מצגת אמצע

פרויקט מס’: 24113064

שם הפרויקט: סימולטור תוכנה להפצת מפתח הצפנה קוונטי מהחלל.

מבצעים:

שם: ניקול פרומקין

ת.ז: 211615372

שם: קרן קויפמן

ת.ז: 208278879

מקום ביצוע הפרויקט: מעבדת הננו-לוויניים של הפקולטה.

חתימת המנחה:

שם: פרופ' מאיר אריאל

חתימה: _____

הקדמה - נושא הפרויקט

- הפרויקט עוסק בפיתוח סימולטור להפצת מפתח הצפנה קוונטי בחלל (QKD- Quantum Key Distribution).
- מפתח הצפנה הוא רכיב הכרחי בכל סוג של תקשורת מאובטחת
  - בהצפנה סימטרית אנו מניחים ששני הצדדים מחזיקים מראש באותו מפתח הצפנה (שהועבר בצורה בטוחה לשניהם).
  - במקרה של הצפנה באמצעות מפתח הצפנה ציבורי, נדרש שלב מקדים של הפצת מפתח ההצפנה כך שמצותת בלתי חוקי לא ידע לעשות בו שימוש על מנת לפענח את המידע המוצפן.
- מסתבר כי הטכנולוגיות הקיימות להצפנה באמצעות מפתח ציבורי עלולות להפוך לבלתי בטוחות בעתיד בגלל יכולתם של מחשבים קוונטיים לפצח הצפנה מסוג זה במהירות רבה.
- תקשורת קוונטית מציעה פתרון לבעיית הפצת מפתח ההצפנה באמצעות קידוד המפתח במצב הפולריזציה של פוטון (במקום באמצעות סיביות רגילות). ניסיון למדוד את מצבו הקוונטי של פוטון מוביל לקריסת פונקציית הגל באופן שלא מאפשר מדידה נוספת ומאפשר לזהות ניסיונות האזנה.
- מטרת הפרויקט היא לדמות את תהליך העברת המפתח בין תחנת קרקע לתחנת חלל, לזהות שגיאות וניסיונות ציתות, ולנתח את הביצועים בתרחישים שונים.
- הסימולטור נבנה בשפת C עם ממשק גרפי בשפת פייתון וישמש למחקר ופיתוח תקשורת קוונטית.

הקדמה - נושא הפרויקט

התמונה הבאה מראה את תהליך יצירת והעברת מפתחות ההצפנה בין תחנת החלל (אליס) ולבין תחנת הקרקע (בוב), באמצעות ערוץ קוונטי וערוץ גלוי נוסף (המסומן בירוק).

הסבר על הפרויקט

הפצת מפתח הצפנה נדרשת בכל סוג של תקשורת מוצפנת א-סימטרית, כלומר תקשורת בין שני משתמשים מזדמנים (אליס ובוב) כנגד ניסיונות האזנה של צד שלישי (איב). הפרוטוקולים להפצת מפתח הצפנה כיום מבוססים על אלגוריתם RSA. בטכנולוגיה של היום, בעזרת המחשוב הקוונטי, הצפנה על ידי אלגוריתם RSA היא אינה בטוחה מכיוון שניתן לזהות את הגורמים הראשוניים המרכיבים את המפתח בזמן קצר יחסית ובכך לשבור את ההצפנה.

מענה לבעיה זו קיים בתקשורת קוונטית באמצעותה מיוצר מפתח הצפנה המבוסס על מצבו הקוונטי של פוטון או חלקיק תת אטומי אחר.

<u>להלן רכיבי הסימולטור להפצת מפתח הצפנה בטכנולוגיית QKD:</u>

- קוד המדמה לוויין המייצר מפתחות הצפנה: הגרלת המפתח מביטים אקראיים, בחירת אורך המפתח, חלוקת למקטעים המאפשרים זיהוי ציתות, אחוז הביטים המואזנים.
- הדמיית יצור הקיוביטים מתוך הביטים באמצעות העברת פוטונים דרך מקטבים (אנכי/אופקי או אלכסוני).
- הדמיית העברת הקיוביטים לתחנת קרקע עם האפשרות להאזנה של איב (שעל מנת להסתיר את ההאזנה איב מייצרת קיוביט חדש), בנוסף הדמייה של הזרקת שגיאות ערוץ.
- הדמיית תהליך המדידה של הקיוביטים באמצעות מקטבים אלכסוני ואנכי.
- הדמיית העברת המידע בערוץ פתוח בין אליס ובוב לגבי הקיטוב שנבחר והקרבת מחצית הקיוביטים לצורך זיהוי האזנה.
- ניתוח ביצועים כנגד ערך סף של שגיאות בתרחישים של העברת מפתחות מלוויין לשני משתמשים שונים.

אופן מימוש הפרויקט

לפרויקט 5 חלקים עיקריים שכולם ימומשו בתוכנה בשפה עילית –שפת C :

1. מימוש סימולטור למקודד קוונטי המייצר סדרה אקראית של קיוביטים. הסימולטור יאפשר דרגת חופש בבחירת המקטב כך שלכל ביט אינפורמציה יתאימו שני מקטבים אפשריים, ובסך הכל 4 מקטבים שונים.
2. מימוש בתוכנה של מפענח קוונטי המגריל את הגלאי בצד הקולט ומודד את מצבו של הקיוביט.
3. סימולטור לערוץ קוונטי ולערוץ קלאסי על פי המוגדר בתקן BB84.
4. סימולטור של גורם מצוטט המזריק שגיאות קוונטיות.
5. פיתוח ממשק הפעלה לסימולטור המאפשר לבחור פרמטרים שונים של דיוק והסתברות שגיאה הן בצד המשדר והקולט והן בערוצים הקוונטי והאופטי, ולהציג את ביצועי המערכת עבור בחירה של פרמטרים שונים ובתרחישי הפעלה וקיצון שונים.

הסימולטור יאפשר לסמלץ ולבחון באופן ריאלי את ביצועי המערכת העתידית תחת פרמטרים שונים של דיוק פגיעת קרן הפוטונים, דיוק הפיענוח הקוונטי, והסתברויות השגיאה בערוצים השונים. ויאפשר להסיק מסקנות בנוגע לרמת הדיוק הנדרשת ממערכת מבצעית.

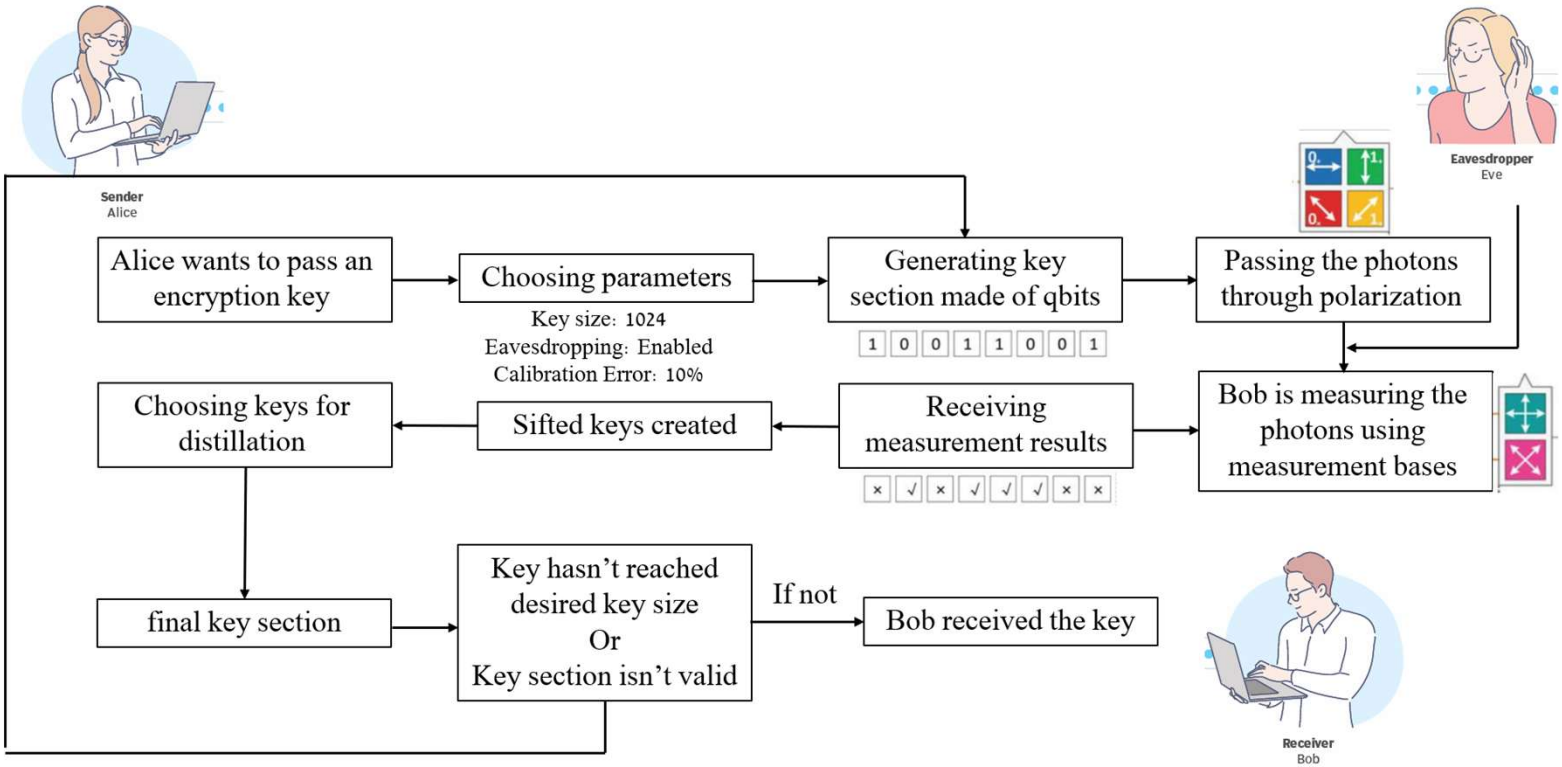
תוצר סופי

התוצר הסופי יכלול מערכת שמספקת פתרון הצפנה מאובטח תוך עמידה בתקנים ובדרישות הביצועים שהוגדרו מראש.

הדרישות הכמותיות שעל המערכת הסופית לעמוד בהן כוללות:

1. זמן ביצוע – המערכת תוכל לייצר מפתח QKD בגודל של x ביטים (לפי הגודל הרצוי) תוך זמן של לא יותר מ-10 שניות.
2. דיוק – המערכת תוכל לזהות ולהגיב לניסיון האזנה או מניפולציה על המידע בכ-99% דיוק.
3. יציבות – המערכת תהיה מסוגלת ליצור מפתח בגודל רצוי ללא ירידה בביצועים.

דיאגרמת בלוקים



תוצרי הפרויקט שהופקו עד כה

תוצאות מתוך הסימולטור שכתבנו המראה את הסטטיסטיקות והחישובים לגבי הרמת דיוק והסתברויות השגיאה שאנחנו בחרנו. למשל עבור הפרמטרים הבאים:

גודל כל בלוק: 128 ביט. שגיאת קליברציה: 7%. אחוז האזנה של איב (פר בלוק): 25%. מספר הבלוקים שאיב מאזינה: 10%.

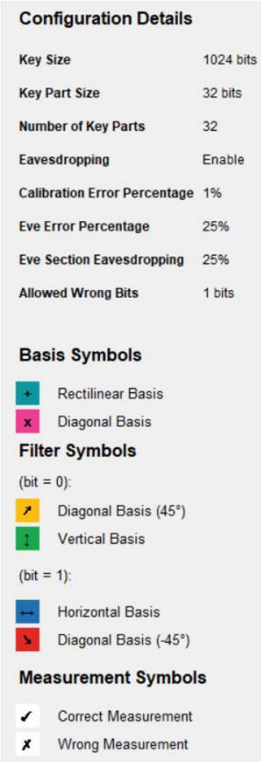
נקבל:

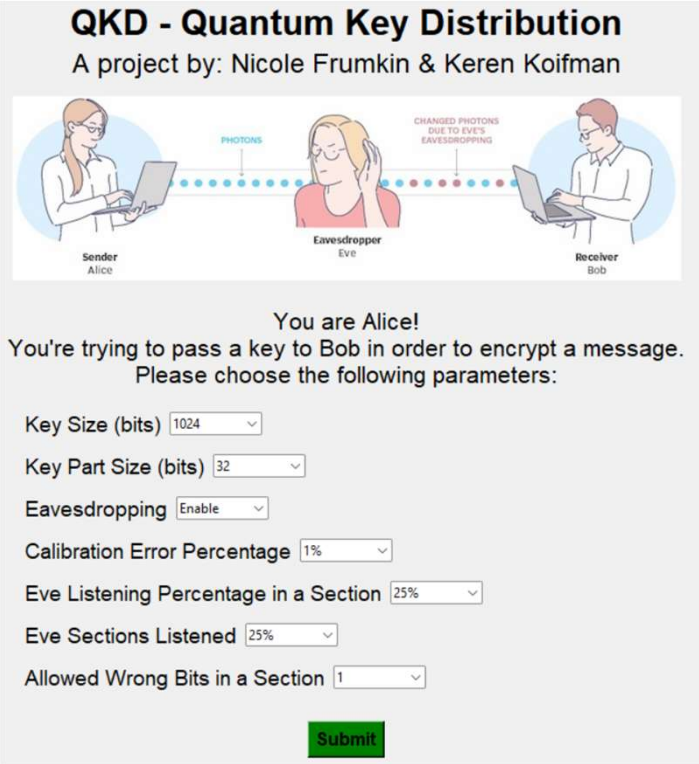
```
==========================================================================================
                                    Final Key (1024 bits)
==========================================================================================

1100 0101 1010 0101 0001 1001 1100 1000 0010 1111 0100 1000 1011 1111 1011 1110 0010 0011 0010 1111 0011 0111 1101 1101 1010 0011 1000 1100 1110 1011 1000 1101 1010 0011 1100 0001 1001 10
11 0100 1100 0111 0011 0010 1000 0000 1000 0111 0001 0011 1001 1110 1100 0110 1000 0011 0100 1110 1010 0100 0000 1011 1110 0010 0110 1110 0110 0100 0001 0101 1001 1101 1110 1011 0110 0111
 1110 0011 1010 1000 1001 0010 0110 0010 1000 0111 0000 1010 0001 1100 1011 1011 0010 0000 0111 1101 1010 0011 0110 1100 1111 1011 0010 0001 1001 1111 0110 0001 1100 0110 1001 1011 1000 1
010 1010 1001 0110 0000 0010 1000 1010 0000 0000 1110 0101 0000 0110 1001 0101 0011 1010 1111 1100 0011 1100 0011 0010 0100 1101 0111 1101 0011 0010 1100 1001 0011 0110 1011 1101 1011 010
0 0000 1100 0001 1010 0101 1100 1010 0010 1110 1001 1001 0110 0101 1000 0100 1101 1010 1110 1011 1100 0100 1001 1101 0100 0010 0110 0100 1110 1001 0000 1100 0011 1101 1110 1111 1101 1101
0110 0010 1001 0010 1010 0111 0110 1111 0111 1100 0100 1001 1010 0111 0011 0101 0101 1010 1111 1011 1110 1111 0001 1000 0101 0000 0111 0000 1000 1101 1100 1011 0010 0111 0010 0111 1111 00
10 0000 1101 1110 1110 1110 1010 0011 0111 0010 0101 1101 0100 0111 0010 0110 0010 1011 0010 1010 1010 1111 0000 0101 1000 0110 1100 0000 0101 1101 0011 1011
final_calib_error_bits_count=72 out of 1024 key-size (7 %)
final_eve_error_bits_count=2 out of 1024 key-size (0 %)
stats: eves_attack_detected=3 out of 4 key-sections
stats: total_run_sections=44
stats: number of running sections to generage the final key=34
```

בריצה זו רצינו לייצר מפתח באורך של 1024 ביטים. לצורך כך הסימולטור הריץ 44 בלוקים של 128 ביט כאשר מכל בלוק לוקחים כמות מסויימת של ביטים לפי התקן הדרוש.
בלוקים נפסלים מכמה סיבות: זיהוי האזנה של איב, כאשר שגיאות הקליברציה עוברות את הסף המותר.

תוצרי הפרויקט שהופקו עד כה

בנוסף לסימולטור, נציג את התהליך עם ממשק משתמש גרפי. בעזרתו נוכל להנגיש את הסימולטור והמשתמש יכול להזין ערכים לפי רצונו ובעזרת הסימולטור נוכל להראות את הסטטיסטיקות והחישובים לגבי הרמת דיוק והסתברויות השגיאה.





תוצרי הפרויקט שהופקו עד כה

תהליך בחירת הביטים למפתח הסופי מתוך בלוק של 32 ביט:

Section #1 (32 bits):

Alice's Key	0	0	1	1	1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0
Key with Calib Errors	0	0	1	1	1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0
Single Photons	↔	↔	↗	↗	↕	↕	↕	↗	↔	↗	↕	↕	↕	↔	↗	↘	↕	↔	↘	↕	↗	↘	↔	↘	↕	↔	↔	↗	↗	↔	↘	↔
Measurement Bases	+	x	+	+	+	+	x	x	+	x	+	+	x	+	x	x	x	x	x	+	x	x	x	x	+	x	x	x	x	x	+	+
Measurement Results	✓	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Bob's Key	0	-	-	-	1	1	-	1	0	1	1	1	-	0	1	0	-	-	0	1	1	0	-	0	1	-	-	1	1	-	-	0
Sifted Keys	0	-	-	-	1	1	-	1	0	1	1	1	-	0	1	0	-	-	0	1	1	0	-	0	1	-	-	1	1	-	-	0
Key Distillation	0	-	-	-	-	1	-	1	-	-	1	-	-	-	-	0	-	-	0	-	1	0	-	-	1	-	-	-	1	-	-	-
Key Bits Error	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Secret Keys	-	-	-	-	1	-	-	-	0	1	-	1	-	0	1	-	-	-	-	1	-	-	-	0	-	-	-	1	-	-	-	0
Final Secret Keys	1	0	1	1	0	1	1	0	1	0																						

The Iby and Aladar Fleischman Faculty of Engineering
Tel Aviv University

לוח זמנים

	אבן דרך	פירוט	תאריך לביצוע	תאריך ביצוע בפועל	הערות
1	לימוד רקע תיאורטי וסקירת ספרות	לימוד עקרונות הצפנה קוונטית ו-QKD, סקירת טכנולוגיות קיימות והבנת הדרישות הטכניות.	10.08.24	10.08.24	בוצע
2	הגדרת דרישות מערכת וכתיבת מסמך דרישות	ניסוח דרישות מערכת כמותיות וכוללות לכל שלב בפרויקט, כולל הגדרת ביצועים קריטיים.	14.08.24	14.08.24	בוצע
3	כתיבת האלגוריתם הראשוני של QKD	כתיבת האלגוריתם הראשוני לפיתוח תהליכי הצפנה ופענוח עם QKD.	1.11.24	01.11.24	בוצע
4	ביצוע סימולציות ראשוניות של האלגוריתם	ביצוע סימולציות להערכת ביצועי האלגוריתמים והזיהוי של בעיות או תקלות בתהליך.	15.11.24	20.11.24	בוצע
5	הרחבת הסימולטור	הוספת פרמטרים נוספים לסימולטור כגון אחוז שגיאה	30.11.24	05.12.24	בוצע
6	ביצוע סימולציות נוספות של האלגוריתם	בחינת האלגוריתם לאחר הוספת הפרמטרים השונים	15.12.24	15.12.24	בוצע
7	ניתוח סטטיסטי של הסימולציות	הסקת מסקנות סטטיסטיות לגבי יעילות ואופן פעולת האלגוריתם	30.12.24	05.01.25	בוצע
8	הגשת מצגת האמצע	הגשת מצגת האמצע	30.01.25	02.02.25	בוצע
9	אופטימיזציה ושיפור האלגוריתמים	ביצוע אופטימיזציה של האלגוריתמים לשיפור ביצועים ודיוק המערכת	15.02.25		
10	ביצוע סימולציות מלאות עם תיקון בעיות	ביצוע סימולציות מעמיקות כדי לוודא שהמערכת פועלת כראוי בכל המצבים	15.03.25		
11	ניתוח ביצועים של המערכת	ניתוח ביצועים של המערכת בתרחישי הפעלה שונים והסקת מסקנות והמלצות לתכנון המערכת מבצעית	15.04.25		
12	הכנת פוסטר לפרויקט	הכנת פוסטר שיכלול את כלל התהליך, הממצאים והתוצרים עד כה	01.05.25		
13	הגשת הפוסטר וסיום העבודה בפרויקט		30.05.25		
14	הכנת דוחות סיום והכנת מצגת סופית	סיכום העבודה, תוצאות הסימולציות, הפיתוחים וההמלצות להמשך	15.06.25		
15	הגשת ספר הפרויקט ומצגת סיום		30.06.25		