



Spherical Codes & Designs in Quantum Cryptography

Joe Renes

renes@phys.unm.edu

Information Physics
University of New Mexico



Motivation & Outline

What is the best key distribution protocol available in quantum information theory?

Examine Equiangular Spherical Codes

1. Spherical Codes and Designs
2. Key Distribution & Quantum Mechanics
3. Spherical Codes vs. Mutually Unbiased Bases
4. Qubit QKD



Spherical Codes & Designs

- Spherical Code

n unit vectors $|\phi_k\rangle \in \mathbb{C}^d$ which minimize the maximal overlap $M = \max_{j \neq k} |\langle \phi_j | \phi_k \rangle|$

- Spherical t -Design

n unit vectors $|\phi_k\rangle \in \mathbb{C}^d$ which minimize the quantity $V_t = \sum_{jk} |\langle \phi_j | \phi_k \rangle|^{2t}$

- Equiangular spherical code/design for $d \leq n \leq d^2$:

$$|\langle \phi_j | \phi_k \rangle|^2 = \frac{n - d}{d(n - 1)} \quad \forall j \neq k$$



Codes & Designs examples

$d = 2$; visualize on Bloch sphere



- ESC: trine, tetrahedron
- 2-design: cardinal directions, tetrahedron

Generic facts

- 1-design = POVM
- $n = d^2$ ESC also a 2-design



Key Distribution: Setup

Goal: create a shared secret key

Resources

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

Strategy

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



Raw Key & Eavesdropper Detection

1. Alice sends signals from set $S = \{\pi_a, \Pi_a = |\phi_a\rangle\langle\phi_a|\}$
2. Eve tampers with signals: $U_{\text{signal, probe}}$
3. Bob measures signal with POVM $\{E_b\}$
4. Alice later reveals some signals sent
 - Is the distribution $p(a, b) = \pi_a \text{Tr}[E_b \Pi_a]$?
 - How much does Eve know?



Alice and Bob

- Equiangular Spherical Codes

Set of $d < n \leq d^2$ unit vectors such that

$$|\langle \phi_j | \phi_k \rangle|^2 = \frac{n - d}{d(n - 1)} \quad \forall j \neq k$$

- Mutually-Unbiased Bases

Set of $2 \leq m \leq d+1$ orthonormal bases such that

$$|\langle \phi_{i,j} | \phi_{k,l} \rangle|^2 = \frac{1}{d} \quad \forall i \neq k$$

- Both form measurements for Bob



Eavesdropping Models

- Intercept-Resend
- Weak Measurement

- Visible Cloning
- Asymmetric Blind Cloning

- General Incoherent
- General Coherent



Simple Attacks

- Intercept-resend
 - Eve measures $\{E_b\}$ and sends Π_b to Bob.
- Weak Measurements
 - Eve measures $\{F_e = (1-\alpha)I + \alpha\Pi_e\}$
 - Assume state transformation is
$$\rho \rightarrow \sqrt{F_e}\rho\sqrt{F_e}/\text{Tr}[F_e\rho]$$
 - Optimal BB84 attack without basis information



General Attacks

General Incoherent

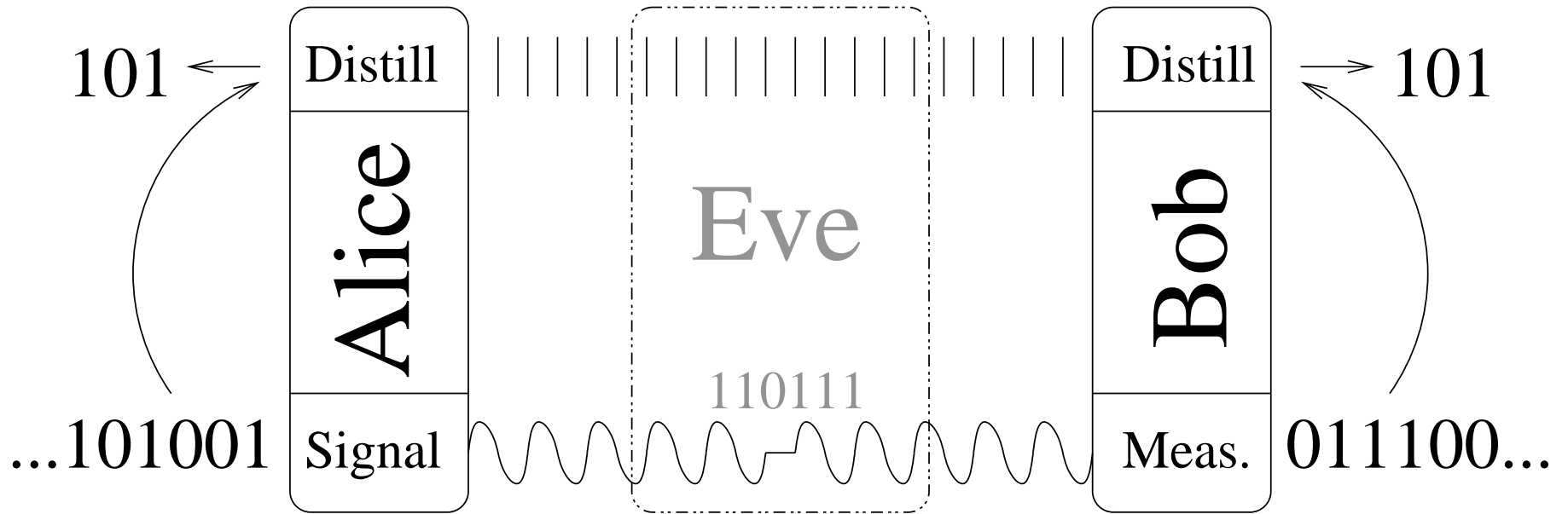
- $U|\phi_k\rangle|0\rangle = |\Phi_k\rangle = \sqrt{1-D}|\phi_k\rangle|\xi_k\rangle + \sqrt{D}|\tilde{\phi}_k\rangle|\chi_k\rangle$
- Disturbance D to Bob's system is fixed
- Optimize over $|\xi_k\rangle, |\chi_k\rangle$

General Coherent

- Probe system and *blocks* of signals interact.
- Best attack physically possible
- Analyze with error-correcting codes



Key Distribution: Schematics



- Distill key from raw sequence using classical channel
- Abort if Eve knows too much



Key Distribution: Information Theory

What secret key generation rates are possible?

- Alice, Bob, and Eve share a distribution $p(a, b, e)$
- From N samples, compute a key with length RN
- The optimal rate R is bounded by:

$$I(A:B) - \min\{I(A:E), I(B:E)\} \leq R \leq I(A:B|E)$$

- One-way communication achieves the lower bound
- Beyond this, *advantage distillation* is required
- Information A+B must share depends on $p(a, b, e)$



Key Distribution: Physics

What distributions $p(a, b, e)$ are possible?

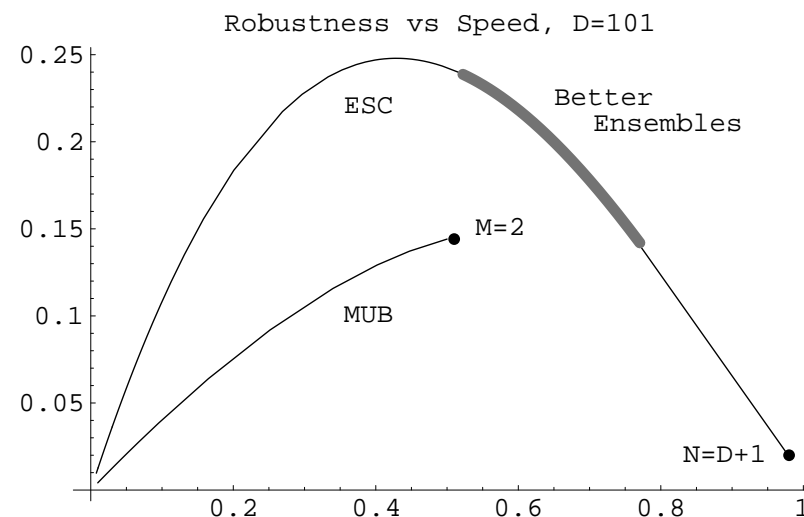
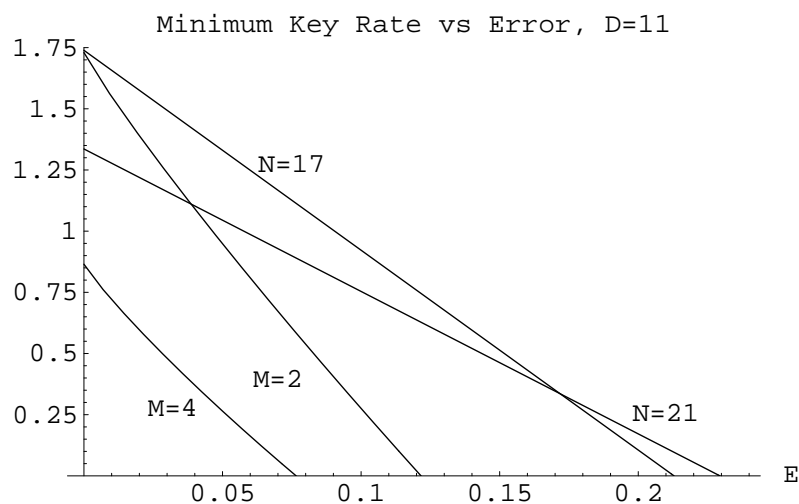
- Distribution $p(a, b, e)$ arises from measurements
- $p(a, b, e)$ depends on the information A+B must share

⇒ Cannot generally separate two parts of problem

- Consider eavesdropping which doesn't depend on "distillation information", e.g. intercept-resend and weak measurement
- Later: sifting protocol for trine & tetrahedron



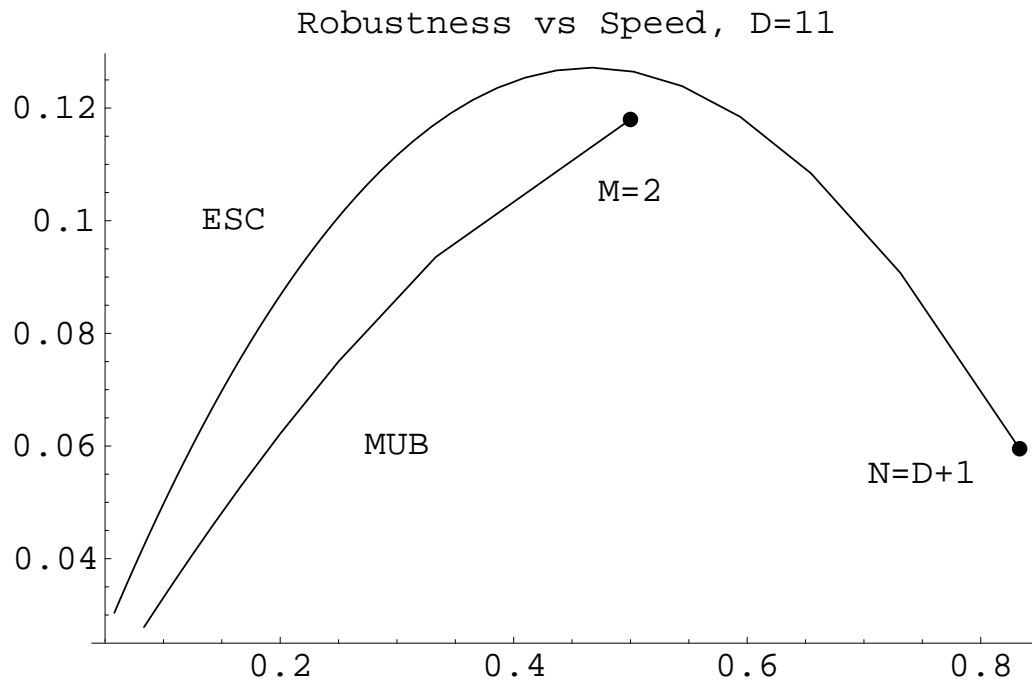
ESC vs MUB, intercept-resend



- ESCs faster, more robust
- Note: MUB analysis doesn't include sifting



ESC vs MUB, weak measurement

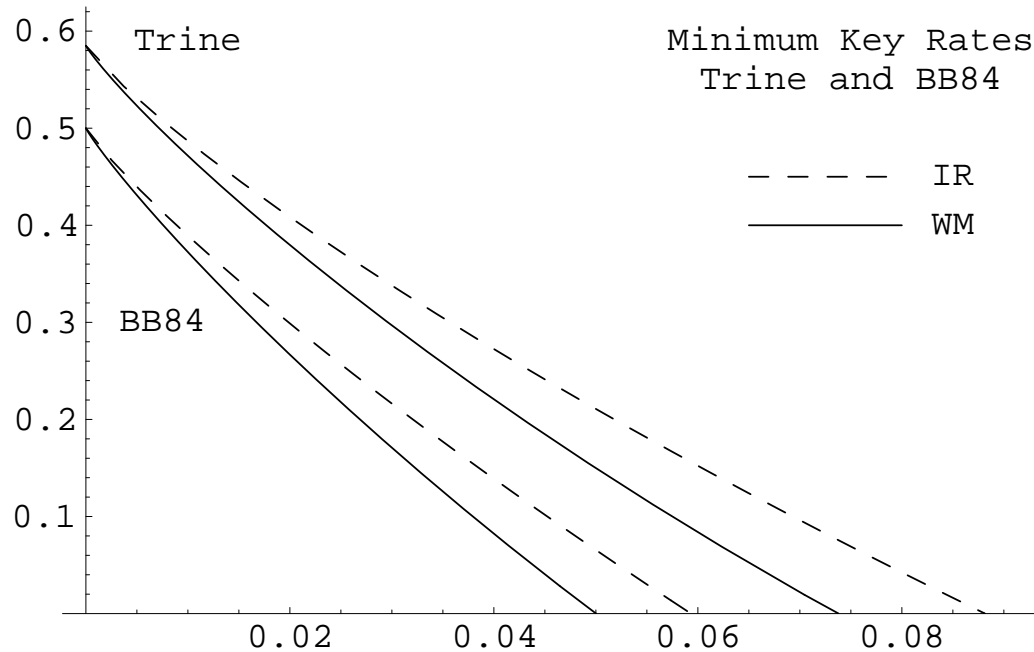


Asymptotics:

code	R_{\max}	E_{\max}
$N = \frac{2+\sqrt{2}}{2} D$	$\frac{2}{2+\sqrt{2}} \log D$	$3 - 2\sqrt{2}$
$M = 2$	$\frac{1}{2} \log D$	$\frac{1}{6}$



Qubit QKD: Trine vs BB84



- Bob uses “inverted trine” for measurement
- Eve uses trine and inverted trine
- Trine outperforms BB84

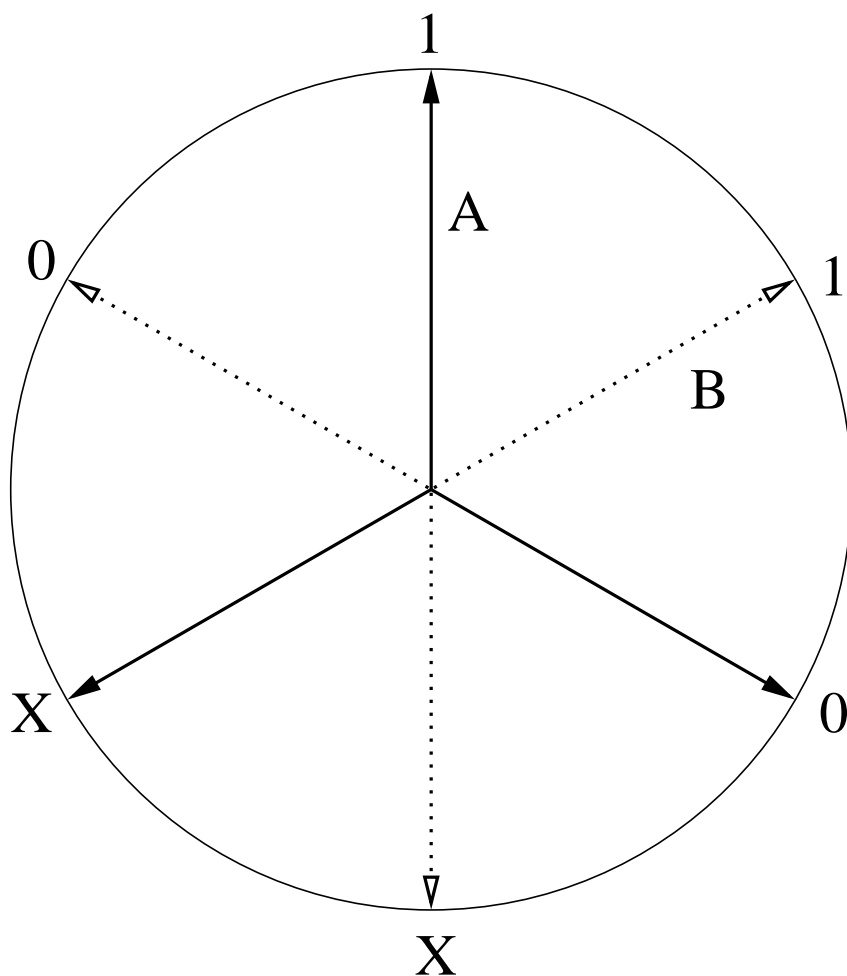


Trine Key Distillation Protocol

- Consider case of no (quantum) eavesdropping
 - A+B each know one value the other *doesn't* have
 - A or B announce one value they don't have
 - Other party confirms
- ⇒ Each knows the other's signal/outcome
- Relative position is the key bit
- ⇒ Alice and Bob create one secret bit half the time



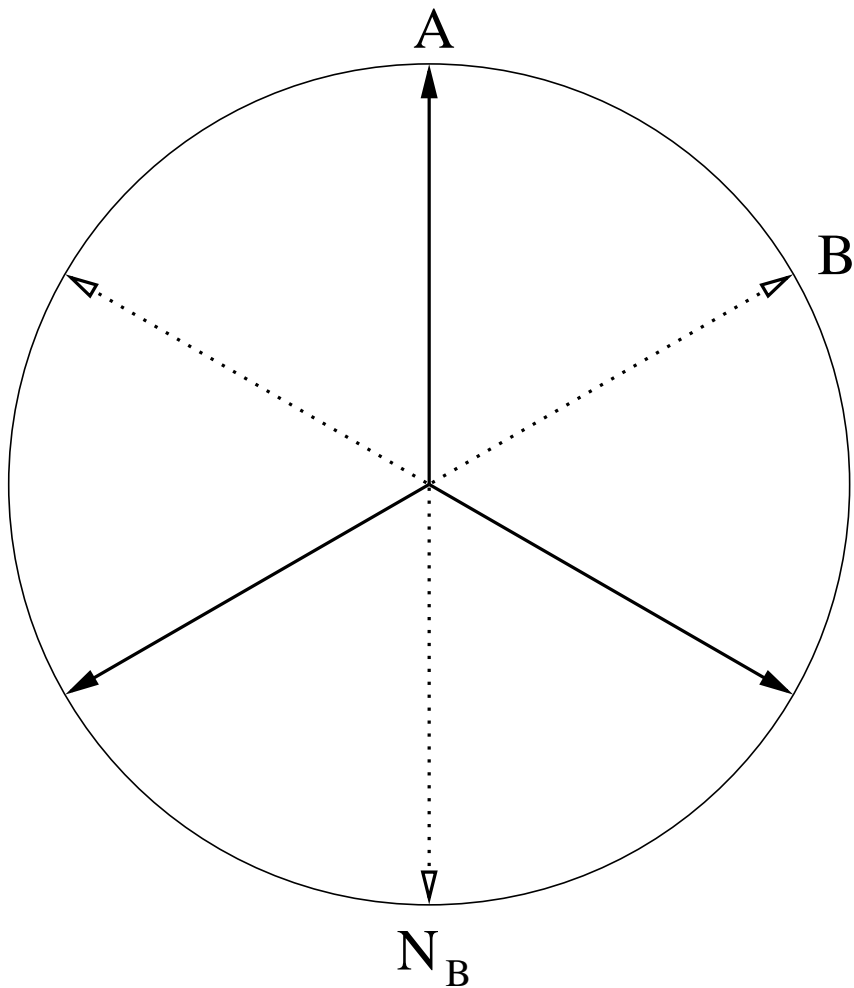
Trine Key Distillation: Labelling



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



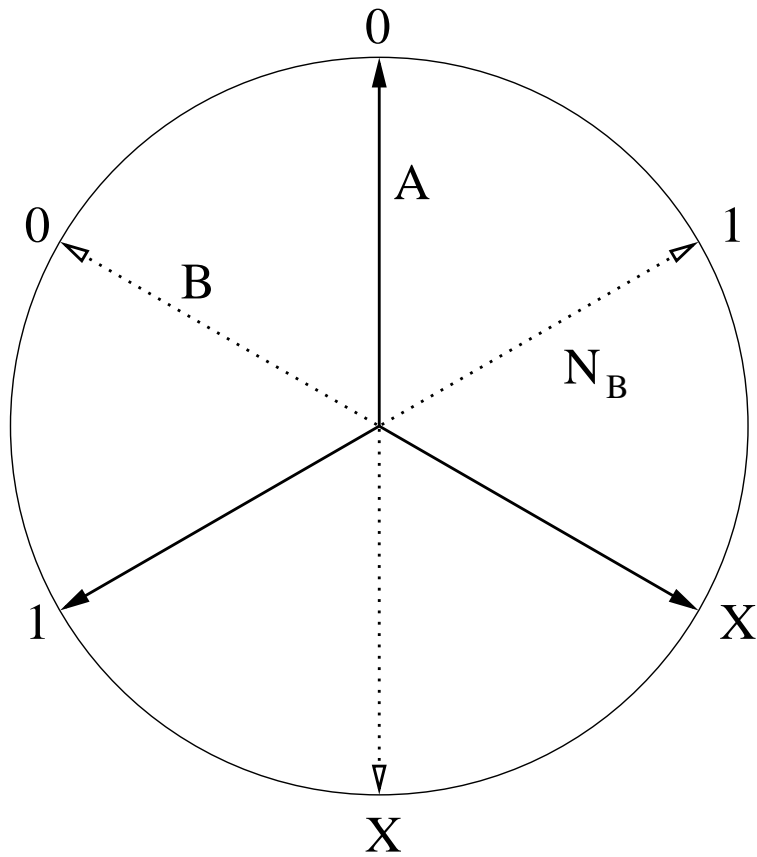
Trine Key Distillation: Failure



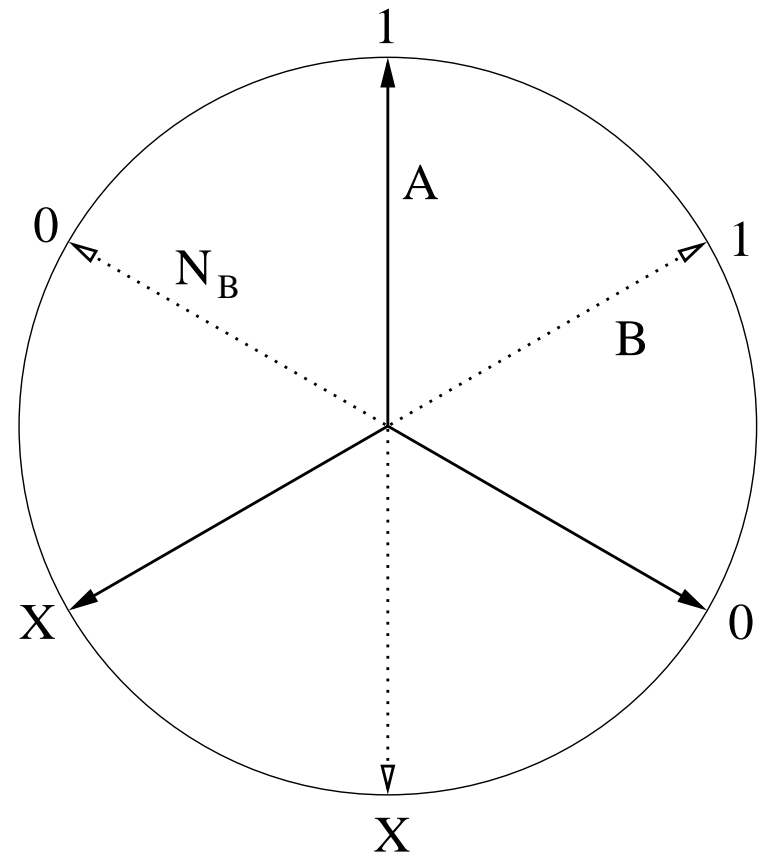
- Doesn't help Alice
- She announces "fail"
- Bob can't say more



Trine Key Distillation: Success



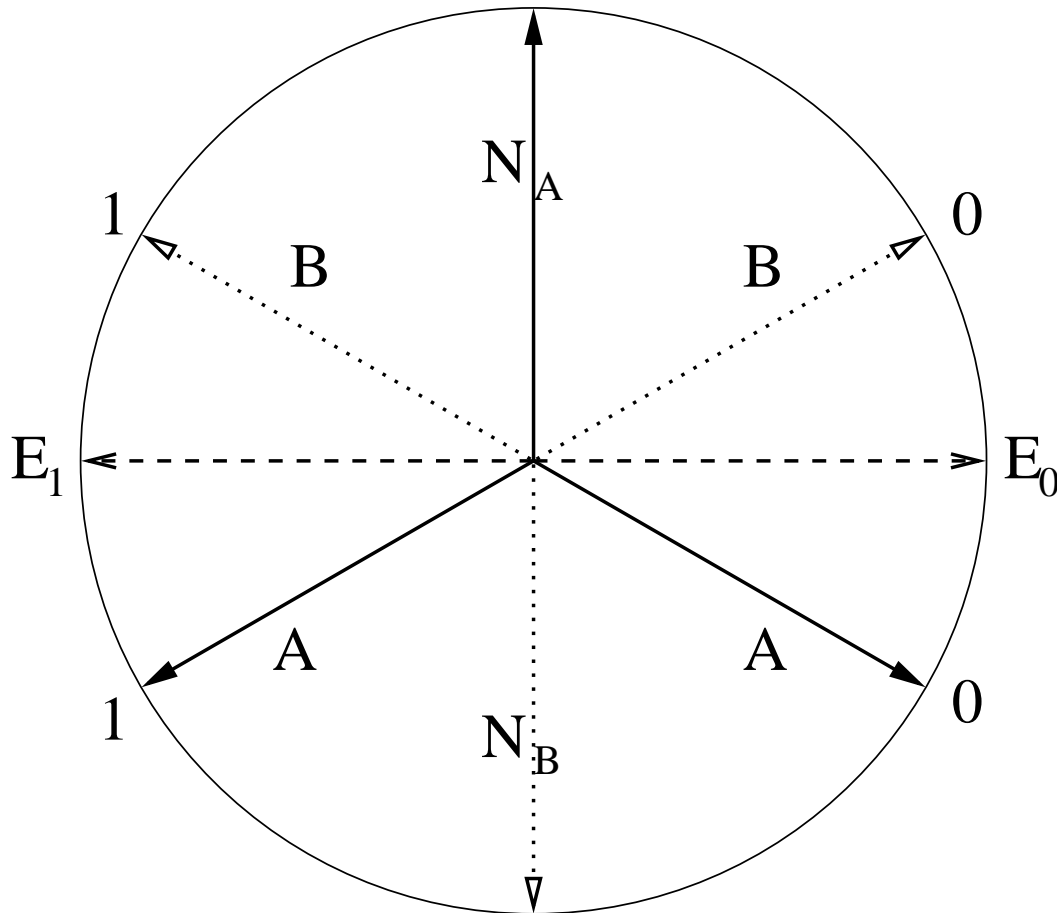
Key Bit = 0



Key Bit = 1



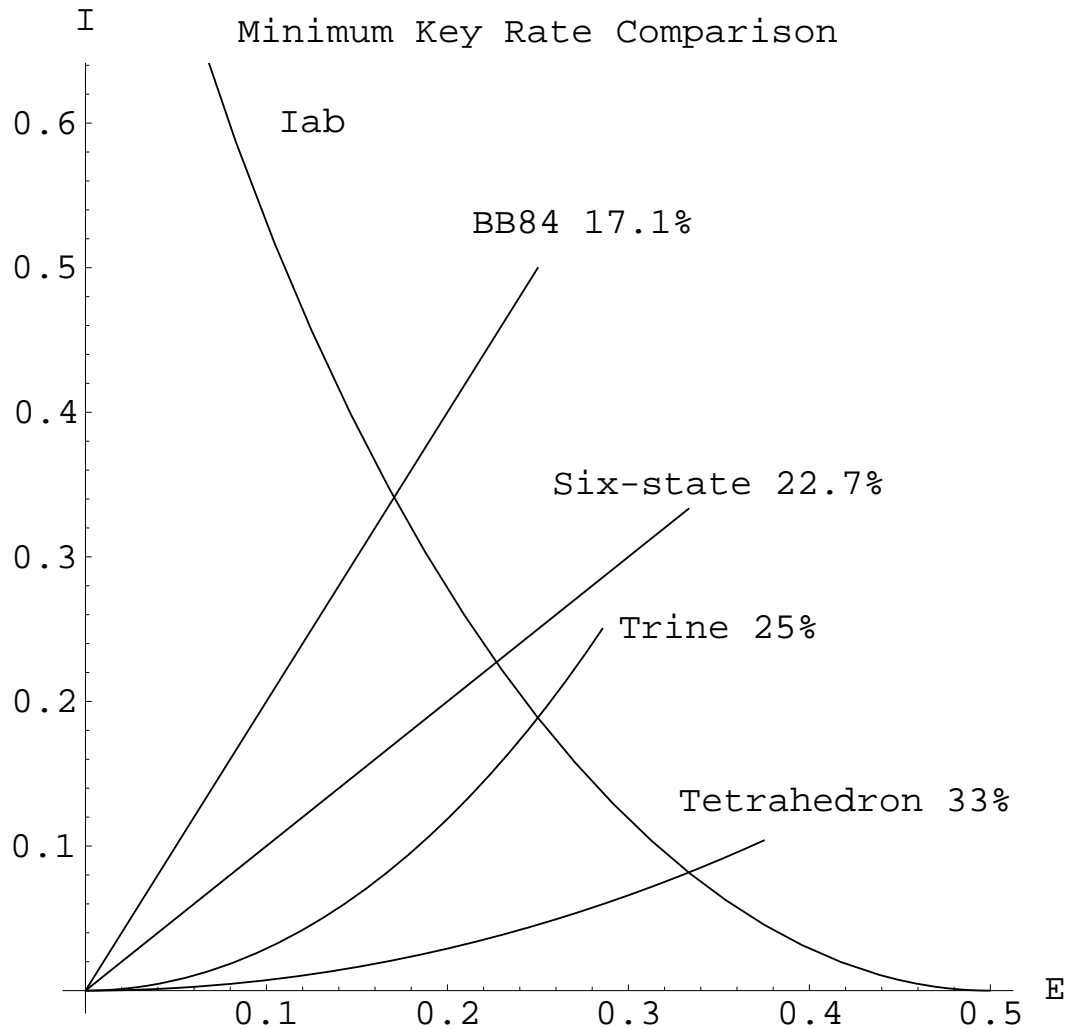
Trine Key Distillation: Eve



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



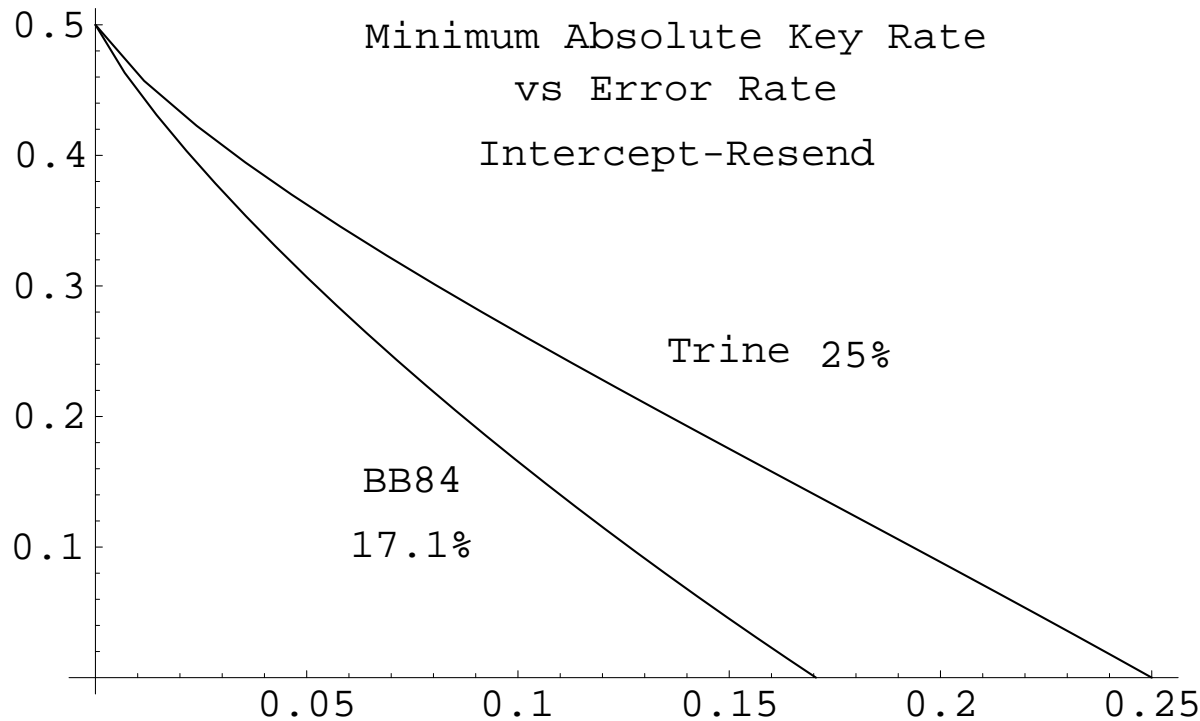
Intercept/Resend Attack



- ESCs better “out of the box”
- Trine : BB84 :: Tetra : Six-state
- ESCs and MUBs each tolerate same intercept rate



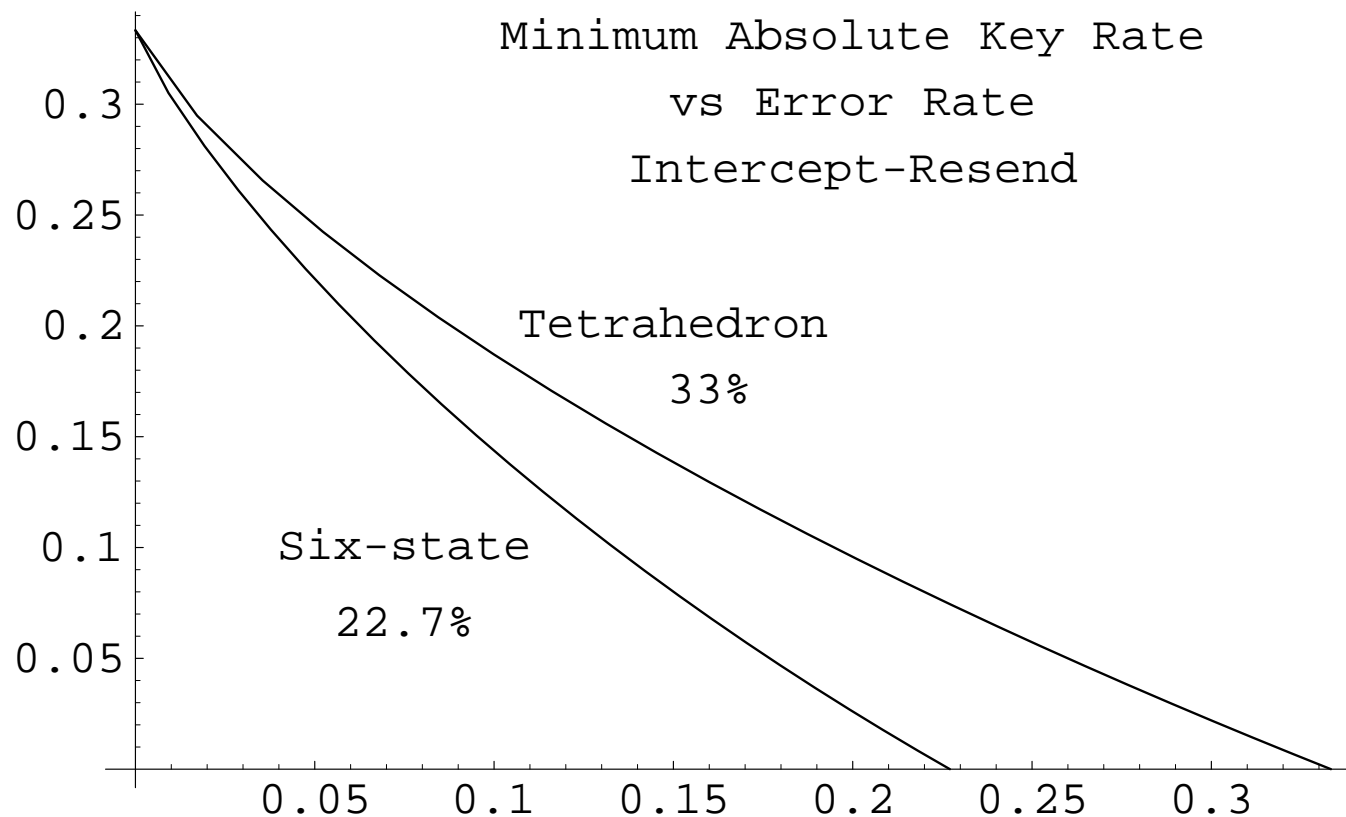
Key Rate Comparisons: Trine & BB84



- Trine failure rate *decreases* with increasing eavesdropping
- Trine \approx BB84 + B92



Tetrahedron & Six-state



- Trine outperforms Six-state
- Tetrahedron most robust



Sifted BB84 QKD

