חזרה לרשימה

פרופ' עודד גולדרייך

שיתוף שיתוף
share
שתפו עמוד:
פרופ' עודד גולדרייך

alert("שגיאה בהעתקת הקישור");
הקישור הועתק
העתק קישור Whatsapp Facebook

על הזוכה

מקבל פרס ישראל לשנת תשפ"א בחקר מדעי המחשב.

עודד גולדרייך תרם תרומות יסודיות וחשובות לתיאוריה של מדעי המחשב במגוון רחב של תחומים הכולל קריפטוגרפיה, סיבוכיות, אקראיות, הוכחות בדיקות מקומית (PCP), קושי של קירובים, והתורה של בדיקת תכונות מדגמית (property testing). גולדרייך תרם תוצאות משמעותיות, הגדרות בסיסיות פורצות דרך, וכיווני מחקר חדשים במשך למעלה משלושה עשורים. נוסף לתרומותיו המרשימות ויוצאות הדופן קידם את השטחים לעיל באמצעות ספרים ומאמרי סקירה מצוינים שכתב.

התכנים בעמוד

נימוקי השופטים

חזרה לראש הדף

פרופ' נגה אלון, יו"ר, פרופ' אירית דינור, פרופ' חגית עטיה, פרופ' ענר שלו

עודד גולדרייך תרם תרומות יסודיות וחשובות לתיאוריה של מדעי המחשב במגוון רחב של תחומים הכולל קריפטוגרפיה, סיבוכיות, אקראיות, הוכחות בדיקות מקומית (PCP), קושי של קירובים, והתורה של בדיקת תכונות מדגמית (property testing).

גולדרייך תרם תוצאות משמעותיות, הגדרות בסיסיות פורצות דרך, וכיווני מחקר חדשים במשך למעלה משלושה עשורים. נוסף לתרומותיו המרשימות ויוצאות הדופן קידם את השטחים לעיל באמצעות ספרים ומאמרי סקירה מצוינים שכתב.

עבודתו של גולדרייך בקריפטוגרפיה מתייחסת למספר נושאים יסודיים. עוד בהיותו פוסטדוק, ביחד עם גולדווסר ומיקלי, ניסח את המושג של "פונקציה פסאודו־אקראית". פונקציה כזו מצד אחד ניתנת לחישוב יעיל ומצד שני לא ניתן להבחין בינה לבין פונקציה

אקראית אמיתית, כל עוד המבחין יכול להתבונן רק במספר פולינומיאלי של קלטים בגישת "קופסה שחורה". נוסף על ניסוח ההגדרה באותו מאמר ניתנה גם בנייה של פונקציה כזו על סמך אובייקט בסיסי (ופשוט בהרבה) אחר שנקרא מחולל פסאודו־אקראי.

בשני מאמרים נוספים, גולדרייך ביחד עם מיקלי וויגדרזון הניח שתי אבני פינה חשובות נוספות בקריפטוגרפיה. הראשונה היא הרחבה משמעותית של המושג הבסיסי של הוכחות אפס־מידע. זהו רעיון שעומד בבסיסה של הקריפטוגרפיה המודרנית, והמאמר הראה שיש הוכחה כזו לכל בעיה ב־NP, מחלקת הסיבוכיות החשובה. כלומר, כל מה שניתן להוכיח ביעילות, ניתן להוכיח באפס מידע. יתרה מכן, המאמר הראה שלבעיות חשובות שלא ידוע שהן ב־NP יש גם הוכחות כאלו, לדוגמה לבעיית הנונ־איזומורפיזם בגרפים.

המאמר השני הראה את כוחו העצום של חישוב רב משתתפים בטוח והראה שכל פונקציה שניתנת לחישוב יעיל ניתנת גם לחישוב בטוח רב משתתפים כל עוד מרבית המשתתפים מתנהגים לפי הפרוטוקול, ובהנחת פונקציה חד־כיוונית עם דלת צונחת.

אחד היהלומים של תורת הסיבוכיות הוא הבנייה היפהפייה של גולדרייך־לוין של פרדיקט בוליאני קשה. הבנייה מספקת פונקציה בוליאנית שנראית כמו ביט אקראי לגמרי, בהתבסס על פונקציה חד־כיוונית. הבנייה נתנה את הדוגמה הראשונה לקוד תיקון שגיאות שיש לו אלגוריתם פענוח לרשימה והשפעתה מרחיקה הרבה מעבר לקריפטוגרפיה.

תרומות חשובות ומקוריות נוספות הן הגדרת ה־ORAM והגדרתה של תוכנית המחקר ב־program obfuscation, שתי תרומות חשובות להסוואה של חישוב, אשר הולידו כיווני מחקר עשירים ופוריים מאוד.

מחוץ לקריפטוגרפיה, בתחום ההוכחות הניתנות לבדיקה אקראית גולדרייך העמיק את חקר הקשר לתורת הקושי של קירובים, ויחד עם בלארה וסודן, הציע קוד חדש לתיקון שגיאות נוסף שנקרא "הקוד הארוך", והראה כיצד קוד זה שימושי להוכחת קושי של קירובים. הקוד הזה הוא אבן יסוד מרכזית בכל השטח של קושי של קירובים.

מאמר פורץ דרך של גולדרייך יחד עם גולדווסר ורון מציג את התורה של בדיקת תכונות מדגמית בהקשרים קומבינטוריים ובפרט עבור תכונות של גרפים. עד למאמר זה כלל התחום כמה עבודות שטיפלו בדוגמאות ספציפיות, והמאמר סיפק הגדרות כלליות חשובות ושלל דוגמאות, ובכך סלל את הדרך לבניית תחום עשיר ופורח.

למאמריו ולספריו של גולדרייך השפעה רבה בתחום, והם משמשים את הדור הבא של מדעני המחשב בארץ ובעולם. הספר בן שני הכרכים על יסודות הקריפטוגרפיה הפך לקלאסיקה והגשים את ההבטחה לעודד עבודה רבה בתחום. לתלמידיו הרבים, שלרבים מהם קריירות אקדמיות מפוארות משלהם, לכנסים שארגן ולהרצאותיו המאלפות הייתה השפעה מרכזית בביסוס מעמדה המוביל של ישראל במדעי המחשב התיאורטיים בעולם.

ועל כן מצאה הוועדה את הפרופ' עודד גולדרייך ראוי לקבלת פרס ישראל בחקר מדעי המחשב לשנת תשפ"א.

קורות חיים

חזרה לראש הדף

פרופ' עודד גולדרייך תרם תרומות מעמיקות ופורצות דרך ליסודות התיאורטיים של הקריפטוגרפיה ולתורת הסיבוכיות החישובית. עבודותיו הידועות ביותר מתייחסות להוכחה באפס ידע, ולבנייה של פרוטוקולים בטוחים למימוש כל משימה חישובית רצויה. עבודות נוספות עוסקות בפסאודו־אקראיות, בשימוש באקראיות בבדיקת הוכחות, ובתחום בדיקת תכונות מדגמית. עודד גולדרייך ידוע גם בספריו ומאמריו אשר תרמו ותורמים רבות לחינוך של דור חוקרים הממשיך את דרכו, תוך ביסוס מעמדה של מדינת ישראל ככוח עולמי מוביל בתיאוריה של מדעי המחשב.

פרופ' עודד גולדרייך גר בתל אביב, ונשוי לדנה רון מאז שנת 1990.

לימודים

1977–1980 תואר ראשון, הפקולטה למדעי המחשב, הטכניון
1981–1982 תואר שני, הפקולטה למדעי המחשב, הטכניון
1982–1983 תואר שלישי, הפקולטה למדעי המחשב, הטכניון

תפקידים אקדמיים בארץ

1983–1985 מרצה, הטכניון, חיפה
1986–1988 מרצה בכיר, הטכניון, חיפה
1988–1994 פרופסור חבר (עם קביעות), הטכניון, חיפה

1994–1995 פרופסור חבר (עם קביעות), מכון ויצמן למדע, רחובות
1995– פרופסור מן המניין, מכון ויצמן למדע, רחובות
1998– מחזיק הקתדרה הפרופסורית ע"ש מאיר וייסגל, מכון ויצמן למדע, רחובות

תפקידים אקדמיים בחו"ל

1983–1986 פוסט־דוקטורנט, MIT, ארה"ב
1995–1998 מדען אורח, MIT, ארה"ב
1996 חוקר אורח, מכון מילר למחקר בסיסי במדע, אוניברסיטת ברקלי, ארה"ב
2003–2004 עמית במכון ראדקליף ללימודים מתקדמים, אוניברסיטת הרווארד, ארה"ב
2011–2012 מדען אורח, המכון ללימודים מתקדמים, פרינסטון, ארה"ב
2019–2020 מדען אורח, אוניברסיטת קולומביה, ארה"ב

ארגון סדנאות וכנסים בין־לאומיים וחברות בוועדות עריכה של כתבי עת [רשימה חלקית]

1992–2011 Editor of the Journal of Cryptology
1996–2018 co-organizer of the Oberwolfach Meeting on Complexity Theory, Germany
1996–2010 Editor of the SIAM Journal on Computing
2003– Associate Editor of Computational Complexity
2003–2013 Member (and chair 2005–2013) of the steering committee of the Theory of Cryptography Conference (TCC)
Served on the program committee of numerous conferences including STOC90, FOCS94, FOCS99 and FOCS04; Crypto85, Crypto88 and Crypto92; Complexity03 and Complexity09

הוקרות ופרסים נבחרים

1994 מרצה מוזמן בקונגרס הבינלאומי למתמטיקה, ציריך
1997 מרצה מוזמן בכינוס CRYPTO, סנטה ברברה
2003– עמית בהתכתבות של האקדמיה הבווארית למדעים
2006 פרס על מצוינות בתחום המתמטיקה, כינוס RSA
2009 עמית של הארגון הבינלאומי למחקר בקריפטוגרפיה
2017 פרס קנות על תרומות בולטות ליסודות של מדעי המחשב

להמשך קורות החיים | סגירה

מפעל חיים

חזרה לראש הדף

עודד גולדרייך נולד בפברואר 1957, בן יחיד להורים מבוגרים, שנישאו שנה קודם לכן. אימו קלרה (ילידת גרמניה 1912) הייתה עורכת דין, לאחר שהשלימה בגרות והחלה בלימודי משפטים בשנת 1950, ואביו איזידור (יליד צ'כיה 1906) היה מהנדס, תחילה בשירות שלטונות המנדט ואחר כך בשירות המדינה. "גדלתי בתל אביב, בדירה שמול בית הספר היסודי 'בלפור' שבו למדתי שמונה שנים", מספר גולדרייך. "זיכרונות מהילדות שלי כוללים שיחות ארוכות עם אימי על נושאים אקטואליים, נסיעות עם אבי לבדיקת גשרים ומבנים של רכבת ישראל, שבה עבד כמהנדס, שעות חינוך בכיתות ד' וה' עם המחנכת יעל העליון, והמתח לפני מלחמת ששת הימים, ובפרט ההכנות לקברים שנעשו בגן מאיר".

את לימודי היסודי סיים עודד בשנת 1971, ואז פנה ללמוד בתיכון עירוני א' בתל אביב. "למדתי באחד המחזורים הראשונים שנהנה מחינוך תיכון חינם. אני זוכר את זה משום שחשבון חיסכון שיועד לתמיכה בחינוך תיכוני הוסב לתמיכה בלימוד אוניברסיטאי". מן התיכון זכור לו המורה למתמטיקה, יוסף ברוקר, שהקסים אותו גם באישיותו וגם בחומר ("שלא לבגרות") שלימד את התלמידים. למרות זאת, בתקופה זאת נמשך יותר למקצועות ההומניים, אך "הוסלל" למגמה הריאלית בשל ציוניו הטובים יותר במקצועות אלו.

בשנת 1975 גויס לצבא, ובשנת 1977 שוחרר בשל תאונת דרכים. השחרור המוקדם פתר אותו מהתלבטות בין לימודי משפטים, פילוסופיה ופסיכולוגיה, משום שההרשמה בכל המוסדות למעט הטכניון כבר נסגרה: מכיוון שלא רצה לחכות שנה, נרשם עודד לטכניון והתקבל ללימודים במדעי המחשב.

"בלימודיי בטכניון, הוקסמתי במיוחד מההרצאות של פרופ' שמעון אבן, שגם הקסים אותי באישיותו", נזכר גולדרייך. כאשר סיים את לימודי התואר הראשון עדיין התלבט, הפעם בין לימודי תואר ראשון בפסיכולוגיה באוניברסיטת תל אביב ובין המשך

הלימודים לתואר שני במדעי המחשב בטכניון. "בהארה של רגע הבנתי שכמה תכונות אופי מרכזיות שלי אינן מתאימות למטפל פסיכולוגי, והמשכתי בטכניון", הוא אומר. שמעון אבן, שהיה דיקן הפקולטה בשנת 1981, בחר בגולדרייך להיות עוזר ההוראה שלו. הפגישות איתו הובילו – שלא במודע – ליחסי מונחה ומנחה. השנים הללו עיצבו הרבה מהשקפותיו ביחס למחקר.

באמצע שנת 1983, כאשר קיבץ את עבודותיו המחקריות לתזת דוקטורט, הופנה לעבודתם של שפי גולדווסר וסילביו מיקאלי, שזיכתה אותם בשנת 2012 בפרס טיורינג (הנחשב ל"פרס נובל של מדעי המחשב"). "מיד הבנתי שדרך המלך הנוכחית שבה הלכתי היא נאיבית, ושדרכם היא הדרך הנכונה", ואכן, בשנותיו כפוסט־דוקטורנט (1983–1986) ב־MIT עבד עם השניים והדבר עיצב את ההשקפה המחקרית שלו. עבודות משותפות איתם ועם אבי ויגדרזון ובני שור הם גולות הכותרת של מחקריו באותן שנים. דמות נוספת הזכורה לו מתקופה זו הוא ליאוניד לוין, שגם ממנו למד אז רבות.

שנותיו של גולדרייך בטכניון (1986–1994) ובמכון ויצמן (החל משנת 1994) עומדות בסימן של קציר של מה שנזרע קודם. אף ששינה את תחומי העניין המחקריים שלו, ושרוב הנושאים שעסק בהם לא היו קיימים באמצע שנות השמונים, אופן ההסתכלות שלו והגישות המחקריות שלו נשארו פחות או יותר כפי שעוצבו בעשור הקודם. נוסף לכך עסק בפעילויות חדשות: הוראה, הנחיה של סטודנטים לתארים מתקדמים וכתיבה של סקירות וספרים מדעיים.

"ברמה האישית, חיי השתנו מאוד בסוף יוני 1990, כאשר פגשתי את דנה רון בנסיבות בלתי צפויות", מספר גולדרייך. "לאחר כמה שעות איתה, היה לי ברור שארצה לחלוק איתה את שארית חיי, וזה אכן מה שקרה מאז ועד היום".

"כחתן פרס ישראל, אני רואה את עצמי כנציג של תחום המחקר הנקרא 'תאוריה של מדעי המחשב'. מבחינה זו, הפרס הזה הוא יום חג לתחום המחקר שלי, ודאי ככל שמדובר בישראל", מסביר גולדרייך וממשיך: "ההשפעות המהפכניות של טכנולוגיית המחשבים על חיי הפרט והחברה בת־ימינו מפעימה ודומיננטית באופן שגורם לציבור הרחב לזהות את מדעי המחשב עם הטכנולוגיה הזו ולפספס את התוכן האינטלקטואלי של מדעי המחשב. אני רוצה לדבר מעט על התוכן הזה. אנחנו חוקרים את מושג 'החישוב היעיל' כאשר חישוב הוא כל תהליך שינוי הכפוף לחוקים פשוטים, ויעילות יכולה להתייחס לשורה של מדדים של שימוש במשאבים, בעיקר זמן ומקום".

את החישוב היעיל מדגים גולדרייך בשתי דוגמאות. האחת: הכפלה של מספרים (בייצוג עשרוני). בבית הספר היסודי לומדים שיטה ("אלגוריתם") לחישוב המכפלה של מספרים רבי־ספרות: מכפילים את המספר הראשון בספרה הימנית ביותר של המספר השני ורושמים את התוצאה, אחר כך מכפילים את המספר הראשון בספרה השנייה של המספר השני ורושמים את התוצאה בהזזה של ספרה אחת, וכך הלאה. מספר הפעולות (של הכפלת ספרה בספרה) שאנחנו מבצעים כאשר אנו מכפילים שני מספרים בני N ספרות היא סדר גודל של N בריבוע. אולם אפשר למצוא את המכפלה על ידי ביצוע הרבה פחות פעולות, כמעט בסדר גודל של N, שזה סדר הגודל הדרוש לחיבור מספרים כאלו.

הדוגמה הזאת חושפת את האפשרות של פער בין שיטות ידועות (אלגוריתמים ידועים) לפתרון בעיות ובין השיטות היעילות ביותר האפשריות. המחקר נע בין מציאת שיטות יעילות יותר לבין הצגת עדויות לכך ששיטות יעילות יותר לביצוע המשימה אינן קיימות. למעשה, מטרת המחקר היא לאפיין את רמת היעילות שאפשר להגיע אליה במשימות שונות. נוסף לכך, מתגלות משימות ובעיות חישוביות חדשות שעולות מתוך הבנה של יישומים אפשריים ומתוך ההיגיון הפנימי של הבנת התחום, כפי שיעלה בסוף הדוגמה הבאה.

דוגמה שנייה: בהינתן תהליך חישוב יעיל (למשל חישוב מכפלה של שני מספרים), האם אפשר למצוא תהליך יעיל אשר "הופך" אותו, כלומר, הולך מתוצרי התהליך הראשון לנתונים ההתחלתיים, למשל מן המכפלה לזוג מספרים (שווי אורך) אשר מכפלתם שווה לאותה מכפלה? יש מקרים שבהם התשובה חיובית, למשל חיבור של שני מספרים רבי־ספרות, אך נראה שיש מקרים שבהם התשובה שלילית, לדוגמה הכפלה של מספרים כאלו. הדוגמאות השליליות נקראות פונקציות חד־כיווניות ויש להם שימושים רבים בקריפטוגרפיה, היא תורת ההצפנה.

הקריפטוגרפיה מזוהה עם בנייה של שיטות לתקשורת סודית, תוך שימוש במערכות של הצפנה ופענוח של הודעות, כאשר הפענוח מבוסס על מידע סודי הנקרא "מפתח". באופן כללי, אפשר לתאר את הקריפטוגרפיה כתחום שעוסק בבנייה של מערכות יעילות לחישוב רב־משתתפים כך שקשה לחלק מן המשתתפים להסיט אותן מהפעולה הרצויה. במקרה של הצפנה מדובר במשלוח של הודעה בין שותפי סוד כך שאדם שלישי אשר רואה את התקשורת אינו מבין את תוכנה (הבנת התוכן על ידי אדם שאינו שותף סוד מוגדרת כהסטה של המערכת מפעולתה הרצויה). באופן כללי מדובר בחישוב רב־משתתפים בטוח של כל משימה שניתן לבצע כאשר כל המשתתפים הגונים לחלוטין.

"אחת מעבודותיי מראה כי כל משימה רבת־משתתפים אשר ניתנת לביצוע כאשר כל הצדדים הגונים, ניתנת לביצוע גם כאשר רק רובם הגונים", מסביר פרופ' גולדרייך. "במילים אחרות, העבודה הזאת מראה שאפשר לממש ישות דמיונית שהגונה לחלוטין ברשת תקשורת שבה רק רוב המשתתפים הגונים ואילו השאר מנסים לחבל בפעילות בכל דרך אפשרית".

לעבודה זו, כמו לעבודות אחרות בתחום הקריפטוגרפיה ובמדעי המחשב בכלל, יש יישומים רבים. בדרך כלל, היישום המעשי של עבודות תאורטיות דורש התאמות רבות, ולעיתים ראוי לומר שהוא רק מקבל השראה מהרעיונות שבבסיס העבודה התיאורטית.

נושא החורז את עשרות השנים האחרונות בפעילותו של פרופ' עודד גולדרייך הוא החינוך והעברת הידע. "אני רואה את תרומותיי העיקריות לחינוך בשני מישורים. המישור האחד הוא ההבהרה והארגון של הידע המדעי הקיים. המאמרים המדעיים נכתבים לרוב באופן הפונה למעשה רק למומחים בתחום, אשר יודעים את הרקע לעבודה ואיך המאמר הנוכחי משתלב בה. הסגנון הזה מקשה מאוד על כניסה של חוקרים חדשים לתחום, והדרך להקל עליהם היא בכתיבה של סקירות וספרי לימוד, אשר מועילים גם למומחים בתחום כי הם כוללים אינטגרציה וניסוח מחודש שקשה לעשות במאמרים רגילים".

"המישור השני של ההוראה הוא של דו־שיח ישיר עם סטודנטים אשר מתייחס לאי־ההבנות השונות שלהם, שיכולות להיות טכניות ונקודתיות או קונספטואליות וכלליות. חוץ מזה אני מקדיש תשומת לב לקושי הנפשי הכרוך בתסכולים הרבים שעולים בעת הלימוד והמחקר. לדעתי, דיבור גלוי על הקשיים הללו וחיפוש הדדי של דרכי התמודדות הוא מרכיב קריטי בהוראה ובהנחיה של דור החוקרים הבא".

להמשך מפעל החיים | סגירה

פרסומים נבחרים

חזרה לראש הדף

- **ספרים**

Modern Cryptography, Probabilistic Proofs and Pseudorandomness, Volume 17 of the Algorithms and Combinatorics series of Springer, 1998
Foundations of Cryptography, Volume 1: Basic Tools, Cambridge University Press, 2001
Foundations of Cryptography, Volume 2: Basic Applications, Cambridge University Press, 2004
Computational Complexity: A Conceptual Perspective, Cambridge University Press, 2008
P, NP, and NP-Completeness: The Basics of Complexity Theory, Cambridge University Press, 2010
A Primer on Pseudorandom Generators, ULECT series (Nr. 55), AMS, 2010
Introduction to Property Testing, Cambridge University Press, 2017

- **מאמרים נבחרים**

O. Goldreich, S. Goldwasser and S. Micali, How to Construct Random Functions. Jour. of the ACM, Vol. 33, No. 4, Oct. 1986, pp. 792-807
O. Goldreich, S. Micali, and A. Wigderson, How to Play any Mental Game or a Completeness Theorem for Protocols with Honest Majority. Proc. of the 19th ACM Symp. on Theory of Computing (STOC), 1987, pp. 218-229
W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, RSA/Rabin Functions: Certain Parts are As Hard As the Whole. SIAM J. on Computing, Vol. 17, No. 2, April 1988, pp. 194-209
B. Chor and O. Goldreich, Unbiased Bits From Sources of Weak Randomness and Probabilistic Communication Complexity. SIAM J. on Computing, Vol. 17, No. 2, April 1988, pp. 230-261
O. Goldreich, and L.A. Levin, Hard-core Predicates for any One-Way Function. Proc. of the 21st ACM Symp. on Theory of Computing (STOC), 1989, pp. 25-32
O. Goldreich, S. Micali, and A. Wigderson, Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs. Jour. of the ACM, Vol. 38, No. 3, July 1991, pp. 691-729
O. Goldreich and R. Ostrovsky Software Protection and Simulation on Oblivious RAMs. Jour. of the ACM, Vol. 43, No. 3, 1996, pp. 431-473
M. Bellare, O. Goldreich and M. Sudan, Free Bits, PCPs and Non-Approximability Towards Tight Results. SIAM J. on Computing, Vol. 27, No. 3, June 1998, pp. 804-915
O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation. Jour. of the ACM, July 1998, pp. 653-750
B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, Private Information Retrieval. Jour. of the ACM, Vol. 45, No. 6, November 1998, pp. 965-982
O. Goldreich and D. Ron, Property Testing in Bounded Degree Graphs. Algorithmica, Vol. 32 (2), 2002, pp. 302-343
O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length. Jour. of the ACM, Vol. 53, No. 4, July 2006, pp. 558-655

E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding. SIAM J. on Computing, Volume 36, No. 4, 2006, pp. 889-974

O. Goldreich and D. Ron, On Proximity Oblivious Testing. SIAM J. on Computing, Volume, Vol. 40, No. 2, 2011, pp. 534-566

B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (Im)possibility of Software Obfuscation. Jour. of the ACM, Vol. 59, No. 2, Art. 6, April 2012