

יסודות חישוב בטוח: בטיחות מושלמת והוגנות

חיבור לשם קבלת התואר "דוקטור לפילוסופיה"

מאת:

גלעד אשרוב

המחלקה למדעי המחשב

הוגש לסנט של אוניברסיטת בר-אילן

אדר א', תשע"ד

רמת גן

עבודה זו נעשתה בהדרכתו של

פרופ' יהודה לינדל

מן המחלקה למדעי המחשב של אוניברסיטת בר-אילן

תוכן עניינים

1	1 מבוא
1	1.1 חישוב בטוח
3	1.2 בטיחות מושלמת
3	1.2.1 הוכחה מלאה לפרוטוקול BGW (פרק 2)
4	1.2.2 פרוטוקול כפל יעיל עם בטיחות מושלמת (פרק 3)
5	1.3 הוגנות מלאה בחישוב בטוח לזוג משתתפים
6	1.3.1 הוגנות בחישוב בטוח - עבודות קודמות
8	1.3.2 העבודה של גורדון, חזאי, כץ ולינדל [58]
9	1.3.3 אפיון מלא של הטלת מטבע (פרק 4)
10	1.3.4 לקראת אפיון מלא של הוגנות מלאה
11	1.4 ארגון ומבנה החיבור
13	I בטיחות מושלמת
15	2 הוכחה מלאה לפרוטוקול BGW
15	2.1 מבוא
15	2.1.1 הפרוטוקול של BGW
16	2.1.2 תוצאות המחקר
19	2.2 הגדרות
19	2.2.1 בטיחות מושלמת בנוכחות יריב סקרן
20	2.2.2 בטיחות מושלמת בנוכחות יריב סקרן
22	2.2.3 מודולריות ומשפטי הרכבה
23	2.3 סכימת שיתוף סוד של שמיר [94] ותכונותיה
23	2.3.1 הסכימה הבסיסית
24	2.3.2 תכונות בסיסיות
27	2.3.3 הצגה בכתב מטריצה
27	2.4 הפרוטוקול כנגד יריב סקרן
27	2.4.1 סקירה כללית
29	2.4.2 חישוב פרטי במודל הכלאיים F_{mult}
35	2.4.3 חישוב פרטי של פונקציונאליות F_{mult}
41	2.4.4 סיכום
41	2.5 שיתוף סוד הניתן לאימות
41	2.5.1 רקע

42	Reed-Solomon של הקוד	2.5.2
43	פולינומים בשני משתנים	2.5.3
46	פרוטוקול לשיתוף סוד הניתן לאימות	2.5.4
49	שיתוף פולינום בשני משתנים	2.5.5
57	פרוטוקול לכפל בנוכחות יריב שקרן	2.6
57	סקירה כללית	2.6.1
59	פונקציונאליות המודעות לזהות המושחתים והשימוש בהן	2.6.2
63	כפל מטריצה בנוכחות יריב שקרן	2.6.3
69	הפונקציונאליות $F_{VSS}^{subshare}$ לשיתוף חלקי סוד	2.6.4
75	הפונקציונאליות F_{eval} לשערוך פולינום מחולק	2.6.5
81	הפונקציונאליות F_{VSS}^{mult} לשיתוף מכפלת חלקי סודות	2.6.6
91	הפונקציונאליות F_{mult} והמימוש שלה	2.6.7
99	חישוב בטוח במודל הכלאיים (F_{VSS}, F_{mult})	2.7
99	חישוב בטוח של כל פונקציונאליות	2.7.1
103	סיבוכיות תקשורת וסבב־תקשורת	2.7.2
104	בטיחות אדפטיבית, הרכבות והמודל החישובי	2.8
106	מכפלה למקרה של $t < n/4$	2.9

3 פרוטוקול כפל יעיל עם בטיחות מושלמת

109	מבוא	3.1
109	סקירה כללית של פרוטוקול הכפל	3.1.1
110	פונקציונאליות $F_{VSS}^{subshare}$ ללא עלות	3.1.2
111	תוצאות המחקר	3.1.3
112	הגדרות	3.2
112	תכונות של פולינומים בשני משתנים	3.2.1
114	שיתוף סוד הניתן לוידוא לפולינום בשני משתנים	3.2.2
114	פרוטוקול הכפל	3.3
114	סקירה כללית	3.3.1
116	הפונקציונאליות \tilde{F}_{extend} להמרת פולינום עם משתנה יחיד לשני משתנים	3.3.2
119	הפונקציונאליות \tilde{F}_{eval} לשערוך פולינום מחולק בשני משתנים	3.3.3
122	הפונקציונאליות \tilde{F}_{VSS}^{mult} לשיתוף מכפלת חלקי סודות	3.3.4
129	הפונקציונאליות \tilde{F}_{mult} והמימוש שלה	3.3.5
133	סיכום - פרוטוקול עם בטיחות מושלמת	3.3.6

II הוגנות מושלמת בחישוב בטוח לזוג משתתפים

4 אפיון מלא של פונקציות הגוררות הטלת מטבע

137	מבוא	4.1
141	הגדרות	4.2
141	חישוב בטוח בשני משתתפים עם הוגנות - יריב שקרן	4.2.1
142	חישוב בטוח בשני משתתפים ללא הוגנות	4.2.2
143	עולם כלאיים והרכבה	4.2.3
144	הגדרות הטלת מטבע	4.2.4

145	הקריטריון	4.3
145	פונקציה δ -מאוזנת	4.3.1
146	הקריטריון	4.3.2
147	חקר תכונת δ -מאוזנת	4.3.3
148	פונקציות מאוזנת גוררות הטלת מטבע	4.4
150	פונקציות לא מאוזנות אינן גוררות הטלת מטבע (במודל תורת האינפורמציה)	4.5
166	הוגנות בנוכחות יריב פרשן	4.6
167	מודל יריב פרשן 1	4.6.1
168	מודל יריב פרשן 2	4.6.2

5 לקראת איפיון מלא של הוגנות

175	מבוא	5.1
177	תוצאות המחקר	5.1.1
179	הגדרות	5.2
179	חישוב בטוח - הגדרות	5.2.1
180	רקע מתמטי	5.2.2
182	הפרוטוקול של גורדון, חזאי, כץ ולינדל [58]	5.3
182	הפרוטוקול	5.3.1
183	בטיחות	5.3.2
186	הקריטריונים	5.4
186	היתכנות של פונקציות ממימד מלא	5.4.1
191	פונקציות שאינן ממימד מלא	5.4.2
195	סיכום: פונקציות בוליאניות סימטריות עם תחום סופי	5.4.3
197	הרחבות: פונקציות לא סימטריות ופונקציות לא בינאריות	5.5
197	פונקציות לא סימטריות	5.5.1
199	פונקציות לא בינאריות	5.5.2

א' תיאור מלא של פרוטוקול BGW

205	הפרוטוקול כנגד יריב שקרן	א'1
205	הגדרות פונקציונאליות	א'1.1
206	הפרוטוקולים	א'1.2
207	הפרוטוקול כנגד יריב שקרן	א'2
207	הגדרות הפונקציונאליות	א'2.1
210	הפרוטוקולים	א'2.2

ב' תיאור מלא של פרוטוקול יעיל לכפל

217	הגדרות פונקציונאליות	ב'1
219	הפרוטוקולים	ב'2

ג' הוכחת פטיחות לפרוטוקול 5.3.3

223	בטיחות כנגד P_2 מושחת	ג'1
224	בטיחות כנגד P_1 מושחת	ג'2

תקציר העבודה

רקע - חישוב בטוח

קריפטוגרפיה בדרך כלל מזוהה עם "הצפנה" - כיצד ניתן לאפשר לשני צדדים מרוחקים לקיים דו־שיח בצורה חופשית ופרטית, ולמנוע מצד שלישי המאזין לשיחה ללמוד את תוכנה. אולם, קריפטוגרפיה מודרנית היא הרבה מעבר לכך. האתגרים הקריפטוגרפיים כיום כוללים מספר שחקנים, המעוניינים לבצע איזשהו חישוב על הקלטים הפרטיים שלהם תוך כדי שמירתם כסודיים. דוגמאות לחישובים כאלה כוללים:

- בעיית המליונר. נניח ששני אילי הון נפגשים ומעוניינים לגלות למי משניהם יש יותר כסף בבנק. אולם, אף צד לא רוצה לחשוף בפני השני מהו בדיוק הונו העצמי. כיצד ניתן לאפשר לשני הצדדים ללמוד למי יש יותר כסף, מבלי שכל צד יחשוף בפני השני שום מידע אחר לגבי כמות הכסף שיש לו?

- הצבעה אלקטרונית ברשת. נניח שמספר משתמשים ברשת החברים באיזשהו ארגון, מעוניינים לנהל הצבעה ("בחירות") לתפקיד היושב ראש. אולם, הצבעתו של כל משתתף היא חשאית, וצריכה להישאר כזו כנגד כל שאר החברים בארגון. בנוסף לזאת, נרצה שגם המשתתפים יוכלו לוודא שההצבעה התנהלה כסדרה, שכל משתתף בחר את הצבעתו באופן בלתי תלוי באחר ועוד. כיצד ניתן לערוך בחירות שכאלה ברשת?

- חישוב על מסד־נתונים משותף. נניח את המצב שבו שני בתי חולים מחזיקים נתונים רפואיים על הלקוחות שלהם, המכילים מידע רגיש ופרטי על כל לקוח, כגון: מחלות, רקע משפחתי ואישי, הרגלים וכדומה. נניח שאחד מבתי החולים מעוניין לבצע מחקר מדעי ומעמיק על מחלה מסויימת, ובכדי להגיע לתוצאות האופטימליות הוא נדרש לכמה שיותר נתונים על כמה שיותר חולים. אולם, כל אחד מבתי החולים מחוייב לשמור על פרטיות החולים שלו, ואינו מורשה להעביר את הנתונים שלו לאיזשהו צד אחר או כל גורם שהוא, ובפרט אינו מורשה להעביר את המידע לבית החולים האחר. כיצד ניתן לבצע חישוב על מסד הנתונים המשותף תוך כדי שמירת הפרטיות של כל חולה, ומבלי שבית חולים אחד יעביר מידע לא הכרחי לבית החולים האחר?

- גישה למסד נתונים תוך כדי שמירה על פרטיות. כולנו ניגשים בכל יום למנוע החיפוש של "גוגל", מבצעים שאילתא ומקבלים תשובה. הפעולה הזו היא למעשה גישה למסד נתונים: צד אחד ("גוגל") מכיל את מסד הנתונים, וכל פעם שאנו מחפשים מידע באתר - אנו למעשה מתשאלים אותו. לעיתים, השאילתות מכילות מידע רגיש כגון: שאלות אישיות, מחלות, אירועים מביכים, מוגבלויות וכו'. מלבד העובדה שהיינו רוצים להסתיר את השאילתות מכל גורם אחר ברשת העלול להאזין לתקשורת, ייתכן שגם נרצה לפעמים להסתיר את השאילתות מ"גוגל" עצמו. כיצד ניתן לתשאל מסד נתונים ולקבל תשובה, מבלי שמסד הנתונים עצמו יידע על מה נשאל?

- מכרזים אלקטרוניים. נניח שמספר חברות מעוניינות לבצע מכרז אלקטרוני לאיזשהו חוזה עבודה על גבי רשת האינטרנט, כך שההצעה הנמוכה ביותר תקבל את החוזה. נרצה להבטיח שההצעה של כל

אחד מהמשתתפים תיבחר באופן בלתי תלוי אחת בשנייה, ושהחברות יוכלו לוודא שההצעה שזכתה היא באמת ההצעה הנמוכה ביותר. כיצד ניתן לבצע מכרז אלקטרוני המבטיח זאת?

כל המשימות שהוצגו לעיל, הן למעשה דוגמאות ומקרים פרטיים של בעיה כללית הרבה יותר ושה נעסוק במסגרת חיבור זה - בעיית **חישוב בטוח**. בבעיה זו אנו מעוניינים לאפשר למספר שחקנים (משתתפים), שאינם בוטחים אחד בשני, לבצע חישוב על הקלטים הפרטיים שלהם מבלי שכל צד ילמד מידע כלשהו על קלטו של האחר. אנו מעוניינים לספק לשחקנים המשתתפים פרוטוקול - סדרת הוראות ברורות ומפורטות כיצד לתקשר אחד עם השני (תוכנית מחשב אינטראקטיבית) ולחשב יחדיו את הפונקציה (המשימה). ריצה של הפרוטוקול תהיה מורכבת ממספר סיבובי תקשורת, כאשר בכל סיבוב ניתן לכל שחקן הוראות כיצד לחשב את ההודעה הבאה שעליו לשלוח על סמך ההודעות שקיבל בסיבובים הקודמים והקלט שלו. בסיום הריצה הצדדים ילמדו את הפלטים לפי הפונקציה שאותה הם מעוניינים לחשב, אך שום דבר מעבר לכך. לדוגמה, במקרה של "בעיית המליונר", נניח שהקלט של השחקן הראשון הוא איזשהו סכום x_1 , הקלט של השחקן השני הוא x_2 , והפונקציה שלמעשה המשתתפים רוצים לחשב היא האם $x_1 > x_2$. נרצה ששני הצדדים ילמדו האם $x_1 > x_2$ ושום דבר מעבר; בפרט, המשתתף הראשון לא ילמד כלום על הערך x_2 , והמשתתף השני לא ילמד דבר על הערך x_1 . באופן כללי נעסוק בחישוב רב משתתפים ("secure multiparty computation"), כמו שראינו בדוגמה של במכרזים אלקטרוניים לעיל. לעיתים, נעסוק בחישוב עם שני משתתפים בלבד ("secure two-party computation"), כמו בדוגמת בעיית המליונר שהוזכרה לעיל.

נרצה להגן על פרטיות הקלטים גם כאשר חלק מהמשתתפים אינם פועלים על פי הוראות הפרוטוקול, משתתפים פעולה ביניהם ומתאמים ביניהם את ההודעות שאותם הם שולחים. למעשה, נחלק את המשתתפים לשתי קבוצות: הקבוצה הראשונה תהיה קבוצת המשתתפים ה"הגונים" - אלו שעוקבים אחר הוראות הפרוטוקול, והקבוצה השנייה תהיה קבוצת ה"מושחתים", אלו המנסים ללמוד מידע נוסף או שאינם עוקבים אחר הוראות הפרוטוקול. נניח שקבוצות המושחתים נשלטת על ידי ישות חיצונית עוינת ("יריב"), ובצורה זו נמדל את העובדה שהשחקנים המושחתים מתאמים את פעולותיהם. כמובן שאנו, כמתכנני הפרוטוקול, לא יודעים את זהויות השחקנים שהיריב החליט להשחית, והמשתתפים ההגונים בזמן ריצת הפרוטוקול לא יודעים דבר לגבי כל שאר המשתתפים - האם הם הגונים או לא.

בטיחות בחישוב בטוח. פרוטוקולים לחישוב בטוח צריכים לעמוד בפני כל מתקפה שהיריב עלול לבצע. כדי להוכיח באופן פורמלי שפרוטוקול הינו "בטוח", אנו נדרשים להגדרת בטיחות פורמלית. לפני שניגש להגדרה עצמה, נפרט קודם מהן דרישות הבטיחות שפרוטוקול בטוח צריך למלא:

- פרטיות: נרצה להבטיח שהיריב לא יוכל ללמוד שום מידע על הקלטים של המשתתפים ההגונים, מלבד מה שנחשף ממילא על ידי פלט החישוב. לדוגמה, נתבונן בדוגמה של חוזה עבודה שהוזכרה לעיל, כאשר ההצעה הנמוכה ביותר מקבלת את החוזה. נניח שפלט החישוב הוא זהות הזוכה, וסכום הצעתו. ממידע זה, ברור שכולם יכולים להסיק שכל שאר ההצעות היו גבוהות יותר; אולם, נרצה להבטיח שזהו המידע הנוסף היחיד שניתן להסיק לגבי הקלטים של המשתתפים, ושום מידע אחר.
- נכוונות: נרצה שהפרוטוקול יבטיח שהפלט של החישוב יהיה נכון (כלומר, בהתאם לפונקציה אותה מחשבים), גם במקרה והיריב מנסה לשבש את ריצת הפרוטוקול. במקרה של דוגמת חוזה העבודה, על הפרוטוקול להבטיח שההצעה הנמוכה ביותר באמת תהיה זו שתזכה ותקבל את חוזה העבודה.
- אי תלות בקלטים: נרצה שכל שחקן יבחר את הקלט שלו לחישוב בצורה בלתי תלויה לקלטו של האחר. נציין שזוהי דרישה שאינה נובעת באופן טריויאלי מפרטיות, ולעיתים פרוטוקולים עלולים לאפשר לשחקנים לבחור קלט על סמך קלט של משתתף אחר, אפילו כאשר הם לא יודעים מהו הקלט של האחר. לדוגמה, נתבונן שוב בדוגמת המכרז, ונניח שבסיבוב הראשון בפרוטוקול כל משתתף מצפין את ההצעה שלו ומפרסם לאחרים. אולם, ישנן סכמות הצפנה המאפשרות ליצור הצפנה חדשה (וחוקית) מבלי לדעת את

ההודעה שהוצפנה, ובכך שחקן עלול ליצור הצפנה של הצעה נמוכה יותר מהצעה של שחקן אחר, מבלי שידע בעצמו מה למעשה הוא מציע.

• הוגנות: נרצה להבטיח שאם היריב לומד את תוצאת החישוב, אזי גם השחקנים ההגונים לומדים את התוצאה. בפרט, אנו אמורים למנוע את המצב שבו היריב למד את פלט החישוב לפני המשתתפים ההגונים, ומונע מהם ללמוד את הפלט על ידי פרישה מריצת הפרוטוקול.

כל הרשימה הזו אינה מהווה הגדרת בטיחות, אלא רק דרישות בטיחות שפרוטוקול צריך למלא. ההגדרה הפורמלית של חישוב בטוח מבוססת על תבנית "ההדמיה" (סימולציה), ששורשיה נטועים בהגדרות בטיחות של סכימות הצפנה [56]. לפי תבנית זו, אנו משווים בין פלט של ריצה אמיתית של הפרוטוקול, לבין ריצה בעולם "אידיאלי", ודורשים שלא ניתן יהיה להבחין בין שתי הריצות.

באופן מפורט יותר, בעולם האמיתי, המשתתפים מריצים בפועל את הפרוטוקול, מנהלים שיחה ביניהם ומתקשרים אחד עם השני עד ללמידת התוצאה. לעומת זאת, בעולם האידיאלי אנו מניחים שהצדדים אינם מתקשרים ביניהם כלל. בעולם זה, אנו מניחים שבנוסף לצדדים המשתתפים בפרוטוקול ישנו צד נוסף, מהימן ושאינו ברהשחתה, והמשתתפים מתקשרים עם צד מהימן זה בלבד. בפרט, הם שולחים את הקלטים שלהם לאותו צד מהימן, האחרון מחשב עבורם את הפונקציה על הקלטים שקיבל ושולח בחזרה את הפלט למשתתפים. נשים לב שעולם זה מקיים את כל דרישות הבטיחות שצינו לעיל, כלומר משמר פרטיות, נכונות, אי תלות בקלטים והוגנות.

ההגדרה הפורמלית משווה בין ריצות של שני העולמות. ראשית, נדרוש שהיריב בעולם האידיאלי יידמה את כל ההודעות הנצפות על ידי היריב בעולם האמיתי. נשים לב שהיריב בעולם האידיאלי יודע אך ורק את הקלטים והפלט של השחקנים המושחתים ושום מידע אחר; לפיכך, אם ניתן לדמות את כל ההודעות שנצפו במהלך הריצה האמיתית על סמך הקלטים והפלט הללו בלבד, אזי הודעות הנצפות במהלך הריצה לא מלמדות שום מידע נוסף (ניתן לייצרן על סמך מידע שאמור להילמד ממילא). לבסוף, נאמר על פרוטוקול שהינו בטוח, אם לכל יריב בעולם האמיתי, קיים יריב מקביל בעולם האידיאלי, כך ששתי הריצות נראות אותו הדבר. מכיוון שבעולם האידיאלי היריב לא יכול לבצע שום התקפה אמיתית, היריב בעולם האמיתי לא יכול לבצע דבר, ולכן הפרוטוקול הוא למעשה, בטוח.

היתכנות של חישוב בטוח. ישנם המון מקרים ומסגרות שבהם חישוב בטוח נלמד. היתכנות או חוסר היתכנות של חישוב בטוח תלוי בהמון גורמים, כגון מהו סוג היריב שאותו מניחים, מהי יכולתו החישובית, מהי תשתית התקשורת ועוד. לגבי היריב, לעיתים מניחים יריב "סקרן", העוקב אחר הוראות הפרוטוקול אך מנסה לדלות מידע נוסף על קלטי השחקנים ההגונים על ידי שילוב כל ההודעות הנצפות על ידי השחקנים המושחתים. לעיתים מתמקדים ביריב חזק יותר, היכול בנוסף גם להפר את הוראות הפרוטוקול (כלומר, לא לשלוח הודעות לפי מה שהוגדר בפרוטוקול), ולעיתים גם לפרוש במהלך הריצה. ליריב זה אנו קוראים בשם יריב "סקרן". בנוסף, אנו מתייחסים ליכולת החישובית של היריב. לעיתים אנו מניחים שהיריב מוגבל לרוץ בזמן פולינומי בקלט שלו, ולעיתים אנו מניחים יריב שאינו מוגבל חישובית. בנוסף, היריב יכול להיות "סטטי" ("נייח"), כלומר הוא מחליט על זהויות המשתתפים שאותם הוא משחית עוד לפני תחילת ריצת הפרוטוקול, או "אדפטיבי" ("נייד"), כזה שמחליט תוך כדי ריצה ולפי התקדמותה על זהות השחקנים שאותם הוא משחית.

באופן מפתיע, חישוב בטוח הוא אפשרי ברוב המקרים. בפרט, כאשר רוב המשתתפים הינם הגונים, חישוב בטוח הוא אפשרי לכל פונקציה¹ תחת ההגדרה הלא פורמלית שהוזכרה לעיל. לעומת זאת, אנו יודעים שקיימות פונקציות שלא ניתן לחשב באופן בטוח כאשר לא מובטח רוב הגון [34], ולכן בפרט המקרה של שני שחקנים כאשר אחד הצדדים עלול להיות מושחת. עבור פונקציות אלו, תכונת הבטיחות המופרת היא "הוגנות", ותוצאת אי התכנות זו מראה שלמעשה לא קיים פרוטוקול כללי הממלא את כל דרישות הבטיחות שצינו לעיל. אולם,

¹ לכל פונקציה - הכוונה היא לכל "משימה" (דוגמאות למשימות אפשריות הובאו בתחילת הפרק). כמובן, אנו מתמקדים רק במשימות שניתנות לחישוב בזמן יעיל, כלומר, ניתנות לחישוב בזמן פולינומי בקלטים.

קיימים פרוטוקולים המשיגים את כל דרישות הבטיחות הללו עלבד הוגנות. הגדרת הבטיחות משתנה בהתאם, כאשר אנו משנים את העולם האידיאלי לעולם פחות "מושלם", על ידי כך שהיריב יוכל ללמוד את הפלט ללא השחקנים ההגונים גם בעולם האידיאלי, לפי בחירתו.

תוצאת ההיתכנות הראשונה לחישוב בטוח ניתנה על ידי Yao [100] בשנת 1986 במודל החישובי וליריב סקרן, למקרה של שני שחקנים. תוצאות היתכנות אחרות הוצגו לקראת סוף שנות השמונים. המרכזיים שבהם מובאים להלן, כאשר אנו מניחים שהיריב הינו מסוג "סקרן" (t מייצג את מספר השחקנים המושחתים, ו- n מייצג את סך השחקנים המשתתפים):

1. עבור $t < n/3$, חישוב בטוח אפשרי לכל פונקציה (עם הוגנות), במודל שבו לכל זוג שחקנים יש ערוץ תקשורת ביניהם. תוצאה זו אפשרית גם למודל שבו כוחו החישובי של היריב מוגבל (תחת הנחות קושי מתאימות) [54], וגם למודל שבו כוחו החישובי של היריב אינו מוגבל [22, 32].

2. עבור $t < n/2$, חישוב בטוח אפשרי לכל פונקציה (עם הוגנות), כאשר אנו מניחים שלשחקנים יש גישה לערוץ שידור (broadcast channel)². תוצאה זו אפשרית גם כאשר כוחו החישובי של היריב מוגבל (תחת הנחות קושי מתאימות) [54], וגם למודל יריב לא מוגבל (עם בטיחות סטטיסטית) [92].

3. עבור $t \leq n$, חישוב בטוח אפשרי לכל פונקציה ללא הוגנות. תוצאה זו אפשרית רק במודל שבו היריב מוגבל מבחינה חישובית, תחת הנחות הקושי המתאימות כאשר אנו מניחים שלמשתתפים יש גישה לערוץ שידור [54, 53].

בעיית חישוב בטוח היא בעיה מאוד כללית ויסודית בקריפטוגרפיה. בעיה זו יכולה למדל כמעט כל בעיה קריפטוגרפית וכל חישוב מבוזר, כולל בעיות פשוטות כגון הטלת מטבע ושידור, וכן בעיות מורכבות כפי שראינו לעיל. היא הועלתה בשנת 1982 על ידי Yao [99], ונלמדה באופן נרחב ומעמיק מאז ועד היום. במסגרת חיבור זה, נעסוק בשאלות יסודיות ובסיסיות של התחום, ונתעמק בשני הבטים של חישוב בטוח: בטיחות מושלמת ו-הוגנות.

חלק ראשון - בטיחות מושלמת

חיבור זה מורכב משני חלקים וחמישה פרקים (כאשר הפרק הראשון הוא ההקדמה). בחלק הראשון של חיבור זה (פרקים 2 ו-3) נעסוק בבטיחות מושלמת. פרוטוקול הבטוח בצורה מושלמת עמיד בפני יריב שאינו מוגבל חישובית, והבטיחות מובטחת ללא תנאי ואינה מבוססת על שום הנחת קושי חישובית. כלומר, הפרוטוקול עמיד בפני כל מחשב על, וכל מחשב שיהיה קיים בעתיד.

פרק 2 - הוכחה מלאה לפרוטוקול של BGW

אחת מהתוצאות הקלאסיות והיסודיות של חישוב בטוח הוצגה בשנת 1988, על ידי בן-אור, גולדווסר ווידגרסון [22] (Ben-Or, Goldwasser and Widgerson (BGW)). השלושה הראו שניתן לחשב כל פונקציה עם בטיחות מושלמת במודל תקשורת שבו לכל זוג שחקנים יש ערוץ תקשורת פרטי, כל עוד היריב מוגבל להשחית חלק מוגבל מהמשתתפים. כאשר היריב הוא "סקרן" ניתן לחשב כל פונקציה כאשר היריב מוגבל להשחית עד חצי מהשחקנים המשתתפים, וכאשר היריב הוא "סקרן" ניתן לחשב כל פונקציה כל עוד היריב משחית פחות משליש מהשחקנים המשתתפים.

²ערוץ תקשורת שבו כל משתתף יכול לשדר הודעה לכל המשתתפים. שידור הודעה דומה למעין פרסום הודעה ב"רדיו", או ב"מערכת כריזה", כלומר כל המשתתפים שומעים בדיוק אותה הודעה. זאת בניגוד לערוץ תקשורת פרטי הדומה יותר לדיבור בטלפון - הודעה שבין שני אנשים בלבד, ולשום צד אחר אין מושג מה הועבר בדו-שיח שביניהם.

תוצאות המחקר. לפרוטוקול של BGW יש חשיבות מכרעת על חישוב בטוח, המון מאמרים מסתמכים עליו והשפעתו על תחום המחקר היא עצומה. לצערנו, על אף החשיבות הגדולה שלו, מעולם לא נכתבה לו הוכחת בטיחות מלאה. במסגרת חיבור זה, אנו מתקנים זאת ומביאים לראשונה הוכחת בטיחות מלאה לפרוטוקול. ההוכחה כוללת תיאור מפורט ומדויק של הפרוטוקול גם למקרה של יריב "שקרן", וכוללת הגדרה זהירה של הפונקציונאליות ותתי-הפונקציונאליות הנמצאים בשימוש בפרוטוקול, כפי שנצרך לשם הצגת הוכחה מודולרית. הצגת הוכחה מלאה לפרוטוקול של BGW משלימה אבן יסוד חשובה בתיאוריה של "חישוב בטוח". המשפט העיקרי שאותו הוכחנו הוא המשפט (הלא פורמלי) המובא להלן:

משפט 1 תחת ההנחה של רשת תקשורת סנכרונית עם ערוצי תקשורת פרטיים בין כל זוג משתתפים וערוץ שידור פומבי:

1. יריב סקרן: לכל פונקציה f עם n -קלטים, קיים פרוטוקול המחשב את f עם בטיחות מושלמת כנגד יריב סקרן סטטי, השולט על $n/2 < t$ משתתפים.

2. יריב שקרן: לכל פונקציה f עם n -קלטים, קיים פרוטוקול המחשב את f עם בטיחות מושלמת כנגד יריב שקרן סטטי, השולט על $n/3 < t$ משתתפים.

נציין שבשני המקרים, הפרוטוקול הוא אופטימלי מבחינת מספר המשתתפים שניתן להשחית. כלומר, קיימות פונקציות עם n -קלטים שלא ניתנות לחישוב בטוח כאשר יריב סקרן שולט על $n/2$ משתתפים, ומן הצד השני, קיימות פונקציות עם n -קלטים שלא ניתנות לחישוב בטוח כנגד יריב שקרן השולט על $n/3$ משתתפים. אנו מוכיחים את משפט 1 במודל הבסיסי, שבו אנו מניחים יריב סטטי ושמתיקיימת ריצה בודדה של הפרוטוקול בזמן נתון. אולם, על ידי שימוש במשפטים המראים שבטיחות מושלמת תחת הנחות מסוימות גוררת בטיחות מושלמת במודל עם יריבים חזקים יותר, אנו מקבלים בטיחות במודל חזק יותר "בחינם". בפרט, אנו מראים שהבטיחות נשמרת גם כאשר מספר ריצות של הפרוטוקול מתרחשות במקביל. בנוסף, אנו מסיקים בטיחות גם עבור יריב אדפטיבי (אולם, תחת סימולטור לא יעיל). לבסוף, אנו מסיקים שבמקום להניח ערוצי תקשורת פרטיים בין השחקנים אפשר להניח ערוצי תקשורת מאומתים בלבד, ולקבל גירסא של המשפט תחת יריב המוגבל מבחינה חישובית (עם הנחת תשתית תקשורת חלשה הרבה יותר).

פרק 3 - פרוטוקול כפל יעיל עם בטיחות מושלמת

בנוסף לאמור לעיל, הבחנו שעל ידי שינויים קלים וטבעיים לפרוטוקול, ניתן לפשט את הבנייה בצורה משמעותית ואחד מתתי הפרוטוקול היקרים ביותר (ואולי המסובכים ביותר) הוא למעשה מיותר וניתן להשמיטו. אנו מציגים פרוטוקול חדש המבוסס על הבנייה המקורית, שהוא גם פשוט וגם יעיל יותר, ומוכיחים את בטיחותו באופן מלא. כפי שצוין לעיל, הפרוטוקול שלנו משיג גם הוא בטיחות מושלמת, ולפיכך אנו יכולים להסיק ממנו בטיחות למודלים של יריבים חזקים יותר, בדיוק כפי שעשינו בהוכחה של BGW בפרק הקודם.

הוגנות בחישוב בטוח לזוג משתתפים

בחלק השני של חיבור זה (פרקים 4 ו-5), אנו מתמקדים בהוגנות בחישוב בטוח לשני שחקנים. באופן לא פורמלי, אנו אומרים על פרוטוקול שהינו הוגן אם הוא מבטיח שבמקרה והיריב לומד את תוצאת החישוב אזי גם המשתתפים ההגונים לומדים את התוצאה. להוגנות יש חשיבות מיוחדת בפונקציות כגון חתימה על חוזים. בפרט, המצב עלול להיות מאוד בעייתי אם הצד המושחת קיבל חוזה חתום, כאשר ההגון לא. כפי שהוזכר לעיל, חישוב בטוח הכולל הוגנות אינו אפשרי ללא רוב הגון, ולכן בפרט במקרה של שני משתתפים. למעשה, בשנת 1986, Cleve [34] הראה תוצאת אי-התכנות האומרת שלא ניתן לבנות פרוטוקול כללי המבטיח הוגנות ללא רוב הגון. בפרט, Cleve הראה שהמשימה הפשוטה יחסית של "הטלת מטבע", שבה זוג שחקנים מסכימים על מטבע אקראי, בלתי אפשרית לחישוב בטוח עם הוגנות. מאז פרסום תוצאה זו, למעלה

משני עשורים, האמונה הרווחת הייתה שלא ניתן לחשב אף פונקציה לא טריוויאלית עם הוגנות במקרה של שני משתתפים. המחקר מאז התמקד בכיצד ניתן להשיג "הוגנות חלקית" (שבה צד אחד לומד יותר מהאחר, אבל לא בצורה משמעותית), או מודלים אחרים שבהם סוג כלשהו של הוגנות הוא אפשרי, אך זנח ויותר לחלוטין על הוגנות מלאה, שכן נראה היה שלא ניתן להשיגה.

אינטואיטיבית, קשה להשיג הוגנות בשני שחקנים. זאת מכיוון שבכל פרוטוקול שמחשב פונקציה לא טריוויאלית³, השחקנים עוברים ממצב של חוסר ידיעה לגבי הפלט למצב של ידיעה מוחלטת לגביו. פרוטוקולים מתנהלים על ידי משלוח הודעות בין הצדדים ובסבבי תקשורת, כאשר בכל סבב תקשורת שכזה השחקנים לא יכולים להעביר מידע בו זמנית (ראשית השחקן הראשון מעביר הודעה לשחקן השני, ולאחר מכן השחקן השני מעביר הודעה לראשון וכן הלאה). לכן, לכאורה, חייבת להיות נקודה בריצת הפרוטוקול שבה לצד אחד יש יותר מידע לגבי הפלט מאשר הצד השני. בשלב זה, אם אותו צד פורש מריצת הפרוטוקול, הוא יכול ללמוד את הפלט לבדו, או לפחות, יכול לנחש אותו טוב יותר מאשר הצד ההגון, ותכונת ההוגנות מופרת. לפיכך, האמונה הרווחת הייתה ששום דבר לא ניתן לחשב עם הוגנות מלאה מלבד מספר מצומצם של פונקציות טריוואליות ולא מעניינות.

התפיסה שלנו לגבי הוגנות שונתה לאחרונה (2008) מן היסוד עם עבודתם של גורדון, חזאי, כץ ולינדל [58]. הארבעה הראו שקיימות פונקציות לא טריוואליות הניתנות לחישוב בטוח לשני שחקנים עם הוגנות מלאה. עבודה זו הראתה שלמעשה הבעיה רחוקה מלהיות סגורה. העובדה שקיימות פונקציות שלא ניתנות לחישוב עם הוגנות, וקיימות פונקציות אחרות שכן ניתנות לחישוב עם הוגנות, העלתה את השאלה היסודית הבאה:

אילו פונקציות ניתן לחשב עם הוגנות מלאה?

למעשה, היינו רוצים להבין מתי הוגנות מלאה היא אפשרית ומתי אינה אפשרית. אנו מתעניינים באפיון מלא וסיווג הפונקציות, ונרצה למצוא איזשהו "כלל", או "תכונה" שיורו לנו האם ניתן לחשב פונקציה נתונה עם הוגנות מלאה. הוגנות היא תכונת בטיחות חשובה, וההבנה מתי ניתן ומתי לא ניתן להשיגה היא שאלה בסיסית ויסודית בתיאוריה של חישוב בטוח.

מאז עבודתם של [58], לא פורסמו עבודות נוספות המעמיקות את ההבנה שלנו לגבי אלו פונקציות בוליאניות ניתן לחשב עם הוגנות מלאה במקרה של שני שחקנים. בפרט, תוצאת אי-ההתכנות של Cleve היא תוצאת אי-ההתכנות היחידה, והפונקציות הבודדות ש-[58] הראו שאפשריות לחישוב עם הוגנות מלאה הן הפונקציות היחידות שאנחנו יודעים לחשב עם הוגנות. לפיכך, ישנה מחלקה גדולה של פונקציות שלגביה אין לנו מושג אם ניתן לחשבן עם הוגנות, או לא.

פרק 4 - אפיון מלא של הטלת מטבע

בפרק 4 אנו מתמקדים בעבודתו של Cleve [34] ולומדים אלו פונקציות נשללות בגלל תוצאת אי התכנות זו. למעשה, אנו שואלים אלו פונקציות (בוליאניות) גוררת הטלת מטבע, כלומר, אנו שואלים מהן בדיוק הפונקציות שאם ניתן היה לחשב אותן עם הוגנות, אזי ניתן היה לקבל פרוטוקול הוגן להטלת מטבע (בסתירה לתוצאת אי התכנות של [34]). לפיכך, כל פונקציה שכזו תהיה בלתי אפשרית לחישוב עם הוגנות מלאה. אנו מגדירים תכונה פשוטה (קריטריון) על טבלת האמת של פונקציה בוליאנית. אנו מראים שכל פונקציה שמקיימת את התכונה גוררת הטלת מטבע, ולכן לא ניתן לחשב אותה עם הוגנות.

החלק המעניין יותר מבחינה טכנית, והמאתגר הרבה יותר היא ההוכחה שהקריטריון שהגדרנו הוא הדוק. בפרט, אנו מראים שכל פונקציה שלא מקיימת את התכונה, אינה גוררת מטבע (במודל תורת האינפורמציה). באופן מפורט יותר, אנו מניחים עולם כלאיים (היברידי) שבו השחקנים יכולים, בנוסף לשליחת הודעות ביניהם, גם לגשת לצד מהימן שלישי המחשב עבורם בצורה הוגנת ואידיאלית פונקציה שלא מקיימת את התכונה. אנו מראים שלכל פרוטוקול להטלת מטבע בעולם כלאיים שכזה (ולכל פונקציה שלא מקיימת את התכונה), קיים

³בהקשר שלנו, פונקציה טריוואלית היא פונקציה קבועה, פונקציה שבה הפלט נקבע על סמך קלט של שחקן יחיד, או פונקציה שבה רק צד אחד אמור ללמוד פלט. כל פונקציה כזו קל לראות שניתן לחשב עם הוגנות מלאה.

יריב (לא יעיל) המטה את תוצאת המטבע. קיום יריב שכזה מוכיח שלמעשה לא ניתן להשתמש בפונקציה כזו לשם קבלת מטבע.

אנו מדגישים שתוצאת אי ההתכנות הזו היא למעשה מקור לאופטימיות, שכן פונקציות שאינן גוררות מטבע ייתכן וניתן לחשב בצורה בטוחה עם הוגנות מלאה. לכן, אפיון מלא של פונקציות הגוררות הטלת מטבע מעמיק את ההבנה שלנו במה לא ניתן לחשב בצורה בטוחה עם הוגנות מלאה, ומאפשר לנו להתמקד בפונקציות שיש פוטנציאל לחשב אותן בצורה בטוחה עם הוגנות מלאה.

פרק 5 - לקראת אפיון של הוגנות מלאה

בחלק האחרון של החיבור, אנו מתמקדים בפונקציות בוליאניות עם תחום סופי ושואלים אלו פונקציות ניתן לחשב עם הוגנות מלאה.

אנו מוצאים קשר מעניין בין הוגנות ובין ייצוג גיאומטרי של הפונקציה, ומראים למעשה שכל פונקציה המגדירה אובייקט גיאומטרי ממימד מלא, ניתן לחשב בצורה בטוחה עם הוגנות מלאה. למעשה, אנו מגדירים תכונה פשוטה, ומראים שכל פונקציה המקיימת את התכונה ניתן לחשב עם הוגנות. זהו צעד נוסף ומשמעותי בדרך לאיפיון מלא להוגנות.

התוצאה שלנו מראה שקיימות יותר פונקציות הניתנות לחישוב עם הוגנות מלאה ממה שחשבנו והאמנו במשך שנים. בניגוד לאמונה שרווחה למעלה מ-20 שנה ולפיה הוגנות מלאה בלתי אפשרית לכל הפונקציות הלא-טרייבוליות, אנו מראים שהוגנות מלאה אפשרית כמעט תמיד בפונקציות בהן התחומים של שני השחקנים מגודל שונה (כלומר, פונקציות $f : X \times Y \rightarrow \{0, 1\}$ כאשר $|X| \neq |Y|$). חשוב לציין שלמרות שאנו מתמקדים בפונקציות עם ביט בודד של פלט, המחלקה שאנו דנים בה מכילה המון משימות לא פשוטות ומעניינות, כגון - בדיקת שייכות לקבוצה, שערך פונקציה בוליאנית תוך שמירה על פרטיות, שידוך פרטי, בדיקת חיתוך ריק ועוד. מתברר שכל הבעיות הללו, להפתעתנו, ניתנות לחישוב בטוח עם הוגנות מלאה.

אנו מדגישים כי האיפיון שהגענו אליו בפרקים 4 ו-5 אינו מלא, וקיימות פונקציות שאיננו יודעים האם הן ניתנות לחישוב עם הוגנות או לא. אנו מראים שכמעט כל פונקציה שבה גודל התחומים הוא זהה (כלומר, כמעט כל פונקציה $f : X \times Y \rightarrow \{0, 1\}$ עם $|X| = |Y|$), לא ניתנת לחישוב בעזרת הפרוטוקול הספציפי שהציגו [58] (עם גישת הסימולציה הספציפית שהציגו). כמובן שתוצאת אי התכנות זו אינה אומרת שלא ניתן לחשב את הפונקציות האלה עם פרוטוקול אחר, אבל היא מראה שלמעשה הטכניקה היחידה שבעזרתה אנו יודעים להשיג הוגנות אינה ישימה עבור פונקציות אלו.

בנוסף לאמור לעיל, אנו מראים שניתן להשיג הוגנות מלאה גם במחלקות נוספות מעבר למחלקת הפונקציות הבוליאניות שבהן שני הצדדים מקבלים את אותו הפלט. אנו מראים שניתן להשיג הוגנות לפעמים גם עבור פונקציות בוליאניות שבהן שני הצדדים לא מקבלים בהכרח את אותו הפלט, וגם לפונקציות שבהן הפלט הוא לא בינארי. זוהי הפעם הראשונה שבה מראים שהוגנות יכולה להתקבל במחלקות אלו, ולומדים שניתן לקבל הוגנות במחלקות הרבה יותר רחבות וגדולות ממה שידענו קודם לכן.