



# Equiangular Spherical Codes in Quantum Cryptography

Joe Renes

renes@phys.unm.edu

Information Physics  
University of New Mexico



# *Outline*

---

- Create Key Distribution Protocols based on Equiangular Spherical Codes
  - Compare to Unbiased Bases (BB84 & Six-state)  
⇒ ESCs better than MUBs
1. Spherical Codes and Unbiased Bases
  2. Qubit Protocols: Trine & Tetrahedron
  3. Intercept/Resend Eavesdropping
  4. Results
-

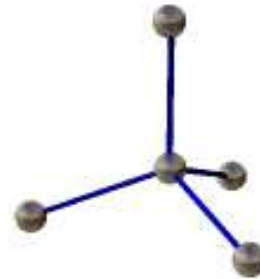


# Qubit ESCs & MUBs

- Visualize on Bloch sphere



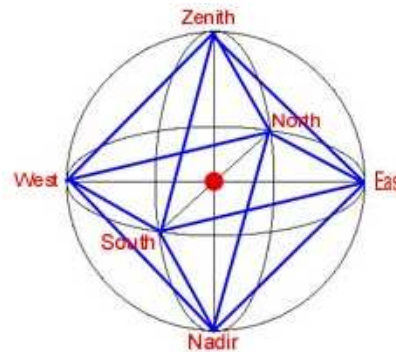
Trine



Tetrahedron



BB84



Six-state



# ***Key Distribution: Setup***

---

Goal: create a shared secret key

Resources

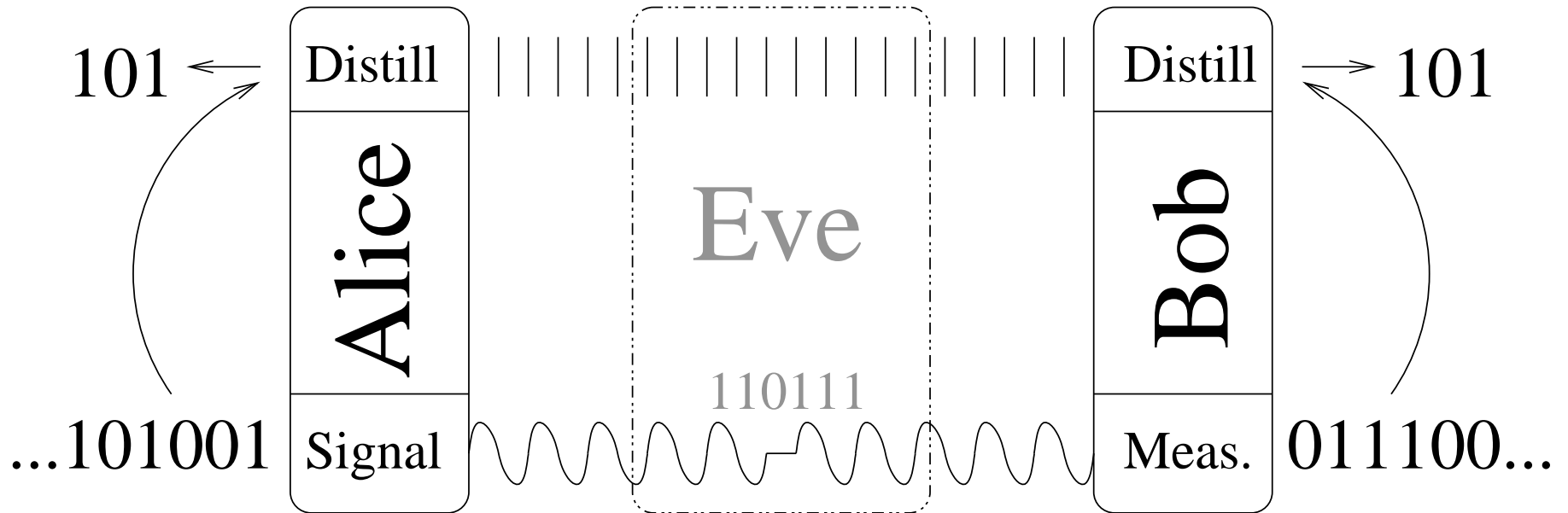
- Previously established short key
- Insecure quantum channel
- Classical broadcast channel

Strategy

- Establish putative key via quantum channel
  - Detect Eve's info via disturbance to signals
  - Reduce Eve's info via classical channel
-



# Key Distribution: Schematics



- Distill key from raw sequence using classical channel
- Optimal Key Rate  $R \geq I(A:B) - \min\{I(A:E), I(B:E)\}$
- A+B determine  $R$  from protocol statistics



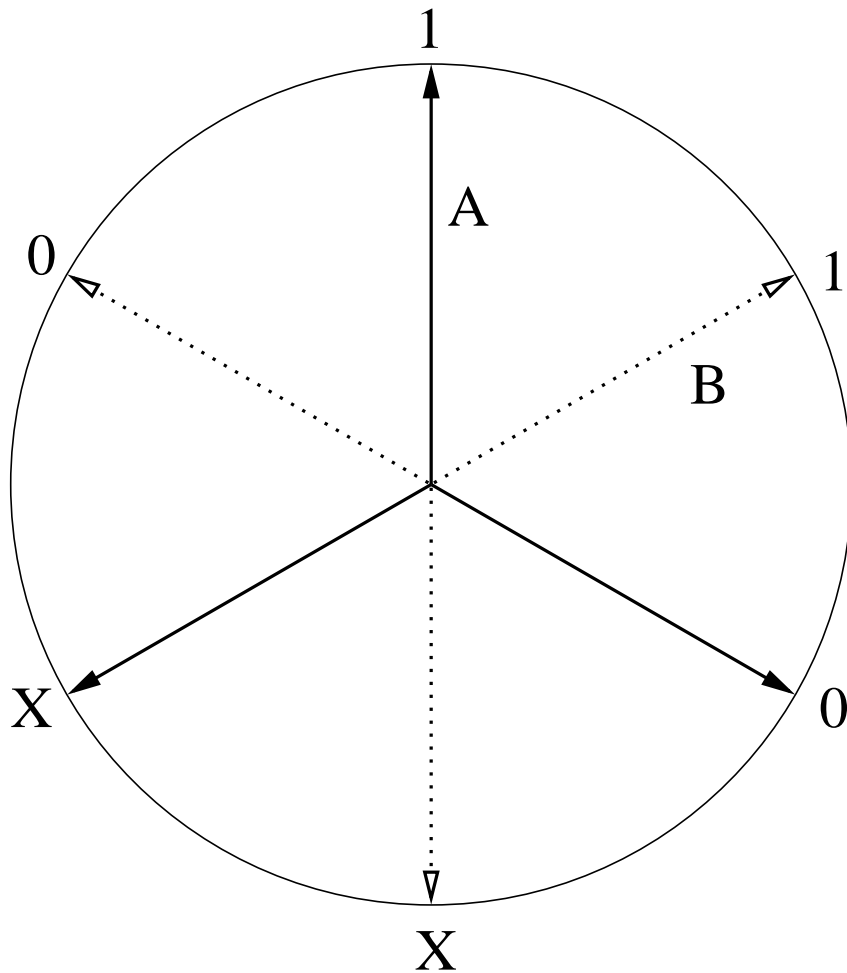
## ***ESC Key Distillation Protocol***

---

- A+B use dual codes
  - A+B each know one value the other *doesn't* have
  - Bob announces values he doesn't have, save one
  - Alice confirms
- ⇒ Each knows the other's signal/outcome
- Relative position is the key bit
- ⇒ Alice and Bob create one secret bit in  $n - 1$  signals



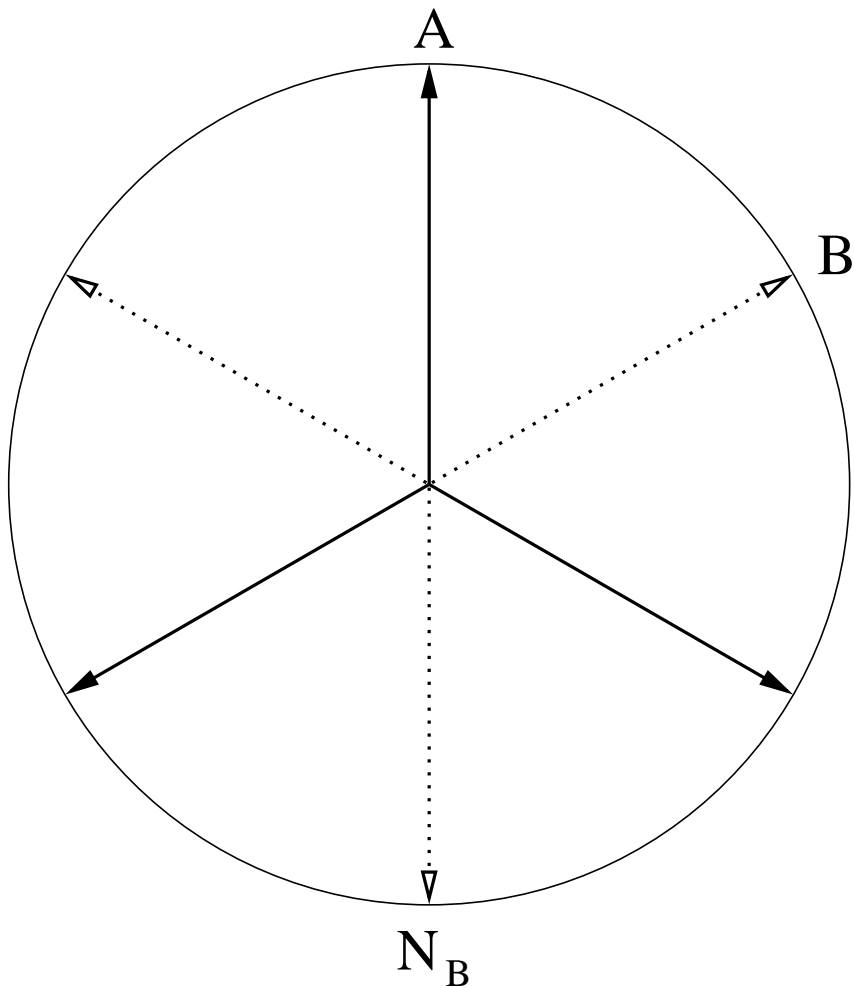
# *Trine Key Distillation: Labelling*



- Label X,0,1
- Start: impossible state
- Alice labels CW
- Bob labels CCW



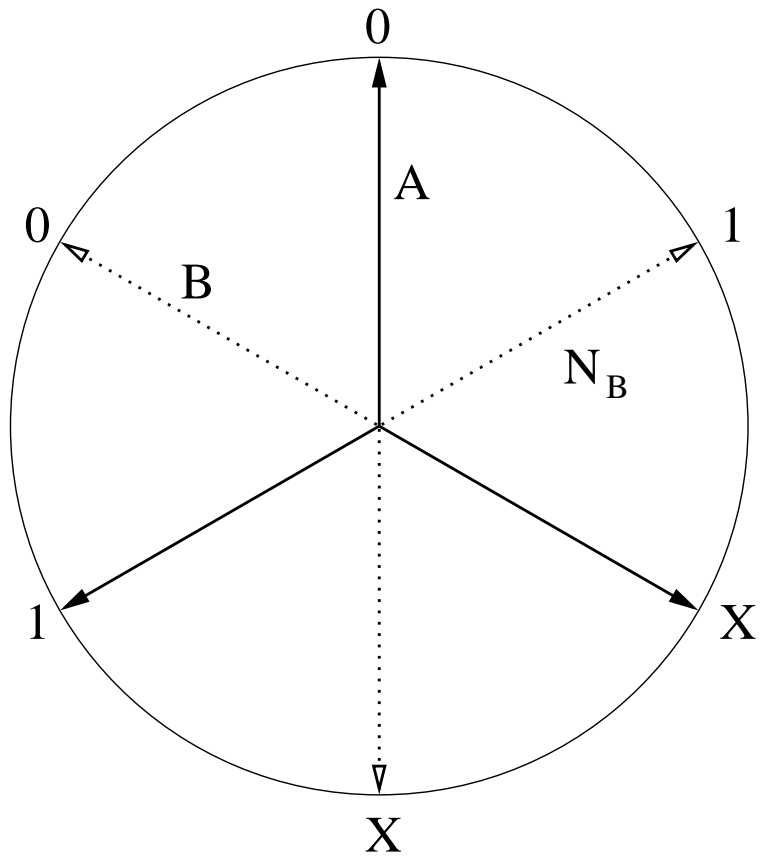
# *Trine Key Distillation: Failure*



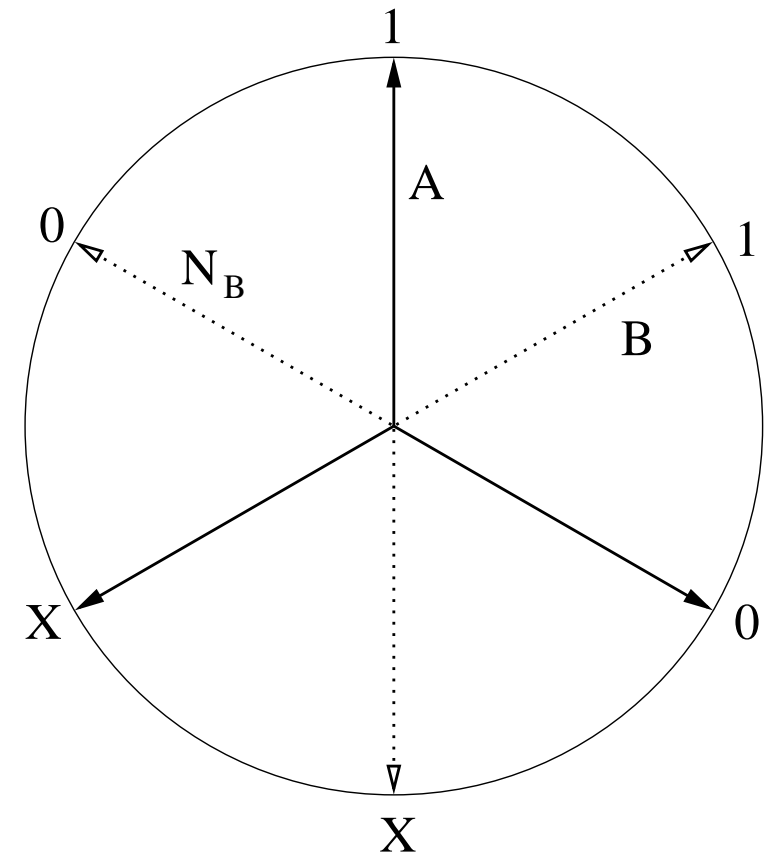
- Doesn't help Alice
- She announces "fail"
- Bob can't say more



# Trine Key Distillation: Success



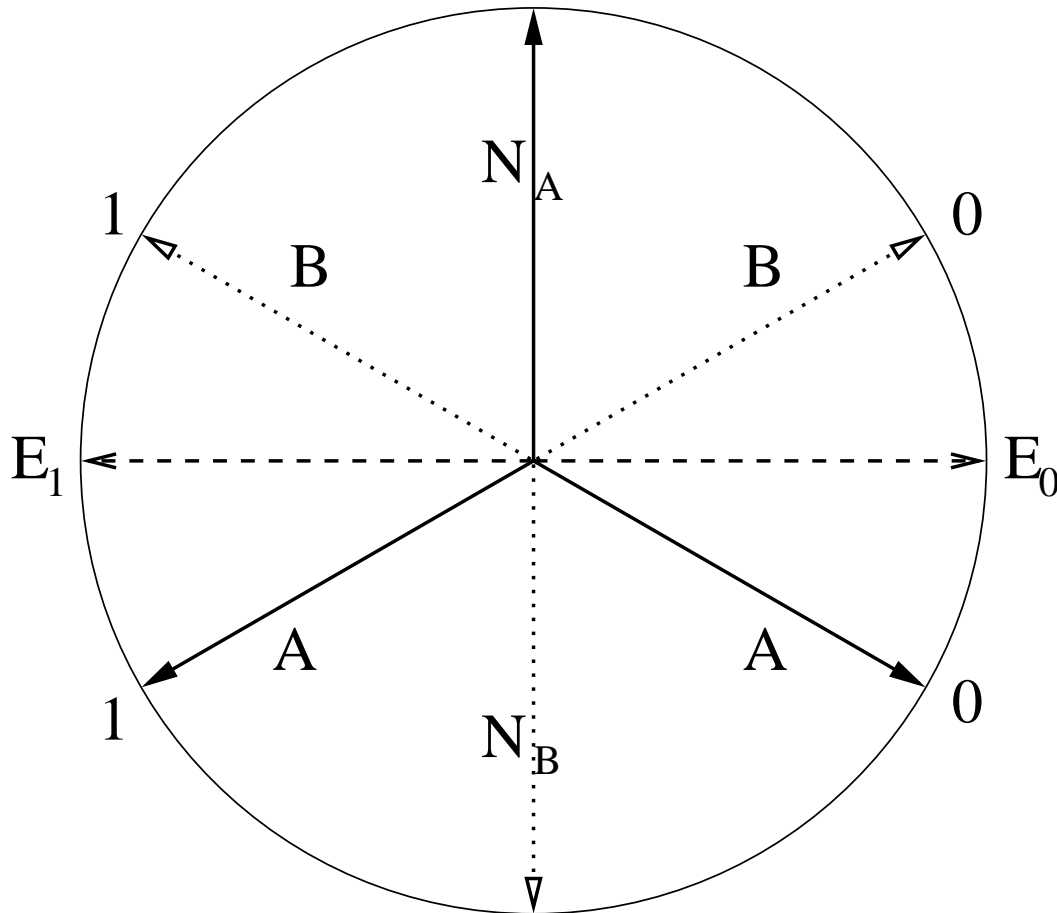
Key Bit = 0



Key Bit = 1



# Trine Key Distillation: Eve



- Eve excludes a diameter
- Strategy:
  1. Make copy
  2. Listen
  3. Meas.  $E_0, E_1$



# Intercept/Resend Eavesdropping

- Standard Intercept/Resend

Eve intercepts a fraction  $\eta$ , measures  $\{\frac{d}{n}|\phi_k\rangle\langle\phi_k|\}$ , sends  $|\phi_k\rangle$  to Bob.

- Gentle Intercept/Resend

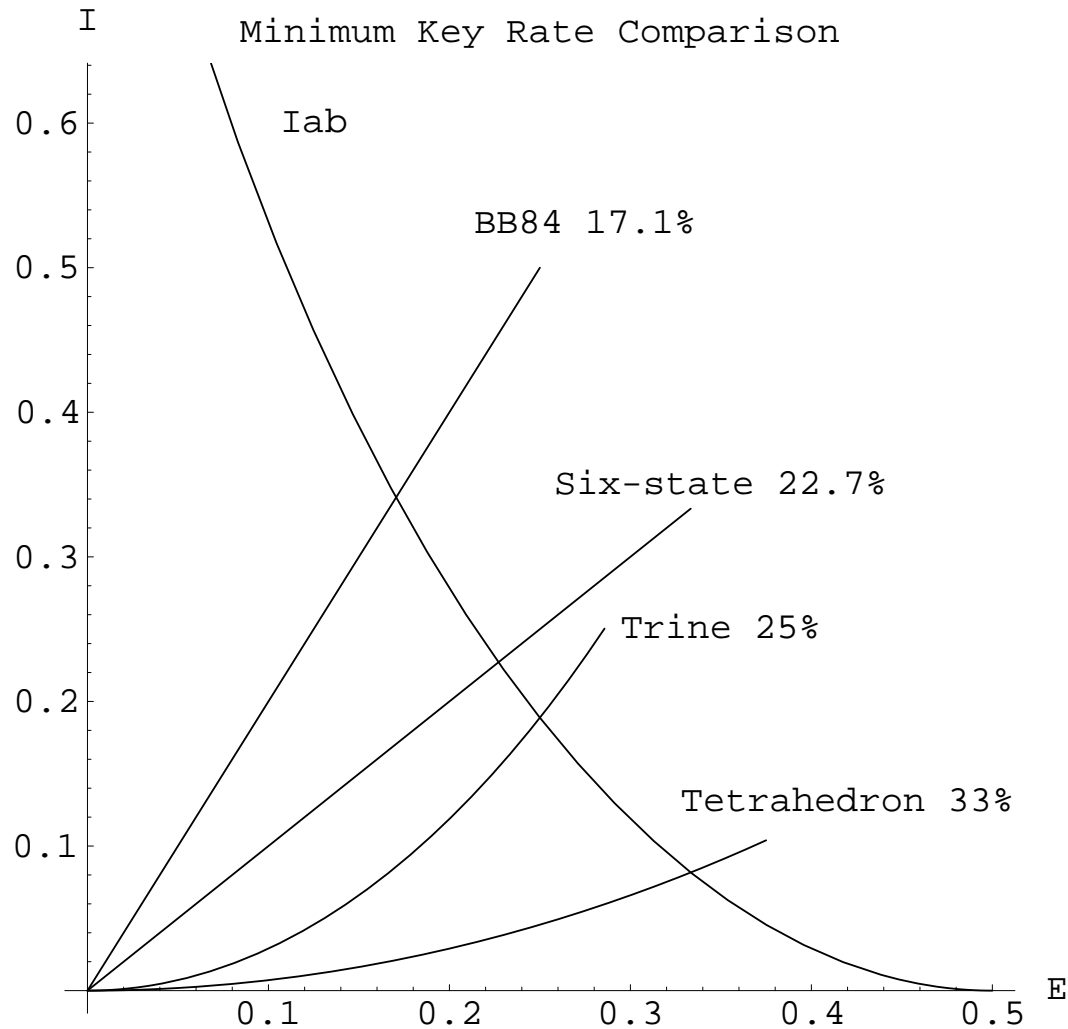
- Eve measures  $\{E_k = \frac{1-\alpha}{n}I + \alpha\frac{d}{n}|\phi_k\rangle\langle\phi_k|\}$
- Assume state transformation is

$$\rho \rightarrow \sqrt{E_k}\rho\sqrt{E_k}/\text{Tr}[E_k\rho]$$

- Optimal BB84 attack without basis information



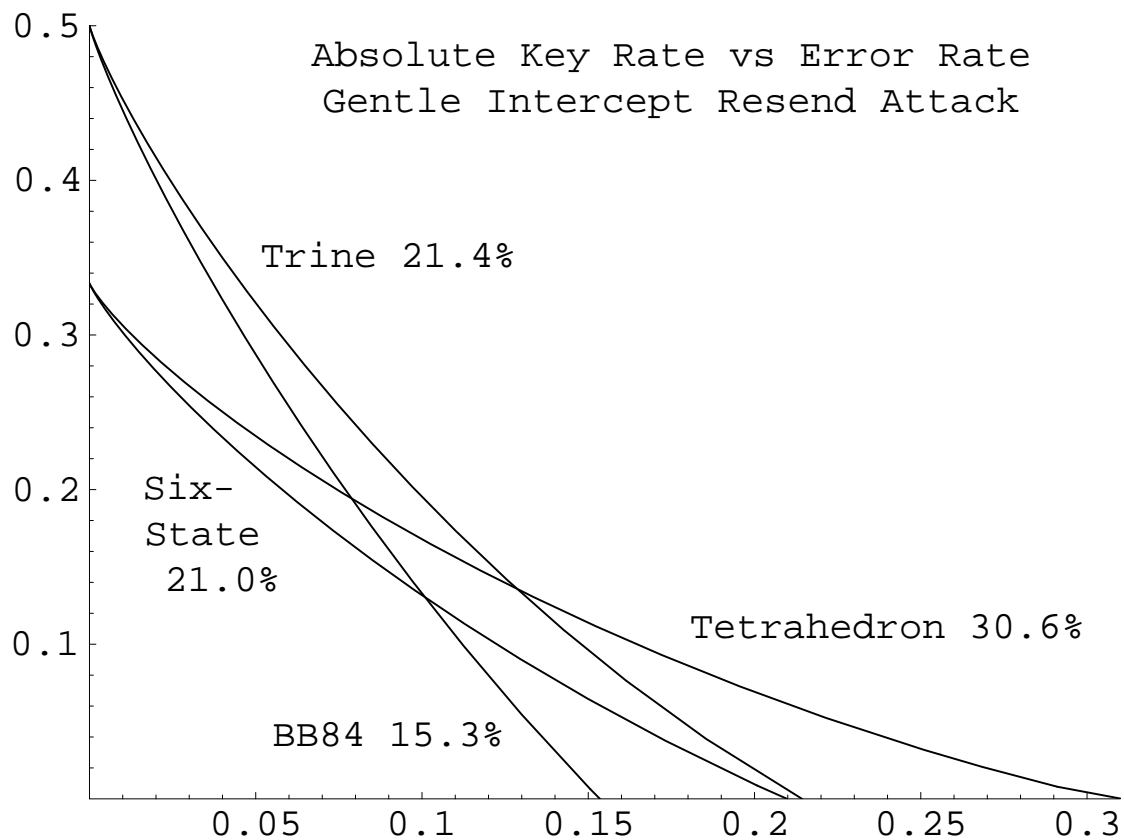
# Standard Intercept/Resend



- ESCs better “out of the box”
- Trine : BB84 :: Tetra : Six-state
- ESC protocol success rate increases with  $\eta$



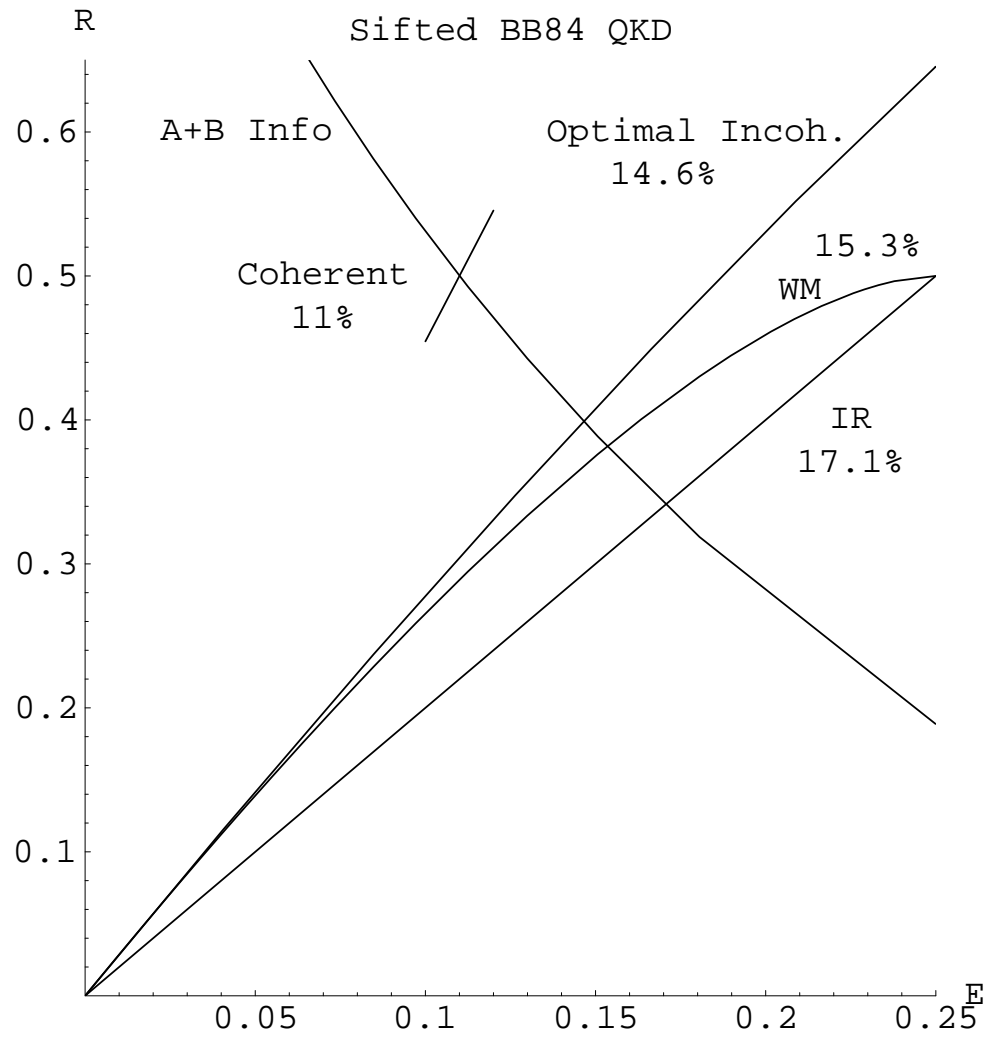
# Key Rate Comparisons



- Trine better than either MUB
- Tetrahedron most secure



# BB84 QKD: Attack Comparison



← Various attacks on BB84

Q: How strong is IR eavesdrop?

A: 30% to go!



## ***Conclusions***

---

- Qubit ESCs faster, more secure
  - Trine outperforms both BB84 and Six-state
  - Tetrahedron offers superior security
  
- Qubit ESCs simpler

Protocol success rate determines Eve's info,  
Key bit sacrifice unnecessary