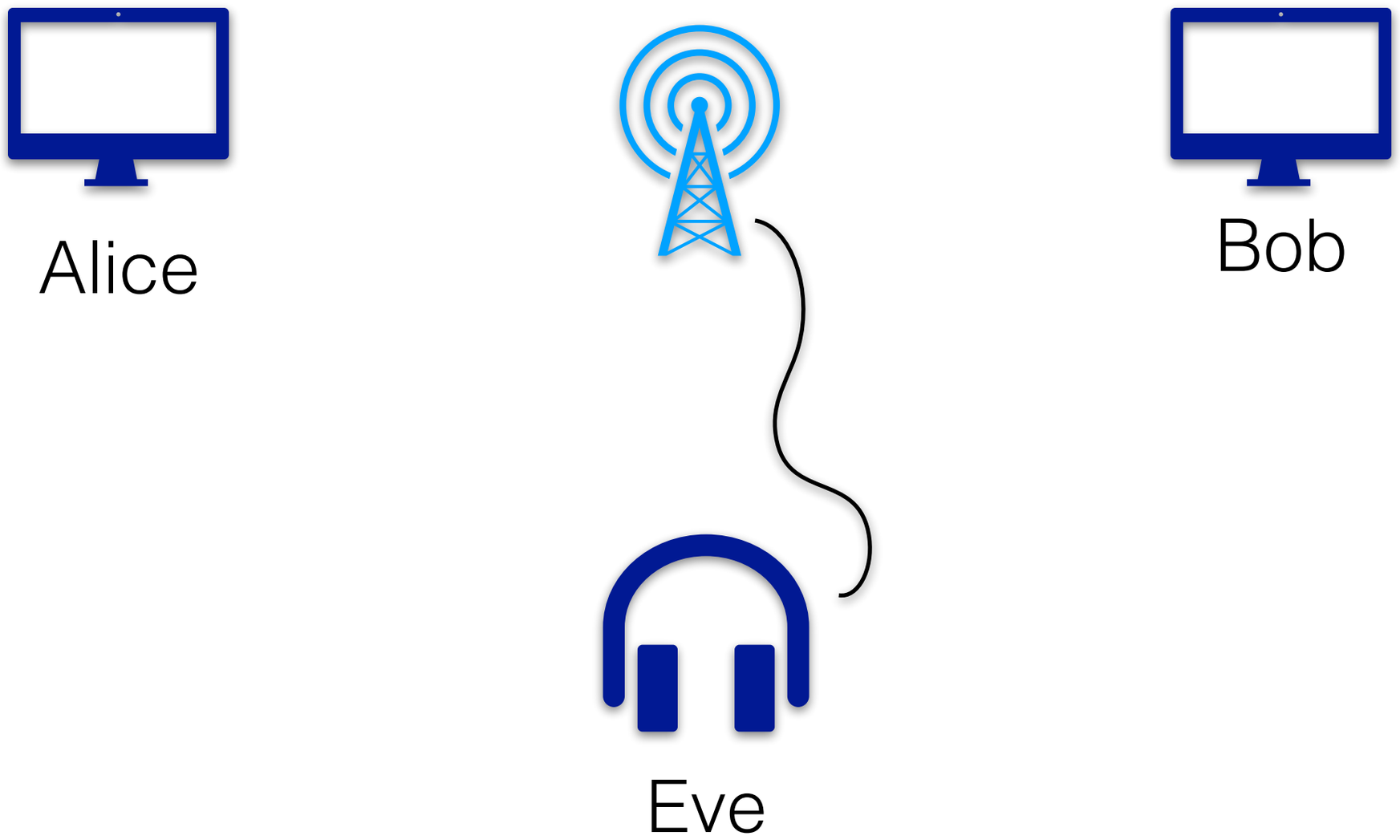
הצפנה קוונטית

6.1 הצפנה קוונטית

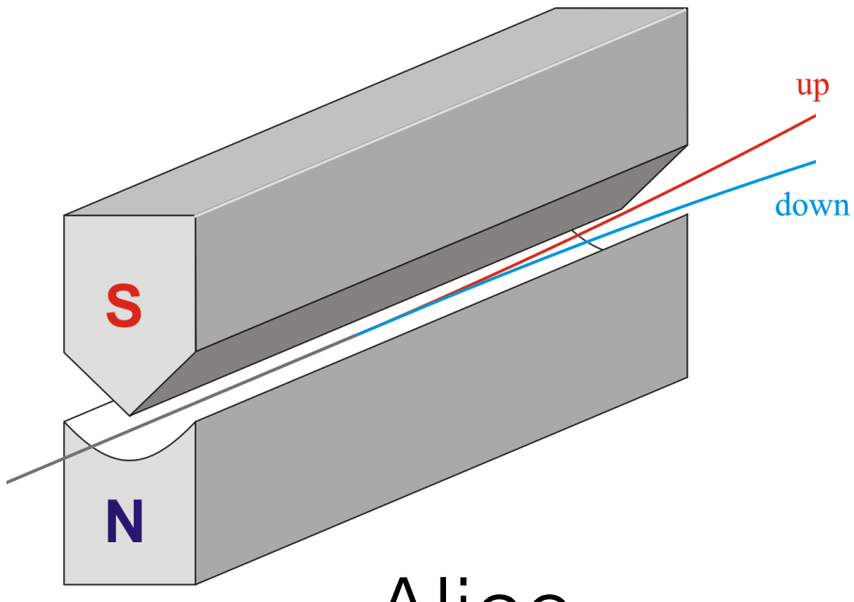


הצפנה קוונטית היא שימוש בתכונות הקיטוב של פוטונים או אלקטרונים על מנת ליצור קוד אשר משמש להצפנת מידע.

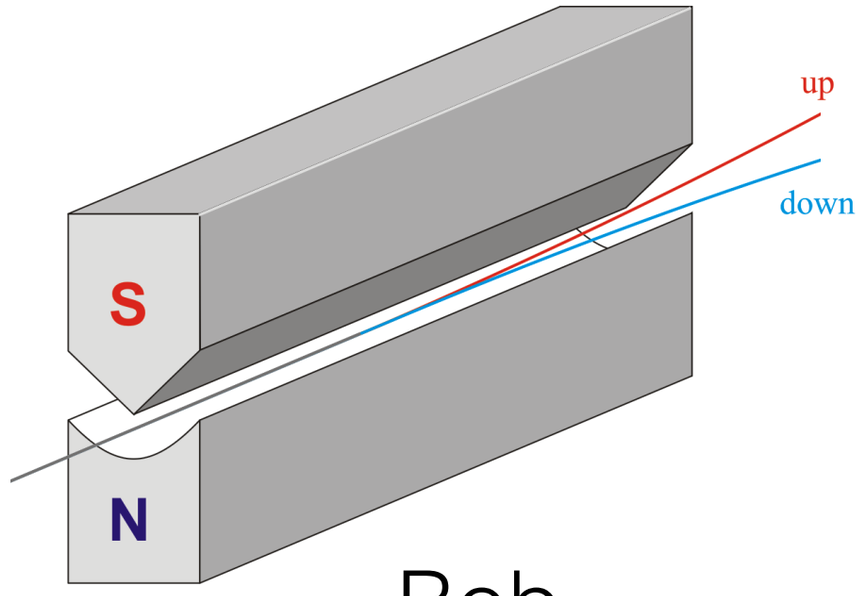
6.2 הגדרת הבסיס

Measured state	Bit recorded
$\|\uparrow\rangle$	1
$\|\downarrow\rangle$	0
$\|\rightarrow\rangle$	1
$\|\leftarrow\rangle$	0

6.3 פרצדורת הכנת הקוד



Alice



Bob

שומרים רק את התוצאות שהתקבלו במדידות שבוצעו באותו כיוון

6.3 פרצדורת הכנת הקוד

Alice Measured	Bob Measured	Code generated
$\|\uparrow\rangle$	$\|\uparrow\rangle$	1
$\|\uparrow\rangle$	$\|\downarrow\rangle$	Impossible
$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	1
$\|\leftarrow\rangle$	$\|\leftarrow\rangle$	0
$\|\uparrow\rangle$	$\|\rightarrow\rangle$	–

בשלב האחרון של הפרוצדורה נדרשת תקשורת טלפונית בלתי מוצפנת על מנת לבדוק (בדיעבד) באילו מחזורי מדידה המכשירים של אליס ובוב היו מוצבים באותו כיוון (אנכי או אפקי).

6.3 פרצדורת הכנת הקוד

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								
Shared secret key	0		1			0		1

6.4 למה זה עובד

הנקודה החשובה בהעברת המפתח - ניתן לאתר ניסיון לצותת לשדר.

זאת בגלל התכונה הבסיסית של מכניקת קוונטים שמדידה משפיעה על התוצאה