
Quantum Key Distribution in a Multi-Node Ring Configuration

Deborah J. Jackson

George Hockney

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA



Quantum Key Distribution



- Classically observed using conjugate variables
 - Polarization
 - Time
 - Frequency

Link Security



- Definition of suitability:

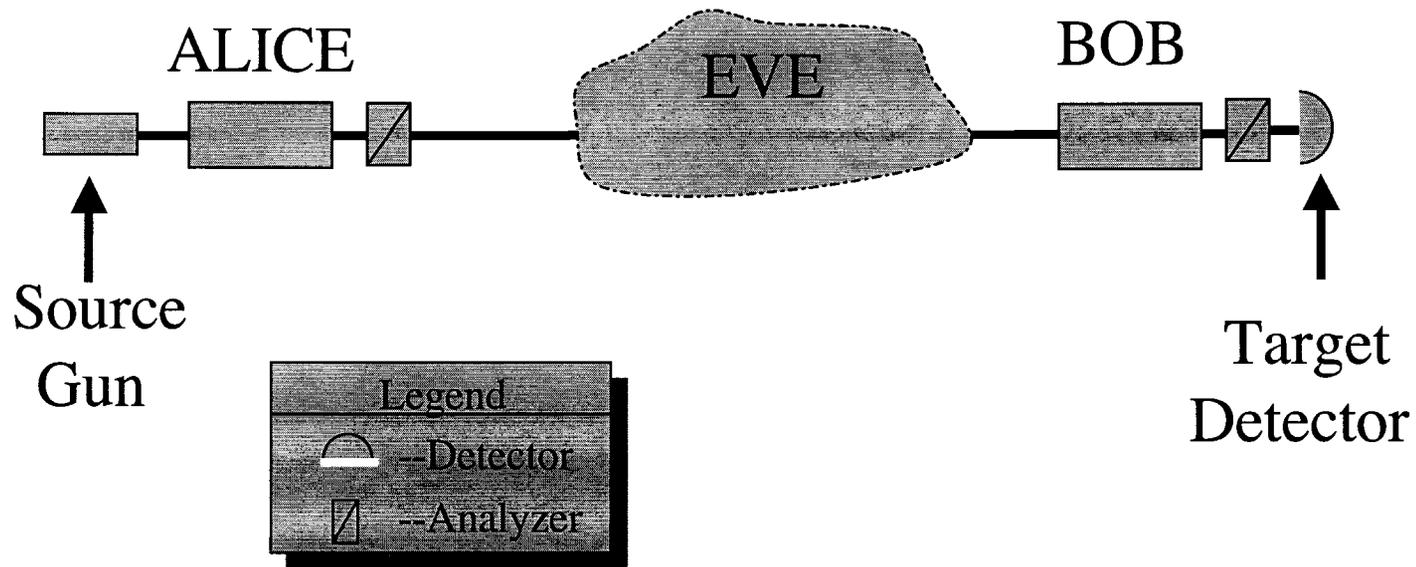
$$F_{AB} = \text{Tr}(\rho_A \rho_b)$$

$$S_{GT} = \frac{F_{GT}}{F_{TT}} = \frac{\text{Tr}(\rho_G \rho_T)}{\text{Tr}(\rho_T \rho_T)}$$

- Suitability measures how efficiently Bob can construct the key in his measurement universe
- How much information Eve can obtain information about the key from her measurement universe.

Simple Case: Generic Two Node Link

JPL



Calculate Bob's Suitability



-
- Assume Alice has perfect single photon gun
 - What is the efficiency with which Bob can construct a key with Alice?
 - Can calculate this directly because we know what Bob is doing.

$$S_{AB} = F_{AB} = \text{Tr}(|1\rangle\langle 1| \cdot 1) = 1$$

Loss mechanisms

$$S_{AB} = F_{AB} = \text{Tr}(L|1\rangle\langle 1| \cdot 1) = \eta \exp(-ax)$$

Calculate Eve's Suitability



-
- Assume Alice has perfect single photon gun
 - How much information could Eve gain about the key being exchanged between Alice and Bob?
 - Cannot calculate directly, but can establish

upper limit

$$S_{AE} = F_{AE} = \text{Tr}(R|1\rangle\langle 1| \cdot 0) = 0$$

Calculate Bob's Suitability



- Assuming coherent states of the radiation field?

$$S_{AB} = F_{AB} = \text{Tr}\left(R\left\{\sum_{n=1}^{\infty} \frac{\alpha^{2n}}{n!} |n\rangle\langle n|\right\} \cdot 1\right) = R\left(1 - e^{-|\alpha|^2}\right)$$

- Use privacy amplification to remove enough bits from the key string to insure that Eve recovers no information.

Calculate Eve's Suitability

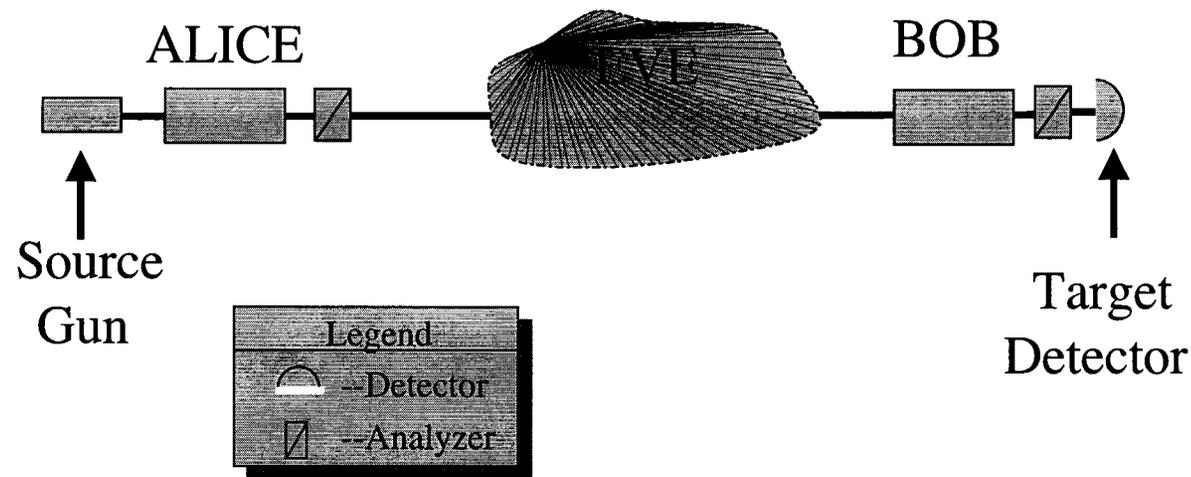


- Assuming coherent states of the radiation field:
- Cannot calculate directly, but can establish upper limit.

$$S_{AE} = F_{AE} = \text{Tr}(R \left\{ \sum_{l=2}^{\infty} \frac{\alpha^{2n}}{n!} |n\rangle\langle n| \right\} \cdot 1) = R \left(1 - e^{-|\alpha|^2} - \alpha^2 e^{-|\alpha|^2} \right)$$

Add Information Coding

- HV, LR; each basis is provided by a different source.



- Also suppose that each source has a slightly different frequency
- Each source has a slightly different timing characteristic.

Calculate Bob's Suitability



- Same answer as before:

$$S_{AB} = F_{AB} = \text{Tr}\left(R\left\{\sum_{n=1}^{\infty} \frac{\alpha^{2n}}{n!} |n\rangle\langle n|\right\} \cdot 1\right) = R\left(1 - e^{-|\alpha|^2}\right)$$

Calculate Eve's Suitability



-
- By accounting for the full Hilbert space when designing her detector, more information can be extracted.
 - When Eve's suitability exceeds that of Bob, the amount of privacy amplification needed to insure security precludes Alice and Bob sharing a key.

Conclusion



-
- It is important to make a mathematical model that includes all physical variables for the system.
 - **MORAL:** The worst thing one can do is think the system is secure when it is not.