הצפנה קוונטית – הסודיות מובטחת

אביתר אוסטר

חיפה, אולימפידע, אוגוסט 2007.

הצפנה – מהות ומטרה

- **הצפנה** *היא תרגום של מסר לסימנים המוכרים ומובנים לנמען בלבד.*
- *מטרת ההצפנה היא לחסום הבנת המידע ע"י מאזין לא רצוי.*

Plain	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
1	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	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

שיטת ורנאם – עקרון הפעולה

- השיטה מבוססת על חיבור הודעה גלויה עם מפתח חשאי, והעברת המסר הנוצר מחיבור זה.
- דוגמא:

כללי החיבור:

1	0	+
1	0	0
0	1	1

ההודעה: 1111100000

המפתח: 0110101011

ההודעה המוצפנת:

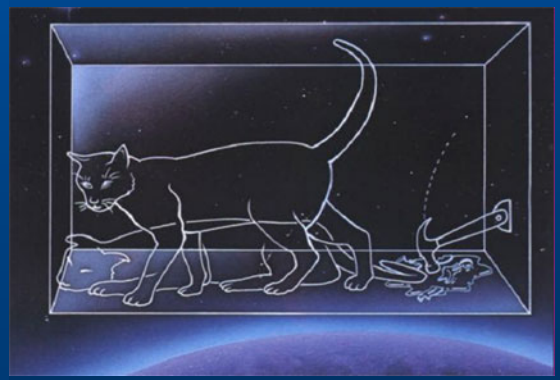
$$\begin{array}{r} 1111100000 \\ + \\ 0110101011 \end{array} = 1001001011$$

שיטת ורנאם – יתרונות וחסרונות

- היתרון העיקרי של שיטה זו, הוא כי ללא המפתח, לא ניתן לפענח את המסר.
- הידד! יש לנו הצפנה חסינה! אבל, רגע... איך נעביר את המפתח?!

קצת קוונטים

- התורה הקוונטית מתארת את הפיזיקה של חלקיקים במימדים בגודל האטום (קטנים מאוד...)
- אחד מעקרונות המפתח בתיאוריה הקוונטית, קובע כי כל חלקיק נמצא באופן טבעי בכל המצבים האפשריים בו זמנית.(בהסתברות שונה לכל מצב)
- ברגע בו אנו מסתכלים ("מודדים אותו") החלקיק "קורס" לפי הסתברויות שניתן לחשב לאחד מהמצבים - כלומר המדידה שינתה את מצבו של החלקיק!
- אבל מה הקשר להצפנה?



הצפנה קוונטית - העקרון

- *בגלל העובדה שהוזכרה שהמדידה משנה את מצבו של החלקיק, חשבו פיזיקאים להשתמש בעקרונות התיאוריה הקוונטית לצורך הצפנה.*
- *כיצד נעשה זאת?*

נוכל לשים על כל חלקיק מידע (0 או 1)

ולשלוח אותו לנמען.

במידה ומישהו יחליט לצותת לנו בדרך,

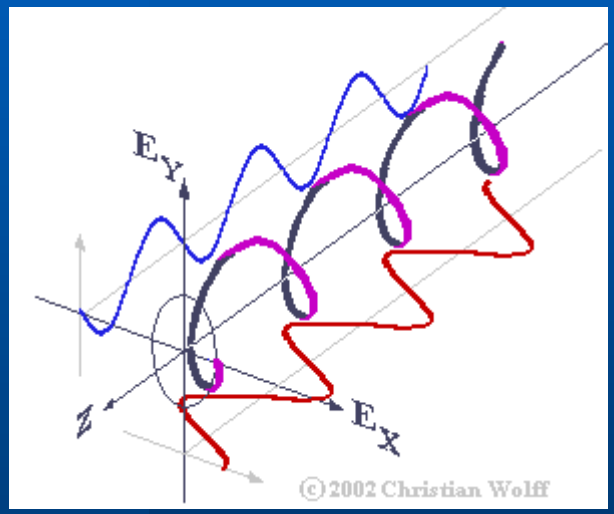
הוא ישפיע על המידע ששמנו על החלקיקים

ונוכל לדעת שמישהו מאזין לנו.

הצפנה קוונטית - קיטוב

- אז איך שמים מידע על חלקיק?
- לצורך העניין ניקח את החלקיק פוטון (חלקיק של אור),

  לחלקיק זה תכונה הנקראת קיטוב, ונוח להסביר אותה במונחים של גל אור.
- קיטוב הינו למעשה כיוון התנודות של השדה החשמלי.
- הקיטוב יכול להיות למשל אנכי, אופקי, אלכסוני שמאלה, ואלכסוני ימינה.

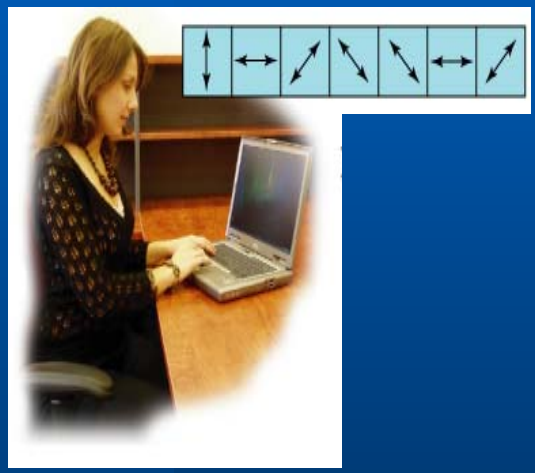


הצפנה קוונטית - דוגמא

- אז איך זה עובד? בואו נבין בעזרת דוגמא:

הצפנה קוונטית - דוגמא

1



- רוחמה רוצה לשלוח לירחמיאל את המפתח הסודי (בשביל שיטת וראנם) כדי לשלוח לו את מתכון העוגיות הסודי של סבתא שלה:
- היא שולחת לו שבעה פוטונים עם קיטובים מסוימים.

הצפנה קוונטית - דוגמא

2

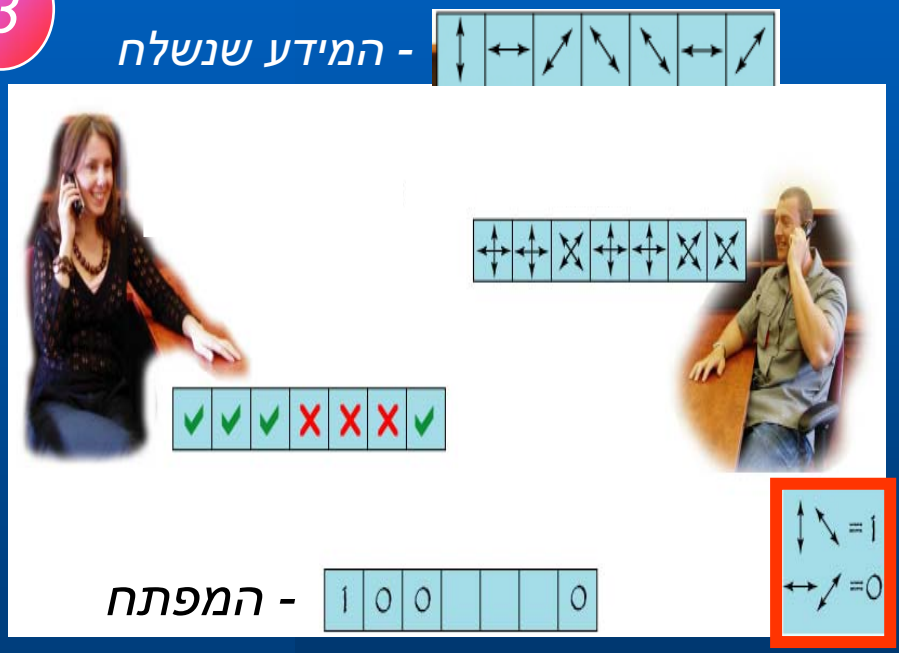
- ירחמיאל מקבל את הפוטונים בברכה, ומעביר אותם דרך מסננים. ישנם שני סוגים של מסננים: ישר ואלכסוני.
- מסנן תואם (למשל מסנן ישר לקיטוב אופקי או אנכי) יציג את סוג הקיטוב, ומסנן לא תואם יחזיר סתם תשובה אקראית.
- ירחמיאל בוחר את סוג המסננים בצורה אקראית.

הצפנה קוונטית - דוגמא

- ירחמיאל מספר לרוחמה בטלפון באיזה מסננים הוא השתמש, והיא מספרת לו אילו מסננים היו תואמים לסוג הקיטוב שהיא שלחה.
- עתה, שניהם לוקחים רק את הפוטונים שתאמו, ולפי טבלה מוגדרת מראש הם מסמנים "1" ו"0". עתה יש להם מפתח סודי משותף!
- שימו לב: ציתות לשיחת הטלפון ביניהם לא תניב שום מידע!

הצפנה קוונטית - דוגמא

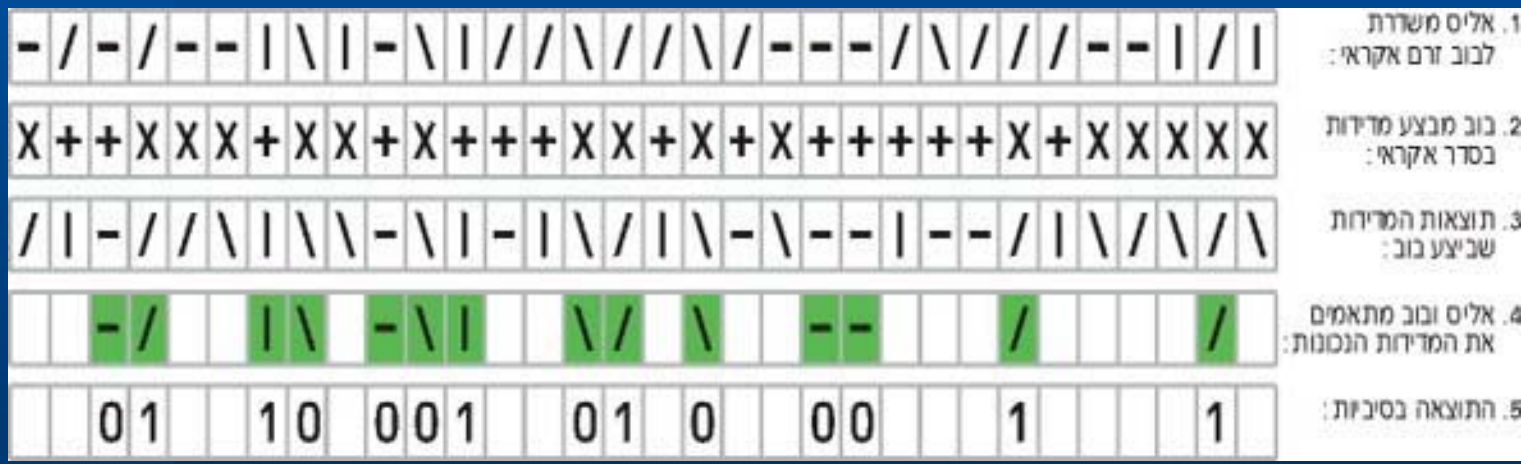
- ירחמיאל מספר לרוחמה בטלפון באיזה מסננים הוא השתמש, והיא מספרת לו אילו מסננים היו תואמים לסוג הקיטוב שהיא שלחה.
- עתה, שניהם לוקחים רק את הפוטונים שתאמו, ולפי טבלה מוגדרת מראש הם מסמנים "1" ו"0". עתה יש להם מפתח סודי משותף!
- שימו לב: ציתות לשיחת הטלפון ביניהם לא תניב שום מידע!



הצפנה קוונטית - דוגמא

- אם מישהו ינסה לצותת בדרך, הוא ישפיע על הקיטוב של הפוטונים, וכך רוחמה וירחמיאל אמנם לא יוכלו להעביר את המפתח, אבל הם יידעו שמישהו מצותת להם, וגם הוא לא יוכל להשיג את המתכון הסודי!
- זוהי למעשה הצפנה ללא יכולת שבירה שלה! לא ניתן לגלות את המפתח!

טבלת סיכום (אם למישהו יש שאלות...):



סיכום

- ראינו כי לצורך הצפנה יש צורך בשליחת מפתח כך שרק לנמען ולשולח יהיה את אותו מפתח.
- למדנו מושגים בסיסים בתיאוריה הקוונטית, וראינו כיצד ניתן ליישם אותם עבור הצפנה.
- האם נגמר הקרב בין המצפינים למפענחים?
- האם סוף-סוף ניתן לשלוח מתכוני עוגיות מבלי שאף אחד בעולם יוכל לפענח אותן?!

- בכל אופן, תודה על ההקשבה...

ביביליוגרפיה

- *ספרו של סיימון סינג: "סודות ההצפנה".*
- *האתר: "סנונית".*
- *האתר: "אלקטרוניקה".*
- *באתר "ויקיפדיה" הערך "הצפנה קוונטית".*