НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК 519.21

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“15” травня 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика»

на тему: Модифікація та аналіз криптографічних методів захисту протоколів електронного голосування

Виконав (-ла): студент (-ка) 2 курсу, групи _____ФІ-63М_____
(шифр групи)

Пекарчук Ніні Андріївна

Керівник д.ф.-м.н. Савчук М.М.

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.ф.-м.н Хом’як О.М.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

РЕФЕРАТ

Робота обсягом 71 сторінку містить 8 рисунків, 2 таблиці та 14 літературних посилань.

Метою роботи є створення нових альтернативних протоколів, як модифікацій вибраної існуючої схеми електронного голосування з максимальним усуненням її недоліків. Основою для їх створення слугують результати дослідження криптографічних примітивів та виконання вимог, поставлених до процесу голосування, в залежності від використання тих чи інших криптографічних блоків у схемі.

Об'єктом дослідження в даній роботі є інформаційні процеси в системах електронного голосування.

Предметом дослідження є алгоритми та протоколи електронного голосування.

Базуючись на результатах проведеного порівняльного аналізу наявних схем електронного голосування, у роботі запропоновано два варіанти модифікації вибраного протоколу з усуненням проблеми порушення конфіденційності голосу.

Результати роботи можуть бути використані в якості моделі для практичної реалізації програмних продуктів відповідного призначення в межах визначених сфер їх ефективного використання.

ЕЛЕКТРОННЕ ГОЛОСУВАННЯ, ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ, КРИПТОГРАФІЧНІ АЛГОРИТМИ, АНОНІМНИЙ КАНАЛ ЗВ'ЯЗКУ, ГОМОМОРФНЕ ШИФРУВАННЯ, КРИПТОСИСТЕМА RSA.

ABSTRACT

This work consists of 71 pages, includes 8 illustrations, 2 tables and 14 literature references.

The aim of this qualification work is to create new alternative protocols, as modifications of the selected existing electronic voting scheme with maximum elimination of its drawbacks. The results of the study about basic cryptographic primitives and fulfillment of the requirements set for the voting process, depending on use of certain cryptographic units in the scheme create the foundation for practical implementation of modern protocols.

The object of the work is information processes in electronic voting systems.

The subject of the work is algorithms and e-voting protocols.

Based on the results of a comparative analysis of existing electronic voting schemes, two variants of modification of the selected protocol were proposed in the work, with the elimination of violation of the voting confidentiality.

The results might be used as models for the practical implementation of software products in the field of electronic voting within defined areas of their effective use.

E-VOTING, ELECTRONIC VOTING, E-VOTING PROTOCOLS, CRYPTOGRAPHIC ALGORITHMS, ANONYMOUS CHANNEL, HOMOMORPHIC ENCRYPTION, RSA CRYPTOSYSTEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

N — загальна кількість виборців у схемі голосування.

V_i — i-й виборець.

v_i — секретний голос i-го виборця.

M – загальна кількість органів влади у схемі голосування.

A_j — j-й орган влади.

t — мінімальна кількість гарантовано чесних владних органів у схемі.

$E_K(m)$ — шифрування повідомлення m ключем K.

$D_K(c)$ — розшифрування шифртексту c ключем K^{-1}.

$x \in_R S$ — x обрано з множини S випадково та рівноймовірно.

$gcd(a, b)$ — найбільший спільний дільник чисел a та b.

ВСТУП

Актуальність роботи. Можливість вільного волевиявлення є основним виявом будь-якого демократичного суспільства, а системи електронного голосування в свою чергу слугують соціальним застосуванням криптографічних методів захисту процесу голосування. Дана робота присвячена дослідженню сучасних криптографічних досягнень у сфері електронного голосування.

Дослідження протоколів електронних виборів є актуальною задачею, оскільки запровадження ефективних схем електронного голосування дає можливість забезпечити спрощення процесу голосування, а отже, в результаті збільшити рівень залучення виборців, водночас знизивши використання як людських, так і матеріальних ресурсів, необхідних для їх підготовки та проведення. Прозорі схеми голосування сприяють зменшенню можливостей корумпування органів влади та підкупу голосів виборців.

Метою роботи є створення нових альтернативних протоколів, як модифікацій вибраної існуючої схеми електронного голосування з максимальним усуненням її недоліків. Основою для їх створення слугують результати дослідження криптографічних примітивів та виконання вимог, поставлених до процесу голосування, в залежності від використання тих чи інших криптографічних блоків у схемі.

У ході дослідження ставляться наступні **завдання**:

– дослідження типового сценарію виборчого процесу, вимог до протоколів електронних виборів, криптографічних примітивів, що використовуються для їх побудови та розробки практичних і безпечних схем електронного голосування.

– аналіз ефективності та практичності різних існуючих схем електронного голосування, їх категоризація, виокремлення основних переваг та критичних функцій безпеки кожного типу схем та відповідний

опис криптографічних методів їх забезпечення.

– створення власних альтернатив вибраному існуючому протоколу голосування, розроблених для коригування його основних недоліків.

– проведення чисельного дослідження потенційних можливостей масштабування запропонованих схем та, відповідно, можливих сфер їх практичного застосування.

Методи дослідження: методи математичного моделювання, системного аналізу, теоретико-числових алгоритмів, теорії чисел та обрахунки на ЕОМ.

Об'єкт дослідження: інформаційні процеси в системах електронного голосування.

Предмет дослідження: алгоритми та протоколи електронного голосування.

Наукова новизна одержаних результатів визначається розробкою двох нових альтернативних модифікацій вибраного існуючого протоколу електронного голосування, що забезпечують покращені показники відповідності основним вимогам, поставленим до протоколів електронних виборів.

Практичне значення одержаних результатів. Запропоновані в роботі модифікації протоколу електронного голосування є готовими моделями для практичної реалізації програмних продуктів відповідного призначення. Отримані результати оцінки потенційної масштабованості схем дозволяють визначають можливі сфери їх ефективного застосування зі збереженням виконання основних критичних функцій безпеки.

1 МОДЕЛЬ ПРОЦЕДУРИ ГОЛОСУВАННЯ. ПРОТОКОЛИ ЕЛЕКТРОННИХ ВИБОРІВ

Процедура голосування як формальна процедура прийняття людьми участі у громадсько-політичному житті є однією з основ забезпечення демократичного суспільства. У порівнянні із традиційним паперовим форматом виборів, електронне голосування є потенційно більш ефективним, точним та швидким, а також забезпечує зручність голосування без територіальної прив'язки до конкретних дільниць. Завдяки цим перевагам, процедура голосування в даний час переходить від ручного паперового процесу обробки до автоматичного електронного аналога.

Термін "електронне голосування" означає процес визначення, збору та розповсюдження волевиявлення учасників голосування з використанням певних електронних засобів в процесі голосування.

На сьогодні процедура голосування має надзвичайно широкий спектр застосувань, починаючи з застосування в телевізійних шоу і закінчуючи прийняттям закону в парламенті. Найбільш важливим, впливовим та розповсюдженим використанням цього механізму є його застосування у національних виборах.

Використання процедури електронного голосування дозволяє зменшити вплив людського фактора на процес, а механізм їх проведення не потребує фізичної присутності виборця на дільниці, що надає можливість взяти участь у виборах солдатам, мандрівникам, а також значно полегшує цю процедуру для людей з обмеженими фізичними можливостями.

Для будь-якого типу голосувань, існують мотиви для шахрайства задля отримання політичної, фінансової або особистої вигоди. Загроза шахрайства чи підробки голосу зростає разом із масштабом виборів, а

відповідно і мірою впливовості результатів голосування. Тому голосування повинне відбивати істинне волевиявлення учасників, а отже задача електронного голосування – забезпечити ефективну заміну традиційним паперовим виборам зі збереженням виконання усіх необхідних вимог за допомогою криптографічних методів захисту.

1.1 Типовий сценарій виборчого процесу. Вимоги до протоколів електронних виборів

У типовому сценарії процедури голосування виділяють п'ять основних етапів. Загальна схема цього процесу зображена на рисунку 1.1.

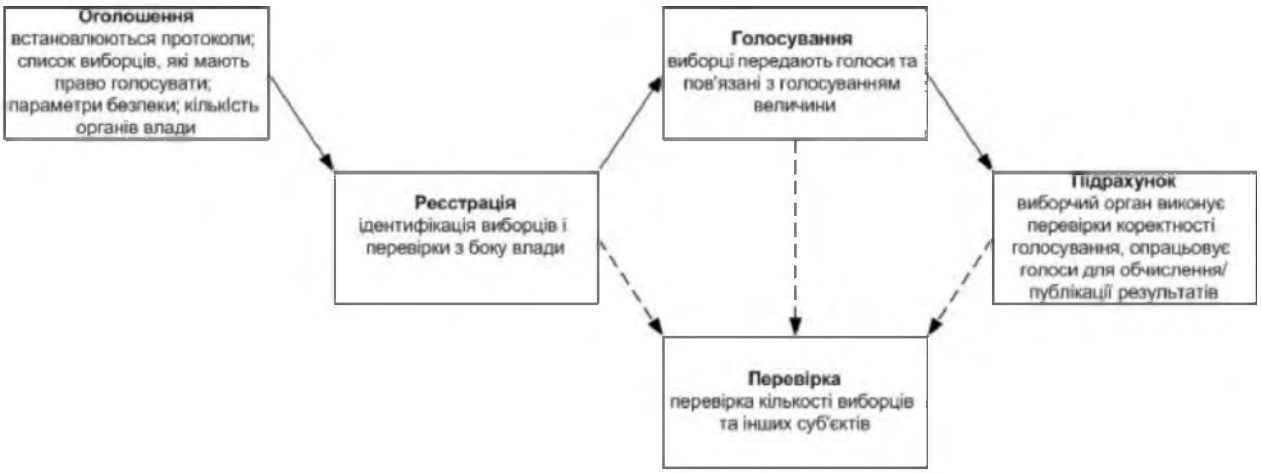

Рисунок 1.1 – Схема процедури голосування

На етапі *налаштування (Set-up phase)* встановлюються параметри голосування. До основних параметрів належать критерії прийняття кандидатів, виборців та органів влади; процедура голосування; критерії дійсності виборчого бюлетеня; правила підрахунку голосів (підбиття підсумків голосування). Кандидати реєструють себе в відповідальних

органах, після чого чинні параметри голосування, кандидати та органи влади розголошуються.

На етапі *реєстрації (Registration phase)* виборцям необхідно зареєструватись в визначених органах реєстрації. Критерії прийняття визначаються з попереднього пункту. Особам, що не відповідають цим критеріям, заборонено брати участь у голосуванні. Список підтверджених виборців розголошується для забезпечення публічної верифікації.

На етапі *голосування (Voting phase)* зареєстрованим виборцям дозволяється брати участь у голосуванні, дотримуючись наступних правил:

– Кожен виборець зобов'язаний бути автентифікованим відповідно до списку зареєстрованих виборців з етапу реєстрації. Особам, не зазначеним у цьому списку, заборонено брати участь у голосуванні.

– Кожен з аутентифікованих виборців отримує порожній бюлетень і фіксує свій голос в бюлетені всередині фізично приватного та безпечного місця для уникнення примусу.

– Виборчий бюлетень повинен бути анонімним – відповідність виборця та його голосу засекречена.

На етапі *обрахунку голосів (Tally phase)* всі бюлетені оброблюються для визначення результатів голосування. Етап складається зі збору голосів, верифікації бюлетенів (відповідно до правил, встановлених на етапі налаштування), обрахунку голосів та оприлюднення отриманих результатів.

Окремим особливим етапом процедури голосування є *перевірка (Check)*. Цей етап може бути використаний декілька разів після етапів реєстрації, голосування або підрахунку для здійснення перевірки необхідних параметрів відповідно до обраної схеми голосування.

Учасниками протоколу електронних виборів традиційно є виборці та органи влади. Усі учасники можуть контактувати один з одним за допомогою каналів зв'язку. Дії виборця під час електронного голосування повинні бути зведені до мінімуму, а протокол голосування повинен

передбачати, що виборець володіє обмеженими часовими та обрахунковими потужностями.

Органи влади керують процесом вибрів, відповідно, потенційно володіють значними обчислювальними потужностями і здатні зберігати значну кількість інформації. Кількість органів влади в різних протоколах може відрізнятись, однак зазвичай автори протоколів відмовляються від виділення єдиного такого органу, через ризикованість перенесення всієї відповідальності на єдиний центр. Протоколи електронного голосування також повинні враховувати можливу корумпованість певної кількості владних органів, кожен учасник повинен розраховувати, що принаймні певна кількість з них є гарантовано чесними.

Структура голосу залежить від типу голосування, а точніше від питання, поставленого виборцям, та можливих варіантів відповіді на нього. Найбільш розповсюдженими є такі види голосів: так/ні (yes/no voting), вибір одного з L варіантів (1-out-of-L voting), вибір K з L варіантів (K-out-of-L voting), власний варіант (write-in voting).

Визначення 1.1. Нехай кожен з учасників багатостороннього протоколу - виборців V_i виробляє свій секрет v_i. Обчислення функції f, що залежить від цих величин, без розголошення жодної з них, однак з подальшим розголошенням результуючого значення функції f називається *електронним голосуванням* [1]. Схема голосування передбачає всі дії та розрахунки виборця та органів влади під час процесу голосування.

Загальність виборчого права є основним принципом демократичних виборів. Брати участь у виборах мають право всі громадяни, що відповідають вимогам виборчого права держави, голоси усіх виборців є рівними і в процесі голосування повинна зберігатись таємниця голосування.

Виходячи з цих основних принципів, схема електронних виборів повинна відповідати таким вимогам [2]:

1) *Правомірність голосу (Eligibility).* Незалежно від схеми виборів,

право голосу мають лише авторизовані виборці. Механізмами, що забезпечують правомірність голосу, є реєстрація правомірних виборців як суб'єктів, що проходять під певний, попередньо встановлений на етапі налаштування набір критеріїв, та їх ідентифікація на момент реєстрації. Правомірність голосу також означає неможливість зарахування більше ніж одного голосу від єдиного виборця.

2) *Конфіденційність (Privacy).* Конфіденційність означає секретність кожного окремого голосу виборця, тобто бюлетень не повинен давати жодної можливості певним чином дізнатись особу виборця або прослідкувати зв'язок з його голосом. Інформаційно-теоретичну приватність досягається, якщо виборчі бюлетені виборців є не розрізнювальними, незалежно від будь-яких криптографічних припущень. В іншому випадку вважається, що досягнуто обчислювальну приватність. Окрім цього, конфіденційність голосу повинна забезпечувати відсутність можливості дублювати голоси інших виборців, навіть без викриття їх значень.

3) *Перевірність голосу (Verifiability).* Виборець повинен мати змогу перевірити коректність інтерпретації свого голосу, а також його врахування на етапі підрахунку результатів. Виділяють два різновиди перевірності голосу.

Можливість індивідуальної перевірки голосу (Individual verifiability), що означає, що лише сам виборець має можливість перевірити врахування свого голосу при підрахунку (підсумки виборів підведені коректно).

Можливість загальної перевірки голосу (Universal verifiability) в свою чергу означає, що після розголошення результатів будь-який учасник або пасивний спостерігач може перевірити справедливість виборів, а саме підтвердити те, що опублікований остаточний результат дійсно отримано з урахуванням усіх голосів.

4) *Справедливість (Fairness).* Жоден учасник не може отримати жодних знань про оцінки (в тому числі часткові) до етапу підрахунку, оскільки знання часткового співвідношення результатів може вплинути

на наміри виборців, які ще не проголосували. Схема повинна працювати коректно в умовах, коли деякі з її учасників є зловмисниками.

5) *Неможливість підробки голосу (Receipt-freeness, incoercibility).* Виборець не повинен мати змоги переконати будь-якого спостерігача, як саме він проголосував. Ця вимога запобігає купівлі голосів та примусу. Схема надає виборцю можливість відкривати його голос будь-яким бажаним способом.

Вимога перевірності голосу означає наявність зв'язку виборця з його голосом, тим самим при практичних реалізаціях напряму суперечить вимозі конфіденційності та неможливості підробки.

6) *Точність (Accuracy).* Голоси повинні бути правильно опрацьовані та обраховані при підбитті результатів. Голоси неправомірних громадян не повинні враховуватись в голосуванні. Вимога загальної перевірності голосу напряму пов'язана з вимогою точності.

1.2 Криптографічні примітиви протоколів електронного голосування

Для задоволення різних вимог безпеки в протоколах голосування використовуються певний набір криптографічних примітивів та модулів. Розглянемо короткий опис основних з них [4].

Протокол розподілу секрету (Secret Sharing Scheme)

Протокол розподілу секрету використовується в схемах електронного голосування для забезпечення надійності відносно корумпованих владних органів або несправностей їхнього функціонування.

Основна ідея схеми полягає в тому, щоб розділити секрет s між N органами влади, так, щоб будь-який набір з не менше, ніж $(t+1)$ органу влади здатен відновити s, а будь-який набір з не більше, ніж t органів влади

не може отримати жодної інформації щодо s. Розподіл секрету зазвичай засновано на інтерполяції поліному.

Прикладом схеми розподілу секрету є $(t + 1,\ N)$ схема Шаміра (Shamir) [14]. Схема вимагає наявності довіреної сторони, що проводить протокол розподілу секрету: створює особистий ключ $s = K^{-1}$, публікує його і генерує N часток секрету. Кожен орган влади отримує власну частку від довіреної сторони. Таким чином секретний ключ захищено від можливої змови t корумпованих органів. В схемах голосування в якості довіреної сторони може виступати незалежний спостерігач або один з виборців.

Для схеми розподілу секрету з можливістю перевірки (verifiable secret sharing scheme, Chor, 1985) в якості довіреної сторони виступають самі органи влади розподіленим чином. Лише всі N центрів можуть підтвердити чинність протоколу, таким чином схема вимагає залучення більших обчислювальних потужностей та широкого використання каналів комунікації.

У загально перевірних схемах розподілу секрету (publicly verifiable secret sharing scheme, Shoenmakers) будь-який сторонній спостерігач має змогу перевірити коректність протоколу на будь-якому його етапі.

Сліпий підпис (Blind Signatures) Криптографічний протокол сліпого підпису використовується у схемах електронного голосування для анонімізації голосу – від'єднання виборчого бюлетеня від автентифікованого правомірного виборця. Протокол сліпого підпису дозволяє виборцю отримати підпис владного центру на свій виборчий бюлетень, не порушуючи при цьому таємницю голосування.

Відповідно до вимог протоколу, підпис повинен були дійсним (лише власник підпису має право його використовувати) і підлягати публічній перевірці (будь-хто може перевірити істинність вказаного підпису до повідомлення).

У загальному вигляді протокол сліпого підпису утворює наступна послідовність дій:

1) Виборець V засліплює свій голос v, використовуючи випадкові дані r та відкритий ключ органу влади K_A: $BV = blind(v,r,K_A)$, підписує, використовуючи свій особистий ключ $K_{V^{-1}}$: $sign_V(BV,\ K_{V^{-1}})$ і надсилає A.

2) A перевіряє чинність V (шляхом перевірки підпису), потім підписує BV власним особистим ключем $K_{A^{-1}}$: $sign_A(BV,\ K_{A^{-1}})$ і надсилає назад до V.

3) V перевіряє підпис A і отримує $sign_A(v,\ K_{A^{-1}})$.

Протоколи інтерактивних доведень (Interactive proofs):

У протоколах інтерактивного доведення учасник P взаємодіє з учасником V, для доведення певного твердження S. Результатом протоколу є відповідь V – прийняття або відхилення доведення P.

Якщо в ході такого протоколу P не відкриває жодної інформації про секрет, такий протокол називається *доведенням з нульовим розголошенням (zero-knowledge proof).*

Такі доведення володіють властивостями повноти (якщо перевірка є чесною, тобто твердження є істинним, тоді верифікатор повинен прийняти доведення), стійкості (якщо перевірка є нечесною, тобто твердження є хибним, тоді верифікатор повинен зі значною ймовірністю відхилити доведення. "нульові знання якщо, незалежно від того, що є верифікатором.

У протоколах голосування інтерактивні доведення з нульовим розголошенням використовуються на багатьох етапах: між владними органами для доведення власної чесності, або між владою та виборцями, наприклад, для підтвердження правдивості обрахунку голосів (Universal Verifiability), тощо.

Гомоморфне шифрування (Homomorphic Encryption)

Визначення 1.2. Алгоритм шифрування E_K називається *гомоморфним*, якщо для даних $E_K(m_1)$ та $E_K(m_2)$ можливо отримати значення $E_K(m_1 \odot m_2)$ для певної операції $\odot$, без безпосереднього розшифрування окремих значень m_1 та m_2.

Властивість гомоморфізму особливо корисна для схем електронного голосування, оскільки надає можливість застосовувати операції до наборів зашифрованих виборчих бюлетенів без необхідності їх розшифрування, а отже без порушення таємниці голосування.

В результаті об'єднання окремих попередньо зашифрованих голосів з використанням певного бінарного оператора, що володіє властивістю гомоморфізму, отримаємо інший шифртекст, розшифрування якого дасть комбінацію вхідних голосів [3].

У якості операції $\odot$ може використовуватись модульне додавання ($\oplus$, адитивний гомоморфізм) або множення ($\otimes$, мультиплікативний гомоморфізм). Прикладами криптосистем, що володіють властивостями адитивного та мультиплікативного гомоморфізму є криптосистема Ель-Гамаля (ElGamal) та RSA відповідно.

Відкритий канал з пам'яттю (Bulletin board)

Ефективним методом задоволення вимоги публічної перевірки виборця та його голосу є використання каналу типу bulletin board.

За визначенням Крамара, *bulletin board* - це загальнодоступний канал зв'язку, що володіє пам'яттю. Будь-яка інформація, що ним транслюється, зберігатиметься у пам'яті та буде легкодоступною для зчитування будь-яким стороннім спостерігачем або учасником схеми.

Канал типу bulletin board може містити спеціальні секції для аутентифікованих, правомірних виборців. Аутентифікований виборець має право на запис до призначеної для нього секції. Такий канал може бути реалізовано надійним чином з використанням певної кількості серверів.

У схемах електронного голосування кожен правомірний виборець публікує свій голос у відповідну секцію. Це дозволяє перевірити правильність обробки та фінального підрахунку результатів в процесі голосування. Уповноважені органи також можуть використовувати відкритий канал з пам'яттю для розміщення певної організаційної інформації.

Окремий вид bulletin board використовується для знищення зв'язку між виборцем та його голосом і не містить спеціального поділу на секції.

Мережі перемішування / Анонімний канал зв'язку (Mix-nets)

Мережі перемішування є важливим інструментом для реалізації анонімності. Цей механізм широко застосовуються у багатьох криптографічних додатках, таких як анонімна електронна пошта, електронний аукціон та електронне голосування.

Анонімний канал зв'язку (anonymous channel) у контексті схем електронного голосування забезпечує приховання особи виборця (відправника) відносно органів влади (отримувачі голосу). Для реалізації анонімного каналу можуть використовуватись багатоетапні схеми криптографічного перемішування, що мають назву мережі перемішування та вперше були запропоновані Шаумом (David Chaum).

У традиційному (паперовому) голосуванні з використанням виборчих бюлетенів, після закінчення етапу голосування повинне здійснюватись перемішування голосів, що гарантуватиме анонімність виборця.

В криптографічних протоколах електронного голосування виборці подають зашифровані голоси (бюлетені) як вхідні дані для мережі перемішування. Виходом мережі перемішування є анонімні голоси в відкритому вигляді, що відповідають вхідним виборчим бюлетеням. Таким чином, результат голосування отримується з підрахунку голосів, поданих відкритим текстом. Завдяки використанню анонімного каналу зв'язку, співвідношення голосу виборця до його особи залишається в таємниці.

Мережа перемішування, як правило, складається з декількох серверів, кожен з яких відповідає за один з етапів перемішування. Нехай декілька користувачів використовують таку мережу для досягнення анонімності. Кожен з них шифрує свій вхід і подає його на вхід мережі перемішування. Кожен сервер послідовно перемішує входи.

Відповідно до способу обробки вхідних даних, що виконуються

кожним сервером, мережі перемішування, як правило, класифікуються як схеми, що використовують ланцюжок розшифрування, і схеми, що використовують ланцюжок повторного шифрування.

Основна ідея полягає у перемішуванні та модифікації (тобто розшифруванні або перешифруванні, залежно від типу мережі) деякої послідовності об'єктів для приховання відповідності між елементами початкової та результуючої послідовності. Для досягнення більш високого рівня анонімності мережа перемішування, як правило, складається з певного набору mix-мереж.

Операція перемішування для кожного сервера містить два етапи. Перший крок - обробка входів, яка може здійснюватись за допомогою повторного шифрування або дешифрування. Після цього порядок вхідних даних змінюються на другому кроці, сама перестановка при цьому зберігається в таємниці. Виходом мережі є перестановка вхідних даних користувачів, але самі дані при цьому стали анонімними та не існує можливості пов'язати їх з особистостями користувачів [5].

Нехай розшифровувальна мережа перемішування складається n серверів (рисунок 1.2) M_1, ..., M_n, кожен з яких володіє власною парою ключів (E_j, D_j) - відкритий та особистий ключ відповідно. Для надсилання повідомлення m через анонімний канал, повідомлення шифрується наступним чином: $E_1(E_2(...(E_n(m))...)$ (при необхідності, застосовується конкатенація вихідного повідомлення з випадковими даними) і надсилається до M_1.

Як видно з рисунка, після отримання повідомлення сервер M_j модифікує вхідні дані, перемішує їх і надсилає $E_{j+1}(E_{j+2}(...(E_n(m))...)$ на наступний сервер M_{j+1}. Останній сервер M_n надсилає вихід мережі отримувачу.

У протоколах електронного голосування можливо вимагати доведення коректності розшифрування та перемішування повідомлень сервером.

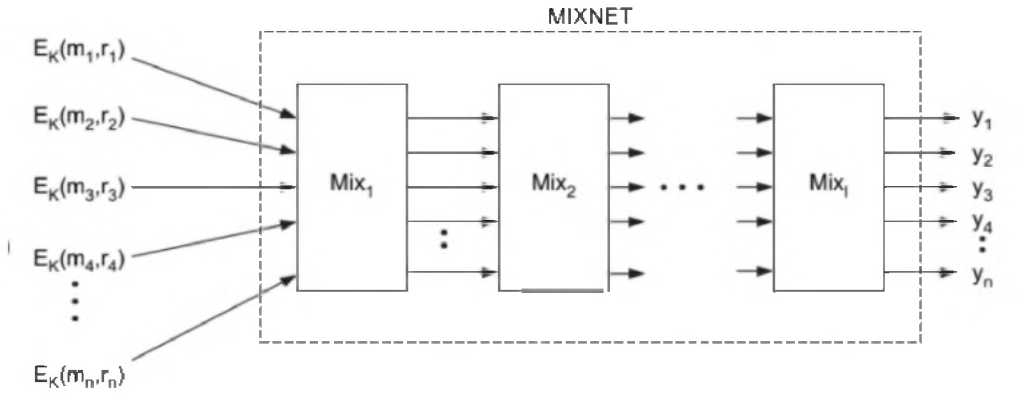

Рисунок 1.2 – Схема процедури голосування

Висновки до розділу 1

У розділі розглянуто опис загальної виборчої моделі, включаючи основні етапи сценарію, учасників виборчого процесу та типи голосування в залежності від структури голосу. Наведено перелік основних вимог, поставлених до протоколів електронного голосування, необхідних для коректного та ефективного розгортання схеми.

У розділі також наведено огляд основних криптографічних примітивів та модулів, що входять до складу протоколів електронного голосування.

2 КЛАСИФІКАЦІЯ ТА ПОРІВНЯННЯ ІСНУЮЧИХ СХЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Ідеальний універсальний протокол електронного голосування повинен відповідати усім вимогам, зазначеним у розділі 1.1, залишаючись при цьому ефективним та масштабованим. На даний момент існує ряд ситуативних протоколів, що в певній мірі задовольняють вимогам до електронного голосування. Однак, попри обширну роботу над створенням протоколів електронного голосування, готового універсального рішення, що могло б забезпечити одночасне виконання принаймні більшості властивостей на даний момент не існує.

Існує велика кількість різних схем електронних виборів, що відрізняються за низкою критеріїв, таких як: наявність чи відсутність ЦВК або центру реєстрації, кількістю таких центрів у схемі та розподілом їх обов'язків, способом реалізації тієї чи іншої властивості, можливостями потенційного масштабування, використанням різних криптографічних примітивів для досягнення певної конкретної мети, орієнтацією під виборчу систему тієї чи іншої країни, тощо.

На відміну від традиційних паперових систем голосування, для протоколів електронного голосування криптографія забезпечує можливість перевірки за допомогою математичних доведень того, що конфіденційність та цілість результатів голосування зберігаються [1].

Першочерговою вимогою до протоколу голосування є його конфіденційність. Для задоволення вимог точності, результат голосування повинен зображати голоси усіх виборців. Для задоволення вимог конфіденційності, зв'язок особистості виборця та його голосу (співвідношення "voter-vote") повинен залишатися приватним для кожного виборця.

Якщо після завершення процесу голосування про кожен голос відомо

лише те, що він лежить у множині голосів (містить усі можливі варіанти вибору), вважається, що досягнуто *повну конфіденційність голосування.*

Якщо ж про кожен голос буде відомо лише те, що він належить до множини опублікованих голосів (чисельність яких набагато більша, ніж кількість усіх можливих варіантів), вважається, що досягнуто *строгу конфіденційність голосування* [3].

В криптографічних протоколах голосування, правильність результатів голосування дотримається водночас зі збереженням в таємниці зв'язку виборця та його голосу. Результати голосування виробляються шляхом розшифрування комбінації дійсних виборчих бюлетенів, або шляхом підрахунку (звичайним чином, без застосування будь-яких криптографічних засобів) анонімних індивідуальних голосів.

Іншими словами, вимога конфіденційності задовольняється або збереженням конфіденційності особистого результату голосування (схеми типу hidden vote), або збереженням конфіденційності кожного ідентифікатора виборця (схеми типу hidden voter). Виділяють також комбінований підхід - прихований голос прихованого виборця (hidden voter with hidden vote), в якому виборець анонімно надсилає зашифрований голос.

Перший спосіб досягається за допомогою функції гомоморфного шифрування (приховування голосу виборця) [6]. Другий спосіб досягається шляхом імітації використання виборчих скриньок шляхом використання анонімного каналу (приховування особистості виборця) [7].

В рамках даного дослідження основну увагу буде зосереджено на класифікацію систем електронного голосування відносно способу забезпечення таємності співвідношення особистості виборця та його голосу. Далі наведено огляд даних підходів, а також розглянуто їх основні переваги та недоліки.

2.1 Забезпечення конфіденційності шляхом приховування голосу виборця

Основним методом побудови схем електронного голосування типу hidden vote є використання гомоморфної схеми депонування повідомлень.

Схемою депонування повідомлень називається криптосхема, яка дозволяє перетворювати та зберігати повідомлення (в найпростішому випадку - 1 біт) таким чином, що саме вихідне повідомлення неможливо буде змінити згодом в залежності від будь-яких зовнішніх обставин. З іншого боку, сторонній спостерігач не повинен мати можливості дізнатись зміст цього повідомлення до визначеного моменту часу. Таку схему умовно можна назвати електронним сейфом [1].

Простим прикладом реалізації депонування деякої величини x, є використання стійкої до колізій геш-функції $H(x) = y$.

Гомоморфні схеми є одним з основних примітивів, що використовуються для задоволення вимог конфіденційності у схемах електронного голосування. Кожен окремий голос не повинен бути пов'язаний з відповідним виборцем. Результат голосування оприлюднюється, не відкриваючи при цьому жодного конкретного голосу.

Гомоморфні схеми голосування вважаються ефективними, коли кількість кандидатів чи варіантів вибору невелика. Проте гомоморфне голосування має недолік, що полягає в тому, що кожен голос повинен бути підтверджений, щоб вважатися дійсним. Без перевірки валідності голосу, правильність підрахунку не може бути гарантована.

Коли кількість кандидатів чи варіантів вибору у голосуванні є істотною, обрахункові та комунікаційні витрати на доведення та верифікацію чинності голосу стають настільки великими, що гомоморфне голосування стає менш ефективним за інші способи досягнення конфіденційності.

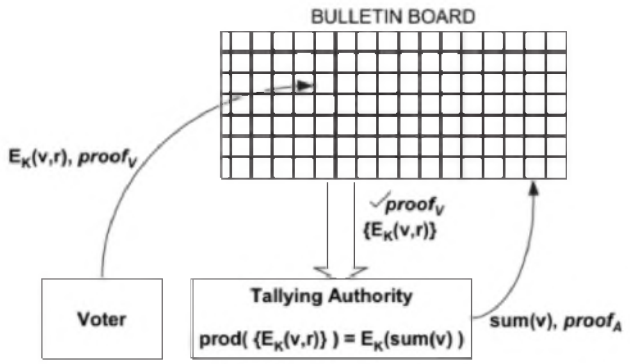

Рисунок 2.1 – Типова структура схеми з приховуванням голосу

Типова схема з приховуванням голосу зображена на рисунку 2.1. Правомірні виборці надсилають свій зашифрований голос до аутентифікованої секції загально доступного каналу типу bulletin board.

Оскільки особистість виборця не є анонімною, для збереження в таємниці зв'язку між виборцем та його голосом, голос повинен залишатись зашифрованим. Гомоморфне шифрування забезпечує механізм прямого об'єднання зашифрованих голосів для здійснення зашифрованого підрахунку. Розшифруванню підлягає лише кінцевий результат голосування.

Враховуючи цю особливість, чинність прихованих голосів повинна бути забезпечена до моменту їх об'єднання. Тому виборцю потрібно надати інтерактивний чи неінтерактивний доказ чинності свого голосу.

Узагальнена форма голосу виборця V_j має вигляд: $(E_k(v_j, r_j), proof_j)$, де K - відкритий ключ гомоморфної схеми шифрування, v_j - голос виборця, $proof_j$ - доказ його дійсності.

Після перевірки підтверджень, наданих виборцями, компетентний орган здійснює процедуру підрахунку голосів з використанням властивості гомоморфізму функції шифрування.

Владний орган повинен опублікувати розшифроване значення суми голосів та доказ правильності розшифрування. Використовуючи опубліковані значення, будь-хто може обчислити та перевірити чинність голосування, задовольняючи таким чином виконання вимоги загальної

перевірності.

На відміну від схем з прихованою особистістю виборця, де кодування голосу v_j може бути гнучким, у схемах даного типу кодування v_j є обмеженим. Оскільки зашифровані голоси безпосередньо об'єднуються для підрахунку результату, формат голосів повинен бути фіксованим. Таким чином, схеми з приховуванням голосу можуть бути використані для врахування лише попередньо визначених кандидатів, вписані вручну голоси на вході такої схеми не оброблюються.

Схеми з приховуванням голосу поділяються на схеми з пороговим розподілом голосів (vote threshold schemes), схеми з пороговим розподілом ключа владного органу (authority key threshold schemes) та схеми з пороговим розподілом ключа виборця (voter key threshold schemes) [8].

Схеми з пороговим розподілом голосів

У цій категорії схем з прихованим голосом, голос виборця сегментується на k частин з використанням виборцем $(t,\ k)$-схеми розподілу секрету, і кожен з k органів влади отримує одну (зашифровану відкритим ключем цього органу) частку. В тому числі, можливе застосування випадку, коли відновлення секретного голосу можливе лише за участі усіх органів влади $t = k$.

Кожен орган влади, використовуючи властивість гомоморфізму своєї криптосистеми, об'єднує частки голосів, отримані від виборців, для отримання зашифрованої часткової суми. Кожен орган розшифровує власну часткову суму і, на останньому етапі, усі органи поєднують свої часткові суми, для отримання остаточного підрахунку голосів.

Першими схеми такого типу були запропоновані Коеном та Юном (Cohen і Yung, 1986) та Бенало (Benaloh, 1987). Основною запропонованих схем стала ідея використання таких криптопримітивів як ймовірнісна схема шифрування з адитивним гомоморфізмом, заснована на задачі знаходження r-го кореня та систем доведень з нульовим розголошенням.

Схема Коена та Фішера (Cohen and Fischer, 1985) мала єдиний орган влади, і була модифікована Коеном та Юном, шляхом поділу голосу між

k владними структурами. Таким чином, досягається стійкість до $(k-1)$ корумпованих органів влади. Проте обидва ці підходи не є надійними: у разі утримання органу влади від участі, процес голосування може бути порушено.

Бенало запропонував схему, яка використовувала метод порогового розподілу секрету для забезпечення надійності: голос v_j розподілявся між k органами з використанням $(t,\ k)$ - порогової схеми.

Практичне обмеження схеми Бенало полягає в залежності від закінчення стадії попереднього голосування: для передачі свого голосу V_j повинен чекати, поки всі інші виборці закінчать етап інтерактивного доведення. Схема, запропонована Іверсоном (Iverson, 1992), долає цю слабкість і робить участь V_j незалежною від участі інших виборців шляхом використання техніки сліпого підпису. Токен зі сліпим підписом, що містить ідентифікатор виборця, надсилається до владного органу з часткою голосів. Недійсне повторне використання токена показує ідентифікатор виборця. Проте ця схема не є ефективною та надійною. Страждає також властивість універсальної перевірності, оскільки схема відмовляється від використання відкритого каналу з пам'яттю.

Іншим недоліком схеми Бенало є використання системи інтерактивних доведень, які потребують інтенсивних обчислень та комунікацій. Цю слабкість усунено варіантами, запропонованими в Сако і Кілліаном (Sako and Killian, 1994) та Крамером (Cramer et al., 1996). Покращенню ефективності у схем типу hidden vote сприяє використання ефективних неінтерактивних доведень та припущення про складність обчислення дискретного логарифма (замість r-го кореню).

Схожий, але більш надійний підхід (з використанням порогової схеми для досягнення ефективності) пропонується в схемі Крамера.

Схеми з пороговим розподілом ключа владного органу

Попри досягнення частини бажаних властивостей, всі наведені вище схеми вимагають обширних обчислень та значної кількості з'єднань, а отже, залишаються немасштабованими та непрактичними в такій їх

формі. Наступний підтип схем пропонує більш ефективне рішення, вимагаючи від виборця виконувати лише одне шифрування для голосування.

Виборець шифрує свій голос відкритим ключем K органу обрахунку голосів. Для забезпечення надійності, вводиться декілька владних органів, які поділяють між собою особистий ключ (розшифрування) шляхом застосування (t,k)-перевірної схеми розподілу секрету. Схема використовує модифікацію криптосистеми Ель-Гамаля (гомоморфне шифрування) та систему неінтерактивних доведень з нульовим розголошенням.

Схема залишається надійною відносно змови $(t-1)$ органу влади, або відносно несправності $(k-t)$ з них. Проте обмеженість формату голосу зумовлює відсутність масштабованості та практичності цієї схеми. Збільшення кількості кандидатів зробить системи доведень та процес обрахунку складним.

Проблема масштабованості значно покращується з початком використання узагальненої криптосистеми Пайліера (Paillier, 1999) замість системи Ель-Гамаля. Розшифрування (а отже і підрахунок) в цій криптосистемі може здійснюватись ефективно.

Схема, запропонована Бодро (Baudron et al., 2001), використовує криптосистему Пайліера, а надійність підрахунків забезпечується ієрархічною 3-рівневою архітектурою, імітуючи реальну структуру виборів. Відповідно до цієї схеми, підрахунок голосів здійснюється надійним чином на кожному з рівнів, однак складність обрахунків та доведень зумовлює непрактичність такої схеми.

Властивість захисту від підробки голосу у схемах, запропонованих в Хірт і Сако (Hirt and Sako, 2000) та Лі і Кім (Lee and Kim, 2002) досягається шляхом обмеження можливості виборця V_j генерувати випадкові дані r_j.

Підхід Хірт і Сако досягає ще більш високого рівня надійності: k органів влади (з використанням порогової схеми розподілу секретного ключа S) спільно генерують випадковий рядок r_j, використовуючи

незмінюваний канал між владою та виборцем, та систему неінтерактивних доведень.

В схемі Лі і Кім завдяки використанню локального надійного генератора випадкових чисел (tamper-resistant randomizer), разом із неінтерактивними доказами, пропадає потреба в застосуванні незмінюваного каналу.

Інший підхід до забезпечення цієї властивості, запропонований Бодро (Baudron et al, 2001), полягає в використанні надійного стороннього генератора разом з незмінюваним каналом, робить схему більш масштабованою, але водночас менш надійною.

Схеми з пороговим розподілом ключа виборців

Схеми попередньої категорії можуть спричинити виникнення суперечностей у зв'язку з використанням протоколів розподіленої генерації ключів з доведеннями коректності на етапі оголошення параметрів, що передбачають низку взаємодій між владою та виборцями.

У схемах з пороговим розподілом ключа виборців, виборці самі виступають в ролі органів влади та беруть участь у процесі спільної генерації секретних ключів, які згодом використовуються для шифрування їх голосів.

Обрахунок голосів може здійснюватись доки порогова кількість виборців бере участь у голосуванні і підрахунку. Такі схеми підходять для дрібномасштабних виборів, якщо наявність окремого владного органу не є обов'язковою, як у схемі Шонмейкерса (Schoenmakers, 1999). Схема використовує загальноперевіну (t,n)-схему розподілу секрету.

Оскільки всі етапи цієї схеми є загальнодоступними, проблема суперечності вирішується в такому протоколі, однак, зменшуючи при цьому масштабованість, ефективність та практичність. Ця схема також вимагає участі всіх виборців у етапі підрахунку голосів.

Варіант, запропонований Кеайесом та Юном (Kiayias і Yung, 2002), долає цю слабкість, дозволяючи підрахунок голосів лише після подачі останнього голосу. Окрім подолання суперечності, схема досягає

властивості максимальної конфіденційності, встановлюючи поріг $t = n$. Однак властивість надійності втрачається, оскільки якщо один з n виборців не відправляє голос, то процедура виборів порушуються.

Через фіксований формат голосу, вибори, які включають варіант вписаного голосу, не можуть бути реалізовані за допомогою схем з застосуванням гомоморфного шифрування. Крім того, створення та перевірка систем доведень, як і сам процес голосування, стає складним та неефективними зі збільшенням кількості кандидатів, обмежуючи придатність цього підходу для реальних систем [8].

2.2 Забезпечення конфіденційності шляхом приховування особистості виборця

У схемах, що належать до цього класу, особистість виборця залишається в таємниці, а його голос надсилається до органів обрахунку за допомогою анонімного каналу, найрозповсюдженішою реалізацією якого є мережі перемішування, описані у пункті 1.2.

Для забезпечення точності голосування вимагається також надійна передача повідомлення від виборця на вхід анонімного каналу. Отже, загальною формою голосу виборця V_j є: $E_K(v_j\ ,\ r_j)$, де r_j - випадковий рядок, K - відкритий ключ анонімного каналу, а v_j - це голос виборця на користь певного кандидата. Орган підрахунку або будь-який сторонній спостерігач отримує набір відкритих голосів $\{v_j\}_R$ як вихід анонімного каналу зв'язку. Таким чином, будь-хто може обчислити результуюче співвідношення $\sum_j v_j$.

Щоб переконатись в правомірності прихованого виборця, необхідне проведення ідентифікації, що забезпечить підтвердження дійсності особи виборця. Базуючись на цьому, схеми з прихованим виборцем поділяють

на схеми з використанням маркерів (token based schemes) і схеми з використанням відкритого каналу зв'язку з пам'яттю (bulletin board based schemes) [8].

Ідентифікаційний об'єкт називається *маркером (токеном)* та отримується виборцем від органу влади на етапі реєстрації шляхом реалізації протоколу генерації токенів.

Для забезпечення анонімності виборців, маркер повинен бути випадковим і генеруватись таким чином, щоб його зв'язок з особистістю виборця було неможливо відновити.

На етапі голосування, виборець надсилає свій маркер у поєднанні з голосом анонімним каналом зв'язку до відповідного уповноваженого органу. Така схема була запропонована в Шаумом (Chaum, 1988) та вдосконалена Бойдом (Boyd, 1990).

У схемі Шаума окрім токенів використовується криптосистема RSA, мережа перемішування та технологія цифрового підпису.

Дана схема задовольняє вимогам правомірності голосу, конфіденційності та індивідуальної перевірності. Обрахункова конфіденційність (еквівалентна злому криптосистеми RSA) забезпечується проти будь-якого зовнішнього супротивника.

Існує потенційна можливість колізії токенів двох або більше виборців, а єдиного некоректного перемішування достатньо для виникнення неточностей, отже схема не є точною та надійною. У разі виявлення виборцем неточності, для того, щоб захистити конфіденційність виборця, необхідний повний перегляд виборчого процесу, таким чином втрачається справедливість голосування, оскільки часткове розголошення голосів може вплинути на рішення виборців при переобранні.

Ще одним недоліком є те, що у разі змови всіх серверів перемішування може порушуватись конфіденційність виборця. Ця слабкість покривається використанням протоколу генерації маркерів з використанням методу сліпого підпису. Максимальна конфіденційність

цих схем досягається, оскільки порушення конфіденційності V_j вимагає змови решти виборців та органів влади. Тим не менш, проблеми точності і стійкості залишаються, оскільки органи влади, що беруть участь у мережі, можуть додавати недійсні голоси без можливого виявлення їх дій.

Отже, схеми з приховуванням особистості виборця з використанням маркерів, мають спільні слабкі місця з надійністю, точністю та справедливістю, в основному пов'язані з використанням анонімного каналу зв'язку. Крім того, схеми надають виборцеві можливість підтвердження свого голосу, що може застосовуватись для тиску на виборця або корумпування голосу.

Схеми з використанням відкритого каналу зв'язку з пам'яттю

Типова схема електронного голосування з використанням каналу типу bulletin board має наступну структуру (рисунок 2.2). Виборець використовує аутентифікований відділ на загальнодоступній bulletin board, для публікації свого голосу, який після проходження перевірки перемішується з іншими з використанням анонімного каналу зв'язку (мережі перемішування).

До основних примітивів, що використовуються в схемах даного типу, належать мережі перемішування (decryption/re-encryption), відкритий канал типу bulletin board та системи неінтерактивних доведень.

Використання маркерів в цій схемі не є необхідним, оскільки лише виборці, що мають право голосу отримують доступ на внесення записів до відповідного каналу.

Схеми, запропоновані в Сако, Кілліан та Шаумом, належать до цієї категорії схем з приховуванням особи виборця.

Поєднання використання мереж перемішування (з доведенням коректності функціонування) із відкритим каналом з пам'яттю (bulletin board) задовольняє вимоги правомірності та конфіденційності голосу. В протоколах такого типу досягається також властивості справедливості, точності та універсальної перевірності схеми.

Виконання вимог справедливості та надійності залишається чинним

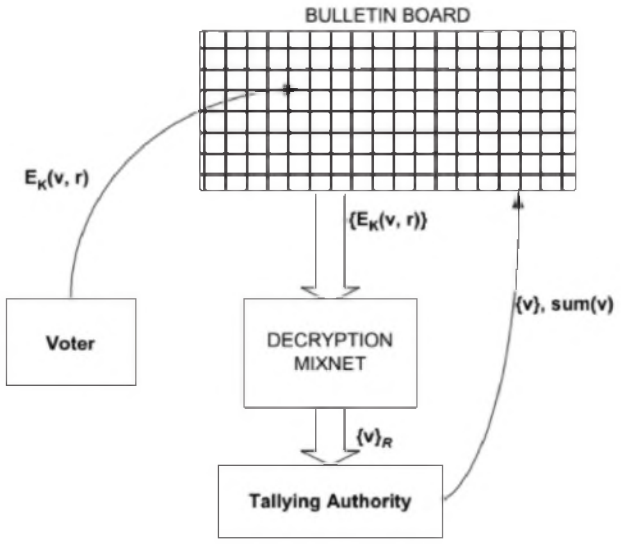

Рисунок 2.2 – Типова структура схеми електронного голосування з застосуванням каналу типу bulletin board

до моменту, поки залишається функціонувати принаймні одне гарантовано чесне перемішування. Вимога неможливості підробки голосу задовольняється при припущенні використання односторонніх незмінюваних каналів, оскільки таким чином виборець не зможе довести свій голос супротивнику.

Однак використання незмінюваних каналів також робить схему менш практичною: наявність значної кількості комунікацій та обчислень, які необхідно виконати виборцю для перевірки, робить схему немасштабованою та неефективною.

Проте головним недоліком схеми є відсутність надійності щодо несправного перемішування, оскільки наявність кроку з відсутнім перемішуванням може призвести до зриву виборів через необхідність повторного голосування [8].

2.3 Комбіновані схеми з приховуванням особистості виборця та його голосу

Для вирішення проблем ефективності та формату голосу у схемах з приховуванням голосу, було запропоновано третій, комбінований підхід Фудзіока (Fujioka et al.,1993) та Парка (Park et al., 1994). У схемах з прихованою особистістю виборця були відсутні обмеження на формат голосу, а процес обрахунку був простий, однак таким схемам була притаманна проблема з досягненням справедливості голосування (необхідність проведення повторного голосування при виникненні неточностей).

Вирішення цієї проблеми можливе у разі застосування зашифрованих голосів, що і пропонує підхід прихованого виборця із прихованим голосом (Hidden voter voter hidden vote).

У такому підході виборець використовує анонімний канал для посилання зашифрованого голосу до відповідального органу.

Залежно від застосованих механізмів, такі схеми поділяють на схеми з використанням маркерів, схеми з використанням гомоморфного шифрування та схеми з використанням маркерів і гомоморфного шифрування.

Комбіновані схеми з застосуванням маркерів

Під час реєстрації виборець отримує сліпий підпис реєстраційного органу на свій зашифрований голос. Далі (рисунок 2.3) виборець анонімно надсилає підписаний прихований голос до органу підрахунку у вигляді: $E_{K_m}(sign_A(E_K(v_j,\ r_j),\ K_A^{-1}))$, де E_{K_m} - зашифрований відкритий ключ анонімного каналу зв'язку (mixnet), а K - відкритий ключ відповідного органу чи виборця, а K_A^{-1} - особистий ключ органу реєстрації.

Першою схемою такого типу була схема Фудзіока. Схема володіє властивістю максимальної чесності, оскільки навіть у разі змови всіх

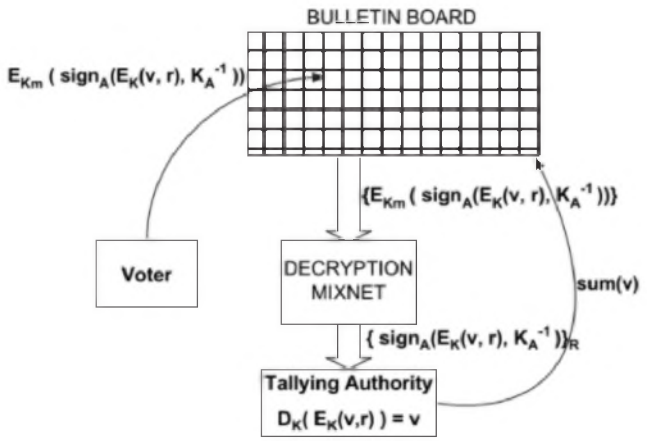

Рисунок 2.3 – Типова структура комбінованої схеми з застосуванням маркерів

органів влади вони не зможуть обрахувати навіть часткову суму голосів. Однак для досягнення цього виборцю потрібно брати участь на етапі підрахунку голосів (після завершення етапу голосування), що робить схему непрактичною.

Основною слабкістю цієї схеми є точність і надійність. Будь-який виборець, що утримався від участі в голосуванні, може бути виявлений реєстраційним органом, і відповідальний орган може додати голоси замість нього. Змова між виборцем та реєстраційним органом або колізії маркерів можуть також створювати неточності в ході голосування.

Схема Барані-Дастрірда (Baraani-Dastjerdi et al., 1995) намагається вирішити проблеми надійності і точності, використовуючи декілька контрольних органів, а також довірений орган з незмінюваними каналами, але використання такого підходу є непрактичним. У схемі Юанга (Juang et al., 2002) запропоновано більш придатне для масштабування вирішення проблеми точності та надійності, включаючи проблему колізії маркерів.

Схема Окамото (Okamoto, 1997) була спрямована на подолання проблеми фальсифікації голосу. Основна ідея схеми полягає в використанні техніки прив'язки до біту, що дозволяє виборцеві довести справедливість голосу v'_j замість v_j. Однак припущення наявності

анонімного незмінюваного каналу робить її непрактичною.

Комбіновані схеми з використанням гомоморфного шифрування

Схеми цього типу були запропоновані для подолання проблеми дотримання властивості точності та загальної перевірності. До них належать схеми Парка (Park et al., 1994), з подальшим покращенням властивостей перевірності та надійності у Огата, Якобсона та Ейба (Ogata et al., 1997; Jakobsson, 1998; Abe, 2000; Golle et al., 2002).

Загальна структура цих схем (рисунок 2.4) полягає в наступному: виборець підтверджує зашифрований голос $E_K(v,r)$ та надсилає до аутентифікованої секції каналу типу bulletin board. Після передачі усіх голосів, вони передаються до органу підрахунку за допомогою мережі перемішування. Голоси розшифровуються для знаходження $sum(v)$ і розголошуються разом з підтвердженням коректності розшифрування $proof_A$.

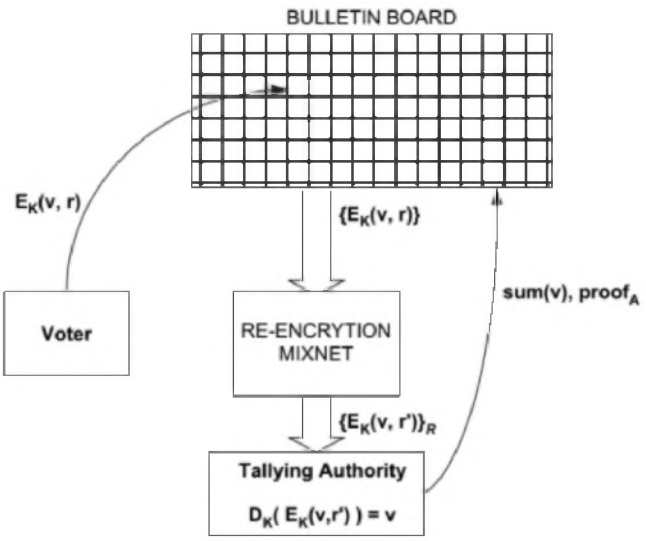

Рисунок 2.4 – Схема процедури голосування для комбінованої схеми з використанням гомоморфного шифрування

Властивості правочинності голосу, конфіденційності, точності, чесності та надійності голосування виконуються в схемах такого типу у разі використання загальноперевірної, надійної мережі перемішування.

Модифікації схем, з використанням систем неінтерактивних доведень та надійних генераторів випадкових чисел (Lee, 2003), досягають виконання умови неможливості підробки голосу (recipient free). Схема Кеайеса та Юна розширює схему такого типу для варіанту використання вписаних голосів (write-in type).

Комбіновані схеми з використанням токенів та гомоморфного шифрування

Такі схеми націлені на задоволення вимог несуперечності та неможливості підробки голосу, вперше запропоновані Джейлсом та Якобсоном (Juels and Jakobsson, 2002) та Аквісті (Acquisti, 2004).

Основна ідея полягає в тому, що протягом етапу реєстрації виборець отримує унікальний маркер, зашифрований відкритим ключем гомоморфної схеми шифрування та розподіленим між k органами влади.

Виборець відправляє зашифрований голос разом з зашифрованим маркером через анонімний широкомовний канал до відкритого каналу зв'язку із пам'яттю. Відповідальний орган перевіряє чинність маркерів до моменту розшифрування.

Властивість непідробності задовольняється завдяки можливості неоднозначного доведення зашифрованого поєднання токена з голосом, оскільки супротивник не може підтвердити ані токен, ані утримання виборця від голосування. Властивості масштабованості, універсальної перевірності та точності знижуються шляхом дотримання властивості несуперечності, а використання анонімного широкомовного каналу є важким для практичної реалізації [8].

Висновки до розділу 2

У даному розділі було розглянуто та узагальнено існуючі підходи до реалізації системи електронних виборів з точки зору різних методів забезпечення секретності зв'язку між виборцем та його голосом.

Схеми з приховуванням особи виборця. Головними перевагами є наявність найпростішого процесу обрахунку голосів, а також низьких вимог до обчислювальних потужностей з боку виборця. Проте в цих схемах точність, справедливість і надійність голосування не можуть забезпечуватись одночасно. Неточності у підрахунках можуть бути вирішені лише за допомогою проведення повторного голосування, що суперечить вимозі справедливості. Характерним криптографічним методом є застосування анонімного каналу зв'язку у вигляді мереж перемішування та відкритого каналу зв'язку з пам'яттю.

Схеми з приховуванням голосу. Залученість виборців у процес голосування для таких схем є мінімальною. Відсутні вимоги щодо будь-якої форми мереж перемішування, характерне легке досягнення універсальної перевірності. У разі використання для дрібномасштабних виборів, можлива реалізація з відсутністю владного органу в схемі та з досягненням властивості несуперечності. Найбільшим недоліком таких схем є фіксованість форматів голосування та неефективність у разі широкомасштабного застосування. Характерними криптографічними методами є використання гомоморфних функцій шифрування і систем інтерактивних та неінтерактивних доведень.

Прихований виборець зі прихованим голосом. Основною перевагою є гнучкий формат голосу та відносно низькі обчислювальні вимоги відносно виборця (як правило, не потрібні складні доведення), що є бажаними властивостями для широкомасштабних виборів. Проте реалізація анонімного каналу є проблематичною для таких схем.

Характерною особливістю схем такого типу є поєднання застосування мереж перемішування та властивості гомоморфізму функцій шифрування.

Досягнення властивості універсальної перевірності з використанням мереж перемішування досягається за рахунок зниження масштабованості схеми. Процес підрахунку голосів може бути трудомістким, оскільки вимагає перевірки індивідуально зашифрованих голосів, розшифровки та перевірки голосів, а потім фактичного підрахунку.

Як видно з наведеного огляду, виконання усіх бажаних вимог до протоколів електронного голосування наразі не забезпечується в жодній з існуючих схем. Побудова ефективних схем голосування можлива лише для визначеного масштабу виборів з відповідним підбором оптимальних параметрів.

3 ЗАПРОПОНОВАНА СХЕМА, ЗАСНОВАНА НА ПОЄДНАННІ МЕТОДІВ ГОМОМОРФНОГО ШИФРУВАННЯ ТА МЕРЕЖІ ПЕРЕМІШУВАННЯ

3.1 Протокол електронного голосування на основі використання криптосистеми RSA та простих чисел

Розглянемо детальніше протокол електронних виборів, описаний у роботі [9] Музиканським та Фуріним.

У роботі протоколу беруть участь N виборців та єдиний владний центр з яким кожен з виборців здійснює обмін даними. Центр забезпечує організацію процесу виборів, в тому числі проведення підрахунку голосів. Даний варіант протоколу використовує модель бюлетеню з трьома варіантами відповіді "за"($"for"$), "проти"($"against"$) та "утриматись"($"pass"$).

Етап налаштування. Початком організації виборчого процесу у даному протоколі є створення та ініціалізація криптосистеми RSA, а саме вибір параметрів. Центр обирає значення (m, e) та (m, d) в якості відкритого та особистого ключів відповідно, значення відкритого ключа розголошується.

Кожен виборець V_i встановлює секретне значення параметру b_i – аналогу виборчого бюлетеня в залежності від власного вибору, користуючись наступним правилом:

$$b_i = \begin{cases} 2, & vote = "for" \\ 3, & vote = "against" \\ 1, & vote = "pass". \end{cases} \tag{3.1}$$

Реєстрація. На етапі реєстрації виборців кожен охочий взяти участь

у голосуванні повинен пройти процедуру аутентифікації у владному центрі.

Згідно з протоколом аутентифікації, виборець надсилає владному центру випадковий рядок s. Центр, в свою чергу, обраховує значення g, використовуючи особистий ключ (m, d) і надсилає його виборцю: $g = s^d \ mod \ m$.

Отримавши число g, виборець обраховує значення s', використавши загальнодоступний відкритий ключ центра: $s' = g^e \ mod \ m$. Аутентифікація приймається, якщо значення s та s' збігаються, та відкидається у будь-якому іншому випадку.

Впевнившись у істинності особи куратора виборів, V_i створює власну пару ключів (m_i, e_i) та (m_i, d_i) і публікує значення відкритого ключа.

Етап голосування. Для збереження таємниці голосування перед тим, як надіслати бюлетень до вповноваженого органу, виборець здійснює його затемнення випадковим множником. В іншому випадку, зашифровані образи значень b_i згідно з 3.1 можуть приймати лише одне з трьох значень, компроментуючи тим самим голос виборця. Затемнення електронного бюлетеня відбувається за формулою:

$$t_i = b_i \cdot q_i,$$

де q_i – обране випадковим чином просте число (в конкретному випадку накладається обмеження $q_i \geq 5$).

По завершенню процедури засліплення, бюлетені підлягають шифруванню за схемою RSA:

$$f_i = t_i^e \ mod \ m.$$

Значення f_i надсилається виборцем до владного центру.

При використанні такого підходу, у разі збігу голосів двох або більше виборців, їх зашифровані бюлетені залишатимуться різними в силу вибору відповідних множників q_i та q_j.

Отримавши бюлетень, центр додає в реєстр обліку виборців запис,

що містить його дані (прізвище, ім'я, додаткова інформація, тощо) для уникнення можливості повторного голосування.

По завершенню етапу голосування, центр публікує таблицю з обліком отриманих бюлетенів у форматі "особа виборця – його бюлетень в зашифрованому вигляді (f_i)".

Етап обрахунку голосів. Безпосереднє розшифрування та обрахунок бюлетенів за наявності опублікованого списку голосів, порушував би таємницю голосування, водночас унеможлививши перевірку обрахунків. Тому процедура обрахунку голосів, запропонована у протоколі [9] має наступну структуру:

1) Попередньо обраховується значення добутку усіх зашифрованих бюлетенів F:

$$F = \prod_{i=1}^{N} f_i.$$

2) Використовуючи значення особистого ключа владного центру, отримується значення Q як:

$$Q = F^d \ mod \ m = (\prod f_i)^d \ mod \ m = \prod (f_i^d \ mod \ m) =$$

$$= \prod t_i \ mod \ m = \prod b_i \cdot q_i \ mod \ m.$$

3) Враховуючи множину можливих значень b_i, Q можливо представити в вигляді:

$$Q = \prod b_i \cdot q_i = (2^r) \cdot (3^p) \cdot R,$$

де $R = \prod q_i$ – добуток усіх випадкових множників, використаних у схемі.

4) Значення r та p відповідають кількості голосів "за" та "проти". Кількість бюлетенів, що містили голос "утриматись" обраховується за формулою $u = N - (r + p)$.

5) Центр публікує результати голосування $\{r, p, u\}$ та контрольне значення R для забезпечення можливості перевірки коректності проведеного обрахунку.

Перевірка. Згідно з запропонованою схемою, володіючи загальнодоступними значеннями відкритого ключа центру (m, e), списком зашифрованих бюлетенів $\{f_i, i = \overline{1, N}\}$ та результатами голосування $\{r, p, u, R\}$ можливо провести процедуру перевірки чесності підбиття результатів.

1) Відновлюється значення $Q = (2^r) \cdot (3^p) \cdot R$, що після цього зашифровується з використанням значення відкритого ключа центру.

2) Обраховується добуток усіх опублікованих бюлетенів в зашифрованому вигляді F.

3) Останнім кроком є перевірка співвідношення $Q^e \ mod \ m \stackrel{?}{=} F$. В залежності від виконання цього співвідношення можливо зробити висновок про коректність підрахунку голосів.

4) Правильність співвідношення значень r та p можливо перевірити, виконавши пробні ділення контрольного значення R (добутку простих чисел $q_i \geq 5$) на значення 2 та 3. Якщо значення R не ділиться націло на жодне з цих чисел, розподіл голосів зазначено правильно.

Даний протокол електронного голосування можна узагальнити для варіанту вибору однієї з багатьох альтернатив (1-out-of-L voting) та вибору кількох варіантів зі списку (k-out-of-L voting).

Вищезазначений варіант протоколу електронного голосування [9] має ряд переваг та недоліків. Перевагами цієї схеми виконання вимог універсальної перевірності (завдяки можливості перевірки результатів сторонньою особою з використанням загальновідомих величин) та індивідуальної перевірності (кожен учасник має можливість простежити факт врахування свого голосу).

Основним вразливим місцем системи є наявність єдиного вповноваженого центру, який порушує таємницю співвідношення виборця та його голосу через необхідність перевірки валідності поданого бюлетеню (запобігання подачі продубльованого чи некоректного голосу). Тобто конфіденційність та справедливість голосування забезпечується відносно усіх його учасників та сторонніх спостерігачів, окрім владного центру. У

разі компрометації центру, можливий витік часткового співвідношення голосів до завершення етапу голосування, що може вплинути на подальший його розвиток. Порушення таємниці голосування може створити умови для здійснення тиску на виборців та виникненню інших неприйнятних ситуацій.

3.2 Модифікація протоколу з використанням анонімного каналу зв'язку

Отже, основним завданням модифікацій даної схеми виборчого процесу є усунення порушення таємниці голосування та забезпечення секретності співвідношення "voter-vote" відносно будь-якого суб'єкту в процесі голосування.

Запропонована схема є комбінацією протоколу електронного голосування 3.1 та поєднання методів гомоморфного шифрування та анонімного каналу зв'язку (а саме re-encryption mixnets), що використовувався у схемі [10].

У новій схемі виокремлено N владних органів для організації виборчого процесу та відповідного поділу обов'язків. Окрім цього, забезпечується неможливість підробки голосу (властивість recipient free), а структура процесу голосування знімає необхідність перевірки голосу, надісланого виборцем, а отже і порушення конфіденційності голосування водночас.

Основна ідея полягає в тому, що відповідальні органи сумісно генерують список усіх можливих коректних варіантів голосів та публікують їх у зашифрованому вигляді та випадково обраному порядку. Виборець при цьому лише вказує позицію обраного голосу в результуючому списку. Таким чином схема не вимагає від виборця

засліплення голосу, тим самим знищуючи можливість доведення сторонній особі істинний зміст свого голосу. Виборець в свою чергу не може надіслати сфальсифікований певним чином бюлетень через відсутність можливості самостійно його створити.

Загальна схема створення зашифрованого та перемішаного випадковим чином списку усіх можливих варіантів вибору зображена на рисунку 3.1 (у загальному випадку відтворюється для кожного виборця $V_i, i = \overline{1, M}$ та N вповноважених центрів A_j). У порівнянні з оригінальною схемою 3.1 додається використання анонімного каналу зв'язку типу re-encryption mixnet.

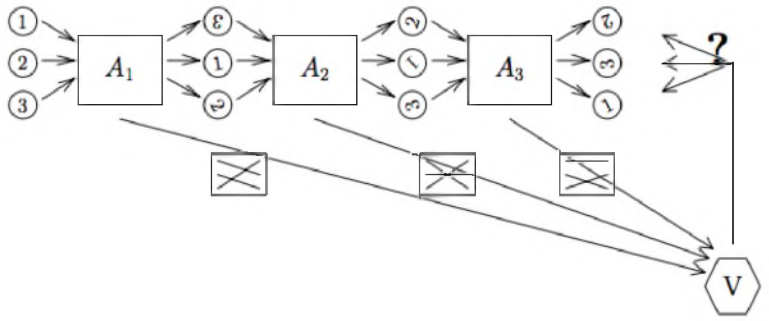

Рисунок 3.1 – Процедура формування голосу для одного з виборців V із залученням трьох владних органів A_1, A_2 та A_3.

На підготовчому кроці вповноважені органи створюють та публікують множину всіх чинних голосів $\{v_k^{(0)}, k = \overline{1, L}\} = \{v_1^{(0)}, v_2^{(0)}, ..., v_L^{(0)}\}$, кожен елемент якої є унікальним та правомірним варіантом відповіді на питання виборів. Даний список є єдиним та універсальним для усіх учасників голосування.

Після цього кожен з органів влади за допомогою re-encryption mixnet почергово здійснює перемішування списку, отриманого від попереднього органу в лацнюжку та після опрацювання передавши наступному (для першого - початковий список) відповідно.

Додатково, кожен центр $A_j, j = \overline{1, N}$ повинен довести виборцю в приватному порядку дійсність перетвореного списку шляхом розкриття

способу перестановки, а саме передачі її в зашифрованому вигляді через односторонній відкритий канал. Це дає виборцеві змогу прослідковувати зміну розташування елементів списку, цим самим дозволяючи відрізняти позицію власного потенційного вибору після кожного з етапів перемішування, слідкуючи при цьому за чесністю дій вповноважених центрів.

Розглянемо варіант розгортання протоколу для типу голосування з вибором одного варіанту з L можливих (1-out-of-L voting). Нехай набір коректних голосів утворює множину $\{v_k, k = \overline{1, L}\} = \{v_1, v_2, ..., v_L\}$ так, що намір виборця обрати варіант v_r відповідає бажанню віддати голос за кандидата, розташованого на r-тій позиції сформованого списку.

Нагадаємо, що метою створення модифікації протоколу електронного голосування [9] є забезпечення виконання базової вимоги конфіденційності голосування відносно вповноважених сторін із збереженням властивостей універсальної та індивідуальної перевірності, що є основними перевагами існуючої процедури.

Етап налаштування (Set-up phase)

Нехай учасниками протоколу є M виборців $\{V_i, i = \overline{1, M}\}$ та N вповноважених центрів (authorities) $\{A_j, j = \overline{1, N}\}$. В рамках запропонованої моделі довіри, введемо порогове значення t як мінімальну кількість вповноважених центрів у схемі з гарантовано чесним функціонуванням .

Основним каналом зв'язку у запропонованій схемі є відкритий канал з пам'яттю (1.2), що характеризується відкритим доступом для зчитування інформації та відсутністю можливості видалення опублікованих записів для будь-яких суб'єктів. Самі записи в свою чергу можуть робити лише автентифіковані дійсні учасники протоколу.

Для створення приватного зв'язку центрів з виборцями запропоновано використання одностороннього каналу з шифруванням. Зв'язок такого типу призначений для підтвердження кожним центром чесності свого функціонування кожному виборцю шляхом розкриття

схеми деяких таємних параметрів та надсилання доведень коректності шифрувань. Використання каналу зв'язку із шифруванням дає можливість уникнути введення односторонніх незмінюваних каналів (untappable channels), практична реалізація яких є проблематичною.

Мережа центрів $\{A_j, j = \overline{1,N}\}$ розпочинає роботу по організації виборчого процесу із розгортання системи шифрування RSA, що буде забезпечувати виконання вимоги секретності голосування в даній схемі. Відповідно, кожен правомірний учасник виборів, що має право голосу і бажання взяти участь у виборчому процесі, повинен в обов'язковому порядку пройти процедуру аутентифікації як електронний аналог реєстрації виборців.

Учасники, що не пройшли аутентифікацію до подальших етапів процесу не допускаються. Учасники, що задовольняють усім визначеним критеріям для участі в виборах, після успішного проходження процедури аутентифікації, отримують персональні значення пари ключів, публікуючи відкритий ключ та залишаючи особистий ключ в таємниці.

$$\forall V_i : (Public\ key\ _{V_i}, Private\ key\ _{V_i}) = ((m_{V_i}, e_{V_i}), (m_{V_i}, d_{V_i})).$$

$$\forall A_j : (Public\ key_{A_j}, Private\ key_{A_j}) = ((m_{A_j}, e_{A_j}), (m_{A_j}, d_{A_j})).$$

При цьому існують певні обмеження на вибір ключових параметрів для забезпечення безпомилкового виконання подальших операцій протоколу – центри незалежним чином обирають модулі у зростаючому порядку:

$$m_{A_1} < m_{A_2} < ... < m_{A_{N-1}} < m_{A_N}. \tag{3.2}$$

Детальне обґрунтування введеного обмеження буде наведено далі.

Далі встановлюються правила голосування для виборців: створюється єдиний загальнодоступний список всіх дійсних варіантів вибору $\{v_k^{(0)}, k = 1...L\} = \{v_1^{(0)}, v_2^{(0)}, ..., v_L^{(0)}\}$, сформований наступним

чином:

$$v_k^{(0)} = \begin{cases} p_1 & for\ candidate_1 \\ p_2 & for\ candidate_2 \\ \vdots & \vdots \\ p_L & for\ candidate_L, \end{cases}$$

де $\{p_1, p_2, ..., p_L\}$ – множина відмінних один від одного простих чисел.

Етап голосування (Voting phase)

Для кожного виборця вповноважені центри генерують окремий незалежний список шифртекстів, що відповідають усім можливим варіантам чинних голосів, з якого виборець обирає той, що відповідає бажаному варіанту. Дана процедура забезпечується використанням анонімного каналу зв'язку, описаного в 1.2.

Окрім цього, кожен владний орган генерує для кожного з виборців окрему множину випадкових відмінних один від одного чисел, взаємно простих з модулями центрів. Кожне випадкове число в ході голосування в встановленому порядку буде використовуватись виборцем для покрокової видозміни списку кандидатів для усунення можливості будь-якому центру самостійно прослідковувати голос виборця.

Нехай ε – гомоморфна функція шифрування RSA, що використовується в даній схемі та володіє властивістю адитивного гомоморфізму. А саме, довільному повідомленню x відповідає зашифроване значення $\varepsilon_{(e,m)}(x) = x^e \mod m$. Як результат, для даної функції справедливе співвідношення:

$$\varepsilon(x_1) \cdot \varepsilon(x_2) = x_1^e \cdot x_2^e \mod m = (x_1 \cdot x_2)^e \ mod\ m = \varepsilon(x_1 \cdot x_2).$$

Елементи сформованого списку проходять обробку методом re-encryption mixnet окремо для кожного виборця V_i. Для цього на кожному з центрів $A_j, j = \overline{1, N}$, виконується послідовне перешифрування

кожного елементу списку окремо на відкритому ключі центра з підмішуванням випадкових величин (засліпленням голосу) та його перемішування з застосуванням випадкової перестановки π_{A_j}.

Сама перестановка в свою чергу передається виборцю V_i разом з введеними випадковими множниками у зашифрованому вигляді для забезпечення можливості прослідковування зміни порядку кандидатів на кожному етапі роботи мережі.

Таким чином, завдяки введенню таємних засліплюючих множників разом з перемішуванням на кожному з центрів послідовно, жодний сторонній спостерігач або учасник схеми не має змоги самостійно відтворити порядок перешифрування та перестановки. А отже, за відсутності змови владних центрів, співвідношення елементів початкового списку $\{v_k^{(0)}, k = 1...L\}$ та списку на виході анонімного каналу зв'язку відоме лише виборцю для якого воно відбувалось.

Додатково, виборець здійснє перевірку коректності роботи кожного з центрів, перевіряючи чинність сформованого центром списку. Саме на цьому етапі виникає необхідність використання односторонніх каналів з шифруванням. Нехай для передачі перестановки та випадкових множників від центру A_j виборцю V_i буде використовуватись шифрування на відкритому ключі виборця, а саме: $x^{e_{V_i}} \ mod \ m_{V_i}$. Розшифрувавши отримане повідомлення особистим ключем, виборець робить висновок щодо чесності функціонування центру A_j.

Якщо виборець заперечує коректність формування списку центром A_j, він публічно оголошує це, після чого список повертається до свого попереднього стану $\{v_1^{(A_{j-1})}, v_2^{(A_{j-1})}, ..., v_L^{(A_{j-1})}\}$ і центр ігнорується. Згідно з встановленими обмеженнями моделі довіри, виборець може поскаржитись не більше ніж на $(N - t - 1)$ владних центрів.

Розглянемо етап голосування покроково – для кожного виборця $V_i, i = \overline{1, M}$:

1) Кожен з центрів $A_j, j = \overline{1, N}$ обраховує список $\{v_1^{(A_j)}, v_2^{(A_j)}, ..., v_L^{(A_j)}\}$, а саме: A_j обирає випадкову перестановку

$\pi_j : \{1...L\} \to \{1..L\}$ і випадкові прості числа $\{q_1^{(V_i)(A_j)}, q_2^{(V_i)(A_j)}, ..., q_L^{(V_i)(A_j)}\} \in_R Z_p$, що відповідають обмеженням:

$$q_k^{(V_i)(A_j)} > max\{p_1, p_2, ..., p_L\}, \tag{3.3}$$

$$gcd(q_k^{(V_i)(A_j)}, m_{A_j}) = 1. \tag{3.4}$$

Такий вибір засліплюючих множників зумовлений необхідністю коректного збереження значення голосу в ході наступних перетворень.

Перешифрування k-го елементу $v_k^{(A_{j-1})}$ списку $(k = \overline{1, L})$ здійснюється центром A_j із застосуванням випадкового значення $q_k^{(V_i)(A_j)}$ за наступним правилом:

$$v_k^{(A_j)} = (t_k^{(A_j)})^{e_{A_j}} mod\ m_{A_j},$$

де

$$t_k^{(A_j)} = v_k^{(A_{j-1})} \cdot q_k^{(V_i)(A_j)}.$$

Таким чином, кожен з випадкових множників $q_k^{(V_i)(A_j)}$ відомий лише двом учасникам голосування – V_i та A_j. Знаючи правила перетворення списку кандидатів лише на своєму кроці, жоден з центрів не має змоги ані самостійно відтворити послідовність траснформацій, ані прослідкувати позицію жодного з його елементів.

Для зручності запису введемо позначення:

$$\varepsilon_{<ijk>}(x) = (x \cdot q_k^{(V_i)(A_j)})^{e_{A_j}} mod\ m_{A_j} \tag{3.5}$$

З врахуванням формули 3.5 перетворення k-тої позиції з списку для виборця V_i після взаємодії з центром A_j має вигляд:

$$v_k^{(A_j)} = (((v_k^{(0)} q_k^{(V_i)(A_1)})^{e_{A_1}} mod\ m_{A_1}\Big|_{\pi_1} \cdot q_k^{(V_i)(A_1)})^{e_{A_2}} mod\ m_{A_2}\Big|_{\pi_2} \cdot ... \cdot$$

$$\cdot\ q_k^{(V_i)(A_j)})^{e_{A_j}} mod\ m_{A_j}\Big|_{\pi_j} = \varepsilon_{<ijk>}(...(\varepsilon_{<i2k>}(\varepsilon_{<i1k>}(v_k^{(0)})\Big|_{\pi_1})\Big|_{\pi_2})\Big|_{\pi_j},$$

де $\Big|_{\pi_j}$ – використовується як позначення зміни позиції елементу в загальному списку $\{v_1^{(A_j)}, v_2^{(A_j)}, ..., v_L^{(A_j)}\}$ згідно з застосуванням перестановки π_j.

2) Не розголошуючи перестановку π_j та випадкові значення $\{q_1^{(V_i)(A_j)}, q_2^{(V_i)(A_j)}, ..., q_L^{(V_i)(A_j)}\}$, A_j доводить факт коректності конструювання свого списку $\{v_1^{(A_j)}, v_2^{(A_j)}, ..., v_L^{A(j)}\}$ за допомогою використання системи неінтерактивних доведень.

3) A_j приховано передає таємні параметри (перестановку π_{A_j}) виборцю в зашифрованому вигляді через односторонній відкритий канал, тобто доводить, що $\forall k = \overline{1, L} : v_k^{(V_i)(A_j)}$ є результатом коректної та чесної обробки вхідного значення $v_k^{(V_i)(A_{j-1})}$ центром A_j.

4) Якщо виборець заперечує коректність формування списку, він публічно оголошує це, після чого список повертається до свого попереднього стану $\{v_1^{(A_{j-1})}, v_2^{(A_{j-1})}, ..., v_L^{(A_{j-1})}\}$ і центр A_j ігнорується. Згідно з встановленими обмеженнями, виборець може поскаржитись не більше ніж на $(N - t - 1)$ владних центрів.

5) Виборець V_i оголошує позицію $v_{chosen}^{(V_i)} = v_{x_i}$ свого голосу у фінальному списку $V_i : \{v_k^{(A_N)}, k = \overline{1, L}\}$, що зараховується до реєстру в якості остаточного вибору.

Таким чином, після виконання етапу голосування для кожного виборця, результатом є набір загальновідомих величин $\{v_{x_i}\} = \{v_{x_1}, v_{x_2}, ..., v_{x_M}\}$, що відповідають зашифрованим значенням голосів кожного правомірного учасника схеми V_i.

Підрахунок голосів (Tally phase)

Розглянемо процедуру підрахунку голосів у даній модифікації та її відмінності від аналогічної в оригінальній схемі [9].

Позиція голосу кожного виборця у його власному списку публікується для загального доступу, однак без знання повного набору перестановок $\{\pi_j, j = \overline{1, N}\}$ та випадкових множників жодним чином не порушує конфіденційності голосування.

Процедура підрахунку голосів, як і в оригінальній схемі, здійснюється з використанням властивості гомоморфності функції шифрування. Підбиття результатів починається з обрахунку добутку всіх зашифрованих бюлетенів:

$$F = \prod_{i=1}^{M} v_{x_i} =$$

$$= [\varepsilon_{<1Nx_1>}(...(\varepsilon_{<12x_1>}(\varepsilon_{<11x_1>}(v_{x_1}^{(0)}))))] \cdot [\varepsilon_{<2Nx_2>}(...(\varepsilon_{<22x_2>}(\varepsilon_{<21x_2>}(v_{x_2}^{(0)}))))]\cdot$$

$$\cdot ... \cdot [\varepsilon_{<MNx_M>}(...(\varepsilon_{<M2x_M>}(\varepsilon_{<M1x_M>}(v_{x_M}^{(0)}))))].$$

По завершенню обрахунку значення F, вповноважені органи сумісно (в послідовному порядку) розшифровують добуток голосів. А саме завдяки властивості гомоморфності функції шифрування та обмеженням 3.3 та 3.4 кожен центр почергово знімає свій шар шифрування, застосувавши відомі лише йому значення секретного ключа та випадкових множників без спотворення голосів виборців.

Таким чином для кожного центру A_j, починаючи з останнього центру A_N справедливе співвідношення:

$$A_N : F = \Big([\varepsilon_{<1(N-1)x_1>}(...(\varepsilon_{<12x_1>}(\varepsilon_{<11x_1>}(v_{x_1}))))] \cdot [\varepsilon_{<2(N-1)x_2>}(...$$

$$...(\varepsilon_{<22x_2>}(\varepsilon_{<12x_2>}(v_{x_2}))))] \cdot ... \cdot [\varepsilon_{<M(N-1)x_m>}(...(\varepsilon_{<M2x_M>}(\varepsilon_{<M1x_M>}(v_{x_M}))))]\cdot$$

$$\cdot R_{A_N}^{-1}\Big)^{e_{A_N} \cdot d_{A_N}} mod\ m_{A_N} =$$

$$= [\varepsilon_{<1(N-1)x_1>}(...(\varepsilon_{<12x_1>}(\varepsilon_{<11x_1>}(v_{x_1}))))]\cdot[\varepsilon_{<2(N-1)x_2>}(...(\varepsilon_{<22x_2>}(\varepsilon_{<12x_2>}(v_{x_2}))))]\cdot$$

$$\cdot ... \cdot [\varepsilon_{<M(N-1)x_m>}(...(\varepsilon_{<M2x_M>}(\varepsilon_{<M1x_M>}(v_{x_M}))))].$$

Де

$$R_{A_j} = [q_{x_1}^{(V_1)(A_j)} \cdot q_{x_2}^{(V_2)(A_j)} \cdot ... \cdot q_{x_M}^{(V_M)(A_j)}]$$

$$\vdots$$

$$A_j : F = \Big([\varepsilon_{<1(j-1)x_1>}(...(\varepsilon_{<12x_1>}(\varepsilon_{<11x_1>}(v_{x_1}))))]\cdot[\varepsilon_{<2(j-1)x_2>}(...(\varepsilon_{<22x_2>}(\varepsilon_{<21x_2>}(v_{x_2})$$

$$\cdot ... \cdot [\varepsilon_{<M(j-1)x_M>}(...(\varepsilon_{<M2x_M>}(\varepsilon_{<M1x_M>}(v_{x_M}))))] \cdot R_{A_j}^{-1}\Big)^{e_{A_j}\cdot d_{A_j}} mod\ m_{A_j} =$$

$$= [\varepsilon_{<1(j-1)x_1>}(...(\varepsilon_{<12x_1>}(\varepsilon_{<11x_1>}(v_{x_1}))))]\cdot[\varepsilon_{<2(j-1)x_2>}(...(\varepsilon_{<22x_2>}(\varepsilon_{<21x_2>}(v_{x_2}))))]\cdot$$

$$\cdot ... \cdot [\varepsilon_{<M(j-1)x_M>}(...(\varepsilon_{<M2x_M>}(\varepsilon_{<M1x_M>}(v_{x_M}))))].$$

$$\vdots$$

$$A_1 : \Big([v_{x_1} \cdot v_{x_2} \cdot ... \cdot v_{x_M}] \cdot R_{A_1}^{-1}\Big)^{e_{A_1}\cdot d_{A_1}} mod\ m_{A_1} =$$

$$= p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_L^{c_L}.$$

Множина значень $\{R_{A_j}, j = \overline{1,N}\}$ публікуються для загального доступу, забезпечуючи виконання властивості універсальної перевірності результатів голосування.

Після розшифрування останнім з центрів у разі дотримання обмежень 3.3 та 3.4 отримуємо добуток значень з початкового списку (єдиного, сформованого однаково для всіх виборців) $\{p_1, p_2, ..., p_L\}$, піднесених в степені c_1, ..., c_L , що відповідають загальній кількості голосів на користь кожного з кандидатів зі списку відповідно.

$$Q = p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_L^{c_L}. \tag{3.6}$$

В силу вимоги коректного виконання усіх наведених вище співвідношень виникає необхідність введення додаткового обмеження – обмеження добутку 3.6 зверху найменшим із модулів центрів.

$$Q = p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_L^{c_L} \leq m_{A_1}. \tag{3.7}$$

Лише за умови виконання співвідношення 3.7 значення величини Q, а отже і всі результати електронного голосування, можуть бути відновлені однозначно та безпомилково. Додаткові розрахунки масштабованості наведеної схеми, пов'язані з цим обмеженням, будуть наведені нижче, після опису усіх її етапів.

Для цієї схеми можливе введення додаткового варіанту відповіді $p_0 = 1 - for\ pass$ у початковий список, що відповідатиме бажанню виборця утриматись від подачі будь-якого іншого варіанту. У такому випадку кількість виборців, що утримались від голосування обраховується відніманням отриманих голосів від загальної кількості: $u = M - (c_1 + c_2 + ... + c_L)$.

Оскільки усі значення p_k є простими та загальновідомими, після публікації значення Q відтворити розклад на множники (а отже і дізнатись підсумки голосування) може будь-хто.

Центр публікує числа $\{c_1, ..., c_L, u\}$ в якості результатів голосування.

Завдяки гомоморфності функції голосування, у ході процедури підрахунку та послідовного розшифрування голосів жоден окремий бюлетень не відкривається, оскільки відомим є лише загальна кількість голосів, поданих за кожного з кандидатів у вигляді їх добутку.

Перевірка (Check)

Кожен охочий власноруч перевірити результати голосування володіє наступними загальнодоступними даними:

– набір відкритих ключів центрів $\forall A_j, j = \overline{1,N} : Public\ key_{A_j} = (m_{A_j}, e_{A_j})$, опублікованих на етапі налаштування;

– зашифрований послідовним чином ланцюжком центрів набір виборчих бюлетенів $\{v_{chosen}^{(V_i)}\} = \{v_{x_1}, v_{x_2}, ..., v_{x_M}\}$, опублікований після завершення етапу голосування;

– значення $\{c_1, ..., c_L, u\}$, опубліковані в якості результатів голосування.

– множина значень $\{R_{A_j}, j = \overline{1,N}\}$ в якості підтвердження коректності обрахунку.

Процедура перевірки при цьому має наступний вигляд:

1) Відновлюється значення $Q = p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_L^{c_L}$ і в встановленому порядку проводиться процедура шифрування отриманого числа за допомогою відкритих ключів центрів та додаткових множників $\{R_{A_j}\}$, а саме

$$(((\lfloor p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_L^{c_L} \rfloor \cdot R_{A_1})^{e_{A_1}} mod\ m_{A_1} \cdot R_{A_2})^{e_{A_2}} mod\ m_{A_2} \cdot ... \cdot R_{A_N})^{e_{A_N}} mod\ m_{A_N}.$$

2) Обраховується значення F, що дорівнює добутку всіх бюлетенів, взятих з реєстру: $F = \prod_{i=1}^{M} v_{chosen}^{(V_i)}$.

3) Перевіряється виконання рівності значень, отриманих у перших двох пунктах.

Таким чином, модифікований протокол електронного голосування задовольняє властивостям конфіденційності, перевірності голосу (як

універсальної, так й індивідуальної), справедливості та точності. Даному протоколу також характерна неможливість підробки голосу (receipt-freeness) завдяки наявності у виборця. можливості неоднозначно трактувати свій голос сторонній особі. Завдяки тому, що набір перестановок та засліплюючих множників відомий виборцю, вимога перевірності голосу залишається актуальною для модифікованого протоколу.

Застосуванням методу анонімного каналу зв'язку та попередньо сформованого єдиного списку дійсних варіантів вибору вирішується основна проблема протоколу [9], яка полягала у необхідності відкритої перевірки надісланих виборцем бюлетенів єдиним центром, що порушувало властивість конфіденційності.

Наявність мережі владних центрів (на відміну від єдиного у оригінальному протоколі) робить отриману схему більш стійкою до можливого їх корумпування, змови або збоїв до встановленого рівня t.

Окремої уваги заслуговує порівняння швидкодії та ефективності модифікованої схеми, а, відповідно, і можливості її потенційного масштабування та сфери ефективного застосування.

3.3 Ефективність та сфера застосування отриманої схеми

Розглянемо розрахунок потенційної кількості можливих учасників схеми 3.2, враховуючи необхідність виконання обмеження 3.7, тобто виконання схемою властивості масштабування.

Нехай, найменший з модулів владних центрів m_{A_1} (згідно з обмеженням 3.2) представлено 1024, 2048 або 4096-бітовим числом для трьох різних випадків відповідно (позначимо ці значення як $b_1 = 1024$,

$b_2 = 2048$, $b_3 = 4096$). В такому випадку, згідно з 3.7 отримуємо:

$$max_{\{p_k, c_k\}}\{p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_L^{c_L}\} < 2^{b_i}.$$

Враховуючи факт, що значення $\{p_1, ..., p_L\}$ є відмінними один від одного простими числами, позначимо $p_{max} = max\{p_1, ...p_L\}$. Водночас значення $\{c_i, i = \overline{1, L}\}$ відповідають кількості виборців, що віддали свій голос на користь того чи іншого варіанту зі списку, таким чином максимальне значення будь-якого з них не перевищує кількість виборців M, що беруть участь у голосуванні. Таким чином отримане вище співвідношення матиме наступний вигляд:

$$p_{max}^M < 2^{b_i} \Longrightarrow M_{max} \cdot log_2\, p_L < b_i,$$

де як M_{max} надалі позначатиметься максимальна можлива кількість учасників схеми, виходячи з розрахунків, що включають введені обмеження та обрану довжину ключа.

Наведемо таблицю значень M_{max}, отриманих з останнього співвідношення для випадків $b_i \in \{1024, 2048, 4096\}$ та різної кількості кандидатів у списку $p_{max} \in \{3, 5, 7, 11, 13\}$.

Таблиця 3.1 – Розрахунок значення максимальної кількості учасників виборів M_{max} для різних значень довжини ключа та кількості кандидатів.

	$b_1 = 1024$	$b_2 = 2048$	$b_3 = 4096$
$p_L = 3$	646	1292	2584
$p_L = 5$	441	882	1764
$p_L = 7$	364	729	1459
$p_L = 11$	296	592	1184
$p_L = 13$	276	553	1106

Як видно з отриманих результатів, обмеження 3.7 зумовлює істотне

зниження кількості можливих учасників електронного голосування за схемою 3.2. Для актуальних довжин ключів криптосистеми RSA кількість учасників не перевищує 2584 для усіх можливих значень параметрів, що значно звужує можливу область застосування отриманої схеми до дрібномасштабних голосувань.

Розглянемо також розрахунок мінімальної допустимої довжини засліплюючих множників $\{q_k^{(V_i)(A_j)}, k = \overline{1,L}, i = \overline{1,M}, j = \overline{1,N}\}$ такої, щоб ймовірністю виникнення колізії однакових множників, використаних одним і тим самим центром, можна було знехтувати.

Нагадаємо, що кожному центру A_j необхідно згенерувати M значень (по одному для кожного виборця) засліплюючих множників так, щоб жодні два з них не збіглися. Використовуючи отримані вище практичні значення M_{max} проведемо розрахунки оптимальної довжини цих множників, використавши для цього формулу визначення ймовірності наявності принаймні однієї колізії [12] для M_{max} значень засліплюючих множників.

$$M_{max} = \sqrt{z \cdot ln\Big(\frac{1}{1-p}\Big)},$$

де $(1-p)$ – ймовірність того, що жодне з M_{max} значень не збігається з будь-яким іншим, а z – потужність множини простих чисел, що задовольняють поставленим умовам вибору значень множників.

Для обчислення обмеження розміру засліплюючих множників, що використовуються в схемі, скористаємося формулою для визначення кількості простих чисел, не менших за x [11]:

$$z = \pi(x) = \sum_{primes \le x} \mathbb{1} = \frac{x}{lnx}.$$

Таким чином, отримавши співвідношення для визначення значення x, отримаємо мінімальне допустиме значення верхньої межі інтервалу, придатного для вибору коректних значень $\{q_k^{(V_i)(A_j)}\}$ з встановленим

рівнем ймовірності знаходження колізії p:

$$\frac{x}{lnx} = \frac{M_{max}^2}{-ln(1-p)}. \tag{3.8}$$

Розрахуємо, згідно із співвідношенням 3.8, числові значення величини x для найбільших значень $M_{max} \in \{646, 1292, 2584\}$, отриманих в 3.1 для кожної з довжин ключів. Нехай ймовірність знаходження колізії для подальших розрахунків становить $p = 2^{-80}$. В таблиці 3.2 вказано довжину в бітах отриманих значень x в двійковому представленні.

Таблиця 3.2 – Мінімальний розмір засліплюючих множників $q_k^{(V_i)(A_j)}$ для забезпечення відсутності колізій з заданою ймовірністю

	$b_1 = 1024$	$b_2 = 2048$	$b_3 = 4096$
$size\ (bits)$	105	107	109

Таким чином бачимо, що обираючи множники $q_k^{(V_i)(A_j)}$ на кожному етапі довжиною 128 біт, виконання усіх необхідних властивостей буде збережено.

Окрім здатності до масштабування, перевіримо також ефективність отриманої модифікації, обрахувавши складність реалізації схеми для різних значень параметрів, що визначають конфігурацію схеми. Відповідно до отриманих результатів можна буде зробити висновки про ефективні сфери застосування схеми.

Нехай, в протоколі електронного голосування 3.2 беруть участь M виборців $\{V_i, i = \overline{1, M}\}$ та N владних органів $\{A_j, j = \overline{1, N}\}$. Кожен бюлетень, відповідно до типу голосування 1-out-of-L-voting містить L можливих варіантів вибору.

Дана модифікація заснована на поєднанні методів гомоморфного шифрування, з використанням криптосистеми RSA та анонімного каналу зв'язку, а саме мереж перемішування. Таким чином, для визначення необхідних обрахункових потужностей для кожного з етапів процедури,

наведемо спочатку складність їх основних складових частин.

Як відомо, шифрування повідомлення у криптосистемі RSA відбувається за правилом $c = m^e \ mod \ n$, де відкритий ключ (e, n) використовується для зашифрування повідомлення $m \in Z_n$. Згідно з [1], швидкість виконання цієї операції з використанням швидкого алгоритму піднесення до степеня становить $O(\ln e)$ операцій множення по модулю.

Нехай для здійснення операції множення по модулю використовується алгоритм Карацуби, тоді для множення двох t-бітових чисел необхідно $t^{log_2 3}$ бітових операцій [13]. Таким чином, процедура шифрування у криптосистемі RSA з використанням відкритого ключа (e, n), де n – b-бітове число потребує $O(\ln e \cdot b^{log_2 3})$.

Складність методу генерації випадкової перестановки, що використовується кожним центром для перемішування L-елементного списку, становить $O(L)$.

Ще одним складовим кроком протоколу є засліплення кожного елементу списку шляхом множення на випадковий множник. Складність цієї операції з використанням ефективного алгоритму Карацуби в гіршому випадку можна оцінити як $O(t^{log_2 3})$, де t – довжина найбільшого з модулів владних центрів, згідно з обмеженням 3.2.

Отже, відповідно до запропонованої модифікації протоколу електронного голосування 3.2, кожним з N владних центрів мережі для кожного з M виборців здійснюється:

– L шифрувань елементів списку по системі RSA з застосуванням ключа (e_{A_j}, m_{A_j}).

– L засліплень елементів списку випадковими множниками $q^{(V_i)(A_j)}$.

– єдине застосування випадкової перестановки до сформованого списку кандидатів, довжиною L

– одне шифрування таємного набору параметрів для підтвердження виборцю коректності трансформації списку (на відкритому ключі виборця (e_{V_i}, m_{V_i})).

В результаті, для N центрів та M виборців з використанням

b-бітового відкритого ключа криптосистеми, складність проведення етапу голосування становить:

$$O\Big((L \cdot \ln e \cdot b^{log_2 3} + L \cdot b^{log_2 3} + L)MN\Big) = O\Big(LMN((\ln e + 1) \cdot b^{log_2 3} + 1)\Big).$$

3.4 Модифікація протоколу з використанням протоколу розподілу секрету

Нагадаємо, що основним недоліком оригінального протоколу 3.1 є здійснення перевірки отриманих від виборців бюлетенів єдиним центром і відповідне порушення конфіденційності та високий ризик корумпованості результатів.

Перший варіант покращення 3.2 вирішує цю проблему шляхом позбавлення виборців можливості самостійно генерувати бюлетені та застосуванням мережі владних центрів для розподілу організаційного навантаження. Однак, як було зазначено вище, основним недоліком запропонованої схеми є низька здатність до масштабування через принципові обмеження в використанні.

Розглянемо альтернативний варіант покращення схеми 3.1 шляхом введення використання схеми розподілу секрету на етапі голосування. Основна ідея полягає в тому, щоб перед передачею голосу до виділеного центру (надалі – центра-колектора) для перевірки, здійснюється розподіл зашифрованого голосу, підписаного виборцем, між учасниками додатково виділеної мережі владних органів (рисунок 3.2).

Перевіривши чинність особи виборця, кожен з них анонімізує власну частку голосу та надсилає її незалежним чином центру-колектору, обов'язком якого є безпосередня перевірка реконструйованого анонімного голосу та результуючий облік та підрахунок голосів.

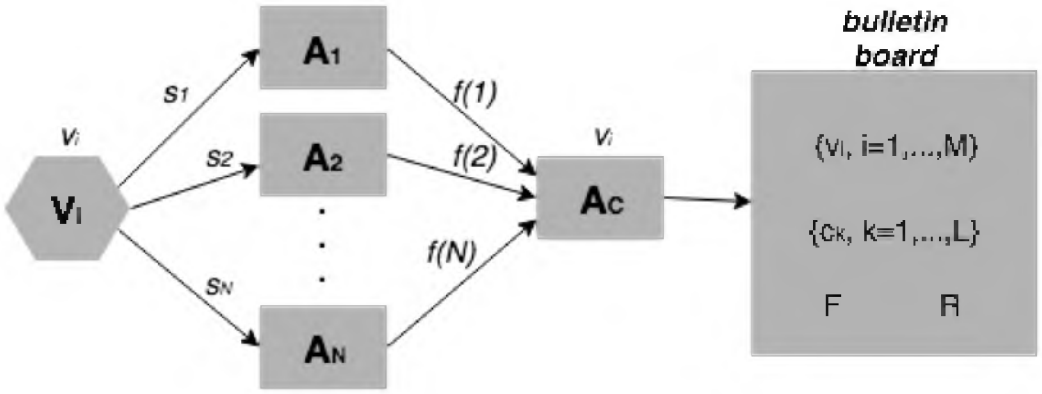

Рисунок 3.2 – Схема модифікації протоколу 3.1 з використанням протоколу розподілу секрету

Загальна структура модифікованого варіанту мало відрізняється від оригінальної схеми, за винятком додавання кроку розподілу та проходження голосом мережі владних центрів перед переходом до етапу підрахунку результатів. Розглянемо запропоновану процедуру покроково.

Етап налаштування передбачає створення та ініціалізацію криптосистеми RSA для всіх учасників протоколу, а саме мережі з N владних органів $\{A_j, j = \overline{1, N}\}$, окремого виділеного органу-колектора A_c з парою ключів $(e_{A_c}, m_{A_c}), (d_{A_c}, m_{A_c})$, $min_i\{m_{V_i}\} > m_{A_c}$ та M виборців, що отримують доступ до процесу голосування лише у разі успішного проходження процедури аутентифікації. Запропонована модель системи владних органів також є пороговою, тобто існує порогове значення t, наявність якого означає, що як мінімум t владних центрів функціонують гарантовано чесно.

Далі формується і розголошується єдиний для всіх учасників голосування список дійсних варіантів вибору, сформований згідно з

наступним правилом:

$$b_i = \begin{cases} p_1 & for\ candidate_1 \\ p_2 & for\ candidate_2 \\ \vdots & \vdots \\ p_L & for\ candidate_L. \end{cases} \tag{3.9}$$

Таким чином набір значень $\{p_1, ..., p_L\}$ є загальнодоступним набором унікальних простих чисел, кожне з яких поставлено у відповідність певному варіанту вибору.

На *етапі голосування* бюлетень виборця v_i формується аналогічно оригінальній схемі 3.1: після вибору секретного значення параметру b_i, що відповідає встановленим правилам подачі голосу за певного кандидата 3.9, виборець самостійно зашифровує засліплений випадковим множником q_i голос на відкритому ключі органа-колектора:

$$V_i: \ v_i = (b_i \cdot \ q_i)^{e_{A_c}} \ mod \ m_{A_c}.$$

Наступним додається використання $(t+1, N)$-схеми розподілу секрету між центрами $\{A_1, ..., A_N\}$ для поділу величини v_i для кожного виборця V_i. Відповідно до обраної схеми відбувається наступна послідовність кроків ([14]).

1) Виборець V_i випадковим чином обирає поліном f степеня t так, що $f(0) = v_i$:

$$f(x) = v_i + a_1 x + ... + a_t x^t.$$

Кожен орган влади A_j отримує власну частку, зашифровану особистим ключем виборця d_{V_i} по незмінюваному каналу:

$$s_j = f(j)^{d_{V_i}} mod \ m_{V_i}.$$

2) Відновлення значення голосу v_i здійснюється в два етапи, починаючи з перевірки істинності особи виборця, шляхом розшифрування частки голосу його відкритим ключем:

$$s_j^{e_{V_i}} = f(j)^{d_{V_i} \cdot e_{V_i}} mod\ m_{V_i} = f(j).$$

Далі кожен з органів $\{A_j, j = \overline{1, N}\}$ передає отриману частку одностороннім незмінюваним каналом органу-колектору A_c, який, в свою чергу, відновлює голос, обчисливши значення v_i за формулою:

$$v_i = \sum_{j \in A} s_j \cdot \lambda_j, \tag{3.10}$$

де λ_j – коефіцієнт Лагранжа [1].

У разі дотримання усіх вказаних заходів безпеки, кожен з органів $A_j, j = \overline{1, N}$ знає лише власну частку голосу s_j, а отже, для випадку відсутності змови більше ніж t центрів, жодним чином відновити голос не може, а лише перевіряє його чинність шляхом перевірки коректності підпису виборця.

Колектор A_c в свою чергу отримує уже перевірені частки голосу без підпису виборця, тому відновити зв'язок "voter-vote" він не може, а отже, таємниця голосування не порушується.

A_c відновлює голоси виборців, перевіряє їх чинність після розшифрування кожного окремого голосу особистим ключем d_{A_c}, а саме:

$$v_i^{d_{A_c}} = (b_i \cdot\ q_i)^{e_{A_c} \cdot d_{A_c}}\ mod\ m_{A_c} = (b_i \cdot\ q_i)\ mod\ m_{A_c}.$$

По завершенню етапу голосування A_c публікує набір голосів $\{v_i, i = \overline{1, M}\}$, що успішно пройшли перевірку, у відкритому каналі з пам'яттю (bulletin board), задовольняючи умови універсальної та індивідуальної перевірності. Якщо після розголошення списку прийнятих бюлетенів жодний з виборців не нарікає на відсутність врахування його голосу, процедура переходить до наступного етапу.

Обрахунок голосів може здійснюватись колектором A_c методом прямого підрахунку, оскільки величина усіх голосів $v_i^{d_{A_c}}$ уже є відомою йому після здійснення процедури відновлення 3.10. Колектор публікує множину результатів $\{c_1, c_2, ..., c_L\}$, кожен елемент якої відповідає кількості виборців, що проголосували за кандидатів $\{1, 2, ..., L\}$ відповідно.

Далі для задоволення властивості універсальної та індивідуальниї *перевірності* здіснюється обрахунок контрольних величин F та Q. F дорівнює добутку опублікованих голосів у зашифрованому вигляді:

$$F = \prod_{i=1}^{M} v_i.$$

Величина Q відповідає добутку голосів виборців після розшифрування:

$$Q = F^{d_{A_c}} mod\ m_{A_c} = (\prod_{i=1}^{M} v_i)^{d_{A_c}} mod\ m_{A_c} =$$

$$= \prod_{i=1}^{M} v_i^{d_{A_c}} mod\ m_{A_c} = \prod_{i=1}^{M} b_i \cdot q_i\ mod\ m_{A_c}.$$

При цьому повинне залишатись справедливим обмеження $Q < m_{A_c}$. Враховуючи множину можливих значень b_i та q_i можливо обрахувати представлення:

$$Q = p_1^{c_1} \cdot p_2^{c_2} \cdot ... \cdot p_2^{c_2} \cdot R,$$

де $R = \prod_{i=1}^{M} q_i$ – добуток усіх використаних випадкових множників. Значення F та R публікуються.

Володіючи цими значеннями та множиною результатів виборів $\{c_1, c_2, ..., c_L\}$, будь-який сторонній спостерігач має можливість відновити значення Q та перевірити виконання співвідношення $Q^e\ mod\ m \stackrel{?}{=} F$.

Даний протокол, аналогічно оригіналу, може бути узагальнений для типу голосування з кількома можливими варіантами відповіді k-out-of-L

voting.

Таким чином, запропонований варіант модифікації протоколу 3.1 відповідає властивостям конфіденційності, перевірності голосу (універсальній та індивідуальній), справедливості та точності. Наявність мережі владних центрів, що сумісно перевіряють підпис виборця на окремих частинах його зашифрованого голосу, позбавляє схему основного недоліку – наявності єдиного центру, що порушує таємність голосування, володіючи співвідношенням голосу виборця та його особистості.

Перейдемо до обрахунку складності реалізації даної модифікації в залежності від параметрів схеми M та N, що дозволять робити висновки щодо її ефективності та здатності до масштабування.

Загальна оцінка складності $(t+1, N)$-схеми розподілу секрету Шаміра становить $O(tN)$ ([1]). Кожен виборець здійснює N зашифрувань по системі RSA отриманих в результаті виконання протоколу розподілу часток. Складність кожної з яких становить $O(\ln e \cdot b^{log_2 3})$ бітових операцій для відповідного відкритого ключа (e, n), де b – довжина модуля n в бітах. Кожен з центрів $\{A_1, ..., A_N\}$ здійснює по одному розшифруванню власної частки голосу для кожного з виборців.

Таким чином етап голосування займає:

$$O\Big(N \ln e \cdot b^{log_2 3} + N \ln d \cdot b^{log_2 3} + tN\Big) = O\Big(N(b^{log_2 3}(\ln e + \ln d) + t)\Big).$$

Складністю підрахунку голосів можна знехтувати, оскільки він здійснється центром-колектором методом прямого підрахунку.

Висновки до розділу 3

У розділі запропоновано дві альтернативних модифікації для вирішення проблеми порушення секретності голосу в оригінальному

протоколі [9], що полягала у необхідності перевірки коректності голосу (відсутності хибних або продубльованих голосів) єдиним центром влади шляхом розшифрування надісланих виборцями голосів $\{v_k, k = \overline{1, M}\}$.

У першій з них (3.2) вирішення полягало у відсутності можливості у виборця спотворити/продублювати свій голос через відсутність можливості його генерації (лише вибір з готового списку коректних голосів), а взаємозв'язок "voter-vote" захищено набором випадкових перестановок re-encryption mixnet за умови виконання початкового припущення про гарантовано чесне функціонування мінімум t владних центрів.

Другий варіант (3.4) вирішував проблему порушення конфіденційності шляхом введення допоміжної мережі владних органів та реалізації схеми розподілу секрету (голосу виборця) між ними. Уже перевірені частки голосів виборців передаються органу-колектору для перевірки та підрахунку в анонімізованому вигляді.

Обидва варіанти модифікацій схем голосування (1-out-of-L voting) можливо модифікувати для використання з іншими типами систем голосування, наприклад, вибору кількох кандидатів зі списку зі (k-out-of-L voting), тощо, зі збереженням усіх заявлених властивостей.

ВИСНОВКИ

В даній роботі досліджено протоколи електронного голосування, криптопримітиви та механізми забезпечення основних функцій безпеки, необхідних для їх практичної реалізації.

Проведено розгорнутий огляд стандартного поділу сценарію виборчого процесу на послідовність етапів, їх взаємозв'язок та характерні особливості функціонування усіх учасників процесу. Також сформульовано постановку задачі електронних виборів, представлено базові криптопримітиви, комбінування та модифікація яких реалізує забезпечення основних критеріїв ефективного та безпечного протоколу електронного голосування.

Далі було проведено роботу над класифікацією наявних підходів до створення та розробки систем електронного голосування, відштовхуючись від способу забезпечення конфіденційності особистого голосу виборця. Порівняльний аналіз кожного з класів систем виділяє набір характерних сильних та слабких сторін типових представників кожного класу та основних криптографічних методів їх реалізації.

Підкресливши брак безпеки в існуючих схемах електронного голосування, подальше дослідження було зосереджено на створенні нового варіанту протоколу електронного голосування, максимально наближеного до універсальної моделі протоколу з відповідністю усім критичним вимогам безпеки.

На основі розглянутих теоретичних результатів, у кінцевому розділі було запропоновано два варіанти модифікації попередньо вибраного протоколу голосування з метою коригування його основних недоліків. Обраний варіант системи голосування не задовольняв критерію конфіденційності голосу відносно єдиного владного центру схеми.

Базуючись на результатах аналізу опорних криптопримітивів-складових протоколів електронного голосування,

перший варіант вдосконаленої схеми використовував анонімний канал зв'язку як основний механізм вирішення наявної проблеми, другий – протокол розподілу секрету.

Перша запропонована модифікація завдяки запровадженню мережі перемішування позбавляє виборця можливості самостійно генерувати бюлетень, тим самим знищивши необхідність розкриття голосу центром з метою його перевірки. Основним недоліком отриманої схеми є її низька здатність до масштабування через наявність кількох принципових обмежень стосовно основних параметрів.

Друга запропонована модифікація після розгортання схеми розподілу секрету анонімізує голос виборця по частинам, що позбавляє центр-колектор можливості відновити зв'язок особистості виборця з його голосом на етапі перевірки та обрахунку голосів. Запропонована схема вирішує проблему конфіденційності, порушену в оригінальному протоколі, без втрати основних його переваг у вигляді універсальної та індивідуальної перевірності.

Отримані вдосконалення протоколу голосування гарантують виконання зазначених в них функцій безпеки, а їх потенційна практична реалізація вважається ефективною для визначених сфер можливого застосування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bruce Schneier. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C. / Bruce Schneier. — N.Y.: Wiley Computer Publishing, John Wiley Sons, Inc, 1996 — 760c. — ISBN 0-471- 12845-7.

2. Gritzalis D., Principles and requirements for a secure e-voting system. / Gritzalis D. — Computers Security, Vol. 21(6), 2002 — C. 539-556, [Електронний ресурс]. — Режим доступу: http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/aegean/paper7.pdf.

3. Aditya Riza. Secure electronic voting with flexible ballot structure. / Aditya Riza — PhD thesis, Queensland University of Technology,2005 — 200 с. [Електронний ресурс]. — Режим доступу: http://eprints.qut.edu.au/16156/1/Riza_Aditya_Thesis.pdf.

4. Evaluating e-voting: theory and practice / Manon de Vries and Wouter Bokslag — Department of Information Security Technology Technical University of Eindhoven, 2016. [Електронний ресурс]. — Режим доступу: https://arxiv.org/pdf/1602.02509.pdf.

5. Survey on Remote Electronic Voting / Alexander Schneider. — Christian Meter Philipp Hagemeister, 2017. [Електронний ресурс]. — Режим доступу: https://arxiv.org/pdf/1702.02798.pdf.

6. Benaloh J.C. "Verifiable Secret Ballot Elections"/ Benaloh J.C. — PhD thesis, Yale University, 1987.

7. Chaum D.L. Secret-Ballot Receipts: True Voter-Verifiable Elections / Chaum D.L. — IEEE Security Privacy Magazine, Feb 2004.

8. Sampigethaya K. A framework and taxonomy for comparison of electronic voting schemes / Sampigethaya K., Poovendran R — Computers security, 2006, 25 — С.137–153. [Електронний ресурс]. — Режим доступу: https://www.ee.washington.edu/research/nsl/papers/JCS-05.pdf.

9. Музыкантский А. И. Лекции по криптографии. / Музыкантский А. И., Фурин В. В. — М.: МЦНМО, 2013 — 2-е изд., — 68 с.

10. Martin Hirt. Efficient Receipt-Free Voting Based on Homomorphic Encryption / Martin Hirt, Kazue Sako — International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2000: Advances in Cryptology — С. 539-556.

11. А.А. Бухштаб. Теория чисел / А.А. Бухштаб — Рипол Классик, 2013. — 331-333 с.

12. Молдовян Н. А. Введение в криптосистемы с открытым ключом. / Молдовян Николай Андреевич — Петербург, 288 С, 2005. — С. 195-199.

13. Alfred J. Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone — CRC Press,ISBN: 0-8493-8523-7.б 2001. — С. 290-291, 612-613.

14. Shamir A. How to Share a Secret / Shamir A. — Communications of the ACM., 1979, Nov. — Vol. 24, N. 11. — С. 612–613.