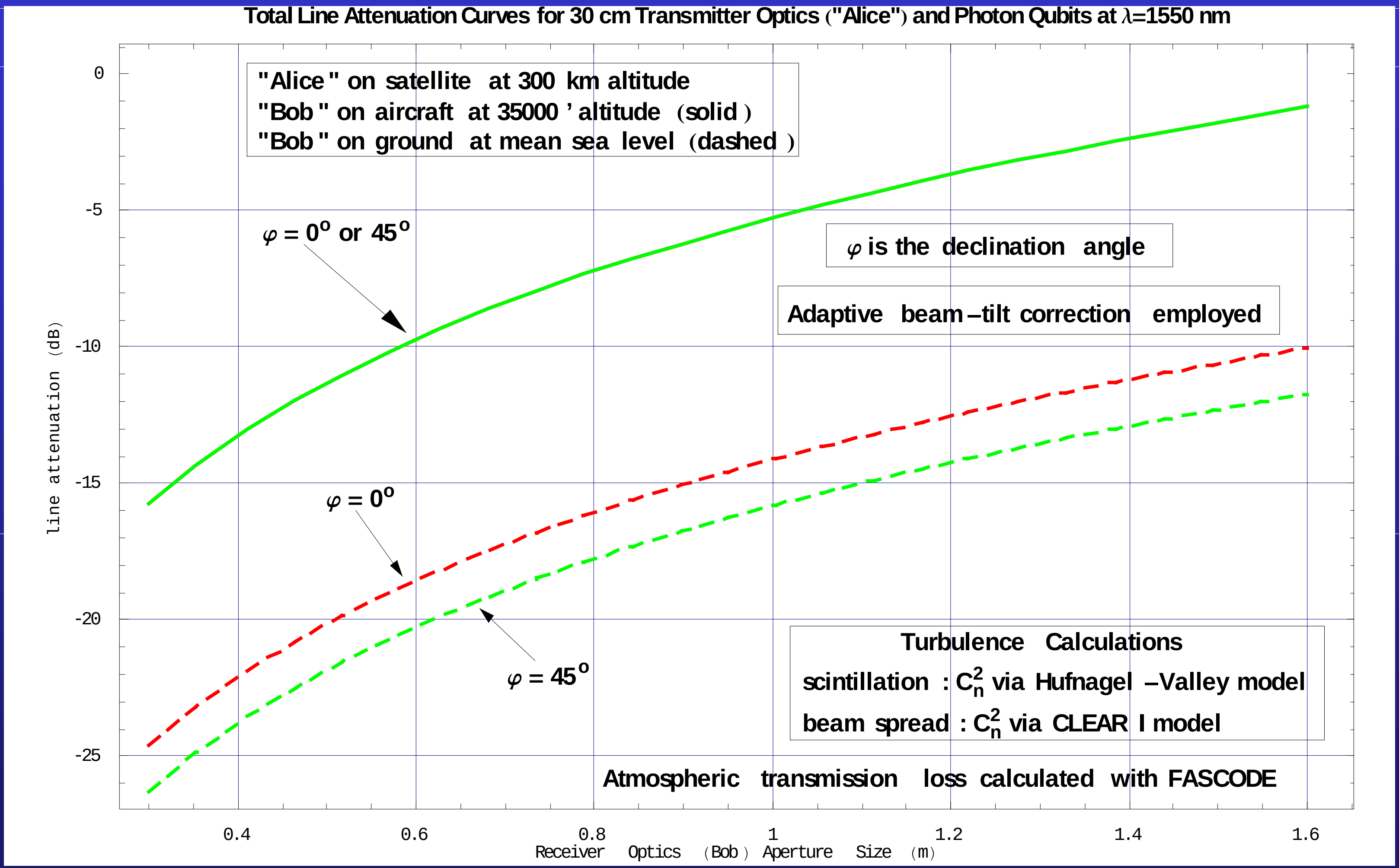


free-space quantum channel

UNCLASSIFIED

MITRE

Quantum Cryptographic Attenuation Curves



UNCLASSIFIED

MITRE

First-Year Accomplishments - Experimental

- “FIRST LIGHT” - MITRE JOINS QUANTUM CRYPTOGRAPHY CLUB

Thursday, 27 July 2000

First successful full demonstration at MITRE of quantum cryptography between “Alice” and “Bob”

MITRE results reproduce benchmark established by Los Alamos National Laboratory

Throughput data rate values for sifted cryptographic Vernam cipher approximately 10 Kilobits/second

Quantum Information Processing: Secure Quantum Communications MSR Team

QUANTUM OPTICS LABORATORY (MITRE BEDFORD)

INNOVATIVE SOLUTIONS FACTORY (MITRE NEW JERSEY)

MITRE is working with US Intelligence Community, Air Force Research Laboratory, Naval Research Laboratory, Caltech Jet Propulsion Laboratory, University of Rochester, others

MITRE

Work in Progress: MITRE & IC funding

- Verification of crucial theoretical predictions:
  - Scaling behavior of computational cost for parallelized links
    - essential to allow for achieving goal of high-speed system throughput, since single link will not support sufficient throughput
  - Combining optical fiber and free space quantum channels (of non-negligible lengths) for real systems applications

Team for Quantum Cryptography

Consortium effort to develop unconditionally secret quantum cryptosystems for National Security level communication, including:

- MITRE
- IC
- IC
- DARPA
- IC
- NRL
- AFRL
- JPL
- University of Rochester

Design of Practical Ultrafast QKD System (1)

Question: How can we increase the throughput rate for a realistic quantum cryptography system?

Answer:

(1) Increase the basic pulse repetition frequency (*i.e.*, reduce the bit cell period) - need fast photon detectors

(2) Increase the number of transmitters (*i.e.*, multiplex Alices) - need: relation between block size and rate

(3) Combine the above techniques

Design of Practical Ultrafast QKD System (2)

Question: What is a practical rate for the internal clock speed of a realistic quantum cryptography system?

Answer: A practical system can be designed with an internal clock speed of 10 GHz, corresponding to a bit cell period, τ, of 100 picoseconds.

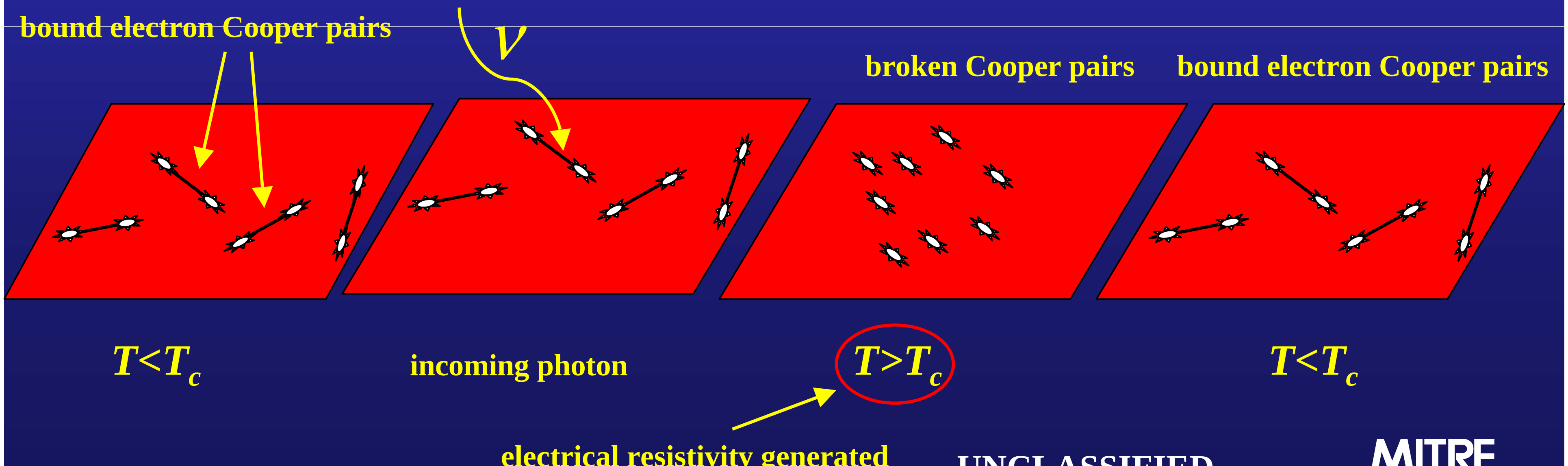
Ultrafast Optoelectronics Requirement

Two essential requirements for ultrafast quantum cryptography:

- Photon detection apparatus as fast as bit cell period
  - Superconducting HEP photon detection
    - University of Rochester group
- Sufficiently fast source of quantum bits
  - Pulsed lasers with high pulse repetition frequency
    - Naval Research Laboratory

Hot Electron Photo-Effect (HEP) Detection

- The HEP effect employs superconducting thin film technology
- Different materials, including Niobium Nitride (NbN) and Yttrium Barium Copper Oxides (YBCO) exhibit the HEP effect
  - NbN has measured HEP cycle time of 30 picoseconds (33 GHz)
    - T_c=9K (slightly higher than liquid helium)
  - YBCO has measured HEP cycle time of 1 picosecond (1 THz)
    - T_c=89K (slightly higher than liquid nitrogen)

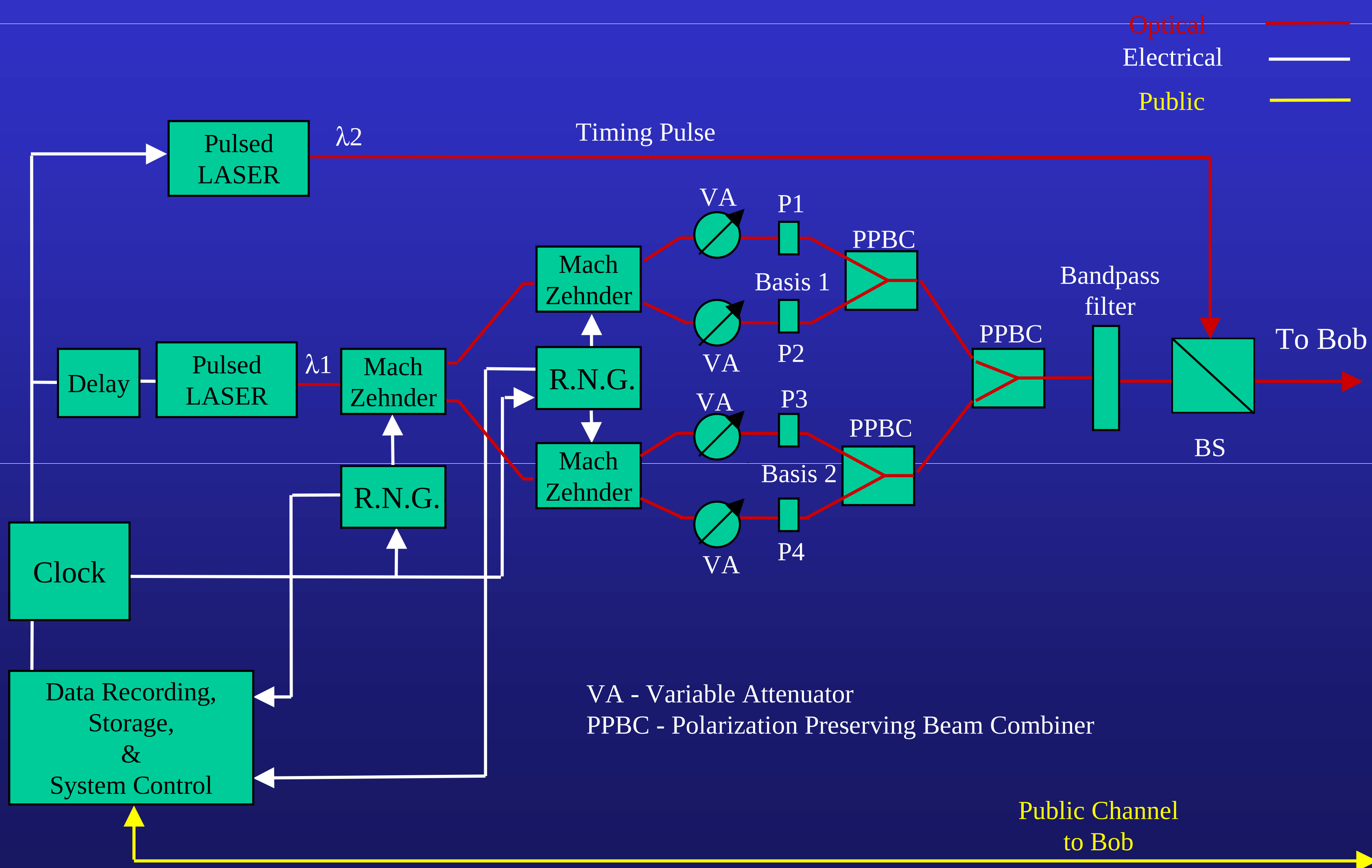


MITRE

Design of Practical High-Speed QKD System

We show the design for a full, high-speed quantum key distribution system

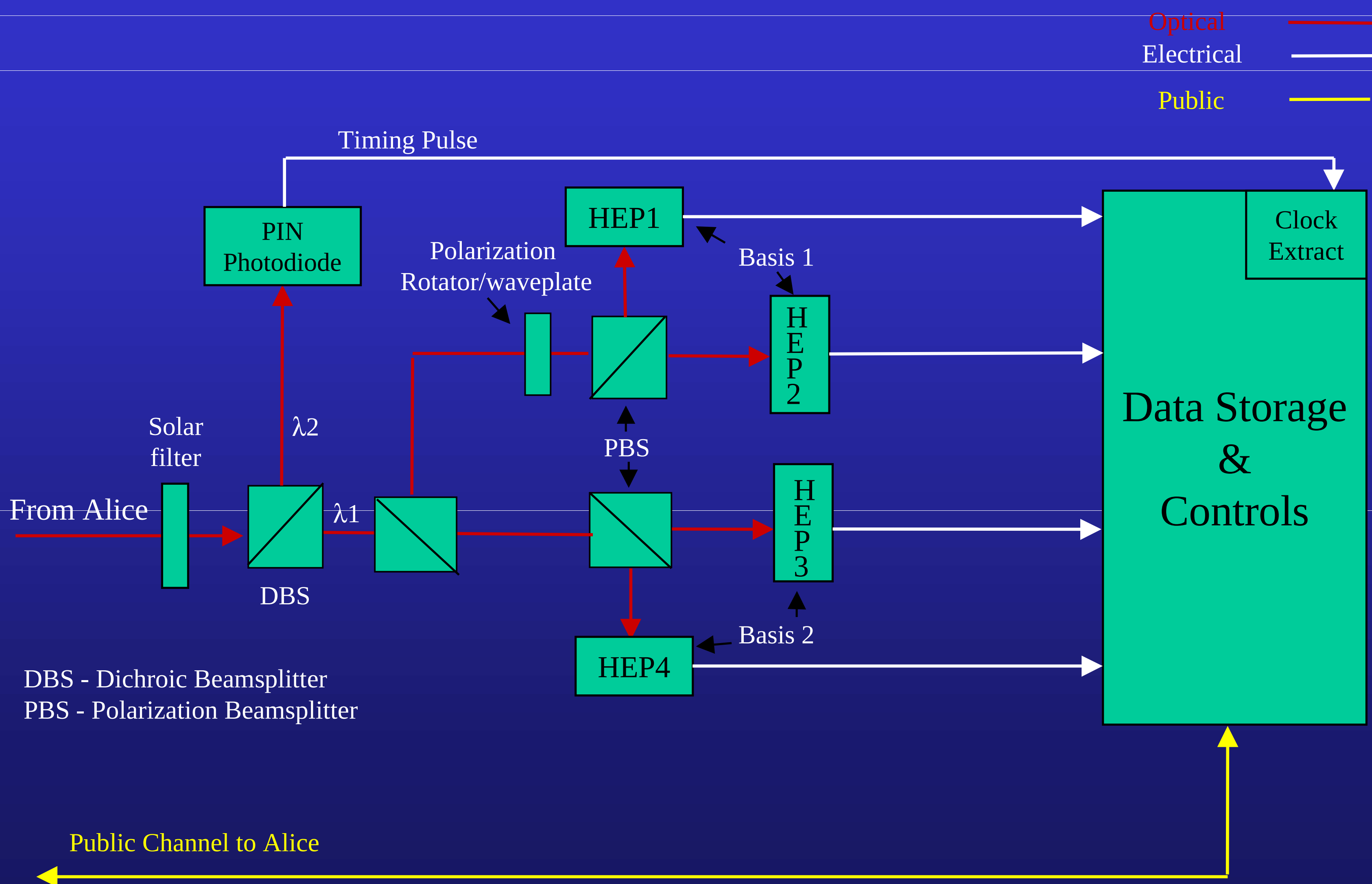
High-Speed Alice



VA - Variable Attenuator
PPBC - Polarization Preserving Beam Combiner

Approved for public release

High-Speed Bob

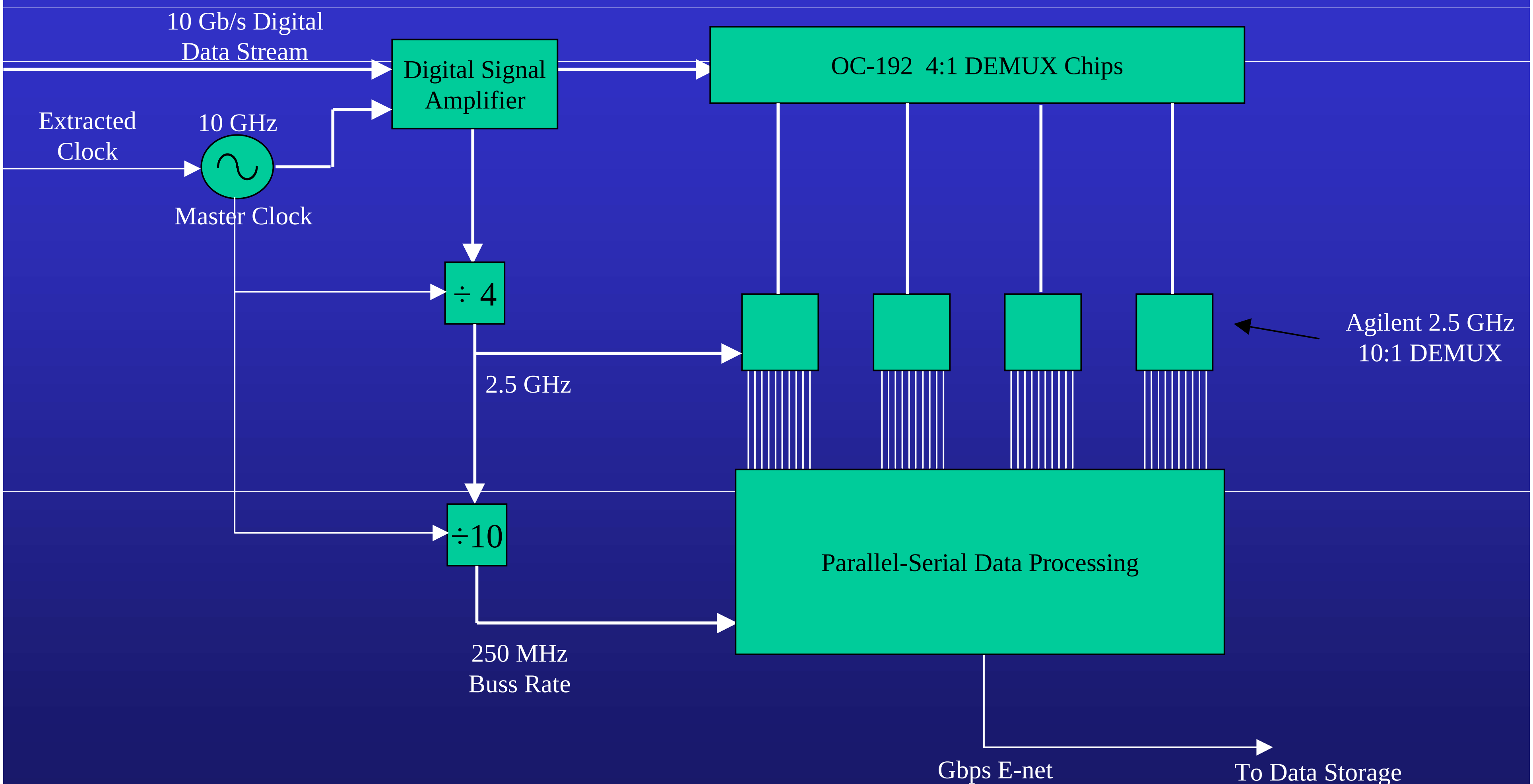


UNCLASSIFIED

MITRE

Approved for public release

High-Speed DEMUX and Data Storage



UNCLASSIFIED