

שבבים של מערכי ננו לייזר: בזכות הלייזר הזעיר ניתן ליצור מעבדת זיהוי שלמה על-גבי ס"מ מרובע

פריצת דרך בתחום ההצפנה הפיסיקלית תשפור את התקשורת המאובטחת

ד"ר קובי שויער מאוניברסיטת תל אביב פיתח תפיסה חדשה להעברה מאובטחת של מפתח הצפנה. בשירות התקשורת המוצפנת ישמשו לייזרים שאורכם מאות קילומטרים, המבוססים סיבים אופטיים

◀ קטיה וליקורודוב

אלגוריתמים מתמטיים. "נכון להיום, אין הוכחה פורמאלית שהאלגוריתמים לא ניתנים לפיצוח; פשוט, עד עכשיו אף אחד לא הצליח", אומר ד"ר קובי שויער. "הרעיון שלי אינו עוסק בניסיון להעביר את המידע המוצפן, אלא ביצירת המפתח המשותף שימש להצפנה. כלומר, בסופו של התהליך שני המשתתפים יחלקו מפתח הצפנה, הכולל סידרה אקראית של מספרים זהים הידועים

שלישי יגלה אותו? "ללא המפתח המשותף לא ניתן לעשות זאת", טוען ד"ר קובי שויער, והוא מציע תפיסה חדשה, מהירה ומאובטחת להרכבת המפתח והעברתו לשומרי סוד. ד"ר שויער הוא ראש המעבדה לננו פוטוניקה בביה"ס להנדסת חשמל באוניברסיטת תל אביב.

בעבר הלא-רחוק פתרו את הבעיה באמצעות בלדרים, והיום הם הוחלפו במערכות הצפנה אשר פועלות על בסיס

עיית הצפנת המידע היא עתיקת יומין. על מנת להעביר מידע מוצפן, שני משתתפים צריכים להשתמש במפתח הצפנה זהה: סדרת מספרים שבאמצעותם מצפינים את המידע. המלכוד: איך מעבירים מפתח לשני אנשים שלא נפגשו מעולם, בעודם נמצאים במרחק של מאות קילומטרים אחד מהשני ומעוניינים להעביר מידע סודי ללא חשש שצד

◀ לשני הצדדים בלבד.

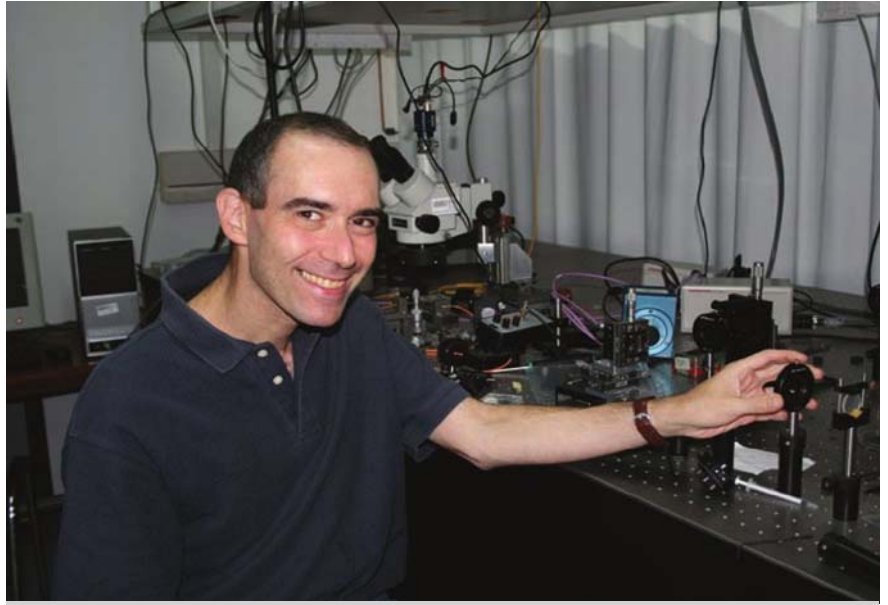
המצאתו של ד"ר שויער מבוססת על שימוש בלייזר סיב אופטי רגיל, אך ארוך במידה ניכרת מהמקובל. "אני בונה לייזר

כרצונם. באופן כזה, שני הצדדים החליפו מפתח שהינו רצף אקראי של מספרים הבלעדי רק להם", מסביר הממציא. לדעתו של ד"ר שויער, רעיון מקורי זה

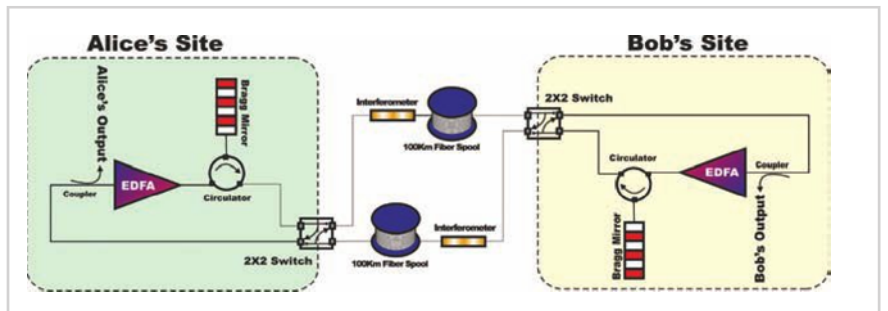
ק"מ, רק אחד מאלף פוטונים שנשלחו מגיע לצד השני", מבהיר ד"ר שויער. בימים אלה הושגה פריצת דרך משמעותית במעבדתו של ד"ר קובי

"נכון להיום, אין הוכחה פורמאלית שהאלגוריתמים לא ניתנים לפיצוח; פשוט, עד עכשיו אף אחד לא הצליח"

שויער: עומר קוטליצקי, סטודנט לתואר שני בהנחייתו של ד"ר שויער, הדגים בהצלחה לייזר המשתרע על פני 200 ק"מ ומסוגל ליצור מפתח בקצב של חצי קילוביט לשנייה, וקבוצתו של ד"ר שויער רשמה פטנט על כך. הקצה השני של כדור הארץ הוא הגבול, מודה אבי הרעיון: "אני משתמש בסיבים האופטיים הרגילים, המצויים כבר בתוך האדמה, ואין לי בעיית של טווח; זה תלוי רק באורכו של הסיב ובמספר המגברים האופטיים. החידוש שלי הוא בתפיסה: עד עכשיו אף אחד לא חשב להשתמש בלייזר בצורה זו עבור מערכת תקשורת. אף אחד לא אמר שהלייזר צריך להיות בצד אחד ובצד השני צריך להיות מקלט; בפיתוח שלנו הלייזר מתוח לכל אורך הקו המחובר בין המשתמשים". ואיך לא - משרד הביטחון מגלה עניין רב בפרויקט זה.



ד"ר קובי שויער במעבדתו: רעיון מקורי זה עשוי להביא למהפכה בנושא התקשורת המוצפנת



סכימת מערכת ההצפנה המבוססת על לייזר סיב אופטי

מעבדה לזיהוי פלילי על פני השבב

פרויקט נוסף, אשר קבוצתו של ד"ר שויער עוסקת בו, הוא פיתוח חיישנים אופטיים על בסיס ננו-לייזרים. חיישנים אופטיים הם לייזרים ננו-מטריים שכאשר הם נחשפים לחומר שהם מנסים לגלות, מתרחש שינוי במאפיינים שלהם. לדוגמה, עשוי לחול שינוי בצבע שהם מאירים בו או בעוצמת האור.

הרעיון של שימוש בלייזרים זעירים לצורך חישה אינו חדש. נוכחותו של חומר זר בקרבת סיב אופטי, או כל מוליך גלים אחר, משנה את מקדם השבירה האפקטיבי, ולייזרים מגיבים לשינויים האלה על ידי הסחה בתדר הלזירה שלהם. כידוע, הלייזר הוא מתנד (oscillator) הכולל תווך מגביר אופטי ומהוד (resonator), ויש לו תדר תהודה הקובע את אורך הגל ("הצבע") של

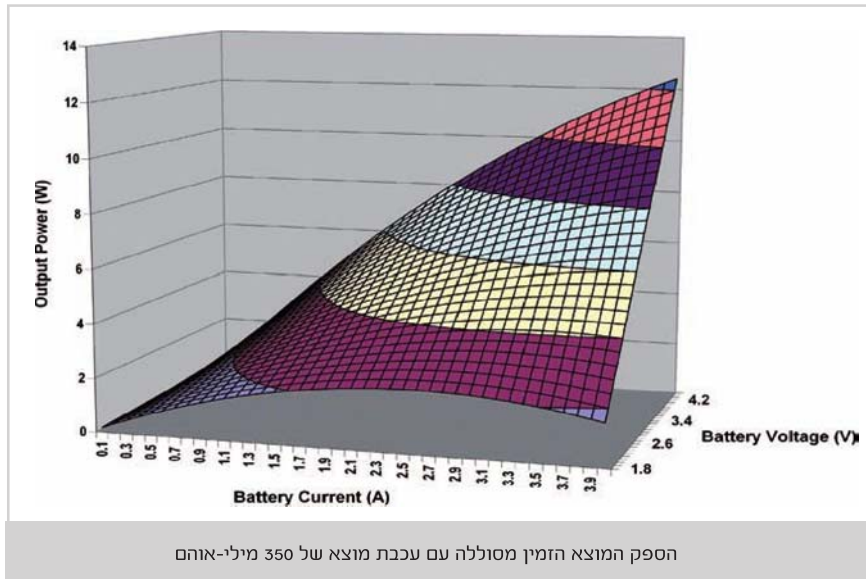
עשוי להביא למהפכה בנושא התקשורת המוצפנת: "זוהי פריצת דרך בתחום ההצפנה הפיסיקלית, לעומת ההצפנה המתמטית השכיחה היום, משום שלמעשה אף מערכת חישובית לא תוכל להתמודד עם מערכת ההצפנה הפיסיקלית ולפצח אותה".

באופן דומה, בשנים האחרונות נסו לבצע את יצירת המפתח על בסיס עקרונות המכניקה הקוונטית, באמצעות שליחת פוטונים בודדים של אור, אך השיטה פועלת עד לטווחים של כ-120 ק"מ בקצב של ביט אחד לשנייה. "הבעיה של עולם הקוונטים היא בכך שהם חייבים לשלוח כל פעם פוטון בודד ולא ניתן להשתמש במגברים אופטיים. לדוגמה, בהתחשב בהפסדים של סיב אופטי באורך של 100

מאוד ארוך, כאשר בכל אחד מקצותיו ניתן לחבר אחת משתי מראות המחזירות אור באורך גל אחר. המראה הראשונה מכונה, לדוגמה, "0" והשנייה "1". על מנת ליצור ביט עבור המפתח כל משתמש בוחר באחת מהמראות ו"מחבר" אותה ללייזר הסיב. המשתמשים חוזרים על התהליך

"זוהי פריצת דרך בתחום ההצפנה הפיסיקלית, לעומת ההצפנה המתמטית השכיחה היום"

שוב ושוב תוך שמירת המקרים הלא-קורלטיביים בלבד (שני הצדדים בחרו מראות שונות) עד שמתקבל סט ארוך



הזמין בתנאי פעולה אופייניים. היא מגבילה גם את התכונות שבהן אפשר לתמוך. כוונון באופן דינמי של מגבלת זרם הכניסה על-פי מצב הסוללה, יכול לאפשר שמירה על זמינותו של מערך תכונות שלם במצב פעיל, בהספק גבוה, בתנאי פעולה אופייניים. כמו כן, הוא מסייע לשמור על יכולת הפעולה של המערכת עם קבוצה של תכונות מינימליות, מוגבלת בתנאים קיצוניים. קבלת חיווי מממיר מתח ישר למתח ישר, לפיה ההספק הזמין ברגע מסוים מוגבל, מסייעת למערכת להחליט לנטרל לזמן מה תכונות שהן חשובות פחות. דוגמה לממיר מתח ישר למתח ישר שתומך באסטרטגיית תכנון זו בדרך פשוטה הוא הממיר המוריד-מעלה TPS63020.

את הקבל שבמוצא בזמן ההמתנה לפולס הטעינה הבא. לדוגמה, כל התכונות האלו ממומשות בממיר המוריד-מעלה TPS63020.

חלקה של הגבלת הזרם של ממיר מתח ישר למתח ישר. ממיר המתח הישר למתח ישר יעבור למצב סרק ברגע שקבל המוצא ייטען למתח הנומינלי המתוכנן. צריכת ההספק של ממיר מתח ישר למתח ישר במצב סרק צריכה להיות נמוכה, ועכבת המוצא חייבת להיות גבוהה, כדי לא לפרק

אם זרם הכניסה הזמין אינו מספיק כדי להפעיל את היישום, על-אף שהזרם הממוצע הנדרש נמוך דיו, יש צורך לבצע חציצה של האנרגיה. החציצה מתבצעת בדרך כלל על ידי שימוש בקבלים גדולים יותר. הפעילות של זרם השיא נתמכות על-ידי קבל, שנטען במהלך ההפסקות שביניהן. לשם כך, יש צורך בפעולה

יורגן נויאהולר הוא מהנדס מערכות בכיר בקבוצת פתרונות דלי-הספק מתקדמים, Texas Instruments.

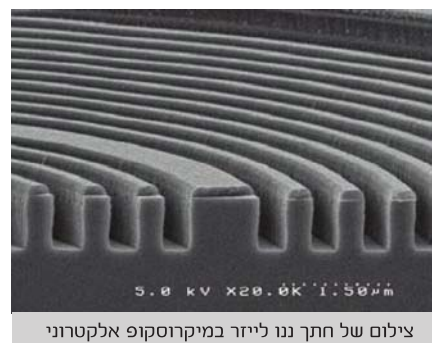
המשך מעמוד 20

לשינוי. הלייזר עצמו אינו מסוגל להבדיל בין חומרים שונים; הוא אינו סלקטיבי. ניתן לפתור בעיה זו על-ידי הצמדה של רצפטורים ללייזר, אשר מתאימים למולקולה או וירוס ספציפיים, וכך לקבל תגובה סלקטיבית לחומר ספציפי.

הגודל הפיסי הכולל של ננו-לייזרים שעמם עובד ד"ר שויער, הוא עד 10 מיקרון, והאור כלוא בקוטר של 300 ננומטר של אוויר. "משמעות כליאתו של האור בתוך אוויר, היא בכך שכל האור הזה חשוף למה שקורה מסביב, וכל חומר זר שיעבור בתחום הלייזר

הלייזר. את צבע האור של הלייזר ניתן לשנות באמצעות שינוי אורכו האופטי של הלייזר, ולא בהכרח רק באמצעות אורכו הפיסי. האורך האופטי = האורך הפיסי x מקדם השבירה. זאת אומרת, ששינוי מקדם השבירה מ-1 ל-1.01 שקול להארכה של אורכו הפיזי של הלייזר באחוז אחד, וכתוצאה מכך אורך הגל של הלייזר משתנה אף הוא בהתאם. כך שעל-ידי מעקב אחר אורך הגל של לייזר, ניתן לגלות נוכחות של חומרים זרים בסביבתו.

"החידוש שלי הוא בתפיסה: עד עכשיו אף אחד לא חשב להשתמש בלייזר בצורה זו עבור מערכת תקשורת"



לדוגמה, האנטיבודי של וירוס מסוים יהווה רצפטור לזיהוי הווירוס. בזכות גודלו הזעיר של הלייזר, ניתן להקים מערך שלם עם מאות לייזרים על גבי שבב בגודל 0.5 ס"מ על 0.5 ס"מ, וליצור מעבדת זיהוי שלמה על גבי סנטימטר מרובע. "כרגע אני בונה בסיס להפעלת לייזר כזה, ובהמשך עלי למוצא קבוצה של ביולוגים או כימאים לשיתוף פעולה", מסכם ד"ר שויער.

ישפיע מאוד חזק על מקדם השבירה. כתוצאה, ניתן לגלות שינויים מאוד קטנים, שנגרמים אפילו על-ידי מולקולה בודדת של החומר שתרים אחריו, מספר ד"ר שויער, "זאת, בניגוד לאופטיקה קונבנציונאלית, שם רק הזנב של האור מרגיש קצת את השינוי; בלייזר הזה, כל האור חשוף

כדי לפתח חיישן רגיש, דרושה תגובה חזקה לשינוי. "אני מתכנן לייזרים בעלי מבנה מאוד מיוחד, שבהם האור לא נמצא בתוך החומר עם מקדם שבירה גבוה, אלא דווקא העיקר שלו נמצא באוויר, שיש לו מקדם שבירה נמוך. זוהי שיטת הולכת גל אחרת, והיא מבוססת על תופעה שנקראת החזרת בראג (Bragg reflection). באמצעות שתי מראות - 'מראות בראג' - אני נותן לאור לדלג ממראה אחת לשנייה, כאשר ביניהן נמצא כל חומר רצוי. אני כולא את האור באוויר ואני יכול לבצע זאת במימדים מאוד קטנים", מסביר ד"ר שויער.