НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2022 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика
на тему: **«Протоколи електронного голосування»**

Виконав: студент 4 курсу, групи ФІ-84
Матвійчук Яна Андріївна

Керівник: д.ф.-м.н., професор Савчук М. М. _____

Консультант: _ _____

Рецензент: звання, степінь, посада Прізвище І.П. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2022

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність (освітня програма) — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2022 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Матвійчук Яна Андріївна

1. Тема роботи: «*Протоколи електронного голосування*»,
керівник: д.ф.-м.н., професор Савчук М. М.,
затверджені наказом по університету №__ від «__» _____ 2022 р.

2. Термін подання студентом роботи: «__» _____ 2022 р.

3. Вихідні дані до роботи: *Відомі криптографічні алгоритми та протоколи електронного голосування.*

4. Зміст роботи: *Проведено огляд основних алгоритмів та елементів електронного голосування, виконано опис централізованого протоколу та децентралізованої схеми електронного голосування з використанням блокчейну. Проведено конкретизацію схеми електронного голосування за допомогою криптографічних алгоритмів.*

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *«Презентація доповіді»*

6. Дата видачі завдання: 10 вересня 2021 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2021 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2021 р.	Виконано
3	Розбір вимог та елементів електронного голосування	Листопад-грудень 2021 р.	Виконано
4	Ознайомлення з відомими протоколами електронного голосування	Січень-лютий 2022 р.	Виконано
5	Вибір протоколів для подальшої роботи	Березень 2022 р.	Виконано
6	Опис обраних протоколів, їхніх переваг та недоліків	Квітень 2022 р.	Виконано
7	Конкретизація обраного протоколу електронного голосування	Травень 2022 р.	Виконано
8	Оформлення дипломної роботи та підготовка до захисту	Червень 2022 р.	Виконано

Студент _____ Матвійчук Я. А.

Керівник _____ Савчук М. М.

РЕФЕРАТ

Кваліфікаційна робота обсягом 49 містить 8 рисунків та 19 джерел.

Метою роботи є конкретизація та дослідження існуючого протоколу децентралізованого електронного голосування з використанням блокчейну.

Об'єктом дослідження є інформаційні процеси в системах та засобах електронного голосування.

Предметом дослідження є криптографічні методи забезпечення захисту протоколів електронного голосування.

У роботі наведено опис схеми електронного голосування з використанням блокчейну, опис протоколу електронного голосування з декількома комісіями для підрахунку голосів. Також у роботі описано загальні принципи децентралізованих схем електронного голосування.

Проведено конкретизацію схеми, яка наведена у роботі за допомогою обраних криптографічних примітивів та алгоритмів. Деякі кроки з неї перетворені та декілька кроків додано для забезпечення кращої захищеності даного протоколу.

Результати роботи можуть слугувати основою для подальшого покращення та реалізації електронного голосування з використанням технології блокчейн.

Ключові слова: ЕЛЕКТРОННЕ ГОЛОСУВАННЯ, ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ, ДЕЦЕНТРАЛІЗОВАНА СХЕМА, БЛОКЧЕЙН, КРИПТОГРАФІЧНІ АЛГОРИТМИ, ГЕШ-ФУНКЦІЯ КУПИНА, КРИПТОСИСТЕМА RSA.

ABSTRACT

Qualification work contains: 49 pages, 8 figures and 19 sources.

The purpose of this work is to specify and explore the existing protocol of decentralized electronic voting using the blockchain.

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

The subject of the research is cryptographic methods to ensure the protection of electronic voting protocols.

The paper describes the scheme of electronic voting using a blockchain, a description of the protocol of electronic voting with several commissions for counting votes. Also in the work the general principles of decentralized electronic voting schemes were described.

The concretization of the scheme, which is given in the work, was done using selected cryptographic primitives and algorithms. Some steps from it have been changed and a few steps have been added to provide better security for this protocol.

The results of the work can serve as a basis for further improvement and implementation of electronic voting using blockchain technology.

Keywords: ELECTRONIC VOTING, ELECTRONIC VOTING PROTOCOLS, DECENTRALIZED SCHEME, BLOCKCHAIN, CRYPTOGRAPHIC ALGORITHMS, KUPYNA HASH FUNCTION, RSA CRYPTOSYSTEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДМТ — детермінованя машина Тьюринга.

ЕПЦ — електронний цифровий підпис.

FBI— фіксований бітовий індекс.

E_k — шифрування повідомлення ключем k.

B — виборчий бюлетень.

A — агенство електронного голосування.

M — повідомлення.

Sign — цифровий підпис відправника.

H — криптографічна геш-функція.

Cert — сертифікат відкритого ключа відправника.

ID — унікальний ідентифікатор відправника виданий йому на етапі первинної ідентифікації.

Status — статус сертифіката відкритого ключа відправника.

PKI — інфраструктура відкритого ключа.

ВСТУП

Актуальність дослідження. Вибори є першочерговою ознакою демократичної політичної системи країни, необхідний і найважливіший механізм здійснення волевиявлення громадян. Електронне голосування є соціальним застосуванням криптографічних методів захисту процесу голосування. Дана робота присвячена дослідженню актуальних схем електронного голосування.

Дослідження протоколів електронного голосування є актуальною задачею, оскільки їх використання спрощує саму процедуру голосування та підвищує інтерес до виборчого процесу. Також електронне голосування допомагає зменшити витрати на виборчий процес, збільшити доступ громадян з обмеженими можливостями до процедури голосування, а також покращує надійність процедури підрахунку голосів.

У ході роботи ставляться наступні завдання:

– формування вимог та дослідження властивостей, яким мають задовольняти протоколи електронного голосування;

- дослідження криптографічних елементів, які використовуються у протоколах електронного голосування;

– аналіз існуючих схем та протоколів електронного;

– конкретизація однієї обраної схеми електронного голосування та аналіз отриманого протоколу.

Метою дослідження є конкретизація та дослідження існуючого протоколу децентралізованого електронного голосування з використанням блокчейну.

Об'єктом дослідження є інформаційні процеси в системах та засобах електронного голосування.

Предметом дослідження є криптографічні методи забезпечення захисту протоколів електронного голосування.

Наукова новизна полягає у розробці деталізованого протоколу

електронного голосування з використанням блокчейну з вибором конкретних криптографічних алгоритмів.

Практичне значення одержаних результатів. Розроблений протокол електронного голосування може слугувати основою для подальшого покращення та реалізації електронного голосування з викорстанням технології блокчейн.

1 ВИМОГИ, АЛГОРИТМИ ТА ЕЛЕМЕНТИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Голосування є важливою подією у багатьох демократичних країнах, однак традиційні системи голосування можуть бути неефективними, враховуючи велику кількість територій та населення, що беруть участь у сучасних виборах.

Очевидний той факт, що враховуючи активний розвиток інформаційних технологій, велика кількість розвинених демократичних країн переходить до електронної політичної інфраструктури та інструментів електронної демократії, зокрема проводить електронні вибори та голосування. Останнє є відносно безпечним, таємним голосуванням за допомогою інформаційно-комунікаційних технологій, результати якого передаються через мережу Інтернет. Електронні вибори, внаслідок своєї простоти та зручності у використанні, збільшують явку виборців, сприяють активному голосуванню молоді, та представництв національних меншин. Отже, процес електронного голосування дозволяє практично унеможливити людський фактор, внаслідок чого результати стають максимально точними та надійними. На сьогодні інструмент електронних виборів широко використовується в США, Канаді, Австралії, Великобританії, Німеччині, Франції, Іспанії, Португалії, Італії, Норвегії, Швейцарії, Бельгії та Естонії.

У даному розділі буде наведено основні відомості та означення, вимоги до протоколів електронного голосування та основні криптологічні алгоритми та елементи, які використовуються у системах електронного голосування.

1.1 Основні відомості та означення

Означення 1.1 Термін електронне голосування визначається як голосування з будь-якого публічного питання, зокрема участь в опитуваннях, виборах, референдумах, що передбачає використання електронних засобів для ідентифікації та підрахунку голосів.[1]

Означення 1.2 Криптографічний протокол – це деяка процедура зі строгими правилами обміну інформацією,з використанням криптографічного захисту, між двома або більше сторонами.[1]

Означення 1.3 Протокол електронного голосування – це набір криптографічних алгоритмів для реалізації безпечного таємного електронного голосування через інтернет за допомогою комп'ютерів, телефонів або інших спеціальних обчислювальних машин.[1]

Означення 1.4 Односторонньою функцією називається відображення $y = f(x)$: X $\rightarrow$ Y, таке що:

– для будь-якого x є X існує алгоритм поліноміальної часової складності на ДМТ обчислення $y = f(x)$;

– майже для будь-якого y є Y не існує поліноміального алгоритму на ДМТ обчислення оберненої функції $x = f^{(-1)}(y)$.[1]

Означення 1.5 Односторонньою функцією з секретом називається відображення y=f (x): X $\rightarrow$ Y, яке залежить від деякого параметра k і таке, що виконуються умови:

– для будь-якого k, x існує поліноміальний часовий алгоритм на ДМТ обчислення $y = f(x)$, при цьому знати k не обов'язково;

– При невідомому k не існує поліноміального алгоритму обчислення оберненої функції $x = f^{(-1)}(y)$ майже для будь-якого k, y;

– При відомому k існує поліноміальний алгоритм (на ДМТ) обчислення оберненої функції $x = f^{(-1)}(y)$ для будь-якого k, y.[1]

Означення 1.6 Електронний цифровий підпис (ЕЦП) — вид електронного підпису, отриманого за результатом криптографічного

перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. ЕЦП використовується для аутентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.[1]

Означення 1.7 Геш-функція – математична функція, що перетворює бітовий рядок будь-якої довжини в бітовий рядок фіксованої довжини. Формат запису цього рядка може бути довільним, наприклад шістнадцятковим. Такий рядок називається геш-значенням. При цьому незначна зміна аргументу функції приводить до того, що в середньому змінюється приблизно половина бітів у значенні функції.[1]

Означення 1.8. Алгоритм шифрування називається гомоморфним, якщо для даних $E_k(m_1)$ та $E_k(m_2)$ можливо отримати значення $E_k(m_1 \bigodot m_2)$ для певної операції $\bigodot$, без безпосереднього розшифрування окремих значень m_1 та m_2.[1]

Означення 1.9. Базою даних можна вважати будь-який структурований набір інформації, що зберігається, в певному форматі, в електронному вигляді в комп'ютерній системі. Частіше за все бази даних мають вигляд таблиці, для спрощення пошуку у великому об'ємі даних.[1]

Означення 1.10. Інфраструктура відкритих ключів (Public Key Infrastructure – PKI) – це інтегрований комплекс методів та засобів (набір служб), призначених забезпечити впровадження та експлуатацію криптографічних систем із відкритими ключами.[3]

1.2 Загальна схема електронного голосування.

Будь-який електронний виборчий процес повинен складатися з п'яти етапів[5]:

Підготовчий етап(налаштування). На даному етапі проводиться

налаштування системи голосування, формуються вимоги та критерії для виборців, кандидатів та органів влади. Також обирається процедура виборів, підрахунку голосів, автентифікації виборців та вимоги для дійсності електронного бюлетеню. Далі проводиться реєстрація кандидатів, після якої всі параметри налаштування розголошуються.

Етап реєстрації. Розміщуються списки можливих виборців, користувачі оголошують про своє бажання голосувати та реєструються в визначених органах реєстрації. Після цього викладаються списки законних виборців.

Етап голосування. Брати участь можуть лише зареєстровані виборці. Кожен виборець автентифікується та отримує пустий бюлетень. Далі учасник фіксує свій вибір. Щоб уникнути тиску, це має відбуватись у надійному та прихованому місці. У бюлетені відповідність виборця та його голосу засекречена. Потім бюлетень відправляється у центр організації виборів.

Етап підрахунку голосів. На цьому етапі центр організації виборів верифіковує бюлетені та підраховує голоси. Далі проводиться публікація фінальних результатів виборів.

Додатковий етап перевірки. На всіх, крім першого етапу відбувається перевірка кількості виборців, коректності голосування відповідно до обраної схеми голосування.

1.3 Вимоги та властивості протоколів електронного голосування

Голосування розбивається на стільки етапів, для того, щоб забезпечувати відповідність вимогам електронного голосування. Для того, щоб бути безпечною, схема електронного голосування повинна задовольняти 8 вимогам[4]:

1. Голосувати може лише зареєстрована людина.

2. Кожен виборець може проголосувати лише один раз.

3. Всі голоси враховуються анонімно – зберігається таємниця виборів.

4. Проголосувавши, ніхто не має змоги змінити своє рішення.

5. Повинна бути забезпечена неможливість підробки результатів голосування.

6. Повинна бути можливість відкрито перевірити результати голосування.

7. Кожен повинен мати можливість впевнитись у правильності підрахунку голосів.

8. Має бути можливість дізнатися скільки людей проголосувало.

Виходячи з основних вимог, схема електронного голосування повинна задовольняти наступним властивостям:

Правомірність голосу

Брати участь можуть лише зареєстровані виборці та кожен виборець має бути автентифікованим. Жоден виборець не може голосувати більше одного разу.

Точність результатів

Системи голосування мають правильно фіксувати голоси та обраховувати результати.

Перевіреність голосу

Повинна бути можливість перевірити правильність підрахунку при остаточному підрахунку голосів. Повинні бути надійні та достовірні записи про вибори. Кожен виборець повинен мати можливість перевірити, що його голос був зарахований правильно та підрахований при підведенні підсумків.

Надійність

Система повинна бути стійкою до активних та пасивних атак, а також бути надійною при змові всіх органів влади. Система повинна працювати надійно навіть при численних збоях. Також система повинна бути стійкою до маніпуляцій.

Доступність

Виборці повинні мати можливість голосувати з будь-яким обладнанням та навичками.

Секретність

Система голосування є секретною, якщо ніяким чином не можна отримати інформацію про те, скільки голосів отримав кожен з кандидатів до опублікування результатів голосування. Ні один учасник процесу не може дізнатися результат голосування до його остаточної публікації.

Прозорість

Система голосування вважається прозорою, якщо всі учасники зможуть зрозуміти будь-які її етапи та компоненти.

Зручність

Обладнання має дозволяти використовувати різні формати бюлетенів для проведення голосування.

1.4 Криптографічні елементи, які застосовуються у електронному голосуванні

Для задоволення всіх вимог безпеки у протоколах електронного голосування використовуються деякі криптографічні елементи та алгоритми. Вони забезпечують криптографічний захист та відповідність властивостям схем електронного голосування. Розглянемо опис основних із них.

Протокол розподілу секрету

Обмін секретами - це метод, що дозволяє розділити секрет S між N учасниками з тією властивістю, що при відсутності хоча б одного з N відновити секрет буде неможливо. Також існують схеми, коли для відновлення секрету S достатня певна фіксована кількість учасників.

В схемах електронного голосування протокол розподілу секрету зазвичай використовується, коли існує значна імовірність компрометації

органів влади. Однією з найвідоміших схем розподілу секрету є схема Шаміра. У ній для того, щоб відновити його могли тільки k<N учасників, використовується поліноміальна інтерполяція. Кожен орган влади отримує свою частину секрету від довіреної сторони. Довіреною стороною може виступати незалежний спостерігач або один із виборців.

У протоколах електронного голосування використовуються лише такі схеми розподілу секрету, у яких, для того, щоб відновити секрет, потрібні всі N учасників [1].

Сліпий цифровий підпис

Сліпий цифровий підпис це вигляд цифрового підпису, який використовується в протоколах електронного голосування для забезпечення анонімності та цілісності вибору учасників.Зазвичай сліпий цифровий підпис накладається органом, який проводить голосування. Цей орган не може побачити вміст бюлетеня, який він підписує, і не зможе зв'язати бюлетені з виборцями, які їх заповнили. Відповідно до вимог протоколу, підпис повинен відповідати наступним властивостям:

-лише власник підпису має право його використовувати;

-будь-хто повинен мати можливість перевірити його істинність відносно повідомлення.

Сліпий цифровий підпис може бути реалізований декількома способами, проте загальна його схема має наступний вигляд:

1) Відправник А шифрує документ і надсилає його стороні В.

2) Сторона В, не маючи можливість побачити вміст документа, підписує його і повертає назад стороні А.

3) Сторона А розшифровує свій документ, в результаті чого на документі залишається підпис сторони В.[1]

Доведення з нульовим розголошенням

Доведення з нульовим розголошенням – це метод доведення однією стороною іншій, що твердження істинне, без розкриття будь-якої

інформації про вміст твердження, окрім самої її достовірності.

Доведення з нульовим розголошенням повинно задовольняти трьом властивостям:

Повнота Якщо твердження істинне, той хто чесно доводить, тобто повністю слідує протоколу, завжди переконає чесного перевіряльника.

Коректність Якщо твердження хибне, то ймовірність обману в будь-якому випадку має бути дуже низькою. Це захищає від прийняття хибного твердження.

Нульове розголошення Якщо твердження істинне, то жоден з тих хто перевіряє та не повністю слідує протоколу, не може дізнатись нічого, окрім факту істинності твердження.

У протоколах електронного голосування доведення з нульовим розголошенням використовуються на багатьох етапах. Наприклад для підтвердження правдивості обрахунку або для доведення чесності органів влади.[1]

Блокчейн

Блокчейн – це структура баз даних, в якій дані організовані у вигляді блоків, а блоки з'єднуються разом, формуючи ланцюг.

Особливість блокчейну, як бази даних полягає у тому, що замість таблиці певного формату ця база використовує блоки даних, які теж мають певний формат, і при цьому утворюють повністю впорядковану множину. Кожен блок має певний (обмежений) об'єм пам'яті.

Крім інформації про транзакції, їх валідність, часову мітку та деяку іншу службову інформацію кожен блок містить у собі геш-функцію від попереднього блоку. Тобто кожен наступний блок "прив'язується"до попередніх, створюючи певний "ланцюжок". Механізм блокчейну дозволяє нам лише додавати інформацію до нових блоків, а також не дозволяє редагувати її та видаляти дані.

Завдяки безпеці даних у блокчейні, їх використовують у протоколах електронного голосування для передачі повідомлення між сторонами

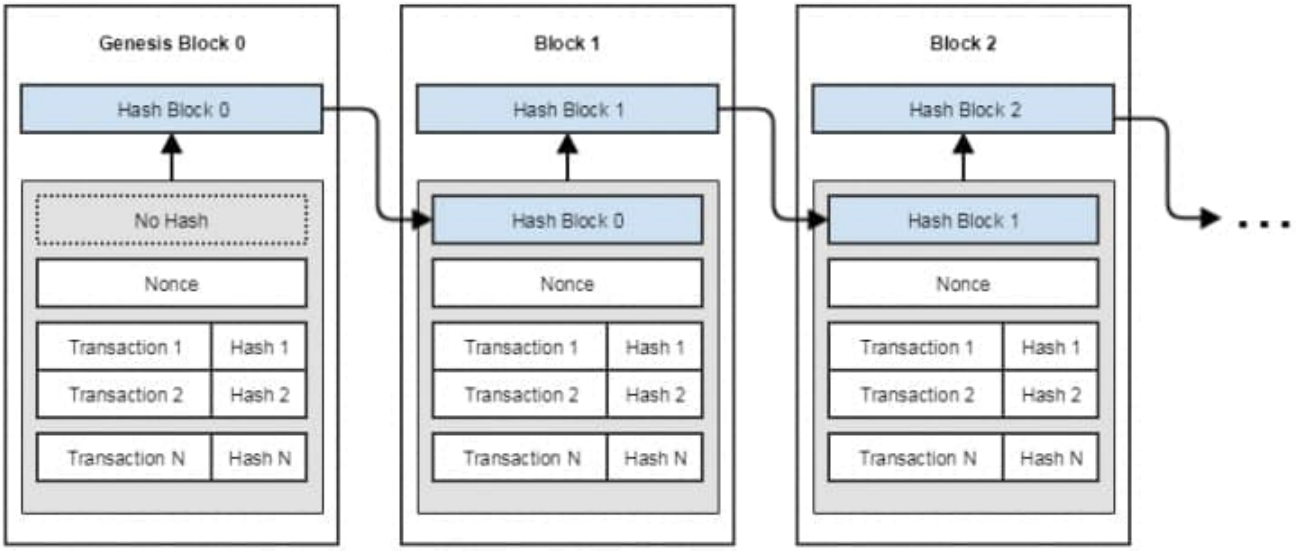

Рисунок 1.1 – Схема побудови блокчейну

виборчого процесу.

Гомоморфне шифрування

Гомоморфним шифруванням називається модель шифрування, яка задовольняє додатковій вимогі гомоморфності щодо будь-яких алгебраїчних операцій над відкритим текстом. Гомоморфні алгоритми шифрування дуже часто використовуються в схемах електронного голосування, оскільки це надає можливість застосовувати алгебраїчні операції до наборів бюлетенів без необхідності їхнього розшифрування. Це дозволяє не порушувати таємницю голосування. Після того як виборці відправляють зашифровані бюлетені, виборча комісія об'єднує їх з використанням певного бінарного оператора, який володіє властивістю гомоморфізму. Після чого отримується інший шифртекст, розшифрувавши який можна буде отримати комбінацію вхідних голосів.

Операцією, яка буде використовуватись для об'єднання бюлетенів може слугувати додавання за модулем $\bigoplus$ (адитивний гомоморфізм) або множення $\bigotimes$ (мультиплікативний гомоморфізм). Першою криптосистемою, яка володіла властивостями гомоморфізму стала система криптосистема RSA.[1]

Мережі перемішування

Мережі перемішування допомагають зберегти властивість анонімності. Даний інструмент використовується для створення анонімних каналів зв'язку, який в свою чергу забезпечує приховування особи виборця відносно органів влади.

В криптографічних протоколах електронного голосування, вхідними даними для мережі перемішування є бюлетені виборців, а вихідними - анонімні голоси у відкритому вигляді. Завдяки цьому, результат підраховується з бюлетенів, які подані відкритим текстом. При цьому зберігається таємність відповідності виборця та його голосу. Мережа перемішування може складатися з декількох серверів, кожен з яких відповідає за певний етап перемішування.

Загальна схема роботи мережі перемішування виглядає наступним чином:

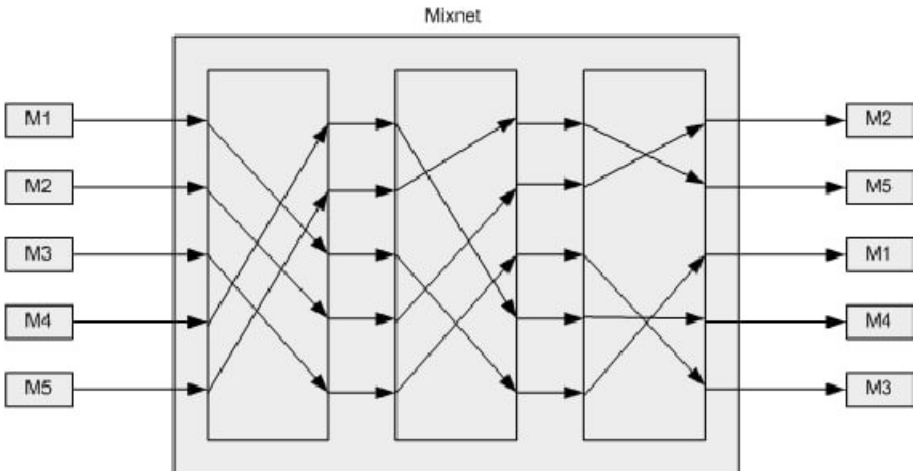

Рисунок 1.2 – Схема мереж перемішування

1) Кожен виборець шифрує свій бюлетень та подає на вхід до мережі перемішування.

2) Кожен сервер здійснює обробку входів, тобто шифрує чи дешифрує бюлетень.

3) Здійснюється перестановка вхідних даних користувачів

(перемішування), яка зберігається у таємниці.

4) Сервер надсилає дані на наступний сервер.

5) Останній сервер надсилає вихід мережі отримувачу.

Для протоколів електронного голосування важлива коректність роботи мереж перемішування. [1]

Протокол секретного продажу секретів "все або нічого" (ANDOS)

Даний протокол дозволяє декільком сторонам (їх має бути не менше 2) купувати або отримувати секрети від одного продавця. В цьому протоколі секрет приставляється у вигляді бітових рядків довжини n. Також потрібно ввести поняття фіксованого бітового індексу (FBI). Фіксованим бітовим індексом називається послідовність номерів бітів, які співпадають у цих рядках. Розглянемо загальну схему цього протоколу.

Нехай у продавця є k n-бітових секретів: $S_1, S_2, \ldots S_k$. Позначимо продавця A, а покупців B та C. B хоче отримати секрет S_b, а C- секрет S_c.

1) A генерує пару "відкритий та закритий ключ" і повідомляє B відкритий ключ. A генерує іншу пару "відкритий та закритий ключ" і повідомляє C відкритий ключ.

2) B генерує k n-бітових випадкових чисел $B_1, B_2, \ldots B_k$, і повідомляє їх C. C генерує свої k n-бітових випадкових чисел $C_1, C_2, \ldots C_k$, і повідомляє їх B.

3) B шифрує C_b відкрити ключем, отриманим від A. Він обчислює значення FBI для C_b і для тільки що зашифрованого результату, після чого відправляє це FBI C.

4) C шифрує B_c відкритим ключем, отриманим від A. Він обчислює значення FBI для B_c і для тільки що зашифрованого результату, після чого відправляє це FBI B.

5) B у кожному з n-бітових випадкових чисел B_1, $B_2, \ldots B_k$ замінює кожен біт, номера якого немає в FBI, яке він отримав від C, його доповненням. Після цього він відправляє новий список n-бітових чисел $B_1^{'}, B_2^{'}, \ldots B_k^{'}$ продавцю A.

6) C в кожному з n-бітових випадкових чисел $C_1, C_2, \ldots C_k$ замінює кожен біт, номера якого немає в FBI, яке він отримав від B, його доповненням. Після цього він відправляє новий список n-бітових чисел $C_1^{'}, C_2^{'}, \ldots C_k^{'}$ продавцю A.

7) A розшифровує всі $C_k^{'}$ закритим ключем користувача C та отримує нові k n-бітових чисел $C_1^{''}, C_2^{''}, \ldots C_k^{''}$, після чого обчислює $S_i \oplus C_i^{''}$ для $i = 1, \ldots k$, і надсилає результати користувачу B.

8) A розшифровує всі $B_k^{'}$ закритим ключем користувача B та отримує нові k n-бітових чисел $B_1^{''}, B_2^{''}, \ldots B_k^{''}$, після чого обчислює $S_i \oplus B_i^{''}$ для $i = 1, \ldots k$, і надсилає результати користувачу C.

9) Користувач B обчислює S_b, виконуючи $\oplus$ C_b та b-го числа, отриманого від A.

10) Користувач C обчислює S_c, виконуючи $\oplus$ B_c та b-го числа, отриманого від A.

Цей протокол використовується в деяких протоколах електронного голосування для анонімного розповсюдження реєстраційних номерів. Так як цей протокол не дозволяє виборчій комісії дізнатись у якого виборця який реєстраційний номер, то це забезпечує таємність відповідності виборця та його голосу.[1]

Висновки до розділу 1

У даному розділі наведено загальну схему та вимоги до протоколів електронного голосування. Розглянуто властивості, яким мають задовольняти схеми електронного голосування для їх коректної та безпечної роботи. Наведено та описано основні криптографічні елементи, які найчастіше використовуються у протоколах електронного голосування.

2 СХЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

За принципом побудови віддалені системи електронного голосування бувають централізовані та децентралізовані. Особливістю централізованної системи є те, що вона має ієрархічну структуру, де вся інформація зберігається, оброблюється, підраховується та публікується за допомогою у центрального довіреного вузла.

У децентралізованій системі не існує такого єдиного довіреного вузла. Замість цього всі вузли є рівноправними учасниками, яким не потрібна довіра один до одного, щоб працювати. Також важливим є те, що будь-яка помилка або збій в роботі одного з вузлів не зможе вплинути на роботу всієї системи, а усі дані щодо голосування зберігаються розподілено на різних вузлах. Очевидно, що децентралізована система електронного голосування є набагато складнішою для реалізації, ніж централізована система електронного голосування.

У даному розділі буде розгянуто основні переваги та недоліки централізованої та децентралізованої схем електронного голосування та наведено огляд на централізований протокол та децентралізовану схему електронного голосування.

2.1 Централізована схема електронного голосування

Майже всі відомі системи електронного голосування є централізованими. Однак не дивлячись на їхню поширеність, вони мають і ряд недоліків.

Недоліками централізованого підходу є наступні:

- будь-яка серйозна проблема або збій у роботі центрального вузла може призвести до зупинки всієї системи;

- збій у функціонуванні центрального вузла може стати причиною

зникнення всіх даних;

- повинна бути довіра виборців до центрального вузла.[11]

Протокол електронного голосування з n комісіями для підрахування голосів

Вважається, що у даному протоколі приймають участь m виборців та n комісій для підрахунку голосів. Завдяки наявності великої кількості комісій забезпечується анонімність виборців, а також здійснюється запобігання можливості фальсифікації результатів голосування.[12]

Дана схема може мати наступний вигляд:

1. Установка системи

Усі комісії для підрахунку голосів повинні мати алгоритм шифрування з відкритим ключем E_i. З фіксованої скінченної абелевої групи A порядку q обираються пара елементів B та G, причому, ні виборці ні комісії не знають значення розв'язку $B = G^x(modq)$. Кожен з виборців має алгоритм підпису з відкритим ключем.

2. Заповнення бюлетеня

Для подачі голосу кожен j-й виборець окремо обирає голос по кожному k-му пункту голосування $v_j,_k \in$ {-1,1}.

Також кожен виборець обирає випадкові числа $a_{j,k}$ з множини всіх можливих залишків від ділення чисел на q і публікує свої результати: $D_{j,k} = D_{a_{j,k}}(v_{j,k}) = B^{v_{j,k}}G^{a_{j,k}}(modq)$.

Результати $D_{j,k}$ стають відомими всім сторонам голосування.

Разом з результатами $D_{j,k}$, користувач публікує, за допомогою протоколу доведення з нульовим розголошенням, свої доведення того, що його голоси дійсно обрані з множини {-1,1}. Голоси разом з доведенням підписуються за допомогою схеми підпису, яка належить виборцю.

Також для доведення коректності голосування, кожен j-й виборець

опубліковує суму $a_j = \sum_k a_{j,k}$.

Так як для кожного числа, яке виборець передає, існує лише одне значення числа $a_{j,k}$, то стає не можливо підібрати якесь інше значення даного числа. Це не дозволить виборцю фальсифікувати голоси.

3. Розподіл бюлетенів

Для підведення підсумків голосування, необхідно передати віддані голоси комісіям. Для передачі значень $a_{j,k}$ та $v_{j,k}$ кожен виборець використовує схему Шаміра для розподілу секрету. З цією метою для кожного k-го голосу виборець обирає два випадкові поліноми за модулем q степені T<n:

$R_{j,k}(X) = v_{j,k} + r_{1,j,k}X + ... + r_{T,j,k}X^T$

$S_{j,k}(X) = v_{j,k} + s_{1,j,k}X + ... + s_{T,j,k}X^T$

Після цього виборець обчислює $(u_{i,j,k}, w_{i,j,k}) = (R_{j,k}(i), S_{j,k}(i))$ при $1 \leqslant i \leqslant n$ і шифрує ці пари використовуючи алгоритм E_i і-ї комісії для підрахунку голосів. Після цього відправляє їй отриманий результат. Також виборець передає поліном $R_{j,k}(X)$ обраховуючи

$$D_{l,j,k} = D_{s_{l,j,k}}(r_{l,j,k}) = B^{r_{l,j,k}} G^{s_{l,j,k}} (mod q)$$

при $1 \leqslant i \leqslant n$.

4. Перевірка достовірності інформації

Кожна із лічильних комісій повинна перевірити чи пара $(u_{i,j,k}, w_{i,j,k})$ дійсно отримана від користувача під номером j. Дана перевірка виконується за допомогою перевірки наступних рівнянь:

$$D_{j,k} \prod_{l=1}^{T} D_{l,j,k}^{i^l} (mod q) = D_{a_{j,k}}(v_{j,k}) \prod_{l=1}^{T} (D_{s_{l,j,k}}(r_{l,j,k}))^{i^l} (mod q) =$$

$$= B^{v_{j,k}} G^{a_{j,k}} \prod_{l=1}^{T} (B^{r_{l,j,k}} G^{s_{l,j,k}})^{i^l} (modq) = B^{(v_{j,k} + \sum_{l=1}^{T} r_{l,j,k} i^l)} G^{(a_{j,k} + \sum_{l=1}^{T} s_{l,j,k} i^l)} (modq) =$$

$$= B^{u_{i,j,k}} G^{w_{i,j,k}} (modq)$$

Крім того, кожна лічильна комісія перевіряє, що всі голоси сформовані коректно, і виборець правильно подав голоси, проголосувавши лише за наперед задану кількість кандидатів. Для цього лічильна комісія обчислює суму v одиниць кількості кандидатів, за яких можна проголосувати, і від'ємних одиниць решти кандидатів та перевіряє рівність:

$$\frac{\prod_k D_{j,k}}{B^v} (modq) = \frac{\prod_k B^{v_{j,k}} G^{a_{j,k}}}{B^v} (modq) = \frac{B^{\sum_k v_{j,k}} G^{\sum_k a_{j,k}}}{B^v} (modq) = G^{a_j} (modq)$$

.

Якщо виборець правильно подав голоси, то тоді $\sum_k v_{j,k} = v$ і тоді рівність повинна виконуватись.

5. Підрахунок голосів

Кожна з n комісій для підрахунку голосів підраховує бюлетені по кожному k-му кандидату та публікує результати

$$U_{i,k} = \sum_{j=1}^{m} u_{i,j,k}$$

.

Крім того вона публікує суму чисел

$$W_{i,k} = \sum_{j=1}^{m} w_{i,j,k}$$

.

Будь-який інші учасники процедури голосування можуть впевнитись в коректності опублікованих сум, зробивши перевірку по

кожному кандидатові наступним чином:

$$\prod_{j=1}^{m}(D_{j,k}\prod_{j=1}^{T}D_{l,j,k}^{j^l})(modq) = \prod_{j=1}^{m}B^{u_{i,j,k}}G^{w_{i,j,k}}(modq) = B^{U_{i,k}}G^{W_{i,k}}(modq)$$

Кожна із сторін процесу може визначити підсумок, беручи T значень $U_{i,k}$ та відновлюючи щодо них остаточний результат. Справа в тому, що $U_{i,k}$ – значення полінома, що становить суму голосів, у точці i для k-го кандидата.

Щоб переконатися в цьому, потрібно розглянути

$$U_{i,k} = \sum_{j=1}^{m}u_{i,j,k} = \sum_{j=1}^{m}R_{j,k}(i) = \sum_{j=1}^{m}v_{j,k} + (\sum_{j=1}^{m}r_{1,j,k})i + ... + (\sum_{j=1}^{m}r_{T,j,k})i^T$$

Результат дорівнює сумі всіх обраних виборцями значень із множини {-1,1} для k-го кандидата. А зробивши співвідношення цієї суми із загальною кількістю тих, хто проголосував, і кількістю кандидатів, за яких можна проголосувати, виходить точний результат за кількістю поданих голосів. Наприклад, якщо h - кількість виборців, що подали голоси, f - кількість кандидатів, за яких можна було проголосувати, то у відсотковому співвідношенні таке значення можна отримати так:

$$\frac{h + \sum_{j=1}^{m}v_{j,k}}{2 * h * f} * 100\%$$

Даний протокол є протоколом голосування з розподілом лічильних комісій. Він дозволяє здійснювати вибір з довільної кількості варіантів та обирати декілька кандидатів зі списку.

2.2 Децентралізована схема електронного голосування

Якщо брати до уваги істотні переваги, то саме розробка децентралізованої системи електронного голосування видається найбільш

перспективним варіантом у контексті розробки національної системи голосування.

Застовування технології блокчейну може допомоготи у побудові такої системи.

Блокчейн являє собою ланцюг з блоків даних (які вміщують іформацію з транзакціями). Властивістю блокчейна є те, що він зберігається на різних вузлах мережі. Нові блоки даних додаються лише після згоди більшості учасників за допомогою досягання консенсусу. Реалізація децентралізації у блокчейні досягається завдяки складним криптографічним механізмам,які зв'язані між собою та можуть гарантувати те, що після того, як події вже відбулися та були задукументовані, не буде існувати змоги їх змінити чи скомпроментувати.

Використання технології блокчейну дає змогу забезпечити те, що:

- інформація зберігається розподілено на різних вузлах;

- не буде зупинки функціонування система під збою роботи одного з вузлів;

- не звачаючи на повну недовіру між вузлами, операції виконуються надійно та безпечно.

Побудова системи електронного голосування на базі блокчейну зможе забезпечити виконання таких вимог, як:

Прозорість

Транзакція має бути достовірною та будь-хто повинен мати можливість перевірити її у будь-який момент;

Цілісність

Якщо у результаті досягнення консенсусу, блок з тразакцією було додано до ланцюга блокчейну, то не можлива зміна або вилучання цієї тразакції;

Анонімність

Неможливість зв'язати транзакцію, яка містить голос виборця з самим виборцем або його особистими даними;

Автоматизація

-автоматичний підрахунок голосів та публікація результатів голосування[7].

На даний момент уже існує декілька блокчейн-платформ, які надають можливість голосувати електронно. Доволі відомими платформами є Agora[8], Polys[9], Waves[10].

Існують наступні принципи побудови децентралізованої схеми електронного голосування:

1. Усі виборці (виборець виступає вузлом) зберігає пару своїх ключів самостійно. Сертифікат відкритого ключа передається разом із підписаним повідомленням.

2. Відповідно до законаів блокчейну, запис про транзакції зберігається в розподіленій базі.

3. Реєстр стану сертифіката міститься у блоці транзакцій.

4. Під час перевірки дійсності сертифіката відкритого ключа, до першої транзакції простежують реєстр стану сертифіката користувача .

5. Сама первинна ідентифікація нового користувача є обов'язковою і вимагає надійного підтвердження. Для цієї мети потрібний довірений вузол, який здійснює видачу первинних сертифікатів для нових користувачів та зміну статусу сертифікатів для старих користувачів. Єдиний раз, коли виникає звернення до довіреного вузла – це перша транзакція користувачів. За допомогою цього, нові користувачі забезпечуються «батьківським» блоком для того. Це потрябно для того, щоб у вже існуючих вузлів була можливість перевірити статуси сертифікату нових вузлів. Буде доцільно, якщо цю роль буде виконувати вузол, який перевіряється та сертифікується з боку контролюючих органів.

У таких схемах використовується PKI. Вона використовується не лише для створення цифрових сертифікатів, а й для зберігання цих сертифікатів. Також її застосовують для зберігання та для резервування ключів, відновлення їх в разі втрати, анулювання сертифікатів та їх

відновлення в разі закінчення терміну їхньої дії.

Обов'язково первинна ідентифікація проводиться вузлом, який сертифікується з боку контролюючих органів. Після звернення виборця до цього вузла, довірений вузол генерує йому його власний унікальний ідентифікатор та сертифікат відкритого ключа, у якого має існувати зв'язок з особистим ключем виборця. При чому, ID не зберігається у довірчого вузла. За вимогами, він навіть не має його знати. Після завершення процедури первинної ідентифікації, формується база даних, яка має наступний вигляд:

H(Cert,ID)	H(Cert,Status)	Status
…	…	…

Рисунок 2.1 – Вигляд розподіленої бази даних

Формування списків виборців

Процес формування списків виборців наступний.

1. Спочатку виборець у вигляді транзакції надсилає запит, у якому міститься: $M; Sign; H(Cert, ID); Cert; Status; M = H(ID)$.

2. Відбувається процедура аутентифікації виборця. Маючи дані з процедури первинної ідентифікації, довірений вузел виконує перевірку на наявність таких даних у розподіленій базі. Також відбувається перевірка, чи не додається даний користувач до списку повторно.

3. Після успішного проходження процедури аутентифікації, орган із сертифікації відповідає користовачу надсиланням його індивідуальної мітки, яка підписана власним особистим ключем довіреного вузла: $Sign(H(ID) + t_i$; де $-t_i$ є ідентифікаційною позначкою (міткою).

4 Органом сертифікації відбувається формування транзакці Tx1, до якої він додає значення від сертифікату виборця $H(Cert)$. Потім учасники мережі блокчейн досягають консенсусу щодо того, чи включати

таку транзакцію до розподіленого реєстру.

Таким чином, після того як закінчився період, який був призначений для формування списків легітимних виборців, відбувається передача даних про мітки між самими вузлами та агентствами, які проводять голосування(відповідність між користувачем та його міткою не зберігається): $H(ID) + t$.

Таким чином, при збереженні анонімності всіх виборців, агенство одержує їхній повний список.

В загальному дана схема може мати наступний вигляд[6]:

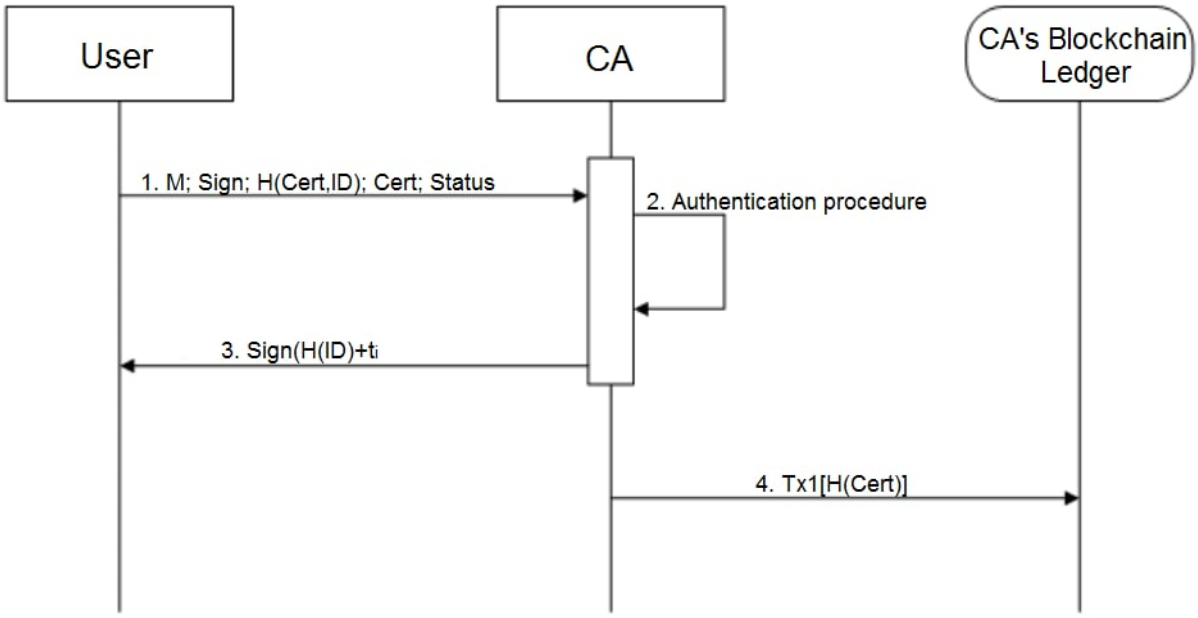

Рисунок 2.2 – Схема формування списків виборців

Етап голосування

Процес голосування відбувається наступним чином:

1.Виборець, після отримання підтвердження від довіреного вузла, надсилає повідомлення зі своїм вибором, яке містить: $H(ID) + t_i$; $encrypt(M*)$, де $M* = H(ID) + t, B$.

2. Перевірка того, що голос при шов саме від легітимного виборця(авторизація), відбувається по зовнішній мітці $H(ID) + t_i$.

3. При успішному проходженні авторизації, агентство розшифровує

повідомлення за допомогою власного приватного ключа. Після цього агентство перевіряє відповідність між зовнішньою міткою та тією, яка була зашифрована.

4. Якщо відбувається збіг міток, агентство формує транзакцію $Tx2$, до якої включається відповідність між $H(ID) + t_i$ та B. Потім учасники мережі блокчейн досягають консенсусу щодо того, чи включати таку транзакцію до розподіленого реєстру. До того ж, хто саме з лигітимних виборців зробив цей вибір не знає ні агентство, ні сторонній спостерігач.

5. При успішному проходження перевірок, агентство відповідає користовачу надсиланням його індивідуальної мітки, яка підписана власним особистим ключем агентства: $Sign(H(ID) + t_i$; де $-t_i$ є ідентифікаційною позначкою (міткою).

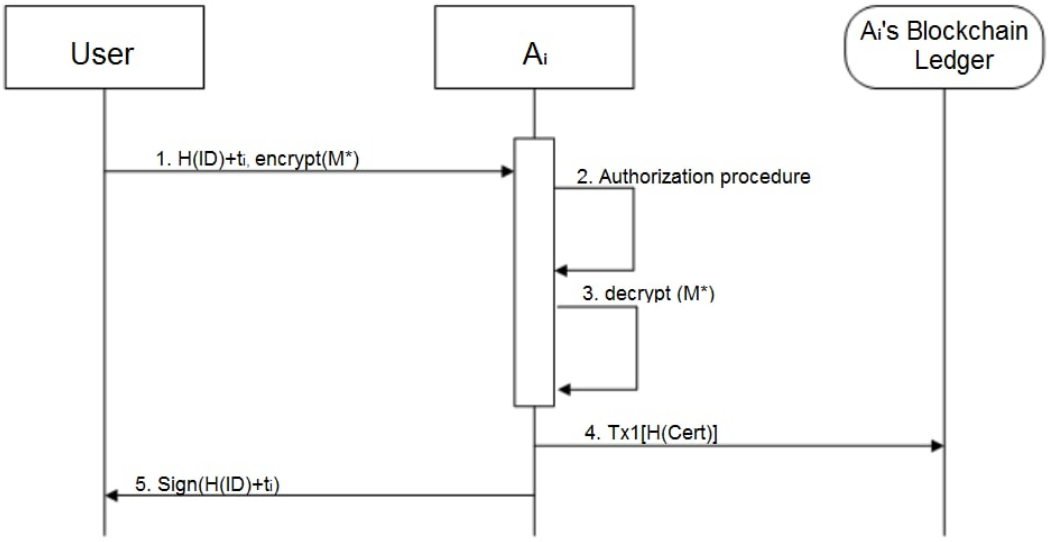

Рисунок 2.3 – Схема голосування

Перед підрахунком голосів, виконуються необхідні перевірки: $N(H(Cert)) = N(H(ID) + t)$.

Кількість геш-значень сертифікатів $N(H(Cert))$ в мережі , яка організована між центром сертифікації та агентством, має дорівнювати кількості $H(ID) + t$, які були надіслані від центрів сертифікації до агентства. Тобто виключається імовірність того, що агентство може не врахувати голоси легітимних виборців .

Наступна перевірка виконується таким чином: $N(H(ID) + t)N(B)$. Тобто, кількість зарєстрованих виборців повинна бути більшою або дорівнювати кількості отриманих бюлетенів.

Якщо всі перевірки є успішними, проводиться підрахунок голосів.

Підрахунок голосів

У блокчейн-мережі, яка організована між представництвами агентства, відбувається формування остаточного списку, у який додають відповідність між мітками виборців та їхнім вибором. Тобто кожен користувач має змогу перевірити правильність врахування свого голосу. У випадку, коли виникає помилка, виборці повідомляють про це до агентства. Голоси підраховуються автоматично.

Ця системи електронного голосування допомагає зберегти всі переваги децентралізованості. Також, так як система децентралізована, немає необхідності повторно генерувати списки виборців.

Висновки до розділу 2

У даному розділі наведено опис схеми електронного голосування з використанням блокчейну та опис протоколу з декількома комісіями для підрахунку голосів. Наведені переваги та недоліки централізованих та децентралізованих схем електронного голосування.

3 КОНКРЕТИЗАЦІЯ ПРОТОКОЛУ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

У цьому розділі описано обрані криптографічні елементи та виконана модифікація до протоколу з розділу 2 за допомгою цих елементів. Обчислено час роботи отриманого протоколу.

3.1 Вибір та опис криптографічних елементів

У даному протоколі використовуються геш-функції та криптографічний алгоритм для шифрування та електронного підпису. У випадках, коли потрібно використовувати геш-функцію, було вирішено використовувати ітеративну функцію "Купина" з національного стандарту України ДСТУ 7564:2014. Дана функція має високі показники криптостійкості та вихідні геш-значення задовольняють вимогам псевдовипадкових послідовностей. Опис даної функції взято з [13].

На вхід до даної функції подається значення довжини N (N належить від 0 до $(2^{96} - 1)$, яке задається у бітах. Вхідне значення функції завжди доповнюється до довжини, яка буде кратна l, де l- розмір блоку. До кожного повідомлення M спочатку додається одиничний біт, а згодом додається d нульових бітів ($d = (-N - 97)mod l$). Також до цього значення додають значення N, яке записане у 96 бітах у форматі little endian. Потім значення розбивається на k блоків m, розмір кожного з яких відповідно буде l. Вибір l залежить від розміру геш-значення n:

$$l = \begin{cases} 512 \text{ для } 8 \leqslant n \leqslant 256 \\ 1024 \text{ для } 256 \leqslant n \leqslant 512 \end{cases}$$

Рекомендовані до застосування режими роботи даної функції "Купина-256", "Купина-384" та "Купина-512".

Обчислення геш-значення відбувається за наступною ітеративною процедурою:

$$h_0 = IV,$$

$$h_v = T_l^{\oplus}(h_{v-1} \oplus m_v) \oplus T_l^{+}(m_v) \oplus h_{v-1}, v = 1,2,...k$$

$$H(IV,M) = R_{l,n}(T_l^{\oplus}(h_k) \oplus h_k$$

де вектор ініціалізації IV = $\begin{cases} 1<<510 \text{ для l } 512 \\ 1<<1023 \text{ для l } 1024 \end{cases}$

$T_l^{\oplus}$ та T_l^{+} — бієктивні перетворення, які виконують відображення вхідного блоку довжини l, у вихідний блок такої самої довжини.

Функція $R_{l,n}(x)$ повертає n старших біт з вхідного блоку довжиною l біт, де результат записується в молодші n біт обчисленого значення.

Бієктивні перетворення $T_l^{\oplus}$ та T_l^{+} є відображеннями, які реалізують ітеративне застосування деякої кількості функцій. Вхідний аргумент подається у вигляді матриці розміром 8 на c байтів, яка складається з елементів поля $GF(2^8)$.

Кількість колонок, ітерацій та розмір внутрішнього стану залежать від розміру геш-значення наступним чином:

Розмір геш-значення	Розмір внутрішнього стану (l)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
$8 \le n \le 256$	512	10	8
$256 < n \le 512$	1024	14	16

Рисунок 3.1 – Залежність внутрішнього стану

До матриці внутрішного стану $G = (g_{i,j})$, $g_{i,j} \in GF(2^8)$, де i проходить всі значення від 0 до 7, а j проходить всі значення від 0 до $c - 1$, записуються байти бієктивних перетворень$T_l^{\oplus}$ та T_l^{+}, які зчитуються з неї за колонками.

Матрицю внутрішнього стану можна зобразити наступним чином:

Вхідна послідовність							
B_1	B_9	B_{17}	B_{25}	B_{33}	B_{41}	B_{49}	B_{57}
B_2	B_{10}	B_{18}	B_{26}	B_{34}	B_{42}	B_{50}	B_{58}
B_3	B_{11}	B_{19}	B_{27}	B_{35}	B_{43}	B_{51}	B_{59}
B_4	B_{12}	B_{20}	B_{28}	B_{36}	B_{44}	B_{52}	B_{60}
B_5	B_{13}	B_{21}	B_{29}	B_{37}	B_{45}	B_{53}	B_{61}
B_6	B_{14}	B_{22}	B_{30}	B_{38}	B_{46}	B_{54}	B_{62}
B_7	B_{15}	B_{23}	B_{31}	B_{39}	B_{47}	B_{55}	B_{63}
B_8	B_{16}	B_{24}	B_{32}	B_{40}	B_{48}	B_{56}	B_{64}

↓

Внутрішній стан функції гешування							
$g_{0,0}$	$g_{0,1}$	$g_{0,2}$	$g_{0,3}$	$g_{0,4}$	$g_{0,5}$	$g_{0,6}$	$g_{0,7}$
$g_{1,0}$	$g_{1,1}$	$g_{1,2}$	$g_{1,3}$	$g_{1,4}$	$g_{1,5}$	$g_{1,6}$	$g_{1,7}$
$g_{2,0}$	$g_{2,1}$	$g_{2,2}$	$g_{2,3}$	$g_{2,4}$	$g_{2,5}$	$g_{2,6}$	$g_{2,7}$
$g_{3,0}$	$g_{3,1}$	$g_{3,2}$	$g_{3,3}$	$g_{3,4}$	$g_{3,5}$	$g_{3,6}$	$g_{3,7}$
$g_{4,0}$	$g_{4,1}$	$g_{4,2}$	$g_{4,3}$	$g_{4,4}$	$g_{4,5}$	$g_{4,6}$	$g_{4,7}$
$g_{5,0}$	$g_{5,1}$	$g_{5,2}$	$g_{5,3}$	$g_{5,4}$	$g_{5,5}$	$g_{5,6}$	$g_{5,7}$
$g_{6,0}$	$g_{6,1}$	$g_{6,2}$	$g_{6,3}$	$g_{6,4}$	$g_{6,5}$	$g_{6,6}$	$g_{6,7}$
$g_{7,0}$	$g_{7,1}$	$g_{7,2}$	$g_{7,3}$	$g_{7,4}$	$g_{7,5}$	$g_{7,6}$	$g_{7,7}$

Рисунок 3.2 – Зповнення внутрішнього стану

Бієктивні перетворення $T_l^{\oplus}$та T_l^{+} визначаються як:

$$T_l^{\oplus} = \prod_{v=0}^{t-1} (\psi \circ \tau^l \circ \pi^{'} \circ \kappa_v^l)$$

$$T_l^{+} = \prod_{v=0}^{t-1} (\psi \circ \tau^l \circ \pi^{'} \circ \eta_v^l)$$

ψ – функція лінійного перетворення, яка виконує операцію множення вектора на матрицю над скінченним полем. Усі елементи матриці внутрішнього стану представлють у вигляді елемента скіченного поля $GF(2^8)$, яке утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$. Результуюча матриця утворюється за допомогою множення векторів довжиною 8 над скінченним полем $GF(2^8)$. Дане перетворення відбувається за наступною формулою: $u_{i,j} = (\upsilon \ggg i) \otimes G_j$ де G_j – j-й

стовпець матриці внутрішнього стану, а $\upsilon = (0x01,0x01,0x05,0x01,0x08,0x06,0x07,0x04)$ – вектор, який утворює циркулярну матрицю МДР-коду.

τ^l – функція, яка виконує перестановку елементів матриці внутрішнього стану, тобто вона циклічно зсуває праворуч рядки матриці стану $G = (g_{i,j})$, при чому рядки з номерами від 0 до 6 зсуваються на i елементів, а елементи у рядку під номером 7 будуть зсуватись на 7 елементів при $l = 512$ та на 11 при $l = 1024$.

Функції κ_v^l та η_v^l додають константи ітерацій за модулями 2 та 2^{64} відповідно. Функція κ_v^l додає за модулем 2 до кожної колонки матриці внутрішнього стану вектор ω_j^v, який належить V_{64} за формулою $\omega_j^v = ((j \ll 4) \oplus v,0,0,0,0,0,0,0)^T$, де v- номер ітерації. Функція η_v^l додає за модулем 2^{64} до кожної колонки матриці внутрішнього стану вектор ς_j^v, який належить V_64 за формулою $\varsigma_j^v = (0xF3,0xF0,0xF0,0xF0,0xF0,0xF0,0xF0((c-1-j) \ll 4) \oplus v)^T$, де v- номер ітерації. Водночас, під час додавання 0xF3- молодші 8 біт вектора ς_j^v, $g_{0,j}$- молодші 8 біт вектора G_j.

Функція $\pi^{'}$ заміняє кожен елемент матриці внутрішнього стану на відповідний елемент згідно підстановки $\pi^{'}_{i \cdot mod4}(g_{i,j})$.

В загальному схема геш-функції має наступний вигляд:

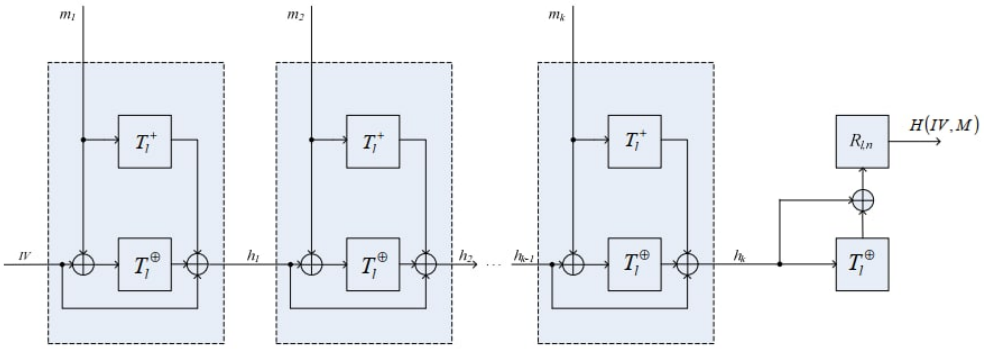

Рисунок 3.3 – Схема геш-функції "Купина"

У якості алгоритму шифрування була обрана криптосистема

RSA[14]. Дана криптосистема є найпоширенішою на даний час, а велика кількість модифікацій дозволяє використовувати її ефективно в залежності від необхідних вимог.

За допомогою RSA можна шифрувати повідомлення та створити цифровий підпис. Її стійкість базується на складності задачі факторизації великих чисел. Для шифрування за допомогою RSA потрібно мати відкритий та закритий ключі. Генерація ключів відбувається наступним чином:

1. Генеруємо два великі прості числа p та q.

2. Обраховуємо добуток $n = p * q$.

3. Обчислюємо функція Ейлера $\phi(n) = (p-1)(q-1)$ та обираємо ключ шифрування e: $1 < e < \phi(n)$, e повинно бути взаємно просте з $\phi(n)$.

4. Також обраховуємо за допомогою РАЕ d, таке що: $ed = 1 mod \phi(n)$.

Так пара (n, e) є відкритим ключем, а d – закритим.

Важливо зазначити, що для отримання захищеного протоколу голосування, обрана схема шифрування RSA повинна бути безпечною. Для забезпечення стійкості важливо, щоб згенеровані числа p та q повинні бути випадковими. Для цього рекомендується використовувати генератори псевдовипадкових послідовностей, наприклад такі як генератор Блюма-Мікалі або Блюм-Блюма-Шуба.

Також, під час генерації ключів потрібно виконувати перевірку чисел на простоту. Це можливо зробити за допомогою тестів перевірки на простоту. Зазвичай використовуються ймовірнісні тести, серед яких тест Міллера-Рабіна та Соловея-Штрассена. Саме їх обирають найчастіше, бо вони працюють набагато швидше ніж інші загальні тести перевірки на простоту.

Важливим параметром також є розмір p та q. За сучасними вимогами вважається безпечно використовувати n довжиною не менше 2048 біти, тобто p та q повинні бути не меншими ніж 1024 біт кожне. В загальному рекомендується використовувати число n не менше ніж 3072 для надзвичайно важливих даних.

Зашифрування повідомлень в алгоритмі RSA відбувається за формулою $c = m^e mod n$, а розшифрування $m = c^d mod n$.

Для формування електронного цифрового підпису спочатку потрібно обчислити геш-значення від вхідного повідомлення. Користувач використовує свій секретний ключ d для формування підпису: $s = H(m)^d mod n$. Для того, щоб перевірити правильність підпису потрібно обчислити $H(m) = s^e mod n$.

3.2 Опис протоколу з використанням обраних елементів

В цілому після використання запропонованих елементів протокол з розділу 2.2 можна сформулювати наступним чином:

Процедура первинної ідентифікації

0. Усі центри сертифікації та агентства генерують свої ключі відповідно до алгоритму шифрування RSA. Їхні відкриті ключі знаходяться у публічному доступі.

1. Виборець генерує p_1 і q_1 та обраховує:

$$n_1 = p_1 * q_1$$

$$\phi(n_1), e_1 : 1 < e < \phi(n_1)$$

та d_1.

2. Виборець надсилає свій відкритий ключ n_1 та e_1 до сертифікованої структури, яка видає йому, зашифроване за допомогою відкритого ключа виборця, ID та сертифікат відкритого ключа $Cert$:

$$c_1 = (ID)^{e_1} mod n_1$$

.

3. Виборець розшифровує за допомогою свого закритого ключа

значення ID:

$$ID = c_1^{d_1} mod n_1$$

.

4. З використанням геш-функції "Купина" виборець обраховує геш-значення $H(ID)$, $H(Cert, ID)$ та $H(Cert, Status)$.

5. Значення $H(Cert, ID)$, $H(Cert, Status)$ та $Status$ відправляються до центра сертифікації, який додає їх у базу даних.

Процедура формування списків виборців

1. Виборець відправляє запит у вигляді транзакції, в яку він включає $H(ID)$, $H(Cert, ID)$, $Cert$, $Status$ та підписане своїм приватним ключем d_1 повідомлення $H(ID)$:

$$s_1 = H(ID)^{d_1} mod n_1$$

.

2. Орган з сертифікації обраховує $H(Cert, Status)$ та перевіряє наявність у базі $H(Cert, ID)$, $H(Cert, Status)$ та $Status$.

3. Орган сертифікації перевіряє правильність підпису s_1 за допомогою відкритого ключа користувача :

$$H(ID) = s_1^{e_1} mod n_1$$

.

4. Якщо процедура аутентифікації була пройдена, то у відповідь на запит орган сертифікації відправляє виборцю

$$c_2 = (H(ID) + t_i)^{e_1} mod n_1,$$

та $s_2 = (H(H(ID) + t_i))^{d_2} mod n_2$, а t_i – ідентифікаційна мітка.

5. Виборець розшифровує $(H(ID) + t_i) = c_2^{d_1} mod n_1$ та отримує своє $(H(ID) + t_i)$ перевіряючи цифровий підпис $H((H(ID) + t_i)) = s_2^{e_2} mod n_2$.

6. Орган формує транзакцію $Tx1$, до якої включає $H(Cert)$. Учасники мережі блокчейн досягають консенсусу, щодо включення даної транзакції до розподіленого реєстру.

7. Всі довірені вузли передають агентству зашифровані дані про мітки, тобто $c_3 = (H(ID) + t_i)^{e_3} mod n_2$.

8. Агентство за допомогою свого закритого ключа розшифровує c_3 та отримує список даних $(H(ID) + t_i)$, тобто список зареєстрованих користувачів.

Процедура голосування

1. Виборець отримавши підтвердження від довіреного вузла, голосує, відправляючи агентству наступний набір даних: $m_1 = (H(ID)+t_i)^{e_3} mod n_3$ та $m_2 = B^{e_3} mod n_3$.

2. Агентство спочатку розшифровує своїм закритим ключем d_3 повідомлення m_1 та перевіряє чи є такий $(H(ID) + t_i)$ у списку зареєстрованих користувачів.

Після проходження такої перевірки агентство розшифровує повідомлення m_2, отримуючи B, та формує транзакцію $Tx2$, в яку включається $(H(ID) + t_i)$ та B.

3. Якщо процедура аутентифікації була пройдена, то у відповідь на запит орган сертифікації відправляє виборцю $s_2 = (H(H(ID)+t_i))^{d_2} mod n_2$, а t_i – ідентифікаційна мітка.

4. Учасники досягають консенсусу щодо включення такої транзакції до розподіленого реєстру.

Етап перевірки

1. Відбувається перевірка рівності $N(H(Cert)) = N(H(ID) + t_i)$.

2. Відбувається перевірка того, що $N(H(ID) + t_i) \geqslant N(B)$.

Підрахунок голосів

Формується остаточний список відповідності між мітками виборців та їхнім голосом, після чого даний список опубліковується. Кожен може перевірити чи враховано його голос. Підрахунок відбувається автоматично.

У даному протоколі під час процедури первинної ідентифікації було додано крок шифрування значення ID користувача. Це дозволяє уникнути формування відповідності між самим виборцем та його ID.

Під час процедури формування списків виборців відбувається перевірка наявності у базі $H(Cert, ID)$, $H(Cert, Status)$ та $Status$. Це забезпечує можливість проголосувати лише тим виборцям, які пройшли процедуру первинної ідентифікації. Тобто це запобігає можливості підробки результатів голосування. Також у даний протокол було додано додаткове шифрування підписаної органом сертифікації індивідуальної мітки виборця. Також виключається можливість порушення цілісності повідомлення з міткою, завдяки наявності цифрового підпису органу сертифікації на ній. З такою самою метою було додано шифрування списку міток виборців під час передачі його до агентства, яке проводить процес голосування. Оскільки шифрування відбувається за допомогою відкритого ключа агентства, то дізнатись список міток може лише саме агентство, розшифрувавши його своїм відкритим ключем.

Під час процедури голосування на першому кроці було змінено набір даних, які відправляє користувач. Так, за рахунок відсутності незашифрованої мітки користувача було забезпечено відсутність можливості підробки голосу на цьому етапі голосування. Хоча це й збільшило складність процедури перевірки, проте це допомогло створити більш захищений протокол голосування.

Етап перевірки дозволяє уникнути можливості неправильного підрахунку голосів за рахунок голосування нелегітимних виборців. Перший крок перевірки дає можливість впевнитись у тому, що всі особи, які проголосували пройшли етап реєстрації. Другий етап перевірки дає змогу переконатись, що всі голоси були враховані.

Також слід вказати особливості формування бюлетеню. Оскільки

кількість кандидатів, тобто кількість можливих результатів вибору для користувача, зазвичай невелика, це дає можливість зловмиснику дізнатися результати голосування для певного користувача. Для цього йому достатньо зашифрувати відкритим ключем агентства всі можливі варіанти вибору та порівняти їх з тими, що були надіслані відповідним користувачем. Для запобігання такої можливості, рекомендується використовувати різні схеми формування бюлетеню. У цих схемах до самого голосу додається ще якась незмістовна інформація, яка не дозволяє зловмиснику визначити голос виборця за допомогою зашифровування всіх можливих варіантів голосування. Це можливо оскільки незалежно від варіантів вибору, усі бюлетені будуть відрізнятись один від одного, тому при шифруванні всіх можливих варіантів, зловмисник не зможе отримати ніякої інформації про зміст бюлетеню.

Для формування такої схеми може використовуватись схема з використанням засліплюючого множника[16]. У ній голос виборця b_i множиться на випадковим чином обране просте число r_i, $r_i > b_i$. Сам бюлетень буде мати вигляд $B = b_i * r_i$. Тоді для коректної роботи протоколу необхідно під час першого кроку процедури голосування додати також і значення $c_4 = r_i^{e_3} mod n_3$. Таким чином агентство зможе розшифрувати значення r_i за допомогою свого відкритого ключа та дізнатись голос виборця b_i розділивши B на r_i. Для вибору r_i можуть використовуватись криптографічно стійкі генератори псевдовипадкових чисел.

Також для роботи даного протоколу може бути обрана будь-яка відома схема формування бюлетенів. Використання захищених каналів зв'язку може вирішити майже всі проблеми даного протоколу і тоді необхідність використання кроків описаних вище зникає.

Час роботи сформованого протоколу

Для оцінки часу роботи отриманого протоколу спочатку потрібно підрахувати кількість шифрувань та розшифрувань, а також кількість

застосувань геш-функції. Варто зазначити, що час формування електронного підпису у криптосистемі RSA дорівнює часу розшифрування повідомлень, оскільки на цих кроках виконується піднесення в таку степінь, яка дорівнює закритому ключу користувача. За аналогією, можна вважати, що час перевірки цифрового підпису дорівнює часу операції шифрування. Для використання RSA обрано n довжиною 2048 біт, оскільки при такій довжині n система вважається надійною. Усі розрахунки, наведені нижче, виконуються на Windows, 64 біта.

У отриманому протоколі, з урахуванням схеми формування бюлетеню, шифрування та розшифрування виконуються по 7 разів. Також у цьому протоколі потрібно врахувати час, який потрібен для генерації ключів трьом учасникам голосування: виборцю, центру сертифікації та агентству. Час генерування ключів для кожного з учасників, дорівнює $570{,}90 \cdot 10^{-3}$ секунд[19]. Час який потрібен для шифрування дорівнює $1{,}69 \cdot 10^{-3}$ секунд, а час, який потрібен для розшифрування складає $26{,}18 \cdot 10^{-3}$[19]. Враховуючи кількість даних операцій час роботи алгоритму RSA у даному протоколі дорівнює:

$$T_1 = 3 \cdot 570{,}90 \cdot 10^{-3} + 7 \cdot 1{,}69 \cdot 10^{-3} + 7 \cdot 26{,}18 \cdot 10^{-3} = 1907{,}79 \cdot 10^{-3}$$

секунд.

Для використання у даному протоколі рекомендується обирати геш-функцію з режимом роботи "Купина-256". Розмір блоку, на які розбивається повідомлення, у такому режимі дорівнює 512 біт. Даний режим має достатню складність знаходження колізій, а довжина вихідного повідомлення у 256 біт дає змогу збільшити швидкість зашифрування повідомлення, оскільки, у такому випадку, на вхід до оперції шифрування буде подаватись невелике повідомлення довжиною 256 біт.

Зазвичай у цьому протоколі на вхід до функції гешування подається

сертифікат відкритого ключа, статус такого сертифікат та ID користувача. Оскільки ID користувача зазвичай дуже мале за розміром число, то все повідомлення складається з одного блоку довжино 512 біт. Також під час формування цифрового підпису один раз доводиться застосовувати геш-функцію до $(H(ID) + t_i)$. Враховуючи що геш-значення ID має довжину 256 біт та t_i доволі короткий нобар даних, то тут також все повідомлення складається з одного блоку довжино 512 біт. Якщо не враховувати дані використання геш-функції, то Купина застосовується у протоколі ще 4 рази. На вхід до неї подаються повідомлення, основний розмір яких складає сертифікат відкритого ключа. У більшості випадків його довжина складає 2000 байт[17]. Швидкодія геш-функції "Купина-256"дорівнює 281,2595 Мбіт за секунду[18]. Тоді час роботи цієї геш-функції при довжині вхідного повідомлення 2000 байт дорівнює: $T_2 = \frac{2000 \cdot 8}{281{,}2595 \cdot 10^6} = 56{,}89 \cdot 10^{-6}$ секунд. Час роботи геш-функції, при вхідному повідомленні ID, дорівнює: $T_3 = \frac{512 \cdot 2}{281{,}2595 \cdot 10^6} = 3{,}64 \cdot 10^{-6}$ секунд.

В загальному час роботи даного протоколу можна визначити за формулою:

$$T = T_1 + T_2 + T_3.$$

Отже час роботи для одного користувача дорівнює:

$$T = 1907790 \cdot 10^{-6} + 56{,}89 \cdot 10^{-6} + 3{,}64 \cdot 10^{-6} = 1907850.53 \cdot 10^{-6} = 1{,}908$$

секунд.

Вважаючи, що всі учасники голосування користуються власними обчислювальними машинами, у яких швидкодія приблизно дорівнює такій, яка використовувалась для даних обчислень, було б доцільно голосування у великих масштабах розділити на декілька днів.

Висновки до розділу 3

У даному розділі проведено підбір криптографічних елементів для використання у протоколі електронного голосування з розділу 2. Обрано геш-функцію “Купина” та криптосистему RSA. До кожної з них наведено детальні алгоритми роботи. До того ж наведені вимоги для параметрів примітивів. Проведено конкретизацію схеми, яка наведена у минулому розділі. Деякі кроки з неї були перетворені для забезпечення вимог електронного голосування. Дані кроки детально описані. Також у даному розділі проведено підрахунок часу роботи даного протоколу без урахування часу, який витрачається на побудову блокчейну.

ВИСНОВКИ

У цій роботі наведено загальну схему та вимоги до протоколів електронного голосування. Розглянуто властивості, яким мають задовольняти схеми електронного голосування для їх коректної та безпечної роботи. Також наведено та описано основні криптографічні елементи, які найчастіше використовуються у протоколах електронного голосування.

Проведено опис децентралізованої схеми електронного голосування на базі блокчейну та централізованої схеми на прикладі протоколу з декількома комісіями для підрахунку голосів. Наведені переваги та недоліки централізованих та децентралізованих схем електронного голосування.

Проведено підбір криптографічних елементів для застосування у протоколі електронного голосування з використанням блокчейну. Обрано геш-функцію “Купина” та криптосистему RSA. До кожної з них наведено детальні алгоритми роботи. До того ж наведено вимоги для параметрів примітивів та способи їхньої генерації і перевірки.

Проведено модифікацію обраної схеми електронного голосування з використанням блокчейну. Деякі кроки з неї перетворені для забезпечення вимог електронного голосування. Дані кроки детально описані. Проведено підрахунок часу роботи даного протоколу.

Після обрахунків визначено, що час виконання процедури голосування для кожного виборця приблизно дорівнює 1,9 секунди без урахування часу, який витрачається на побудову блокчейну.

Дані результати можна використовувати для подальшого покращення, допрацювання та можливої реалізації децентралізованої схеми електронного голосування на базі блокчейну.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bruce Schneier (1996). Applied cryptography - protocols, algorithms, and source code in C, 2nd Edition. Wiley.

2. Концепція розвитку електронної демократії в Україні, схвалена розпорядженням Кабінету Міністрів України від 08.11.2017 р. № 797-р.

3. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 197 с.

4. 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: https://www.researchgate.net/publication/226060607.

5. Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування// Управління розвитком складних систем. – 2014. – Вип. 20. – С. 110 – 115.

6. К. В. Ісірова, О.В. Потій: Принципи побудови електронного системи таємного голосування з використанням децентралізованих технологій ISSN 0485-8972 Радіотехніка. 2019. Вип.199.- с. 125-128 [Електронний ресурс]. — Режим доступу:http://rt.nure.ua/article/view/194028/194221.

7. І. Д. Горбенко, В. В. Онопрієнко, Ю. І. Горбенко, О. О. Кузнецов, К. В. Ісірова, М. Ю. Родінко: Проблеми, принципи побудоваи та перспективи розвитку національної системи електронного голосування в Україні ISSN 0485-8972 Радіотехніка. 2020. Вип.200. - с. 85-88 [Електронний ресурс]. — Режим доступу:http://rt.nure.ua/article/view/210067/210124.

8. https://www.agora.vote/.

9. https://ru.polys.me/.

10. https://wavesenterprise.com/ru/products-and-services/voting.

11. Смарт Н. Мир программирования. Криптография. –Москва:

Техносфера, 2005. - с. 340 [Електронний ресурс]. — Режим доступу:https://dut.edu.ua/uploads/l112872002441.pdf.

12. С. А. Македонский, В. С. Лукьянов: Универсальный протокол защищенного электронного голосования//Волгоградский государственный технический университет//2010.- с. 156-157. [Електронний ресурс]. — Режим доступу:https://www.vstu.ru/uploadiblok/files/izvestiya/archive/2/2010-11.pdf.

13. Національний стандарт України Криптографічний захист інформації Функція гешування ДСТУ 7564:2014. С. 4-6. [Електронний ресурс]. — Режим доступу:https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-7564-2014.pdf.

14. Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"1978.- С 6-10. [Електронний ресурс]. — Режим доступу:http://people.csail.mit.edu/rivest/Rsapaper.pdf.

15. 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.

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

17. Міністертсво юстиції України//Адміністрація спеціальної служби державного зв'язку та захисту інформації України Наказ 20.08.2012 № 1236/5/453. [Електронний ресурс]. — Режим доступу:https://zakon.rada.gov.ua/laws/show/z1398-12n25.

18. Національний стандарт України Криптографічний захист інформації Функція гешування ДСТУ 7564:2014. Основні властивості. - Київ 2015.- с. 26. [Електронний ресурс]. — Режим доступу: https://www.slideshare.net/oliynykov/kupyna.

19. Muhammad Ariful Islam, Md. Ashraful Islam, Nazrul Islam, Boishakhi Shabnam "A Modified and Secured RSA Public Key Cryptosystem Based on “n” Prime Numbers"Department of Information

and Communication Technology (ICT), Mawlana Bhashani Science and Technology University, Tangail, Bangladesh Uttara University, Dhaka, Bangladesh 2018. - с 85. [Електронний ресурс]. — Режим доступу:https://www.scirp.org/journal/paperinformation.aspx?paperid=83244.