Title: A Brief Introduction to Quantum Cryptography

Date: Jul 20, 2011 09:30 AM

URL: http://pirsa.org/11070062

Abstract: By exploiting the properties of quantum mechanical systems, two parties can achieve cryptographically secure communication in a manner not possible in a purely classical world, through the process of quantum key distribution. In this talk, I will briefly introduce the field of cryptography and explain one of the most fundamental applications of quantum mechanics to cryptography.

A Brief Introduction to Quantum Cryptography

Women in Physics Canada 2011

Stacey Jeffery

Example 1:

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	E	M	L	C	S	B	R	I	X	U	H	D	T	K	N	W	A	V	O	Z	J	P	F	G	Q	Y

Example 1:

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	E	M	L	C	S	B	R	I	X	U	H	D	T	K	N	W	A	V	O	Z	J	P	F	G	Q	Y

E LNTWJZSV NKLS MSEZ TS EZ LISOO, MJZ XZ FEO KN TEZLI BNV TS EZ HXLHMNGXKR.

Example 1:

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	E	M	L	C	S	B	R	I	X	U	H	D	T	K	N	W	A	V	O	Z	J	P	F	G	Q	Y

E LNTWJZSV NKLS MSEZ TS EZ LISOO, MJZ XZ FEO KN TEZLI BNV TS EZ HXLHMNGXKR.

A COMPUTER ONCE BEAT ME AT CHESS, BUT IT WAS NO MATCH FOR ME AT KICKBOXING.

Example 2: One-time Pad

Example 2: One-time Pad

Barb

Alice

Example 2: One-time Pad

Example 2: One-time Pad

Example 2: One-time Pad

Barb

Alice

Example 2: One-time Pad

Barb

$\bar{b}$

Alice

Example 2: One-time Pad

message:	0	0	1	0	1	0	0	1
key:	1	1	1	0	1	0	0	0
ciphertext:								

Solution 1: Public Key Cryptography

Solution 1: Public Key Cryptography

Encryption key (public): e

Solution 1: Public Key Cryptography

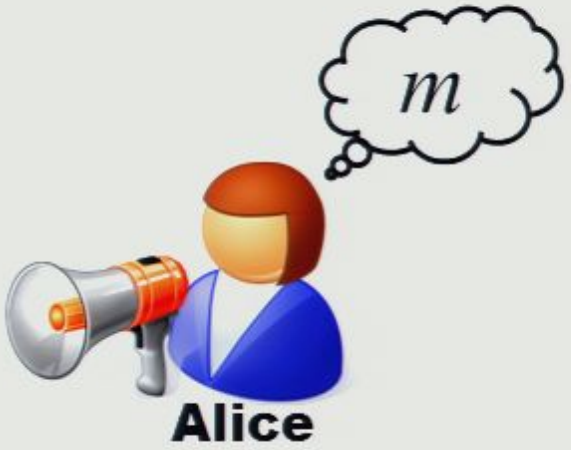
Encryption key (public): e

Decryption key (private): d

Solution 1: Public Key Cryptography

Encryption key (public): e

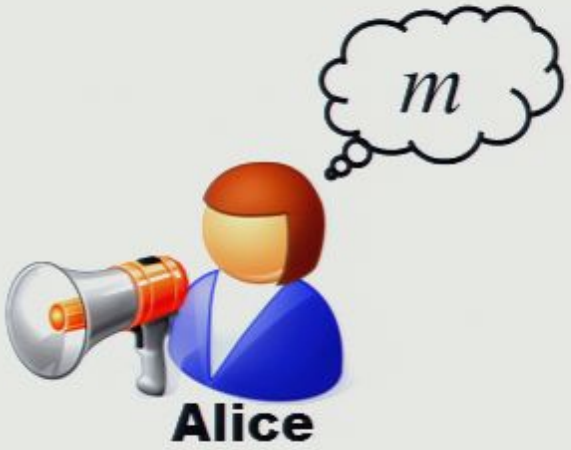
Decryption key (private): d



Solution 1: Public Key Cryptography

Encryption key (public): e

Decryption key (private): d



Solution 1: Public Key Cryptography

Encryption key (public): e

Decryption key (private): d

Solution 1: Public Key Cryptography

Encryption key (public): e

Decryption key (private): d

Alice

Barb

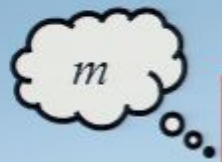
Public information

p g

Barb

Public information

p g



Alice

Barb

$a \in_R \{1, \ldots, p-1\}$

$b \in_R \{1, \ldots, p-1\}$

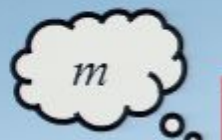
B

$B = g^b \pmod{p}$

Public information

p g

B



Alice

Barb

$a \in_R \{1, \ldots, p-1\}$

$A = g^a \pmod{p}$

B

$\longleftarrow$

$b \in_R \{1, \ldots, p-1\}$

$B = g^b \pmod{p}$

$c = mB^a = m(g^b)^a$

$= mg^{ab} \pmod{p}$

Public information

p g

B

Alice

Barb

$a \in_R \{1, \ldots, p-1\}$

$A = g^a \pmod{p}$

B

$b \in_R \{1, \ldots, p-1\}$

$B = g^b \pmod{p}$

$c = mB^a = m(g^b)^a$
$= mg^{ab} \pmod{p}$

c, A

$m = c(A^b)^{-1}$
$= c(g^{ab})^{-1} \pmod{p}$

Public information

p *g*

c, A *B*

Solution 2: Quantum Key Distribution

Quantum Key Distribution

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

1

11

×

×+

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

1

11

×

×+

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

1

11

XX

X+

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

11

111

XX

X+X

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

11

111

××+

×+×

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

110

1110

××+

×+××

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

110

1110

××+×

×+××

basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

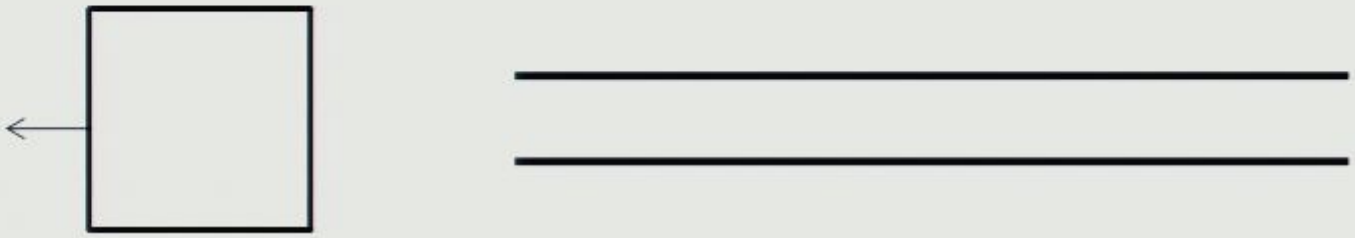
Quantum Key Distribution

1100110100

XX+X+XX+++

1110110100

X+XX+X++X+



basis	state	bit
+	→	0
+	↑	1
×	↗	0
×	↘	1

Quantum Key Distribution

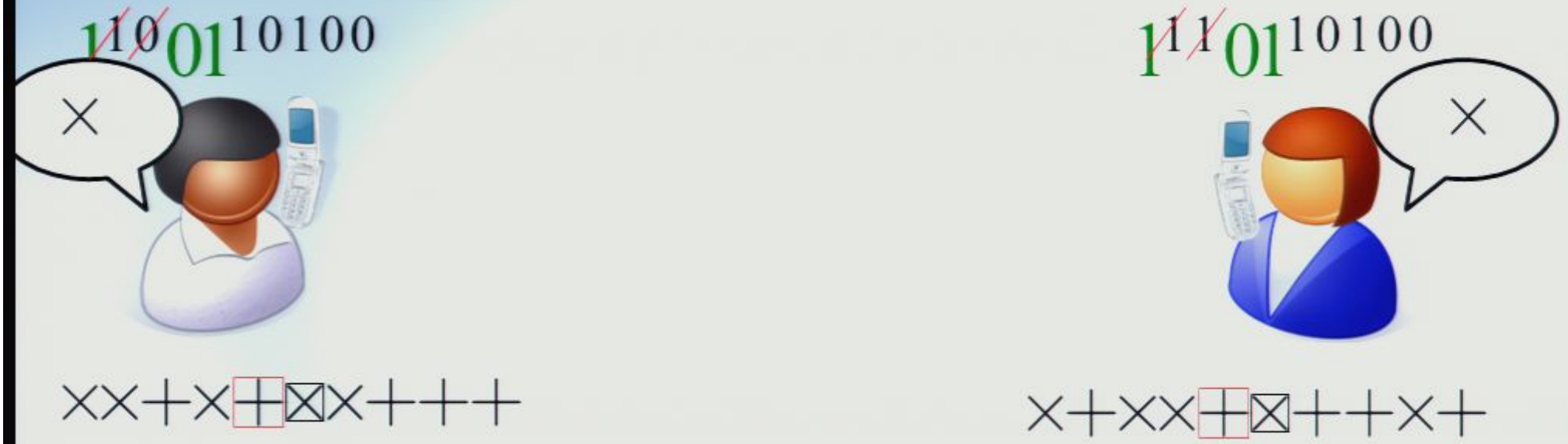
1100110100

××+×+××+++

1110110100

×+××+×++×+

Quantum Key Distribution



Quantum Key Distribution

XX+X+XX+++

X+XX+X++X+

Quantum Key Distribution

Eve

Pirsa: 11070062

There is so much more to quantum cryptography:

- Quantum money
- Quantum multiparty computation
- Quantum coin flipping
- Quantum bit commitment

...just to name a few