אוניברסיטת בר אילן

פרוטוקול לחישוב בטוח בעל יעילות קונקרטית (מספר סיבובים קבוע)
עבור מודל מרובה שחקנים ויריב אקטיבי

אבישי ינאי

עבודה זו מוגשת כחלק מהדרישות לשם קבלת תואר מוסמך
במחלקה למדעי המחשב של אוניברסיטת בר אילן

רמת-גן תשע"ה

אוניברסיטת בר אילן

פרוטוקול לחישוב בטוח בעל יעילות קונקרטית (מספר סיבובים קבוע)
עבור מודל מרובה שחקנים ויריב אקטיבי

אבישי ינאי

עבודה זו מוגשת כחלק מהדרישות לשם קבלת תואר מוסמך
במחלקה למדעי המחשב של אוניברסיטת בר אילן

רמת-גן תשע"ה

עבודה זו נעשתה בהדרכתם של

פרופסור יהודה לינדל ופרופסור בני פנקס

מן המחלקה למדעי המחשב של אוניברסיטת בר אילן

תקציר העבודה

חישוב בטוח מרובה שחקנים מתמודד עם הבעיה של חישוב מבוזר, בו לשחקנים יש מידע אותו הם מעוניינים לשמור בסוד אך המידע עדיין דרוש לצורך החישוב, זאת אומרת, החישוב יפיק תוצאה נכונה באופן שהשחקנים לא ילמדו שום מידע מעבר למה שהיו לומדים אילו החישוב היה נעשה בעזרת שחקן-צד-שלישי הגון אשר מקבל את הקלטים של השחקנים, מבצע את החישוב ומחזיר את התוצאה לשחקנים (יכולה להיות תוצאה שונה לכל שחקן).

פרוטוקולים שפותרים את הבעיה הנ"ל מתמודדים עם סוגים שונים של יריבים כאשר עבודה זו מתמודדת עם יריב סטטי - הבוחר את השחקנים אותם הוא חפץ להשחית מבעוד מועד (לפני תחילת הריצה של הפרוטוקול, בניגוד ליריב אדפטיבי לו מותר להשחית שחקנים תוך כדי ובהתאם לריצה); היריבים הנלמדים ביותר, וכן היריבים איתם נתמודד בעבודה זו, הם יריבים פסיביים ואקטיביים. ליריב פסיבי ניתנת האפשרות לבחון את כל תעבורת ההודעות של השחקנים אותם השחית בעוד שיריב אקטיבי יכול בנוסף להחליף או לשבש הודעות.

הפתרון הראשון לבעיית החישוב הבטוח עבור שני שחקנים הוצגה ב 82' ע"י Yao וניתנה הוכחת בטיחות של הפרוטוקול כנגד יריב פסיבי (עבודה זו הורחבה על ידי LP ב 07' כך שהפרוטוקול יהיה עמיד גם בפני יריב אקטיבי ע"י שיטת ה cut-and-choose); את בעיית החישוב הבטוח עם שחקנים מרובים פתרו לראשונה GMW ב 87' גם כנגד יריב פסיבי

וגם כנגד אקטיבי. פתרון נוסף עבור הבעיה עם שחקנים מרובים הציגו BMR ב 90' ע"י הרחבת הפתרון של Yao לשחקנים מרובים (כאשר רוב השחקנים הם הגונים).

הפתרונות הנ"ל מאוד חשובים בכך שמראים שקיימים פתרונות לבעיה, עם זאת הפתרונות נחשבים מאוד לא יעילים, במיוחד כאשר מממשים אותם כנגד יריבים אקטיביים, ולכן רחוקים מאוד משימושים פרקטיים בחיינו.

משתני היעילות אותם אנו בוחנים כאשר מסתכלים על פרוטוקול לחישוב בטוח הם סיבוכיות חישובית (כמות העבודה הלוקאלית שכל שחקן מבצע), סיבוכיות סיבובי תקשורת (מספר הפעמים בהן שחקן נדרש לשלוח/לקבל הודעה) וסיבוכיות הודעות (כמות המידע הנדרש להעביר בין השחקנים על מנת לבצע את החישוב). בפרוטוקולים הנ"ל, המשתתפים ממירים קודם את הפונקציה אותה רוצים לחשב למעגל אריתמטי או בוליאני ועליו מבצעים את כל החישובים, לכן ניתוח הסיבוכיות של הפרמטרים לעיל בדרך כלל יחסי לגודל המעגל (מספר שערים, מספר חוטי כניסה/יציאה וכו').

כפי שצוין לעיל, הפרוטוקול של BMR הוא גרסה מרובת משתתפים של הפרוטוקול של Yao בה מספר סיבובי התקשורת הוא קבוע (ואינו תלוי בגודל המעגל); בשלב ה offline של הפרוטוקול השחקנים בונים מעגל מוצפן ובשלב ה online השחקנים מחליפים ביניהם קלטים מוצפנים עבור חוטי הקלט של המעגל ולאחר מכן מחשבים את המעגל ללא צורך באינטראקציה נוספת. למרות תוצאה מאוד טובה של הפרוטוקול מבחינת סיבוכיות סיבובי התקשורת, קיימים שני חסרונות עיקריים בגרסה של הפרוטוקול כנגד יריב אקטיבי: (1) בטיחות נשמרת רק כאשר היריב משחית מיעוט של השחקנים, (2) הפרוטוקול משתמש

בפרוטוקול כללי נוסף לחישוב בטוח כדי לאמת שפעולה שבוצעה ע"י השחקנים אכן בוצעה בהגינות - מה שגורם לתקורה גבוהה מאוד בזמן הריצה.

הפתרונות הפרקטיים היחידים היום הם TinyOT ו SPDZ, מתבססים על הרעיון של GMW וגם הם עובדים בצורה של offline-online. שני הפתרונות הללו מתגברים על החסרונות המצויינים לעיל, זאת אומרת, הם גם עובדים תחת יריב אקטיבי שיכול להשחית כל מספר של שחקנים (ולא רק מיעוט) וכן משיגים סיבוכיות חישובית מאוד טובה. עם זאת, כיוון שהפתרונות הללו מתבססים על השיטה של GMW הם חובים בתוכם בעיה מהותית שקיימת גם שם. הבעיה היא שב GMW השחקנים חייבים לבצע אינטראקציה (סיבוב תקשורת) עבור כל שער כפל במעגל (אריתמטי) ולכן מספר הסיבובים תלוי במספר השערים. כאשר מספר השחקנים מאוד קטן או שכל השחקנים נמצאים ברשת LAN הפרוטוקולים יהיו מאוד מהירים אך כאשר השחקנים נמצאים באיזורים גיאוגרפים שונים (WAN) התקורה של פתיחה וסגירה של סיבובי תקשורת מהווים חסרון.

בעבודה זו אנחנו מספקים את הפרוטוקול הראשון שמשיג יעילות קונקרטית, ובפרט סיבוכיות סיבובים של O(1) כנגד יריב אקטיבי שמסוגל להשחית כל מספר של שחקנים. הרעיון הבסיסי הוא להשתמש בפרוטוקול חישוב בטוח אחר, שסיבוכיות סיבובי התקשורת שלו אינה קבועה, בכדי להצפין את המעגל בצורה דומה לזו של BMR, וכיוון

שכל שער במעגל מוצפן בנפרד אנחנו מצליחים להשיג סיבוכיות סיבובים שהיא כן קבועה. הבחנה מאוד משמעותית שעזרה לפרוטוקול שלנו להיות יותר יעיל היא שבשלב ה offline לא נדרש לאמת כלל שהשחקנים ביצעו את הצפנת השערים בצורה הגונה, הבדיקות הללו מתקבלות ללא עלות בשלב ה online. משמעות ההבחנה היא שגם אם חלק מהשחקנים "רימו" בזמן חישוב המעגל המוצפן, הרמאות הזו תגרום לשאר השחקנים (ההגונים) לעצור את החישוב - כך הם לא יוציאו כפלט ערך שגוי (זאת אומרת שנכונות הפרוטוקול נשמרת). (היריב אומנם יוכל ללמוד את הפלט הנכון של החישוב אך דבר זה הוא בלתי נמנע במודל של יריב אקטיבי שיכול להשחית כל מספר של שחקנים). בעבודה זו אנו מוכיחים שגם אם חלק מהשחקנים רימו בשלב החישוב, עדיין לא יצליחו ללמוד שום מידע על הקלטים שהשחקנים ההגונים הכניסו לפרוטוקול.