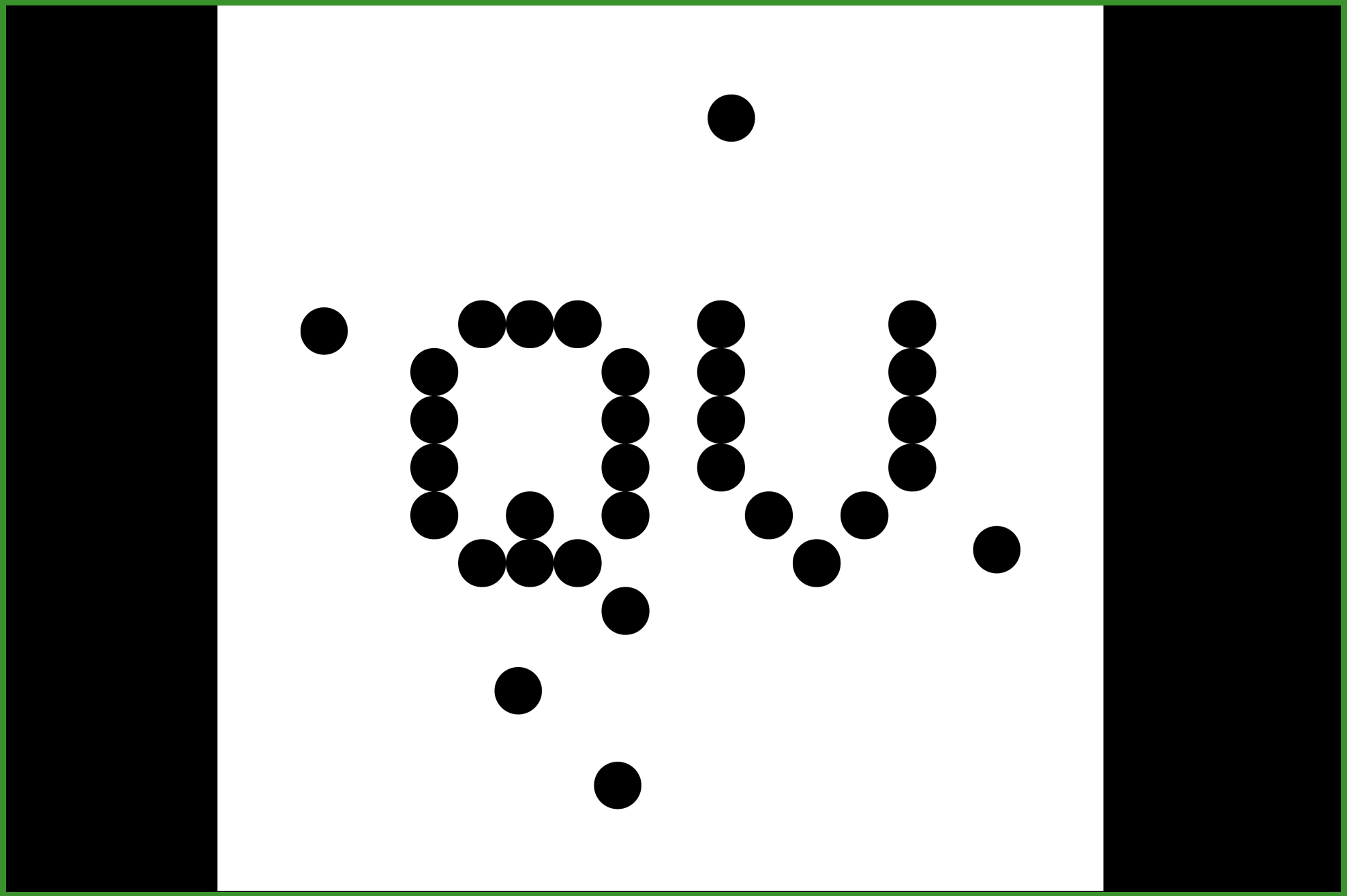
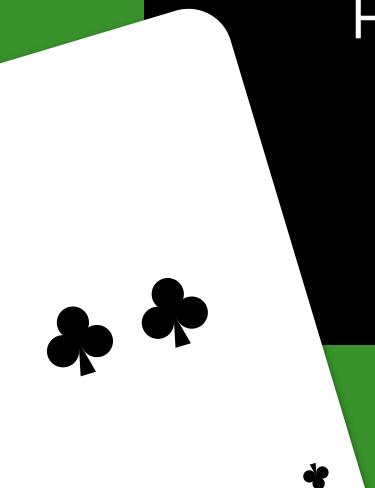


World's Cheapest QKD

How can I exchange a key



DEFCON 31 2023

Quality University of Business Information Technology presents

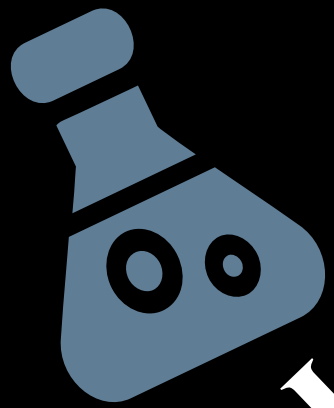
QKD for fun and non - profit from home

I can't do QKD!

I have no budget

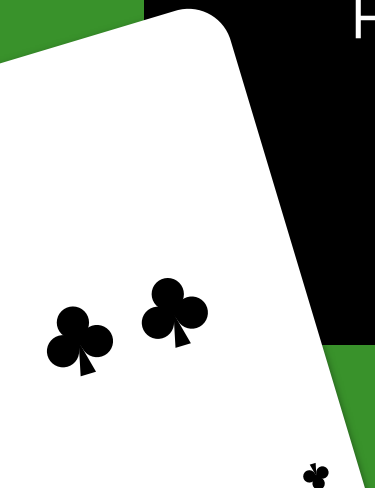
I have no LAB

I have no LASER



World's Cheapest QKD

How can I exchange a key

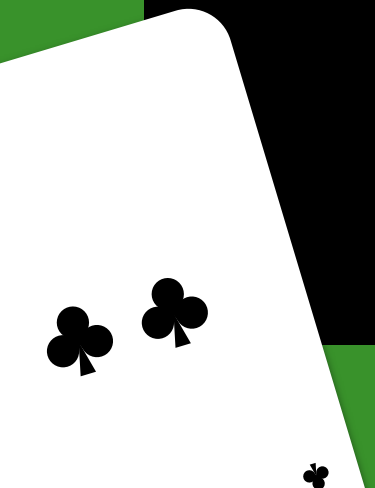


Quantum Kard Distribution

Chris Vasko, Mark Carney, Victoria Kumaran, Jose Pizarro, Ben Varcoe

01

Instructions




Take 2 sets of
Poker playing
Cards


Introduce
ALICE


Introduce
BOB

01 STEP

Alice and Bob

- Take a piece of paper
- A deck of cards each
- Shuffle
- Select a Basis to measure : RED or BLACK
- Measure

Horizontal bias : Measure 0

|0>

Vertical Bias : Measure 1

|1>

Define Basis

Look at Suit and Colour : Measure

Horizontal bias : Measure 0

|0> ♣ ♥

+

Vertical Bias : Measure 1

|1> ♦ ♠

×

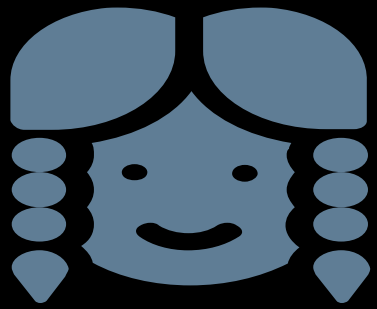
Player Sheet

BASIC BB84 BASIS KEY

|0> ♣ ♥ |1> ♦ ♠

	ALICE				EVE	BOB			X= BOB MATCH	Plain BB84 Key
	DECK		SUIT				SHOUTS			
ROUND	CARD			BASIS		BASIS				
1				---	0	---	MISS			**0**
2				---	0	---	MISS			**0**
3				---	0	---	MISS			**0**
4				---	0	---	MISS			**0**

02 Step Alice



- Take a piece of paper
- Pick a card
- Note down the suit
  - C Clubs
  - D Diamonds
  - H Hearts
  - S Spades
- Enter "X" in BOB Match Column when Bob Shouts Match Basis : RED or BLACK
- Note: 0 or 1 |0> |1>
- After hearing "Match" for 10 times
  → Shout "KEY" you have enough valid digits

|0> ♣ ♥

|1> ♦ ♠

03 Step BOB

- Take a piece of paper
- Pick a card : Note Colour
- Compare BOB Colour With Alice Colour CARD

2. When Bob card colour Matches Alice
   - Shout Match
   - Enter "X" in BOB Match Column

Basis : RED or BLACK

- Note: 0 or 1 |0> |1> based on ALICE Card
- When 10 Matches Shout "KEY" -> valid digits

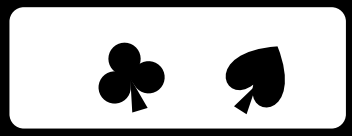
04 Step EVE

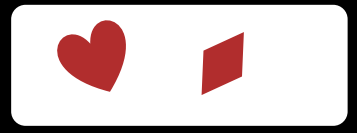
NEED INSTRUCTIONS ?
HACK IT ?

- Take a piece of paper

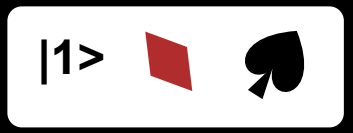
- Try recreate BoB key

- Listen to BOB
- Try and recreate the shared key
- CAN YOU SUCCEED? HOW and WHY?





ROUND 1 Example



	ALICE				EVE	BOB		X= BOB MATCH	Plain BB84 Key
	DECK	BLUE	SUIT			RED	SHOUTS		
ROUND	CARD			BASIS		BASIS			
1	♣	1	C	BLACK	0	BLACK	MATCH	x	0
2	♥	q	H	RED	---	---	MISS		---
3	♣	5	C	BLACK	0	BLACK	MATCH	X	0
4	♦	7	D	RED	---	---	MISS		---
5	♠	8	S	BLACK	1	BLACK	MATCH	X	1
6	♦	6	D	RED	---	---	MISS		---
7	♥	5	H	RED	0	RED	MATCH	X	0
8	♣	J	C	BLACK	---	---	MISS		---
9	♦	10	D	RED	1	RED	MATCH	x	1
10	♣	7	C	BLACK	---	---	MISS		---
11	♦	2	D	RED	---	---	MISS		---
12	♠	4	S	BLACK	1	BLACK	MATCH	x	1

BB84 Keys	
KEY PLAIN	00101111100010

REAL WORLD QKD DEMO

Using Excel sheet “QV Defcon 31 DEMO” and video link

|0>

|1>

Show back of deck only at start of video

What did WE do

- Exchanged a key
  Using a simplified BB84/BBM92 <- what's that ?
- Limitations
  Where is the QUANTUM??
- EVE has an easy job

- Can we add Quantum?

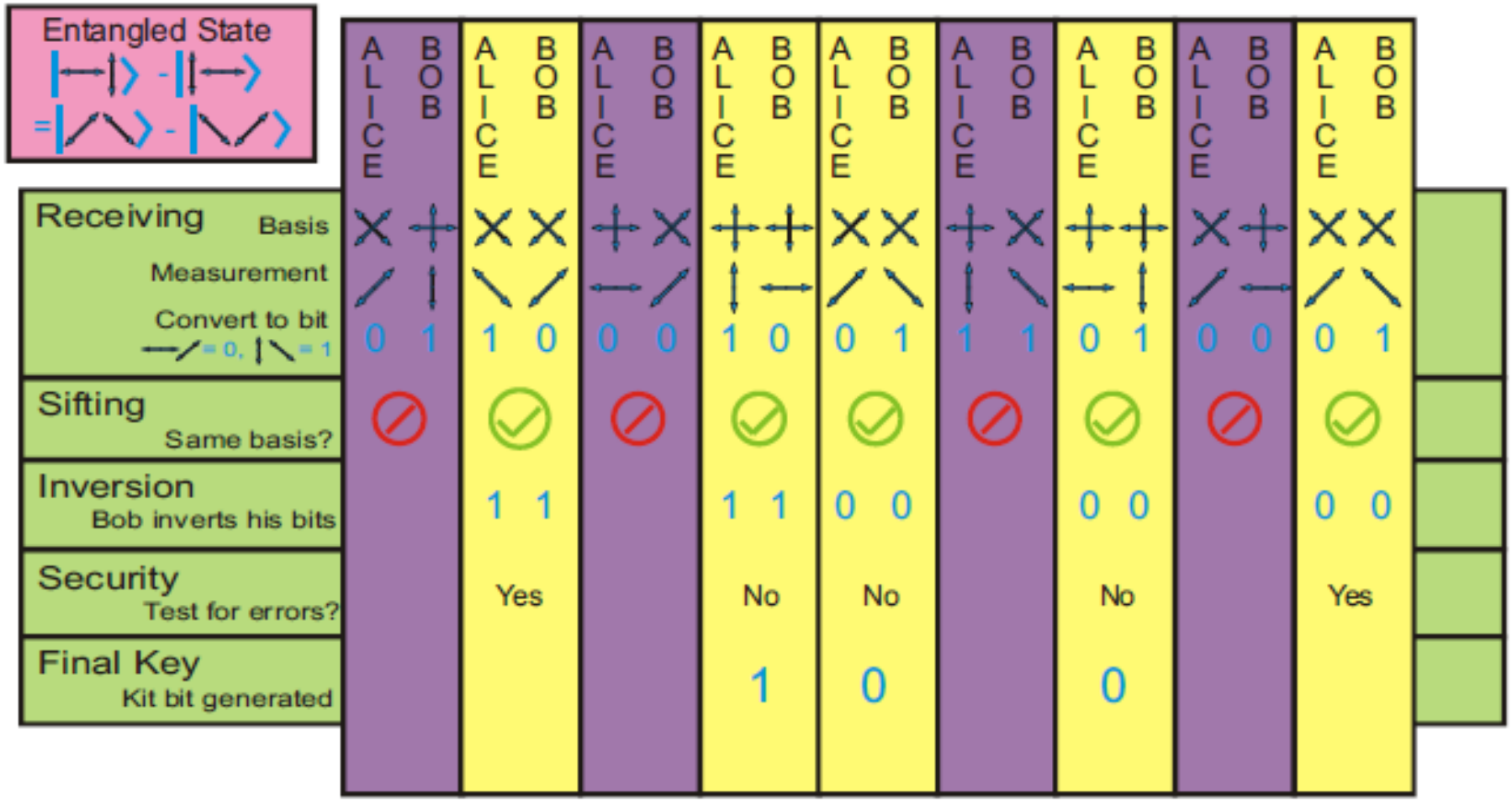
BB 84

- From original BB84 paper

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

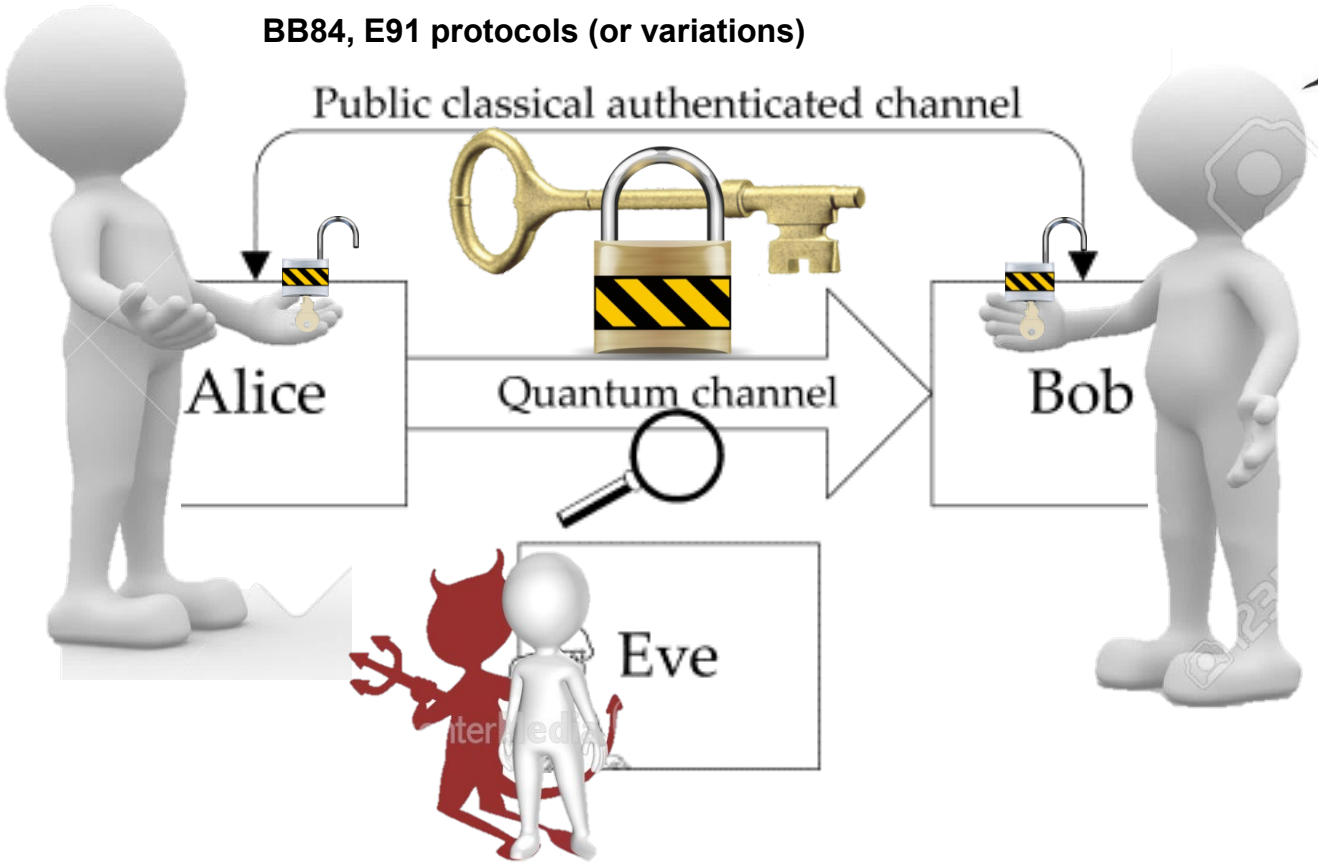
BBM 92

https://en.wikipedia.org/wiki/BBM92_protocol



QKD What is it

BB84, E91 protocols (or variations)

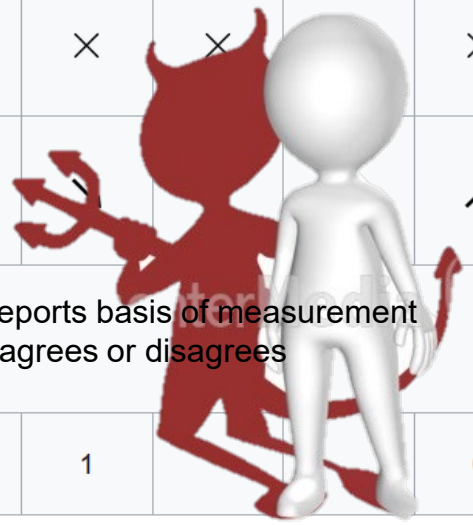


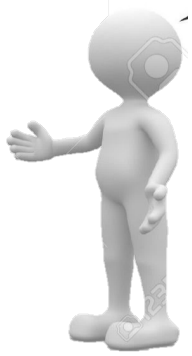
https://en.wikipedia.org/wiki/Quantum_key_distribution

BB84 Example

Alice
(prepares Qubits or Photons)

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×		×	+	+
Photon polarization Bob measures	↑	↗	↘			↗	→	→
PUBLIC DISCUSSION OF BASIS	Bob reports basis of measurement Alice agrees or disagrees							
Shared secret key	0		1			0		1





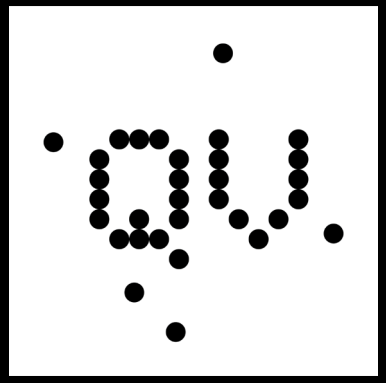
Bob

Eve Listening means
>p bits differ abort the key and try again

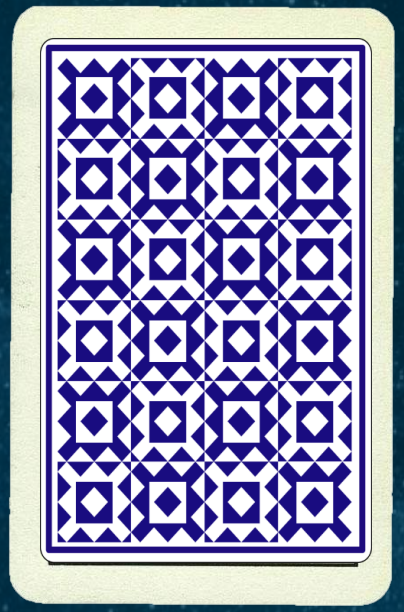
Adding Quantum Ingredients

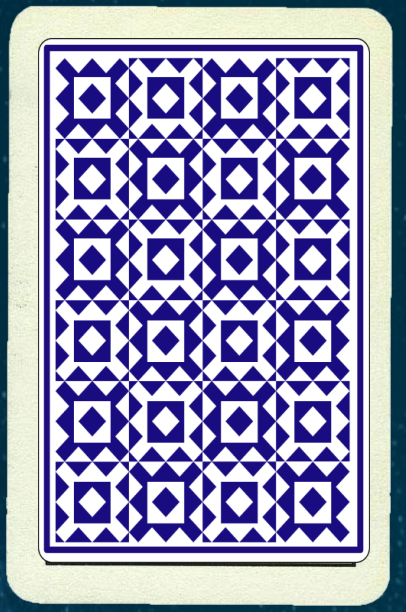
Simplified addition of entanglement

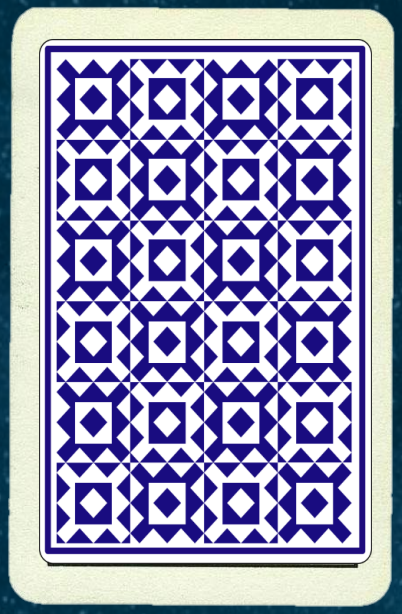
QUICK AD BREAK

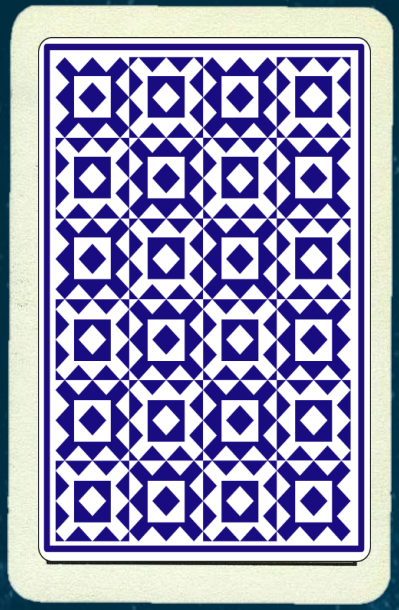


Entanglement

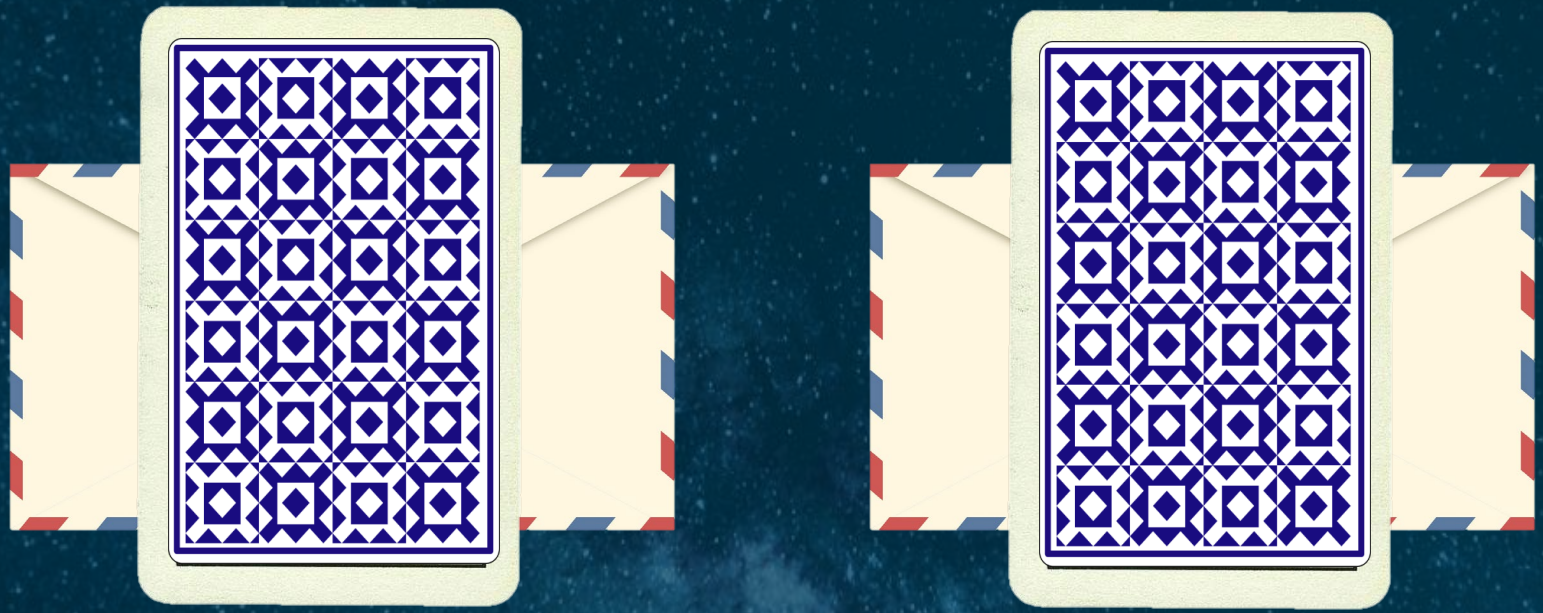








Now shuffle
Err
Entangle



Which is Which ?

Faster than light communication?

Measure one entangled qubit

Deduce properties of its partners

Physics of Entanglement

Two identical particles $u_{1,2}$ can be either in state α and β and are indistiguinishable !

$$u_{12}(\alpha, \beta) = u_1(\alpha)\, u_2(\beta) \qquad u_{21}(\alpha, \beta) = u_2(\alpha)\, u_1(\beta)$$

Schrödinger Equation

$$H = \left[\frac{-\hbar^2}{2\,\mu}\nabla^2 + V(r)\right]$$

$$H_{12}\, u_{12}(\alpha, \beta) = E\, u_{12}(\alpha, \beta) \qquad H_{21}\, u_{21}(\alpha, \beta) = E\, u_{21}(\alpha, \beta)$$

ENTANGLEMENT

Solution

$$\Psi_{12} = A\, u_{12}(\alpha, \beta) + B\, u_{21}(\alpha, \beta)$$

$$\Psi_{21} = A\, u_{21}(\alpha, \beta) + B\, u_{12}(\alpha, \beta)$$

$$|\Psi_{12}|^2 = |\Psi_{21}|^2 \qquad A^2 = B^2 \qquad A = \pm B$$

$$\Psi^S = u_{12}(\alpha, \beta) + u_{21}(\alpha, \beta) \qquad \Psi^A = u_{12}(\alpha, \beta) - u_{21}(\alpha, \beta)$$

Entangled Qubits

Qubit ***A photon can have two orthogonal polarizations.***

It is also in a superposition of state 0 and state 1.

This state is $\alpha|0> = \alpha|0> + \beta|1>$

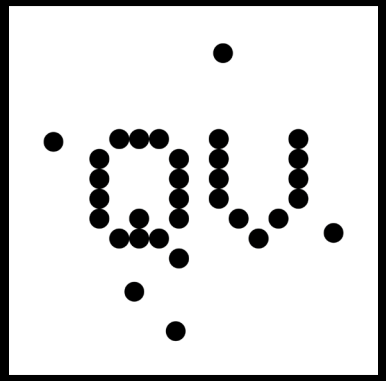
Superposition of two Qubit's

$$(\alpha|0> + \beta|1>)\oplus(\alpha|0> + \beta|1>) = \alpha^2|00> + \alpha\beta|01> + \beta\alpha|10> + \beta^2|11>$$

$|0>|0>$ ***are two independent Qubits***

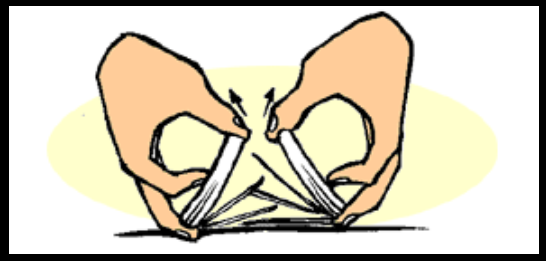
$|00>$ ***are correlated (entangled) Qubits***

AD BREAK
RETURN TO NORMAL PROGRAMMING



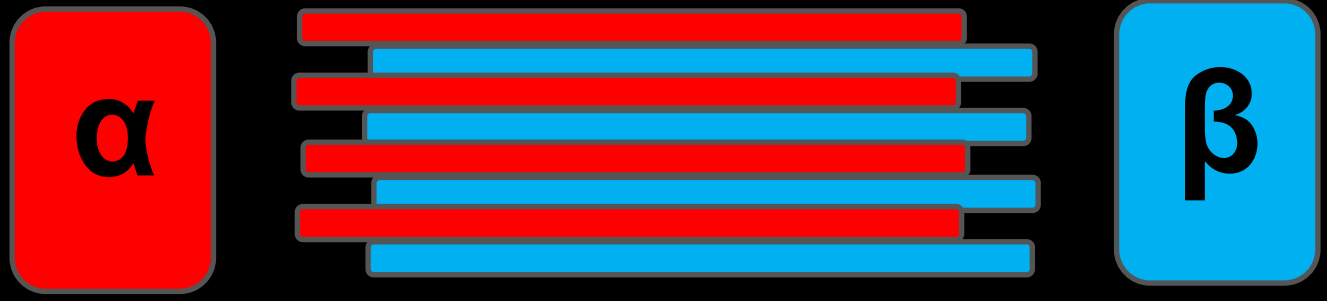
Lets Entangle

Lets Entangle



Entangle two DECKS rather than two cards
Faro Shuffle the two decks by interleaving cards.

Card back represents *initial entangled state*



BUT ALICE AND BOB CANNOT DO THIS !

Reference: https://gurmeet.net/puzzles/card-shuffling/
https://en.wikipedia.org/wiki/Faro_shuffle

Lets Entangle

- Entangle two DECKS rather than two cards
- Intialise a Sequence equivalent to interleaving

[α,β,α,β,α,β,α,β,α,β,α,β,α,β, etc.]

Deck back represents *initial entangled state*

BOB DECK COLOUR = START OF SEQUENCE

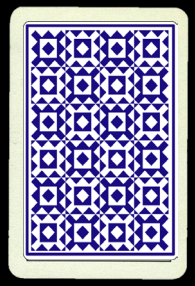
Sequence is State of Basis Measurement

CARD DECK Entangler	BLUE	α	RED	β
	α		β	
	|1>		|1>	
	|0>		|0>	

Sequence continues even if there is a MISS

Lets Entangle

BOB DECK
BLUE



Deck back represents *initial entangled state*
Sequence is State of Basis Measurement

[α,β,α,β,α,β,α,β,α,β,α,β,..

1	2	3	4	5	6
α	β	α	β	α	β
|1> ♦ ♠ |0> ♣ ♥	|1> ♣ ♥ |0> ♦ ♠	|1> ♦ ♠ |0> ♣ ♥	|1> ♣ ♥ |0> ♦ ♠	|1> ♦ ♠ |0> ♣ ♥	|1> ♣ ♥ |0> ♦ ♠
α	β	α	β	α	β

Sequence continues even if there is a MISS

Lets Entangle

BOB DECK
RED

Deck back represents *initial entangled state*
Sequence is State of Basis Measurement

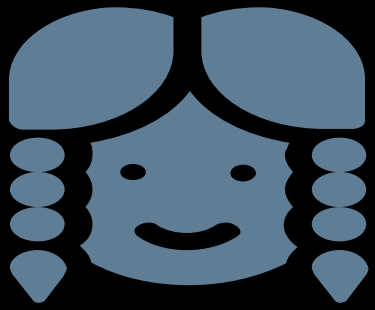
[β,α,β,α,β,α,β,α,β,α,β,α,β,. . .]

1	2	3	4	5	6
β	α	β	α	β	α
|1> ♣ ♥ |0> ♦ ♠	|1> ♦ ♠ |0> ♣ ♥	|1> ♣ ♥ |0> ♦ ♠	|1> ♦ ♠ |0> ♣ ♥	|1> ♣ ♥ |0> ♦ ♠	|1> ♦ ♠ |0> ♣ ♥
β	α	β	α	β	α

Sequence continues even if there is a MISS

Steps

Alice



Bob

1. Entangle the Decks Alice and Bob
   - Entangle two cards or other SECRET entanglement
   - Two Decks with Different Backs One RED the Other BLUE
2. Measure Entangled deck
   - Look at Colour of Deck Back
   - Enter BLUE or RED in Alice Deck
3. Alice note ALICE SUIT and Card Value {1-10 JQKY} Y is Other
4. Enter "X" in BOB Match Column when Bob Shouts Match
   - Bob draws a card from their deck
   - If Colour Matches Alice Card Shout Match
5. Depending on DECK entangled state Measure in α or β
   - Entangled measurement sequence for simple
   - Sequence starts from entangled Bob state followed by [α,β,α,β,α,β,α,β,α,β,α,β,α,β, etc.]
6. Key is automagically generated

Simple Entanglement

Lets Entangle ++

Deeper Entangle :
Picture Cards resets sequence to (n-1)

[α, β, α, β, α, β, α, β, α, β, α, β, α, β, ...]

[-, -, -, -,  , -, -, -,   -, -,  , -,...]

[α, β, α, β, β, α, β, α α, α, β, α, α, β, α, ...]

n-1 n-1

Steps Additional

Alternate Changing Entangled State

5. Depending on DECK entangled state Measure in α or β

- Entangled measurement sequence for simple
- Sequence starts from entangled BoB state followed by [α,β,α,β,α,β,α,β,α,β,α,β,α,β, etc.]
- The sequence continues even if there is a MISS
- Deeper Entangled (Picture Cards) reset the sequence to state (n-1)

If you are about measure α in the sequence you measure β instead and the sequence resets so next State to measure is α

N-1 state Measured in α

N state about to measure in β BUT *PICTURE CARD*

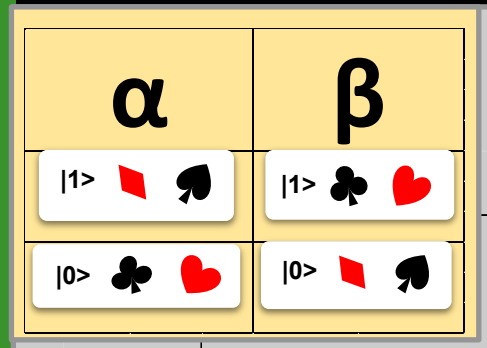
N state *Now measure in state n-1 i.e. α*

N+1 State *now measure in β unless PICTURE CARD*

```
[α, β, α, β, α, β, α, β, α, β, α, β, α,β, etc.] Simple Sequence
[-, -, -, -, P, -, -, -, P, P, P, -, -, P, -, -, -, etc.] <- step with Picture Cards
[α, β, α, β, β, α, β, α, β, β, β, α, β, β, α, β, α, etc.] Changing Sequence
```

Deeper Entanglement

ROUND 2 Example



KEY PLAIN	00011101111100010
KEY SIMPLE	10110110101001000
KEY CHANGER	11001000110011111
EVE KEY	00011101111100010

	ALICE				EVE	BOB	SHOUTS	X= BOB MATCH	Plain	ENTANGLER			
										Simple Entangled State	SIMPLE Entangled Key	Changing Entangled State	CHANGE Entangled Key
DECK		BLUE				RED				β		β	
CARD			SUIT	BASIS		BASIS							
1	♣	1	C	BLACK	0	BLACK	MATCH	X	0	β	1	β	1
2	♥	q	H	RED	0	RED	MATCH	X	0	α	0	β	1
3	♣	5	C	BLACK	0	BLACK	MATCH	X	0	β	1	α	0
4	♦	7	D	RED	1	RED	MATCH	X	1	α	1	β	0
5	♠	8	S	BLACK	1	BLACK	MATCH	X	1	β	0	α	1
6	♦	6	D	RED	1	RED	MATCH	X	1	α	1	β	0
7	♥	5	H	RED	0	RED	MATCH	X	0	β	1	α	0
8	♣	J	C	BLACK	---	---	MISS		---	α	---	α	---
9	♦	10	D	RED	1	RED	MATCH	x	1	β	0	β	0
10	♣	7	C	BLACK	---	---	MISS		---	α	---	α	---

Key Reconciliation & Advantage Distillation "Ben's Game"

Alice and Bob, **distil** a secret key from matching parity of random numbers.
(Card Colour)

Mutual Information : Alice and Bob both know Alice card

Conditional mutual information : Expected value of the mutual information of two random variables given the value of a third.
- Alice and Bob card colour matches
- Entanglement Sequence

Topics for further self learning
- The Gibbs Paradox
- The Microcanonical Ensemble
- Microcanonical Mutual Information

Reference: Unraveling Gibbs Paradox: A Microcanonical Ensemble Analysis of Mutual Information B. T. H. Varcoe and F. L. Wilson
https://en.wikipedia.org/wiki/Conditional_mutual_information

DISTILLATION
Ben's Game

The Algorithm (Modified for Qkard)

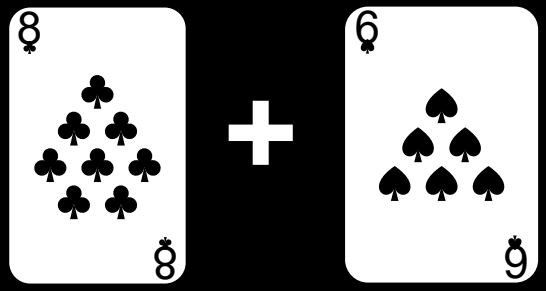
1. Random sequence agreement between Alice and Bob (BB84 Qkard)
2. Data Matching (advantage distillation):
3. Error Correction
4. Privacy Amplification

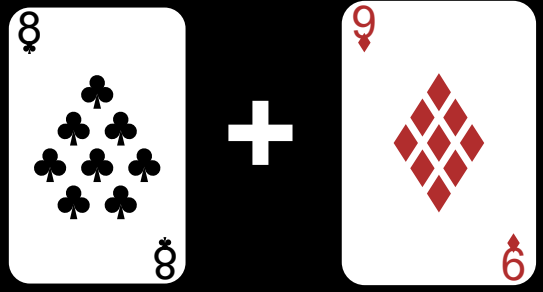
Reference: Unraveling Gibbs Paradox: A Microcanonical Ensemble Analysis of Mutual Information B. T. H. Varcoe and F. L. Wilson

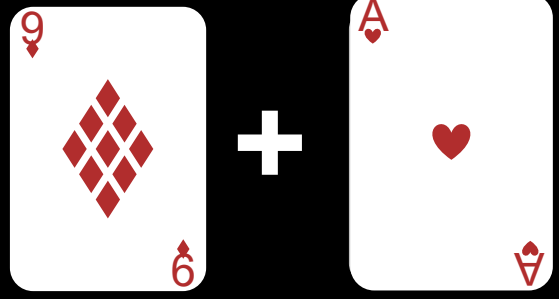
Ben's Game

ALICE & BOB Personal Parity

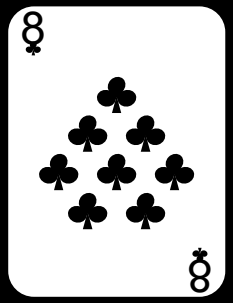
n-1 n







BLACK = 1



RED = 0

Calculate Alice and Bob Parity Values

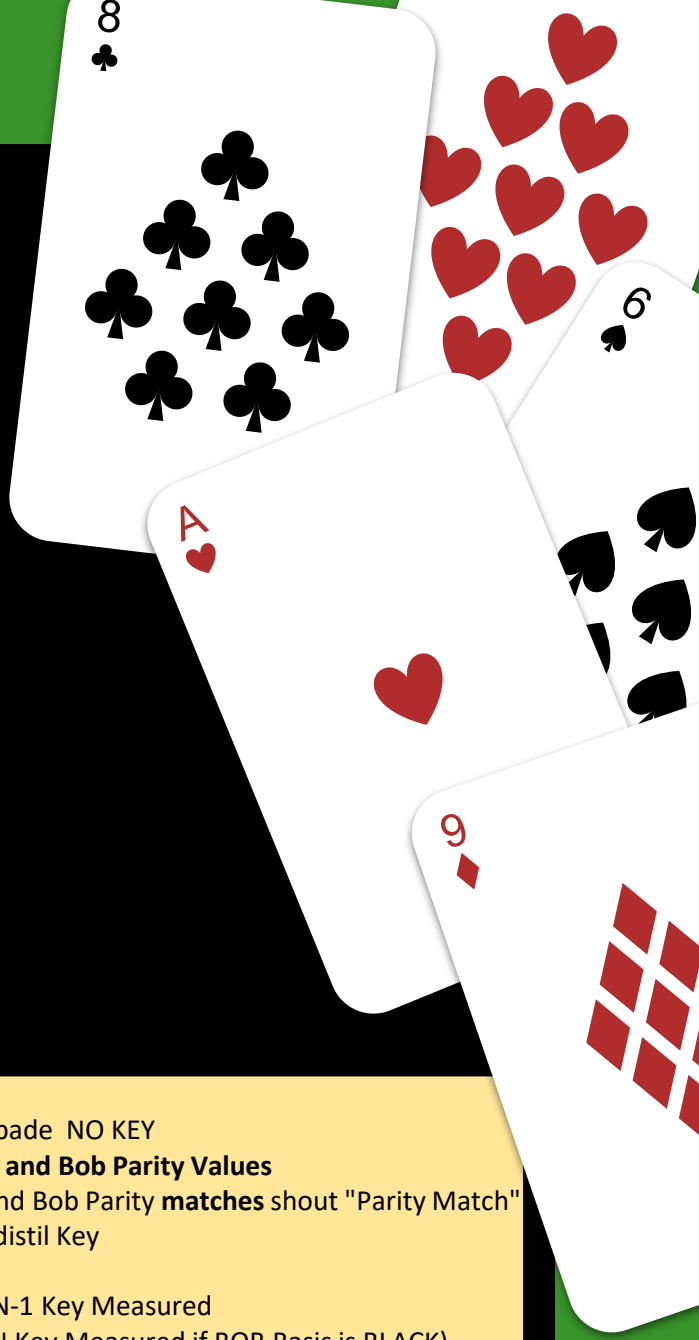
-Using Card Value (N) & Card Value Previous Round (N-1)

Parity Value is a binary addition

MOD(v(N)+v(N-1),2) results in 0 or 1 (EVEN or ODD)

Ben's Game

DISTILLED + PARITY BPIADAD



ALICE	BOB	
Parity EVEN	Parity EVEN	= n-1
Parity ODD	Parity ODD	=
Parity ODD	Parity ODD BOB = BLACK	= n
Parity ODD	Parity EVEN	=

Alice Draws a Spade NO KEY

Calculate Alice and Bob Parity Values

Alice Parity and Bob Parity **matches** shout "Parity Match"

Parity Match distil Key

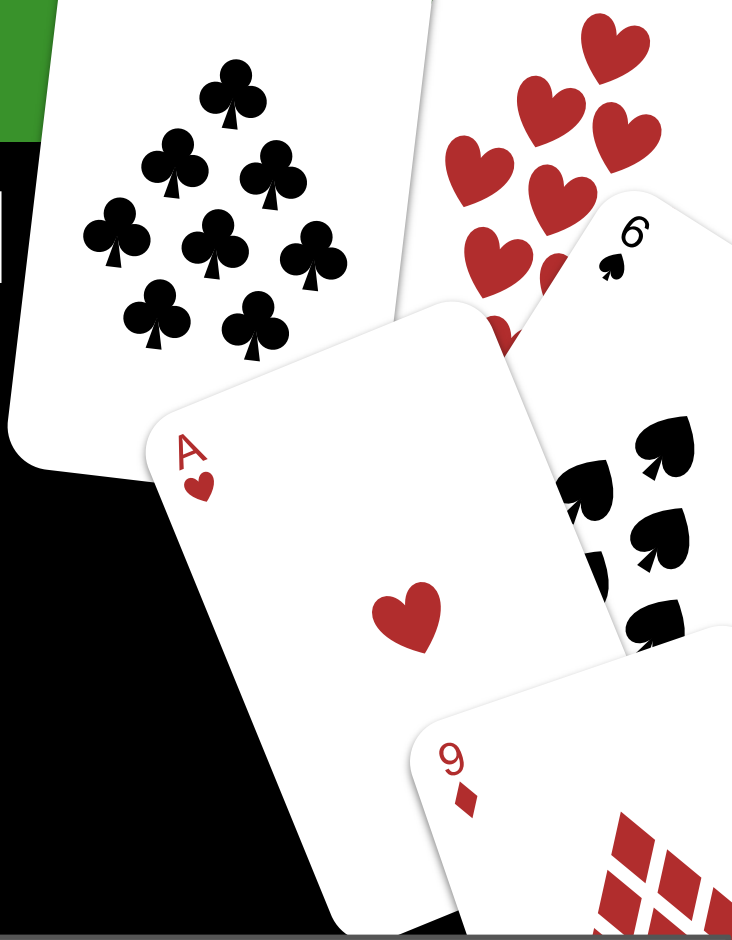
EVEN : Key = N-1 Key Measured

ODD : Key = N Key Measured if BOB Basis is BLACK)

The resulting string of keys is the Distilled Key

DISTILLATION
Ben's Game

Advantage Distillation BB84 INSTRUCTIONS



Calculate the value of Alice Card and Bob Card
- Red cards are assigned a value of 0.
- Black cards are assigned a value of 1.

Note :- Alice can deduces Bob Card Value from when Basis Measurements Match

N is Card Round (Qubit)

-Set Round ZERO to value 0 for ALICE and BOB Card Value

For N Rounds

-If Alice Draws a Spade IGNORE Alice Parity Value & Set Parity MATCH to FAIL"---"

Calculate Alice and Bob Parity Values

-Using Card Value (N) & Card Value Previous Round (N-1)

Parity Value is a binary addition

MOD(v(N)+v(N-1),2) results in 0 or 1 (EVEN or ODD)

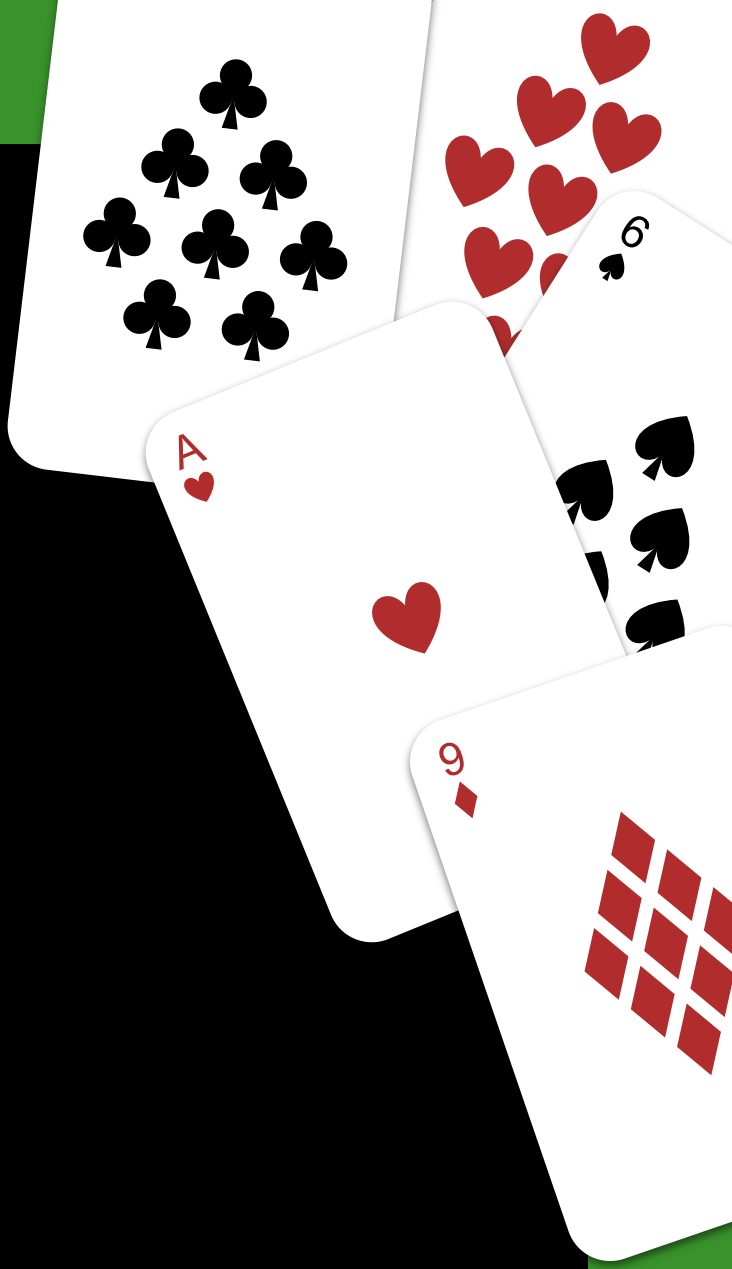
- If Bob calculation of Alice Parity and Bob Parity **matches** shout "Parity Match"

"Distilled BB84 key based on parity
When there is a Parity Match distil that
Plain BB84 key Digit
-EVEN PARITY Key Value is (N-1 Key Measured)
-ODD PARITY Key Value is
(N Key Measured if BOB Basis is BLACK)

The resulting string of keys is the Distilled Key

PARITY - BPIADAD Variant					0=N-1 Value 1=N Value if Bob Black	DISTILLATION		
ALICE CARD	**BOB CARD**	**Alice Value**	**Bob Value**	**Allice PARITY Value v(N)+v(N-1)**	**Bob PARITY Value v(N)+v(N-1)**	**PARITY MATCH**	**MATCH BB84 Key**	**Distilled BB84 key based on parity EVEN PARITY Key Value is (Key Measured N-1) ODD PARITY Key Value is (Key Measured if BOB Basis is BLACK)**
		0	0	0	0			
		0	0	0	0			
RED	**RED**	**0**	**0**	**0**	**0**	**MATCH**	**1**	**0**
BLACK	**BLACK**	**1**	**1**	**1**	**1**	**MATCH**	**1**	**1**

DISTILLATION Ben's Game Keys



BB84 Keys	
KEY PLAIN	00011101111100010
KEY SIMPLE	10110110101001000
KEY CHANGER	11001000110011111
EVE KEY	00011101111100010

Ben's Distilled Keys	
KEY Matched 84	000101001
KEY Distilled BB84	00110
KEY distilled SIMPLE	11100
KEY distilled Change	10011

Reference: Unraveling Gibbs Paradox: A Microcanonical Ensemble Analysis of Mutual Information B. T. H. Varcoe and F. L. Wilson

REAL WORLD QKD DEMO 2

Look at Excel “QV Defcon 31 Demo” Sheet and video link

3 Keys were exchanged simultaneously

3 Keys were distilled

Show back of deck only at start of video

What did WE do

- Exchanged a key (3+ simultaneous different keys)
  - Using a simplified BB84/BBM92 variant
  - Demonstrated distillation

- Limitations
  - Need one secret the initial entangled state of the deck

- EVE has an tougher job if they do not know the intial entangled state

Why This Talk?

- Teach in an intuitive way how BB84/BBM92 QKD works
- How keys are generated with QKD
- Show why Key rate is so slow. Large number of photons needed
- Show that easiest way to hack QKD is to hack the implementation
- Understand that you should always question

Observations

- Exchanged and generated key from various random streams
    1. Alice Random Suit stream
    2. Bob Random Colour Stream
    3. Alice Picture Random Card stream (Entangler)
- Bob “Match” public classical communication channel
    - No need for real time
    - No need for secrecy but need Authentication
- Alice can communicate different keys with the same random stream to different parties.
    - Seperate “Match channel” and authenticate a start/stop time of the stream .
    - Different entangler stream for each party Alice communicates to.
- Provided you agree on coordinated start/stop in stream keys could be generated without Quantum
- Non-QKD starts to look feasible

Way Forward

- Is there a better way to confuse EVE?
- Can you use VEGAS Blackjack tables as Key Generator?
- Is Poker a better key generator?
- Can QKarDs be more secure?
- We Assume that QKardD is not ITS but why ?

Quantum Kard Distribution

Chris Vasko, Mark Carney, Victoria Kumaran, Jose Pizarro

Thanks!

Do you have any questions?

www.esa.int

www.quantumvillage.org

Reference: Unraveling Gibbs Paradox: A Microcanonical Ensemble Analysis of Mutual Information B. T. H. Varcoe1,2* and F. L. Wilson2,3:

"Ben's Game"

The Algorithm (Modified for Qkard)

1. Alice and Bob – Random sequence of Card Colours
2. Alice and Bob select strings with an equal number of 0s and 1s:
   Perform BB84 Qkard Variant with/without entanglement
3. Data Matching (advantage distillation):

(a) Alice and Bob perform a parity match check

(b) Bob sends a "keep" response if the result is :
   Even or (Odd && BoB Suit Black)

(c) If Keep use BB84 Key digit Distilled based on parity
   EVEN PARITY Key Value is (N-1 Key Measured)
   ODD PARITY Key Value is
   (Key Measured if BOB Basis is BLACK)

4. Error Correction:
   Alice and Bob accumulate bits from additional rounds of comparison.
5. Privacy Amplification: (Not yet implemented ? The Entangled Sequence)

(a) Alice and Bob have a matching key set (with high probability).

(b) Alice and Bob now need to create a string about which the Eavesdropper has very little information.

(c) Privacy amplification involves applying a reducing hash function H,
   where
   $H(A) = A'$, $|A'| < |A|$, and $\frac{|A'|}{|A|} \leq I(A,B|Z)$

where $I(A,B|Z)$ is the conditional mutual information for N = 4.

Reference: Unraveling Gibbs Paradox: A Microcanonical Ensemble Analysis of Mutual Information B. T. H. Varcoe and F. L. Wilson

Key Reconciliation & Advantage Distillation "Ben's Game"

- Mutual Information : Think Sliding doors and choices
  mutual third party is like escrow.....
- Conditional mutual information : The "envelope" in the
  entanglement is like an escrow
- .. Solved/explains the faster than light paradox
  Quantum Comms is not FTL
- mutual information is not intentional located limits FTL comms.

why are we bothering with classical when the quantum done?