האוניברסיטה הפתוחה

המחלקה למתמטיקה ולמדעי המחשב

מערכות הצבעה אלקטרוניות בטוחות מבוססות קריפטוגרפיה

עבודה מסכמת זו הוגשה כחלק מדרישות לקבלת תואר
מוסמך למדעים M.sc. במדעי המחשב
באוניברסיטה הפתוחה

על ידי
תום ליבוביץ

העבודה הוכנה בהדרכתו של פרופ' תמיר טסה

מרץ 2023

1. תוכן עניינים

1. תוכן עניינים 2
2. תקציר 3
3. מבוא 5
   3.1 מבנה העבודה 6
4. רקע קריפטוגרפי 10
   4.1 סכמת התחייבות ביטים 10
   4.2 פרוטוקול RSA 12
   4.3 חתימה דיגיטלית 13
   4.4 סכמת חתימה עיוורת 13
   4.5 פרוטוקול דיפי-הלמן 16
   4.6 הצפנה מבוססת סיסמה 17
   4.7 שיתוף סודות 17
5. בחירות אנונימיות על גבי רשת לא מאובטחת 19
   5.1 תקציר 19
   5.2 מבוא 19
   5.3 סימונים 20
   5.4 מערכת דוא"ל 21
   5.5 אישור שליחה חתום 23
   5.6 שרשרת של מערבלים 23
   5.7 כתובות החזרה 24
   5.8 פסבדונים דיגיטליים 25
   5.9 מערכת בחירות אנונימית 25
   5.10 מערכת דוא״ל לשימוש כללי 27
   5.11 מערבל מסוג חדש 27
   5.12 סיכום 29
6. סכמת הצבעה פרקטית לבחירות בסדר גודל ארצי 30
   6.1 תקציר 30
   6.2 מבוא 30
   6.3 הגדרות לבטיחות מערכת בחירות 31
   6.4 סכמת ההצבעה 32
   6.5 מבנה הסכמה 32
   6.6 בטיחות הסכמה 35
   6.7 סיכום 38
7. סכמת הצבעה מבוססת חתימה עיוורת לשמירת סודיות המצביעים 39
   7.1 תקציר 39

7.2 מבוא 39
7.3 דרישות האבטחה 40
7.4 מנגנוני אבטחה 40
7.5 הצפנת המפתח ב-E-voting 41
7.6 ארכיטקטורת E-Voting 41
7.7 שלבי הבחירות 42
7.8 מימוש 44
7.9 סיכום 45
8. סכמת הצבעה בטוחה לחישוב תוצאות הבחירות עבור כללי הצבעה מבוססי ציון 48
8.1 מבוא 48
8.2 מאמרים קודמים בנושא 56
8.3 כללי הצבעה מבוססי ציון 57
8.4 פרוטוקול מאובטח לחוקי הצבעה מבוססי ציון 58
8.5 אבטחת הפרוטוקול 61
8.6 וידוא תקינות ההצבעות 62
8.7 הערכת עלויות 65
8.8 דיון 70
8.9 סיכום 72
9. סכמת הצבעה בטוחה לחישוב תוצאות הבחירות עבור כללי הצבעה מבוססי סדר 74
9.1 הפרוטוקול 74
9.2 וידוא חוקיות ההצבעות 77
9.3 חישוב מאובטח מרובה משתתפים של המועמדים המנצחים 81
9.4 פרטיות הפרוטוקול 83
9.5 הערכת עלויות 84
9.6 חוקים מבוססי סדר אחרים 88
10. מקורות 90

2.תקציר

מערכות בחירות קיימות כבר למעלה מ-3000 שנים, מאז ערש הדמוקרטיה ביוון העתיקה. מדינות דמוקרטיות משתמשות בבחירות על מנת לבחור נשיא או ראש ממשלה. ברוב המדינות כיום הבחירות מתבצעות באופן אנושי בלבד, כלומר ללא התערבות מחשבים בתהליך. קהל המצביעים צריך להגיע למקום מסוים בו מתבצעת ההצבעה. ההצבעה מתבצעת ע"י הכנסת פתק או מעטפה לקלפי והספירה מתבצעת באופן ידני. קיום מערכת בחירות ידנית בצורה זו מציבה אתגרים וחסרונות רבים. החל מעלות גבוהה, בעיות של הפרת חוקי הבחירות וניסיונות להטות את התוצאות, הצורך שכל תושבי המדינה יגיעו להצביע, זמן ספירת ההצבעות, הפגיעה באיכות הסביבה וכלה באופרציה מורכבת - שכירת עובדים ומקומות שיהוו קלפי, אבטחה, ועוד. כמו כן, בתקופת הקורונה הגעה פיזית לקלפיות יוצרת סכנת הידבקות.

באופן טבעי, עם התפתחות הטכנולוגיה והאינטרנט בשנים האחרונות, יש יותר ויותר הבנה בצורך בבחירות אלקטרוניות. כיום ב-37 מדינות שונות יש שימוש באמצעים אלקטרוניים שונים שמסייעים לקיום הבחירות. החל מהצבעה במכונה אוטומטית בקלפי, דרך ספירה ממוחשבת מרכזית וכלה בניסיונות לבצע הצבעה אינטרנטית לחלוטין. למרות שבחירות אלקטרוניות מייתרות את הקלפיות הפיזיים, פותרות הרבה מן האתגרים הלוגיסטיים ויכולות לחסוך עלויות, הן מציבות אתגרים נוספים ומשמעותיים לא פחות. בעבודה זו, נתמקד בהיבט מרכזי בבחירות דמוקרטיות - סודיות ובטיחות ההצבעה - איך לשמור על פרטיות המצביעים וההצבעה בכל שלבי התהליך - ברישום המצביעים, בהצבעה עצמה ובהעברתה אל מקור חיצוני. ואיך לשמור על תקינות ונכונות ספירת הקולות ולמנוע זיופים, הטיות ושינוי התוצאה הסופית.

3. מבוא

בחירות הן אבן יסוד של הדמוקרטיה, הן מאפשרות לאזרחים להביע את רצונם בדרך של הצבעה. האופן שבו מתקיימות בחירות כיום הוא מסורבל ודורש שכל אזרח יגיע פיזית לקלפי על מנת להצביע. עקב כך, אחוזי ההצבעה נמוכים במדינות דמוקרטיות רבות. להצבעה אלקטרונית יש יתרונות רבים על פני הצבעה פיזית. בחירות אלקטרוניות לא דורשות מהבוחר להגיע למיקום פיזי, וכל אחד יכול להצביע מביתו או משרדו. בחירות כאלו הרבה יותר מהירות ויעילות ולא דורשות מבצע לוגיסטי על מנת להקים קלפיות ברחבי הארץ ולשכור אלפי עובדים. עקב כך, עלות מערכת בחירות אלקטרוניות נמוכה מזו של מערכת בחירות פיזית. כמו כן, טביעת הרגל הפחמנית של מערכת בחירות פיזית היא גבוהה מאוד. היא דורשת הדפסת פתקים ומעטפות בסדר גודל של מספר הבוחרים. כלומר בבחירות ארציות בארץ מודפסים עשרות מיליוני פתקים ומיליוני מעטפות בכל מערכת בחירות. כמו כן, מאז הקורונה שפרצה ב-2020, הצורך בריחוק חברתי גדל ברחבי העולם והגעה של אלפי אנשים לקלפיות יוצרת סיכון הדבקה. שירותים ממשלתיים שבעבר פעלו רק באופן פיזי כבר עברו למערכות אלקטרוניות וגם במקרה של בחירות אין שום מגבלה טכנית שמונעת דיגיטציה של התהליך. עם זאת, עולה באופן טבעי החשש מהטיות ורמאויות. בעוד שבבחירות פיזיות קל לרמות בקנה מידה קטן, למשל שסופר קולות יכניס עוד 20 פתקים של מפלגתו, במערכת בחירות אלקטרונית האתגר הטכנולוגי גדול יותר, אבל ברגע שהתבצעה פריצה למערכת כזו ניתן לשנות את תוצאות הבחירות באופן ניכר. לכן עיקר הדיון במאמרים מסוג זה הוא בטיחות המערכת, דהיינו שלא ניתן להטות את תוצאות הבחירות, ובסודיות ההצבעה, כלומר שלא ניתן לקשר בין הצבעה לבין המצביע. אם מצביע לא יהיה בטוח שהקול שלו נשמר בסוד הוא עלול להצביע אחרת מאיך שהוא היה רוצה להצביע, או להימנע מהצבעה בכלל.

בעבודה זו נסקור חמישה מאמרים שונים בתחום מערכות בחירות אלקטרוניות בטוחות מבוססות קריפטוגרפיה. נציג מאמרים מתקופות שונות - החל מתחילת שנות ה-80 ועד לשנת 2022, ובהיבטים שונים - חלק מהמאמרים דנים באבטחת התקשורת על בסיס רשת לא מאובטחת, חלקם דנים בהיבטים פרקטיים של מימוש מערכת בחירות מאובטחת וחלקם דנים בחישוב מאובטח של תוצאות הבחירות ושמירה על סודיות מושלמת של המצביעים והבחירה שלהם. כמו כן, כלל המאמרים מתבססים על אלגוריתמים וטכניקות קריפטוגרפיות ידועות שאותן נסקור לפני הדיון במאמרים.

3.1 מבנה העבודה

בחלק הראשון של העבודה נדבר על המאמר

Untraceable electronic mail, return addresses and digital pseudonyms

של דייוויד צ'אום שפורסם ב-1981. בזמנו היה המאמר פורץ דרך בתחום אבטחת רשתות תקשורת. המאמר מציג טכניקה לפתרון בעיית ניתוח התקשורת. בעיה זו עוסקת בשמירת סודיות התקשורת ובפרט בהסתרת הצדדים המתקשרים וזמני שליחת ההודעות ביניהם. במאמר מוצגת מערכת דוא"ל שמאפשרת להסתיר את הנמען ואת תוכן הדוא״ל גם כאשר הדוא״ל עצמו אינו מוצפן. המערכת מבוססת על קריפטוגרפיית מפתח ציבורי ולא דורשת יישות מרכזית. כלומר המערכת מבוזרת ומשתמשת "במערבלים" שמקבלים את נמען ההודעה כחלק מההודעה המוצפנת ומעבירים את ההודעה אליו.

למרות שעיקר המאמר לא מדבר על מערכות בחירות אלקטרוניות, הוא מציע דרך לקיים בחירות אנונימיות. המאמר מתאר רשות מרכזית אשר מחזיקה רשימה של מפתחות ציבוריים שמאפשרת וידוא שהודעה נתונה נשלחה ע"י מחזיק המפתח הפרטי. כאשר רוצים לקיים בחירות רושמים מראש את כל המצביעים כך שלכל אחד יש מפתח ציבורי שמור במערכת. עובדה זו מאפשרת לרשות המרכזית לוודא שאין הצבעות כפולות או מזויפות.

בהמשך המאמר מתוארת "שרשרת של מערבלים". כל הודעה מוצפנת בשכבות לפי המפתחות הציבוריים של המערבלים, וכל אחד מהמערבלים פותח שכבה אחת בהצפנה ומעביר את ההודעה למערבל הבא עד שההודעה מגיעה ליעד. למרות שאין לכך עדויות, ניתן לנחש שמאמר זה היווה את הבסיס הרעיוני לדפדפן TOR שפועל בצורה זהה ופותח בצבא ארה"ב מספר שנים לאחר פרסום המאמר. יותר מ-40 שנים לאחר פרסום המאמר, טכניקה זו של שרשרת מערבלים עדיין נמצאת בשימוש של ארגוני ביון וחברות סייבר התקפי על מנת להסוות את מסלול התקשורת ולהסתיר את יעדן הסופי של פקטות תקשורת.

במאמר השני,

A practical secret voting scheme for large scale elections

מוצעת מערכת פרקטית להצבעה אנונימית לבחירות עם מספר מצביעים גדול. מאמר זה מתבסס על המאמר הראשון בהיבט של בטיחות התקשורת. כלומר הוא מניח שיש ערוץ אנונימי בו אפשר להעביר הודעות לשאר בעלי התפקידים בבחירות כפי שתואר במאמר הראשון. לכן מאמר זה מתמקד בהיבטים קריפטוגרפיים שיאפשרו למצביעים לשלוח את הצבעתם באופן אנונימי מצד אחד, אבל מצד שני אם המצביעים לא מוצאים את הצבעתם בלוח ההצבעות הציבורי, יש להם דרך לדווח על שיבוש הבחירות מבלי לחשוף את הצבעתם.

בניגוד למאמר הראשון, הממוקד בבטיחות התקשורת ובו יש רשות אחת מרכזית שמקבלת את כל הקולות ומפרסמת את התוצאה הסופית, מאמר זה משדרג את הסודיות וההוגנות של מערכת הבחירות ע"י שימוש במנהל בחירות, סופר קולות ולוח הצבעות פומבי. כלומר המערכת לא מניחה שיש יישות אחת הגונה שניתן לסמוך עליה, ושומרת על הוגנות הבחירות וסודיות המצביעים אפילו במקרה ומנהל הבחירות וסופר ההצבעות קושרים קשר ומנסים לחשוף את זהות המצביעים.
המאמר משתמש בטכניקות קריפטוגרפיות על מנת לשמר סודיות זו. בניגוד למאמר הקודם, המצביעים אינם שולחים את ההצבעה שלהם מוצפנת בלבד, אלא שולחים אותה מוסתרת באמצעות חתימה עיוורת. ההצבעות המוסתרות מתפרסמות בלוח הצבעות פומבי שמאפשר למצביעים למצוא את ההצבעה ולוודא שהיא אכן נספרה מבלי להפר את סודיות המצביעים. מצד שני, משתמשים בסכמת התחייבות ביטים על מנת לוודא שלאחר שליחת ההודעה המוסתרת, המצביע אינו יכול לשנות את בחירתו ולטעון שהקולות לא נספרו כתקנם. כמו כן, נשמרת הוגנות מערכת הבחירות משום שלא ניתן לדעת שום תוצאה חלקית של ספירת הקולות וכל ההצבעות המוסתרות נחשפות רק לאחר שכל ההצבעות נשלחו ופורסמו בלוח הבחירות. כך ניתן למנוע הסקת מסקנות ממידע חלקי שתשפיע על המשך הבחירות.

המאמר השלישי

Secure E-Voting With Blind Signature

דומה למאמר השני בגישה שלו לאופן ההצבעה ולביזור תחומי האחריות ליישויות שונות. גם מאמר זה משתמש בחתימה עיוורת על מנת לשמור על סודיות ההצבעות מחד ומאפשר למצביעים לטעון שהצבעתם לא נספרה מאידך. מאמר זה לוקח את הפרדת הרשויות צעד אחד קדימה ויוצר שתי יישויות חדשות בנוסף למנהל הבחירות - רשם שאחראי על רישום המצביעים ואימות זהותם לפני הבחירות, ומוודא שאחראי על וידוא המצביעים בזמן הבחירות ופרסום רשימת המצביעים הרשומים.
הדגש במאמר זה הוא על מימוש פרקטי של מערכת בחירות במספר היבטים שונים. ראשית, המערכת לא רק מתוארת בצורה תיאורטית, אלא גם ממומשת בשפת ג'אווה. נעשה שימוש בשקעים (sockets) בשביל לתקשר בין המשתתפים במערכת הבחירות ומשתמשים בספריית BouncyCastle על מנת לממש אלגוריתמי הצפנה ושקעים מאובטחים (secure sockets). המערכת למעשה מורכבת מ-7 תוכנות שונות שממממשות את כל תפקידי המשתתפים השונים בבחירות. ההיבט הפרקטי הנוסף הוא שמירת מפתח פרטי (ארוך) באופן בטוח ושחזור שלו באופן ידידותי למשתמש. המאמר מציג שיטה לשמירת מפתח RSA על כרטיס זיכרון ושחזורו ע"י הצפנה מבוססת סיסמה. עם זאת, יש מספר בעיות במאמר הקשורות לקריפטוגרפיה, סודיות המצביעים ושימושיות עליהן נפרט בסיכום המאמר.

בחלק האחרון של העבודה נסקור את המאמרים

Fear ar not, Vote Truthfully: Secure MultipartyComputation of Score Based Rules

שמציג מערכת הצבעה המנוהלות על ידי חוקי הצבעה מבוססי ציון, ואת המאמר

Towards Secure Virtual Elections Multiparty Computation of Order Based Voting Rules

שמציג מערכת הצבעה מבוססת חוקי סדר.

שני המאמרים שונים בתכלית משאר המאמרים בעבודה זו משום שהם אינם מתעסקים כלל באבטחת התקשורת בין המצביעים לסופרי הקולות אלא בחישוב מאובטח וסודי של תוצאות הבחירות מתוך כלל ההצבעות, כפי שנגזר מכלל ההצבעה. בשני המאמרים מוצגים פרוטוקולים שמסתמכים על קבוצה של סופרי קולות שמבצעים את החישוב של תוצאות הבחירות מבלי להחשף לקולות עצמם או לשום תוצאת ביניים במהלך החישוב, מלבד הפלט הסופי שהוא המועמדים הזוכים (או המועמדים הזוכים וציונם, או דירוג המועמדים הזוכים, על פי המקרה ודרישות המערכת). ברוב המאמרים בנושא מערכת הצבעה אלקטרונית כאשר דנים בסודיות ההצבעה, הכוונה היא שלמרות שהקולות גלויים לא ניתן לשייך הצבעות למצביעים שלהן. בשני המאמרים האחרונים מספקים תכונה חזקה יותר - סודיות מושלמת, כלומר בהינתן כל קואליציית מצביעים, הפרוטוקול לא חושף שום מידע על הקולות מעבר למה שניתן להסיק מהתוצאות. הפרוטוקולים מספקים תכונה זו תחת ההנחה שיש רוב הגון של סופרי קולות.

שני המאמרים מתבססים על חישוב מרובה משתתפים שמבצעים סופרי הקולות כמו גם על הטכניקה הקריפטוגרפית של שיתוף סודות.

המאמר הראשון מתמקד בחוקי הצבעה מבוססי ציון. מדובר במשפחה של חוקי הצבעה שבהם כל מצביע נותן לכל אחד מהמועמדים ציון, על סמך חוקיות מסוימת המוגדרת בחוק ההצבעה (למשל, כל מועמד מקבל ציון בין 0 ל-10, או שכל המועמדים מקבלים ציון 0 למעט מועמד אחד בלבד שמקבל את הציון 1).. המנצח הוא המועמד שסכום הציונים שקיבל מכל המצביעים הוא הגבוה ביותר.

המאמר השני מתמקד בבחירות מבוססות סדר. במשפחת חוקים זו כל מצביע שולח מטריצת הצבעה שמכילה השוואה בין כל זוג מועמדים. כלומר בכל תא במטריצה בשורה א ובעמודה ב מצוין האם המצביע מעדיף את מועמד א' על פני מועמד ב' או להפך. סופרי הקולות מחברים את המטריצות המתקבלות מכלל המצביעים וזהות המנצח נקבעת מתוך מטריצת הסכום הזו, כאשר כל חוק הצבעה במשפחה זו מגדיר דרך חישוב אחרת.

4. רקע קריפטוגרפי

4.1 סכמת התחייבות ביטים

התחייבות ביטים מדמה קופסה נעולה בעולם הפיזי. כמו קופסה נעולה, התחייבות ביטים משמשת להעברת מידע ברגע נתון באופן חסוי, את היכולת לחשוף אותו בשלב מאוחר יותר (לפתוח את הקופסה) ולהבטיח שהמידע לא השתנה מרגע השליחה ועד רגע החשיפה. בעולם הקריפטוגרפי אליס רוצה להעביר לבוב מידע (ביט אחד או יותר) ולחשוף את המידע שנשלח רק בשלב מאוחר יותר, אחרי שבוב חושף מידע נוסף. נשתמש בדוגמה של בלום [Blu83] על מנת להסביר את הצורך בהתחייבות ביטים. נניח שאליס ובוב התגרשו, הם גרים בערים שונות והם רוצים להחליט מי יקבל את הרכב ע"י הטלת מטבע דרך הטלפון (תוצאת הטלת המטבע שקולה לביט אחד). אם אליס תבחר "עץ" כניחוש שלה לתוצאות הטלת המטבע שבוב מבצע, בוב יכול להגיד לאליס שיצא "פלי" ולקחת את הרכב לעצמו. לכן נדרשת סכמה בה אליס תתחייב על "עץ" או "פלי" ותעביר לבוב את בחירתה באופן כזה שהוא לא יוכל לדעת מה בחרה. אבל לאחר שהוא יחשוף את תוצאת הטלת המטבע אליס תוכל לחשוף את בחירתה באופן כזה שבוב יהיה משוכנע שזו הייתה בחירתה המקורית ולא ייתכן שאליס שינתה את בחירתה לאחר שחשף את תוצאת הטלת המטבע.

באופן פורמלי יותר נגדיר סכמת התחייבות ביטים כשתי פונקציות:

1. פונקציית התחייבות - תקבל כקלט את ההודעה *msg* ומחרוזת אקראית סודית *r* ותניב מחרוזת com שאותה אליס תשלח לבוב. נסמן את פונקציית ההתחייבות כך $commit(msg,r) \rightarrow com$
2. פונקציית וידוא תקבל את ההודעה *msg*, את המחרוזת האקראית *r* ואת מחרוזת ההתחייבות *com*, ותוודא שאכן הקלט *msg* הוא התוצאה של פתיחת מחרוזת ההתחייבות *com* ביחס למחרוזת האקראית *r*. נסמן את פונקציית הוידוא כך $verify(msg,com,r) \rightarrow accept \vee reject$

כלומר, אליס תפעיל את הפונקציה commit על ההודעה שהיא רוצה לשלוח לבוב msg ועל מחרוזת אקראית r כלשהי שהיא תגריל. הפונקציה תניב את הפלט com, שאותו אליס תשלח לבוב. כאשר אליס תחליט לחשוף את הודעתה, היא תשלח לבוב את ההודעה המקורית msg ואת r והוא יוודא, באמצעות פונקציית verify , שאכן המחרוזת com נוצרה ע"י הפעלת הפונקציה commit על msg ו-r.

אם נחזור לדוגמת הטלת המטבע, אליס תבחר "עץ" לדוגמה ותכניס אותו לקופסה מטאפורית ע"י שימוש בפונקציה commit על "עץ" ועל מספר אקראי r. בוב יקבל את ההודעה com, יטיל את המטבע ויגיד לאליס מה יצא. רק בשלב זה אליס תחשוף את בחירתה המקורית ע"י שליחת r ו-msg. כך לא ייתכן

שבוב ירמה ויגיד לאליס מה יצא לפי בחירתה ובוב יכול להיות בטוח שבחירתה הייתה הגונה משום שהיא נעשתה לפני הטלת המטבע.

עם זאת, בני הזוג יכולים לרמות אחד את השני בשני המקרים הבאים:

1. אם לפונקציה commit שאליס השתמשה ניתן למצוא זוגות $(m_1, r_1), (m_2, r_2)$ שמקיימים $verify(m_1, com, r_1) = verify(m_2, com, r_2) = accept$.
במקרה זה לאחר שאליס תדע את הטלת המטבע היא תוכל לספק m_2, r_2 אשר שונים מההודעה והמחרוזת האקראית m_1, r_1 אשר בעזרתן היא יצרה את com. כלומר אליס תוכל להחליט מה היא בחרה בהתאם להטלת המטבע ותמיד לזכות ברכב.
2. אם בוב יכול להסיק משהו על msg בהינתן com בלבד. כלומר, אם בוב יודע למשל שבהינתן ההודעה שקיבל, אליס בחרה "עץ" בהסתברות של 80% הוא תמיד יגיד לאליס שיצא "פלי" וימקסם את סיכויו לזכות.

לכן בשביל למנוע רמאויות כאלו, סכמת התחייבות הביטים צריכה לקיים שתי תכונות:

1. לא ניתן לייצר $com, (m_1, r_1), (m_2, r_2)$, $m_1 \neq m_2$ כך שמתקיים: $verify(m_1, com, r_1) = verify(m_2, com, r_2) = accept$
2. המחרוזת com לא חושפת שום דבר על msg. במילים אחרות אם r נבחר בהתפלגות אחידה אז com בלתי תלוי סטטיסטית ב msg.

לצורך מימוש פשוט ניתן להיעזר בפונקציות גיבוב קריפטוגרפיות כדוגמת 256sha. מימוש הפונקציות הוא פשוט ואמין במקרה זה משום ש-256sha נמצאות בשימוש רחב מאוד כיום וניתן למצוא קוד שמממש את הפונקציה בכל שפת תכנות נפוצה. כמו כן, למרות שהפונקציה התפרסמה ב2001 עוד לא נמצא זוג קלטים שיניב את אותו הגיבוב. ניתן להשתמש בכל פונקציה גיבוב קריפטוגרפית אחרת ואין זה משנה את פרטי המימוש. נסמן את פונקציית הגיבוב ב H. פונקציות ההתחייבות והוידוא ימומשו באופן הבא:

$$commit(msg, r): H(msg, r)$$

$verify(msg, com, r)$: accept if and only if $com = H(m, r)$

ניתן להוכיח בקלות שהפונקציות הנ"ל מקיימות את התכונות הנדרשות לסכמת התחייבות ביטים:

1. התכונה הראשונה מתקיימת משום שלפונקציות גיבוב קריפטוגרפיות יש הסתברות אפסית להתנגשויות. כלומר לא ניתן למצוא זוג m_1, m_2 שמקיים $H(m_1) = H(m_2)$.

2. התכונה השנייה מתקיימת משום שבהינתן הגיבוב לא ניתן להסיק משהו על הקלט שיצר אותו. גם זו תכונה של פונקציות קריפטוגרפיות. עם זאת ניתן לבצע brute force ולנסות את כל הקלטים האפשריים. במקרה זה ניתן לדרוש ש r יהיה גדול מספיק, למשל 128 ביטים.

השימוש בפונקציות גיבוב הוא נפוץ ופשוט ולכן בחרתי להדגים את הסכמה בעזרתן. עם זאת, ישנם מימושים נוספים לסכמת התחייבות הביטים כפי שמתוארים ב [.[Blu83,Nao89]

4.2 פרוטוקול **RSA**

RSA היא מערכת הצפנת מפתח ציבורי. היא מערכת הצפנת מפתח ציבורי הראשונה שהומצאה ועדיין נמצאת בשימוש נרחב. ב–RSA כמו בכל מערכת הצפנת מפתח ציבורי, יש זוג מפתחות, אחד ציבורי שאיתו מצפינים ואחד פרטי שאיתו מפענחים, כאשר מתקיים שלא ניתן להסיק בקלות את המפתח הפרטי בהינתן המפתח הציבורי. על מנת ליצור זוג מפתחות יש לבצע את השלבים הבאים:

1. נבחר שני מספרים ראשוניים, גדולים, אקראים ושווי גודל (מבחינת מספר הביטים ביצוג הבינארי שלהם) p ו- q.
2. $n := pq$
3. $\Phi(n) := (p-1)(q-1)$
4. נבחר מספר שלם אקראי נוסף e, כך ש $1 < e < \Phi(n)$
5. נבחר מספר d כך ש-d הוא ההופכי של e מודולו $\Phi(n)$
6. המפתח הציבורי הוא (n, e)
7. המפתח הפרטי הוא (n, d)

לאחר יצירת המפתחות ניתן להצפין הודעה כלשהי m ולקבל הודעה מוצפנת c באופן הבא:

$$c := m^e mod n$$

פענוח ההודעה המוצפנת מתבצע באופן הבא:

$$c^d mod n = m^{de} mod n = m$$

4.3 חתימה דיגיטלית

חתימה דיגיטלית היא סכמה שמאפשרת לוודא אותנטיות של הודעה ושל השולח שלה. חתימה תקינה נותנת ביטחון גבוה מאוד למקבל ההודעה שאכן ההודעה נשלחה ע"י גורם מזוהה ושתוכן ההודעה לא השתנה בדרך משולח ההודעה אל הנמען.

בהצפנת RSA אנחנו מצפינים עם e שהוא חלק מהמפתח הציבורי ומפענחים את ההודעה עם d שהוא חלק מהמפתח הפרטי. עובדה זו מאפשרת לכל אחד להשתמש ב e להצפין הודעות שמיועדות אל הנמען ולהיות בטוח שרק הנמען יכול לפענח אותן. בחתימות דיגיטליות אנחנו רוצים להשיג בדיוק את ההפך. אנחנו רוצים שרק מחזיק המפתח הפרטי יוכל לחתום על תוכן ההודעה ומצד שני שכל אחד יוכל לוודא את החתימה ולאמת שההודעה אכן נשלחה ע"י מחזיק המפתח הפרטי. לכן חתימה דיגיטלית בסכמת RSA תראה כדלקמן. אם m היא ההודעה אז החתימה עליה DS תחושב כך -

$$DS := m^d mod n$$

ניתן לוודא את אותנטיות ההודעה באופן הבא:

$$m = DS^e mod n \rightarrow accept$$

4.4 סכמת חתימה עיוורת

חתימה עיוורת היא סוג של חתימה דיגיטלית כאשר ההודעה מוסתרת לפני שהיא נחתמת. הצדדים המשתתפים בסכמה זו הם יוצר ההודעה שמבקש את החתימה, היישות החותמת ומקבל ההודעה שמוודא את החתימה. בניגוד לחתימה דיגיטלית, היישות החותמת לא נחשפת להודעה המקורית אלא חותמת "באופן עיוור" על הודעה מוסתרת. עם זאת, ניתן לוודא שההודעה המקורית אכן נחתמה ע"י היישות החותמת.

המטרה בסכמה זו היא לאפשר ליוצר ההודעה להסתיר הודעה ולקבל חתימה על ההודעה המוסתרת מבלי לחשוף את תוכנה ליישות החותמת. כמו כן, הסכמה מאפשרת למקבל ההודעה לוודא את החתימה ולאפשר לו לקרוא את ההודעה המקורית אחרי ששולח ההודעה חשף אותה.

באופן כללי סכמת חתימה עיוורת מורכבת מארבע פעולות ושני צפנים.

הצפנים:

- זוג מפתחות בסכמת הצפנה אסימטרית. היישות החותמת תחזיק במפתח הפרטי ותחתום בעזרתו. המפתח הציבורי יהיה ידוע לכל ויאפשר לוודא את החתימה ע"י יוצר ההודעה ומקבל ההודעה.
- מספר רנדומלי r ו-r^{-1} המספר ההופכי לו מודולו n. יוצר ההודעה יסתיר את ההודעה בעזרת r ויחשוף את ההודעה המקורית מתוך ההודעה המוסתרת בעזרת r^{-1}.

הפעולות:

- הסתרה - ראשית יש לבצע "הסתרה" של ההודעה המקורית. תהליך זה מתבצע בעזרת r שנקרא "גורם ההסתרה". נוצרת "הודעה מוסתרת" חדשה ע"י שילוב עם גורם ההסתרה כך שלא ניתן להסיק את ההודעה המקורית ממנה.
- חתימה - ההודעה המוסתרת נשלחת אל היישות החותמת, שלא יכולה לקרוא את ההודעה המקורית וחותמת עליה בטכניקת חתימה דיגיטלית סטנדרטית כלשהי.
- וידוא - מקבל ההודעה מוודא שההודעה אכן נחתמה ע"י היישות החותמת.
- חשיפה - יוצר ההודעה שולח את r' ומקבל ההודעה חושף את ההודעה המקורית בעזרתו.

ניתן לממש את סכמת החתימה העיוורת בעזרת מספר סכמות חתימה עם מפתח ציבורי. אנחנו נדגים את הסכמה בעזרת RSA:

- הסתרה: הסתרת ההודעה m מתבצעת ע"י בחירת מספר אקראי r זר ל n בין 0 ל n העלאתו בחזקת e (שני הפרמטרים הם חלק מהמפתח הציבורי של היישות החותמת) וכפילתו בהודעה המקורית כך: $m' = mr^e(modn)$. זוהי ההודעה המוסתרת. הכפל במספר האקראי, שיכול להיות כל ערך שהוא, לא מאפשר להסיק כלום על ההודעה המקורית m מתוך m'.
- חתימה - היישות החותמת יוצרת את החתימה באופן הבא: $s' = m'^d(modn)$.
- שליחה – הישות החותמת שולחת את חתימתה s' ליוצר ההודעה.
- וידוא - מקבל ההודעה מוודא את החתימה $s'^e = m'^{de} = m'\ (mod\ n)$. במידה והווידוא הצליח אז הוא מקבל את ההודעה המוסתרת m'.
- חשיפה - יוצר ההודעה המקורית יכול לחשוף את ההסתרה על החתימה, בעזרת r^{-1} ולקבל את s, חתימה דיגיטלית סטנדרטית על m:

$$s = s'r^{-1}(modn) = m'^d r^{-1} = m^d r^{ed} r^{-1} = m^d(modn)$$

זוהי חתימת RSA סטנדרטית שניתן לוודא בעזרת המפתח הציבורי (n,e)

כעת נעבור לתאר את סכמת ההצבעה. לשם כך נציג את הסימונים הבאים:

- מצביע i יסומן V_i.
- ההצבעה של מצביע i תסומן v_i.
- מספר הזיהוי של מצביע i יסומן ID_i.
- מנהל הבחירות יסומן A.
- סופר הקולות יסומן C.
- המפתח הפרטי של המצביע V_i. יסומן (n_i, d_i)
- המפתח הציבורי של המצביע V_i. יסומן (n_i, e_i)
- המפתח הציבורי של מנהל הבחירות A יסומן (n_A, e_A)
- סכמת התחייבות הביטים להודעה v עם מפתח k תסומן $\xi(v,k)$.
- סכמת החתימה הדיגיטלית על הודעה m של מצביע i תסומן $\sigma_i(m)$.
- סכמת החתימה העיוורת על הודעה m של המנהל A תסומן $\sigma_A(m)$.
- טכניקת ההסתרה של החתימה העיוורת להודעה m ומספר אקראי r תסומן $\chi_A(m,r)$.

טכניקת החשיפה של החתימה העיוורת לחתימה s ומספר אקראי r תסומן $\delta_A(s,r)$.

4.5 פרוטוקול דיפי-הלמן

פרוטוקול דיפי-הלמן (Diffie-Hellman) הוא פרוטוקול החלפת המפתחות הראשון שהומצא. הפרוטוקול יוצר מפתח משותף על גבי רשת לא מאובטחת, לשני משתתפים שלא החליפו ביניהם סוד משותף קודם לכן. על מנת ליצור מפתח משותף, שני המשתתפים, אליס ובוב, צריכים לבצע את הפעולות הבאות:

1. אליס ובוב מסכימים על מספר ראשוני גדול p.
2. אליס מגרילה ל-p שורש פרימיטיבי מודולו p שנסמן ב-g.
3. אליס בוחרת מספר שלם אקראי וסודי $a \in [1, p-1]$.
4. המפתח הציבורי של אליס הוא $A = g^a \ (mod \ p)$
5. אליס שולחת לבוב את g, A
6. בוב בוחר מספר שלם אקראי וסודי $b \in [1, p-1]$
7. המפתח הציבורי של בוב הוא $B = g^b \ (mod \ p)$
8. בוב שולח לאליס את B.
9. אליס מחשבת את $B^a (mod \ p)$
10. בוב מחשב את $A^b (mod \ p)$
11. המפתח המשותף הוא $K = A^b = g^{ab} = g^{ba} = B^a \ (mod \ p)$

יש לציין שהמספרים a, b נשמרו סודיים ולא נשלחו באף שלב בפרוטוקול. סודיות הפרוטוקול נובעת מהעובדה שלא ניתן לחשב ביעילות את g^{ab} בעזרת הערכים g^a, g^b. בעיה חישובית זו נקראת בעיית הלוגריתם הדיסקרטי, והיא מקובלת כבעיה חישובית קשה.

4.6 הצפנה מבוססת סיסמה

בתוכנות רבות, מבוססת פרטיות המשתמש על סיסמה או קוד סודי כלשהו. משום שסיסמה מכילה בדרך כלל מספר קטן של תווים, היא אינה מתאימה לשימוש בתור מפתח הצפנה. עם זאת, ניתן לעבד את הסיסמה וליצור ממנה מפתח באורך מתאים. יש שיטות רבות לגזור מפתח מסיסמה, אך באופן כללי ניתן להפעיל על הסיסמה פונקציה כלשהי עם אורך פלט קבוע, ולהוסיף מלח (salt) - ערך קבוע שמאריך את המפתח ומונע "מתקפות מילון" (dictionary attack) בהן התוקף מנסה כל סיסמה אפשרית עד אורך מסוים.

גישה נוספת להצפנה מבוססת סיסמה היא לבנות מפתח באמצעות טכניקות לגזירת מפתח (key derivation techniques) שהן יחסית יקרות, ובכך מעלות את הזמן והמשאבים שתוקף צריך להשקיע בשביל לבצע מתקפות מילון. פונקציית 2PBKDF לדוגמא, מקבלת פונקציה פסאודו-אקראית PRF, סיסמה P, מלח S ומספר איטרציות C ומריצה C איטרציות של PRF על הסיסמה P והמלח S. באמצעות הפרמטר C ניתן להגביר את קושי יצירת המפתח בהתאם לצורכי האבטחה.

4.7 שיתוף סודות

שיטות לשיתוף סודות מאפשרות לפרק סוד נתון למספר חלקים ולהפיצם לקבוצה של משתתפים. כל משתתף מקבל חלק רנדומלי הקשור לסוד כך שמתקיים:

1. לא ניתן להרכיב את הסוד אלא ע"י תת-קבוצה מאושרת כלשהי של משתתפים.
2. קומבינציה של חלקים מתת-קבוצה של משתתפים שאינה מאושרת לא חושפת שום מידע על הסוד.

הרעיון של שיתוף סודות הוצג באופן בלתי תלוי ע"י שמיר [Sha79] ובלייקלי [Bla79]. בשני המאמרים מניחים שיש D משתתפים וכל תת-קבוצה מגודל D' או יותר $(D' \leq D)$ יכולה להרכיב את הסוד. סכמות אלו נקראות $D' \; out \; of \; D$.

הסכמה של שמיר עובדת באופן הבא. נניח ש-p הוא מספר ראשוני גדול מספיק כך שכל סוד אפשרי ניתן לייצג בתור איבר בשדה הסופי Z_p. יהי x הסוד שנרצה לשתף. הסכמה של שמיר מכילה שתי פרוצדורות - שיתוף ובנייה מחדש.

פרוצדורת השיתוף $Share_{D',D}(x)$ דוגמת פולינום רנדומלי g מעל Z_p מדרגה $D' - 1$ כאשר המקדם החופשי של הפולינום הוא הסוד x אותו רוצים לשתף. כלומר

$g(t) = x + \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_{D'-1} t^{D'-1}$ כאשר המקדמים a_j נבחרים באקראי ובאופן בלתי תלוי בהתפלגות אחידה מתוך Z_p. הפלט של הפרוצדורה הם D ערכים $x_1, \ldots, x_D$ כאשר $x_d = g(d)$ הוא החלק שניתן למשתתף d, כאשר $1 \leq d \leq D$.

פרוצדורת הבנייה מחדש $Reconstruct_{D'}(x_1, \ldots, x_D)$ מקבלת כל תת-קבוצה של D' חלקים מתוך $\{x_1, \ldots, x_D\}$ ובונה מתוכם פולינום g מדרגה $D' - 1$ לכל היותר על ידי אינטרפולציה. הפלט של הפרוצדורה הוא $x = g(0)$.

מצד אחד, משום שאין כל אפשרות ללמוד דבר על ערכו בנקודה 0 של פולינום מדרגה $D' - 1$ מתוך ערכיו בפחות מ-D' נקודות, אי אפשר ללמוד שום דבר על הסוד מתת-קבוצה שיש בה פחות מ-D' חלקים. מצד שני, לכל תת-קבוצה של D' נקודות או יותר קיים פולינום אחד ויחיד מדרגה $D - 1$ או פחות שעובר דרך D' נקודות ולכן פרוצדורת הבניה מחדש יכולה לייצר פולינום ולמצוא את הנקודה $g(0)$ שהיא הסוד המקורי.

הפרוצדורות הנ"ל הן ליניאריות במובן הבא: יהיו x, y שני סודות מעל השדה Z_p ויהיו a, b שני ערכים ציבוריים מעל אותו שדה. בהנחה ש $x_1, \ldots, x_D$ ו- $y_1, \ldots, y_D$ הם חלקים בסכמת שיתוף הסודות של שמיר אז $ax_1 + by_1, \ldots, ax_D + by_D$ הם חלקים בסכמת שיתוף הסודות של שמיר כאשר הסוד הוא $ax + by$. כמו כן, אם g_x ו-g_y הם פולינומים שנוצרו ע"י פרוצדורת השיתוף לסודות x ו-y בהתאמה אז הפולינום $f := ag_x + bg_y$ הוא פולינום מדרגה $D' - 1$ שמקיים $f(0) = ax + by$.

כמו כן נשים לב שגם $a + x_d$ הוא חלק סוד בערך $a + x$.

5. בחירות אנונימיות על גבי רשת לא מאובטחת

5.1 תקציר

במאמר זה מוצגת טכניקה המבוססת על קריפטוגרפיית מפתח ציבורי[DH76] שמאפשרת למערכות דוא״ל להסתיר את הנמען ואת תוכן הדוא״ל גם כאשר מערכת הדוא״ל מבוססת על תקשורת לא מאובטחת. במערכת זו, אין צורך ביישות מתווכת מרכזית. כלומר המערכת מבוזרת וכל משתתף יכול להעביר הודעות ממנו אל נמען כלשהו על פי בחירתו. המשתתף יכול להישאר אנונימי ועדיין לאפשר לנמען לשלוח לו דוא״ל בחזרה. בנוסף, כל משתמש יכול לוודא שההודעה שלו נשלחה כמו שהיא, ללא שינויים או מחיקות.
טכניקה זו מאפשרת ליצור רשימה של פסבדונים - רשימה של יישויות שניתן לוודא שהודעה כלשהי נוצרה על ידם. כל משתמש במערכת הפסבדונים חותם דיגיטלית על התוכן שנשלח, ומערכת הערבוב יכולה לפתוח את ההודעה רק עם המפתח הציבורי שנשלח אליה מראש.
שימוש נוסף של טכניקה זו הוא בחירות אנונימיות אשר ממומשות ע״י שימוש בפסבדונים, כך שלכל מצביע יש פסבדונים במערכת, ואפשר בעזרתו לוודא שכל המצביעים אושרו קודם לכן ע״י המערכת.

5.2 מבוא

״בעיית ניתוח התקשורת״ (the traffic analysis problem) עוסקת בשמירת סודיות התקשורת ובפרט בהסתרת הצדדים המתקשרים וזמני שליחת ההודעות בין הצדדים. בעקבות התקדמויות שנעשו בתחום הקריפטוגרפיה בכלל ובתחום ״בעיית החלפת המפתחות״[DH76] בפרט, בעיית ניתוח התקשורת מקבלת חשיבות גדולה יותר ככל שנפח התקשורת ברשת עולה והשימוש בדוא״ל הופך לנפוץ יותר ויותר. מאמר זה מציג פתרון לבעיה זו אשר מבוסס על קריפטוגרפיית מפתחות ציבוריים ועל ההנחה שכל משתתף חייב לבטוח לפחות ביישות נוספת אחת שהיא לא הנמען. המערכת המוצגת לא שומרת על סודיות ההודעות במקרה של קשירת קשר בין כל היישויות שדרכן נשלחת הודעה.

5.3 סימונים

במערכת הצפנה אסימטרית (כמו RSA למשל [RSA78]) נשתמש בסימונים הבאים:

- K - מפתח ציבורי שניתן לשתף אותו עם משתמשים אחרים על מנת שהם יוכלו להצפין איתו תוכן המיועד למחזיק המפתח הפרטי.
- K^{-1} - מפתח פרטי - משמש לפענוח של הודעה שהוצפנה עם מפתח K. נשמר סודי ולא משותף עם אף יישות.
- $K(X)$ - הצפנה של X עם מפתח K.
- $K^{-1}(Y)$ - פענוח של Y עם המפתח K^{-1}.
- $K(K^{-1}(X)) = K^{-1}(K(X)) = X$ - כלומר אפשר להצפין עם המפתח הפרטי ולפענח עם הציבורי או להפך והתוצאה תהיה זהה בשני המקרים.

בשיטות הצפנה דטרמיניסטיות, כגון RSA, מתקיים שאם X=Y אז $K(X) = K(Y)$. תכונה זו מהווה בעיה משום שבמצב שבו נשלחת אותה הודעה פעמיים, אז ניתן לזהות חזרה זו. על מנת להתגבר על בעיה זו אפשר לשרשר מחרוזת אקראית ארוכה מספיק R להודעה X כך שהסתברות החזרה של המחרוזת האקראית תהיה אפסית.
את ההצפנה של השרשור של תוכן X עם מחרוזת רנדומלית R נסמן $K(R, X)$.

שימוש נוסף להצפנה אסימטרית הוא שמשתמש יכול לחתום הודעה ע"י הצפנה של התוכן עם המפתח הפרטי שלו, וכל מחזיק במפתח הציבורי המתאים יכול לוודא שהתוכן אותנטי משום שרק מחזיק המפתח הפרטי יכול היה להצפין איתו.
גם כאן יש בעיה דומה שאם הודעה נחתמה פעמיים, יהיה ניתן להעתיק את החתימה ולזייף את שליחת ההודעה בשם מחזיק המפתח הפרטי. גם במקרה זה אפשר לשרשר מחרוזת אקראית שתסומן C לגוף ההודעה.
נסמן את תהליך החתימה כך $K^{-1}(C, X) = Y$.
מקבל ההודעה יכול לאמת את C ע"י פענוח של Y ובדיקה ש-C תואם.

בפתרון זה לבעיית ניתוח התקשורת נניח שתי הנחות לגבי התקשורת:

1. תקשורת מוצפנת כמתואר בסעיף הקודם נשארת סודית ואף גורם מלבד יוצר ההודעה ומחזיק המפתח הפרטי לא יכול לקרוא אותה או לזייף את תוכנה.
2. כל אחד יכול להאזין לתקשורת ולראות מי שלח את ההודעה ומי הנמען. כמו כן, כל אחד יכול לשנות את ההודעה, למחוק אותה או להוסיף הודעות חדשות.

במילים אחרות, תווך התקשורת הוא גלוי וניתן למניפולציות, אך משום שההודעות מוצפנות לא ניתן להבין את תוכנן או לזייף הודעה אשר נחתמה עם מפתח פרטי.

5.4 מערכת דוא"ל

בשביל לפתור את בעיית ניתוח התקשורת, מוצגת מערכת דוא"ל בה יש שימוש ביישות נוספת הנקראת "מערבל" שמעבדת כל דוא"ל בדרכו מהשולח אל הנמען. אל מערבל זה יישלחו כל ההודעות באופן הבא:

- כל משתמש שישלח הודעה M שמיועדת לנמען A יצפין אותה עם המפתח הציבורי של הנמען - K_A
- השולח ישרשר להודעה המוצפנת את הכתובת של A לא מוצפנת.
- לאחר מכן יצפין את ההודעה עם המפתח הציבורי של המערבל K_1 .
- לפני כל הצפנה, יוסיף המשתמש להודעה אותה הוא מתכוון להצפין מחרוזת אקראית כפי שתואר בפרק ״סימונים״.

לסיכום המשתמש ישלח את ההודעה הבאה: $K_1(R_1, K_A(R_0, M), A)$
לאחר שהמערבל יקבל את ההודעה ויפענח אותה, הוא יקבל את הכתובת A ואת ההודעה הבאה, שאותה יעביר ל-A:

$$K_A(R_0, M)$$

המערכת הנ״ל פותרת את בעיית ניתוח התקשורת משום שאי אפשר לדעת מי שלח למי איזו הודעה. כל ההודעות נשלחות למערבל וכל ההודעות יוצאות מהמערבל. עם זאת, ניתן היה להסיק מי השולח ומי הנמען במקרים הבאים המבוססים על הנחה מספר 1 לעיל:

1. אם כל הודעה הייתה נשלחת מיד עם הגעתה, או אם ההודעות היו נשלחות לנמען לפי אותו סדר שבו הן הגיעו למערבל, גורם אשר מאזין לתקשורת בצד השולח ובצד המקבל יכול לגלות עקביות בזמני השליחה והקבלה של הודעות ולהסיק ששני הצדדים מתקשרים.
2. אם המערבל היה מוציא הודעות ללא שינוי, היה ניתן לעקוב אחרי אורכי ההודעות שנשלחות ולהסיק מי השולח ומי הנמען.

לכן, המערבל פותר את שתי הבעיות הנ״ל ע״י שליחת הודעות באצוות, כאשר כל הודעה באורך קבוע (ניתן לרפד במחרוזות רנדומליות) ובסדר לקסיקוגרפי של התוכן המוצפן.
כל זאת, בהנחה שמשתמשים במחרוזות אקראיות אשר לא חוזרות על עצמן ועל כן גם התוכן המוצפן לא חוזר על עצמו.

אחרת, ניתן להסיק ששתי ההודעות זהות שנשלחו הגיעו לנמען שקיבל שתי הודעות מוצפנות זהות.
המערבל יכול להתמודד גם עם הודעות זהות באופן הבא:

- אם ההודעות חוזרות על עצמן (מבחינת תוכנן והנמען שלהן) בתוך אותה אצווה, ניתן להסיר עותקים.
- אם משתמשים באותו מערבל (ובאותו מפתח הצפנה של מערבל) אז המערבל צריך לשמור את כל ההודעות שנשלחו דרכו עד החלפת מפתח הצפנה. במקרה זה ניתן לבדוק אם הודעה נשלחה בעבר ולהחליט לא לשלוח אותה.
- בשביל להימנע משמירת כל היסטוריית ההודעות, המערבל יכול להחליף מפתח הצפנה K_1 לכל אצווה, כך שכל הודעה מוצפנת בכל פעם עם מפתח אחר והתוכן המוצפן אינו חוזר על עצמו.
- אלטרנטיבה יעילה יותר, היא לא לחזור על מחרוזות אקראיות כלל (R_1) ומומלץ להשתמש במחרוזת ייחודית לכל הודעה, למשל כזו המחושבת על סמך זמן השליחה, שתמיד עולה ולכן לעולם לא יחזור על עצמו.

5.5 אישור שליחה חתום

אם השולח מקבל "אישור שליחה חתום" לכל הודעה שהוא שולח אל המערבל, אז במידה וההודעה שלו לא הגיעה ליעדה, אז הוא יוכל לספק בעתיד ראיה לכך שהוא העביר את ההודעה למערבל אך זה לא העביר את אותה הלאה באופן תקין או בכלל.

"אישור שליחה חתום" - הוא אישור אשר נשלח מהמערבל לכל אצוות הודעות שנשלחת ממנו. הוא חתום עם המפתח הפרטי של המערבל ולכן לא יכול להיות מזויף ע"י אף גורם אחר. תוכן ההודעה החתומה הוא האצווה כולה. לכן בקבלת אישור השליחה החתום, יכול השולח לוודא שההודעה שלו אכן נמצאת בתוך האצווה כמו שהיא.

אישור שליחה חתום יראה כך: $K_1{}^{-1}(C, Z)$

כאשר ההודעה המקורית שנשלחה על המערבל היא $Z = K_1(R_1, K_A(R_0, M), A))$

משום שלכל שולח יש את המפתח הציבורי של המערבל הוא יכול לחלץ את ההודעה שלו: $K_A(R_0, M)$ וגם את כתובת הנמען A.

אם ההודעה אינה תקינה, או אם כתובת הנמען אינה נכונה, יוכל השולח לספק את שתי המחרוזות הנ"ל כראיות לעובדה שההודעה לא נשלחה כמו שצריך. המחרוזת R_1 תשמש כראייה שההודעה אכן נשלחה ע"י השולח. משום שאף אחד אחר לא יכול היה לפענח את ההודעה המקורית ולחלץ אותה, ע"ב הנחה (1).

5.6 שרשרת של מערבלים

עד כה, תיארנו מערכת עם מערבל יחיד אבל אפשר להשתמש גם בשרשרת של מערבלים. הודעה שנשלחת דרך שרשרת של n מערבלים תראה כך:

$$K_n(R_n, K_{n-1}(R_{n-1}, \ldots, K_2(R_2, K_1(R_1, K_A(R_0, M), A)) \ldots))$$

כל מערבל המקבל הודעה כזו, יפתח את ההצפנה החיצונית ביותר בביטוי שמתאימה למפתח ההצפנה שלו.

אם נמשיך עם הדוגמא הנ"ל, המערבל הראשון בשרשרת שיקבל את ההודעה הוא המערבל ה-n והביטוי שיישלח ממנו הוא:

$$K_{n-1}(R_{n-1}, \ldots, K_2(R_2, K_1(R_1, K_A(R_0, M), A)) \ldots)$$

והמערבל האחרון בשרשרת יפתח את ההודעה המיועדת אליו ויישאר עם כתובת הנמען וההודעה המיועדת אליו בלבד: $K_A(R_0, M), A$

היתרון בסדרה של מערבלים הוא שכל מערבל בסדרה יכול לוודא שנשמרה תקינות ההודעות ויכול לדעת אם כל מערבל בשרשרת שלח הודעה לא תקינה. בקבלת אישור שליחה חתום יכול כל מערבל לוודא שההודעה שנשלחה בחזרה מתאימה להודעה שהוא הצפין ולדעת אם המערבל הבא בשרשרת לא שלח את ההודעה באופן תקין.
אם מתגלה מערבל כזה, ניתן לשלוח הודעה לכל כתובות ההחזרה להסיר אותו משרשרת המערבלים. כך ניתן לשמור על שרשרת מערבלים הגונים שאינם עורכים או מוחקים הודעות.

5.7 כתובות החזרה

הטכניקות שתוארו עד כה מתארות את תהליך שליחת הודעה של שולח x לנמען y.
בחלק הבא נתאר איך יכול y לענות ל x ולשלוח לו הודעה מוצפנת בחזרה מבלי לדעת את הזהות שלו.
השולח x יוצר כתובת החזרה ושולח אותה ביחד עם ההודעה. כתובת ההחזרה היא $K_1(R_1, A_x), K_x$ כאשר:

- K_1 הוא המפתח הציבורי של המערבל.
- R_1 מחרוזת רנדומלית שתשמש גם להצפנת ההודעה החוזרת מ y.
- A_x היא הכתובת האמיתית של x.
- K_x הוא מפתח ציבורי שנוצר בשביל הודעה זו.

בקבלת הודעה זו y ישלח את ההודעה $K_1(R_1, A_x), K_x(R_0, M)$ אל המערבל כאשר M היא המענה שהוא מבקש לשלוח לשולח האנונימי x.
המערבל יפענח את החלק שמוצפן עם K_1 בשביל:

- למצוא את הכתובת האמיתית של x.
- להשתמש במחרוזת הרנדומלית R_1 בשביל להצפין את החלק בהודעה שנשלחה מ y ל x.

כלומר ההודעה שתשלח מהמערבל ל x היא: $R_1(K_x(R_0, M))$
רק x יכול לפענח אותה משום שהוא יצר את R_1 ואת K_x.
נשים לב שבשום שלב לא יכול y לדעת את כתובתו האמיתית של x משום שהתוכן שנשלח אליו מוצפן עם המפתח הציבורי של המערבל.

משום שכאמור, אסור לחזור על תוכן הודעות, אסור גם לחזור על כתובות החזרה. לכן שני משתתפים אשר שולחים אחד לשני כתובות החזרה, צריכים ליצור מפתחות חדשות (כמו R_1 ו- K_x) לכל הודעה חדשה שהם שולחים.

ניתן לספק אישרור לשליחת הדוא"ל בעזרת כתובת ההחזרה. כתובת החזרה יכולה לשמש את המערבל להעביר אישור שליחה חתום מהנמען או ממערבל אחר בשרשרת אל השולח המקורי. כך הוא יכול לוודא שהדוא"ל נשלח והגיע לנמען ללא שינויים או מחיקות.

.

5.8 פסבדונים דיגיטליים

באמצעות טכניקה דומה, ניתן ליצור פסבדונים דיגיטליים - קבוצה של מפתחות ציבוריים שמאפשרים וידוא שהודעה נשלחה ע"י מחזיק המפתח הפרטי.
רשימת הפסבדונים מוחזקת ע"י "הרשות" - יישות כלשהי שמאגדת את הפסבדונים הקיימים ומקבלת בקשות הרשמה לפסבדונים.
הרשמה מתבצעת ע"י שליחת בקשה באמצעות דוא"ל מאובטח (כמתואר מעלה) כאשר כל בקשה תכיל:

1. את כל המידע הרלוונטי להרשמה הדרוש בשביל לאפשר לרשות להחליט מי מתקבל ומי לא.
2. מפתח ציבורי.

הרשות תקבל את כל הבקשות כאצווה אחת ממערבל או משרשרת מערבלים, על מנת לא לחשוף את זהות הפסבדונים. כמו כן, ניתן גם להודיע לכל שולחי הבקשות האם הם התקבלו או לא באמצעות יצירת אצווה אחת לקבלה ואצווה אחת לדחייה.

5.9 מערכת בחירות אנונימית

על בסיס טכניקת הפסבדונים הדיגיטליים הנ״ל, ניתן ליצור מערכת הצבעות אנונימית.
גם במערכת הבחירות תהיה "רשות" אשר תחזיק את כל פסבדוני המצביעים ותספור את קולות הפסבדונים.
לכל מצביע רשום יש פסבדונים דיגיטלי (יחיד) ברשות וכך כל אחד מהמצביעים מזין את הבחירה שלו למערכת באופן אנונימי, אבל מבלי לאפשר למשתמשים לא רשומים להטות את הבחירות.

במערכת זו, כל מצביע שולח את הבחירה שלו באופן הבא: $K_1(R_1, K, K^{-1}(C, V))$
כאשר K הוא הפסבדונים של המצביע, K_1 הוא המפתח הציבורי של המערבל, C היא מחרוזת רנדומלית שמשמשת לאימות החתימה ו-V היא ההצבעה עצמה. ניתן לשים לב שההצבעה חתומה ע״י המפתח הפרטי של המצביע, מה שמאפשר לוודא שהצבעה זו אכן נשלחה ממצביע רשום עם מפתח ציבורי K.

הצבעה זו משתמשת במערבל יחיד. באופן דומה ניתן להשתמש בשרשרת מערבלים כדלקמן:
$K_n(R_n,\dots,K_2(R_2,K_1(R_1,K,K^{-1}(C,V)))\dots)$
גם כאן כל ההצבעות צריכות להישלח כאצווה אחת על מנת להסוות את התקשורת בין הרשות לבין המצביעים.

ספירת הקולות תתבצע באופן הבא:

- משום שלרשות יש את המפתחות הציבוריים של כל המצביעים, הרשות יכולה לוודא את כל ההצבעות ממשתמשים רשומים.
- לאחר וידוא ההצבעות ניתן לספור את הקולות.
- כמו כן, ניתן לוודא שכל פסבדונים שלח לכל היותר הצבעה אחת.

משום שכל מצביע נדרש להירשם כפסבדונים במערכת, ובתהליך ההרשמה שולח כל מצביע פרטים שבעזרתם קובעת הרשות האם לשמור את הפסבדונים או להתעלם מהבקשה, ייתכן כי יש לרשות מידע כלשהו, בעזרתו ניתן לזהות את המצביע. יש כאן פשרה - מצד אחד הרשות תרצה לקבל כמה שיותר פרטים מזהים כדי לוודא שאין מצביע אחד שנרשם עם יותר מפסבדונים אחד. מצד שני, ככל שהרשות תדרוש יותר פרטים מזהים כך מערכת הבחירות פחות אנונימית.

אם אנחנו רוצים לבצע הצבעה לא אנונימית, בה כל המשתתפים צריכים לזהות את עצמם, המשתתף יכול לשלוח את זהותו וע״י חתימה עם המפתח הפרטי, הארגון יכול להיות בטוח שאותו משתתף לא יכול להזדהות בשם משתתף נוסף.

5.10 מערכת דוא״ל לשימוש כללי

דרך אחת ליצור מערכת כללית של דוא״ל שלא ניתן למעקב הוא לדרוש שכל הודעה תעבור דרך שרשרת של מערבלים. מערבלים יוכלו לעבוד באצוות או באופן רציף. עבודה באצוות יכולה לגרום לעיכובים אם אין מספיק הודעות לשלוח באותה אצווה. מצד שני עבודה באופן רציף עלולה לשלוח רק הודעה אחת בכל פעם ועלולה לגרום לחשיפת זהות השולח של אותה הודעה. בשביל לטפל בשני מקרים אלה ניתן לדרוש מכל שולח לשלוח מספר הודעות קבוע, כך שחלק מההודעות יהיו הודעות ליעדים רנדומליים. בקבלת ההודעות, המקבל יצטרך לסרוק את האצווה כולה, ולעבד רק הודעות שנשלחו אליו. הודעות אשר גדולות מגודל האצווה יצטרכו להישלח בחלקים רק לאחר שיוצפנו.

הפתרונות עלולים להיות יקרים מדי לחלק מהמשתתפים או לתשתית האינטרנט בה הם משתמשים ולכן ניתן לחלק את קבוצות המשתתפים לתת-קבוצות זרות שייצרו כל אחת רשת מקומית. חברים ברשת מקומית יצטרכו לחפש רק את ההודעות המיועדות אליהם.
דרך נוספת להפחית את כמות ההודעות שנשלחות בכל פעם, היא לשלוח מספר רנדומלי של הודעות בכל פעם ולאו דווקא את המספר המקסימלי.

5.11 מערבל מסוג חדש

באופן כללי, מערכת דוא״ל שכוללת מערבלים רבים וכל הודעה בה צריכה לעבור דרך כולם היא לא יעילה.
לכן מוצע פתרון שבו כל הודעה תעבור דרך מספר קבוע של מערבלים שיקבעו מראש. כלומר, כל הודעה תעבור דרך מערבלים שונים, שנבחרים בכל פעם ע״י השולח, על בסיס טופולוגיית רשת או אמון במערבלים שונים.

לכן מוצע מערבל מסוג חדש, אשר יאפשר לכל שולח הודעה לבחור את שרשרת המערבלים הייחודית להודעה המסויימת שהוא שולח. מעבר לשיפור המשמעותי ביעילות המערכת, יש פה שיפור נוסף בהתמודדות עם בעיית ניתוח הרשת משום שהמערבל מסתיר גם את המערבל הבא אליו כל הודעה עוברת. כמו בשיטה שתוארה קודם, גם סוג זה מאפשר לוודא אם הודעה הגיעה או לא וניתן לדעת איזה מערבל לאורך השרשור נכשל בהעברת ההודעות שנשלחו אליו באופן תקין.
יש לציין שהמערבל לא מבדיל בין סוגי ההודעות אלא מתבסס על העובדה שכל דוא"ל מכיל מספר קבוע של בלוקים באותו גודל.

המערבל החדש פועל בצורה הבאה:

1. הוא מסיר את הבלוק הראשון בהודעה.
2. הוא מוסיף בלוק רנדומלי J בסוף ההודעה בשביל לשמור על המספר הקבוע של הבלוקים.
3. הוא מפענח את הבלוק הראשון שהוסר עם המפתח הפרטי שלו. הפענוח מניב שני דברים:
   a. מפתח שישמש להצפנת שאר הבלוקים שיסומן R.
   b. כתובת של המערבל הבא או הנמען הסופי שאליה תועבר ההודעה המוצפנת שתסומן A.
4. הוא מפענח את שאר הבלוקים שמוצפנים עם המפתח הפרטי שלו.

לדוגמא אם מספר הבלוקים הקבוע הוא t אז ההודעה שהמערבל A_1 מקבל היא: (כל בלוק תחום ב [...])

$$[K_A(R_A, A)], [R^{-1}{}_{A_1}(M_1)], [R^{-1}{}_{A_1}(M_2)], \ldots . [R^{-1}{}_{A_1}(M_{t-1})]$$

לאחר הפענוח תתקבל ההודעה הבאה שתועבר למערבל A כפי שמוצפן בבלוק הראשון:

$$[M_1], \dots [M_{t-1}], [R_A(J_{A_1})]$$

הודעה שצריכה לעבור דרך שני מערבלים A_1, A_2, ומיועדת לכתובת A תראה כך:

$$[K_{A_1}(R_{A_1}, A_2)], [R^{-1}{}_{A_1}(K_{A_2}(R_{A_2}, A)], [R^{-1}{}_{A_1}(R^{-1}{}_{A_2}(M_1))], \dots . [R^{-1}{}_{A_1}(R^{-1}{}_{A_2}(M_{t-2}))]$$

לאחר הפענוח של מערבל A_1, ההודעה שתועבר למערבל A_2 תראה כך:

$$[K_{A_2}(R_{A_2}, A)], [(R^{-1}{}_{A_2}(M_1)], [(R^{-1}{}_{A_2}(M_2)], \dots, [(R^{-1}{}_{A_2}(M_{t-2})], [R_{A_1}(J_{A_1})]$$

ולבסוף ההודעה שתגיע ליעד A היא:

$$[M_1], [M_2], \dots, [M_{t-2}], [R_{A_2}(R_{A_1}(J_{A_1})], [R_{A_2}(J_{A_2})]$$

5.12 סיכום

הוצג פתרון לבעיית ניתוח הרשת, ללא יישות מרכזית אלא ע"י שרשרת של מערבלים. כל מערבל שמתעורר לגביו חשד שהוא אינו מעביר את ההודעות בצורה תקינה ניתן להסרה.

הפתרון מאפשר שליחת הודעות אנונימית, תוך שליחת אישור שההודעה אכן התקבלה ללא שינוי.

בנוסף, המערכת מאפשרת למשתמש לשלוח הודעות מבלי בהכרח לדעת את כתובתו או זהותו של הנמען.

כמו כן, הוצגו שימושים נוספים כמו פסבדונים ומימוש של מערכת בחירות השומרת על אנונימיות המשתמשים. המאמר אינו מציין אם מערבל הוא יישות מיוחדת, או שכל משתתף יכול גם להיות גם מערבל. לכן, למעשה זהו תיאור של מערכת מבוזרת שנועדה להעביר הודעות בצורה אנונימית, בה כל משתתף יכול להיות גם שולח הודעות וגם מערבל.

ניתן לראות דמיון רב בין מערכת TOR לבין המערכת המוצעת במאמר זה. במיוחד החלק האחרון שמתאר "מערבל מסוג חדש" ששולח כל הודעה דרך שרשרת מערבלים אקראית. ייתכן ומאמר זה היווה את הבסיס התיאורטי ל-TOR או לפחות את ההשראה לפיתוחו.

6. סכמת הצבעה פרקטית לבחירות רחבות היקף

6.1 תקציר

במאמר זה מוצעת מערכת פרקטית להצבעה סודית לבחירות עם מספר מצביעים גדול. הצדדים המשתתפים במערכת זו הם המצביעים, מנהל הבחירות וסופר הקולות. המערכת שומרת על סודיות ההצבעות אפילו במקרה ומנהל הבחירות וסופר הקולות קושרים קשר ומנסים לחשוף את זהות המצביעים. כמו כן, לא ניתן לדעת שום תוצאה חלקית של ספירת הקולות על מנת למנוע הסקת מסקנות ממידע חלקי אשר יפגע בסודיות ובתוצאות הבחירות.

6.2 מבוא

מאמרים רבים הציעו פרוטוקולים תיאורטיים ופרקטים להצבעה סודית, אך עד למאמר זה השתמשו כל הפרוטוקולים בחישוב מרובה משתתפים שבו כלל המצביעים ורק הם לוקחים חלק בחישוב התוצאה הסופית. עם זאת, נדרשים תהליכים רבים של תקשורת על מנת להוכיח שכל ההצבעות נספרו כפי שהן נשלחו ע״י המצביעים. לכן גישה זו אינה פרקטית. גישה פרקטית חייבת להציע סוגי משתתפים נוספים - יישות מרכזית אמינה או מנהל בחירות. ישנן שתי גישות עיקריות שהוצגו במאמרים קודמים.

הגישה הראשונה [Ben87,CF85,IK91] היא שימוש במרכזים מבוזרים, כך שכל מצביע שולח את הקול שלו למספר גורמים שונים שמקבלים את אותה הודעה בדיוק. כל אחד ממרכזים אלו יכול לחשב את התוצאה הסופית ולכן תקינות הבחירות נשמרת. עם זאת, המצביע צריך להוכיח שההצבעה המבוזרת שלו תקינה ולכן כל ההצבעות צריכות להתבצע באותו הזמן. הבעיה העיקרית עם גישה זו היא במקרה שבו כל המרכזים המבוזרים קושרים קשר, ואז סודיות המצביעים נפגעת. כמו כן, עלות התקשורת הגבוהה כאשר יש מספר רב של מצביעים הופכת את הגישה הזו ללא פרקטית.

בגישה השנייה [Cha88] משתמשים בערוץ תקשורת אנונימי על מנת להסוות את מקור התקשורת ואת המצביעים עצמם. כל ההצבעות נשלחות אל יישות מרכזית אחת שסופרת את הקולות ועיקר הפרוטוקול עוסק במניעת מעקב אל מקור ההצבעות. גישה זו יותר מתאימה לבחירות, משום שגם אם מספר המצביעים גדול, סיבוכיות התקשורת עדיין סבירה.

עם זאת לשתי הגישות שני חסרונות זהים:

1. בעיית ההוגנות (fairness) - כל מרכז מבוזר בגישה הראשונה או יישות מרכזית בגישה השנייה יודע את תוצאות הביניים של הבחירות ולכן יכול לפרסם אותן. פירסום תוצאות הביניים עלול להשפיע על התוצאה הסופית.
2. בעיית הפרטיות (privacy) - פרטיות המצביע נפגעת כאשר הוא שם לב שההצבעה שלו לא נספרה ומציג את ההוכחה לכך. כלומר בסכמות הנ"ל, המצביע שולח את ההצבעה שלו באופן אנונימי אך היא אינה מוסתרת ע"י התחייבות ביטים או חתימה עיוורת. לכן בשביל לטעון שההצבעה לא נספרה, המצביע צריך לחשוף את תוכן ההצבעה שלו ולהוכיח שהיא לא קיימת בלוח ההצבעות. במקרה זה, שאר המשתתפים נחשפים לזהות המצביע וההצבעה שלו.

מאמר זה מציג סכמת הצבעה סודית שמתאימה לבחירות עם מספר רב של מצביעים ופותרת את שתי הבעיות הנ"ל. כלומר, הפרוטוקול מבטיח את פרטיות המצביעים גם במקרה של שיתוף פעולה בין גורמים שונים. כמו כן, הפרוטוקול שומר על הוגנות משום שאף גורם במערכת לא נחשף לתוצאות ביניים.

6.3 הגדרות לבטיחות מערכת בחירות

המאמר מגדיר מערכת הצבעות כמאובטחת אם היא מקיימת את התכונות הבאות:

1. שלמות - כל הצבעה תקינה נספרת.
2. עמידות - מצביע לא יכול להפריע למהלך התקין של ההצבעה.
3. פרטיות - כל ההצבעות נשמרות סודיות.
4. יחידות - כל מצביע יכול להצביע פעם אחת בדיוק.
5. זכאות - מי שאינו מורשה להצביע לא יכול להצביע.
6. אמינות - שום דבר לא יכול להשפיע על תוצאות הבחירות, מלבד ההצבעות התקינות.
7. אימות - לא ניתן לזייף את תוצאת הבחירות.

6.4 סכמת ההצבעה

הסכמה כוללת שלוש יישויות - מצביעים, מנהל הבחירות, וסופר קולות. המצביעים וסופר הקולות מתקשרים באמצעות ערוץ אנונימי כפי שתואר ב-[Cha81] (המפורט כחלק מעבודה מסמכת זו). הסכמה משתמשת בהתחייבות ביטים (bit commitment) כמתואר ב-[Nao89], חתימות דיגיטליות (digital signatures) כמתואר ב-[DH76] וחתימות עיוורות (blind signatures) כמתואר ב-[Cha83]. נושאים אלו תוארו בפרק הרקע הקריפטוגרפי.

6.5 מבנה הסכמה

הסכמה מורכבת מהשלבים הבאים:

1. הכנה - המצביע יוצר הודעה המכילה את הבחירה שלו, מפעיל עליה את פונקציית התחייבות הביטים, מסתיר אותה על מנת שמנהל הבחירות יחתום עליה, חותם דיגיטלית על ההודעה ושולח את ההודעה למנהל.
2. אימות - המנהל חותם על ההודעה המוסתרת ומחזיר אותה למצביע.
3. הצבעה - המצביע שולח בצורה אנונימית את ההודעה המוסתרת והחתומה אל סופר הקולות.
4. איסוף - סופר הקולות מפרסם רשימה של כל הקולות (המוסתרים) שקיבל בצורה אנונימית. לכל קול מוסתר שהוא מקבל הוא מצמיד מספר סידורי (על פי סדר ההגעה שלהם). כעת, כל מצביע יכול למצוא את הצבעתו ברשימה הזו ולראות מה המספר הסידורי המוצמד לה.
5. חשיפה - המצביע חושף את הקול שלו ע"י כך שהוא שולח באופן אנונימי לסופר הקולות את הנתונים הבאים: המספר הסידורי של הצבעתו, המספר ההופכי לגורם ההסתרה שהשתמש בו בחתימה העיוורת, ובנוסף את פונקציית התחייבות הביטים וההודעה המקורית על מנת שסופר הקולות יוכל לוודא שהמצביע לא שינה את הצבעתו המקורית.
6. ספירה - סופר הקולות פותח את כל ההצבעות, סופר את הקולות ומפרסם את התוצאה הסופית.

זוהי הסכמה ממעוף הציפור מבלי להיכנס לפרטים טכניים. כעת נתאר כל שלב באלגוריתם בפירוט ובסימונים הנ"ל. מספרי השלבים יהיו זהים אך כעת נפרק כל שלב לתת-שלבים.

1. הכנה

1.1. המצביע V_i יוצר הצבעה v_i ומכין את ההצבעה עם התחייבות ביטים ע"י הפעלת פונקציית ההתחייבות $x_i = \xi(v_i, k_i) = sha256(v_i, k_i)$ עם מפתח אקראי k_i. בשלב מאוחר יותר יחשוף המצביע את הצבעתו ע"י שליחת v_i ו- k_i.

1.2. V_i יוצר את ההודעה $e_i = \chi(x_i, r_i) = x_i r_i^{e_A} mod n_A$ ע"י הסתרת ההודעה עם מספר אקראי r_i בחזקת e_A שמאפשר למנהל לחתום דיגיטלית על ההודעה מבלי להיחשף לתוכנה.

1.3. V_i חותם על ההודעה דיגיטלית $s_i = \sigma_i(e_i) = {e_i}^{d_i} mod n_i$ עם המפתח הפרטי שלו (n_i, d_i) ושולח למנהל את ההודעה e_i, המספר המזהה שלו ואת החתימה הדיגיטלית - (ID_i, e_i, s_i).

2. אימות

2.1. המנהל A בודק שהמצביע שמזוהה ע"י ID_i רשאי להצביע.

2.2. A בודק אם V_i כבר הגיש בקשת חתימה בעבר.

2.3. A בודק שהחתימה s_i על e_i תקינה ושהיא אכן נחתמה ע"י V_i .

2.4. אם אחד התנאים הנ"ל אינו מתקיים, המנהל דוחה את הבקשה.

2.5. המנהל חותם על ההודעה ויוצר את $d_i = \sigma_A(e_i) = {e_i}^{d_A} mod n_A$ עם המפתח הפרטי שלו (n,d) שמוכיח ש-A אישר את הבקשה. A שולח את d_i למצביע V_i.

2.6. בסוף סבב האימותים ולאחר שכל המצביעים הגישו בקשת אימות, המנהל מכריז על מספר המצביעים המאושרים ומפרסם את רשימת המצביעים כשלשות מהצורה הבאה (ID_i, e_i, s_i)

3. הצבעה

3.1. V_i מקבל את ההודעה החתומה מ-A וחושף את החתימה על התוכן המקורי בעזרת המספר ההופכי ל- r_i שאיתו הסתיר את ההודעה בסעיף 1.2. כלומר

$$y_i = \delta(d_i, r_i) = d_i {r_i}^{-1} = {e_i}^{d_A} {r_i}^{-1} = (x_i {r_i}^{e_A})^{d_A} {r_i}^{-1} = {x_i}^{d_A} {r_i}^{e_A d_A} {r_i}^{-1} = {x_i}^{d_A} \ mod n_A$$

3.2. V_i בודק ש y_i היא אכן החתימה של A על x_i. אחרת V_i יכול להוכיח שהתשובה שהוא קיבל d_i אינה מכילה חתימה של A בעזרת הצגת $< x_i, y_i >$.

3.3. V_i שולח את $< x_i, y_i >$ לסופר הקולות C דרך ערוץ אנונימי כמתואר ב [.[Cha81

4. איסוף

4.1. C מקבל את $< x_i, y_i >$ ומוודא שהחתימה y_i תקינה ואכן נחתמה על x_i בעזרת המפתח הציבורי של A. אם החתימה תקינה, מוסיף C את ההצבעה לרשימת ההצבעות עם מספר סידורי l (המאותחל להיות 1 ובכל פעם שמתקבלת הצבעה חדשה הוא עולה ב-1)

4.2. אחרי שכל הקולות התקבלו, מפרסם C את רשימת ההצבעות.

5. חשיפה

5.1. V_i בודק שמספר הקולות ברשימה שווה למספר המצביעים כפי שדווח ע"י המנהל בסעיף 2.6.

5.2. V_i בודק שהקול שלו $< x_i, y_i >$ נמצא ברשימה ומוצא מה המספר הסידורי l המוצמד אליה. אחרת הוא יכול להוכיח שההודעה שלו נחתמה ע"י A אך לא הגיעה לרשימה הסופית. הוא יכול להוכיח שזה הקול שלו משום שהוא היחיד שיכול לחשוף את החתימה העיוורת בעזרת r_i^{-1}.

5.3. V_i שולח ל-C דרך ערוץ אנונימי את הפרטים לחשיפת ההצבעה שלו - פונקציית התחייבות הביטים, המספר ההופכי לגורם ההסתרה שהשתמש בו בחתימה העיוורת k_i , ההצבעה עצמה v_I שנוצרו בסעיף 1.1 ואת המספר הסידורי l.

6. ספירה

6.1. לאחר קבלת כל המידע המאפשר לפתוח את ההצבעות המוסתרות, פותח C את כל ההצבעות המוסתרות x_i וחושף את הקולות v_i.

6.2. סופר הקולות מוודא לכל מצביע שהתחייבות הביטים שלו תקינה. כלומר, לכל i מתקיים $x_i = sha256(v_i, k_i)$. אם השוויון לא מתקיים הוא לא סופר את v_i.

6.3. C סופר את הקולות התקינים ומכריז על תוצאות הבחירות.

6.6 בטיחות הסכמה

הסכמה מאובטחת לפי "הגדרות לבטיחות מערכת הצבעות" הנ"ל. נוכיח כל אחת מהטענות בנפרד.

- שלמות (כל הצבעה תקינה נספרה): אם כל המשתתפים הוגנים אז כל הקולות נספרים ותוצאות הבחירות שלמות ואמינות. ההוכחה טריוויאלית.

- עמידות - מצביע לא יכול להשפיע או להפריע למערכת ההצבעות. ההוכחה מבוססת על העובדה שהדרך היחידה לשבש את תוצאות הבחירות היא שמצביע ישלח הרבה קולות שאינם תקינים. עם זאת, אם ברשימת ההצבעות קיימת הצבעה עם מפתח לא תקין, לא ניתן לדעת האם המצביע שלח את הצבעתו עם מפתח שאינו תקין או שסופר הקולות אינו הגון. ניתן להתמודד עם בעיה זו ע"י יצירת מספר סופרים או ע"י שליחת ההצבעות החתומות למתמודדים עצמם, שניתן להניח שאינם משתפים פעולה.

- פרטיות - גם אם המנהל וסופר הקולות קושרים קשר הם אינם יכולים לגלות את הקשר בין הצבעה v_i למצביע V_i. הוכחה: הקשר בין זהות המצביע ID_i לבין ההודעה שנשלחת לסופר הקולות x_i מוסתר ע"י החתימה העיוורת. x_i ו k_i נשלחים דרך ערוץ אנונימי ולכן לא ניתן לקשר אותם לשולח. בנוסף, גם אם המצביע טוען שהקול שלו לא נספר הוא לא צריך לחשוף את v_i ולכן ההצבעה שלו נשמרת פרטית בכל מקרה:

  - בשלב ההצבעה (3), אם המנהל מציג אישור שליחה שאינו תקין, המצביע צריך לחשוף רק את הצמד x_i, y_i שכאמור מסתיר את v_i.

  - בשלב החשיפה (5), אם הקול של המצביע לא רשום ברשימת הקולות הוא רק צריך לחשוף את x_i, y_i על מנת לטעון שנעשה שיבוש בספירת הקולות.

- יחידות - האי-יכולת להצביע יותר מפעם אחת נובע מהאי-יכולת של מצביע לזייף את החתימה העיוורת של המנהל. זאת ההנחה בסעיף זה. הוכחה: בשביל להצביע פעמיים יש להשיג שני זוגות מהצורה x_i, y_i , את הזוג הראשון ניתן להשיג מהמנהל אך את הזוג השני הוא צריך ליצור בעצמו, כלומר הוא שובר את החתימה העיוורת בסתירה להנחה.

- זכאות - מי שאינו מורשה להצביע לא יכול להצביע. ההנחה היא שלא ניתן לזייף חתימה דיגיטלית. הוכחה: נניח בשלילה שמשתתף שאינו רשאי להצביע מצביע. משום שהמנהל בודק את החתימה הדיגיטלית של כל מצביע שמגיש בקשה, המשתתף חייב לעבור דרך המנהל ולקבל את אישורו ולכן הצליח לזייף חתימה דיגיטלית מבלי להיות רשום כמצביע, בסתירה להנחה.

- הוגנות - ספירת הקולות לא משנה את ההצבעות עצמן. שלב הספירה מתבצע לאחר שלב ההצבעה וזהות המצביעים מוסתרת ע"י החתימה העיוורת. כל ההצבעות נרשמות ברשימת ההצבעות, לכן אין אפשרות שהקולות ישתנו בשלב הספירה.

- אימות - בהנחה וכל המצביעים הצביעו ולא ניתן לזייף חתימה דיגיטלית, אז אם המנהל וסופר הקולות קושרים קשר, הם לא יכולים לשנות את תוצאות הבחירות.
ההוכחה מתמקדת במנהל בלבד משום שסופר הקולות אינו יכול לשבש את הבחירות, מלבד היכולת לא לפרסם הצבעה אחת או יותר ברשימת ההצבעות. במקרה זה המצביע שאינו רואה את ההצבעה שלו ברשימה יכול להציג את הזוג $< x_i, y_i >$ ולהוכיח שקיימת הצבעה תקינה שלא התפרסמה.
נניח שאין מצביע שלא שלח את הקול שלו. אז אין למנהל דרך לזייף הצבעות. כל הקולות תקינים ולכן התוצאה הסופית של הבחירות תקינה.

6.7 סיכום

במאמר זה הוצגה מערכת הצבעות שמתאימה לבחירות בסדר גודל גדול. מערכת זו ייחודית משום שאין בה תקשורת בין המצביעים אך יש שתי יישויות נוספות - המנהל וסופר הקולות. הוכחנו שהמערכת מאובטחת ומבטיחה את פרטיות המצביעים גם במקרה שמצביע טוען שההצבעה שלו לא נספרה. כמו כן, מערכת זו פותרת את בעיית ההוגנות שהוצגה במבוא ומאפשרת את חשיפת הקולות רק לאחר שכל הקולות נשלחו.

נראה שסכמת ההצבעה המוצגת במאמר זה מתבססת על שתי הנחות שלא בטוח שקל לקיים אותן בבחירות בהיקף ארצי. ראשית מתבססים על העובדה שכולם מצביעים. מצב זה לא קורה במדינות דמוקרטיות. בבחירות האחרונות בישראל היו רק 67% מצביעים ולכן לטעמי זאת לא הנחה שאפשר להתבסס עליה כאשר רוצים לוודא שכל הקולות תקינים. ייתכן מאוד שגורם שרוצה לשבש את הבחירות ינסה לשלוח קולות מזויפים במקום אלו שלא מצביעים או אפילו לנסות להזדהות בשמם.

כמו כן, מתבססים על העובדה שכל המצביעים מוודאים שהקול שלהם אכן נמצא ברשימת ההצבעות שמפרסם סופר הקולות ועל העובדה שכל מצביע חושף בסוף הבחירות את ההצבעה שלו יחד עם המספר הרנדומלי ששימש אותו בהתחייבות הביטים. נדרש מהמצביע לבצע שלוש פעולות שונות בזמנים שונים ולכן לא בטוח שסכמה זו מתאימה לשימוש בבחירות ארציות.

7. סכמת הצבעה מבוססת חתימה עיוורת לשמירת סודיות המצביעים

7.1 תקציר

בעקבות הצמיחה המהירה של רשת האינטרנט ומספר האנשים שיכולים להתחבר אליה, הצבעה אלקטרונית יכולה להוות אמצעי לקיום בחירות, ברמת אבטחה לא פחות גבוהה מהבחירות הסטנדרטיות שמתקיימות היום. במאמר זה מוצגת מערכת הצבעה אלקטרונית שנקראת E-voting המתאימה לבחירות כלליות. המערכת משתמשת בטכניקות קריפטוגרפיות על מנת להתמודד עם בעיות אבטחה בתהליך הבחירות. בנוסף למערכת התיאורטית, המערכת גם ממומשת בשפת ג'אווה. נעשה שימוש בשקעים (sockets) בשביל לתקשר בין המשתתפים במערכת הבחירות ומשתמשים בספריית BouncyCastle על מנת לממש אלגוריתמי הצפנה ושקעים מאובטחים (secure sockets). כמו כן, יש שימוש בפרוטוקול דיפי הלמן, בחתימה דיגיטילית, חתימה עיוורת וטכניקות קריפטוגרפיות נוספות.

7.2 מבוא

בחירות הן אבן יסוד של הדמוקרטיה, הן מאפשרות לאזרחים להביע את רצונם בדרך של הצבעה. האופן שבו מתקיימות בחירות כיום הוא מסורבל ודורש שכל אזרח יגיע פיזית לקלפי על מנת להצביע. עקב כך, אחוזי ההצבעה נמוכים במדינות דמוקרטיות רבות. אלטרנטיבה אחת שקיימת כיום היא הצבעה בדואר שמאפשרת לאזרחים שגרים באזורים מרוחקים להצביע מבלי להגיע לקלפי. עם זאת, שיטה זו מציבה אתגרים לוגיסטיים נוספים כמו שליחה איסוף וספירת כל הקולות שהגיעו בדואר, כמו גם אתגרי אבטחה, למשל איך ניתן לוודא שהדואר אכן נשלח ע"י האזרח הרשום בכתובת הדואר ממנה נשלחה ההצבעה.

מערכת הצבעות אלקטרונית מאפשרת להתגבר על אתגרים אלו ואמורה להפוך את הבחירות הארציות לפעילות נוחה, יעילה וזולה, כך שכל אזרח יוכל להצביע מביתו ללא חשש. לכן מערכת הצבעות אלקטרונית חייבת לעמוד בדרישות אבטחה כמו סודיות, אמינות, אימות ויכולת וידוא. מערכת הצבעות אלקטרונית יותר פגיעה בשל אופיה הדיגיטלי, משום שיותר קל לשנות מידע במחשב מאשר לזייף פתקים בבניין מאובטח. לכן, אי עמידה בדרישות הנ"ל עלולה להוביל למניפולציות, זיופים ושחיתות.

במאמר זה ממומש אב-טיפוס של מערכת הצבעות אלקטרונית שנקראת E-voting שממממשת את כל ארבע דרישות האבטחה על מנת ליצור מערכת הצבעה מאובטחת. כמו כן, יש למערכת ממשק משתמש שנועד למנוע טעויות אנוש.

7.3 דרישות האבטחה

1. סודיות - ההצבעה צריכה להישמר סודית. כמו כן, הפרוטוקול לא יכול לאפשר למשתמש להוכיח שהוא הצביע בדרך זו או אחרת, משום שהוכחה כזו עלולה לשמש לסחיטה או לקניית קולות.
2. אמינות - רק הצבעות חוקיות נספרות. בזמן ספירת הקולות לא ניתן לחבל בתוצאות מבלי להתגלות.
3. אימות - המערכת חייבת לאמת בזמן ההצבעה את כל המצביעים. לא יתקבלו קולות ממצביעים לא רשומים או לא מאומתים. לכן יש לבצע תהליך רישום בו כל מצביע יקבל פריט מידע שישמש אותו לאחר מכן בשלב האימות. כמו כן, המערכת צריכה לוודא שכל אזרח מצביע פעם אחת בלבד.
4. יכולת וידוא - זו תכונה שמורכבת משתי תת-תכונות. ראשית, כל מצביע יכול לוודא שההצבעה שלו התקבלה ונספרה. שנית, כל אחד יכול לוודא שכל ההצבעות נספרו והתוצאה משקפת את כל הקולות. במערכת הצבעות אלקטרונית, תכונה זו מתקבלת ע"י פרסום רשימת הקולות.

7.4 מנגנוני אבטחה

המערכת E-voting משתמשת במספר מנגנוני אבטחה על מנת לממש את ארבע דרישות האבטחה הנדרשות למערכת הצבעה אלקטרונית מאובטחת. במערכת זו, פרטיות המשתמש נשמרת ע"י שימוש בחתימה עיוורת על מנת לשמור על סודיות ההצבעה וחתימה דיגיטלית בשביל לאמת את המשתמש. כמו כן, התקשורת בין המשתתפים בפרוטוקול מוצפנת ע"י שימוש ב-RSA. החלפת מפתחות מתבצעת ע"י שימוש בפרוטוקול דיפי-הלמן. נפרט על השיטות האלה להלן.

7.5 הצפנת המפתח ב-**E-voting**

ב-E-voting מפתח RSA הפרטי ארוך מדי בשביל לזכור ולכן הוא מאוחסן על דיסק חיצוני. על מנת לשמור על סודיותו הוא מאוחסן בצורה מאובטחת באמצעות הצפנה המבוססת על סיסמת המשתמש P. המערכת מצפינה את המפתח הפרטי PK באופן הבא:

- ראשית הסיסמה P עוברת דרך פונקציית גיבוב SHA-1.
- לפלט של פונקציית הגיבוב משרשרים את המלח S והתוצאה היא מפתח הצפנה סימטרי שנסמן K.

- המפתח הפרטי PK מוצפן בעזרת אלגוריתם הצפנה סימטרי עם המפתח K ויוצר את C.
- המערכת מאחסנת את המלח S ואת C על הזיכרון החיצוני.

כאשר המצביע רוצה להשתמש במפתח הפרטי שלו הוא מזין את הסיסמה למערכת. המערכת שוב גוזרת את המפתח ההצפנה הסימטרי K מהסיסמה ומהמלח ואז מפענחת באמצעותו את C ומקבלת את המפתח הפרטי PK.

7.6 ארכיטקטורת **E-Voting**

ארכיטקטורת המערכת מורכבת מ-8 ישויות, כמפורט להלן:

1. מצביע - רק מצביעים רשומים יכולים להגיש מועמדות ולהיבחר.
2. מנהל הבחירות - אחראי לקבוע את תאריך רישום המצביעים והמועמדים ותאריך הבחירות.
3. סופר הקולות - סופר את כלל ההצבעות ומפרסם את התוצאות.
4. מוודא - אחראי על וידוא כל מצביע ופרסום רשימת המצביעים הרשומים. כמו כן, בזמן הבחירות הוא מוודא כל הצבעה שנשלחת למערכת ומייצר לה מספר סידורי.
5. רשם - אחראי על רישום המצביעים ואימות זהותם.
6. בסיס הנתונים של E-voting - מחזיק את המפתחות הציבוריים של כל המשתמשים ואת ההצבעות עצמן.
7. בסיס הנתונים הארצי - מחזיק את פרטי כל האזרחים וזכאותם להצביע.
8. אתר אינטרנט בו יתפרסמו תוצאות הבחירות.

7.7 שלבי הבחירות

יש ארבעה שלבים לבחירות ב-E-voting. רישום מצביעים, רישום מועמדים, הצבעה וספירה. נתאר כל שלב בפירוט. תנאי מקדים להתחלת השלב הראשון הוא שנוצר זוג מפתחות הצפנה לכל הישויות מלבד המצביעים, להם נוצר מפתח בשלב הרישום. כך שכל תקשורת בין ישויות במערכת מתבצעת בצורה מוצפנת.

שלב רישום מצביעים

כל מצביע חייב להירשם לפני שלב ההצבעה על מנת להצביע. הרישום מתבצע באופן הבא:

- כל מצביע שולח את הפרטים המזהים שלו לשרת הרשם.

- שרת הרשם בודק את פרטי המשתמש בבסיס הנתונים הארצי על מנת לבדוק את זכאותו להצביע.
    - אם פרטי המצביע לא קיימים אזי הבקשה נדחית.
    - אחרת, המערכת תייצר זוג מפתחות RSA. המפתח הציבורי יאוחסן בבסיס הנתונים של E-voting והמפתח הפרטי יישלח למצביע באמצעות פרוטוקול דיפי-הלמן ויאוחסן בכרטיס הזיכרון שמחזיק המצביע כפי שתואר בפרק "הצפנת המפתח ב-E-voting". כמו כן, הרשם ייצור מספר ייחודי (ballot-id) לכל מצביע שישמש את המוודא בשלב ההצבעה.

שלב רישום המועמדים

על מנת לרשום מועמד, לפחות שני מצביעים רשומים צריכים לשלוח בקשה למנהל הבחירות לפני תחילת שלב ההצבעה. הבקשה צריכה לכלול את שם ומספר הזהות גם של המצביע ששולח את הבקשה וגם של המועמד. כל בקשה חתומה דיגיטלית ע"י המצביע ואז מוצפנת עם המפתח הציבורי של מנהל הבחירות.

שלב ההצבעה

הצבעה מתבצעת באופן הבא:

1. המצביע שולח את שמו ומספר הזהות שלו למוודא.
2. המוודא בודק שהמצביע רשום ושזו הפעם הראשונה שהוא מצביע. אם שני התנאים מתקיימים המוודא יחזיר למצביע את מספר פתק ההצבעה (ballot-id) - מספר ייחודי שנוצר למצביע בשלב רישום המצביעים.
3. המצביע יוצר הודעה שמכילה את ההצבעה שלו ואת מספר פתק ההצבעה שזה עתה נשלח אליו. המצביע מסתיר אותו בטכניקת החתימה העיוורת, חותם דיגיטלית את ההודעה המוסתרת ומצפין את ההודעה לפני שהיא נשלחת בחזרה אל המוודא.
4. המוודא חותם חתימה עיוורת על ההודעה שנשלחה אליו ומחזיר אותה למצביע.
5. המצביע מוודא את החתימה העיוורת ע"י שימוש בטכניקת החשיפה והשוואה להודעה המקורית.
6. המצביע שולח את ההודעה המקורית ואת ההודעה החתומה בחתימה עיוורת לסופר הקולות.
7. סופר הקולות מוודא שהחתימה העיוורת אכן נוצרה ע"י המוודא בעזרת המפתח הציבורי שלו ושומר את ההצבעה בבסיס הנתונים של E-voting.
8. סופר הקולות יוצר הודעה שמכילה את ההצבעה, מספר פתק ההצבעה וזמן ההצבעה, חותם אותה דיגיטלית ושולח את ההודעה החתומה בחזרה למצביע.

שלב הספירה

כשכל המצביעים סיימו להצביע, סופר הקולות יספור את הקולות, יקבע את המועמד המנצח וישמור את התוצאה בבסיס הנתונים של E-voting. לאחר וידוא תקינות התוצאה היא תתפרסם באתר האינטרנט של המערכת. כל הצבעה תתפרסם המספר המזהה שלה והמועמד הנבחר, ללא הפרטים המזהים של המצביע.

פרסום ה- ballot-id של כל הצבעה מאפשר לכל מצביע לוודא שההצבעה שלו נספרה באופן תקין. אם המצביע אינו מוצא את ההצבעה שלו באתר האינטרנט, או אם המועמד שמופיע שונה מהמועמד שהצביע לו, הוא יכול לטעון לשיבוש הבחירות בעזרת ההודעה החתומה שנשלחה אליו בצעד 8 של שלב ההצבעה.

כמו כן, פרסום כלל ההצבעות מאפשר לכל משתתף במערכת לוודא שהמועמד שהוכרז כמנצח קיבל את מירב הקולות.

7.8 מימוש

המערכת ממומשת בשפת ג'אווה בגרסא 1.3.1jdk ומורכבת משבע תוכנות שונות ואתר אינטרנט אחד. בסעיף זה נפרט את הספריות בשימוש וכל אפליקציה ומטרתה.

ספריית קריפטוגרפיה

המימוש מתבסס על ארכיטקטורת הקריפטוגרפיה של ג'אווה (Java cryptography architecture) והרחבות קריפטוגרפיה של ג'אווה (Java cryptography extension) על מנת לספק ספריות הצפנה קיימות שיעבדו בסביבות שונות ולייתר את הצורך לממש מחדש את כל אלגוריתמי הצפנה הסטנדרטים הנמצאים בשימוש במערכת. יוצרי המערכת בחרו להשתמש בספריית BouncyCastleJCE משום שבזמן כתיבת המאמר היא הייתה ספריית הקוד הפתוח המבוססת ביותר.
במהלך רישום המשתמשים, תקשורת מאובטחת בין המצביע לרשם מתבצעת ע"י הצפנת המידע עם מפתח שנוצר בפרוטוקול דיפי-הלמן. הבעיה בפרוטוקול היא ששני הצדדים צריכים להסכים על מספר ראשוני גדול p. לכן קיים פרוטוקול SKIP שקובע מספר ערכים קבועים לשימוש. במערכת E-voting משתמשים במפרט של SKIP לערכים בגודל 1024 ביטים.

חיבור לרשת

המערכת מבוססת על ארכיטקטורת שרת-לקוח שמבוססת על שימוש בשקעים (sockets). תקשורת מבוססת שקעים מאפשרת לתוכנה להתייחס לפקטות התקשורת כמו לקבצים. שפת ג'אווה מספקת תמיכה בתקשורת מבוססת שקעים באמצעות ספריית java.net. במערכת יש שימוש ב- Stream socket שמממש את פרוטוקול TCP. פרוטוקול זה נבחר על מנת לספק תקשורת אמינה ולהבטיח שהודעות מגיעות ליעדן.

פירוט התוכנות ב-**E-voting**

המערכת מורכבת משבע תוכנות שונות. ישנן ארבע תוכנות בצד השרת: הרשם, מנהל הבחירות, המוודא וסופר הקולות. בצד הלקוח יש שלוש תוכנות שמייצגות שלבים שונים של ההצבעה: תוכנה ראשונה אחראית על רישום המצביעים, תוכנה שנייה על רישום המועמדים ותוכנה שלישית אחראית על שלב ההצבעה. בנוסף, פותח אתר אינטרנט שמאפשר לכל המצביעים לראות את התוצאות ולבדוק שההצבעות שלהם תקינות.

7.9 סיכום

במאמר זה הוצגה מערכת הצבעה אלקטרונית שנקראת E-voting המתאימה לבחירות כלליות. קיום בחירות אלקטרוניות אמור להגדיל את שיעור ההצבעה ולהקטין את הזמן מהרגע שהסתיימו ההצבעות ועד לחשיפת התוצאה. כמו כן, הבחירות אמינות יותר משום שהציבור יכול לוודא את תוצאות הבחירות. עם זאת, ישנן מספר דרכים בהן ניתן לשפר את המערכת ואת רמת האבטחה שלה.

1. ראשית, בשלב רישום המצביעים, כאשר המערכת מייצרת זוג מפתחות למצביע, המפתח הציבורי נשמר בבסיס הנתונים של המערכת בעוד המפתח הפרטי נשלח אל המצביע באמצעות פרוטוקול דיפי הלמן ומאוחסן על דיסק או התקן אחסון חיצוני כלשהו. פתרון זה אינו מאובטח ופגיע למספר מתקפות שונות:

- קודם כל המפתח הפרטי נוצר במערכת ולא ע"י המצביע עצמו. זה אומר שאם קיים גורם כלשהו שרוצה לשבש את הבחירות ויש לו גישה למחשבי המערכת הוא יכול לזייף הצבעות משום שהוא יכול לחתום דיגיטלית הצבעה בשם כל אחד מהמצביעים.
- כמו כן, באופן כללי שליחת מפתח פרטי זו פרקטיקה לא נפוצה ונחשבת לא בטוחה בפני עצמה. מפתח פרטי אמור להישאר על המערכת בה הוא נוצר ולא להישלח על גבי הרשת.
- השימוש בדיפי הלמן על מנת לשלוח את המפתח חושף את המערכת למתקפות מסוג man in the middle, בהן גורם שלישי יכול לקבל את פקטות התקשורת ולשנות אותן או לשלוח מידע אחר לגמרי. נדגים באמצעות אליס, בוב ואיב:
  - אליס ובוב מסכימים על מספר ראשוני גדול p.
  - אליס מגרילה שורש פרימיטיבי מודולו p שנסמן ב-g.
  - אליס בוחרת מספר שלם אקראי וסודי $a \in [1, p-1]$.
  - המפתח הציבורי של אליס הוא $A = g^a \ (mod \ p)$
  - אליס שולחת לבוב את g, A
  - איב בוחרת מספר שלם אקראי וסודי $c \in [1, p-1]$
  - איב מיירטת את הפקטה שנשלחה מאליס לבוב, חוסמת את הפקטה בדרכה ובמקומה שולחת פקטה המכילה את המפתח הציבורי שלה במקום את המפתח של אליס. כלומר בוב מקבל g, C כאשר $C = g^c (mod \ p)$.
  - בוב בוחר מספר שלם אקראי וסודי $b \in [1, p-1]$
  - המפתח הציבורי של בוב הוא $B = g^b \ (mod \ p)$
  - בוב שולח לאליס את B.

- איב מיירטת גם את הפקטה הזו שנשלחת מבוב לאליס ומשנה את תוכנה ל-D במקום B.
- אליס ובוב חושבים שהמפתח המשותף ביניהם הוא $K = A^b = g^{ab} = g^{ba} = B^a \ (mod\ p)$
- בפועל, לאיב יש מפתח משותף עם כל אחד מהם g^{ac} ו-g^{bd} ויכולה ליירט ולשנות כל תקשורת ביניהם.

- ניתן במקום זאת ליישם תשתית של מפתחות ציבוריים (public key infrastructure) שתספק את הדרישה לאמת שהמפתח הציבורי אכן שייך למצביע. כלומר לפני שלב רישום המצביעים תתפרסם רשות אישורים (cerftificate authority) שיחזיק הרשם, כך שכל מצביע יכול לוודא שהוא יוצר תקשורת מאובטחת עם הרשם עצמו או עם כל גורם אחר שאושר ונחתם ע"י הרשם. בנוסף כל מצביע ייצור לעצמו זוג מפתחות, המפתח הפרטי יישמר על המחשב של המצביע והמפתח הציבורי יישלח לחתימה אצל הרשם. כך כל מי שמחזיק במפתח הציבורי של רשות האישורים יכול לסמוך על המצביע.

2. בשלב רישום המועמדים, על מנת לרשום מועמד, שני מצביעים שונים צריכים לשלוח בקשה למנהל הבחירות שכוללת את שם ומספר הזהות של המצביע שמגיש את המועמדות. בקשה זו גורמת להזדהות המצביע וחושפת כמעט בודאות למי הוא יצביע בבחירות. ניתן לחשוב על מנגנונים אחרים שמאפשרים רישום מועמדים ללא חשיפת מגישי המועמדות. לדוגמה ניתן להגיש מועמדות באופן דומה להצבעה. מצביע שרשום במערכת שולח בקשת הגשת מועמדות למוודא, הוא בודק שאכן המצביע רשום במערכת וחותם באופן עיוור על הבקשה. לאחר מכן המצביע חושף את הבקשה ושולח את הבקשה החתומה למנהל הבחירות דרך ערוץ אנונימי. כך מצב אחד ניתן לוודא שרק מצביעים רשומים יכולים להגיש מועמדות ומצד שני לא פוגעים בפרטיות המצביע.
3. כלל המצביעים נדרשים להוריד ולהתקין את התוכנה. זו דרישה שלא מתאימה לכלל האוכלוסיה וחלק ממנה עלול להתקשות עם דרישה זו. ניתן להקל על קושי זה עם מימוש תוכנות צד-הלקוח כאתר אינטרנט או אפליקציה. כך, המצביעים והמועמדים לא צריכים להוריד ולהתקין שום דבר מראש אלא רק להיכנס לאתר ביום הבחירות ולהצביע.
4. ניתן לשפר את אבטחת צד הלקוח משמעותית בעזרת אימות ביומטרי, כגון טביעת אצבע או זיהוי פנים. כך יהיה קל יותר לזהות את המשתמשים ולמנוע הצבעות מזויפות.

8. סכמת הצבעה בטוחה לחישוב תוצאות הבחירות עבור כללי הצבעה מבוססי ציון

8.1 מבוא

להצבעה אלקטרונית יש יתרונות רבים על פני הצבעה פיזית. בחירות אלקטרוניות לא דורשות מהבוחר להגיע למיקום פיזי, וכל אחד יכול להצביע מביתו או משרדו. בחירות כאלו הרבה יותר מהירות ויעילות ולא דורשות מבצע לוגיסטי על מנת להקים קלפיות ברחבי הארץ ולשכור אלפי עובדים. עקב כך, עלות מערכת בחירות אלקטרוניות נמוכה מזו של מערכת בחירות פיזית. כמו כן, טביעת הרגל הפחמנית של מערכת בחירות פיזית היא גבוהה מאוד. היא דורשת הדפסת פתקים ומעטפות בסדר גודל של מספר הבוחרים. כלומר בבחירות ארציות בארץ מודפסים עשרות מיליוני פתקים ומיליוני מעטפות בכל מערכת בחירות.

כמו כן, מאז הקורונה שפרצה ב-2020, הצורך בריחוק חברתי גדל ברחבי העולם והגעה של אלפי אנשים לקלפיות יוצרת סיכון הדבקה. שירותים ממשלתיים שבעבר פעלו רק באופן פיזי כבר עברו למערכות אלקטרוניות וגם במקרה של בחירות אין שום מגבלה טכנית שמונעת דיגיטציה של התהליך. עם זאת, באופן טבעי עולה החשש מהטיות ורמאויות. בעוד שבבחירות פיזיות קל לרמות בקנה מידה קטן, למשל שסופר קולות יכניס עוד 20 פתקים של מפלגתו, במערכת בחירות אלקטרונית האתגר הטכנולוגי גדול יותר, אבל ברגע שהתבצעה פריצה למערכת כזו ניתן לשנות את תוצאות הבחירות באופן ניכר. לכן עיקר הדיון במאמרים מסוג זה הוא בטיחות המערכת, דהיינו שלא ניתן להטות את תוצאות הבחירות, ובסודיות ההצבעה, כלומר שלא ניתן לקשר בין הצבעה לבין המצביע. אם מצביע לא יהיה בטוח שהקול שלו נשמר בסוד הוא עלול להצביע אחרת מאיך שהוא היה רוצה להצביע, או להימנע מהצבעה בכלל. לכן מטרת המערכת היא לספק סודיות מושלמת.

במאמרים אחרים בנושא מערכת הצבעה אלקטרונית כאשר מדברים על סודיות ההצבעה, הכוונה היא לאנונימיות: כלומר, כל הקולות גלויים אך לא ניתן לשייך הצבעות למצביעים שלהן. בשני המאמרים הבאים לוקחים תכונה זו צעד אחד קדימה ומספקים סודיות מושלמת, כלומר בהינתן כל קואליציית מצביעים, הפרוטוקול לא חושף שום מידע על הקול של אף מצביע מעבר למה שניתן להסיק מהתוצאות הסופיות שמתפרסמות.

אנונימיות בלבד אינה מספיקה לבדה כפי שמוסבר בשתי הדוגמאות הבאות:

1. חברי פקולטה מעוניינים לבחור בין מספר מועמדים לקבלה לפקולטה. כל חבר בפקולטה מצביע בצורה אנונימית למועמד בו הוא בחר. סופר הקולות סופר את כלל הקולות של חברי הפקולטה

ומכריז על המועמד הנבחר. למרות שבמקרה זה לא ניתן לקשר בין המצביעים לקולות, סופר הקולות רואה את כלל הקולות ולכן נחשף למידע נוסף מלבד התוצאה הסופית. מידע זה יכול להיות מידע רגיש שעלול לפגוע בסודיות המצביעים. למשל, אם סופר הקולות מגלה שמועמד א' לא קיבל כלל קולות, זה עלול להוות בעיה אם למשל היו חברי פקולטה שהתחייבו להצביע לאותו מועמד; לפיכך, הסודיות הלא מושלמת במקרה עלולה לגרום לחלק מהמועמדים להצביע בניגוד לדעותיהם ולפגוע במהימנות הבחירות. בעיה נוספת נוצרת עבור המועמדים עצמם: אם יתגלה שמועמד מסוים לא קיבל אף קול, אז זה עלול לפגוע בסיכויי המועמד למצוא משרה במוסד אחר. המערכות שמוצגות במאמרים הבאים מספקות סודיות מושלמת. על כן הן עשויות לעודד מצביעים להצביע בכנות ומועמדים להתמודד.

2. דוגמא נוספת היא LIBOR - שער הריבית להלוואות בין בנקים בעולם. הריבית מחושבת באופן יומי. כל בנק מצביע עם שער הריבית שבו הוא מעוניין וה-LIBOR מחושב כפונקציית מיצוע כלשהי על שערי הריבית השונים שנשלחו. שער הריבית שנשלח ע"י בנק מסוים יכול לאותת על היכולת של הבנק להחזיר הלוואות. לכן בנקים שחוששים שהצבעה על שער ריבית מסוים תעיד על מצב כלכלי בעייתי של הבנק, עלולים להצביע על שער ריבית שלא תורם להם. בשביל למנוע מצב כזה, ההצבעות מפורסמות רק שלושה חודשים לאחר קביעת שער ה-LIBOR. עם זאת, הגורם שמחשב את שער ה-LIBOR על בסיס כל ההצבעות נחשף לשערי הריבית (אך לא למי ששלח אותן) ועלול לקשר בין השער שנשלח לבנק באמצעות ניתוח פיננסי. לכן גם במקרה זה, למרות שההצבעות אנונימיות, סודיות המצביעים אינה מושלמת. המערכות המוצגות במאמרים שנסקור בחלק זה של העבודה יכולות לסייע גם במקרה זה כך שבנקים לא יצטרכו לבצע הצבעות אסטרטגיות.

סודיות מושלמת זו שתוארה לעיל עשויה להגדיל את הביטחון של המצביעים בסודיות הצבעתם ולעודד אותם להצביע באופן כן בהתאם להעדפותיהם האמיתיות. משום שהפרוטוקולים ממומשים בצורה יעילה ומהירה, הם מתאימים למימוש מערכות בחירות בעולם האמיתי.

לכן במאמרים בנושא של מערכות בחירות אלקטרוניות היעד העיקרי הוא מניעת חשיפת מידע על הצבעות בודדות תוך אפשור ספירת הקולות וחישוב תוצאות הבחירות הרצויות. במאמרים רבים יעד זה מושג באמצעות הצפנה הומומורפית, כלומר הצפנה שמשמרת את המבנה האלגברי ומאפשרת חישובים על המידע המוצפן. במערכות כאלה יש לרוב סופר קולות יחיד וההצבעות נשלחות אליו תחת הצפנה הומומורפית, כך שסופר הקולות לא יוכל לדעת את תוכנן אך עדיין יוכל לבצע עליהן את החישובים הנחוצים בצורתן המוצפנת. עם זאת, להצפנה הומומורפית יש עלויות חישוב גבוהות. בשני המאמרים

הבאים הרעיון הוא להשתמש במספר סופרי קולות, פיצול כל קול למספר חלקים ולבצע את ספירת הקולות באופן מבוזר. כך ניתן להחליף את מרכיב ההצפנה ההומורפית, המספקת את הסודיות הרצויה, בפרוטוקול שיתוף סודות שעלויותיו נמוכות בהרבה. הרעיון הוא להשתמש במספר סופרי הקולות (בניגוד לסופר קולות משתתפים בחישוב מרובה משתתפים מאובטח שמאפשר להם לוודא כל הצבעה ואז לחשב את התוצאה המצטברת. כל זאת מבלי להיחשף אפילו לקול אחד.

במאמר הראשון מוצגת מערכת הצבעות מאובטחת עם סודיות מושלמת לחישוב תוצאות בחירות מבוססות ציון. בחירות מבוססות ציון הן משפחה של חוקים שבהם כל מצביע נותן לכל אחד מהמועמדים ציון, על סמך חוקיות מסוימת. המנצח הוא המועמד שסכום הציונים שקיבל מכל המצביעים הוא הגבוה ביותר. בחירות מבוססות ציון כוללות את השיטות רוב (Plurality), טווח (Range), הסכמה (Approval), וטו (Veto) ובורדה (Borda).
הפרוטוקול מסתמך על קבוצה של סופרי קולות המבצעים את הסכימה של ציון המועמדים, אך הם אינם רשאים לגשת לקולות עצמם או לשום תוצאה מלבד תוצאת הבחירות הסופית שהם נדרשים לחשב (המועמד הזוכה, או המועמדים הזוכים, או דירוג של המועמדים לפי ציוניהם, בהתאם לדרישות הישום). הפרוטוקול מאובטח תחת ההנחה שלסופרי הקולות יש רוב הגון. כלומר אם רוב סופרי הקולות הגונים ואינם קושרים קשר אז אף אחד מסופרי הקולות (ההגונים והלא הגונים אם יש כאלה) אינו יכול להסיק שום דבר על הקולות, על התוצאות החלקיות או על ציון המועמדים הסופי.

המאמר השני עוסק בחוקי הצבעה מבוססי סדר. במשפחת חוקים זו כל מצביע שולח מטריצת הצבעה שמכילה השוואה בין כל זוג מועמדים. כלומר בכל תא במטריצה מצוין האם המצביע מעדיף את מועמד א' או את מועמד ב'. סופרי הקולות מחברים את המטריצות המתקבלות מכלל המצביעים והמנצח הוא המועמד שסכום הדירוגים שלו הוא הגבוה ביותר.
בפרט המאמר השני מתמקד בשני חוקים - קופלנד (Copeland) וקרמר-סימפסון (Kramer Simpson) שנקרא גם חוק Maximin. מתוארים שני חוקים נוספים בהמשך, קמני-יונג (Kemeny-Young) ודירוג מודאלי (Modal rnaking) ומתואר כיצד ניתן להרחיב את המערכת לחוקים אלו. הפלט של הפרוטוקול הוא המועמדים המנצחים המסודרים לפי הדירוג שלהם בסיכום כלל ההצבעות.

העקרונות הקריפטוגרפיים של הפרוטוקולים
בבסיס שני הפרוטוקולים ישנה קבוצה של סופרי קולות שתסומן $\{T_1, \ldots, T_D\}$ וקבוצת מצביעים שתסומן $\{V_1, \ldots, V_n\}$. כל מצביע מייצר וקטור או מטריצת הצבעה, המתארים את הצבעתו, ואז הם מבצעים

עליהם את סכמת שיתוף הסודות של שמיר, על כל איבר בוקטור או מטריצה בנפרד, ומפיצים את חלקי הסוד המתקבלים לסופרי הקולות. הסכמה שמופעלת היא D'-out-of-D.
כך ש- $D' = \lfloor (D+1)/2 \rfloor$. בחירה זו מכתיבה שרק במקרה ורוב סופרי הקולות יקשרו קשר על מנת לחשוף את ההצבעות אז הסודיות תיפגע. מקרה זה מאוד לא סביר משום שאנחנו מניחים שקיים רוב הגון של סופרי קולות. כל קשירת קשר של פחות מחצי מסופרי הקולות לא תניב שום מידע על אף הצבעה. ערכי D גבוהים יותר יגבירו את אבטחת הפרוטוקול ע"י הפיכת קשירת קשר לאירוע פחות סביר אבל מצד שני יגררו עלויות חישוב ותקשורת גבוהות יותר.

בתחילת התהליך סופרי הקולות מקבלים את חלקי הסוד מהמצביעים וצריכים לוודא שההצבעות תקינות מבלי להיחשף אליהן. בסוף התהליך סופרי הקולות מבצעים השוואה מאובטחת על הציון המצטבר של כל מועמד על מנת למצוא את K המועמדים עם הציון הגבוה ביותר. על מנת לבצע זאת מבלי לחשוף את ההצבעות עצמן, סופרי הקולות צריכים לבצע חישוב מרובה משתתפים על מנת לחשב את ארבע הפונקציות הבאות. נניח ש- $x_1, x_2, \ldots, x_L$ הם ערכים סודיים בהם מחזיקים סופרי הקולות חלקי סוד, בסכמת D'-out-of-D של שמיר. אז עליהם לחשב את הערכים הבאים, מבלי לשחזר את $x_1, x_2, \ldots, x_L$:

3. פונקציות אריתמטיות $y = f(x_1, \ldots, x_L)$.
4. אם הפונקציה $y = 1_{x_1 < x_2}$ היא פונקציה שמחזירה 1 אם $x_1 < x_2$ ו-0 אחרת, חשב את פרוצדורת הבנייה מחדש בסכמת שיתוף הסודות של שמיר על y.
5. אם $p > 2N$ כאשר N הוא מספר המצביעים ו-$x_1 \in [-N, N]$, חשב את פרוצדורת הבנייה מחדש בסכמת שיתוף הסודות של שמיר על $1_{x_1 > 0}$.
6. אם $p > 2N$ כאשר N הוא מספר המצביעים ו-$x_1 \in [-N, N]$, חשב את פרוצדורת הבנייה מחדש בסכמת שיתוף הסודות של שמיר על $1_{x_1 = 0}$.

חישוב פונקציות אריתמטיות

ניתן לחשב פונקציות מהסוג $f(x_1, \ldots, x_L)$ עם L משתנים, בעזרת מעגל אריתמטי C, שמורכב משערי חיבור ושערי כפל. המעגל מקבל כקלט את כל L המשתנים ומחשב באמצעותם ובאמצעות שערי חיבור וכפל את הפונקציה הרצויה. לסופרי הקולות יש D' חלקי סוד מתוך D בכל אחד מהקלטים האלו אבל הם אינם רשאים להשתמש בפרוצדורת השחזור על מנת לחשב אותם. האתגר בחישוב המעגל הוא לחשב את פונקציית המעגל מבלי לחשב כל אחד מהקלטים או מתוצאות הביניים של הפונקציה. כלומר, בהינתן D' חלקי סוד מתוך D חלקי סוד בסכמת שיתוף הסודות של שמיר על שני משתנים $u, v \in Z_p$, יש לחשב D' חלקי סוד מתוך D ב-$u + v$ וב-$u \cdot v$ מבלי לבנות מחדש את הסודות $u, v, u + v, u \cdot v$

יהיו u_d , v_d חלקי סוד שבידי סופר הקולות $T_d , d \in [D]$ בשני הקלטים u, v בהתאמה. חישוב צירוף ליניארי $au + bv$ יתבצע ע"י הכפלה של חלקי הסוד בקבועים: au_d , bv_d וחיבורם יחד $au_d + bv_d$ מקומית וללא אינטרקציה עם אף סופר קולות נוסף. זאת משום ששיתוף סודות הוא ליניארי וחיבור חלקי הסוד הוא חלק סוד בעצמו בסכמת שיתוף סודות על $au + bv$ כאשר $a, b \in Z_p$. לכן ניתן לחבר ולכפול את המשתנים מקומית והערך יתקבל בסוף החישוב (פעם אחת בלבד) כאשר סופרי הקולות ישתפו את חלקי הסוד ביניהם.

בניגוד להכפלה בקבוע, ביצוע כפל בין חלקי סוד הוא מורכב יותר משום שעל מנת לחשב $u \cdot v$ סופרי הקולות צריכים להחליף ביניהם את חלקי הסודות השונים. לכן המדידה של מעגלים אריתמטיים תתבסס על מספר שערי הכפל במעגל (משום שאלו דורשים חישוב ותקשורת) ומספר השכבות במעגל (משום שלא ניתן למקבל חישובים בשכבות שונות).

השוואה מאובטחת

נניח $T_1 , \ldots , T_D$ מחזיקים D' חלקי סוד מתוך D בשני מספרים שלמים $x_1, x_2 < p$ (בשדה Z_p).

פרוטוקול מאובטח הוא פרוטוקול המאפשר לסופרי הקולות לחשב D' חלקי סוד מתוך D על $1_{x_1<x_2}$ מבלי לדעת את ערכי x_1, x_2

במאמר [NO07] של נישיד (Nishide) ואוטה (Ohta) מוצגת שיטה להשוואה מאובטחת שמבוססת על עיקרון פשוט. נסמן את הביטים $1_{x_1<x_2}$, $1_{[(x_1-x_2)\ mod p]<p/2}$, $1_{x_2<p/2}$, $1_{x_1<p/2}$ במשתנים w, x, y, z בהתאמה.

ואז מתקיים: $z = w\underline{x} \vee \underline{w}\ \underline{x}\ \underline{y} \vee wx\underline{y}$

ניתן לאמת את התוצאה לפי טבלת האמת הבאה:

w	x	y	z
T	F	*	T
F	T	*	F
F	F	F	T
F	F	T	F

T	T	F	T
T	T	T	F

על מנת להזין את המשוואה הלוגית למעגל אריתמטי נתרגם את הביטוי לביטוי אריתמטי שקול:

$z = w(1-x) + (1-w)(1-x)(1-y) + wx(1-y) = 1 - x - y + xy + w(x + y - 2xy)$

כך ניתן להמיר את בעיית השוואת x_1 ל-x_2 למעגל אריתמטי. אנחנו טוענים שהמעגל האריתמטי הנ"ל קל לחישוב בעזרת הלמה הבאה:

בהינתן שדה סופי Z_p ואלמנט בשדה $q \in Z_p$ אז $q < p/2$ אם ורק אם הביט הימני ביותר של $(2q \ mod \ p)$ הוא 0.

הוכחה:

- אם $q < p/2$ אז $2q < p$ ולכן $2q \ mod \ p = 2q$, משום ש-$2q$ זוגי הביט הימני ביותר שלו הוא 0.
- אם $q > p/2$ אז $2q > p$ ולכן $2q \ mod \ p = 2q - p$ משום ש-p ראשוני הוא אי זוגי ולכן התוצאה גם אי זוגית והביט הימני ביותר הוא 1.

בעזרת למה זו סופרי הקולות יכולים לחשב D' חלקי סוד מתוך D ב-w באופן הבא: כל T_d יתרגם את חלק הסוד שלו ב-x_1 לחלק סוד ב-$2 \cdot x_1$ ע"י הכפלת חלק הסוד ב-2 ואז כל סופרי הקולות יחשבו D' חלקי סוד מתוך D על הביט הימני ביותר של $2 \cdot x_1$. באותו אופן ניתן לשתף את הביט הימני ביותר של $2 \cdot x_2$ ולחשב את w,x,y ולהשוות בין x_1 ל-x_2 מבלי לדעת את ערכם.

חישוב חלקי סוד על הביט הימני ביותר לוקח 13 סיבובים של תקשורת ו- $93log_2p + 1$ פעולות כפל.

נדרשים $279log_2p + 3$ לחישוב שלושת הביטים ובסך הכל בשביל לחשב את הביטוי $1 - x - y + xy + w(x + y - 2xy)$ נדרשים 15 סיבובים ו $279log_2p + 5$ פעולות כפל.

בדיקה מאובטחת של חיוביות

יהי $x \in Z_p$ מספר שלם בטווח $[-N, N]$ ומתקיים $p > 2N$ ואנחנו רוצים לבדוק האם הוא חיובי או שלילי מבלי לחשוף את סופרי הקולות לערכו, כלומר אנחנו רוצים שלסופרי הקולות יהיו D' חלקי סוד מתוך D על $1_{x>0}$. דרך אחת לבצע זאת היא ליצור משתנה $y = x + N$ ולהשתמש בשיטה שהוצגה בסעיף "השוואה מאובטחת". כלומר להציב $x_1 = N, x_2 = y$ ולהשוות ביניהם. עם זאת, יש דרך יעילה יותר בעזרת הלמה הבאה:

נניח $T_1, \ldots, T_D$ מחזיקים D' חלקי סוד מתוך D ב-$x \in Z_p$ ומתקיימים $x \in [-N, N]$, $p > 2N$
אז $x > 0$ אם ורק אם הביט הימני ביותר של $(-2x \ mod \ p)$ הוא 1.
הוכחה:

- אם $x > 0$ אז $-2x \in [-2N,)$ ומשום ש-$p > 2N$ מתקיים $(-2x \ mod \ p) = -2x + p$ כלומר מספר חיובי אי זוגי ולכן הביט הימני ביותר שלו הוא 1.
- אם $x < 0$ אז $-2x \in [0,2N]$ אז מתקיים $(-2x \ mod \ p) = -2x$ משום שמספר זה חיובי הביט הימני ביותר שלו הוא 0.

כפי שהראנו בדיקת חיוביות דורשת העברה של ביט יחיד ולכן עלויות החישוב הן 13 סיבובי תקשורת ו-$93log_2 p + 1$ פעולות כפל.

בדיקה מאובטחת של שוויון לאפס
בשביל לבדוק האם מספר שלם כלשהו $x \in [-N, N]$ שווה לאפס מבלי לחשוף את ערכו, ניתן להשתמש בבדיקת החיוביות לעיל פעמיים, פעם אחת ל-x ופעם נוספת ל-$-x$ ואם התוצאה תהיה 0 בשתי הפעמים נדע בודאות ש- $x = 0$.
אבל גם כאן יש דרך יעילה יותר בעזרת "המשפט הקטן של פרמה" (Fermat's little thoerem).
המשפט טוען שאם $x \in Z_p \backslash \{0\}$ אז $x^{p-1} = 1 \ mod \ p$. נשכתב את אותה הלוגיקה $1_{x \neq 0} = (x^{p-1} \ mod \ p)$.
כלומר ניתן ליצור חלקי סוד ב-$1_{x \neq 0}$ ע"י חישוב $x^{p-1} \ mod \ p$. ניתן לחשב את הביטוי האחרון ע"י אלגוריתם square and mulitply בו מייצגים את החזקה כמספר בינארי ומבצעים ריבוע או כפל בהתאים לכל ספרה בינארית. חישוב זה לוקח לא יותר מ-$2log_2 p$ פעולות כפל (לא מקבילות) ו-13 סיבובי תקשורת.
משום שניתן להמיר חלקי סוד מ-$1_{x \neq 0}$ לחלקי סוד ב-$1_{x=0}$ בקלות באופן הבא $1_{x=0} = 1 - 1_{x \neq 0}$ עלויות החישוב נמוכות בהרבה מאשר ביצוע שתי בדיקות לחיוביות.

8.2 מאמרים קודמים בנושא

מחקרים קודמים על בחירות מאובטחות התמקדו בתכונות אחרות, למשל אנונימיות המצביע - לא ניתן לקשר בין הקול למצביע, ייחודיות ההצבעה - כל מצביע יכול להצביע פעם אחת בלבד, נכונות - המועמד המנצח הוא זה שקיבל את התוצאה הכי גבוהה לפי סט החוקים שנבחר לבחירות אלו והוגנות - על המצביעים להצביע ללא ידע על הצבעות אחרות או תוצאות חלקיות של הבחירות.

מאמר זה מתמקד בשימור הפרטיות והשגת סודיות מושלמת. דרך אחת להשיג סודיות מושלמת היא לאפשר למצביעים לספור את הקולות בעצמם מבלי להסתמך על סופרי קולות [Cha88]. דרך נוספת היא להשתמש בגורם צד שלישי, כלומר סופר קולות. על מנת להעביר את הקולות מהמצביעים אל סופר הקולות בצורה מאובטחת מאמרים קודמים השתמשו בשלל טכניקות מתחום הקריפטוגרפיה.

מאמרים מוקדמים השתמשו בערוצים אנונימיים ומערבלים [Ben86,CL06,FSS+17], פרוטוקולים אחרים להצבעות מאובטחות השתמשו בחתימה עיוורת [NO07], מאמר נוסף [CGS97] הציע מערכת בחירות מאובטחת באמצעות בעיית הלוגריתם הדיסקרטי. במאמר [CL06] של בנלו (Benaloh) הציע סכמת בחירות שבה תוצאת הבחירות ניתנת לוידוא ע"י כל אחד ממשתתפי הפרוטוקול ואפילו צופים מן הצד. הסכמה מבוססת על שיתוף סודות משמר צורה (homomorphic) שמאפשר חישובים על מידע משותף [[BE15]

מחקרים רבים השתמשו בהצפנה משמרת צורה (homomorphic encryption) משום שהיא מאפשרת צבירה של הקולות בעודם מוצפנים. לדוגמה, קריימר (Cramer) ואחרים [Ben87] הציעו סכמה שבה כל מצביע שולח קול אחד מוצפן. בעזרת ההצפנה משמרת הצורה, כל אחד יכול לוודא את התוצאה הסופית. דאמגארד (Damgård) ואחרים [CPS+18] הציעו הכללה למערכת המפתח הציבורי ההסתברותית של פיליר [Kra77] ואז הראו איך ניתן להשתמש בה ביצירת מערכת הצבעות אלקטרונית יעילה. בעוד רוב המערכות להצבעה אלקטרונית המשתמשות בהצפנה משמרת צורה מבוססות על שימור צורה חיבורי, פנג (Peng) ואחרים [Pai99] הציעו סכמה המבוססת על שימור צורה כפלי. בסכמה זו סופר הקולות מקבל את המכפלה של כל הקולות במקום את סכומם ואז הוא מבצע פירוק לגורמים על מנת להסיק את התוצאה.

רק שני מאמרים קודמים חשבו על הרעיון של חישוב חוקי הצבעה מבוססי ציון בצורה פרטית. קנארד [Cha81] ואחרים כתבו על חוק "הרוב קובע" (majority judgement), שלא נכלל במשפחת חוקי ההצבעה מבוססי הציון. נאיר ואחרים [CCJ+14] הציעו להשתמש בשיתוף סודות (secret sharing) לחישוב תוצאות בחירות בשיטת הרוב (plurality) אך השיטה לא מספקת סודיות מושלמת משום שתוצאת כל מועמד נחשפות בתהליך. כמו כן, הפרוטוקול שהציעו חשוף לרמאות משום שאינו מספק אף

מנגנון לגילוי הצבעות מזויפות. במאמר זה, שמאפשר שימוש בכלל חוקי ההצבעה מבוססי הציון, מובטחת סודיות מושלמת ואמצעים למניעת רמאויות באמצעות חישוב מרובה משתתפים ושיתוף סודות.
קוסטרס (Kusters) ואחרים [KLM+20] הציגו מערכת הצבעות שמשמרת את סודיות ההצבעות ומאובטחת מקצה לקצה. המערכת שנקראת Ordinos מממשת את חוק הרוב ומחשבת את K המועמדים הזוכים או K המועמדים שעברו סף מסוים של קולות.
בנושא חוקי הצבעה מבוססי סדר, ישנן מספר מאמרים חדשים יחסית. היינס (Heines) ואחרים [HPT20] הציעו פתרון לחישוב מאובטח של חוק שולזה (Schulze). הפתרון שלהם לא מגן על אנונימיות המשתמשים באופן מושלם ואינו מתאים לכל תרחיש בחירות בשל זמן הוידוא הארוך של כמות מצביעים קטנה יחסית.
הרטל (Hertel) ואחרים [HHK+21] הציעו פתרונות לחוקי קופלנד, מקסימין ושולזה. חישוב התוצאות לקח למעלה משבוע ל-20 מועמדים ולכן גם הוא אינו מתאים לתרחיש בחירות מציאותי. כמו כן, המערכת במאמר של קורטייר (Cortier) ואחרים [CGY22] לוקחת מספר שעות לוודא 1024 הצבעות עם 20 מועמדים.
המאמרים המוצגים בעבודה זו הם המאמרים היחידים שמציעים מערכות לחישוב חוקים מבוססי ציון וחוקים מבוססי סדר בצורה מאובטחת, מהירה ומתאימה לתרחיש בחירות בו יש מספר רב של מועמדים ומיליוני מצביעים. וידוא של מיליון מצביעים בבחירות עם 20 מועמדים תיקח מספר דקות בודדות לעומת שעות או ימים במאמרים אחרים.

8.3 כללי הצבעה מבוססי ציון

במודל שבו יש N מצביעים $V = \{V_1, \ldots, V_N\}$ שמקיימים בחירות בין M מועמדים $C = \{C_1, \ldots, C_M\}$ הבחירות קובעות ציון $w(m)$ לכל מועמד C_m כאשר $m \in [M] := \{1, \ldots, M\}$ באופן הבא. יהי $K \in [M]$ פרמטר אז כל אלגוריתם הצבעה מבוסס ציון יחזיר את K המועמדים עם הציון w הכי גבוה. אם K=1 אז המודל מתאים לבחירות רגילות בהן יש מנצח יחיד מתוך המועמדים. אפשר להרחיב את הפרוטוקול כך שיחזיר דירוג של המועמדים לפי התוצאה הסופית של כל מועמד. עם זאת המשך המאמר מתמקד בהחזרת K המועמדים הראשונים.
כל מצביע V_n מייצר וקטור הצבעה $w_n := (w_n(1), \ldots, w_n(M))$ כך שכל הצבעה בודדת $w_n(m)$ היא אי-שלילית וחסומות מלמעלה באופן אחיד. התוצאה המצטברת w_n היא הציון של מועמד כלשהו C_m.
המאמר מתרכז בחמשת חוקי ההצבעה מבוססי-ציון הבאים:

1. Plurality (רוב) - $w_n \in \{e_1, \ldots, e_m\}$ כאשר כל e_m הוא וקטור בינארי ממימד M שבו האיבר ה-m הוא 1 וכל שאר האיברים הם 0. כאשר המיקום של ה-1 מתאים לאינדקס של המועמד. המנצח a הוא המועמד עם הניקוד המצטבר הגבוה ביותר.
2. Range (טווח) - $w_n \in \{0,1, \ldots, L\}^M$ למספר L ציבורי כלשהו. כל מצביע נותן ציון בין 0 ל-L לכל מועמד והמועמד עם התוצאה המצטברת הגבוהה ביותר הוא המנצח.
3. Approval (הסכמה) - $w_n \in \{0,1\}^M$. כל מצביע שולח וקטור בינארי שבו עד K איברים הם 1 והשאר הם 0.
4. Veto (וטו) - $w_n \in \{\hat{e}_1, \ldots, \hat{e}_M\}$ הוא וקטור בינארי שבו יש איבר יחיד ששווה ל-0 וכל שאר האיברים שווים ל-1. בשיטה זו כל מצביע מציין מי המועמד הכי פחות מועדף עליו והמנצח הוא המועמד שקיבל הכי פחות הצבעות אפס.
5. Borda (בורדה) - $w_n \in \{(\pi(0), \ldots, \pi(M-1)) : \pi \in \Pi_M\}$ כאשר Π_M היא קבוצת כל הפרמוטציות האפשריות מעל $\{0, \ldots, M-1\}$. בשיטה זו כל מצביע שולח את סידור המועמדים המועדף עליו, כאשר המועמד הכי פחות רצוי לפי דעתו של המצביע, יקבל את הציון 0 והמועמד המועדף יקבל את הציון M-1. המנצח הוא המועמד שסכום הציונים שלו הוא הגבוה ביותר.

8.4 פרוטוקול מאובטח לחוקי הצבעה מבוססי ציון

הפרוטוקול מבוסס על קבוצה של סופרי קולות $T = \{T_1, \ldots, T_D\}$ שמבצעים את חישוב התוצאה אך אינם נחשפים לקולות עצמם. מספר סופרי הקולות D יכול להיות כל מספר גדול מ-2. ערכים גבוהים יותר של D יגררו עלויות תקשורת וחישוב גבוהות יותר אך ישפרו את האבטחה ויפחיתו את הסיכוי לקשירת קשר בין סופרי קולות לא הגונים.

לפני שנציג את הפרוטוקול יש לשים לב לשתי אבחנות. ראשית p הוא מספר ראשוני הגדול יותר מכל המספרים שאפשר להגיע אליהם בחישובים, אז כלל החישובים בפרוטוקול מחושבים בשדה Z_p .

האבחנה השנייה היא שיש חסם עליון B שמקיים $B < p$, על ערכי w בחמשת כללי ההצבעה שתיארנו בסעיף "כללי הצבעה מבוססי ציון". בכללי ההצבעה רוב, הסכמה ווטו מתקיים $B = N$. בבורדה מתקיים $B = NM$. ובטווח מתקיים $B = NL$.

בשלב הראשון כל מצביע V_n יוצר וקטור הצבעה $w_n \in (Z_p)^M$ תחת ההנחה שכל מצביע יודע את האינדקס של כל מועמד. לדוגמא, ניתן לסדר את המועמדים לקסיקוגרפית לפי שם המשפחה.

בשלב השני המצביע יוצר D חלקים רנדומליים מתוך וקטור ההצבעה שיצר בעזרת הסכמה של שמיר כאשר $D' = \lfloor (D+1)/2 \rfloor$. המצביע מבצע את פרוצדורת השיתוף לכל איבר בוקטור בנפרד. כלומר

לכל $m \in [M]$, המצביע V_n יוצר פולינום רנדומלי $g_{n,m}$ מדרגה $D' - 1$ מעל השדה Z_p שמקיים $g_{n,m}(0) = w_n(m)$.

בשלב השלישי המצביע V_n שולח לכל סופר קולות T_d את הוקטור $w_{n,d} = (g_{n,1}(d), \ldots, g_{n,M}(d))$ לכל $d \in [D]$.

בשלב הרביעי לאחר שקיבל את חלקי הסוד שנוצרו מקולות כל המצביעים, סופר הקולות T_d מחשב את הסכום של כל הוקטורים $w_{n,d}$ $\widehat{w_d} = \sum_{n=1}^{N}$. כל וקטור כזה לא חושף שום מידע על תוכן הקולות משום שהוא סכום של חלקים רנדומליים של הצבעות שונות. אבל משום שכל חלק נוצר בעזרת פרוצדורת השיתוף של שמיר, ובגלל הליניאריות של הפרוצדורות שהוזכרה בסעיף הקודם, הקבוצה : $\{\widehat{w_d}(m)$ $d \in [D]\}$ היא קבוצה של D חלקים בסכמת שיתוף הסודות של שמיר. כלומר, לכל $m \in [M]$ קיים פולינום g_m מדרגה $D' - 1$ מעל שדה Z_p שמקיים $g_m(0) = w(m)$ ו- $g_m(d) = \widehat{w_d}(m)$ לכל $d \in [D]$ כלומר אם נציב 0 בפולינום נקבל את הציון המצטבר של המועמד m.

בשלב החמישי והחשוב ביותר, כל סופרי הקולות מבצעים חישוב מרובה משתתפים מאובטח (MPC - multiparty computation) על מנת למצוא את K המועמדים עם הציון המצטבר הגבוה ביותר. החישוב מרובה המשתתפים הוא תהליך מורכב והוא יפורט בסעיף הבא.

בשלב השישי והאחרון, סופרי הקולות מפרסמים את K האינדקסים המובילים וכלל המצביעים יכולים לתרגם את האינדקסים בחזרה לשמות המועמדים ולמצוא את המנצחים.

מיון וקטורים משותפים

האתגר העיקרי בשלב חמש בפרוטוקול הוא למצוא את K האינדקסים עם הציון המצטבר הגבוה ביותר. סופרי הקולות צריכים למיין את w על מנת למצוא את K האינדקסים עם הציון הגבוה ביותר אבל הם אינם יכולים לבנות מחדש את ההצבעות המקוריות או להסיק שום מידע נוסף עליהן. לכן הם צריכים לבצע השוואות מבלי לדעת שום דבר על הוקטורים אותם הם ממיינים, וזאת רק באמצעות חלקי הסוד שיש בידם.

יהיו שני ערכי וקטורים שצריך להשוות ביניהם $u = w(m)$ ו- $v = w(m')$ לשני אינדקסים שונים $m, m' \in [M]$. כל סופר קולות $T_d, d \in [D]$, מחזיק חלקי סוד $u_d, v_d \in Z_p$ ב-u ו-v בהתאמה, בסכמת שיתוף הסודות של שמיר. סופרי הקולות רוצים לדעת האם $u < v$, אבל לעשות זאת מבלי לחשוף שום מידע נוסף על u ו-v.

בשביל לוודא שאילתות מהסוג הנ"ל, משתמשים בחישוב מרובה משתתפים מאובטח (MPC). פרוטוקולי MPC מאפשרים למשתתפים $T_1, \ldots, T_D$ לחשב כל פונקציה f על קלטים פרטיים $x_1, \ldots, x_D$ שכל אחד מהם מחזיק בהתאמה כך שבסוף החישוב כל אחד מהמשתתפים יודע את התוצאה של $f(x_1, \ldots, x_D)$ אבל שום דבר אחר.

גישה מקובלת ליצירת פרוטוקול MPC יעיל היא לייצג כל פונרציה f כמעגל אריתמטי C כך שלכל קבוצה של קלטים $x_1,\ldots,x_D$ הפלט של המעגל $C(x_1,\ldots,x_D)$ שווה $f(x_1,\ldots,x_D)$.
המעגל מורכב משערי קלט ופלט כך שלכל שער קלט מוזן ערך סודי יחיד ע"י אחד המשתתפים, וכל שער פלט מניב ערך יחיד שנחשף לכלל המשתתפים. בנוסף, בין שער הקלט לשער הפלט יש מספר שכבות של שערים אריתמטיים שמחברים ביניהם. שער הקלט הוא השכבה הראשונה ושער הפלט הוא השכבה האחרונה. שער אריתמטי יכול להיות שער חיבור או שער כפל. לכל שער אריתמטי מוזנים בדיוק שני קלטים והוא מניב פלט יחיד אך הפלט הזה יכול לשמש כקלט לשערים מרובים בשכבה הבאה. רק הערך של שער הפלט נחשף לכלל המשתתפים. שאר הערכים שעוברים בין שער אחד לאחר נשארים סודיים ולא מתגלים לאף אחד מהמשתתפים. בפרט האלגוריתם שמאפשר את זה מפורט בסעיף "שיתוף סודות". תכונה זו מתאפשרת בזכות ליניאריות הפרוצדרות לשיתוף סודות. לכן אפשר לסכום ולהכפיל מבלי להיחשף לערכים המקוריים. כאשר מחשבים את שער הפלט, כל המשתתפים שולחים את החלק שלהם בסוד כך שכולם יוכלו לבנות מחדש את הקלט.

עלויות החישוב והתקשורת של חישוב מעגלים תלויות בעיקר במספר שערי הכפל ומספר השכבות במעגל. זאת משום שחישוב של שער כפל עם שני קלטים דורש תקשורת בין משתתפים שצריכים לשלוח אחד לשני מידע על קלטים אלו. לעומת זאת חישוב של שער חיבור או שער כפל עם משתנה אחד וקבוע לא דורשים תקשורת בין המשתתפים אלא מחושבים מקומית בלבד. לכן יעילות החישוב תלויה בעיקר במספר שערי הכפל ומספר השכבות במעגל, בעיקר משום שהשערים תלויים אחד בשני ולא ניתן למקבל חישוב של שערי כפל משכבות שונות.
במאמר זה יש שימוש בעיצוב מעגלים אריתמטיים כפי שמתואר במאמר [BS05] של נישיד (Nishide) ואוטה (Ohta) בו יש שימוש בהשוואת שני סודות $u,v \in Z_p$ בחישוב מרובה משתתפים.
מניחים שלכל אחד מהמשתתפים יש חלק בסוד לפי סכמת שיתוף הסודות של שמיר כאשר $D' = \lfloor (D+1)/2 \rfloor$. המעגל מניב את הביט שמציין האם $u < v$. עומק המעגל אינו תלוי במספר המשתתפים או בגודל השדה p. למעשה הוא קבוע ולכן לשינוי פרמטרים אלה אין הרבה השפעה על זמן הריצה של המעגל.

8.5 אבטחת הפרוטוקול

בחלק זה נדון באבטחת הפרוטוקול כולו. יעד חשוב של הצבעה מאובטחת הוא אנונימיות המצביעים. כלומר אף יישות לא יכולה לקשר בין הצבעה לבין המצביע. הפרוטוקול משיג זאת באמצעות חלוקת כל הצבעה ל-D חלקים ושליחת כל אחד מהם לסופר קולות שונה. כל חלק סוד בפני עצמו לא מכיל שום

מידע על ההצבעה ואפילו תתי קבוצות של $D' - 1$ חלקים (או פחות) לא חושפות שום מידע על ההצבעה. הנחת העבודה במקרה זה היא שמתקיים רוב הגון - רוב סופרי הקולות הגונים, וגם אם יש כאלו שאינם הגונים מספרם קטן ממספר סופרי הקולות ההגונים. משום שכל קול מחולק ל-$D' = \lfloor (D + 1)/2 \rfloor$ חלקי סוד בסכמת שיתוף הסודות של שמיר, אז מספר סופרי הקולות הלא הגונים שצריכים לקשור קשר הוא $D' \geq D/2$ ומקרה זה לא אפשרי תחת ההנחה שרוב סופרי הקולות הגונים. לכן תחת הנחה זו, סופרי הקולות לא יכולים להסיק שום דבר על הקולות עצמם.

לגבי שלב 5, בו מתבצע החישוב מרובה המשתתפים (MPC), הסודיות שלו מוכחת ב- [BS05]. ע"י שימוש בפרוטוקול MPC סופרי הקולות נחשפים רק ל-K אינדקסים המנצחים מבלי להיחשף לשום מידע בזמן חישוב המעגל. בשל השימוש בסכמת שיתוף הסודות של שמיר, גם חישוב המעגל בשלב 5 שומר על סודיות ההצבעות תחת הנחת הרוב ההגון.

לסיכום, אנונימיות המצביעים נשמרת ע"י הפרוטוקול אלא אם כן יותר מ-$D' = \lfloor (D + 1)/2 \rfloor$ קושרים קשר ומשתפים פעולה על מנת לחשוף את תוכן ההצבעות. לדוגמא כאשר $D = 3$ לפחות שני סופרי קולות צריכים לשתף פעולה בשביל לחשוף את ההצבעות. באותו אופן כאשר $D = 5$ נדרשים לפחות שלושה סופרי קולות בשביל לקשור קשר. אם רוב כזה לא מתקיים אז יהיה ניתן לחשב רק את K המועמדים המנצחים מבלי לחשוף מידע נוסף.

מקרה של קשירת קשר הוא לא סביר משום שהוא דורש רוב לא הגון. כמו כן, ההסתברות שתרחיש כזה יקרה יורד ככל שהערך של D עולה. באופן אידיאלי, סופרי הקולות יהיו אנשים או גופים עם מוניטין חיובי שזוכים לאמון רב בתוך הארגון או הממשלה בה הם נמצאים. בגידה באמון זה הניתן להם, תגרור פגיעה קשה למוניטין שלהם, לעסק שלהם או תגרור ענישה משמעותית. לכן אפילו לערך D נמוך של 5 למשל, הסיכוי ששלושה סופרי קולות יפרו אמונים הוא קלוש וזניח.

מכאן שיש פה פשרה. מצד אחד ערכי D גבוהים יפחיתו את הסיכוי לקשירת קשר ופגיעה בפרטיות, מצד שני ערכי D גבוהים יגרמו לעלויות תקשורת גבוהות יותר.

מתקפה אפשרית נוספת היא שמצביע V_j יצוטט לתקשורת היוצאת ממנו אל סופרי הקולות ויחליף את w_n בהצבעה מזויפת w_j. אפשר למנוע מתקפה זו בקלות ע"י הוספת דרישה שכל תקשורת בין מצביעים לסופרי קולות תתבצע באופן מוצפן עם מפתח ציבורי הידוע לשני הצדדים ותהיה חתומה עם מפתח פרטי. בכל קבלה של הודעה יצטרך המקבל לוודא שההודעה שנשלחה נחתמה עם המפתח הפרטי המתאים. כלומר כל הודעה שנשלחת מהמצביע V_n לסופר הקולות T_d בשלב 3 של הפרוטוקול תצטרך להיות חתומה עם המפתח הפרטי של V_n ואז מוצפנת עם המפתח הציבורי של T_d. בנוסף, אפשר לדרוש שכל סופר קולות ישלח אישור קבלה על כל הצבעה שנשלחה אליו.

הנחה יסודית בכל מערכות הבחירות האלקטרוניות המאובטחות היא שניתן לסמוך על סופרי הקולות שמקבלים את הצבעות המצביעים, שאינם עושים בהן שום שימוש לרעה וששומרים עליהן בסוד. בניגוד

לרוב מערכות הבחירות הקיימות, פרוטוקול זה מפחית באופן משמעותי את הצורך לסמוך על סופרי קולות משום שאין להם גישה להצבעות עצמן. אפילו במקרה ומיעוט כלשהו מסופרי הקולות מפר את האמון שניתן בהם, פרטיות המצביעים והקולות נשמרת. הפחתה זו באמון הנדרש בסופרי הקולות היא הכרחית על מנת להעלות את ביטחון המצביעים ולעודד אותם להצביע באופן כנה בהתאם להעדפותיהם האמיתיות וללא חשש.

8.6 וידוא תקינות ההצבעות

הפרוטוקול מיועד למצביעים הגונים ששולחים הצבעות תקינות. עם זאת, מצביעים עלולים לנסות לרמות ולשלוח הצבעות שאינן תקינות על מנת לעזור למועמד המועדף עליהם להיבחר. לדוגמה נניח שלמצביע V_n יש מועמד מועדף C_m וחוק ההצבעה הוא רוב. במקרה זה מצביע הגון V_n ישלח וקטור הצבעה $w_n = e_m$. מצביע שמנסה לרמות יכול לשלוח את הוקטור $w_n = Ne_m$. הצבעה לא חוקית זו יכולה להגביר את הסיכויים של C_m לנצח, או במקרה וזו ההצבעה הלא תקינה היחידה, זה יבטיח ש-C_m ינצח משום שהתוצאה המצטברת שלו תהיה גדולה מכל שאר ההצבעות יחדיו. באופן דומה ניתן ליצור הצבעות לא חוקיות בכל שאר חוקי ההצבעה מבוססי הציון. משום שסופרי הקולות לא נחשפים להצבעות עצמן הם אינם יכולים לוודא את תקינותן.

בבחירות לא תיאורטיות, מצביעים בדרך כלל יצביעו בקלפי מסודרת בה יש מחשבים מוגנים בבעלות הקלפי ולכן הסיכוי לפרוץ למחשבים אלו ולשנות את התוכנה שהם מריצים ואת אלגוריתם ההצבעה הוא קטן. עם זאת, לשם שלמות האלגוריתם והצגת פתרון מלא לכל בעיות האבטחה, מוצג פתרון מבוסס חישוב מרובה משתתפים שמאפשר לסופרי הקולות לוודא שכל הצבעה שמתקבלת היא תקינה, למרות שאינם נחשפים לתוכנה. במקרה וההצבעה אינה תקינה, סופרי הקולות יכולים לחבר את כל חלקי הסוד ביחד ולחשוף את המצביע ששלח אותה.

וידוא שיטת הרוב

נתחיל בלבחון וקטורים בשיטת הרוב. וקטור w_n הוא חוקי אם ורק אם $w_n(m) \leq 1$, כלומר הוקטור יכול להכיל ערכים 0 או 1 בלבד. לכן אפשר לוודא אי שוויון זה באמצעות חישוב מרובה משתתפים. ניתן ליצור מעגל שמחשב $w_n(m)(w_n(m) - 1)$ ולוודא שהתוצאה שמתקבלת היא 0 לכל m ולכל הצבעה. באופן דומה ניתן לוודא שקיים רק מקום יחיד בוקטור עם ערך 1 ע"י חישוב הסכום $\sum_{m\in[M]} w_n(m)$ ובדיקה שהוא מחזיר 1 בדיוק. העובדה ש- $N < p$ מבטיחה שהסכום לא יעבור את $p - 1$ ויתאפס.

וידוא שיטות וטו והסכמה

בשביל לוודא הצבעות במקרים של וטו והסכמה צריך לוודא שהוקטור מכיל רק 0 ו-1. אם כל המקומות בוקטור תקינים סופרי הקולות צריכים לוודא את החוק המצטבר. כלומר במקרה של חוקי וטו יש לוודא ש- $\sum_{m\in[M]} \quad w_n(m) = M-1$ ניתן לעשות זאת ע״י מעגל פשוט שסוכם את כל הכניסות בוקטור ומחזיר את התוצאה, כלומר סופרי הקולות נחשפים רק לסכום ולא להצבעות עצמן. הסכום לא חושף שום מידע רגיש משום שבכל וקטור הצבעה חוקי הסכום יהיה 1.

במקרה של הסכמה יש לוודא ש- $\sum_{m\in[M]} \quad w_n(m) \le K$. ניתן לבדוק תנאי זה בעזרת מעגל שמניב את התוצאה $S_n(S_n-1)\dots(S_n-K)$. סופרי הקולות יקבלו את ההצבעה אם ורק אם היא שווה ל-0. אם המצביע הצביע ליותר מ-K מועמדים אז אף אחד מהביטויים לא יהיה שווה ל-0. כך יכולים סופרי הקולות לוודא שהמצביע V_n הצביע לעד K מועמדים מבלי להיחשף לזהות המועמדים שהצביע אליהם. במקרה שהתוצאה אינה שווה ל-0 סופרי הקולות יכולים לדחות את ההצבעה.

וידוא שיטת הטווח

בשיטת הטווח הצבעה מוגדרת חוקית אם ורק אם $w_n(m) \le L$ לכל $m \in [M]$. ניתן לוודא שהצבעה חוקית בעזרת מעגל שמניב את התוצאה של $w_n(m)(w_n(m)-1)(w_n(m)-2)\dots(w_n(m)-L)$. סופרי הקולות יקבלו את ההצבעה אם ורק אם התוצאה היא 0. כך ניתן להבטיח שאף הצבעה לא מכילה ציון גבוה מהטווח.

וידוא שיטת בורדה

במקרה של בורדה הצבעה היא חוקית אם היא מכילה פרמוטציה כלשהי על $\{0,1,\dots,M-1\}$. לכן היא צריכה לקיים את שני האי-שוויונים הבאים:

1. $w_n(m) \le M-1 \; \forall m \in [M]$
2. $w_n(m) \ne w_n(m') \; \forall m > m' \in [M]$

את סעיף 1 ניתן לוודא באמצעות מעגל שמחזיר את הביטוי הבא: $w_n(m)(w_n(m)-1)(w_n(m)-2)\dots(w_n(m)-(M-1))$ וסופרי הקולות מקבלים את ההצבעה אם ורק אם הביטוי שווה ל-0 לכל m. את סעיף 2 ניתן לוודא ע"י בדיקה שכל הפרשי הזוגות $w_n(m)-w_n(m'), m>m'$ לא שווים לאפס. עם זאת משיקולי פרטיות אסור שסופרי הקולות יחשפו להפרשים אלו משום שבעזרתם ניתן להסיק את כל ההצבעות. על מנת למנוע את דליפת ההצבעות ועדיין לוודא את תקינות ההצבעות בבורדה, סופרי הקולות יכולים לייצר $\frac{M}{2}$ סודות אקראיים מעל שדה Z_p שנסמן ב- $\rho_{m,m'}, m>m' \in [M]$ ואז לחשב את $\zeta_{m,m'} := \rho_{m,m'}(w_n(m)-w_n(m'))$. אם השדה Z_p מספיק גדול אז בהסתברות גבוהה של $1/p$ $\rho_{m,m'}$

הוא לא אפס. במקרה זה $\zeta_{m,m'} \neq iff\ w_n(m) - w_n(m') \neq 0$ ולכן $\zeta_{m,m'}$ אינה חושפת שום מידע על $w_n(m) - w_n(m')$.

דבר אחרון שיש לשקול בנושא זה היא תוצאה שלילית כוזבת (false negative). במקרה ו-$\rho_{m,m'} = 0$ אז $\zeta_{m,m'} = 0$ גם במקרה ש-$w_n(m) - w_n(m') \neq 0$. לכן סופרי הקולות מזהים שהקול אינו תקין, כלומר שהוא מכיל מועמד אחד שמופיע פעמיים בפרמוטציית המועמדים. בסעיף הבא נדון בזמני ריצה ל-Z_p כאשר $p = 2^{61} - 1$, במקרה זה ההסתברות $1/p$ היא זניחה. כמו כן, במקרה ויש חשד לשליחת הצבעה לא תקינה ניתן להריץ את הבדיקה פעם נוספת עם $\rho_{m,m'}$ חדש. ניתן להריץ בדיקה זו פעמים נוספות ולהקטין את ההסתברות מעריכית כרצוננו וניתן גם לחכות עד לקבלת כל שאר ההצבעות ולחשוף את $w_n(m) - w_n(m')$.

8.7 הערכת עלויות

בחלק זה מנתחים את עלויות התקשורת והחישוב של המצביעים וסופרי הקולות. למצביעים ננתח את עלות ההצבעה. לסופרי הקולות ננתח את עלות חישוב התוצאה הסופית ועלות הוידוא שההצבעות חוקיות.

עלויות למצביעים

עלויות החישוב מסתכמות ביצירת $M(D-1) \cdot log_2 p$ ביטים אקראיים וביצוע $M(D-1)$ פעולות חיבור מעל השדה Z_p. פעולות אלה מתבצעות בסעיפים a1 ו-b1 של הפרוטוקול.

עלויות התקשורת מסתכמות בשליחת D הודעות לסופרי הקולות שכל אחת בגודל של $M \cdot log_2 p$ ביטים כפי שמפורט בסעיף c1 של הפרוטוקול.

עלויות אלו זניחות משום שערכם של שלושת הפרמטרים הוא קבוע ויחסית קטן.

- $p = 2^{61} - 1$ ולכן $log_2 p < 61$.
- מספר סופרי הקולות D הוא מספר קבוע וחד ספרתי.
- מספר המועמדים M הוא מספר סופי ויחסית קטן בכל תרחיש בחירות מציאותי.

עלויות לסופרי הקולות - חישוב התוצאה הסופית

עלויות חיבור כל ההצבעות לוקטור אחד כפי שמפורט בסעיף a2 בפרוטוקול הן זניחות משום שיש לבצע $M(N-1)$ פעולות חיבור. עם זאת, עלויות חישוב המועמדים המנצחים גבוהות יותר משום שיש לבצע חישוב מאובטח מרובה משתתפים. מספר שערי הכפל במעגל ההשוואה הוא $279 \cdot logp + 5$ בעומק

של 15. עלות התקשורת של כל שער כפל היא $12 \cdot logp$ לכל סופר קולות (ע"פ צ'ידה (Chida) טבלה 2 [PIK93]).

לכן סך כל התקשורת לכל סופר קולות היא בערך $3348 \cdot log^2 p$ ביטים אקראיים בקירוב. (או בערך מגהבייט וחצי כאשר $p = 2^{61} - 1$).

על מנת להעריך את זמן הריצה של ביצוע פעולות ההשוואה, נעשה שימוש במכונות AWS מסוג m5.4xlarge באיזור צפון וירג'יניה על רשת עם רוחב פס של 9.6 ג'יגהביט לשנייה. התבצעו ניסויים שונים עם מספר סופרי קולות שונים $D \in \{3,5,7,9\}$. פרמטר נוסף שמשפיע על זמן הריצה וגם הוא נבדק עם ערכים שונים הוא החסם העליון על התוצאה המצטברת B. נבחנו שני מקרים עיקריים $p_1 = B < 2^{13} - 1$ שמתאים לבחירות בהן מספר המצביעים יחסית קטן ו- $p_2 = B < 2^{31} - 1$ שמתאים לכל תרחיש בחירות מציאותי אחר.

המספרים המוצגים בטבלה מטה בשורות 1-2 מציינים את מספר אלפיות השנייה לביצוע של השוואה בודדת. על מנת למצוא את K המועמדים המנצחים, יש לבצע עד $K \cdot M$ השוואות. ניתן לראות שאפילו עם ערכים גבוהים של מועמדים אפשריים, מועמדים זוכים, חסם עליון $B < 2^{31} - 1$ ומספר סופרי קולות $D = 9$, עדיין עיבוד תוצאות הבחירות יכול להסתיים תוך מספר שניות בודדות.

D=9	D=7	D=5	D=3	
12.81	6.6	4.3	2.83	$B < p_1 = 2^{13} - 1$
15.0	9.64	9.54	9.07	$B < p_2 = 2^{31} - 1$
65.55	52.9	42.2	41.3	וידוא $5 \cdot 10^4$ הצבעות בשיטת הרוב
1311	1058	844	826	וידוא $5 \cdot 10^4$ הצבעות בשיטת הטווח עם $L = 20$
7050	5770	4945	4210	וידוא $5 \cdot 10^4$ הצבעות בשיטת הטווח עם $L = 100$
2622	2116	1688	1652	וידוא $5 \cdot 10^4$ הצבעות בשיטת בורדה עם $M = 5$
11799	9522	7596	7434	וידוא $5 \cdot 10^4$ הצבעות בשיטת בורדה עם $M = 10$

טבלה 1

עלויות לסופרי הקולות - וידוא תקינות ההצבעות

חוקי הצבעה שונים גוררים עלויות שונות ולכן נדון בנפרד בחוקים רוב, טווח ובורדה. (הסכמה ווטו דומים לרוב). החישובים התבצעו על בסיס התוצאות במאמר של צ'ידה, בו הריצו ניסויים על תצורת רשת דומה עם מעגל שמורכב ממיליון שערי כפל שפוזרו באופן אחיד על $\{20,100,1000\}$ שכבות. לכן בכל שכבה היו $\{5 \cdot 10^4, 10^4, 10^3\}$ שערי כפל בהתאמה. זמני הריצה כפונקציה של D, מספר סופרי הקולות במקרה שלנו מוצגים בטבלה הבאה. הערכים בטבלה מצינים את מספר אלפיות השנייה שלקחו לחשב 10^6 שערי כפל.

מספר השכבות	מספר שערי הכפל בכל שכבה	D=3	D=5	D=7	D=9
20	50000	826	844	1058	1311
100	10000	842	989	1154	1410
1000	1000	1340	1704	1851	2243

טבלה 2

חוק הרוב

כפי שמתואר בסעיף 'וידוא תקינות ההצבעות' על מנת לוודא הצבעות בשיטת הרוב יש להריץ מעגל שבודק $w_n(m) \leq 1$. מעגל כזה מורכב ממעגל כפל יחיד בעומק 1. בנוסף בשביל לוודא שיש רק מיקום יחיד בוקטור עם ערך 1, יש לבצע חיבור שניתן להריץ מקומית ואינו דורש שערי כפל כלל. בסך הכל מעגל לוידוא של q הצבעות דורש בדיוק $q \cdot M$ שערי כפל בשכבה אחת. זמני הריצה בשורה 1 של טבלה 2 מציינים את הזמן שלוקח להריץ מעגל עם 10^6 שערי כפל שמפוזרים באופן אחיד על גבי 20 שכבות. לכן זמן הריצה של הרצת $10^6/20 = 5 \cdot 10^4$ שערי כפל בשכבה אחת מתקבל כאשר מחלקים את זמן הריצה ב-20, כך מתקבל זמן הריצה בשורה 3 של טבלה 1, שהוא חסם עליון של וידוא $5 \cdot 10^4$ הצבעות בשיטת חוק הרוב, משום שזמן זה הושג עם $p = 2^{61} - 1$ שהוא יותר גדול מאשר p_1, p_2 שמספיקים לכל תרחיש בחירות מציאותי. המסקנה ממספרים אלו היא שניתן לוודא 50 מיליון הצבעות בפחות מדקה. במילים אחרות המערכת מהירה ומתאימה לבחירות ארציות.

חוק הטווח

עלות הוידוא של הצבעות בחוק הטווח היא פונקציה של הציון המקסימלי שמצביע יכול לתת למועמד - L. לכן וידוא של הצבעה לפי חוק הטווח דורשת מעגל עם L שערי כפל בטור, במימוש נאיבי ללא אופטימיזציות. לכן הניסוי ב-[PIK93] שמריץ מעגל עם מיליון שערי כפל ב-20 שכבות מתאים בדיוק

למקרה של וידוא $5 \cdot 10^4$ הצבעות בחוק הטווח כאשר $L = 20$. זמני ריצה אלו מוצגים בטבלה 1 בשורה 4. באותו אופן אם $L = 100$ ניתן להסתמך על זמני הריצה המוצגים ב-[PIK93] למעגל עם מיליון שערי כפל שפרוסים על גבי 100 שכבות כפי שמופיעים בטבלה 2 בשורה 2. על מנת להתאים את מספר השכבות לזמני הריצה המוצגים ב-[PIK93] ניתן לפרוס את שערי הכפל על פני 20 שכבות ולהכפיל את זמני הריצה ב-5. כך מתקבלת שורה 5 בטבלה 1.

למרות שזמני הריצה גבוהים לעומת וידוא של הצבעות בחוק הרוב, וידוא הצבעות בשיטת הטווח היא פעולה פרקטית שתסתיים יחסית מהר. לדוגמה וידוא של 50 מיליון הצבעות בשיטת הטווח עם $L = 100$ ו-$D = 9$, ייקח פחות משעתיים. ברוב תרחישי ההצבעות כיום, הצבעה לוקחת לפחות יום שלם ולכן שעתיים הן עדיין זמן נמוך יחסית.

חוק הבורדה

וידוא הצבעות בחוק הבורדה הן פונקציה של מספר המועמדים M. כפח שמתואר בסעיף "וידוא תקינות ההצבעות", וידוא כל הצבעה מורכב משני שלבים. בשלב הראשון בודקים שכל איבר בוקטור הוא בטווח $[0, M-1]$. ניתן לבדוק זאת באמצעות מעגל בעומק 1-M עם $M \cdot (M-1)$ שערי כפל. בשלב השני יש לוודא שההצבעה כולה היא פרמוטציה של $\{0, \ldots, M-1\}$. בדיקה זו דורשת לייצר $\frac{M}{2}$ חלקי סודות בסכמת שיתוף הסודות של שמיר וחישוב של $\frac{M}{2}$ שערי כפל במעגל עם שכבה אחת. עלויות החישוב והתקשרות הכרוכות ביצירת חלקי סודות ושיתופם קטנה משמעותית מאלו הכרוכות בחישוב מעגל כפל לפי [PIK93]. לכן עלויות השלב השני חסומות מלמעלה ע"י העלויות לחישוב $2\frac{M}{2} = M(M-1)$ שערי כפל בשתי שכבות. בסך הכל ניתן לחסום את עלויות שני השלבים ע"י $2M \cdot (M-1)$ פעולות כפל על גבי 1-M שכבות. כאשר $M = 5$ העלות הכוללת של וידוא הצבעה אחת היא $2M \cdot (M-1) = 40$ פעולות כפל שפרוסות על גבי 4 שכבות. לכן בשביל לוודא $2.5 \cdot 10^4$ הצבעות יש לבצע מיליון פעולות כפל על גבי 4 שכבות. זמני ריצה אלו חסומים ע"י זמן הריצה שבטבלה 2 בשורה 1, משום שהזמן בטבלה הוא על אותו מספר של פעולות כפל אבל על גבי יותר שכבות. לכן נסכם ונטען שהזמן ריצה של וידוא $5 \cdot 10^4$ הצבעות בשיטת חוק בורדה מתקבל ע"י הכפלת זמן הריצה שמפורט בטבלה 2 בשורה 1, והתוצאה המתקבלת מפורטת בטבלה 1 בשורה 6.

מציאת חסם עליון לזמני הריצה כאשר $M = 10$ מתבצע באופן דומה. העלות לוידוא הצבעה אחת במקרה זה היא $2M(M-1) = 180$ פעולות כפל הפרוסות על גבי 9 שכבות. לכן על מנת לוודא $10^6/180$ הצבעות יש לבצע מיליון פעולות כפל על גבי 9 שכבות. זמני ריצה אלו חסומים מלמעלה ע"י

זמני הריצה בשורה 1 בטבלה 2. לסיכום זמן הריצה הכולל לוידוא של $5 \cdot 10^4$ הצבעות בשיטת בורדה מתקבלים ע"י הכפלת זמני הריצה בשורה 9 בטבלה 2 והתוצאה מתקבלת בשורה 7 של טבלה 1.
לסיכום, וידוא של הצבעות בורדה הוא יחסית מהיר ומאוד פרקטי כאשר $M = 5$ או $M = 10$. לדוגמה וידוא של מיליון הצבעות כאשר $M = 10$ ו- $D = 9$ ייקח פחות מ-4 דקות. ערכים גבוהים יותר של M יגררו זמני וידוא איטיים יותר אך מקרים אלו הרבה פחות פרקטיים, משום שקשה לצפות מכל בוחר להכיר ולדרג מספר רב של מועמדים.

8.8 דיון

מערכות הצבעה אלקטרוניות צריכות לספק מספר דרישות חיוניות. בחלק זה נדון בדרישות אלו כפי שמוצגות במאמר של צ׳אנג ולי [DJN10] ונפרט כיצד המערכת המוצגת עונה על דרישות אלו.

פרטיות ואנונימיות -ההצבעות צריכות להישאר אנונימיות לאורך כל תהליך הבחירות.
המערכת המוצגת במאמר שומרת על סודיות ההצבעות ואנונימיות המצביעים כפי שמפורט בסעיף ״אבטחת הפרוטוקול״. כמו כן, תוצאת הפרוטוקול כוללת אך ורק את תוצאת הבחירות ולא חושפת שום מידע נוסף לכן נשמרת פרטיות המצביעים וההצבעות.
הוגנות - מנגנון בחירות הוגן אינו חושף תוצאות חלקיות.
המערכת שומרת על הוגנות משום שאינה חושפת בשום שלב את ציון המועמדים אלא רק את התוצאה הסופית בסוף הבחירות.
נוחות - אין צורך בציוד מיוחד והמצביעים אינם צריכים ללמוד שום טכניקה מיוחדת.
הפרוטוקול מתבסס על פונקציות קריפטוגרפיות מוכרות שניתן למצוא בספריות קריפטוגרפיה חינמיות רבות. משום שהפרוטוקול כולל פונקציות לוידוא ההצבעות, המצביעים יכולים להצביע מכל מקום ולא בהכרח ממרכזי הצבעה. כל שהמצביע צריך לעשות הוא להוריד את התוכנה שממממשת את התקשורת מול סופרי הקולות.
עמידות - שום גורם זדוני לא יוכל לשבש את פעילות המערכת.
דרישה זו נענית באמצעות מימוש של דרישות אבטחה סטנדרטיות כפי שמפורט בסעיף ״אבטחת הפרוטוקול״. בפרט, הפרוטוקול דורש חתימת ההצבעות, וידוא הצבעות שהתקבלו ובדיקה שכל הצבעה התקבלה כפי שנשלחה.
ניידות - המערכת יכולה לרוץ על גבי האינטרנט.
הפרוטוקול ניתן למימוש על גבי האינטרנט משום שלא נדרש שום ציוד מיוחד והכל יכול להיות ממומש כאתר אינטרנט.

ייחודיות - כל מצביע יכול להצביע רק פעם אחת.
אם מצביע מנסה להצביע יותר מפעם אחת, רק ההצבעה הראשונה שלו תעובד במערכת בעוד השנייה תדחה. כמו כן, גורם זדוני לא יכול ליירט הצבעה ולשנות אותה מבלי להתגלות משום שכל מצביע מקבל קבלה מסופרי הקולות ומוודא שההצבעה שהתקבלה זהה להצבעה שנשלחה. אם הקבלה לא התקבלה המצביע יכול לשלוח את הצבעתו שוב.
שלמות - רק מצביעים שרשאים להצביע יכולים להצביע.
דרישה זו מסופקת משום שלכל מצביע חייב להיות מפתח ציבורי שאיתו הוא מצפין את ההצבעה שלו.
אי יכולת לשחד - מצביע לא יכול להוכיח לצד שלישי למי הוא הצביע, על מנת למנוע שוחד.
הדרך היחידה להוכיח לגורם שלישי שמצביע הצביע למועמד מסוים היא אם רוב סופרי הקולות ישלחו אחד לשני את חלקי הסודות של ההצבעות של אותו מצביע ויחברו אותן באמצעות סכמת שיתוף הסודות של שמיר. משום שהפרוטוקול מניח שיש רוב הגון של סופרי קולות, דרישה זו מתקיימת.
נכונות - כל הצבעה נספרת.
נכונות ספירת הקולות נובעת מההנחה שסופרי הקולות מבצעים את החישובים בצורה נכונה. פרקטית ניתן למלא דרישה זו ע"י וידוא התוכנה של סופרי הקולות והרצתה על מחשב מאובטח במקום פיזי מאובטח כך שלא ניתן לפרוץ אליו בשום צורה.
יעילות -הפרוטוקול צריך להחזיר את תוצאות הבחירות בזמן סביר.
הפרוטוקול עומד בדרישה זו כפי שמפורט בסעיף "הערכת עלויות".
היכולת להימנע - מצביע שרוצה להימנע יוכל לעשות זאת מבלי לחשוף עובדה זו לגורם שלישי.
בכל חוקי ההצבעה שנידונו במאמר זה, כל הצבעה היא וקטור והתוצאה הסופית היא סכום הוקטורים. לכן מצביע V_n שרוצה להימנע, יכול לשלוח את וקטור האפס $w_n = 0$. משום שוקטור זה אינו משפיע על התוצאה הסופית הוא שקול להימנעות. סופרי הקולות לא יכולים לדעת שנשלח וקטור שכולו אפסים משום שהם אינם יכולים לראות אף הצבעה בפני עצמה. לכן הפרוטוקול עומד בדרישה זו.

כאמור לעיל, המערכת המוצגת במאמר זה מתאימה לבחירות אלקטרוניות מכל סוג ולכל גודל, מבחירות קטנות כמו בחירת ראש פקולטה, ועד בחירות ארציות עם אוכלוסיה בכל גודל, בהנחה וחוקי הבחירות מבוססי ציון. במקרה של בחירות ארציות ניתן לממש את המערכת באופן דומה לאיך שבחירות מתקיימות כיום. אזרחים יגיעו לקלפיות ויזדהו בעזרת תעודות הזהות שלהם. לאחר שלב ההזדהות הם יקבלו גישה למחשב בו הם יוכלו להצביע באופן פרטי. המחשב יתרגם את בחירתם לוקטור הצבעה בהתאם לחוק מבוסס הציון שנבחר לאותן בחירות. הוקטור יפוצל למספר חלקי סודות בהתאם למספר סופרי הקולות ויישלח אליהם. בסיום תקופת הבחירות, המערכת תחזיר את המועמדים הזוכים בתוך שניות בודדות.

8.9 סיכום

במאמר זה מוצגת מערכת לבחירות אלקטרוניות מאובטחות שבהינתן תצורת בחירות בה מצביעים נדרשים לבחור מבין K מועמדים בשיטת חוקי בחירות מבוססי ציון, המערכת תחזיר את K המועמדים הזוכים תוך שמירה על סודיות מושלמת. כלומר, מלבד התוצאה הסופית, לא נחשף שום מידע נוסף לא למצביעים ולא לסופרי הקולות. כולל ההצבעות עצמן, זהות הבוחרים, ציון כל מועמד או תוצאות חלקיות של הבחירות. תכונה זו מושגת באמצעות חישוב מאובטח מרובה משתתפים ופיצול כל הצבעה למספר חלקי סודות בסכמת שיתוף הסודות של שמיר.

סודיות מושלמת תעודד מצביעים להצביע בביטחון לפי העדפותיהם האמיתיות ללא חשש שההצבעה שלהן תחשף לגורם שלישי. כמו כן, המערכת יכולה לשמש גם בתרחישים של בחירות איטרטיביות, בהן ישנם מספר סבבי בחירות. משום ששום מידע לא נחשף על ההצבעות או על תוצאות חלקיות לפי אזורים מסוימים לדוגמא, המערכת מונעת הצבעה אסטרטגית. (כמובן שהמערכת לא יכולה למנוע התפשטות מידע בערוצים אחרים כמו תקשורת, שמועות ורשתות חברתיות)

המערכת עונה על כל הדרישות למערכת בחירות אלקטרונית מאובטחת וזמני הריצה והתקשרות שנותחו לעיל מראים שהמערכת מהירה ופרקטית ולכן ניתן לממש אותה לבחירות בכל תרחיש, כולל בחירות ארציות. הפרוטוקול מבוסס על אלגוריתמים קיימים בתחום הקריפטוגרפיה בלבד ולכן ניתן לממש את המערכת על גבי כל ספריות קיימות בשפות תכנות שונות. עובדה זו מהווה יתרון נוסף משום שלא צריך לממש פרוטוקולים חדשים, לבחון אותם ולוודא שהם באמת מאובטחים.

9. סכמת הצבעה בטוחה לחישוב תוצאות הבחירות עבור כללי הצבעה מבוססי סדר

9.1 הפרוטוקול

הגדרות

במודל שלנו יש N מצביעים שיסומנו $V = \{V_1, \ldots, V_N\}$ ו-M מועמדים שיסומנו $C = \{C_1, \ldots, C_M\}$.
הפלט של הבחירות הוא המועמדים המנצחים. נדון בשני חוקי בחירות מבוססי סדר - קופלנד ומקסימין.
בשתי השיטות המועמדים שולחים סידור מלא של העדופתיהם על כלל המועמדים. ההצבעה נשלחת כמטריצה שבה כל כניסה היא השוואה בין זוג מועמדים
ובכל שיטה מחשבים את המועמדים המנצחים אחרת. בחלק זה ניצור פרוטוקול לחישוב מאובטח מרובה משתתפים לשני החוקים:

1. קופלנד (Copeland) - לכל מצביע נגדיר מטריצה $P_n = (P_n(m, m') : m, m' \in [M])$ כאשר $P_n(m, m') = 1$ כאשר המועמד C_m מדורג גבוה יותר מאשר המועמד $C_{m'}$ בדירוג של המצביע V_n, במקרה ההפוך ו-$P_n(m, m') = -1$, $P_n(m, m') = 0$ אם $m = m'$.
   סכום המטריצה $P = \sum_{n=1}^{N} P_n$ מניב את הציון הבא לכל מועמד:

$$w(m) := |\{m' \neq m : P(m, m') > 0\}| + \alpha|\{m' \neq m : P(m, m') = 0\}|$$

   כלומר, $w(m)$ שווה למספר המועמדים ש-C_m ניצח (שרוב המצביעים דירגו נמוך יותר מאשר C_m) ועוד α כפול מספר המועמדים שיצאו בתיקו עם C_m (כלומר מספר שווה של מצביעים דירגו אותם בסידורים הפוכים).
   הפרמטר α יכול לקבל כל ערך בין 0 ל-1. הערך הנפוץ הוא חצי. במקרה זה החוק נקרא קופלנד-חצי.

2. מקסימין (Maximin) - לכל מצביע נגדיר מטריצה P_n כך ש- $P_n(m, m') = 1$ כאשר המועמד C_m מדורג גבוה יותר מאשר המועמד $C_{m'}$ בדירוג של המצביע V_n ו- $P_n(m, m') = 0$ אחרת. גם בשיטה זו נסכום את כל כניסות המטריצה $P = \sum_{n=1}^{N} P_n$ רק שהפעם הסכום מייצג פשוט את מספר המועמדים שהעדיפו מועמד C_m על פני מועמד אחר $C_{m'}$. הציון הסופי של מועמד C_m הוא $w(m) := min_{m' \neq m} P(m, m')$

אפיון הצבעות חוקיות בקופלנד ומקסימין

מכאן ואילך נתייחס למטריצה P_n בתור ההצבעה של מועמד V_n, ונתייחס למטריצה P בתור מטריצת הסכומים.

משפט 1 - מטריצה Q מהצורה $M \times M$ היא הצבעה חוקית תחת חוק קופלנד אם ורק אם היא מספקת את התנאים הבאים:

1. כל ערך במטריצה הוא 1 או -1 למעט איברי האלכסון.
2. כל איברי האלכסון שווים ל-0.
3. לכל $1 \leq m < m' \leq M$ מתקיים $Q(m', m) + Q(m, m') = 0$
4. סכום כל שורה (או עמודה) שונה מכל שאר השורות.

משפט 2 - מטריצה Q מהצורה $M \times M$ היא הצבעה חוקית תחת חוק מקסימין אם ורק אם היא מספקת את התנאים הבאים:

1. כל ערך במטריצה הוא 1 או 0 למעט איברי האלכסון.
2. כל איברי האלכסון שווים ל-0.
3. לכל $1 \leq m < m' \leq M$ מתקיים $Q(m', m) + Q(m, m') = 0$
4. סכום כל שורה (או עמודה) שונה מכל שאר השורות. כלומר כל מצביע שולח דירוג מלא בין כל המועמדים כך שאין מועמדים עם דירוג שווה.

המשמעות של התנאים בשני המשפטים:

1. כל מועמד א' מדורג גבוה יותר או נמוך יותר ממועמד ב'. האלכסון מכיל השוואה בין כל מועמד לעצמו ולכן חוק זה אינו חל על האלכסון.
2. כל מועמד שווה בדירוג לעצמו.
3. אם מועמד א' מדורג גבוה יותר בהצבעה נתונה מאשר מועמד ב' הוא יקבל 1, אז מועמד ב' חייב להיות מדורג נמוך יותר ממועמד א' ויקבל את הערך -1 בקופלנד ו-0 במקסימין. לכן סכום זוג כניסות של אותם מועמדים יהיה שווה ל-0 בקופלנד ול-1 במקסימין.
4. כל מצביע שולח דירוג מלא בין כל המועמדים כך שאין מועמדים עם דירוג שווה.

פרוטוקול מאובטח לחוקי הצבעה מבוססי סדר

הפרוטוקול מחשב באופן מאובטח ומשמר פרטיות את המועמדים המנצחים בבחירות מבוססות חוקי קופלנד או מקסימין. לפרוטוקול שני שלבים עיקריים.

השלב הראשון הוא שלב ההצבעה. בשלב זה כל מצביע בונה את מטריצת ההצבעה שלו P_n (שורה 2), מגריל פולינום מדרגה $D' - 1$ לכל אחד מ-$M(M-1)/2$ האפשרויות של השוואת זוג מועמדים מהצורה $Q(m, m')$ לפי החוק המתאים (שורות 3-5) ואז שולח לכל סופר קולות T_d את חלק הסוד שלו, שהוא ערך הפולינום כאשר $x = d$ (שורות 6-7).

לאחר שכל סופרי הקולות קיבלו את חלקי הסוד שלהם, הם מבצעים חישוב מאובטח מרובה משתתפים בשביל לוודא את תקינות ההצבעה (שורה 8).

בשלב השני לאחר שהסתיים שלב ההצבעה, כל סופר קולות מחבר את כל n חלקי הסוד של כל ההשוואות מהצורה $Q(m, m')$ שקיבל ע"י המצביעים. ערך זה יסומן $G_d(m, m')$. לבסוף סופרי הקולות מבצעים חישוב מאובטח מרובה משתתפים בו הם משתפים את ערכי ה- G_d של כל אחד, על מנת לקבוע את המועמדים המנצחים מבלי להיחשף לאף הצבעה.

9.2 וידוא חוקיות ההצבעות

הפרוטוקול מיועד למצביעים הגונים ששולחים הצבעות תקינות. עם זאת, מצביעים עלולים לנסות לרמות ולשלוח הצבעות שאינן תקינות על מנת לעזור למועמד המועדף עליהם להיבחר. למשל מצביע לא הגון יכול לשלוח לסופרי הקולות חלקי סוד של מטריצה מהצורה cQ, כאשר c הוא מספר כלשהו גדול מ-1 שמנפח את המשקל של ההצבעה שלו בתוצאה המצטברת. כלומר אם c=5 אז ההצבעה שלו שקולה לחמש הצבעות. הבעיה בפרוטוקול היא שלא ניתן לשתף את חלקי הסוד ולחשוף הצבעות בודדות בשביל לשמור על פרטיות המצביעים (תחת ההנחה של סופרי קולות הגונים) ולכן הכרחי למצוא דרך שבה סופרי הקולות יוכלו לוודא את תקינות ההצבעות מבלי לדעת את מטריצת ההצבעה. עובדה זו לבדה אמורה להרתיע מצביעים מלרמות מלכתחילה.

כעת נסביר איך לוודא את תנאי ההצבעה הנ"ל שפורטו בסעיף "אפיון הצבעות חוקיות בקופלנד ומקסימין".

ראשית נשים לב שתנאי 2 בשני המשפטים לא דורש וידוא משום שהמצביע אינו שולח חלקי סוד של ערכי האלכסון משום שהם כולם שווים לאפס. כמו כן אין צורך לוודא את תנאי 3 משום שהמצביע אינו שולח את המשולש התחתון של המטריצה משום שניתן לחשב אותו מתוך המשולש העליון.

וידוא תנאי 1

על מנת לוודא את תנאי 1 סופרי הקולות צריכים לוודא שכל ערך במשולש העליון של המטריצה הוא 1 או -1 במקרה של חוק קופלנד ו-1 או 0 במקרה של חוק מקסימין. כל כניסה x במטריצה במשולש העליון של המטריצה תיבדק בנפרד. נשים לב לשקילות הבאה במקרה של קופלנד:

$$x \in \{-1,1\} \Leftrightarrow (x+1)\cdot(x-1) = 0$$

ולשקילות דומה בחוק מקסימין:

$$x \in \{0,1\} \Leftrightarrow x\cdot(x-1) = 0.$$

ניתן ליצור מעגל שיחזיר את הפלט של משוואות אלו. אם המעגל החזיר 0 אז תנאי 1 אומת ואם המעגל החזיר כל תוצאה אחרת אז תנאי 1 לא מתקיים ועל כן נדחה את ההצבעה.

וידוא תנאי 4

ראשית נשים לב שסופרי הקולות יכולים לחשב את הסכום של כל עמודה Q_m בזכות ליניאריות פרוצדורת השיתוף שהוזכרה ברקע הקריפטוגרפי. לפי תנאים 2 ו-3 בחוק קופלנד:

$$Q_m = \sum_{m\prime\in[M]} Q(m',m) = \sum_{m\prime<m} Q(m',m) - \sum_{m<m\prime} Q(m,m')$$

ובאופן דומה לפי תנאים 2 ו-3 בחוק מקסימין:

$$Q_m = \sum_{m\prime<m} Q(m',m) - \sum_{m<m\prime} Q(m,m') + (M-m)$$

כעת, אחרי שכל סופר קולות מחשב את החלק שלו בסכום כל עמודה במטריצה ההצבעה, יש לוודא שכל הסכומים שונים. ניתן לבצע זאת ע"י חישוב המכפלה הבאה ובדיקה שהסכום שונה מאפס.

$$F(Q) := \prod_{1\le m\prime<m\le M} (Q_m - Q_{m\prime})$$

אם הסכום שווה לאפס ניתן להסיק שישנן לפחות שתי עמודות עם סכום זהה ועל כן בכאלה מקרים ההצבעה תיפסל.

וידוא חוקיות ההצבעות - שמירה על פרטיות

השאלה המתבקשת לאחר הדיון בסעיף הקודם היא האם וידוא תקינות ההצבעות פוגע בפרטיות המצביעים. פרטיות זו חשובה על מנת לעודד מצביעים להצביע בהתאם להעדפותיהם האמיתיות.
במהלך וידוא תנאי 1 של חוקי קופלנד ומקסימין, אם ההצבעות תקינות אז כל שערי הכפל יחזירו 0. לכן סופרי הקולות לא ילמדו דבר מוידוא ההצבעות והפרטיות המושלמת תישמר.
הוידוא של תנאי 4 מבטיח סודיות כמעט מושלמת במובן הבא. אם Q היא הצבעה חוקית לפי חוק קופלנד אז $(Q_1 ,\dots, Q_M)$ היא פרמוטציה של $(-M+1, -M+3, \dots, M-3, M-1)$. בכזה מצב ניתן להראות שתמיד מתקיים

$$F(Q) := \prod_{1\le m\prime<m\le M} (Q_m - Q_{m\prime}) = \pm 2^{\frac{M}{2}} \cdot \prod_{1\le m\prime<m\le M} (m-m')$$

כאשר הסימן $(\pm)$ קשור לחתימה של הפרמוטציה המיוצגת בהצבעה של המצביע. כלומר, יש פה דליפת מידע קלה, האם החתימה היא חיובית או שלילית. גם דליפה זו ניתן להעלים על ידי העלאה בריבוע של כל הביטוי. על כן, החישוב הזה אינו מדליף דבר לגבי חוקיות ההצבעה מעבר לקיומו או אי-קיומו של תנאי 4.

וידוא חוקיות ההצבעות - עלויות חישוב

וידוא תנאי 1 יכול להתבצע במקביל על כל $M(M-1)/2$ הרשומות בהצבעה אחת. באותו אופן ניתן לוודא מספר הצבעות במקביל, ולכן בשביל לוודא B הצבעות, סופרי הקולות צריכים לחשב $BM(M-1)/2$ שערי כפל במקביל.

וידוא תנאי 4 לעומת זאת דורש לבצע $M(M-1)/2$ פעולות כפל באופן סדרתי ולכן בשביל לוודא B הצבעות סופרי הקולות צריכים לבצע $M(M-1)/2$ סבבי חישוב כאשר בכל אחד הם מחשבים B שערי כפל במקביל.

וידוא חוקיות שיתוף הסודות

מצביע זדוני יכול לנסות לחבל במהלך הבחירות ע"י הפצת חלקי סוד שלא מהווים חלק מפולינום בדרגה $D'-1$. כלומר המצביע שולח את חלקי הסוד $\{s_1,\dots,s_D\}$ לסופרי הקולות $\{T_1,\dots,T_D\}$ כך שלא קיים פולינום g מדרגה $D'-1$ לכל היותר שמקיים $g(d)=s_d$ לכל $d\in[D]\}$. ע"י בחירה ספציפית של חלקי סוד, בדיקת תקינות ההצבעה עלולה לעבור בהסתברות לא זניחה וחלקי סוד אלו ישתתפו בחישוב התוצאה הסופית. משום שחלקי סוד אלו לא יוצרים פולינום מדרגה לכל היותר $D'-1$, הם עלולים לחבל בחישוב התוצאה. בחלק זה אנחנו מסבירים איך ניתן לוודא את חלקי הסוד מבלי לחשוף שום מידע נוסף על ההצבעה.

על מנת לוודא זאת, סופרי הקולות מבצעים את הצעדים הבאים בקבלת הצבעה:

1. כל סופר קולות T_d מייצר מספר רנדומלי r_d ומפיץ חלקי סוד שלו לכל סופרי הקולות $\{r_{d,1},\dots,r_{d,D}\}$.
2. כל סופר קולות T_d מחשב $\widehat{s_d}=s_d+\sum_{j\in[D]} r_{j,d}$ כלומר סופר הקולות מחבר לחלק הסוד שקיבל מהמצביע את כל חלקי הסודות שקיבל מסופרי הקולות האחרים (כולל את חלק הסוד שלו עצמו).
3. כל סופר קולות T_d מפיץ את הערך שחישב $\widehat{s_d}$ לכלל סופרי הקולות.
4. כל סופר קולות T_d מחשב פולינום f עם דרגה $D-1$ לכל היותר כך שמתקיים $f(d)=\widehat{s_d}$ לכל $d\in[D]$.
5. אם הדרגה של הפולינום f היא $D'-1$ לכל היותר אז חלקי הסוד $\{s_1,\dots,s_D\}$ ששלח המצביע V הם חלקי סוד חוקיים בסכמת שיתוף הסודות של שמיר.
6. אחרת, סופרי הקולות יידחו את ההצבעה.

הוכחה שהפרוצדורה המפורטת לעיל נכונה ומשמרת את פרטיות המצביעים

נניח שמצביע V הגון. אז קיים פולינום g מדרגה $D'-1$ כך שמתקיים $s_d=g(d), d\in[D]$.

נגדיר $G := g + \sum_{j\in[D]} g_j$ כאשר $j \in [D]$, g_j הוא הפולינום מדרגה $D' - 1$ שכל סופר קולות ייצר באלגוריתם הנ"ל בסעיף 1. אז

$$G(d) = g(d) + \sum_{j\in[D]} g_j(d) = s_d + \sum_{j\in[D]} r_{j,d} = \widehat{s_d}, d \in [D]$$

לכן הפולינום שכל אחד מסופרי הקולות מחשב בסעיף 4 באלגוריתם שווה ל-G.

משום ש-G הוא סכום של פולינומים מדרגה $D' - 1$ לכל היותר הבדיקה בסעיף 5 עוברת.

במקרה זה סופרי הקולות יכולים לחשב את $G(0) = g(0) + \sum_{j\in[D]} r_j$ שלא חושף שום מידע על ההצבעה של V. לכן בדיקה זו מספקת פרטיות מושלמת למצביע.

בכיוון ההפוך, נניח שהמצביע V הפיץ חלקי סוד $\{s_1, \ldots, s_D\}$ מפולינום g עם דרגה גדולה מ- $D' - 1$.

במקרה זה הפולינום שמחושב בסעיף 4 לעיל יהיה שווה $f = g + \sum_{j\in[D]} g_j$. משום שהדרגה של g גדולה מ- $D' - 1$ אז גם הדרגה של f תהיה גדולה מ- $D' - 1$ ולכן סופרי הקולות יידחו את ההצבעה. גם כאן לא ניתן להסיק שום דבר על g ולכן גם פה נשמרת הפרטיות המושלמת.

9.3 חישוב מאובטח מרובה משתתפים של המועמדים המנצחים

חישוב מאובטח מרובה משתתפים של המועמדים המנצחים בחוק קופלנד

בחלק זה נסביר איך ניתן מחשבים את הציון המצטבר של כל מועמד ואיך ניתן לקבוע את המועמדים המנצחים.

כאמור לעיל הציון של כל מועמד מחושב לפי חוק קופלנד באופן הבא:

$$w(m) := |\{m' \neq m : P(m,m') > 0\}| + \alpha|\{m' \neq m : P(m,m') = 0\}|$$

כאשר α הוא מספר רציונלי בין 0 ל-1 (לרוב 1/2). כלומר $\alpha = s/t$ לשני מספרים שלמים s, t.

נשים לב שביטוי זה מכיל את כל הכניסות במטריצה למעט האלכסון. עם זאת, המצביעים אינם שולחים את כל המטריצה אלא רק את המשולש העליון. לכן בשלב הראשון בחישוב נצטרך לתרגם את החישוב של $w(m)$ בהתאם. לפי תנאי 3 במשפט חוק קופלנד אם $P_n(m,m') = 1$ אז $P_n(m',m) = -1$. לכן לכל זוג $\{(m,m') : m' < m\}$ ניתן להחליף את כל ההשוואות המאובטחות מהצורה $1_{P(m,m')=0}$ בביטוי $1_{P(m',m)=0}$ ואת כל הביטויים מהצורה $1_{P(m,m')>0}$ בביטויים $1_{-P(m',m)>0}$. כך נקבל

$$t \cdot w(m) = t \cdot \left\{ \sum_{m'>m} 1_{P(m,m')>0} + \sum_{m'<m} 1_{-P(m',m)>0} \right\}$$

$$+s \cdot \left\{ \sum_{m'>m} 1_{P(m,m')=0} + \sum_{m'<m} 1_{P(m,m')=0} \right\}$$

ביטוי זה מאפשר לסופרי הקולות לחשב את ציון המועמדים באמצעות חישוב מאובטח מרובה משתתפים רק בעזרת חלקי הסודות של הערכים במשולש העליון של המטריצה באמצעות מעגל חישוב עם שערי כפל וחיבור בלבד.

בשלב הראשון סופרי הקולות מחשבים את הביטוי הנ"ל ע"י החלפת חלקי סוד בביטים של כל ביטויי האי שוויון וביטויי השוויון לאפס (כפי שתואר בסעיף "השוואה מאובטחת") . לאחר שלב זה יש לכל סופר קולות חלק סוד בביטוי $t \cdot w(m)$ ובשלב הבא סופרי הקולות מבצעים השוואה מאובטחת על הציון של כל מועמד על מנת למצוא את K המועמדים עם הציון הגבוה ביותר. בשביל למצוא את המועמד עם הציון הגבוה ביותר הם צריכים לבצע $M-1$ השוואות, בשביל המועמד הבא יש לבצע $M-2$ השוואות וכך הלאה. באופן כללי מספר ההשוואות שיש לבצע בשלב זה הוא $m = K \cdot (M - \frac{K+1}{2})$ $\sum_{m=M-K}^{M-1}$.

לאחר סיום החישוב סופרי הקולות מפרסמים את האינדקסים של המועמדים המנצחים.

חישוב מאובטח מרובה משתתפים של המועמדים המנצחים בחוק מקסימין

לכל $m \in [M]$, סופרי הקולות צריכים למצוא את האינדקס $m' \neq m$ שיניב את הערך המינימלי $P(m, m')$. בשביל למצוא את הערך המינימלי מבין $M-1$ ערכים סופרי הקולות צריכים לבצע $M-2$ השוואות מאובטחות. כלומר $M(M-2)$ השוואות בסך הכל בשביל לחשב את הציון המצטבר לכל מועמד. ואז כמו בחישוב המועמדים המנצחים בחוק קופלנד, מבצעים $M(M-1)/2$ השוואות מאובטחות בין הציונים המצטברים בשביל לדרג את המועמדים.

פרטיות חישוב המועמדים המנצחים

סופרי הקולות מחזיקים D' חלקי סוד מתוך D בסכמת שיתוף הסודות של שמיר בכל אחת ממטריצות ההצבעה P_n, לכל אחד מהמצביעים, ובמטריצת הציון המצטבר P. תחת ההנחה של רוב הגון והגדרת הערך $D' = \lfloor (D+1)/2 \rfloor$, סופרי הקולות אינם יכולים לחשב שום ערך במטריצת ההצבעה או במטריצת הציון המצטבר. בחישוב התוצאה הסופית, חלקי הסוד נוצרים רק על הביטים של ההשוואה והם אינם חושפים שום מידע על הערכים שמושווים כפי שפורט בסעיף "השוואה מאובטחת". כל טכניקות ההשוואה שנמצאות בשימוש בחישוב התוצאה מספקות סודיות מושלמת ולכן גם תת-הפרוטוקול לעיל מספק סודיות מושלמת.

9.4 פרטיות הפרוטוקול

המטרה העיקרית ביצירת פרוטוקול בחירות אלקטרוניות היא שמירה על אנונימיות הבוחרים. פרוטוקולים אלה נדרשים לממש תכונה פשוטה - לא ניתן לקשר הצבעה למצביע. הפרוטוקול המוצג במאמר זה משיג מטרה זו מעל ומעבר. כל מצביע יוצר חלקי סוד בסכמת שיתוף הסודות של שמיר ושולח כל חלק לסופר קולות אחר. בשל השימוש בסכמת שיתוף הסודות של שמיר לא רק שלא ניתן לקשר בין מצביע להצבעה שלו אלא סופרי הקולות בכלל לא יכולים להיחשף להצבעות עצמן. כמו כן, סופרי הקולות לא נחשפים לשום תוצאת ביניים, לתוכן מטריצת ההצבעה או למטריצה המצטברת. סופרי הקולות מסיקים את דירוג המועמדים בלבד ומפרסמים אותו. כל זאת תחת ההנחה שמתקיים רוב הגון ויותר מחצי מסופרי הקולות אינם קושרים קשר. כאמור תרחיש של קשירת קשר בין סופרי הקולות אינו סביר ויורד ככל שערכו של D עולה. באופן אידיאלי, סופרי הקולות יהיו אנשים או גופים עם מוניטין חיובי שזוכים לאמון רב בתוך הארגון או המדינה בה הם נמצאים. בגידה באמון זה הניתן להם תגרור פגיעה קשה למוניטין שלהם, לעסק שלהם או תגרור ענישה משמעותית. לכן אפילו לערך D נמוך של 5 למשל, הסיכוי ששלושה סופרי קולות יפרו אמונים הוא קלוש וזניח.

ניתן לממש מערכת דומה המבוססת על שיתוף סודות בשיטת "הכל או כלום", בה צריך שיתוף פעולה של כלל סופרי הקולות (D מתוך D) על מנת לבנות מחדש סודות או לבצע חישובים מרובי משתתפים על סודות אלו. באופן טבעי ככל שנדרוש שיותר סופרי קולות ישתתפו בתהליך הרכבת הסוד, הפרוטוקול יהיה בטוח יותר ובמקרה של "הכל או כלום" יאכוף את הדרישה שכל סופרי הקולות יהיו הגונים. עם זאת לשיטה זו יש חיסרון ברור - צריך את כלל סופרי הקולות בשביל לשחזר את הסוד במלואו. מספיק שיש תקלה במחשב של אחד מסופרי הקולות ונוצר שיבוש משמעותי בבחירות שעלול להוריד את אמון הציבור במערכת.

המסקנה היא שערך גבוה יותר של D אמנם מגביר את בטיחות המערכת מפני קשירת קשר וסופרי קולות לא הגונים אך מצד שני ערכים גבוהים של D גוררים עלויות חישוב ותקשורת גבוהות יותר ודורשות אמון גבוה יותר בסופרי הקולות על מנת שלא ישבשו את מהלך הבחירות.

חשוב לציין שהפרוטוקול מתמקד בחישוב מאובטח של תוצאות הבחירות אבל אינו מספיק בפני עצמו בשביל ליצור בחירות מאובטחות. בשביל לעשות זאת הפרוטוקול צריך להיות משולב במערכת בחירות מאובטחת, בה התקשורת בין המשתתפים מוצפנת, מוודאים שכל מצביע הצביע רק פעם אחת, המחשבים בעזרתם מצביעים מוגנים מפריצות וכו'. לדוגמא תוקף יכול להאזין לתקשורת הנשלחת ממצביע V_n לסופרי הקולות ואם התקשורת איננה מוצפנת, מספיק שינטר את התקשורת ל-D' סופרי קולות הוא יוכל לחשב את מטריצת ההצבעה. ניתן למנוע מתקפות כאלו בקלות ע"י שימוש בהצפנת מפתח פומבי שתוארה לעיל.

לדוגמה מתקפה אפשרית על המערכת היא שמצביע V_n יצותת לתקשורת היוצאת ממצביע אחר V_m אל סופרי הקולות ויחליף את ההצבעה המקורית שלו בהצבעה אחרת. אפשר למנוע מתקפה זו בקלות ע"י הוספת דרישה שכל תקשורת בין מצביעים לסופרי קולות תתבצע באופן מוצפן עם מפתח ציבורי הידוע לשני הצדדים ותהיה חתומה עם מפתח פרטי. בכל קבלה של הודעה יצטרך המקבל לוודא שההודעה שנשלחה נחתמה עם המפתח הפרטי המתאים. כלומר כל הודעה שנשלחת ממצביע כלשהו לסופר הקולות כלשהו תצטרך להיות חתומה עם המפתח הפרטי של המצביע ואז מוצפנת עם המפתח הציבורי של סופר הקולות. בנוסף, אפשר לדרוש שכל סופר קולות ישלח אישור קבלה על כל הצבעה שנשלחה אליו.

9.5 הערכת עלויות

בסעיף זה אנחנו מנסים להעריך כמה פרקטי הפרוטוקול והאם ניתן לממש אותו במערכות בחירות מציאותיות. הפרוטוקול מתבסס על פעולות קריפטוגרפיות יקרות כמו השוואה מאובטחת וחישוב מעגלי כפל מורכבים ולכן יש להעריך עם אילו פרמטרים ניתן לממש את המערכת. יש לציין שניתוח זה יתמקד בפעולות הכבדות ביותר בפרוטוקול, פעולות נוספות שהמצביעים וסופרי הקולות מבצעים, כמו ייצור מספרים אקראיים או פעולות חישוב לא מאובטחות, הן זניחות ביחס לפעולות הקריפטוגרפיות היקרות ולכן נתעלם מהן בחישוב זה.

פרמטרים

ישנם 4 פרמטרים שמשפיעים על ביצועי הפרוטוקול:

1. גודל השדה

יש לציין את הגודל המינימלי של p שמגדיר את השדה Z_p בו מתבצעים כל החישובים באלגוריתם.

המספר הראשוני p צריך להיות גדול מארבעת הערכים הבאים:

1. מספר סופרי הקולות D.
2. 2N - מספר המצביעים כפול 2, על מנת שהערכים ב-P יוכלו להכיל את הציון של מועמדים.
3. הפרמטרים של חוק קופלנד s, t משום שחישוב התוצאה מתבצע בעזרת שיתוף סודות.
4. $2(M-1)$, משום שבזמן וידוא מטריצת ההצבעות Q, סופרי הקולות צריכים לבדוק האם ההפרש $Q_m - Q_m$, שווה לאפס, וההפרש יכול להיות שווה לכל היותר $2(M-1)$ בחוק קופלנד.

משום שברוב המקרים s, t, D, M נמוכים משמעותית מ-N, ניתן לקבוע ש-N2 הוא החסם התחתון לערך של p. נבחר הערך $p = 2^{31} - 1$ שמספיק לכל תרחיש בחירות מציאותי, משום שמספר זה הוא מספר

מרסן (mersenne, מספר ראשוני מהצורה $2^t - 1$ למספר t שלם וחיובי) שמאפשר חישוב כפל של שני מספרים בשדה בצורה יעילה יותר וללא צורך בחילוק.

2. מספר סופרי הקולות **D**

נבחן את הביצועים של הערכים הבאים: 3,5,7,9. כאמור לעיל, ערכים גבוהים יותר יספקו אבטחה גבוהה יותר אך גם עלויות חישוב גבוהות יותר.

3. מספר המועמדים **M**

חוקי הצבעה מבוססי סדר דורשים מכל בוחר לספק רשימה מלאה של סידור המועמדים לפי בחירתו. יצירת סדר מלא בין כלל המועמדים בבחירות יכולה להיות משימה לא פשוטה עבור מצביע ממוצע ולכן דרך אלטרנטיבית ליצור רשימה כזו היא ע"י השוואת זוג מועמדים בכל פעם. כלומר המצביע נשאל בכל פעם איזה מועמד הוא מעדיף מבין שני מועמדים. במקרה זה מספר השאלות האלו הוא בערך $log_2(M!)$

לכן בשני המקרים ברור שמספר המועמדים צריך להיות קטן. הערכים שנבחרו הם $M \in \{5,10,20\}$

4. מספר המצביעים **N**

ככל שמספר המצביעים עולה כך עולה זמן וידוא ההצבעות. וידוא ההצבעות מתבצע באצוות מגודל B ולכן בפרק זה מפורטות עלויות החישוב לאצוות מגודל $B \in \{500, 5000, 25000\}$. בשביל לקבל את זמני הריצה המלאים לוידוא הצבעות יש להכפיל ב-N/B.

עלות וידוא הצבעות

כפי שתואר לעיל בסעיף "וידוא הצבעות", וידוא אצווה של B הצבעות דורשת $BM(M-1)/2$ פעולות כפל מקביליות לוידוא תנאי 1, ונדרשות $M(M-1)/2$ פעולות כפל סדרתיות בשביל לוודא את תנאי 4. ניתן לבצע את שתי הפעולות האלו במקביל ע"י ביצוע $BM(M-1)/2$ פעולות הכפל של וידוא תנאי 1 על פני $M(M-1)/2$ סיבובים עם B שערי כפל בכל סיבוב. לכן סך כל זמן הריצה של וידוא אצווה של B הצבעות היא $M(M-1)/2$ סיבובים עם $2B$ פעולות כפל מקביליות בכל סיבוב.

במאמר [PIK93] של צ'ידה (Chida) בוצע ניסוי על זמני ריצה של פעולות כפל מאובטחות. על מנת להעריך את זמן הריצה של ביצוע פעולות ההשוואה, נעשה שימוש במכונות AWS מסוג m5.4xlarge באיזור צפון וירג'יניה על רשת עם רוחב פס של 9.6 ג'יגהביט לשנייה. ההגדרות היו מעט שונות וכמובן שאפשר להשתמש בחומרה חזקה יותר אבל ניתן להשתמש במספרים אלו בתור חסם עליון לזמני הריצה של הפרוטוקול. הניסויים התבצעו על שדה גדול יותר $(p' = 2^{61} - 1)$ שבו פעולות כפל לוקחות יותר זמן מאשר גודל השדה שהוגדר מעלה $p = 2^{31} - 1$. את שאר הפרמטרים נתאים כך שיהיו זהים

לפרמטרים של הפרוטוקול. במאמר של צ'ידה התנסו בפריסת מיליון שערי כפל על פני $\{20,100,1000\}$ שכבות. לכן בכל שכבה היו $\{5 \cdot 10^4, 10^4, 10^3\}$ שערי כפל בהתאמה. זמני הריצה כפונקציה של D מוצגים בטבלה הבאה

מספר השכבות	מספר שערי הכפל בכל שכבה	D=3	D=5	D=7	D=9
20	50000	826	844	1058	1311
100	10000	842	989	1154	1410
1000	1000	1340	1704	1851	2243

על מנת לחשב $B = 500$ הצבעות עם $M = 20$ יש לבצע $M(M-1)/2 = 190$ סיבובים עם $2B =$ 1000 פעולות כפל מקביליות בכל סיבוב. ניתן לראות בטבלה שבשורה מספר 3 ישנם 1000 שערי כפל בכל שכבה ולכן שורה זו מתאימה למקרה זה. עם זאת מספר השכבות הנדרשות הוא רק 190 ולא 1000, לכן ניתן להכפיל את זמני הריצה ב- $190/1000$ ולקבל את זמן הריצה המשוער. כמו כן, ניתן להכפיל את זמני הריצה שקיבלנו ל-500 הצבעות לכל תרחיש בחירות שהוא. אם נרצה לקבל את זמני הריצה לבחירות עם מיליון מצביעים נכפיל את זמני הריצה ב-$1000000/500$. לכן במקרה זה זמני הריצה לוודא מיליון הצבעות עם $D \in \{3,5,7,9\}$ יהיו שווים ל-$510, 648, 704, 852$ שניות בהתאמה. כמובן ככל שנגדיל את גודל האצוות כך נוכל למקבל יותר פעולות, להוריד את מספר השכבות ולהוריד את זמני הריצה. לדוגמה אם נבחר $B = 25000$ הצבעות עם $M = 20$ נוכל לחשב את זמני הריצה מתוך שורה 1 בטבלה, שמספקת את זמן הריצה לחישוב 50000 שערי כפל במקביל. נכפול שוב את בגורם שייתן לנו את מספר השכבות רצוי $190/20$ ונקבל שוידוא של מיליון הצבעות כאשר גודל האצווה היא 25000 ייקח 314, 321, 402, 498 שניות כאשר מספר סופרי הקולות הוא 3, 5, 7, 9 בהתאמה.
משום שבחירות לרוב לוקחות יום אחד לפחות ניתן לראות שזמני הריצה הנ"ל זניחים ולא גורמים שום עיכוב למהלך הבחירות.

עלות חישוב התוצאה הסופית

כפי שתואר בסעיף "חישוב מאובטח מרובה משתתפים של המועמדים המנצחים" העלות הכוללת של חישוב התוצאה הסופית הוא לכל היותר $K \cdot (M - \frac{K+1}{2})$ השוואות מאובטחות. ניתן לחסום ערך זה מלמעלה ע"י $M(M-1)/2$. משום שניתן לחסום מלמעלה את זמן הריצה של שוויון לאפס ע"י העלות

של השוואה מאובטחת ניתן לשים חסם עליון נוסף של $4M(M-1)$. בשביל להעריך את זמני הריצה השתמשו בקונפיגוריצה זהה לזו של המאמר של צ'ידה עם מכונות AWS מסוג m5.4xlarge באיזור צפון וירג'יניה על רשת עם רוחב פס של 9.6 ג'יגהביט לשנייה.

סופרי קולות	D=3	D=5	D=7	D=9
זמן לחישוב השוואה מאובטחת	9.07	9.54	9.64	15.0

כפי שניתן לראות בטבלה, זמני הריצה זניחים. לדוגמה כאשר $M = 5$ זמן הריצה של חישוב התוצאה חסום ע"י 1.2 שניות בלבד. כאשר $M = 20$ ו-$D = 9$ זמן הריצה הוא 22.8 שניות. זמני הריצה בחוק מקסימין אפילו קטנים יותר משום שיש לבצע פחות השוואות מאובטחות. בכל תרחיש בחירות עלויות אלו זניחות לעומת העלויות של וידוא ההצבעות ובכל מקרה בחירות לרוב לוקחות יום אחד לפחות שבסופו ספירת הקולות לוקחת לפחות כמה שעות ולכן זה בכל מקרה שיפור לעומת המצב הקיים כיום.

9.6 חוקים מבוססי סדר אחרים

קמני-יאנג (**Kemney-young**)

בחוק זה שולח כל מצביע דירוג מלא של רשימת המועמדים בתור מערך בגודל M, שבו כל כניסה m היא הדירוג של המועמד, כאשר 1 הוא הדירוג הגבוה ביותר. בשיטה זו יכול להתקיים תיקו בין מועמדים לכן הדירוג הנמוך ביותר הוא לא בהכרח M. לדוגמה אם יש חמישה מועמדים הדירוג שלהם יכול להיות $[1,2,3,4,4]$.

את המערך הזה אפשר לתרגם למטריצה $P_n \in \{0,1\}^{M\times M}$ כאשר כל כניסה $(m,l)=1$ אם המועמד C_m מדורג גבוה ממש ממועמד C_l ו-0 אחרת.

סופרי הקולות סוכמים את כל מטריצות ההצבעה האלו למטריצה P_n כך שכל כניסה $P=\sum_{n\in[N]}$ במטריצה $P(m,l), 1\le m\neq l\le N$ מכילה את מספר המצביעים שדירגו את המועמד C_m גבוה יותר מאשר המועמד C_l .

מכאן שסכום כל שורה הוא הציון המצטבר של כל מועמד כאשר ציון גבוה יותר אומר שהמועמד מדורג גבוה יותר. (באותו אופן ניתן לסכום עמודות והמועמדים המנצחים הם אלה עם הדירוג הנמוך יותר).

מימוש מאובטח של חוק קמני-יאנג

באופן דומה לחוקי קופלנד ומקסימין, כל מועמד שולח חלקי סוד במטריצת ההצבעה שלו לכל אחד מסופרי הקולות. כל מצביע יוצר חלקי סוד לכל אחת מהכניסות במטריצה למעט האלכסון הראשי.
על מנת לוודא את שהמטריצה תקינה על סופרי הקולות לבדוק שכל הכניסות הן 0 או 1 וסכום כל זוג כניסות של אינדקסים לא שווים הוא אחד. ניתן לבצע בדיקות אלו באופן דומה מאוד לאלו של חוקי קופלנד ומקסימין כפי שמפורט בסעיף "השוואות מאובטחות".
לאחר וידוא ההצבעות, כל סופר קולות בנפרד מחבר את חלקי הסוד בכל הכניסות במטריצה למעט האלכסון ולבסוף סופרי הקולות מבצעים השוואות מאובטחות על מנת למצוא את המועמדים המנצחים.

דירוג מודאלי

בדירוג מודאלי כל מועמד יוצר סידור מלא של כלל M המועמדים מתוך C לפי בחירתו, ללא תיקו בין זוג מועמדים.

הקבוצה R_C מכילה את כל $M!$ הדירוגים האפשריים וההצבעה היא למעשה בחירה של דירוג יחיד מתוך קבוצה זו. בשלב חישוב המועמדים המנצחים ניתן לשקלל כל פרמוטציה ומספר המצביעים שבחרו בה וכך למצוא את המועמדים המנצחים. למרות שדירוג מודאלי הוא חוק הצבעה מבוסס סדר ולא מבוסס ציון, אופן החישוב שלו שקול לחוק הריבוי שמפורט עליו המאמר הקודם בעבודה זו.

10. מקורות

[ASV08] Alwen, J., Shelat, A., & Visconti, I. (2008). Collusion-free protocols in the mediated model. In CRYPTO (pp. 497-514).

[BE15] Benkaouz, Y., & Erradi, M. (2015). A distributed protocol for privacy preserving aggregation with non-permanent participants. Computing, 97, 893-912.

[Blu83] Blum, M. (1983). Coin flipping by telephone a protocol for solving impossible problems. ACM SIGACT News, 15(1), 23-27.

[BS05] Brandt, F., & Sandholm, T. (2005). Decentralized voting with unconditional privacy. In Autonomous agents and multiagent systems (pp. 357-364).

[Ben86] Benaloh, J. (1986). Secret sharing homomorphisms: Keeping shares of a secret secret. In CRYPTO (pp. 251–260).

[Ben87] Benaloh, J. (1987). Verifiable Secret-Ballot Elections. Technical Report MSR-TR-1987-1

[Bla79] Blakley, G. (1979). Safeguarding cryptographic keys. In International Work-shop on Managing Requirements Knowledge (pp. 48:313–317).

[CCJ+14] Chen, C. L., Chen, Y. Y., Jan, J. K., & Chen, C. C. (2014). A secure anonymous e-voting system based on discrete logarithm problem. Applied Mathematics & Information Sciences, 8(5), 2571.

[CF85] Cohen, J. D., & Fischer, M. J. (1985). A robust and verifiable cryptographically secure election scheme (pp. 372-382). Yale University. Department of Computer Science.

[CGH+18] Chida, K., Genkin, D., Hamada, K., Ikarashi, D., Kikuchi, R., Lindell, Y., & Nof, A. (2018). Fast large-scale honest-majority MPC for malicious adversaries. In CRYPTO (pp. 34–64).

[CGS97] Cramer, R., Gennaro, R., & Schoenmakers, B. (1997). A secure and optimally efficient multi-authority election scheme. European transactions on Telecommunications, 8(5), 481-490.

[CGY22] Cortier, V., Gaudry, P., & Yang, Q. (2022). A toolbox for verifiable tally-hiding e-voting systems. In Computer Security (pp. 631-652).

[CL06] Chang, C. C., & Lee, J. S. (2006). An anonymous voting mechanism based on the key exchange protocol. Computers & Security, 25(4), 307-314.

[CPS+18] Canard, S., Pointcheval, D., Santos, Q., & Traoré, J. (2018). Practical strategy-resistant privacy-preserving elections. In European Symposium on Research in Computer Security (pp. 331–349).

[Cha81] Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84-90.

[Cha83] Chaum, D. (1983). Blind signatures for untraceable payments. In Advances in Cryptology: Proceedings of Crypto 82 (pp. 199-203). Springer US.

[Cha88] Chaum, D. (1988, May). Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA. In Eurocrypt (Vol. 98, pp. 177-182).

[Cop51] Copeland, A. H. (1951). A reasonable social welfare function. USA: Mimeo, University of Michigan.

[DH76] - Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22, no. 6 (1976): 644-654.

[DJN10] Damgård, I., Jurik, M., & Nielsen, J. B. (2010). A generalization of Paillier's public-key system with applications to electronic voting. International Journal of Information Security, 9, 371-385.

[EFL+17] Elkind, E., Faliszewski, P., Laslier, J.-F., Skowron, P., Slinko, A., & Talmon, N. (2017). What do multiwinner voting rules do? an experiment over the two-dimensional euclidean domain. In AAAI.

[FOO92] Fujioka, A., Okamoto, T., & Ohta, K. (1992). A practical secret voting scheme for large scale elections. In International Workshop on the Theory and Application of Cryptographic Techniques (pp. 244-251).

[FSS+17] Faliszewski, P., Skowron, P., Slinko, A., & Talmon, N. (2017). Multiwinner voting: A new challenge for social choice theory. Trends in computational social choice, 74(2017), 27-47.

[HHK+21] Hertel, F., Huber, N., Kittelberger, J., Küsters, R., Liedtke, J., & Rausch, D. (2021). Extending the tally-hiding ordinos system: implementations for Borda, Hare-Niemeyer, Condorcet, and instant-runoff voting. Cryptology ePrint Archive.

[HPT20] Haines, T., Pattinson, D., & Tiwari, M. (2020). Verifiable homomorphic tallying for the Schulze vote counting scheme. In Verified Software. (pp. 36-53).

[IK91] Iversen, K. R. (2001). A cryptographic scheme for computerized general elections. In Advances in Cryptology—CRYPTO'91: Proceedings (pp. 405-419).

[KLM+20] Küsters, R., Liedtke, J., Müller, J., Rausch, D., & Vogt, A. (2020, September). Ordinos: a verifiable tally-hiding e-voting system. In 2020 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 216-235). IEEE.

[Kra77] Kramer, G. H. (1975). A dynamical model of political equilibrium.

[NBK15] Nair, D. G., Binu, V. P., & Kumar, G. S. (2015). An improved e-voting scheme using secret sharing based secure multi-party computation. arXiv preprint arXiv:1502.07469.

[NO07] Nishide, T., & Ohta, K. (2007). Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In PKC (pp. 343–360).

[Nao89] Naor, M. (2001, July). Bit commitment using pseudo-randomness. In Advances in Cryptology—CRYPTO'89 Proceedings (pp. 128-136).

[PAB+04] Peng, K., Aditya, R., Boyd, C., Dawson, E., & Lee, B. (2005). Multiplicative homomorphic e-voting. In INDOCRYPT (pp. 61-72).

[PIK93] Park, C., Itoh, K., & Kurosawa, K. (1993). Efficient anonymous channel and all/nothing election scheme. In EUROCRYPT (pp. 248–259).

[Pai99] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In EUROCRYPT (pp. 223–238).

[RSA78] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[Sha79] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

[Sim69] Simpson, P. B. (1969). On defining areas of voter choice: Professor tullock on stable voting. The Quarterly Journal of Economics, (pp. 478–490).

Abstract

Democratic elections have existed for over 3000 years, since the rise of the world's first democracy in ancient Athens. Until these days most countries in the world use democratic elections to elect a president. In most countries, elections are carried out in the traditional way without computer involvement in the voting or tallying processes. The voters have to come to a certain location where the voting takes place. Voting is done by inserting a ballot or an envelope into the ballot box and the counting is done manually. Having such elections poses many challenges and disadvantages - high costs, enforcing election laws, preventing attempts to tamper the elections, the time it takes to tally the votes, the environmental damage and a complex operation.

With the rise of technology and the Internet in recent years, electronic elections seem to be the natural evolution of voting system and a way of overcoming these challenges. Up until now 37 different countries have incorporated various digital means into their elections process. Each country employed different means - ballot machines, centralized tallying and completely online voting processes. Although electronic elections make the physical ballot stations redundant, solve many of the logistical challenges and reduce costs, they pose additional challenges.

In this paper, we will focus on a vital aspect of democratic elections - the secrecy and safety of the elections. We will discuss different cryptographic techniques and protocols that maintain the privacy of the votes through all stages of the election process and prevent forgeries, biases and changes to the final result.

The Open University of Israel

Department of Mathematics and Computer Science

Cryptography based secure elections

Thesis submitted as partial fulfillment of the requirements
towards an M.Sc. degree in Computer Science
The Open University of Israel
Computer Science Division

By
Tom Leibovich

Prepared under the supervision of Prof. Tamir Tassa

March 2023