

*Rabeeh Farah*

*R. Farah Physics Teacher*

*M.Sc Student at Science Teaching Department*

*The Hebrew University Jerusalem*

*Mobile : (+972) 0545941394*

*Phone : (+972) 049964416*

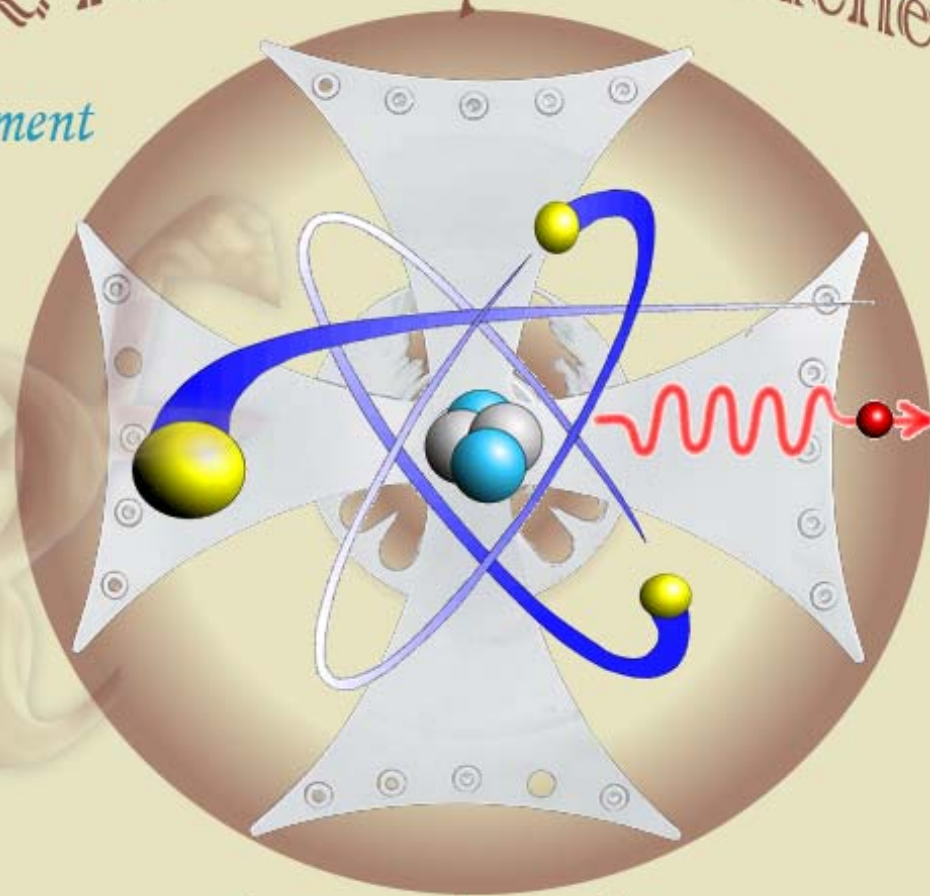
*E-mail : [Rabeeh.Farah@gmail.com](mailto:Rabeeh.Farah@gmail.com)*

*home page : [www.rabeeh-farah.net](http://www.rabeeh-farah.net)*

*Kfar Yassif 24908*

*P.O.BOX 806*

*ISRAEL*



*I never teach my pupils; I only attempt to  
provide the conditions in which they can learn*

*Albert Einstein*

# Quantum Key Distribution

באופטיקה קוונטית

(חגי איזנברג)

החוג להוראת המדעים האוניברסיטה העברית

3/2008

# פנקס חד-פעמי (OTP) one-time pad

- **הגדרה:** הוא שיטת הצפנה שהומצאה בשנת 1917, שייחודה בכך שקיימת הוכחה מתמטית לפיה אם המפתח המשמש להצפנה נבחר באקראי והשימוש בו הוא חד-פעמי, ההצפנה בלתי ניתנת לשבירה.
- **אופן ההצפנה:** מניחים כי המסר להצפנה מיוצג כרצף ספרות בינארי, שכן הייצוג הטבעי של אינפורמציה במחשב הנו כזה. המפתח המשמש להצפנה גם הוא מיוצג כמחרוזת בינארית שאורכה כאורך הקלט. ההצפנה מבוצעת על ידי הפעלת פעולת XOR על המסר והמפתח. הפענוח מבוצע באותה דרך, אך על הצופן והמפתח.

## Example One-Time Pad

48173	19839	90183
51834	00182	47865
01983	47362	32
60120	98754	2874

# פנקס חד-פעמי (OTP) one-time pad

## הצפנה בטוחה:

מפתח ההצפנה צריך להיבחר באופן אקראי  
אסור להשתמש בו יותר מפעם אחת  
שימוש חוזר במפתח יהפוך את הצופן לקל מאוד לשבירה

## חסרונות:

- "הפיכת שליחת מסרים ארוכים לבעייתית": הצורך בשימוש במפתח שאורכו כאורך המסר המיועד להצפנה. הצורך במפתח ארוך יוצר מספר בעיות - הן בשל הקושי בייצור כמות גדולה מהמפתח שתספיק לאורך זמן, והן בשל הקושי להשמיד את המפתח לחלוטין לאחר השימוש כדי להבטיח שלא ייפול לידיים הלא נכונות.

# פנקס חד-פעמי (OTP) one-time pad

## חסרונות:

- **”בעיית העברת המפתח”:** כדי ששני הצדדים יוכלו לתקשר ביניהם באופן בטוח על שניהם לדעת מהו המפתח, אך על מנת לשתף את המפתח עליהם להיות מסוגלים להעבירו באופן בטוח מהאחד לשני.
- **”הבטחת השלמות”:** מונעת שינוי של המסר המוצפן בידי גורם זר המסוגל ליירט את הצופן, לשנות חלקים ממנו ולאפשר למסר להמשיך ליעדו המקורי מבלי שיעד זה יוכל לזהות שינוי זה.

# פנקס חד-פעמי (OTP) one-time pad

## • יישום פנקס חד-פעמי באמצעות הצפנה קוונטית

בעיית העברת המפתח פוגמת ביעילות השיטה. לאור זאת יש הסבורים כי כאשר תהיה פריצת דרך בתחום המחשבים הקוונטיים, ניתן יהיה לנצל הצפנה קוונטית לצורך העברת המפתח ובכך לייעל את שיטת הפנקס החד-פעמי, מה שישנה את פני ההצפנה באופן דרמטי.

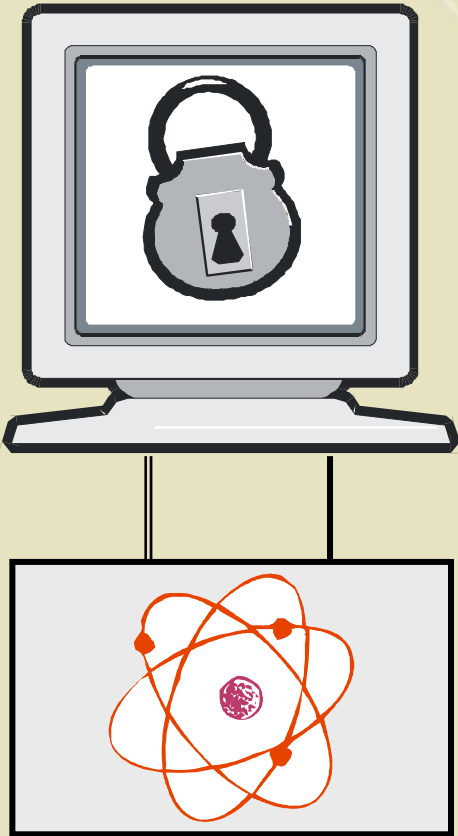


# הצפנה קוונטית (QKD) quantum key distribution

## קריפטוגרפיה :

• מקורו במילה היוונית "קריפטו" שמשמעותה **נסתר** או אמנות ההסתרה. בתרגום חופשי פירוש השם הוא **תורת ההצפנה**.

• משמש בדרך כלל כדי לתאר את הענף המדעי שעוסק במחקר שיטות הצפנה, אלגוריתמים קריפטוגרפיים, פרוטוקולים ומנגנוני אבטחת מידע, הדרכים ליישומן והשיטות לפיצוחן.



## מה זאת הצפנה קוונטית ?

- **הצפנה קוונטית משתמשת במכאניקה קוונטית לאבטחת ערוץ תקשורת.**  
בניגוד לקריפטוגרפיה מסורתית, המיישמת טכניקות מתמטיות כמו הצפנה סימטרית ומפתח פומבי (Public key), כדי להסתיר את תוכן המידע מפני מצותת.
- **הצפנה קוונטית מתבססת על חוקים פיזיקליים מתורת הקוונטים כמו עיקרון אי הוודאות של הייזנברג, סופרפוזיציה ושזירה קוונטית, הבאים לידי ביטוי בהתנהגות פוטונים, כדי ליצור ערוץ תקשורת בטוח שאינו ניתן בשום אופן לציתות מבלי להפריע לשידור.**
- **חוקי הפיזיקה מגנים על הערוץ מפני מצותת בעל עוצמת חישוב בלתי מוגבלת. מאחר ומדידות קוונטיות של חלקיקי האור משבשות את מצבם הקוונטי ובכך מותירות אחריהן עקבות המובילות לחשיפת המצותת.**



## סוגי הצפנות קוונטיות

1. הראשונה של צ'ארלס בנט וז'יל ברסרד (BB84), מנצלת את הקיטוב (פולריזציה) של פוטונים כדי לקודד סיביות מידע ומסתמכת על ההתנהגות האקראית של החלקיקים כדי למנוע מהמצותת לחלץ את המפתח.

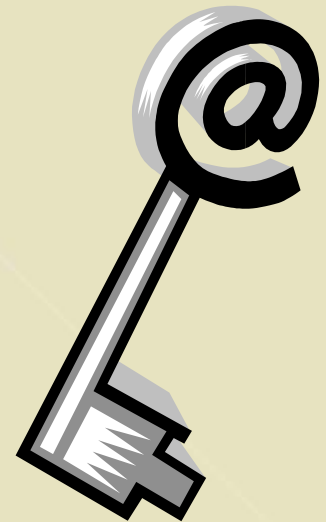
2. השנייה של ארתור אקרט (1991), מנצלת את תכונת השזירה הקוונטית ומסתמכת על הקשר הקיים בין מצבם הקוונטי של זוגות פוטונים שנוצרו ממוקור אחד, שלמרות המרחק ביניהם המצב המתקבל במדידה הנעשית במקומות מרוחקים, זהה.

# הצפנה קוונטית (QKD) quantum key distribution

Quantum Cryptography: public key distribution and coin tossing (B.B.84)

## Keys and Key Distribution :

- The key is known only to sender and receiver: it is **secret**.
- **Anyone** who knows the key can decrypt the message.
- **Key distribution** is the problem of exchanging the key between sender and receiver.



# הצפנה קוונטית (QKD) quantum key distribution

Quantum Cryptography: public key distribution and coin tossing (B.B.84)

• על ידי השפעות קוונטיות נוכל להעביר המפתח בסודיות מושלמת.

• אחת הדרכים על ידי OPT כך ש

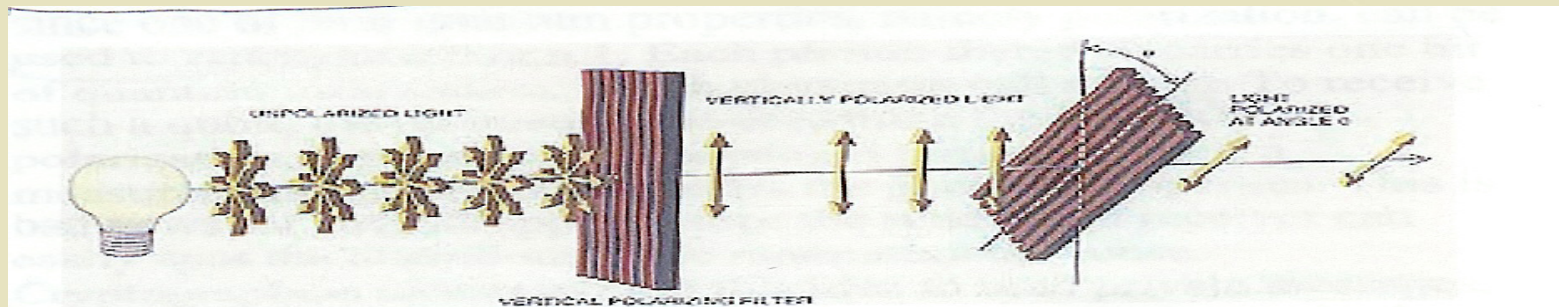
$$QC = QKD + OTP$$

Cryptosystem, quantum key distribution, one-time pad



## פולריזציה וסופר-פוזיציה רעיון בסיסי של ההצפנה הקוונטית

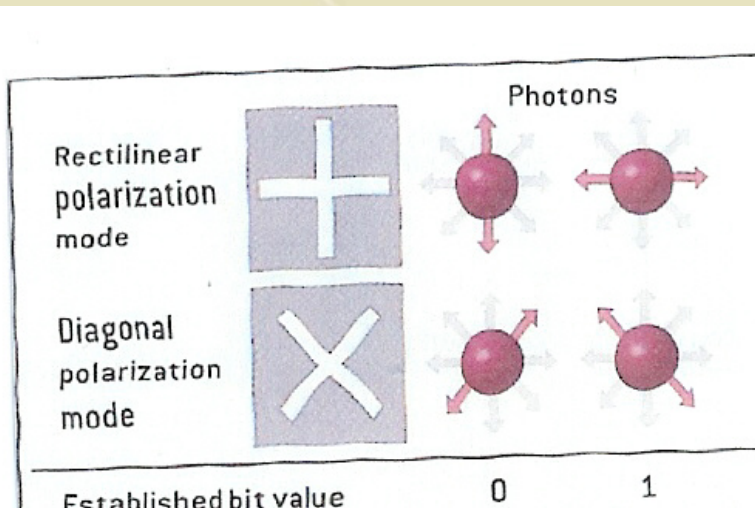
- שפוטונים שאינם מקוטבים, יכולים להימצא בכל זווית אפשרית.
- אם נטיל אלומת פוטונים אופקיים במקטב ונסובב אותו בתשעים מעלות מספר הפוטונים שיעברו דרכו ילך ויפחת בהדרגה, עד כי יחסמו לגמרי.
- בזמן המדידה הפוטון יקרוס למצב יחיד באופן אקראי וככל שזווית הקיטוב של הפוטון קרובה יותר לזווית המקטב כן יגדלו סיכוייו לעבור דרכו.
- במקטב אופקי, לפוטון אנכי יש אפס סיכויים לעבור. בעוד שלפוטון המצוי בזווית 45 מעלות, יש סיכויים של חמישים אחוז לעבור.



# פולריזציה וסופר-פוזיציה רעיון בסיסי של ההצפנה הקוונטית

## סוגי הקיטובים :

- קיטוב אורתוגונאלי שהוא קיטוב ישר זווית המסומן (+), קרי מצבים אנכיים ואופקיים בלבד של הגל האלקטרומגנטי. בבסיס זה מדידת הפוטון וודאית .



$$\theta = 0^\circ \Rightarrow \text{state } |0\rangle$$

$$\theta' = 90^\circ \Rightarrow \text{state } |1\rangle$$

$$\theta = 45^\circ \Rightarrow \text{state } |0\rangle$$

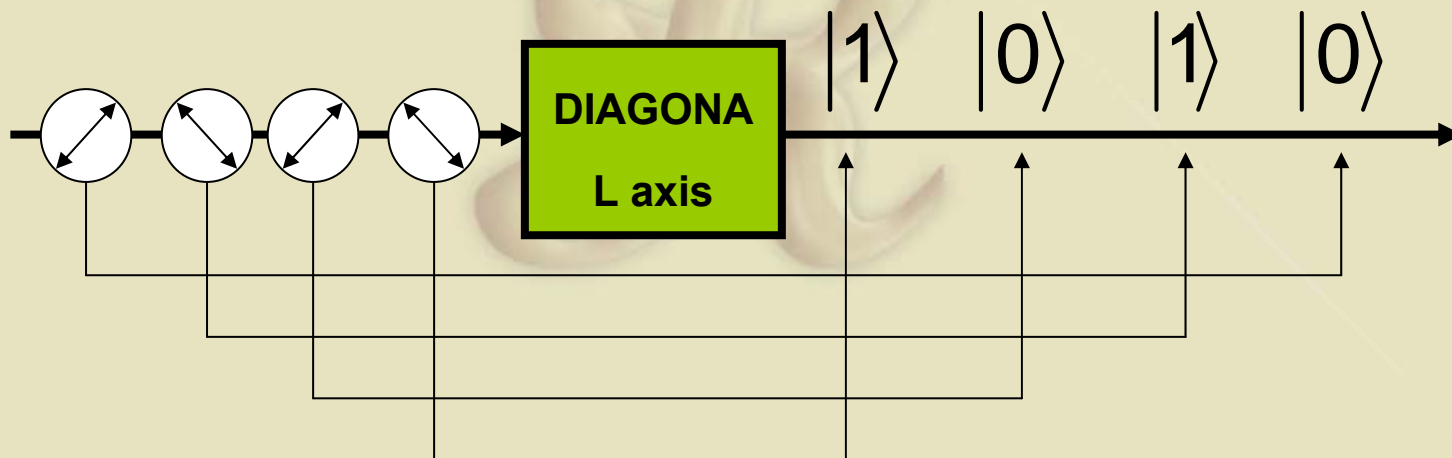
$$\theta' = 135^\circ \Rightarrow \text{state } |1\rangle$$

- קיטוב מעגלי או קיטוב אלכסוני של הגל המסומן (x), הוא מצב בו נמדדים הקיטובים האלכסוניים, למשל אלכסון ימני או אלכסון שמאלי. בבסיס זה מדידת הפוטון אקראית.

# פולריזציה וסופר-פוזיציה רעיון בסיסי של ההצפנה הקוונטית

• ניתן לקבוע בוודאות באיזה מצב הפוטון מקוטב רק אם נמדד במקטב בעל בסיס מתאים.






• חוק הפיזיקאלי אוסרים מדידה נוספת לפוטון כי המדידה הורסת את מצב אי הוודאות של החלקיק.





# העברת מפתח קוונטית






- אליס משדרת לבוב באמצעות ערוץ אופטי מיוחד, זרם של פעימות פוטונים.
- כל פוטון מקוטב באופן אקראי באחד מארבעת הכיוונים.

Bit	0	1	0	1	1
Basis	+	x	x	+	x
Photon					



# העברת מפתח קוונטית






- לבוב יש גלאי קיטוב. כאמור הוא יכול לכוון את בסיס הגלאי כך שימדוד קיטוב ישר או קיטוב אלכסוני אך לא שניהם בו זמנית. בוב מבצע את המדידות באופן אקראי, כאשר עם כל מדידה הוא משנה את בסיס הגלאי.
- כעת אם בוב קבע את הגלאי באופן הנכון (בהתאם לבסיס הקיטוב שנקבע על ידי אליס) מדידתו תהיה נכונה, הוא יקבל את הקיטוב הנכון של הפוטון. אולם אם קבע בסיס שגוי, יקבל תוצאה אקראית

Photon					
Basis?	+	+	x	+	x
Bit?	0	0	0	1	1

# העברת מפתח קוונטית

- לאחר שאליס שדרה די פוטונים לבוב, כל שעליהם לעשות הוא להתקשר זה עם זה בערוץ פתוח שאינו מאובטח (כגון בטלפון) ולהסכים ביניהם על סדר המדידות הנכון .
- אליס תיידע את בוב אילו מבין המדידות שביצע נכונות, כך שתוצאתם תהיה זהה אצל שניהם.
- אם בוב יפטר מכל הפוטונים שמדד באופן שגוי, יקבל זרם של פוטונים המקוטבים באופן זהה לזה של אליס.
- ניתן להכין מפתח הצפנה מתוך זרם הפוטונים אם מסכימים מראש על דרך המרתם לסיביות כגון פוטון אנכי או אלכסון-ימני שווה 1, פוטון אופקי או אלכסון שמאלי שווה 0.

# העברת מפתח קוונטית

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits








The **test bits** allow Alice and Bob to test whether the channel is secure.

# העברת מפתח קוונטית

- היות שהתנהגות הפוטונים אקראית, יצליח בוב לבצע מדידה נכונה במחצית מן המקרים בממוצע, כך שניתן להמיר כמחצית מזרם הפוטונים למפתח הצפנה אפקטיבי.
- ליתר ביטחון הם יכולים גם לוודא התאמה של רצף הסיביות שבידיהם, על ידי בדיקה מדגמית של כמה סיביות, באמצעות הערוץ הפתוח.

# העברת מפתח קוונטית

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits  
discarded

Final Key = 01

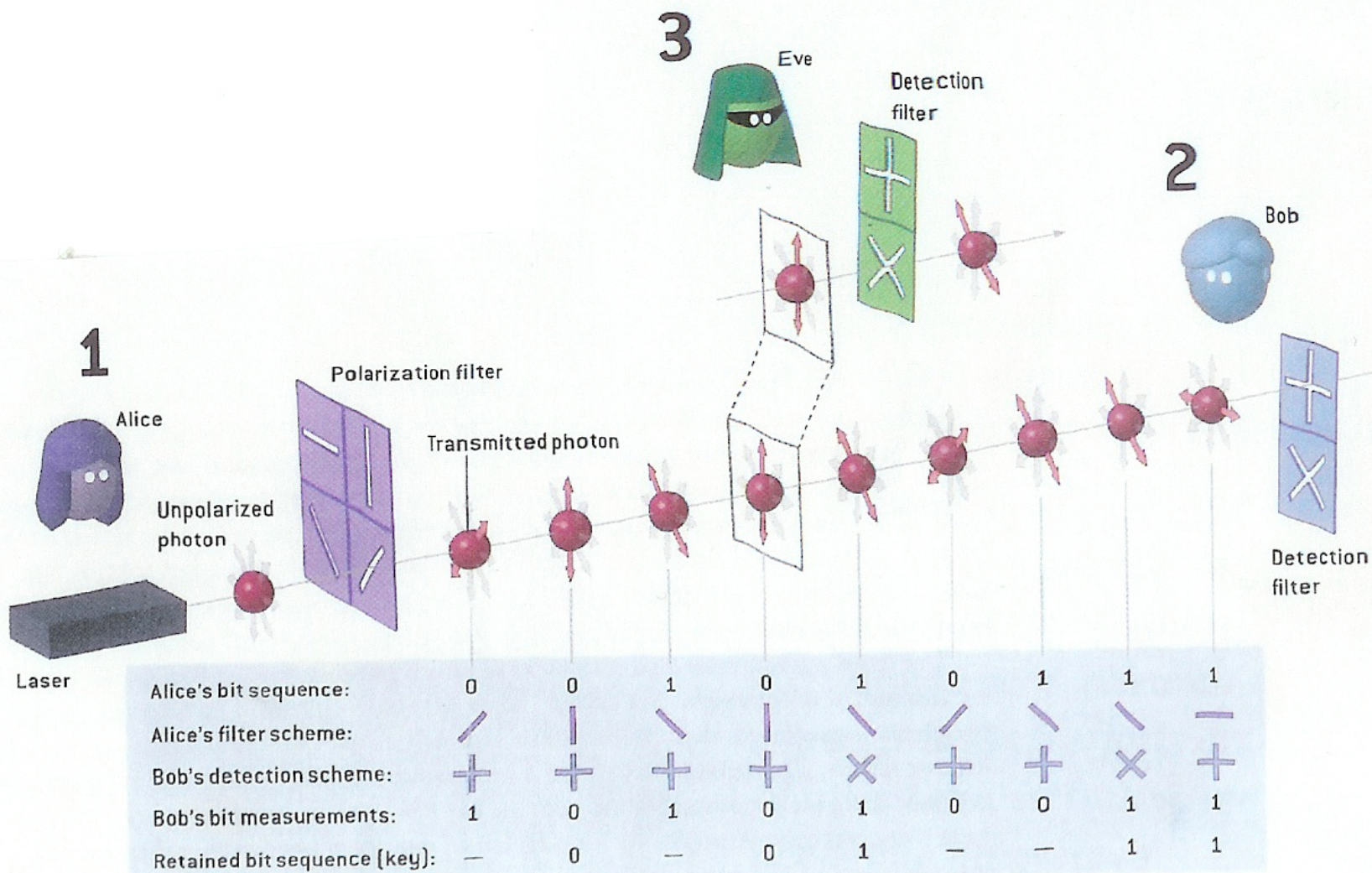


Quantum  
Cryptography  
BB84 Protocol

# בטיחות העברת מפתח קוונטית

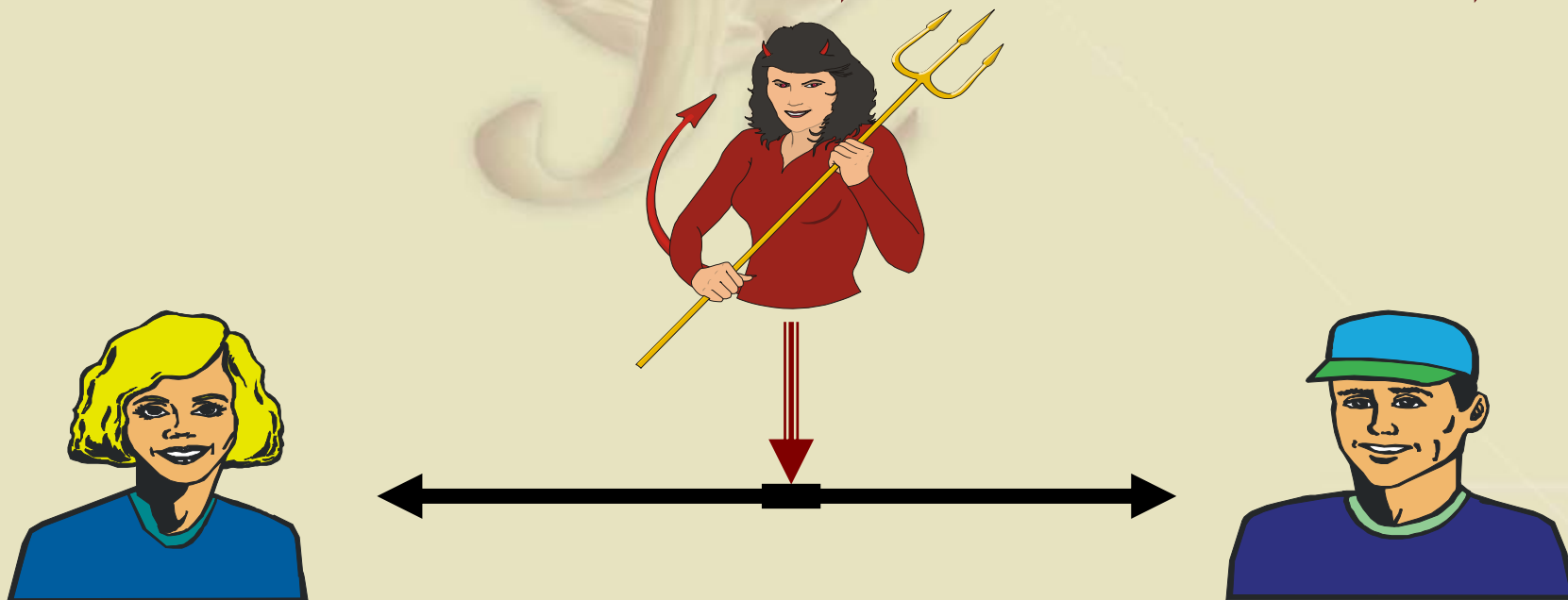
- איב (המצותתת) אינה יכולה עם כל כוח החישוב ליירט את המפתח.
- איב יכולה לחבר גלאי לערוץ התקשורת שיקלוט את זרם הפוטונים שמשדרת אליס, למדוד את קיטוביותם ולאחר מכן לשדרם הלאה לבוב.
- איב כמו בוב גם היא, **כמחצית מן המדידות שתעשה יהיו נכונות.**
- אבל איב אינה מסוגלת לדעת מה סדר המדידות שיקבע בוב אצלו, כל שהיא יכולה לעשות הוא רק לנחש.
- כל מדידה של איב למעשה הורסת את מצב הפוטון, באופן כזה שבוב עלול לקבל תוצאות שגויות גם במדידה בבסיס נכון.

# הדגמה



# בטיחות העברת מפתח קוונטית

- לאחר השידור אליס ובוב יכולים לזהות, כי זרם הפוטונים שבידיהם אינו זהה, משמע מישהו צותת לערוץ כמו בדיקת זוגיות (Parity) התאמה מעל ערוץ פתוח תוך חשיפה מינימאלית של סיביות
- בהצפנה קוונטית לא קיים מושג של "ציתות פסיבי". מצותת המנסה לחלץ את סיביות המפתח מתוך הפוטונים, ישבש בהכרח את ערוץ התקשורת ויגרום לאי התאמה בין זרם הסיביות שבידי אליס ובוב.



# QKD Protocols

- **פרוטוקול** סידרה של כללים מושלים בהחלפה של מסרים מעל ערוץ .
- פרוטוקול בטחון הוא פרוטוקול מיוחד המבטיח העברות במהלך ההתקשרות.
- **בנט וברסרד** בנו מודל מעשי של העברת מפתח קוונטית ואף הצליחו לשתף סיביות מפתח בטוחות בעזרת שולחן לייזר בלי ציטות.
- הפרוטוקול שלהם מסתמך על הפולריזציה של הפוטונים ב**סיבים** **אופטיים** .
- **סיביות המפתח** (key bits) מועברת כפוטון , כל סיבית מפתח מוצפנת עם בסיס קיטוב מקרי.

## information reconciliation & privacy amplification

הפרוטוקול של BB84 הוא לא די מאובטח בהערת המפתח בין אליס לבוב, שתי סיבות לכך :

1. הציתות של איב בקו.

2. פגמים בקיו ובגלאים.

שני השגיאות האלה לא ניתנות להבדלה. אבל בשנת 2007 נקבע סף מינימאלי לשגיאות והוא **12.9%**.

קיימים שתי שיטות בכדי להתגבר על השגיאות

1. **information reconciliation** : סילוק הביטים השגויים (erroneous bits) .

2. **privacy amplification** (הגברת הפרטיות) : הקטנת אורך המפתח כך שאיב תשיג פחות ידע.

C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin "Experimental Quantum Cryptography" Journal of Cryptology vol.5, no.1, 1992, pp. 3-28.



# information reconciliation

העיקרון של השיטה הזו להעביר מינימום מידע בכל מפתח . הפרוטוקול

המתעסק בשיטה זו נקרא **cascade protocol**

G. Brassard and L. Salvail "Secret key reconciliation by public discussion" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23 (1993)

- השיטה מתבצעת במספר סיבובים, בכל סיבוב מחולקים שני מפתחים בתוך בלוק (blocks), ולאחר מכן משווים הסיבית בלוקים.
- אם נמצא הבדל בסיבית בשלב ההשוואה, אז ניתן לחפש על השגיאה ולתקנה באופן בינארי.
- אחרי השוואת כל הבלוקים, אליס ובוב מעברים מחדש את המפתחות שלהם באותו דרך מקרית, ומתחיל סיבוב חדש.
- בסוף הסיבובים אליס ובוב יהיו בעלי מפתחות זהים עם סיכוי טוב.

# פרטיות הגברת privacy amplification

- הגברת פרטיות היא שיטה בשביל להקטין ולסלק באופן אפקטיבי את המידע החלקי שמקבלת איב על המפתח המועבר בין אליס ובוב.
- המידע החלקי הזה היה יכול להיות מועבר לאיב על ידי ציתות בערוץ הקוונטי במשך העברת המפתח ואז תתגלה השגיאה.
- הגברת פרטיות מקצרת את אורך המפתח המועבר בין אליס ובוב, בהקטנה זו איב תקבל פחות מידע ואפילו אפסי על המפתח המועבר
- תהליך זה מבוסס על universal hash function שמקבלת קוד בינארי באורך שווה למפתח ופולטת קוד בינארי קצר יותר .

# פרוטוקול לשלושה בסיסים

• דוגמה השימוש בפרוטוקול הזה biphotons ,namely, photon  
 • paris in symmetric Fock states

• Let  $|\alpha\rangle, |\beta\rangle, |\gamma\rangle$  unit vectors of one of the bases.

$$\frac{e^{\frac{2\pi i}{3}} |\alpha\rangle + |\beta\rangle + |\gamma\rangle}{\sqrt{3}} \text{ and cyclic perm}$$

$$\frac{e^{-\frac{2\pi i}{3}} |\alpha\rangle + |\beta\rangle + |\gamma\rangle}{\sqrt{3}} \text{ and cyclic perm}$$

$$|\alpha'\rangle = \frac{|\alpha\rangle + |\beta\rangle + |\delta\rangle}{\sqrt{3}}$$

$$|\beta'\rangle = \frac{|\alpha\rangle + e^{\frac{2\pi i}{3}} |\beta\rangle + e^{-\frac{2\pi i}{3}} |\gamma\rangle}{\sqrt{3}}$$

$$|\gamma'\rangle = \frac{|\alpha\rangle + e^{-\frac{2\pi i}{3}} |\beta\rangle + e^{\frac{2\pi i}{3}} |\gamma\rangle}{\sqrt{3}}$$

# פרוטוקול לשלושה בסיסים

תהליך:

- אליס בוחרת באופן אקראי אחד מ 12 הוקטורים ושולחת לבוב סיגנל אשר מהווה מידע על המצב הקוונטי של כל וקטור.
- בוב בוחר באופן אקראי אחד מארבעת הבסיסים ובוחר איזה סיגנל הוא אחד מווקטורי הבסיס.
- בסיום, בוב מודיע איזה בסיסים הוא בחר, אבל לא התוצאות שהוא קיבל.
- אליס מגלה איזה וקטורים שייכים לבסיס הנבחר מבוב.
- אם זה אותו בסיס אז משתפים המידע, אם לא ההעברה לא תצליח
- איב נכנסת לקו מקבלת מאלס ושולחת לבוב,  $3/4$  מהמקרים היא משתמשת בבסיס שגוי, לא מקבלת מידע, וגורמת להפרעה בהעברה.

# פרוטוקול לשלושה בסיסים

• אחוז השגיאה של בוב  $2/3$ . בממצוע איב מקבלת  $E_A = \frac{1}{4}$  ושגיאת בוב

$$E_B = \frac{1}{2}$$

• זה נכון לשני בסיסים בשלושה בסיסים מקבלים שליש ממה שהיה בשני בסיסים, משם איב מקבלת פחות מידע וגורמת והפרעה גדולה.

• פרוטוקול זה הוא במרחב הילברט כי וקטורי הבסיס שייכים למספר בסיסים.

• לאליס יש 21 וקטורים לבחירה, ובוב בוחר 13 בסיסים. במקרה הזה הבסיסים האלה *not mutually unbiased*, אם איב בוחרת בסיס שונה ( $12/13$  פעמים) היא עדיין תקבל לפחות סיכוי למידע מהוקטורים של אלים.

• במצב שבוב מודיע את הבסיסים שלו אלים מאשרת אותם, איב יכולה להסיק שקיבלה המצבים הנכונים ולא גרמה לשגיאות.

# פרוטוקול לשלושה בסיסים

הפרוטוקול הזה הוא בתנאי שיש ההתקפות על העברת המפתח בין אליס

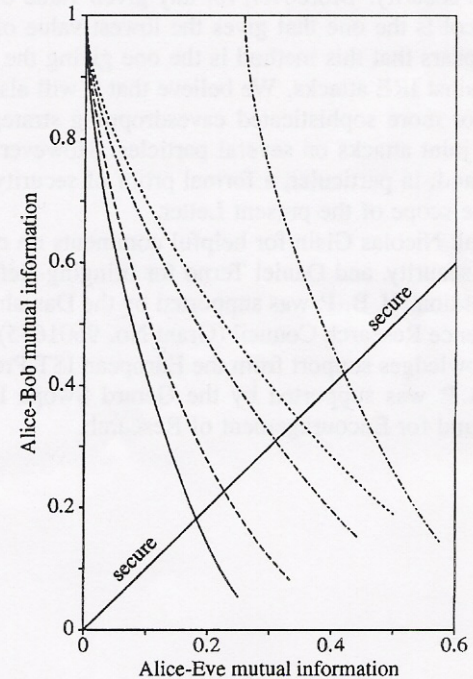
$$I_B > I_E$$

$$I_B = 1 + (1 - E_B) \log_3(1 - E_B) + E_B \log_3(E_B / 2)$$

$$I_E = (9/13)(1 + \log_3 2) = 0.255510 \text{ trit}$$

TABLE II. Result of IRE on various cryptographic protocols: Eve's information, Bob's information and error rate for a single IRE event, and the fraction of eavesdropped transmissions needed to make both informations equal to each other.

Units	Bases	Vectors	$I_E$	$I_B$	$E_B$	$x$
Bits	2	4	0.500 000	0.188 722	0.250 000	0.682 14
Bits	3	6	0.333 333	0.081 710	0.333 333	0.681 28
Trits	4	12	0.250 000	0.053 605	0.500 000	0.717 70
Trits	13	12	0.575 142	0.143 418	0.391 738	0.510 07
Trits	13	21	0.442 765	0.150 431	0.385 022	0.689 94



- ..... 2-dim., 2 bases [2]
- 2-dim., 3 bases [3,4]
- .-.-.- 3-dim., 13 bases, 12 vectors
- 3-dim., 13 bases, 21 vectors
- 3-dim., 4 mutually unbiased bases

FIG. 2. Mutual informations for the various protocols listed in Table II, when the fraction of intercepted particles is  $0 < x < 1$ . For the case of 13 bases and 12 vectors, it is assumed that in the remaining fraction  $(1 - x)$ , Eve performs passive eavesdropping on incomplete bases. The data are given in bits for 2-dimensional systems, and trits for 3-dimensional ones.



# בטיחות פרוטוקולים

