

# SECURITY OF QUANTUM KEY DISTRIBUTION

## *the BB84 protocol*

MICHEL BOYER

Dept. IRO, Université de Montréal

<http://www.iro.umontreal.ca/~boyer>



## **SYMMETRIC KEY CRYPTO**

- **DEFINITION**
- **ONE TIME PAD**
- **PROBLEMS AND A SOLUTION**

### **THE BB84 PROTOCOL**

---

### **CODES**

---

### **EVE'S ATTACK**

---

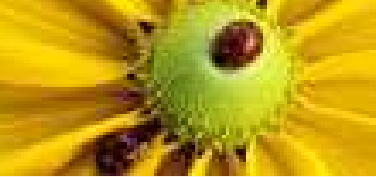
### **INFO VS. DISTURBANCE**

---

### **REFERENCES**

---

# **SYMMETRIC KEY CRYPTO**



# DEFINITION

To send a secret message

**SYMMETRIC KEY CRYPTO**

▸ **DEFINITION**

▸ **ONE TIME PAD**

▸ **PROBLEMS AND A SOLUTION**

**THE BB84 PROTOCOL**

---

**CODES**

---

**EVE'S ATTACK**

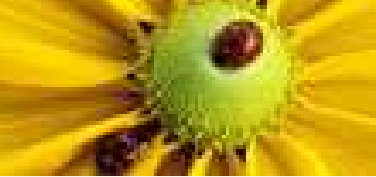
---

**INFO VS. DISTURBANCE**

---

**REFERENCES**

---



# DEFINITION

To send a secret message

## ■ Brute force method

- ◆ put the message in a safe and send
- ◆ the unlock key is a copy of the lock key
- ◆ make sure the addressee gets the package
- ◆ make sure he can open the safe and no one else

SYMMETRIC KEY CRYPTO

▸ DEFINITION

▸ ONE TIME PAD

▸ PROBLEMS AND A SOLUTION

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# DEFINITION

To send a secret message

## ■ Brute force method

- ◆ put the message in a safe and send
- ◆ the unlock key is a copy of the lock key
- ◆ make sure the addressee gets the package
- ◆ make sure he can open the safe and no one else

## ■ Informational method: encrypt (code) and decrypt (decode)

- ◆  $\mathcal{M}$  = Set of possible messages,  $\mathcal{K}$  is set of keys
- ◆  $E : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{M}$  encryption function
- ◆  $D : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{M}$  decryption function
- ◆  $M' = E(M, k)$  is message  $M$  encrypted with key  $k$
- ◆  $D(M', k) = D(E(M, k), k) = M$ .

SYMMETRIC KEY CRYPTO

▶ DEFINITION

▶ ONE TIME PAD

▶ PROBLEMS AND A SOLUTION

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES

# DEFINITION

To send a secret message

## ■ Brute force method

- ◆ put the message in a safe and send
- ◆ the unlock key is a copy of the lock key
- ◆ make sure the addressee gets the package
- ◆ make sure he can open the safe and no one else

## ■ Informational method: encrypt (code) and decrypt (decode)

- ◆  $\mathcal{M}$  = Set of possible messages,  $\mathcal{K}$  is set of keys
- ◆  $E : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{M}$  encryption function
- ◆  $D : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{M}$  decryption function
- ◆  $M' = E(M, k)$  is message  $M$  encrypted with key  $k$
- ◆  $D(M', k) = D(E(M, k), k) = M$ .

## ■ $M'$ should give as little information on $M$ as possible if $k$ is unknown.

SYMMETRIC KEY CRYPTO

▶ DEFINITION

▶ ONE TIME PAD

▶ PROBLEMS AND A SOLUTION

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES

# ONE TIME PAD

To send a secret message

## ■ Encryption and decryption function:

- ◆  $\mathcal{M} \subseteq \mathcal{K} = \{0, 1\}^n, P[k] = \frac{1}{2^n}$

- ◆  $E(M, k) = M \oplus k$

- ◆  $D(M', k) = M' \oplus k$

## ■ Properties

- ◆  $D(E(M, k), k) = (M \oplus k) \oplus k = M \oplus (k \oplus k) = M \oplus 0^n = M$

- ◆  $P[M | M'] = \frac{1}{|\mathcal{M}|}$ .

- ◆ Knowledge of  $M'$  gives no information on  $M$  if  $k$  is unknown.

- We could also use  $\mathcal{K} = \mathcal{M} \subseteq \{0, 1\}^n$ .

- Or  $\mathcal{M} = \mathcal{K} \subseteq G$  (group),  $E(M, k) = Mk$  and  $D(M', k) = M'k^{-1}$ .

- This is the only provably unconditionally secure protocol known.

SYMMETRIC KEY CRYPTO

▸ DEFINITION

▸ ONE TIME PAD

▸ PROBLEMS AND A SOLUTION

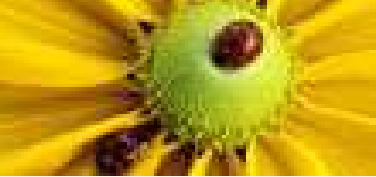
THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PROBLEMS AND A SOLUTION

**SYMMETRIC KEY CRYPTO**

---

▶ **DEFINITION**

▶ **ONE TIME PAD**

▶ **PROBLEMS AND A SOLUTION**

**THE BB84 PROTOCOL**

---

**CODES**

---

**EVE'S ATTACK**

---

**INFO VS. DISTURBANCE**

---

**REFERENCES**

---





# PROBLEMS AND A SOLUTION

## ■ Limitations

- ◆ keys of one time pads are as long as messages
- ◆ they can be used only once
- ◆ classical communication channels can be tapped in silence
- ◆ trusted couriers are expensive (can they be trusted?)

SYMMETRIC KEY CRYPTO

▶ DEFINITION

▶ ONE TIME PAD

▶ PROBLEMS AND A SOLUTION

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PROBLEMS AND A SOLUTION

## ■ Limitations

- ◆ keys of one time pads are as long as messages
- ◆ they can be used only once
- ◆ classical communication channels can be tapped in silence
- ◆ trusted couriers are expensive (can they be trusted?)

## ■ A solution: going quantum

- ◆ bits can be encoded using conjugate bases
- ◆ decoding requires knowledge of those bases
- ◆ quantum channels cannot be tapped without inducing noise
- ◆ the bases are told publicly once the encoded bits are received
- ◆ the owner of the encoded bits can decode them
- ◆ eavesdroppers get exponentially small information
- ◆ this holds even with publicly known error correction data.

SYMMETRIC KEY CRYPTO

▶ DEFINITION

▶ ONE TIME PAD

▶ PROBLEMS AND A SOLUTION

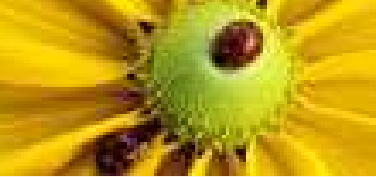
THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



---

## SYMMETRIC KEY CRYPTO

---

### THE BB84 PROTOCOL

- THE PLAYERS
- THE BB84 STATES
- A FIRST PROTOCOL
- GOOD & BAD

---

## CODES

---

---

## EVE'S ATTACK

---

---

## INFO VS. DISTURBANCE

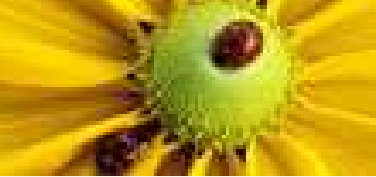
---

---

## REFERENCES

---

# THE BB84 PROTOCOL



# THE PLAYERS

---

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### ▶ THE PLAYERS

#### ▶ THE BB84 STATES

#### ▶ A FIRST PROTOCOL

#### ▶ GOOD & BAD

---

## CODES

---

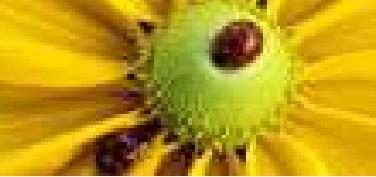
## EVE'S ATTACK

---

## INFO VS. DISTURBANCE

---

## REFERENCES



# THE PLAYERS

## ■ *Alice* and *Bob*

### SYMMETRIC KEY CRYPTO

---

### THE BB84 PROTOCOL

#### ▶ THE PLAYERS

#### ▶ THE BB84 STATES

#### ▶ A FIRST PROTOCOL

#### ▶ GOOD & BAD

### CODES

---

### EVE'S ATTACK

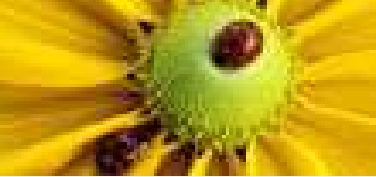
---

### INFO VS. DISTURBANCE

---

### REFERENCES

---



# THE PLAYERS

- *Alice* and *Bob*: they want to share a key

---

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### ▶ THE PLAYERS

#### ▶ THE BB84 STATES

#### ▶ A FIRST PROTOCOL

#### ▶ GOOD & BAD

---

## CODES

---

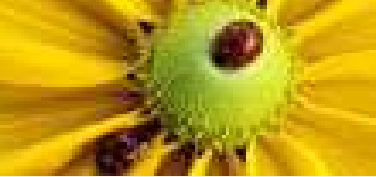
## EVE'S ATTACK

---

## INFO VS. DISTURBANCE

---

## REFERENCES



# THE PLAYERS

- *Alice* and *Bob*: they want to share a key
  - ◆ Alice can prepare qubits

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### ▶ THE PLAYERS

#### ▶ THE BB84 STATES

#### ▶ A FIRST PROTOCOL

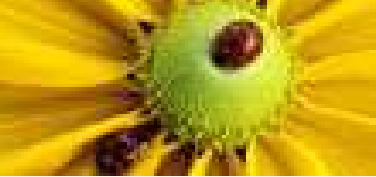
#### ▶ GOOD & BAD

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a *quantum channel*

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### ▶ THE PLAYERS

#### ▶ THE BB84 STATES

#### ▶ A FIRST PROTOCOL

#### ▶ GOOD & BAD

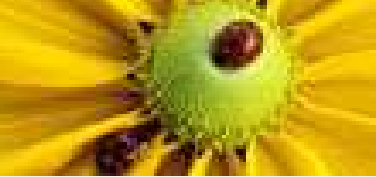
## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES





# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a *quantum channel*
  - ◆ Bob can apply H or not and measure a qubit

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### THE PLAYERS

#### THE BB84 STATES

#### A FIRST PROTOCOL

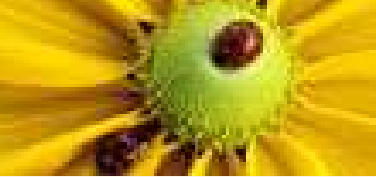
#### GOOD & BAD

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a *quantum channel*
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### THE PLAYERS

#### THE BB84 STATES

#### A FIRST PROTOCOL

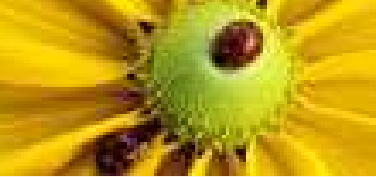
#### GOOD & BAD

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### THE PLAYERS

#### THE BB84 STATES

#### A FIRST PROTOCOL

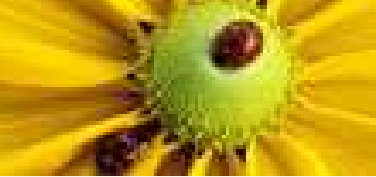
#### GOOD & BAD

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**
- **Eve** (the eavesdropper) wants to know the key and can

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

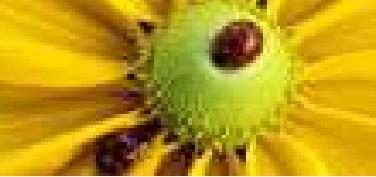
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**
- **Eve** (the eavesdropper) wants to know the key and can
  - ◆ do whatever quantum mechanics allows

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

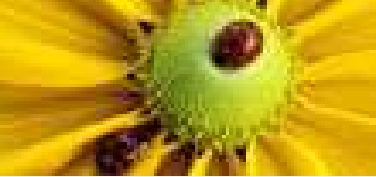
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**
- **Eve** (the eavesdropper) wants to know the key and can
  - ◆ do whatever quantum mechanics allows
  - ◆ read all data on the classical channel

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

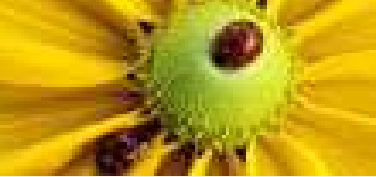
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**
- **Eve** (the eavesdropper) wants to know the key and can
  - ◆ do whatever quantum mechanics allows
  - ◆ read all data on the classical channel
  - ◆ catch the qubits sent by Alice

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

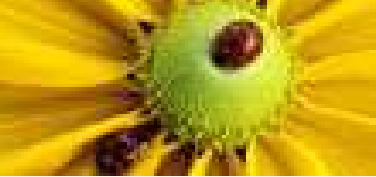
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**
- **Eve** (the eavesdropper) wants to know the key and can
  - ◆ do whatever quantum mechanics allows
  - ◆ read all data on the classical channel
  - ◆ catch the qubits sent by Alice
  - ◆ attach them a probing device

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

▶ GOOD & BAD

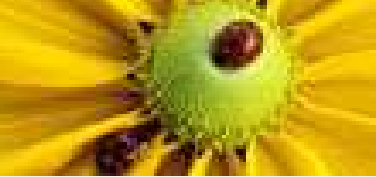
CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES





# THE PLAYERS

- **Alice** and **Bob**: they want to share a key
  - ◆ Alice can prepare qubits
  - ◆ she can send them to Bob via a **quantum channel**
  - ◆ Bob can apply H or not and measure a qubit
  - ◆ we assume he can also memorize qubits
  - ◆ they also use a good public **classical channel**
- **Eve** (the eavesdropper) wants to know the key and can
  - ◆ do whatever quantum mechanics allows
  - ◆ read all data on the classical channel
  - ◆ catch the qubits sent by Alice
  - ◆ attach them a probing device
  - ◆ wait to choose the optimal way of measuring it

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

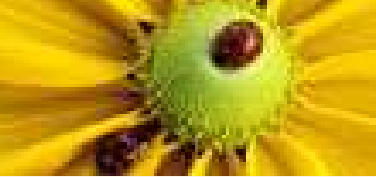
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# THE BB84 STATES

- Those are the states Alice sends to Bob

- They are:  $|0\rangle$ ,  $|1\rangle$ ,  $H|0\rangle$ ,  $H|1\rangle$

- $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}} [ |0\rangle + |1\rangle ]$  and

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}} [ |0\rangle - |1\rangle ]$$

- Measuring in the standard basis  $\{|0\rangle, |1\rangle\}$

- ◆ state  $|0\rangle$  gives 0 with probability 1

- ◆ state  $|1\rangle$  gives 1 with probability 1

- ◆ state  $|+\rangle$  gives a random bit [ $p(0) = 1/2$ ,  $p(1) = 1/2$ ]

- ◆ state  $|-\rangle$  gives a random bit [ $p(0) = 1/2$ ,  $p(1) = 1/2$ ]

- $H|+\rangle = |0\rangle$  and  $H|-\rangle = |1\rangle$

## SYMMETRIC KEY CRYPTO

### THE BB84 PROTOCOL

#### ▶ THE PLAYERS

#### ▶ THE BB84 STATES

#### ▶ A FIRST PROTOCOL

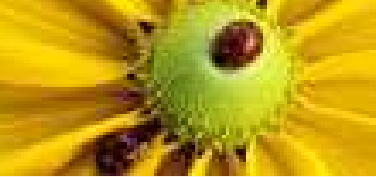
#### ▶ GOOD & BAD

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES



# A FIRST PROTOCOL

## ■ Notations

- ◆  $H^0 = I, H^1 = H$
- ◆  $H^{\mathbf{b}} = H^{b_1} \otimes \dots \otimes H^{b_{2n}}$  if  $\mathbf{b} = b_1 \dots b_{2n}$ .

- Alice selects randomly  $\mathbf{i}, \mathbf{b} \in \{0, 1\}^{2n}$  and  $\mathbf{s} \in \{0, 1\}^{2n}$  with  $|\mathbf{s}| = n$ .
- She sends Bob  $H^{\mathbf{b}} |\mathbf{i}\rangle$
- When Bob has them all, she announces publicly  $\mathbf{b}$  and  $\mathbf{s}$
- Bob applies  $H^{\mathbf{b}}$  to his state and measures
- If there is no noise he recovers  $\mathbf{i}$
- Bob and Alice publicly check for errors on the bits with  $b_j = 0$
- The key is the parity of the bits  $i_j$  for which  $b_j = 1$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

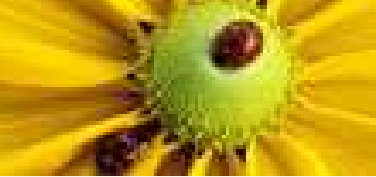
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# GOOD & BAD

## ■ Good thing:

- ◆ to know the key, Eve has to guess all  $b_j$  s.t.  $s_j = 1$
- ◆ to be undetected, she has to guess the  $b_j$  s.t.  $s_j = 0$
- ◆ ... or be lucky with Bob's random outputs

## ■ Bad thing:

- ◆ the quantum channel cannot be noisy
- ◆ the key has just one bit

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

▶ THE PLAYERS

▶ THE BB84 STATES

▶ A FIRST PROTOCOL

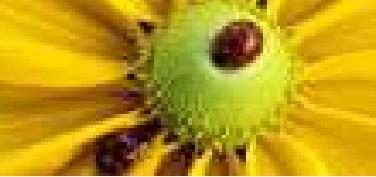
▶ GOOD & BAD

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



---

## SYMMETRIC KEY CRYPTO

---

---

## THE BB84 PROTOCOL

---

## CODES

- BITSTRINGS AS VECTORS
- BINARY CODES
- ERROR CORRECTION
- PRIVACY AMPLIFICATION
- BB84 WITH CODES

---

## EVE'S ATTACK

---

---

## INFO VS. DISTURBANCE

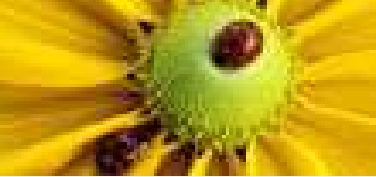
---

---

## REFERENCES

---

# CODES



# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $F_2$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

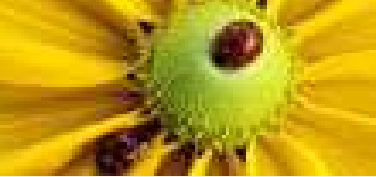
▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $F_2$
- The sum  $+$  is the sum modulo 2, i.e.  $\oplus$  (exclusive or)

## SYMMETRIC KEY CRYPTO

## THE BB84 PROTOCOL

## CODES

### ▶ BITSTRINGS AS VECTORS

### ▶ BINARY CODES

### ▶ ERROR CORRECTION

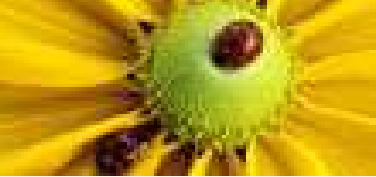
### ▶ PRIVACY AMPLIFICATION

### ▶ BB84 WITH CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

## REFERENCES



# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $\mathbb{F}_2$
- The sum  $+$  is the sum modulo 2, i.e.  $\oplus$  (exclusive or)
- $\mathbf{x} = x_1 x_2 \dots x_n$  identified with  $[x_1, x_2, \dots, x_n] \in \mathbb{F}_2^n$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

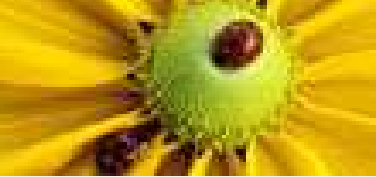
▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES





# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $\mathbb{F}_2$
- The sum  $+$  is the sum modulo 2, i.e.  $\oplus$  (exclusive or)
- $\mathbf{x} = x_1 x_2 \dots x_n$  identified with  $[x_1, x_2, \dots, x_n] \in \mathbb{F}_2^n$
- Linear maps  $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ 
  - ◆  $m \times n$  matrix  $A$  acting on columns  $\mathbf{x}^T \mapsto A\mathbf{x}^T$
  - ◆  $m \times n$  matrix  $A$  acting on rows  $\mathbf{x} \mapsto \mathbf{x}A^T$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $\mathbf{F}_2$
- The sum  $+$  is the sum modulo 2, i.e.  $\oplus$  (exclusive or)
- $\mathbf{x} = x_1 x_2 \dots x_n$  identified with  $[x_1, x_2, \dots, x_n] \in \mathbf{F}_2^n$
- Linear maps  $\mathbf{F}_2^n \rightarrow \mathbf{F}_2^m$ 
  - ◆  $m \times n$  matrix  $A$  acting on columns  $\mathbf{x}^T \mapsto A\mathbf{x}^T$
  - ◆  $m \times n$  matrix  $A$  acting on rows  $\mathbf{x} \mapsto \mathbf{x}A^T$
- Example: select bits 2, 3 and 6 from  $\mathbf{i} = i_1 i_2 i_3 i_4 i_5 i_6$

$$P_s \mathbf{i}^T = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \\ i_5 \\ i_6 \end{bmatrix} = \begin{bmatrix} i_2 \\ i_3 \\ i_6 \end{bmatrix}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $\mathbf{F}_2$
- The sum  $+$  is the sum modulo 2, i.e.  $\oplus$  (exclusive or)
- $\mathbf{x} = x_1 x_2 \dots x_n$  identified with  $[x_1, x_2, \dots, x_n] \in \mathbf{F}_2^n$
- Linear maps  $\mathbf{F}_2^n \rightarrow \mathbf{F}_2^m$ 
  - ◆  $m \times n$  matrix  $A$  acting on columns  $\mathbf{x}^T \mapsto A\mathbf{x}^T$
  - ◆  $m \times n$  matrix  $A$  acting on rows  $\mathbf{x} \mapsto \mathbf{x}A^T$
- Example: select bits 2, 3 and 6 from  $\mathbf{i} = i_1 i_2 i_3 i_4 i_5 i_6$

$$P_s \mathbf{i}^T = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \\ i_5 \\ i_6 \end{bmatrix} = \begin{bmatrix} i_2 \\ i_3 \\ i_6 \end{bmatrix}$$

- Row representation  $i_2 i_3 i_6 = \mathbf{i} P_s^T$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

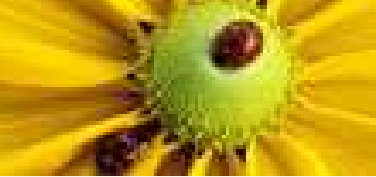
▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# BITSTRINGS AS VECTORS

- $\{0, 1\}$  identified with the two element field  $\mathbf{F}_2$
- The sum  $+$  is the sum modulo 2, i.e.  $\oplus$  (exclusive or)
- $\mathbf{x} = x_1 x_2 \dots x_n$  identified with  $[x_1, x_2, \dots, x_n] \in \mathbf{F}_2^n$
- Linear maps  $\mathbf{F}_2^n \rightarrow \mathbf{F}_2^m$ 
  - ◆  $m \times n$  matrix  $A$  acting on columns  $\mathbf{x}^T \mapsto A\mathbf{x}^T$
  - ◆  $m \times n$  matrix  $A$  acting on rows  $\mathbf{x} \mapsto \mathbf{x}A^T$
- Example: select bits 2, 3 and 6 from  $\mathbf{i} = i_1 i_2 i_3 i_4 i_5 i_6$

$$P_s \mathbf{i}^T = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \\ i_5 \\ i_6 \end{bmatrix} = \begin{bmatrix} i_2 \\ i_3 \\ i_6 \end{bmatrix}$$

- Row representation  $i_2 i_3 i_6 = \mathbf{i} P_s^T$
- Similarly  $i_1 i_4 i_5 = \mathbf{i} P_s^T$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

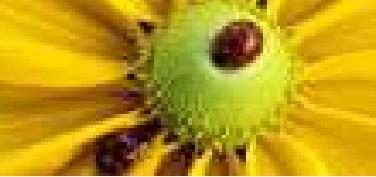
▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# BINARY CODES

Notation  $|\mathbf{x}| = \textit{Hamming weight}$  of  $\mathbf{x}$  = number of ones in  $\mathbf{x}$ .

■  $C$  is a binary  $(n, n - r, d)$  *linear code* if

- ◆  $C \subseteq \mathbb{F}_2^n$  is a  $\mathbb{F}_2$  linear subspace
- ◆  $\dim C = n - r$  (dimension over  $\mathbb{F}_2$ )
- ◆  $\min \{|\mathbf{x}| : \mathbf{x} \in C \wedge \mathbf{x} \neq 0\} = d$

■ This implies

$$(\mathbf{x} \in C \wedge |\mathbf{x}| < d) \Rightarrow \mathbf{x} = 0 \quad (1)$$

■  $C$  is a  $(n, n - r, d)$  code iff there is a  $n \times r$  matrix  $P_C$  of full rank such that

$$C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}P_C^T = 0\} \quad (2)$$

■  $P_C$  is called *parity check* matrix for code  $C$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES

# ERROR CORRECTION

- Alice encoded  $\mathbf{i} \in \{0, 1\}^{2n}$ , Bob measured  $\mathbf{j} \in \{0, 1\}^{2n}$
- Alice announced publicly  $\mathbf{s}$ ; let  $\mathbf{x} = \mathbf{i}P_{\mathbf{s}}^T$ ,  $\mathbf{y} = \mathbf{j}P_{\mathbf{s}}^T$
- The error is  $\mathbf{e} = \mathbf{y} - \mathbf{x}$
- We assume that  $2|\mathbf{e}| < d$  (less than  $d/2$  bit flips)
- Alice announces publicly  $P_C$  ( $n \times r$  bits) and  $\boldsymbol{\xi} = \mathbf{x}P_C^T$  ( $r$  bits)

$$2|\mathbf{e}| < d \quad (3)$$

$$\mathbf{e}P_C^T = (\mathbf{y} - \mathbf{x})P_C^T = \mathbf{y}P_C^T - \boldsymbol{\xi} \quad (4)$$

There is a unique solution  $\mathbf{e}$ . Proof: if  $\mathbf{e}$  and  $\mathbf{e}'$  were two solutions

$$(\mathbf{e} - \mathbf{e}')P_C^T = 0 \quad \text{by (4)}$$

$$\mathbf{e} - \mathbf{e}' \in C \quad \text{by (2)} \quad (5)$$

$$|\mathbf{e} - \mathbf{e}'| < d \quad \text{by (3) and } |\mathbf{e} - \mathbf{e}'| \leq |\mathbf{e}| + |\mathbf{e}'| < d \quad (6)$$

$$\mathbf{e} - \mathbf{e}' = 0 \quad \text{by (5), (6) and (1)}$$

- Bob finds  $\mathbf{e}$  and  $\mathbf{x} = \mathbf{y} + \mathbf{e}$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

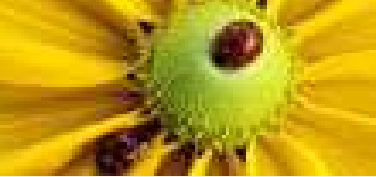
▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PRIVACY AMPLIFICATION

Problem:

- $\xi = \mathbf{x}P_C^T$  gives out  $r$  bits of information on  $\mathbf{x}$
- we want  $m$  secret bits ( $m =$  size of the key)
- how do we get them?

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PRIVACY AMPLIFICATION

Problem:

- $\xi = \mathbf{x}P_C^T$  gives out  $r$  bits of information on  $\mathbf{x}$
- we want  $m$  secret bits ( $m =$  size of the key)
- how do we get them?

Solution:

- let  $v_1, \dots, v_r$  be the (linearly independent) rows of  $P_C$
- extend this set to a basis  $v_1, \dots, v_n$  of  $\mathbf{F}_2^n$
- take  $P_K$  with rows  $v_{r+1}, \dots, v_{r+m}$
- $\kappa = \mathbf{x}P_K^T$  is a good key

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES





# PRIVACY AMPLIFICATION

Problem:

- $\xi = \mathbf{x}P_C^T$  gives out  $r$  bits of information on  $\mathbf{x}$
- we want  $m$  secret bits ( $m =$  size of the key)
- how do we get them?

Solution:

- let  $v_1, \dots, v_r$  be the (linearly independent) rows of  $P_C$
- extend this set to a basis  $v_1, \dots, v_n$  of  $\mathbf{F}_2^n$
- take  $P_K$  with rows  $v_{r+1}, \dots, v_{r+m}$
- $\kappa = \mathbf{x}P_K^T$  is a good key

Why?

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PRIVACY AMPLIFICATION

Problem:

- $\xi = \mathbf{x}P_C^T$  gives out  $r$  bits of information on  $\mathbf{x}$
- we want  $m$  secret bits ( $m =$  size of the key)
- how do we get them?

Solution:

- let  $v_1, \dots, v_r$  be the (linearly independent) rows of  $P_C$
- extend this set to a basis  $v_1, \dots, v_n$  of  $\mathbf{F}_2^n$
- take  $P_K$  with rows  $v_{r+1}, \dots, v_{r+m}$
- $\kappa = \mathbf{x}P_K^T$  is a good key

Why?

- choose  $m = n - r$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PRIVACY AMPLIFICATION

Problem:

- $\xi = \mathbf{x}P_C^T$  gives out  $r$  bits of information on  $\mathbf{x}$
- we want  $m$  secret bits ( $m =$  size of the key)
- how do we get them?

Solution:

- let  $v_1, \dots, v_r$  be the (linearly independent) rows of  $P_C$
- extend this set to a basis  $v_1, \dots, v_n$  of  $\mathbf{F}_2^n$
- take  $P_K$  with rows  $v_{r+1}, \dots, v_{r+m}$
- $\kappa = \mathbf{x}P_K^T$  is a good key

Why?

- choose  $m = n - r$
- $\mathbf{x} \rightarrow [\xi, \kappa]$  is an isomorphism between  $\mathbf{F}_2^n$  and  $\mathbf{F}_2^r \times \mathbf{F}_2^{n-r}$
- $\xi$  and  $\kappa$  are independent

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# PRIVACY AMPLIFICATION

Problem:

- $\xi = \mathbf{x}P_C^T$  gives out  $r$  bits of information on  $\mathbf{x}$
- we want  $m$  secret bits ( $m =$  size of the key)
- how do we get them?

Solution:

- let  $v_1, \dots, v_r$  be the (linearly independent) rows of  $P_C$
- extend this set to a basis  $v_1, \dots, v_n$  of  $\mathbf{F}_2^n$
- take  $P_K$  with rows  $v_{r+1}, \dots, v_{r+m}$
- $\kappa = \mathbf{x}P_K^T$  is a good key

Why?

- choose  $m = n - r$
- $\mathbf{x} \rightarrow [\xi, \kappa]$  is an isomorphism between  $\mathbf{F}_2^n$  and  $\mathbf{F}_2^r \times \mathbf{F}_2^{n-r}$
- $\xi$  and  $\kappa$  are independent

$P_K$  is called *privacy amplification* matrix.

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

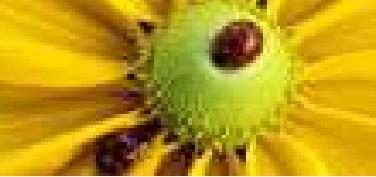
▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



# BB84 WITH CODES

We assume  $0 < p_a < 1$  (maximum error rate) fixed in advance.  
Announce = tell on a public secure channel

1. Alice randomly selects  $\mathbf{i}, \mathbf{b} \in \mathbb{F}_2^{2n}$  and sends Bob  $H^{\mathbf{b}} |\mathbf{i}\rangle$
2. Bob keeps them in quantum memory and announces when he has them all
3. Alice randomly chooses  $\mathbf{s} \in \mathbb{F}_2^{2n}$  such that  $|\mathbf{s}| = n$  and announces  $\mathbf{b}, \mathbf{s}, \mathbf{i}_{\overline{\mathbf{s}}} = \mathbf{i}P_{\overline{\mathbf{s}}}^T$ .
4. Bob applies  $H^{\mathbf{b}}$  to his state and measures, getting<sup>a</sup>  $\mathbf{j} \in \mathbb{F}_2^{2n}$ .
5. If  $|\mathbf{i}_{\overline{\mathbf{s}}} + \mathbf{j}_{\overline{\mathbf{s}}}| > np_a$  (unacceptable error rate) the protocol aborts.
6. Alice announces  $P_C, P_K$  and  $\xi$  (where  $\xi = \mathbf{x}P_C^T$  and  $\mathbf{x} = \mathbf{i}P_{\mathbf{s}}^T$ )
7. Bob uses  $\xi$  to recover  $\mathbf{x}$  and get the key  $\kappa = \mathbf{x}P_K^T$

---

<sup>a</sup>To simplify our proof, Bob also announces  $\mathbf{j}_{\overline{\mathbf{s}}} = \mathbf{j}P_{\overline{\mathbf{s}}}^T$ .

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

▶ BITSTRINGS AS VECTORS

▶ BINARY CODES

▶ ERROR CORRECTION

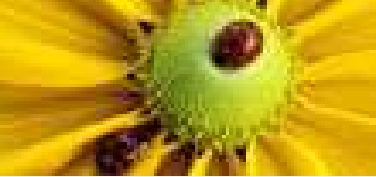
▶ PRIVACY AMPLIFICATION

▶ BB84 WITH CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

REFERENCES



**SYMMETRIC KEY CRYPTO**

---

**THE BB84 PROTOCOL**

---

**CODES**

---

**EVE'S ATTACK**

- PROBING
- PARTIAL TRACES
- EVE'S STATES
- MEASUREMENTS
- MUTUAL INFORMATION
- ACCESSIBLE INFORMATION
- CASE  $|K| = 2$

**INFO VS. DISTURBANCE**

---

**REFERENCES**

---

# EVE'S ATTACK

# PROBING

- Probing a quantum state  $|\phi\rangle \in \mathcal{H}$  is
  - ◆ attaching it an *ancilla*  $|a\rangle \in \mathcal{H}'$  to get  $|\phi\rangle \otimes |a\rangle$
  - ◆ applying a unitary  $A$  to  $|\phi\rangle \otimes |a\rangle \in \mathcal{H} \otimes \mathcal{H}'$
  - ◆ letting go the subsystem in  $\mathcal{H}$
  - ◆ keeping the subsystem in  $\mathcal{H}'$  for further measurement
- A *collective* attack probes qubits independently.
- In a *joint* or *general* attack,  $H^b |i\rangle$  is probed globally

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# PARTIAL TRACES

If  $\rho$  is a state on a bipartite system AB and

$$\rho = \sum_{i,j} \rho_i^A \otimes \rho_j^B$$

then the state induced on A and on B are respectively

$$\rho^A = \sum_{i,j} \text{tr} [\rho_j^B] \rho_i^A \quad \rho^B = \sum_{i,j} \text{tr} [\rho_i^A] \rho_j^B$$

When given state  $|\Psi\rangle$  we take  $\rho = |\Psi\rangle\langle\Psi|$ .

$$\text{Note: } \text{tr} [|\phi\rangle\langle\psi|] = \langle\psi | \phi\rangle.$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES





# EVE'S STATES

- Let  $|\mathbf{i}^b\rangle = H^b |\mathbf{i}\rangle$ ,  $|\mathbf{j}^b\rangle = H^b |\mathbf{j}\rangle$  and  $A$  be Eve's attack

$$A|0^E\rangle |\mathbf{i}^b\rangle = \sum_{\mathbf{j}} |E_{\mathbf{i},\mathbf{j}}^b\rangle |\mathbf{j}^b\rangle$$

- Given  $\mathbf{b}$  and  $\mathbf{s}$ , when Eve learns  $\mathbf{i}_{\bar{\mathbf{s}}}$ ,  $\mathbf{j}_{\bar{\mathbf{s}}}$ , and  $\xi$ , she is left with  $2^m$  non normalized operators

$$\rho_{\kappa} = \sum_{\mathbf{i},\mathbf{j}} |E_{\mathbf{i},\mathbf{j}}^b\rangle \langle E_{\mathbf{i},\mathbf{j}}^b|$$

where the sum is over the  $\mathbf{i}$ ,  $\mathbf{j}$  such that

- ◆  $\mathbf{i}_{\bar{\mathbf{s}}}$ ,  $\mathbf{j}_{\bar{\mathbf{s}}}$  are equal resp. to Eve's and Bob's test bits
- ◆  $\mathbf{i}_{\mathbf{s}} P_C^T = \xi$
- ◆  $\mathbf{i}_{\mathbf{s}} P_K^T = \kappa$

- She now measures to optimize her information on  $\kappa$ .

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

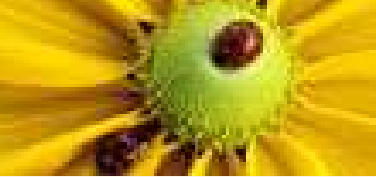
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# MEASUREMENTS

## General procedure to measure

**SYMMETRIC KEY CRYPTO**

---

**THE BB84 PROTOCOL**

---

**CODES**

---

**EVE'S ATTACK**

---

‣ **PROBING**

‣ **PARTIAL TRACES**

‣ **EVE'S STATES**

‣ **MEASUREMENTS**

‣ **MUTUAL INFORMATION**

‣ **ACCESSIBLE INFORMATION**

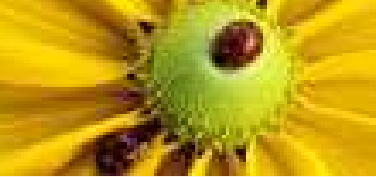
‣ **CASE  $|K| = 2$**

**INFO VS. DISTURBANCE**

---

**REFERENCES**

---



# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

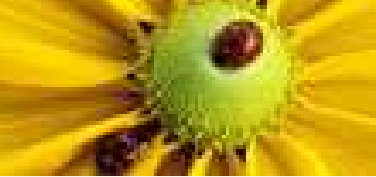
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

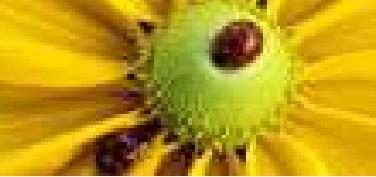
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_{m'}^\dagger$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▸ PROBING

▸ PARTIAL TRACES

▸ EVE'S STATES

▸ MEASUREMENTS

▸ MUTUAL INFORMATION

▸ ACCESSIBLE INFORMATION

▸ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_{m'}^\dagger$ 
  - ◆ measure the ancilla

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_m^\dagger$ 
  - ◆ measure the ancilla
  - ◆ get  $m$  with probability  $p(m | \rho) = \text{tr}[A_m \rho A_m^\dagger]$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_m^\dagger$ 
  - ◆ measure the ancilla
  - ◆ get  $m$  with probability  $p(m|\rho) = \text{tr}[A_m \rho A_m^\dagger]$
  - ◆ resulting state  $\frac{A_m \rho A_m^\dagger}{p(m|\rho)}$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

◆ PROBING

◆ PARTIAL TRACES

◆ EVE'S STATES

◆ MEASUREMENTS

◆ MUTUAL INFORMATION

◆ ACCESSIBLE INFORMATION

◆ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_m^\dagger$ 
  - ◆ measure the ancilla
  - ◆ get  $m$  with probability  $p(m|\rho) = \text{tr}[A_m \rho A_m^\dagger]$
  - ◆ resulting state  $\frac{A_m \rho A_m^\dagger}{p(m|\rho)}$
- Let  $O_m = A_m^\dagger A_m$  then

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

◆ PROBING

◆ PARTIAL TRACES

◆ EVE'S STATES

◆ MEASUREMENTS

◆ MUTUAL INFORMATION

◆ ACCESSIBLE INFORMATION

◆ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_m^\dagger$ 
  - ◆ measure the ancilla
  - ◆ get  $m$  with probability  $p(m|\rho) = \text{tr}[A_m \rho A_m^\dagger]$
  - ◆ resulting state  $\frac{A_m \rho A_m^\dagger}{p(m|\rho)}$
- Let  $O_m = A_m^\dagger A_m$  then
  - ◆  $O_m$  is hermitian positive,  $\sum_m O_m = I$  (POVM condition)

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

◆ PROBING

◆ PARTIAL TRACES

◆ EVE'S STATES

◆ MEASUREMENTS

◆ MUTUAL INFORMATION

◆ ACCESSIBLE INFORMATION

◆ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# MEASUREMENTS

## General procedure to measure

- given  $|\phi\rangle$  attach an ancilla to get  $|0\rangle|\phi\rangle$
- apply a unitary transform  $A$

$$A|0\rangle|\phi\rangle = \sum_m |m\rangle \otimes A_m |\phi\rangle$$

- A unitary translates as  $\sum_m A_m^\dagger A_m = I$
- For a density operator:  $|0\rangle\langle 0| \otimes \rho \mapsto \sum_{mm'} |m\rangle\langle m'| \otimes A_m \rho A_m^\dagger$ 
  - ◆ measure the ancilla
  - ◆ get  $m$  with probability  $p(m | \rho) = \text{tr}[A_m \rho A_m^\dagger]$
  - ◆ resulting state  $\frac{A_m \rho A_m^\dagger}{p(m | \rho)}$
- Let  $O_m = A_m^\dagger A_m$  then
  - ◆  $O_m$  is hermitian positive,  $\sum_m O_m = I$  (POVM condition)
  - ◆  $p[m | \rho] = \text{tr}[A_m \rho A_m^\dagger] = \text{tr}[A_m^\dagger A_m \rho] = \text{tr}[O_m \rho]$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

◆ PROBING

◆ PARTIAL TRACES

◆ EVE'S STATES

◆ MEASUREMENTS

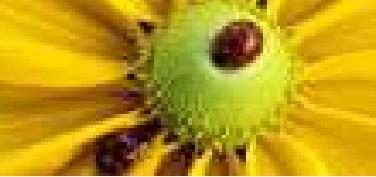
◆ MUTUAL INFORMATION

◆ ACCESSIBLE INFORMATION

◆ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# MUTUAL INFORMATION

Given random variables  $X, Y$ ,  $p(x) = P[X = x]$ ,  $p(y) = P[Y = y]$ ,  $p(x, y) = P[X = x, Y = y]$ , and  $\lg = \log_2$ , their **mutual information** is

$$I(X; Y) = \sum_{x, y} p(x, y) \lg \left( \frac{p(x, y)}{p(x)p(y)} \right)$$

- $I(X; Y) = 0$  if and only if  $X$  and  $Y$  are independent
- $I(X; Y) = 0$  if knowing  $X$  reveals nothing about  $Y$
- $I(X; Y) = H(X) + H(Y) - H(X, Y) \geq 0$
- $I(X; X) = H(X)$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

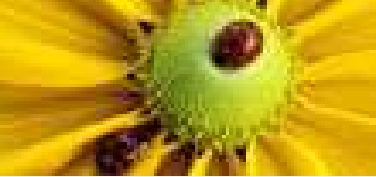
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# ACCESSIBLE INFORMATION

- Input:  $\rho_{\kappa}$  with probability  $p_{\kappa}$  with  $\kappa \in K$
- Problem: guess  $\kappa$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# ACCESSIBLE INFORMATION

- Input:  $\rho_{\mathbf{k}}$  with probability  $p_{\mathbf{k}}$  with  $\mathbf{k} \in K$
- Problem: guess  $\mathbf{k}$
  
- If  $\rho_{\mathbf{k}}$  are  $d \times d$  matrices let  $E$  be a set with  $d^2$  elements

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# ACCESSIBLE INFORMATION

- Input:  $\rho_{\mathbf{k}}$  with probability  $p_{\mathbf{k}}$  with  $\mathbf{k} \in K$
- Problem: guess  $\mathbf{k}$
- If  $\rho_{\mathbf{k}}$  are  $d \times d$  matrices let  $E$  be a set with  $d^2$  elements
  - ◆ if  $\mathcal{O} = (O_e)_{e \in E}$  is a POVM

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



# ACCESSIBLE INFORMATION

- Input:  $\rho_{\mathbf{\kappa}}$  with probability  $p_{\mathbf{\kappa}}$  with  $\mathbf{\kappa} \in K$
- Problem: guess  $\mathbf{\kappa}$
  
- If  $\rho_{\mathbf{\kappa}}$  are  $d \times d$  matrices let  $E$  be a set with  $d^2$  elements
  - ◆ if  $\mathcal{O} = (O_e)_{e \in E}$  is a POVM
  - ◆ then  $p_{\mathcal{O}}(e | \mathbf{\kappa}) = \text{tr}[O_e \rho_{\mathbf{\kappa}}]$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# ACCESSIBLE INFORMATION

- Input:  $\rho_{\mathbf{k}}$  with probability  $p_{\mathbf{k}}$  with  $\mathbf{k} \in K$
- Problem: guess  $\mathbf{k}$
  
- If  $\rho_{\mathbf{k}}$  are  $d \times d$  matrices let  $E$  be a set with  $d^2$  elements
  - ◆ if  $\mathcal{O} = (O_e)_{e \in E}$  is a POVM
  - ◆ then  $p_{\mathcal{O}}(e | \mathbf{k}) = \text{tr}[O_e \rho_{\mathbf{k}}]$
  - ◆  $p_{\mathcal{O}}(e, \mathbf{k}) = p_{\mathcal{O}}(e | \mathbf{k}) p(\mathbf{k})$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# ACCESSIBLE INFORMATION

- Input:  $\rho_{\mathbf{\kappa}}$  with probability  $p_{\mathbf{\kappa}}$  with  $\mathbf{\kappa} \in K$
- Problem: guess  $\mathbf{\kappa}$
  
- If  $\rho_{\mathbf{\kappa}}$  are  $d \times d$  matrices let  $E$  be a set with  $d^2$  elements
  - ◆ if  $\mathcal{O} = (O_e)_{e \in E}$  is a POVM
  - ◆ then  $p_{\mathcal{O}}(e | \mathbf{\kappa}) = \text{tr}[O_e \rho_{\mathbf{\kappa}}]$
  - ◆  $p_{\mathcal{O}}(e, \mathbf{\kappa}) = p_{\mathcal{O}}(e | \mathbf{\kappa}) p(\mathbf{\kappa})$
  - ◆  $I_{\mathcal{O}}(K; E)$  measures how much info on  $K$  the outputs in  $E$  give

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

# ACCESSIBLE INFORMATION

- Input:  $\rho_{\mathbf{k}}$  with probability  $p_{\mathbf{k}}$  with  $\mathbf{k} \in K$
- Problem: guess  $\mathbf{k}$
- If  $\rho_{\mathbf{k}}$  are  $d \times d$  matrices let  $E$  be a set with  $d^2$  elements
  - ◆ if  $\mathcal{O} = (O_e)_{e \in E}$  is a POVM
  - ◆ then  $p_{\mathcal{O}}(e | \mathbf{k}) = \text{tr}[O_e \rho_{\mathbf{k}}]$
  - ◆  $p_{\mathcal{O}}(e, \mathbf{k}) = p_{\mathcal{O}}(e | \mathbf{k}) p(\mathbf{k})$
  - ◆  $I_{\mathcal{O}}(K; E)$  measures how much info on  $K$  the outputs in  $E$  give
- ***accessible information*** on  $\mathbf{k} = \max_{\mathcal{O}} I_{\mathcal{O}}(K; E)$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



## CASE $|K| = 2$

**Theorem.** *If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM*

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

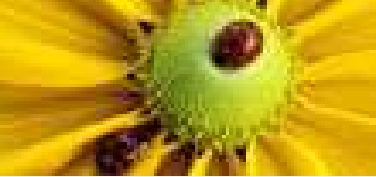
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$I_{\mathcal{O}}(K; E) = H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e)$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

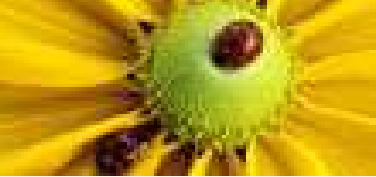
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\ &\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

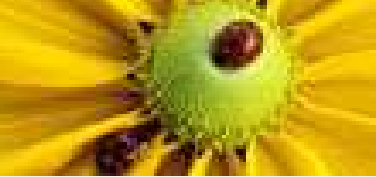
▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES





## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\ &\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

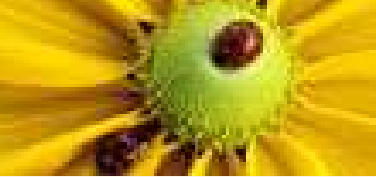
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned}
I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\
&= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\
&\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \\
&= \frac{1}{2} \sum_e |\text{tr}[O_e(\rho_0 - \rho_1)]|
\end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

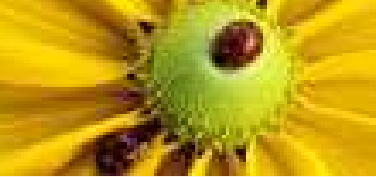
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned}
I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\
&= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\
&\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \\
&= \frac{1}{2} \sum_e |\text{tr}[O_e(\rho_0 - \rho_1)]| = \frac{1}{2} \sum_e \left| \text{tr} \left[ O_e \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| \right] \right|
\end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\ &\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \\ &= \frac{1}{2} \sum_e |\text{tr} [O_e(\rho_0 - \rho_1)]| = \frac{1}{2} \sum_e \left| \text{tr} \left[ O_e \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| \right] \right| \\ &= \frac{1}{2} \sum_e \left| \sum_i \lambda_i \text{tr} [\langle\phi_i| O_e |\phi_i\rangle] \right| \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\ &\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \\ &= \frac{1}{2} \sum_e |\text{tr} [O_e(\rho_0 - \rho_1)]| = \frac{1}{2} \sum_e \left| \text{tr} \left[ O_e \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| \right] \right| \\ &= \frac{1}{2} \sum_e \left| \sum_i \lambda_i \text{tr} [\langle\phi_i| O_e |\phi_i\rangle] \right| \\ &\leq \frac{1}{2} \sum_{i,e} |\lambda_i| \langle\phi_i| O_e |\phi_i\rangle \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\ &\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \\ &= \frac{1}{2} \sum_e |\text{tr} [O_e(\rho_0 - \rho_1)]| = \frac{1}{2} \sum_e \left| \text{tr} \left[ O_e \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| \right] \right| \\ &= \frac{1}{2} \sum_e \left| \sum_i \lambda_i \text{tr} [\langle\phi_i| O_e |\phi_i\rangle] \right| \\ &\leq \frac{1}{2} \sum_{i,e} |\lambda_i| \langle\phi_i| O_e |\phi_i\rangle = \frac{1}{2} \sum_i |\lambda_i| \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES

## CASE $|K| = 2$

**Theorem.** If  $\hat{\rho}_0$  and  $\hat{\rho}_1$  are equally likely and  $\mathcal{O}$  is any POVM

$$I_{\mathcal{O}}(K; E) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad (7)$$

**Proof.** Let  $\hat{\rho}_0 - \hat{\rho}_1 = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ ; note:  $1 - H(p, q) \leq |p - q|$ .

$$\begin{aligned} I_{\mathcal{O}}(K; E) &= H(K) - H_{\mathcal{O}}(K | E) = 1 - \sum_e H_{\mathcal{O}}(K | e) p_{\mathcal{O}}(e) \\ &= \sum_e [1 - H(p_{\mathcal{O}}(\mathbf{k} = 0 | e), p_{\mathcal{O}}(\mathbf{k} = 1 | e))] p_{\mathcal{O}}(e) \\ &\leq \sum_e |p_{\mathcal{O}}(\mathbf{k} = 0 | e) - p_{\mathcal{O}}(\mathbf{k} = 1 | e)| p_{\mathcal{O}}(e) = \sum_e |p_{\mathcal{O}}(0, e) - p_{\mathcal{O}}(1, e)| \\ &= \frac{1}{2} \sum_e |\text{tr} [O_e(\rho_0 - \rho_1)]| = \frac{1}{2} \sum_e \left| \text{tr} \left[ O_e \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| \right] \right| \\ &= \frac{1}{2} \sum_e \left| \sum_i \lambda_i \text{tr} [\langle\phi_i| O_e |\phi_i\rangle] \right| \\ &\leq \frac{1}{2} \sum_{i,e} |\lambda_i| \langle\phi_i| O_e |\phi_i\rangle = \frac{1}{2} \sum_i |\lambda_i| = \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \quad \square \end{aligned}$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

▶ PROBING

▶ PARTIAL TRACES

▶ EVE'S STATES

▶ MEASUREMENTS

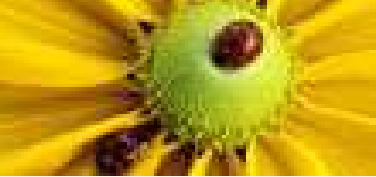
▶ MUTUAL INFORMATION

▶ ACCESSIBLE INFORMATION

▶ CASE  $|K| = 2$

INFO VS. DISTURBANCE

REFERENCES



**SYMMETRIC KEY CRYPTO**

**THE BB84 PROTOCOL**

**CODES**

**EVE'S ATTACK**

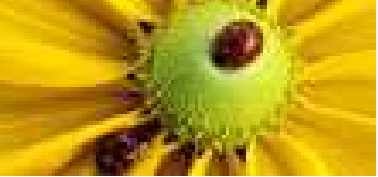
**INFO VS. DISTURBANCE**

- **ATTACKING ONE QBIT**
- **EVE'S INFORMATION**
- **METHOD**
- **THE BIHAM BASIS**
- **THE BOUND**
- **HOEFFDING'S THEOREM**
- **SECURE CODES**

**REFERENCES**

# INFO VS. DISTURBANCE





# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_{\bar{e}}^b = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

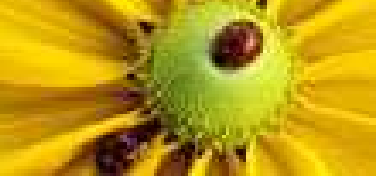
$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_{\bar{e}}^b = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E [ |\psi_0\rangle\langle\psi_0| ]$

If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E [ |\psi_1\rangle\langle\psi_1| ]$ .



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_{\bar{e}}^b = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E [ |\psi_0\rangle\langle\psi_0| ]$

If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E [ |\psi_1\rangle\langle\psi_1| ]$ .

Take  $\theta$  s.t.  $\langle\psi_0 | \psi_1\rangle = \cos(2\alpha) \in \mathbf{R}_+$ .



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_{\bar{e}}^b = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E[|\psi_0\rangle\langle\psi_0|]$

If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E[|\psi_1\rangle\langle\psi_1|]$ .

Take  $\theta$  s.t.  $\langle\psi_0 | \psi_1\rangle = \cos(2\alpha) \in \mathbf{R}_+$ .  $1 - 2p_{\bar{e}}^b \leq \cos(2\alpha) = 1 - 2\sin^2(\alpha)$



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

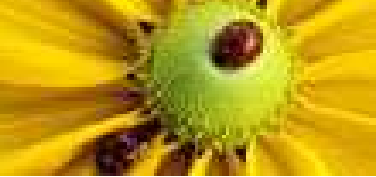
$$p_e^{\bar{b}} = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E [ |\psi_0\rangle\langle\psi_0| ]$

If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E [ |\psi_1\rangle\langle\psi_1| ]$ .

Take  $\theta$  s.t.  $\langle\psi_0 | \psi_1\rangle = \cos(2\alpha) \in \mathbf{R}_+$ .  $1 - 2p_e^{\bar{b}} \leq \cos(2\alpha) = 1 - 2\sin^2(\alpha)$

$$\boxed{\sin(\alpha) \leq \sqrt{p_e^{\bar{b}}}}$$



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_{\bar{e}}^b = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E [ |\psi_0\rangle\langle\psi_0| ]$

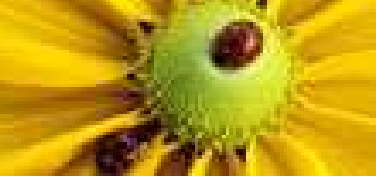
If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E [ |\psi_1\rangle\langle\psi_1| ]$ .

Take  $\theta$  s.t.  $\langle\psi_0 | \psi_1\rangle = \cos(2\alpha) \in \mathbf{R}_+$ .  $1 - 2p_e^{\bar{b}} \leq \cos(2\alpha) = 1 - 2\sin^2(\alpha)$

$$\boxed{\sin(\alpha) \leq \sqrt{p_e^{\bar{b}}}}$$

Let  $|\psi_0\rangle = \cos(\alpha) |0'\rangle + \sin(\alpha) |1'\rangle$ ,  $|\psi_1\rangle = \cos(\alpha) |0'\rangle - \sin(\alpha) |1'\rangle$





# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_e^{\bar{b}} = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E[|\psi_0\rangle\langle\psi_0|]$

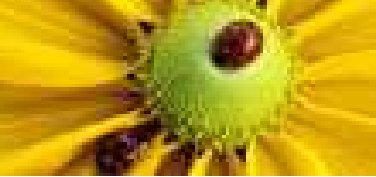
If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E[|\psi_1\rangle\langle\psi_1|]$ .

Take  $\theta$  s.t.  $\langle\psi_0 | \psi_1\rangle = \cos(2\alpha) \in \mathbf{R}_+$ .  $1 - 2p_e^{\bar{b}} \leq \cos(2\alpha) = 1 - 2\sin^2(\alpha)$

$\sin(\alpha) \leq \sqrt{p_e^{\bar{b}}}$

Let  $|\psi_0\rangle = \cos(\alpha) |0'\rangle + \sin(\alpha) |1'\rangle$ ,  $|\psi_1\rangle = \cos(\alpha) |0'\rangle - \sin(\alpha) |1'\rangle$

$$SD(\rho_0, \rho_1) \leq SD(\psi_0, \psi_1) \leq \frac{1}{2} \left| |\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1| \right| = \cos(\alpha) \sin(\alpha) \left| |0'\rangle\langle 1'| + |1'\rangle\langle 0'| \right|$$



# ATTACKING ONE QBIT

$$U |0^E\rangle |0^b\rangle = |E_{00}^b\rangle |0^b\rangle + |E_{01}^b\rangle |1^b\rangle = |\Phi_0^b\rangle$$

$$U |0^E\rangle |1^b\rangle = |E_{10}^b\rangle |0^b\rangle + |E_{11}^b\rangle |1^b\rangle$$

$$\rho_0^b = |E_{00}^b\rangle\langle E_{00}^b| + |E_{01}^b\rangle\langle E_{01}^b|$$

$$\rho_1^b = |E_{10}^b\rangle\langle E_{10}^b| + |E_{11}^b\rangle\langle E_{11}^b|$$

$$p_e^b = \langle E_{01}^b | E_{01}^b \rangle \frac{1}{2} + \langle E_{10}^b | E_{10}^b \rangle \frac{1}{2}$$

$$p_e^{\bar{b}} = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{01}^b \rangle \right) \right]$$

If we let  $|\psi_0\rangle = |E_{00}^b\rangle |0\rangle + |E_{01}^b\rangle |1\rangle$  then  $\rho_0 = \text{tr}_E[|\psi_0\rangle\langle\psi_0|]$

If we let  $|\psi_1\rangle = e^{i\theta} |E_{11}^b\rangle |0\rangle + e^{i\theta} |E_{10}^b\rangle |1\rangle$  then  $\rho_1 = \text{tr}_E[|\psi_1\rangle\langle\psi_1|]$ .

Take  $\theta$  s.t.  $\langle\psi_0 | \psi_1\rangle = \cos(2\alpha) \in \mathbf{R}_+$ .  $1 - 2p_e^{\bar{b}} \leq \cos(2\alpha) = 1 - 2\sin^2(\alpha)$

$$\boxed{\sin(\alpha) \leq \sqrt{p_e^{\bar{b}}}}$$

Let  $|\psi_0\rangle = \cos(\alpha) |0'\rangle + \sin(\alpha) |1'\rangle$ ,  $|\psi_1\rangle = \cos(\alpha) |0'\rangle - \sin(\alpha) |1'\rangle$

$$SD(\rho_0, \rho_1) \leq SD(\psi_0, \psi_1) \leq \frac{1}{2} \left| |\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1| \right| = \cos(\alpha) \sin(\alpha) \left| |0'\rangle\langle 1'| + |1'\rangle\langle 0'| \right|$$

$$\boxed{SD(\rho_0, \rho_1) \leq 2\sqrt{p_e^{\bar{b}}}}$$

# EVE'S INFORMATION

- We want a similar result for Eve's information on  $\kappa$  for BB84 with codes.
- If Eve keeps the state sent by Alice and sends random info to Bob, she gets full information whenever the test passes.
- To average Eve's information, we need to take into account when the test fails
- For each  $\mathbf{b}, \mathbf{s}, \mathbf{i}_{\bar{\mathbf{s}}}, \mathbf{j}_{\bar{\mathbf{s}}}, \xi$  there is an accessible information from the  $(\rho_{\kappa})_{\kappa \in K}$ ; we denote it  $I(K; E | \mathbf{b}, \mathbf{s}, \mathbf{i}_{\bar{\mathbf{s}}}, \mathbf{j}_{\bar{\mathbf{s}}}, \xi)$
- Let

$$I_{(p_a)}(K; E | \mathbf{b}, \mathbf{s}, \xi, \mathbf{i}_{\bar{\mathbf{s}}}, \mathbf{j}_{\bar{\mathbf{s}}}) = \begin{cases} I(K; E | \mathbf{b}, \mathbf{s}, \xi, \mathbf{i}_{\bar{\mathbf{s}}}, \mathbf{j}_{\bar{\mathbf{s}}}) & \text{if } \frac{|\mathbf{i}_{\bar{\mathbf{s}}} + \mathbf{j}_{\bar{\mathbf{s}}}|}{n} \leq p_a \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

- Eve's information  $\langle I_{\text{Eve}}^{(p_a)} \rangle$  is the expectancy of  $I_{(p_a)}$  over all the parameters  $\mathbf{b}, \mathbf{s}, \xi, \mathbf{i}_{\bar{\mathbf{s}}}, \mathbf{j}_{\bar{\mathbf{s}}}$ .
- $\langle I_{\text{Eve}}^{(p_a)} \rangle$  is what is bounded in [BBBMR].

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES

# METHOD

- Use  $I((K_1, \dots, K_m); E | \xi \dots) \leq \sum_{j=1}^m I(K_j; E | K_1, \dots, K_{j-1}, \xi \dots)$
- Establish a bound for  $I(K_j; E | k_1, \dots, k_{j-1}, \xi, \dots)$
- i.e for  $I(K_j; E | \xi', \dots)$  with  $\xi' = \xi k_1 \dots k_{j-1}$  a  $r + j - 1$  bit syndrome for the code having parity matrix with lines  $v_1, \dots, v_{r+j-1}$ .
- The problem has been reduced to 1-bit keys. Eve's non normalized operators are

$$\rho_k = \sum_{\mathbf{i}, \mathbf{j}} |E_{\mathbf{i}, \mathbf{j}}^{\mathbf{b}}\rangle \langle E_{\mathbf{i}, \mathbf{j}}^{\mathbf{b}}|$$

where the sum is over the  $\mathbf{i}, \mathbf{j}$  such that

- ◆  $\mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}$  are equal resp. to Eve's and Bob's test bits
- ◆  $\mathbf{i}_s P_C^T = \xi$
- ◆  $\mathbf{i}_s \cdot v_{r+1} = k$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

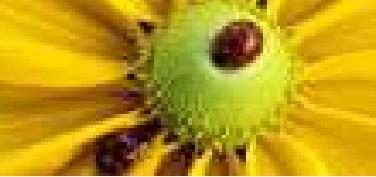
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $i_s, j_s, \mathbf{b}, \mathbf{s}, \xi$  be fixed.

## SYMMETRIC KEY CRYPTO

## THE BB84 PROTOCOL

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

### ▶ ATTACKING ONE QBIT

### ▶ EVE'S INFORMATION

### ▶ METHOD

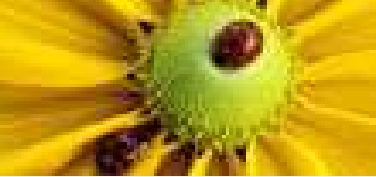
### ▶ THE BIHAM BASIS

### ▶ THE BOUND

### ▶ Hoeffding's THEOREM

### ▶ SECURE CODES

## REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbf{F}_2^n$

## SYMMETRIC KEY CRYPTO

## THE BB84 PROTOCOL

## CODES

## EVE'S ATTACK

## INFO VS. DISTURBANCE

### ▶ ATTACKING ONE QBIT

### ▶ EVE'S INFORMATION

### ▶ METHOD

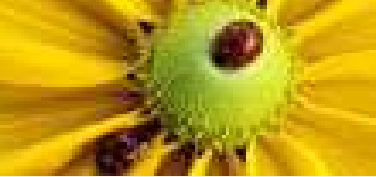
### ▶ THE BIHAM BASIS

### ▶ THE BOUND

### ▶ Hoeffding's THEOREM

### ▶ SECURE CODES

## REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

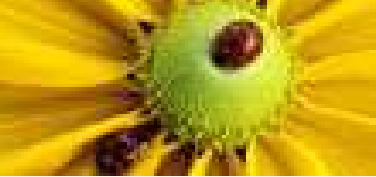
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_s, \mathbf{j}_s, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_s + \mathbf{j}_s$ .

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

▶ THE BIHAM BASIS

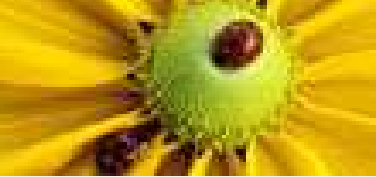
▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES





# THE BIHAM BASIS

- Let  $\mathbf{i}_s, \mathbf{j}_s, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_s + \mathbf{j}_s$ .
- Then there are vectors  $|\eta_{\mathbf{c}}\rangle$  ( $\mathbf{c} \in \{0, 1\}^n$ ) of Eve's probe space s.t.

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

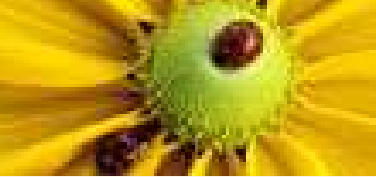
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_s, \mathbf{j}_s, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_s + \mathbf{j}_s$ .
- Then there are vectors  $|\eta_{\mathbf{c}}\rangle$  ( $\mathbf{c} \in \{0, 1\}^n$ ) of Eve's probe space s.t.
  - ◆  $|\eta_{\mathbf{c}}\rangle = |\eta_{\mathbf{c}'}\rangle$  if  $\mathbf{c} + \mathbf{c}' \in V_r$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

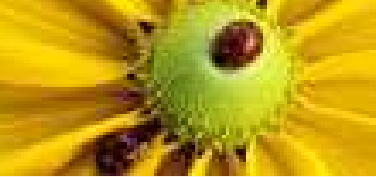
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_s, \mathbf{j}_s, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_s + \mathbf{j}_s$ .
- Then there are vectors  $|\eta_{\mathbf{c}}\rangle$  ( $\mathbf{c} \in \{0, 1\}^n$ ) of Eve's probe space s.t.
  - ◆  $|\eta_{\mathbf{c}}\rangle = |\eta_{\mathbf{c}'}\rangle$  if  $\mathbf{c} + \mathbf{c}' \in V_r$
  - ◆  $\langle \eta_{\mathbf{c}} | \eta_{\mathbf{c}'} \rangle = 0$  if  $\mathbf{c} + \mathbf{c}' \notin V_r$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} \mid E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} \mid E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_s + \mathbf{j}_s$ .
- Then there are vectors  $|\eta_{\mathbf{c}}\rangle$  ( $\mathbf{c} \in \{0, 1\}^n$ ) of Eve's probe space s.t.
  - ◆  $|\eta_{\mathbf{c}}\rangle = |\eta_{\mathbf{c}'}\rangle$  if  $\mathbf{c} + \mathbf{c}' \in V_r$
  - ◆  $\langle \eta_{\mathbf{c}} \mid \eta_{\mathbf{c}'} \rangle = 0$  if  $\mathbf{c} + \mathbf{c}' \notin V_r$
  - ◆  $\langle \eta_{\mathbf{c}} \mid \eta_{\mathbf{c}} \rangle = P[C_I \in \mathbf{c} + V_r, \mathbf{j}_{\bar{s}} \mid \mathbf{i}_{\bar{s}}, \mathbf{b} + \mathbf{s}, \mathbf{s}]$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

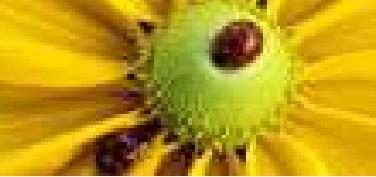
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_s + \mathbf{j}_s$ .
- Then there are vectors  $|\eta_{\mathbf{c}}\rangle$  ( $\mathbf{c} \in \{0, 1\}^n$ ) of Eve's probe space s.t.

- ◆  $|\eta_{\mathbf{c}}\rangle = |\eta_{\mathbf{c}'}\rangle$  if  $\mathbf{c} + \mathbf{c}' \in V_r$
- ◆  $\langle \eta_{\mathbf{c}} | \eta_{\mathbf{c}'} \rangle = 0$  if  $\mathbf{c} + \mathbf{c}' \notin V_r$
- ◆  $\langle \eta_{\mathbf{c}} | \eta_{\mathbf{c}} \rangle = P[C_I \in \mathbf{c} + V_r, \mathbf{j}_{\bar{s}} | \mathbf{i}_{\bar{s}}, \mathbf{b} + \mathbf{s}, \mathbf{s}]$
- ◆ If  $\tilde{\rho}_k = |V_{r+1}^\perp| \sum_{\mathbf{c}' \in V_r^c} \left\{ |\eta_{\mathbf{c}'}\rangle \langle \eta_{\mathbf{c}'}| + (-1)^k |\eta_{\mathbf{c}'}\rangle \langle \eta_{\mathbf{c}'+v_{r+1}}| \right\}$  then  
 $\text{tr}[\tilde{\rho}_k] = \rho_k.$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BIHAM BASIS

- Let  $\mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}, \mathbf{b}, \mathbf{s}, \xi$  be fixed.
- $V_r = \langle v_1, \dots, v_r \rangle$  and  $V_r^c = \langle v_{r+1}, \dots, v_n \rangle$  with  $v_1, \dots, v_n$  basis of  $\mathbb{F}_2^n$
- Let the attack be symmetric i.e.

$$\langle E_{\mathbf{i}+\mathbf{m}, \mathbf{j}+\mathbf{m}}^{\mathbf{b}} | E_{\mathbf{i}'+\mathbf{m}, \mathbf{j}'+\mathbf{m}}^{\mathbf{b}} \rangle = (-1)^{(\mathbf{i}+\mathbf{j}+\mathbf{i}'+\mathbf{j}') \cdot \mathbf{m}} \langle E_{\mathbf{i}\mathbf{j}}^{\mathbf{b}} | E_{\mathbf{i}'\mathbf{j}'}^{\mathbf{b}} \rangle$$

- Let  $C_I$  be the error random variable on information bits  $\mathbf{i}_{\bar{s}} + \mathbf{j}_{\bar{s}}$ .
- Then there are vectors  $|\eta_{\mathbf{c}}\rangle$  ( $\mathbf{c} \in \{0, 1\}^n$ ) of Eve's probe space s.t.

- ◆  $|\eta_{\mathbf{c}}\rangle = |\eta_{\mathbf{c}'}\rangle$  if  $\mathbf{c} + \mathbf{c}' \in V_r$
- ◆  $\langle \eta_{\mathbf{c}} | \eta_{\mathbf{c}'} \rangle = 0$  if  $\mathbf{c} + \mathbf{c}' \notin V_r$
- ◆  $\langle \eta_{\mathbf{c}} | \eta_{\mathbf{c}} \rangle = P[C_I \in \mathbf{c} + V_r, \mathbf{j}_{\bar{s}} | \mathbf{i}_{\bar{s}}, \mathbf{b} + \mathbf{s}, \mathbf{s}]$
- ◆ If  $\tilde{\rho}_k = |V_{r+1}^\perp| \sum_{\mathbf{c}' \in V_r^c} \left\{ |\eta_{\mathbf{c}'}\rangle \langle \eta_{\mathbf{c}'}| + (-1)^k |\eta_{\mathbf{c}'}\rangle \langle \eta_{\mathbf{c}'+v_{r+1}}| \right\}$  then

$$\text{tr}[\tilde{\rho}_k] = \rho_k.$$

- ◆  $\text{tr} |\tilde{\rho}_0 - \tilde{\rho}_1| \leq 2 \sqrt{P \left[ |C_I| \geq \frac{d_{r,1}}{2} \mid \mathbf{i}_{\bar{s}}, \mathbf{j}_{\bar{s}}, \mathbf{b} + \mathbf{s}, \mathbf{s} \right]}$

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

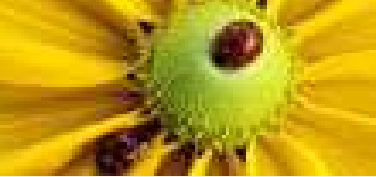
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# THE BOUND

**Theorem.** If  $v_1, \dots, v_r$  are the lines of  $P_C$ ,  $v_{r+1}, \dots, v_{r+m}$  those of  $P_K$ , and if  $d_{r,m} = d_H(\langle v_1, \dots, v_r \rangle, \langle v_{r+1}, \dots, v_{r+m} \rangle - \{0\})$  where  $d_H$  is the minimum Hamming distance between the two sets (spans) then

$$\langle I_{\text{Eve}}^{(p_a)} \rangle \leq 2m \sqrt{P \left[ \left( \frac{|C_I|}{n} \geq \frac{d_{r,m}}{2n} \right) \wedge \left( \frac{|C_T|}{n} \leq p_a \right) \right]} \quad (9)$$

where  $\frac{|C_T|}{n}$  is the error rate on test bits (determined by  $\bar{s}$ ) and  $\frac{|C_I|}{n}$  is the error rate on information bits (determined by  $s$ ).

**Proof.**

- Given by Biham bases for symmetric attacks.
- Reduction of general attacks to symmetric attacks [BBBMR]
- Direct proof for non symmetric collective attacks in [BGM].

□

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

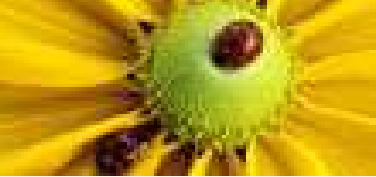
▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



# HOEFFDING'S THEOREM

**Theorem** (Hoeffding 1963). Let  $X_1, \dots, X_n$  be either

1. independent random variables with finite first and second moments such that  $a_i \leq X_i \leq b_i$  ( $1 \leq i \leq n$ )
2. or a random sample of size  $n$  without replacement taken from a population  $c_1, \dots, c_N$  s.t.  $a_i \leq c_i \leq b_i$  ( $1 \leq i \leq N$ )

let  $\bar{X} = (X_1 + \dots + X_n) / n$  and  $\mu = E[\bar{X}]$  be the expectancy of  $\bar{X}$  then for any  $\epsilon > 0$

$$\Pr \left[ \bar{X} - \mu \geq \epsilon \right] \leq e^{-2n^2\epsilon^2 / \sum_{i=1}^n (b_i - a_i)^2}$$

In the same way  $\Pr \left[ \mu - \bar{X} \geq \epsilon \right] \leq e^{-2n^2\epsilon^2 / \sum_{i=1}^n (b_i - a_i)^2}$ . In case (2),  $\mu$  is nothing else than the average of all the  $c_i$ . This theorem can be found in [Hoef63].

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

▶ THE BIHAM BASIS

▶ THE BOUND

▶ HOEFFDING'S THEOREM

▶ SECURE CODES

REFERENCES



# SECURE CODES

**Theorem.** Let us be given  $\delta > 0$ ,  $R > 0$  and, for infinitely many values of  $n$ , a family  $\{v_1^n, \dots, v_{r_n+m_n}^n\}$  of linearly independent vectors in  $\mathbb{F}_2^n$  such that  $\delta \leq \frac{d_{r_n, m_n}}{n}$  and  $\frac{m_n}{n} \leq R$ . Then for any  $p_a > 0$  and  $\epsilon_{\text{sec}} > 0$  such that  $p_a + \epsilon_{\text{sec}} \leq \frac{\delta}{2}$ , Eve's accessible information satisfies the following bound.

$$\langle I_{\text{Eve}}^{(p_a)} \rangle \leq 2R n e^{-\frac{\epsilon_{\text{sec}}^2}{4} n}$$

All we need to guarantee security is thus vectors  $\{v_1^n, \dots, v_{r_n+m_n}^n\}$  satisfying the conditions of the theorem. Such families were proven to exist in [BBBMR].

Codes providing both security and reliability are then proven to exist in [BBBMR].

SYMMETRIC KEY CRYPTO

THE BB84 PROTOCOL

CODES

EVE'S ATTACK

INFO VS. DISTURBANCE

▶ ATTACKING ONE QBIT

▶ EVE'S INFORMATION

▶ METHOD

▶ THE BIHAM BASIS

▶ THE BOUND

▶ Hoeffding's THEOREM

▶ SECURE CODES

REFERENCES



## REFERENCES

- [BBBGM] E. BIHAM, M. BOYER, G. BRASSARD, J. VAN DE GRAAF, AND T. MOR, *Security of quantum key distribution against all collective attacks*, *Algorithmica*, 34 (2002).
- [BBBMR] E. BIHAM, M. BOYER, P. O. BOYKIN, T. MOR AND V. ROYCHOWDHURY, *A proof of the security of quantum key distribution*, *Journal of Cryptology*, (2006).
- [BGM] M. BOYER, R. GELLES, AND T. MOR *Security of BB84 against collective attacks*, In preparation.
- [Hoef63] W. HOEFFDING, *Probability inequalities for sums of bounded random variables*, *J. Amer. Stat. Assoc.*, 58 (1963), pp. 13–20.