

# Spherical Codes in Quantum Cryptography

---

Joseph Renes

renes@info.phys.unm.edu



Information Physics  
University of New Mexico

## Quantum Cryptography:

- Eavesdropper Detection
- Public Key Distribution

## Spherical Codes:

- Place  $n$  points on  $S^d$  so as to maximize the minimal distance
- Find  $n$  unit vectors in  $\mathbb{C}^d$  so as to minimize the maximal overlap

## Eavesdropper Detection

1. Alice sends states from set  $S = \{\pi_k, \Pi_k\}$
2. Bob measures incoming states with  $\{B_j\}$
3. Alice later reveals the sent states
4. Is the distribution  $p(j, k) = \pi_k \text{Tr}[B_j \Pi_k]$ ?

## Decision Process

1. Decision question is either “yes/no?” or “how much?”
2. Need a model of eavesdropping

## Eavesdropping Models

1. Cloning. Eve attempts  $|\phi_k\rangle|0\rangle \rightarrow |\Psi_k\rangle \approx |\phi_k\rangle|\phi_k\rangle$
2. Intercept/resend. Eve measures  $\{E_j\}$  and sends  $\sigma_j$  along to Bob
3. Incoherent. Eve performs  $U|\phi_k\rangle|0\rangle = |\Gamma_k\rangle = \sqrt{1-D}|\phi_k\rangle|\xi_k\rangle + \sqrt{D}|\tilde{\phi}_k\rangle|\chi_k\rangle$
4. Coherent. Eve causes probe system and *blocks* of signals to interact

Cloning:  $|\phi_k\rangle|0\rangle \rightarrow |\Psi_k\rangle \approx |\phi_k\rangle|\phi_k\rangle$

- Choose  $U$  to maximize  $\sum_k |\langle\phi_k|\langle\phi_k|U|\phi_k\rangle|0\rangle|^2$
- In general solution not known
- Foundational question — “how well can a set be cloned?”
- Decision question is “yes/no”, but model “how much” with a parameter  $q$

## Intercept/resend

- Simplest to analyze
- For spherical codes, an obvious choice for  $E_j$  and  $\sigma_j$  exists
- Foundational question — “how well can a set be sent over a classical channel?”
- Decision question is “yes/no”, but model “how much” with a parameter  $q$ .

## Incoherent

- Generic single-system attack
- Disturbance  $D$  to Bob's system is fixed; optimize over  $|\xi_k\rangle, |\chi_k\rangle$

## Coherent

- Eve's strongest attack
- Difficult to deal with here

## Deciding on the presence of Eve

- The protocol should realize  $p(j, k)$  but due to Eve, Alice and Bob sample instead from  $\tilde{p}(j, k)$ .
- Given the data, A+B work to determine which distribution they're sampling from
- We want to know how well they're likely to do
- $\Rightarrow$  consider the *difference* between  $p(j, k)$  and  $\tilde{p}(j, k)$ . Assume Eve's attack is symmetric: consider the difference of the error rates.
- Should correct for variable sensitivity to this difference.

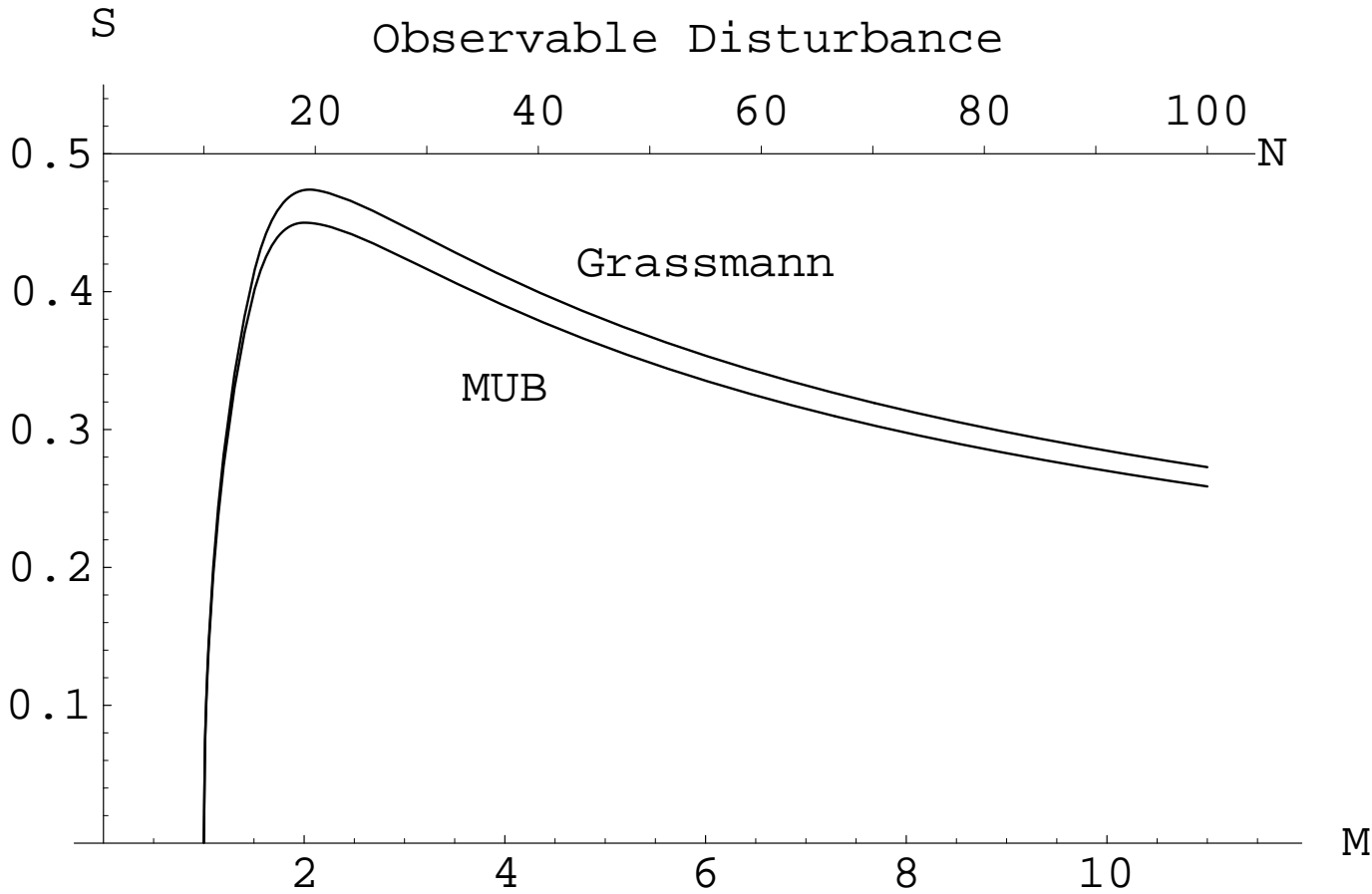
## Signal Sets:

- Spherical code: In  $\mathbb{C}^d$ ,  $d < n \leq d^2$  vectors  $|\phi_k\rangle$  such that  $|\langle\phi_j|\phi_k\rangle|^2 = \frac{n-d}{d(n-1)}$  when  $j \neq k$
- MUBs: Bases such that  $|\langle\phi_{j,k}|\phi_{l,m}\rangle|^2 = \frac{1}{d}$  whenever  $j \neq l$
- Random: Pick vectors randomly

## Measurements:

- Both spherical codes and MUBs are POVMs
- “Bend” random vectors into a POVM

# Observable disturbance in 10 dimensions

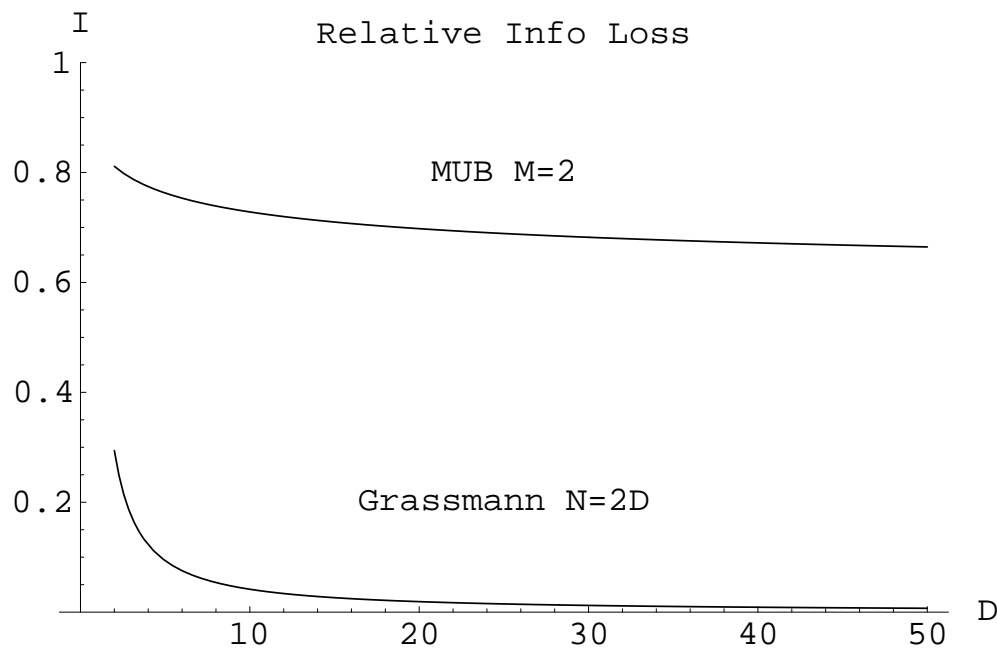
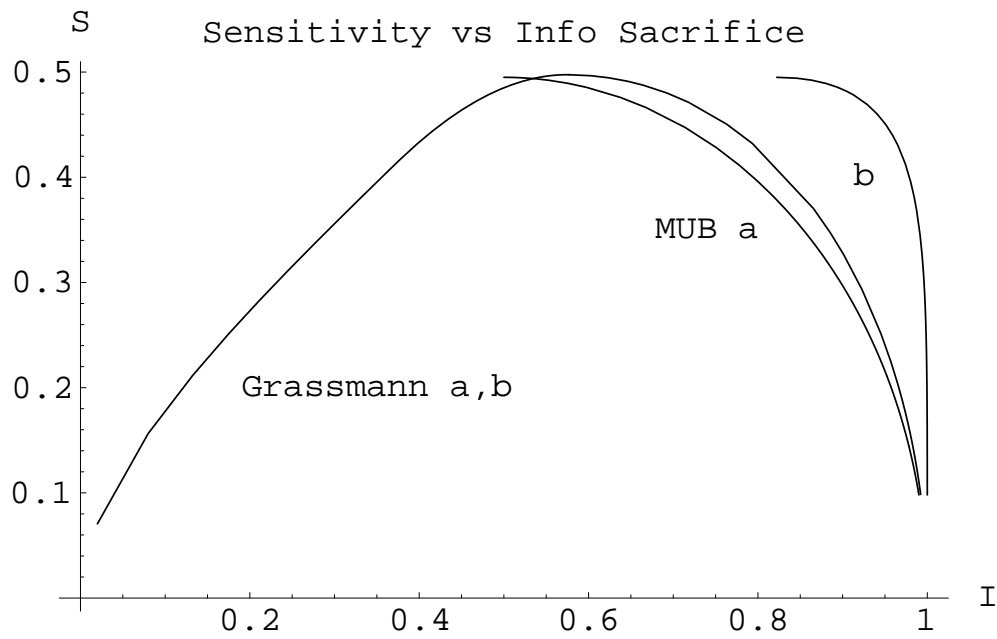


$n = 2d$  is the maximum for both types

## Tradeoffs

- between information Eve obtains and disturbance she causes to Bob's system (fixed signal set)
- between  $A+B$  channel capacity and their eavesdropper sensitivity
- between Bob's information and Eve's

⇒ useful in QKD analysis

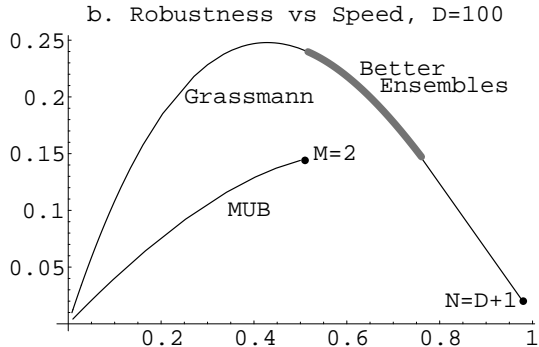
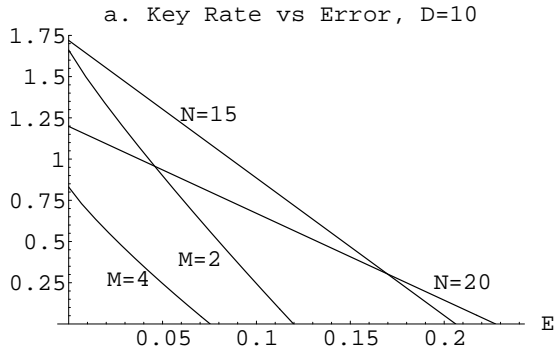


⇒ Spherical codes more robust to jamming than MUBs

## Public Key Distribution

- A+B share a distribution  $p(a, b)$
- Compute a key, with rate  $R$
- Eve is in the background —  $p(a, b, e)$
- $I(A : B) - I(A : E) \leq R \leq I(A : B|E)$
- Let  $p(a, b, e)$  arise from measurements
- $I(A : B|E) > 0$  iff state is entangled

# QKD in 10 dimensions



# QKD for qubits (using inverted measurements)

