Digital Whisper
Technologic Papers

קריפטוגרפיה קוונטית

מאת גדי אלכסנדרוביץ'

במאמר זה ארצה להציג יישום חזק ומעניין של הרעיונות הבסיסיים בקוונטים שראינו עד כה עבור הצפנה. ומכיוון שזה נושא מעניין למדי אשתדל להפוך את המאמר הזה לעומד בפני עצמו ככל הניתן (למעט אולי בכניסה לחישובים הטכניים שתהיה בסוף, אחרי שהרעיונות יובהרו) כך שכל מי שנקלע לכאן מוזמן להמשיך לקרוא - ואפילו אם אתם לא מכירים מתמטיקה או קריפטוגרפיה או קוונטים. בואו נתחיל עם הסבר קצר על קריפטוגרפיה ומה שאנחנו מנסים לעשות.

הסיפור הבסיסי שבו עוסקת הקריפטוגרפיה הוא זה: אליס ובוב רוצים לתקשר זו עם זה. יש להם ערוץ תקשורת כלשהו שבו הם יכולים לשלוח הודעות זו לזה (שליח / יונת דואר / מכתב / קו טלפון / אינטרנט / איתותי עשן / דיבור פנים אל פנים) הבעיה היא שקו התקשורת **אינו בטוח**: יש מישהי בשם איב שיש לה שליטה כלשהי בקו התקשורת ומסוגלת לכל הפחות לצותת לכל המידע שעובר דרכו; במקרה הגרוע ביותר היא גם מסוגלת לטפרד הודעות שנשלחות דרך קו התקשורת ולשלוח כאלו בעצמה (לירות ביונת הדואר ולשלוח יונות דואר עם מכתבים שהיא כתבה ומתחזים למכתבים שאליס או בוב כתבו). המטרה של אליס ובוב היא להעביר מידע מבלי שאיב תוכל לדעת מה היה **תוכן** המידע הזה (כמובן שאם איב פשוט מחליטה לירות בכל יוני הדואר אז אבוד לאליס ובוב - שום מידע לא יעבור - אבל גם זה לא יעזור לאיב לגלות את **תוכן** המידע).

למה השמות המוזרים הללו, אליס בוב ואיב? אליס ובוב הם דרך נוחה לכתוב A ו-B כדי לתאר את שני הצדדים של הפרוטוקול (אני מעדיף אותם על עברותים או וריאציות, למרות ש"אריק ובנץ" חביב עלי) ו"איב" באנגלית היא Eve, מה שנשמע כמו ההתחלה של Eavesdropper. בעברית משחק המילים לא קיים אבל מילא.

האופן שבו נפתרת הבעיה של אליס ובוב היא באמצעות שימוש ב**הצפנה**. הצפנה פירושה שלוקחים טקסט קריא והופכים אותו לג'יבריש לא קריא, שולחים לצד השני ואז הוא עושה קסם שמפענח את הג'יבריש חזרה לטקסט קריא, כאשר ההצפנה והפענוח מסתמכים על מידע סודי כלשהו - נאמר, סמא. ייתכן מאוד שרובכם השתמשתם בהצפנה בצורה מודעת, אם בתור משחק ואם בצורה קצת יותר מחוכמת (למשל, קובץ zip עם סמא). פרט לכך בעידן האינטרנט רובנו משתמשים בהצפנה בצורה לא מודעת כל הזמן (למשל, בכל גישה לשרת הדואר שלנו הגישה מוצפנת אוטומטית על ידי הדפדפן - לפחות אני מקווה שזה כך עם שרת הדואר שלכם!). אם השתמשתם בהצפנה בצורה מודעת אתם כנראה יודעים שמה שחשוב הוא ששני הצדדים ידעו את **שיטת** ההצפנה, אבל ברוב המוחלט של המקרים גם צריך לדעת

מידע סודי כלשהו בנוסף לשיטת ההצפנה (שעדיף לא להניח שהיא סודית) - מין סמא משותפת שכזו. למידע הסודי הזה קוראים בקריפטוגרפיה **מפתח**.

בימינו, אם לאליס ובוב יש מפתח משותף, מצבם טוב מאוד; יש שיטות הצפנה חזקות ומהירות שמאפשרות להם להשתמש במפתח קטן יחסית כדי לשלוח כמויות גדולות מאוד של מידע במהירות בצורה מוצפנת. השיטה המוכרת ביותר נקראת AES, ומפתח סטנדרטי בה הוא יחסית קטנטן - בן 256 סיביות (סיבית - "ביט" - היא או 0 או 1, יחידת המידע הבסיסית ביותר במחשב). יש גם שיטות הצפנה שהבטיחות שלהן מושלמת - אין שום דרך לפרוץ אותן, ויש לזה הוכחה מתמטית - ב"מחיר" של שימוש במפתח גדול יותר (גודל המפתח צריך להיות שווה לגודל המידע ששולחים). בקיצור, הבעיה הזו היא (יחסית) פתורה ולא עליה אני הולך לדבר במאמר הזה.

הבעיה המהותית יותר בקריפטוגרפיה היא מה שנקרא "בעיית החלפת המפתח". איך אליס ובוב יגיעו מלכתחילה למצב שבו יש להם מפתח משותף? ובכן, ביטוי המפתח פה הוא **ערוץ תקשורת מאובטח**. זה יכול לומר שאליס ובוב נפגשים פיזית ויושבים באותו חדר ואליס לוחשת לבוב סמא באוזן; זה יכול להיות שליח מסור שמקבל לידו מחברת קודים ומעביר אותה ליעדה תוך שהוא יורה בכל מרגלי האויב שמנסים לעצור אותו; וזה יכול להיות קו טלפון פיזי עם מיגון סופר-דופר-מתוחכם שמונע מכוחות הרוע להתקרב אליו. בקיצור, כל ערוץ תקשורת שלאיב פשוט אין גישה אליו. לרוב השימוש בערוץ תקשורת מאובטח הוא יקר משמעותית יותר מאשר להשתמש בתקשורת לא מאובטחת אבל עם הצפנה, ולכן משתמשים בערוץ התקשורת המאובטח הזה כדי להחליף מפתח ותו לא, ואז עוברים לדבר עם הצפנה בערוץ תקשורת לא מאובטח.

ערוצי תקשורת מאובטחים היו הפתרון לבעיית החלפת המפתח במשך אלפי שנים, אבל בימינו הם לא מסוגלים לפתור את הבעיה עבור כולנו. כפי שכבר רמזתי, באינטרנט אנחנו משתמשים שוב ושוב בהצפנה בתקשורת עם אתרים שמעולם לא היה לנו ערוץ תקשורת מאובטח איתם (גוגל לא שלחו ג'יימס בונד עם מעטפה שהעביר לכם את הסמא הראשונית שלכם, ואני טוען שהם בכל זאת עבדו בצורה יותר בטוחה מאשר בנק ששולח לכם סמא בדואר). אז הבעיה שאנחנו מנסים לפתור כרגע היא זו - איך לשתף מפתח **בלי** ערוץ תקשורת מאובטח?

פתרונות לבעיה הזו הם חדשים יחסית. הפתרון הראשון שפורסם הוא זה של דיפי והלמן שפורסם ב-1976 (המודיעין הבריטי גילה אותו באופן בלתי תלוי כמה שנים לפני כן אבל שמר אותו בסוד). השיטה של דיפי והלמן היא מבריקה; היא מאפשרת לאליס ובוב ליצור מפתח משותף תוך שימוש בערוץ תקשורת לא מאובטח, כך שאם איב מצותתת לערוץ התקשורת היא **לא תוכל לדעת** מה המפתח המשותף למרות שהוא נוצר מתוך התשדורות שאליס ובוב שולחים זו לזה. אז אם הכל כל כך טוב, מה הבעיה? הבעיה היא שהשיטה מגנה היטב מפני הסיטואציה שבה איב יכולה רק **לצותת** לערוץ התקשורת, אבל אם לאיב יש יכולת גם **לשלוט** על ערוץ התקשורת, כלומר לטרפד הודעות ולשלוח אחרות במקומן, אז דיפי-הלמן

קורסת לחלוטין בצורה מחרידה. מה שאיב מסוגלת לעשות היא להתחזות לאליס בפני בוב, להתחזות לבוב בפני אליס, לתת לשניהם את הרושם שהם הצליחו לשתף מפתח זו עם זה, ואז לשלוט בצורה מוחלטת בכל הודעה שהם שולחים - לקרוא אותה, לשנות בה כל מה שהיא רוצה ולהעביר הלאה. לא רק שקו התקשורת של אליס ובוב לא יהיה בטוח, אלא גם שלא תהיה להם שום אינדיקציה לכך שבכלל יש בעיה. בקיצור - דיפי-הלמן, בגרסה הנאיבית שלו, הוא בעייתי.

אז מה הפתרון שבו משתמשים כיום באינטרנט? שיטה יותר מתוחכמת שנקראת **הצפנת מפתח ציבורי**. בהצפנה כזו, יש לאליס **שתי** סמאות - סודית (פרטית) וידועה לכל העולם (ציבורית). כשבוב רוצה לשלוח לאליס הודעה, הוא מצפין אותה עם המפתח הציבורי; מאותו רגע והלאה הדרך היחידה לפענח את ההודעה היא עם השימוש במפתח הפרטי של אליס. איך מתבצע הקסם הזה? ובכן, מתמטיקה. יש הרבה מערכות שונות שממממשות הצפנת מפתח ציבורי בדרכים שונות; המפורסמת שבהן היא RSA [ויש לי פוסט על איך היא עובדת]; לא אכנס לפרטים כעת. עכשיו, בהצפנת מפתח ציבורי שכזו אפשר להשתמש תיאורטית גם לתקשורת באופן כללי; בפועל, הצפנה כזו היא איטית וכבדה יותר מהצפנה "רגילה" (סימטרית) ולכן משתמשים בה בעיקר להחלפת מפתח, שאחרי משתמשים באלגוריתם כמו AES כדי לשלוח את עיקר התקשורת.

אז מה **עדיין** הבעיה? שכדי לשלוח לאליס הודעה סודית, בוב צריך לדעת את המפתח הפומבי שלה. מאיפה הוא משיג אותו? ובכן, מהאינטרנט, ולרוב מאליס עצמה. אבל מי מבטיח לו שהמפתח הפומבי של אליס שהוא קיבל הוא המפתח האמיתי של אליס ושאיב לא התחזתה לאליס ושלחה לו מפתח ציבורי שהוא בכלל לא המפתח של אליס? ובכן, התשובה היא שזה מסובך. יש משהו שנקרא "תשתית מפתח ציבורי" שבה גופים אמינים חותמים קריפטוגרפית על מפתחות של גופים אחרים כדי להבטיח שהם אותנטיים, ואז צריך רק לדעת את המפתחות של הגופים האמינים (וזה מידע שיש בתוך הדפדפן שלכם - אבל מי מבטיח שהדפדפן שהורדתם אכן אמין?). בקיצור, זה לא פתרון מושלם, למרות שהוא עובד טוב בפועל ובלעדיו האינטרנט לא היה מה שאנחנו מכירים כיום.

וכאן סוף סוף נכנסת תורת הקוונטים לתמונה. כרגיל בעניינים כאלו, תיאורי מדע-פופולרי (למשל, זה) עושים סמטוחה אחת גדולה מכל העסק. הם לרוב משתמשים בביטוי "הצפנה קוונטית" כדי לדבר על שני דברים עיקריים שאף אחד מהם אינו הצפנה והם אינם קשורים אחד לשני בשום צורה. הראשון הוא שימוש בחישוב קוונטי כדי **לפרוץ** מערכות הצפנה פומביות כדוגמת RSA (שכדי לפרוץ אותה מספיק לפתור ביעילות את בעיית הפירוק לגורמים של מספרים גדולים). אני מתכנן לדבר על זה בהמשך, אבל זה לא קשור לנושא מאמר זה. הדבר השני שמדובר עליו הוא **שיתוף מפתח** באמצעות ערוץ תקשורת קוונטי, וזה מה שאדבר עליו במאמר זה. השם "ערוץ תקשורת קוונטי" נשמע מפוצץ, אבל בפועל ערוץ תקשורת שכזה יכול להיות, למשל, סיב אופטי שמעביר פוטונים. זה עדיין לא אומר שערוץ תקשורת שכזה הוא יעיל לשימוש, בטח לא כמו ערוצים תקשורת "רגילים", אבל כבר כיום שיתוף מפתחות קוונטי הוא משהו שעושים בפועל וממשיכים לעבוד עליו (השאלה המרכזית שנשאלת היא לא אם זה אפשרי -

השאלה שנשאלת לגבי חישוב קוונטי יעיל - אלא אם יש טעם להקדיש לזה מאמצים בזמן שתשתיות המפתח הציבורי הרגילות עושות את העבודה טוב).

ערוץ תקשורת קוונטי הוא **לא** ערוץ מאובטח בשום צורה - איב יכולה לצותת למה שעובר בו ויכולה לטרפד הודעות ולשלוח הודעות משלה; אלא שהקסם הוא שתורת הקוונטים מונעת ממנה לבצע מניפולציות מתוחכמות **מדי**. השורה התחתונה של שיתוף מפתח באמצעות ערוץ קוונטי ופרוטוקול חכם לשיתוף מפתח היא זו: לאיב **אין שום דרך** לגלות מה המפתח שאליס ובוב שיתפו; ואם איב תנסה לצותת לאליס ובוב או לשנות הודעה כלשהי שלהם, אליס ובוב **יהיו מודעים** לכך (לא בודאות של 100 אחוז, אבל בודאות טובה מאוד - לפרטים נגיע בהמשך). בקיצור, תורת הקוונטים עושה קסם. אבל איך הקסם הזה עובד? כאמור, יש כאן פרוטוקול שצריך להסביר את פרטיו הטכניים, שהם לא נוראיים בכלל ואפילו די פשוטים, אבל עדיין יותר מתוחכמים מאשר "אליס שולחת לבוב את המפתח שלה בערוץ תקשורת קוונטי ואם איב תנסה לקרוא אותו המפתח ייהרס הסוף" (למשל כאן אפשר לראות תיאור ברוח זו). כמו כן, הפרוטוקול שאני אציג לא משתמש **בכלל** בתופעת השזירה שדיברתי עליה במאמרים קודמים. קיימים פרוטוקולים שכן מתבססים על שזירה, אבל לא כולם כאלו.

מה הרעיון באלגוריתם? מכיוון שאני מנסה לשמור את המאמר הזה עצמאי מהיתר, אתחיל עם הסבר אינטואיטיבי שישתמש באנלוגיה, ורק אחר כך אגש לניסוח הפורמליסטי. האנלוגיה עוסקת באופן ישיר בתכונה של תורת הקוונטים שאנחנו מנצלים כאן - העובדה שקיוביט יכול להימדד ביחס לשני בסיסים שונים, כאשר כל מדידה "מקלקלת" את חברתה.

ובכן, נניח שאנחנו כימאים מתחילים ואנחנו מקבלים אבקה לבנה שאנו תוהים על קנקנה. אנחנו יודעים שהאבקה היא אחד מבין ארבעה חומרים: סוכר, מלח, קמח או חימר. מה עושים? מה שהכימאי מנצל תמיד הוא **תכונות כימיות** של החומר שהוא בודק. אפשר כמובן לטעום את החומר, או להסתכל עליו במיקרוסקופ או שלל ניסויים שונים, אבל בואו נניח שיש בדיוק שני ניסויים שהכימאי המתחיל יודע לבצע: ראשית, הוא יכול לשפוך מים על החומר ולראות מה קורה; ושנית, הוא יכול לנסות להצית את החומר ולראות מה קורה.

כאשר שופכים מים על סוכר או מלח הם **מתמוססים** במים ונעלמים; לעומת זאת אם שופכים מים על חימר או קמח מקבלים עיסה. אם כן, הרטבה במים היא דרך להבדיל בין מלח וסוכר ובין קמח וחימר. כמו כן, סוכר וקמח הם דליקים (אל תנסו את זה בבית!) בעוד שמלח וחימר לא, ולכן הבערה היא דרך להבדיל בין סוכר וקמח ובין מלח וחימר. אם כן, עומדים לרשות הכימאי שני ניסויים, אבל האם הם יאפשרו לו לדעת בודאות מה החומר? אם שפכנו מים על החומר וקיבלנו עיסה, לא נוכל להדליק אותו יותר; ואם הדלקנו את החומר והוא בער, לא נוכל לשפוך עליו מים ולראות מה קורה. כל ניסוי "הרס" את היכולת שלנו לבצע ניסוי אחר. כמובן, בעולם האמיתי אפשר להתחכם - לחלק את האבקה לשתי ערימות, לשפוך

מים על אחת ולהבעיר את השניה; ואפשר להתחכם עוד יותר - אם החומר התמוסס במים אפשר לאדות את המים ולקבל את החומר מחדש וכדומה. אז אנא - רחמו עלי וזכרו שמדובר על אנלוגיה.

עכשיו אפשר להציג את שיטת ההצפנה הקוונטית בלי להשתמש בכלל בקוונטים, אלא רק באבקה הלבנה שלנו. אליס רוצה לשלוח לבוב ביט יחיד של מידע, שנסמן b. הדבר הראשון שהיא עושה הוא להטיל מטבע ולסמן את התוצאה שלו ב-a. ועכשיו היא שולחת משהו לבוב, על פי הכללים הבאים:

1. $a = 0$, $b = 0$ - שולחת תערובת של מלח וסוכר.
2. $a = 0$, $b = 1$ - שולחת תערובת של קמח וחימר.
3. $a = 1$, $b = 0$ - שולחת תערובת של מלח וחימר.
4. $a = 1$, $b = 1$ - שולחת תערובת של סוכר וקמח.

בוב מקבל את האבקה. אם בוב היה יכול לדעת בודאות מהי האבקה, הוא היה יודע מהם a ו-b של אליס - העניין הוא שהוא לא יכול לדעת בודאות מה האבקה. הוא יכול או לשפוך עליה מים, או לשרוף אותה. אז מה הוא יעשה? הוא **יגריל** את הבדיקה שהוא רוצה לעשות, שוב על ידי הטלת מטבע. נקרא לתוצאה של המטבע שלו a'. אם הוא קיבל 0, אז הוא **מנחש** שגם אליס קיבלה a ולכן החומר הוא תערובת של מלח וסוכר, או קמח וחימר. איך אפשר להבדיל? בקלות: הוא **שופך מים** על האבקה. אם היא התמוססה אז בוב מסמן לעצמו $b'=0$ ואחרת הוא מסמן לעצמו $b'=1$.

באופן דומה, אם בוב קיבל $a'=1$ הוא מנחש שהחומר הוא או תערובת של מלח וחימר, או תערובת של סוכר וקמח. ואז היא **מדליק את האבקה** ורואה אם היא בוערת. אם לא, אז $b'=0$, ואם כן, אז $b'=1$.

אבל מה קורה אם בוב ניחש לא נכון? נאמר, אם אליס הגרילה $a=0$ ובוב הגריל $a'=1$? במקרה זה בוב ינסה להצית תערובת של מלח וסוכר, או תערובת של קמח וחימר. עכשיו, בעולם האמיתי מה שיקרה הוא שחלק מהתערובת יבער וחלק לא, אבל אני רוצה להמשיך את האנלוגיה לתורת הקוונטים, אז בואו תזרמו איתי למרות שאני לא מדויק פיזיקלית: אני מניח שמה שיקרה כשבוב מנסה להצית תערובת של מלח וסוכר הוא ש**או שהכל יבער או ששום דבר לא יבער**, כשיש הסתברות $\frac{1}{2}$ לכל אחד מהמקרים. ואני מניח שתופעה מוזרה דומה תתרחש גם עם שפיכת מים על תערובת של מלח וחימר או על תערובת של סוכר וקמח - או שהכל יתמוסס, או ששום דבר לא יתמוסס. בעולם האמיתי זה לא יקרה (למרות שאולי אפשר למצוא אנלוג כימי שבו זה כן קורה; הידע שלי בכימיה עלוב), אבל במודל הקוונטי זה יקרה ועוד איך ואסביר בדיוק איך. בכל אחד מהמקרים בוב יקבל ערך b' שהוא אקראי, ולכן חסר ערך (בוב יכל לנחש את b' בעצמו באותה מידה), אבל בוב **לא ידע** שהערך חסר ערך, לא בשלב הזה.

אליס תחזור על המשחק הזה מספר גדול של פעמים ותשלח לבוב הרבה אבקות; מה שקורה הוא שהיא מקודדת סדרת ביטים $b_1,b_2,\ldots,b_n$ כאשר ההחלטה על אופן הקידוד נתונה על ידי סדרת ביטים אחרת, $a_1,\ldots,a_n$. בצד של בוב נוצרת סדרת ביטים שהתקבלו, $b'_1,\ldots,b'_n$ על פי בחירות שבוב ביצע, $a'_1,\ldots,a'_n$.

כשהעסק מסתיים בוב מודיע לאליס שהוא גמר את כל הניתוחים הכימיים שלו, ואז אליס שולחת לו **בערוץ גלוי ולא קוונטי** את הסדרה $a_1,...,a_n$ שמתארת מה היו הניסויים ה"נכונים" שבוב היה צריך לבצע.

מה בוב עושה? לכל i, הוא בודק אם $a_i=a'_i$. אם $a_i=a'_i$ בוב יודע שהניסוי שביצע הוא הניסוי הנכון, ולכן $b_i=b'_i$ - איזה יופי, הביט b_i עבר מאליס אל בוב. אם לעומת זאת $a_i\neq a'_i$ אז בוב מבין שהביט b'_i היה אקראי לגמרי, ולכן הוא זורק אותו לפח ושוכח ממנו. הוא שולח לאליס את הסדרה $a'_1,...,a'_n$ שלו, ועכשיו גם אליס יודעת אילו מהביטים שלה עברו, ועכשיו סיימנו - אליס ובוב חולקים סדרת ביטים. כמה? בערך חצי מהביטים שאליס שלחה יעברו בצורה הזו.

יפה, הבנו איך הפרוטקול עובד, אבל למה הוא בטוח? מה קורה אם איב מנסה להתערב?

ראשית, אם איב רק מצותתת, היא בוודאי לא מסוגלת להפיק אינפורמציה - היא רואה רק אבקה לבנה וזה לא אומר כלום. כדי להפיק מידע כלשהו על האבקה היא צריכה **למדוד** אותה - לשפוך עליה מים או להצית אותה. אחרי שהיא עושה דבר כזה, האבקה נהרסת. אם איב לא תשלח לבוב אבקה, בוב יבין שמשהו השתבש - הוא ציפה לקבל אבקה מאליס ולא קיבל. לכן איב חייבת לשלוח לבוב אבקה. הבעיה היא שאיב **לא יודעת מה לשלוח**. נאמר, למשל, שהיא ניסתה להבעיר את האבקה והאבקה אכן בערה; אז איב יכולה לחשוב שאליס שלחה סוכר וקמח, אבל זה לא המקרה היחיד - גם אם אליס שלחה מלח וסוכר, או קמח וחימר, אז ייתכן שהאבקה תבער. עכשיו איב בצרות - היא לא יודעת בודאות מה אליס שלחה לבוב, ואם היא תשלח לבוב את הדבר הלא נכון, זה עשוי להוביל לכך שבוב ואליס יחשבו שהם מסכימים על ביט כלשהו למרות שבפועל הביט הזה אצלם הוא הפוך. זו נראית כמו בעיה של אליס ובוב, אבל זו למעשה בעיה של איב: כדי לשמור על בטיחות, אליס ובוב יכולים לקחת כמות מסויימת (נאמר, חצי?) מהביטים שהם הסכימו עליהם, ולפרסם אותם בפומבי זה לזו. זה כמובן יהפוך את הביטים הללו לחסרי ערך מבחינת השימוש בהם (כי עכשיו כל העולם מכיר אותם) אבל זה יאפשר לאליס ובוב להבחין ברמאות בסבירות טובה ("רגע אחד!" אתם צועקים, "אבל מה אם איב שולטת על הערוץ שבו הם מפרסמים זו לזה את הביטים?". ובכן, שאלה טובה, כפי שאתם רואים קריפטו זה עסק מתוסבך - לא מספיק שיש פרוטוקול "נקי", צריך איכשהו לנטרל את העולם החיצוני ה"מלוכלך" שבו הוא פועל).

ועכשיו, משהסיפור נגמר, בואו נתחיל להתעסק איתו בצורה קצת יותר מדויקת, למרות שאולי זה יגרום לי לאבד את חלקכם. נתחיל דווקא בהכרזה פשוטה שבעולם האמיתי המצב הוא, כמובן, מסובך יותר. הסיבה לכך היא שבעולם האמיתי, ערוצי תקשורת הם **רועשים**. כלומר, מידע שמעבירים בהם עשוי להתקלקל גם בלי שום איב מרושעת באמצע. הרעש הזה הוא לא בעיה זניחה - יש תחום שלם במדעי המחשב שמתעסק בשאלה כיצד ניתן לטפל בו וכיצד ניתן לתקשר גם בערוץ "מלוכלך". לא אכנס לפרטים הללו - ולשאלה איך פותרים את הבעיה במקרה של הצפנה קוונטית - בכלל.

בואו נעבור עכשיו לתיאור המתמטי של הפרוטוקול, בלי אבקות לבנות אבל עם מצבים קוונטיים. אנחנו מתחילים כמו קודם - לאליס יש ביט b שהיא רוצה לשלוח והיא מגרילה a. ה-a הזה בוחר **בסיס** למרחב שמתאר קיוביט בודד. הבסיס ה"רגיל" כולל את האיברים $|0\rangle$ ו-$|1\rangle$, וזה יהיה הבסיס שבו אליס תשתמש אם a=0. הבסיס השני יהיה בנוי משני איברים שהם "תערובת חצי-חצי" של אברי הבסיס הרגיל: $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ ו-$|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. שני המצבים הללו מעניינים כי אם נקבל אחד מהם ונמדוד אותו ביחס לבסיס הסטנדרטי נקבל $|0\rangle$ בהסתברות חצי ו-$|1\rangle$ בהסתברות חצי, בלי קשר לשאלה אם קיבלנו את $|+\rangle$ או את $|-\rangle$. במילים אחרות, **מבחינת הבסיס הסטנדרטי** אין הבדל בין $|+\rangle$ ובין $|-\rangle$ למרות שבבסיס "שלהם" הם כמובן שונים לגמרי. באופן דומה, מדידה של $|0\rangle$ או $|1\rangle$ ביחס לבסיס $|+\rangle,|-\rangle$ תניב את אחד מאברי הבסיס בהסתברות חצי.

הסיטואציה הזו מדגישה נקודה עדינה במודל המתמטי של תורת הקוונטים, שיצא לי לראות אנשים מפספסים פה ושם: **מצב קוונטי הוא הרבה יותר מסתם הסתברויות**. אם אני אומר "יש לי מצב קוונטי, ואם מודדים אותו ביחס לבסיס $|0\rangle,|1\rangle$ אז מקבלים כל איבר בסיס בהסתברות חצי" זה **ממש לא** מאפיין את המצב בשלמותו. המידע השלם על המצב נמצא בתוך המקדמים של המצב, וההסתברויות הן רק הערך-המוחלט-בריבוע של אותם מקדמים - המעבר הזה מ"מקדם" אל "ערך מוחלט בריבוע של מקדם" גורם **לאובדן מידע**, והמידע הזה, כפי שניתן לראות בדוגמה שלנו למשל, הוא קריטי לחלוטין.

אם לסכם, מה שאליס שולחת נקבע כך:

1. a=0,b=0 - שולחת $|0\rangle$.
2. a=0,b=1 - שולחת $|1\rangle$.
3. a=1,b=0 - שולחת $|+\rangle$.
4. a=1,b=1 - שולחת $|-\rangle$.

בוב, בצד שלו, מנחש a'. אם a'=0 הוא מודד לפי הבסיס $|0\rangle,|1\rangle$ וקובע את b' בהתאם, ואם a'=1 הוא מודד לפי הבסיס $|+\rangle,|-\rangle$.

ככה אליס ובוב יוצרים סדרה של ביטים, ובסוף שולחים את ה-a-ים שלהם זו לזה, משווים, זורקים את ה-b-ים עבור המקומות שבהם ה-a-ים היו שונים, ושומרים את היתר. זה כל הפרוטוקול.

בואו ננתח עכשיו את ההסתברות של איב "לקלקל" אם היא מנסה למדוד את הביטים שאליס שלחה. הכל סימטרי, אז מספיק להסתכל על מקרה יחיד. איב צריכה לנחש בעצמה מה היה ה-a של אליס. אם היא ניחשה את ה-a הנכון, מה חבל; נניח שהיא תמיד שולחת לבוב קיוביט תקין שזהה למה שאליס שלחה. אז

בהסתברות $\frac{1}{2}$ איב מצליחה לצותת. מה קורה במקרה שבו איב לא ניחשה את ה-a הנכון? במצב זה, איב תקבל ביט חסר משמעות, כמובן. עם זאת, היא תבין שהביט היה חסר משמעות כאשר אליס, בסיום הפרוטוקול, תשלח את רשימת ה-a-ים שלה. לכן זה שאיב קיבלה ביט חסר משמעות היא לא מה שרלוונטי כאן, אלא מה שאיב תשלח הלאה עבור בוב, והאם בוב ישים לב לכך שמשהו השתבש.

ניתוח קריפטוגרפי מלא של הסיטואציה חייב לכסות כל אסטרטגיה אפשרית של איב. אני לא אכנס לזה ופשוט נראה מה קורה אם איב מתנהגת בצורה שעל פניו נראית הכי אפקטיבית - אחרי המדידה שלה היא שולחת את המצב הקוונטי שקיבלה אל בוב. זה מבטיח שאם היא ניחשה את a נכון, אז בוב לא יוכל לשים לב לכך שמשהו השתבש. זה אמנם נכון, אבל כאמור - בהסתברות $\frac{1}{2}$ זה לא מה שקורה. ואז, אם בוב בחר עבור הביט הזה את a הנכון מבחינת אליס, זה אומר שהוא מודד את הביט שאיב שלחה לו בבסיס **שהביט לא נמצא באף איבר שלו**, כלומר שהוא נמצא "באמצע" שלו ויש סיכוי של $\frac{1}{2}$ לקריסה לכל אחד מאברי הבסיס - בפרט, סיכוי של $\frac{1}{2}$ שבוב ימדוד את הביט הלא נכון. זה אומר שאם איב מצותתת לכל הביטים, אז מבין הביטים שה-a-ים של אליס ובוב מסכימים עליהם, בערך רבע מתוכם יהיו "מקולקלים".

זה הרעיון; יש כמובן עוד פרטים לדבר עליהם, ועוד שיטות שיתוף מפתחות קוונטיות, אבל צריך להשאיר משהו לפעם הבאה.

יש רק עניין אחד שאני רוצה לדון בו לסיום. כל עוד היינו בדוגמת האבקה הלבנה היינו יכולים תמיד להתחכם ולומר שאיב תערוך ניסוי על חצי מהאבקה ותשלח לבוב את היתר. אבל בקוונטים, לכאורה, זה לא קורה. וזו בעצם השאלה - למה? האם איב לא יכולה לקחת את המצב הקוונטי שקיבלה, נסמן אותו $|\psi\rangle$ כדי להדגיש שזה מצב כללי כלשהו, ו**לשכפל** אותו? ליצור לעצמה עוד קיוביט שגם הוא במצב $|\psi\rangle$, למדוד את הקיוביט המשוכפל הזה ולשלוח הלאה אל בוב את הקיוביט המקורי? בסך הכל, בחישוב "רגיל" אין בעיה לשכפל דברים. שלחתם אימייל? שכפלתם את התוכן שלו. שמרתם עותק גיבוי של קובץ? שכפלתם את התוכן שלו. האם אי אפשר לשכפל מצב קוונטי? ובכן, **לא**!

הטענה שלא ניתן לשכפל מצב קוונטי היא טענה מתמטית, עם הוכחה מתמטית, שמבוססת על האקסיומות הפשוטות שיש לנו עבור תורת הקוונטים. זו לא תוצאה פיזיקלית; דהיינו, אני לא יכול לשלול את הטענה שכן ניתן לשכפל מצב קוונטי כלשהו. אני רק אומר שאם מישהו ידגים שהוא מסוגל לעשות את זה, זה יאמר שהפורמליזם המתמטי הנוכחי של תורת הקוונטים אינו מספק ואינו תואם את העובדות בשטח. משפרסמתי את דברי ההבהרה הללו, בואו נעבור להוכיח את המשפט, שבאנגלית נקרא No cloning theorem.

ההוכחה היא פשוטה בצורה מגוחכת. אנחנו מתחילים עם מערכת קוונטית במצב כללי $|\psi\rangle$ שאיננו יודעים מהו (אם אנחנו כן יודעים מה המצב, ייתכן מאוד שנוכל לשכפל אותו פשוט על ידי יצירה בצד של מערכת חדשה במצב הזה; כפי ששמתם לב, אני נוטה להניח שאנחנו יודעים לייצר מערכות במצב נתון ספציפי),

ועם עותק נפרד של המערכת שנמצא במצב "התחלתי" כלשהו שאנחנו לא מניחים עליו כלום, $|s\rangle$. בין שתי המערכות אין קורלציה בהתחלה, ולכן המערכת שמורכבת משתיהן מתוארת על ידי הוקטור $|\psi\rangle \otimes |s\rangle$. עכשיו, הדינמיקה של המערכת (האופן שבו היא משתנה בזמן) כוללת שתי אפשרויות - או ביצוע מדידה שמקריס את המערכת - אבל אז, הוא הורס את המצב הקוונטי $|\psi\rangle$ ובוודאי שלא שכפלנו כלום (הקריסה של $|\psi\rangle$ אינה בעייתית רק אם אנחנו יודעים מה המצב $|\psi\rangle$ ובוחרים אופרטור מדידה ש-$|\psi\rangle$ הוא וקטור עצמי שלו). לכן הדינמיקה של המערכת לא כוללת מדידה, ומכאן שהיא מתוארת על ידי הפעלה של אופרטור אוינטרי. אם באמת הצלחנו לבצע שכפול, זה אומר שקיים אופרטור אוניטרי U כך ש-$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$. כעת, ה-U אינו תלוי בזהות הספציפית של $|\psi\rangle$ (כי אמרתי שאנחנו לא יודעים מהו $|\psi\rangle$). לכן אותה משוואה תתקיים גם עבור מצב אחר, $|\varphi\rangle$: $U\left(|\varphi\rangle \otimes |s\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle$.

עכשיו נכניס לתמונה מכפלה פנימית. ראשית, איך נראית מכפלה פנימית של מכפלה טנזורית? פשוט מאוד - מכפלה של כל רכיב בנפרד. כלומר: $\langle\psi\psi|\varphi\varphi\rangle = \langle\psi|\varphi\rangle\ \langle\psi|\varphi\rangle = \left(\langle\psi|\varphi\rangle\right)^2$. קיבלנו את המשוואה הפנימית של שני אגפי ימין של המשוואות. ומה עם אגף שמאל? ובכן, ראשית כל צריך לזכור שטרנספורמציה אוניטרית **משמרת מכפלה פנימית**, במובן הבא: $\langle Ux|Uy\rangle = \langle x|y\rangle$ לכל x, y. מכאן שאם נכפול את שני אגפי שמאל, נקבל:

$$\langle U\left(\psi s\right)|U\left(\varphi s\right)\rangle = \langle\psi s|\varphi s\rangle = \langle\psi|\varphi\rangle \cdot \langle s|s\rangle = \langle\psi|\varphi\rangle$$

כאן אנו משתמשים בכך ש-$\langle s|s\rangle$ = 1; זו תכונה שכל מצב קוונטי מקיים.

מה קיבלנו? את המשוואה הבאה, מעל המספרים המרוכבים: $\langle\psi|\varphi\rangle = \left(\langle\psi|\varphi\rangle\right)^2$. למשוואה הזו יש רק שני פתרונות אפשריים: $\langle\psi|\varphi\rangle = 1$ ו-$\langle\psi|\varphi\rangle = 0$.

במקרה הראשון $\psi = \varphi$ ובמקרה השני הם אורתוגונליים. אולי אתם לא רואים מייד למה מהמקרה הראשון נובע שוויון, אז תסתכלו על המשוואה הזו:

$$\langle\psi - \varphi|\psi - \varphi\rangle = \langle\psi|\psi\rangle - \langle\psi|\varphi\rangle - \langle\varphi|\psi\rangle + \langle\varphi|\varphi\rangle = 1 - 1 - 1 + 1 = 0$$

מכפלה פנימית של וקטור בעצמו היא 0 רק אם זה וקטור האפס, כלומר רק אם $|\psi\rangle$ = $|\varphi\rangle$.

מה קיבלנו? שפרוצדורת השכפול שמתוארת על ידי U, אם היא יודעת לשכפל את $|\psi\rangle$, יכולה לשכפל פרט ל-$|\psi\rangle$ רק וקטורים אורתוגונליים לו - בוודאי שהיא לא יכולה לשכפל כל מצב קוונטי אפשרי שבו המערכת יכולה להיות. לכן כדי להיות מסוגלת לשכפל את המצב הקוונטי שמגיע אליה, איב חייבת לדעת מהו; אבל אם היא הייתה יודעת מהו, היא לא הייתה צריכה למדוד אותו מלכתחילה ונגמר העניין. וזה גם מקום טוב לסיים את המאמר.

המאמר פורסם לראשונה כפוסט בבלוג "לא מדויק".