УДК 004.056.55

Р. Н. КВЄТНИЙ, Є. О. ТИТАРЧУК

ВИКОРИСТАННЯ ЧАСТКОВО ГОМОМОРФНОГО АЛГОРИТМУ ШИФРУВАННЯ НА ЕЛІПТИЧНИХ КРИВИХ У ХМАРНІЙ СИСТЕМІ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Вінницький національний технічний університет,
21021, вул. Хмельницьке шосе, 95, м. Вінниця, Україна

Анотація. У даній роботі представлено новий підхід побудови сервісу електронного голосування, що за рахунок використання частково гомоморфного шифрування на основі еліптичних кривих дозволяє забезпечити принцип таємниці волевиявлення користувачів. Запропонована у роботі система використовує магнітні картки для ідентифікації користувачів, комп'ютери на виборчих дільницях, та дозволяє користувачам системи перевірити правильність врахування свого вибору з дому, не передаючи системі жодних особистих даних.

Ключові слова. Електронне голосування, Хмарні обчислення, Частково гомоморфне шифрування

Аннотация. В данной работе представлено новый подход построения сервиса электронного голосования, который за счет использования частично гомоморфного шифрования на основе эллиптических кривых позволяет обеспечить принцип тайны волеизъявления пользователей. Предложенная в работе система использует магнитные карты для идентификации пользователей, компьютеры на избирательных участках, и позволяет пользователям системы проверить правильность учета своего выбора из дому, не передавая системе каких-либо персональных данных.

Ключевые слова: Электронное голосование, Облачные вычисления, Частично гомоморфное шифрование.

Abstract. This paper presents a new approach to building cloud services of electronic voting, with usage of the homomorphic encryption. This allow to ensures in secret balloting. In the proposed system uses magnetic cards to identify users, computers at polling stations, and it allows customers to verify the account of their choice from home, without transferring any personal data.

Keywords. Electronic voting, Cloud computing, Homomorphic encryption

ВСТУП

Важливим елементом демократичних систем управління у багатьох країнах світу є вибори. Вони є реальним вираженням волі народу, конституційним способом формування не тільки органів державної влади, а й органів місцевого самоврядування на основі вільного та невимушеного волевиявлення громадян.

Як і у всіх сферах людської діяльності у сучасному світі, головною тенденцією виборчого процесу є його насичення найрізноманітнішими інформатизованими та автоматизованими електронними засобами. Адже розвиток інформаційних і комунікативних технологій багато в чому визначає суспільний і політичний прогрес кожної держави, що до речі є актуальним для нашої країни. Логічним напрямком використання сучасних інформаційних технологій є розвиток електронного голосування виборців. [3]

Електронне голосування (англ. e-voting) термін, що використовується для характеристики різних типів голосування, та охоплює як процес здійснення голосування за допомогою електронних засобів, так і процес автоматичного підрахунку голосів за допомогою електронних пристроїв та спеціального програмного забезпечення [4].

Вперше експеримент з голосування через Інтернет був проведений в 2000 р. у штаті Орегона, США [5]. Пізніше технології голосування вдосконалювалися. Так, в Естонії електронне голосування застосовується з 2005 р. на місцевих виборах, з 2007 р. — на парламентських. Відсоток громадян, що віддають перевагу цій системі голосування, поступово зростає, для прикладу, якщо у 2005 р. у такий спосіб проголосувало лише 2 % естонських виборців, то на парламентських виборах 2015 року цей показник сягнув 30,5 %.

Швейцарія — лідер у запровадженні систем електронного голосування. У країні введена система електронного голосування «EVoting» у рамках реалізації стратегічного проекту «Vote électronique». Експериментальне електронне голосування відбулося вперше у 2003 р. За попередніми планами

швейцарського уряду, на парламентських виборах у 2015 р. в мережі Інтернет планувалася можливість проголосувати для абсолютної більшості громадян, навіть тих, які перебуватимуть поза межами країни. Проте, через підозри на присутність спеціальних «чорних ходів» у ПЗ системи, що дали б змогу порушити конфіденційність виборців, введення системи було обмежене лише двома кантонами та громадянами що знаходяться поза межами крани, що становить приблизно 30 % усіх виборців [6, 7].

Основними проблемами електронного голосування, що заважають його загальному використанню вже сьогодні є проблеми автентифікації виборців, рівного виборчого права, забезпечення принципу таємності голосування та проблема довіри виборців до інформаційної системи.

І якщо для рішення перших двох проблем існують методи, що вже давно та успішно використовуються у інших видах інтернет послуг, то для вирішення проблем таємності вибору та довіри виборців до інформаційної системи необхідно розробити нові підходи та системи, що їх використовують.

Тому метою даної роботи є розробка нової моделі хмарної системи електронного голосування, що дасть користувачам системи можливість впевнитися у вірності зарахування їх вибору і при цьому забезпечить його таємність.

ОГЛЯД СТАНУ ПРОБЛЕМИ

Розглянемо основні ризики системи електронного голосування у порядку, в якому їх повинна вирішувати система електронного голосування:

— проблема автентифікації виборців

— проблема забезпечення рівного виборчого права

— проблема забезпечення принципу таємного голосування

— проблема довіри виборців до системи

Проблема автентифікації виборців — полягає у необхідності визначенні особи виборця перед голосуванням для перевірки його правомірності. Серед основних відомостей, що необхідно визначити, є повне ім’я, вік, громадянство, право голосувати. Для рішення цієї проблеми застосовують методи, що вже використовуються у інших видах інтернет послуг (наприклад інтернет банкінг, декларування доходів) — цифрові підписи та ідентифікаційні картки.

Проблема рівного виборчого права — жоден з користувачів системи не повинен мати право голосувати більше ніж один раз, чи впливати на голоси інших користувачів. Зазвичай кожна з існуючих систем має одну централізовану базу даних виборців, за допомогою якої ведеться облік виборців. До впливу на інших користувачів варто віднести такі важливі проблеми як підкуп, вмовляння, погрожування та інше. Цим небезпекам важко запобігти при голосуванні на дому, тому в багатьох країнах світу електронне голосування відбувається за допомогою спеціалізованих терміналах на виборчих дільницях [9].

Проблема забезпечення принципу таємного голосування — система не повинна збирати жодних даних про вибір окремого з користувачів. За звичайної схеми виборів для забезпечення таємниці голосування достатньо не фотографувати бюлетень, впевнитись, що бюлетень не підписаний вашою фамілією, і що в кабінці для голосування не присутні сторонні лиця. При застосуванні систем дистанційного голосування виборці вже не можуть самостійно впевнитись, що інформація, яка дозволяє ідентифікувати їх особистість, не була прикріплена до електронного бюлетеня, при надсиланні його до серверу. На практиці, вироблені достатньо універсальні підходи до вирішення цього питання. Так, наприклад, в Швейцарії використовується підхід, який забезпечує таємницю голосування відсутністю поіменного списку виборців, що містить ідентифікуючі виборця данні, а лише наявністю списку, що містить номера дійсних карток для голосування. Інший метод полягає у використанні серверів деперсоніфікації. Проте складність реалізації усіх цих засобів полягає в тому, що організатори виборчого процесу є однією з зацікавлених у конфіденційній інформації сторін, і дані методи стають неефективними, при неправомірних діях на стороні серверу голосування. [1, 2]

Проблема довіри виборців до системи — в певній мірі ця проблема пов’язана з двома вище згаданими. За звичайної схеми виборів є велика кількість письмових підтверджень перемоги одного з кандидатів/пропозицій у вигляді бюлетенів та протоколів. Так, після вкидання бюлетеню в урну на виборчій дільниці, він буде оброблений людьми з виборчої комісії під наглядом спеціально обраних наглядачів. По завершенні голосування, виборець може бути впевнений, що його голос (бюлетень) вже не буде використаний. У випадку ж сучасних систем електронного голосування, після обрання одного з запропонованих варіантів, виборець вже не може бути впевнений, як саме зарахувався його голос у системі, адже особа з доступом до внутрішніх серверів має змогу підтасувати кінцевий результат без жодних слідів. Для вирішення даної проблеми у представленій системі пропонується спеціальний механізм, що у зручній формі (з використанням QR кодів) дозволить виборцю визначити правильність зарахування його голосу після завершення та оголошення результатів виборів, основою якого є частково гомоморфне шифрування на еліптичних кривих.

ОПИС СИСТЕМИ

Система електронного голосування складається з трьох частин: керуючого модулю, модулю голосування, клієнтського модулю.

Архітектури системи представлено на UML діаграмі прецедентів (рис. 1).

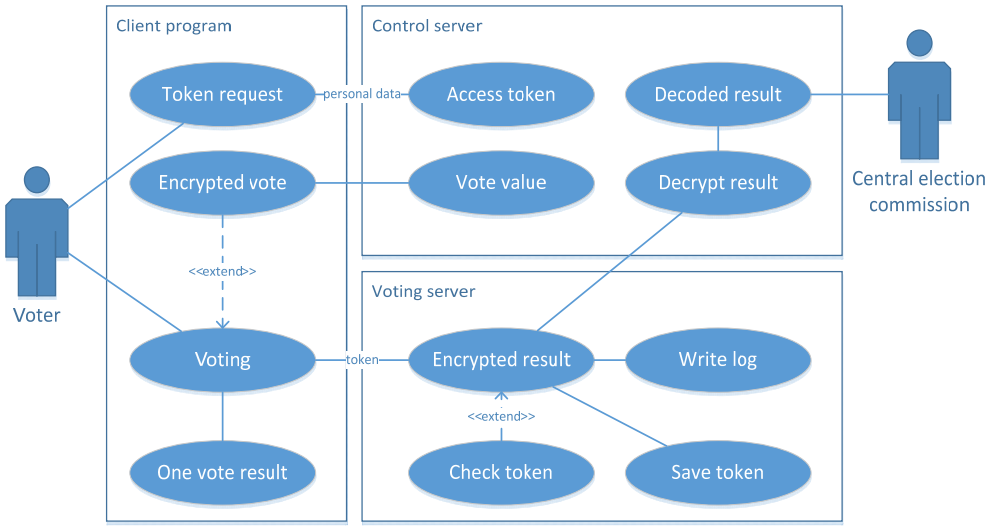

Рис. 1. Архітектура системи

Керуючий модуль (Control server) — це сервер що відповідає за авторизацію користувачів (видає access token), зберігає у відкритому вигляді ваги варіантів для голосування (Vote value) та за отримання, розшифрування і обробку результатів голосування (Decrypt and Decode result).

Модуль голосування (Voting server) — це сервер на якому зберігається поточний стан виборчої системи, до нього звертаються клієнтські модулі виборців для реєстрації свого вибору.

Клієнтський модуль (Client program) — це додаток, що використовує виборець для авторизації у системі (Token request) та процесу голосування (Voting).

Автентифікація виборців

Для ідентифікації користувача у системі пропонується використання спеціальних ID карток. Магнітну ID карту виборець повинен отримати на одній з виборчих дільниць свого міста. Вона містить підписані сертифікатом, особисті данні виборця. Голосування відбувається на виборчій дільниці, за допомогою підготованих обчислювальних машин, з встановленою сертифікованою клієнтською програмою та зчитувачем для магнітних карток.

ID картки дадуть змогу користувачу бути впевненими, що ніхто не зможе проголосувати замість нього, навіть знаючи його особисті дані. Також не є критичною втрата самої картки, адже pin код до неї відомий тільки користувачу і нікому крім нього.

Після запуску клієнтської програми користувач авторизується у системі за допомогою своєї ID картки та pin коду до неї. Особиста інформація користувача передається по захищеному SSL протоколу на керуючий сервер де виконується її перевірка. Керуючий сервер містить загальній перелік виборців. Якщо, користувач може бути допущений до голосування, керуючий сервер повертає клієнтській програмі користувача спеціально згенерований ключ доступу (token), що містить хеш даних користувача (отриманий за допомогою хеш-функції (H) на основі персональних даних користувача з його ID картки) підписаний сертифікатом керуючого серверу та термін його дії:

$$Token \rightarrow H(Personal\ data) + Certificate \qquad (1)$$

Після отримання, цей ключ може бути використаний клієнтською програмою для доступу на сервер голосування.

Процес голосування

Перед голосуванням, комп'ютери на виборчій дільниці повинні бути певним чином налаштовані. У кожному з комп'ютерів повинен бути відомий IP адрес серверів для голосування та авторизації, а також перелік комп'ютерів своєї виборчої дільниці та їх адреси. Один з комп'ютерів обирається локальним сервером виборчої дільниці. Контрольні суми програм (CRC) повинні бути перевірені наглядачами виборчої дільниці.

При голосуванні, клієнтська програма користувача, передає серверу для голосування отриманий при авторизації ключ доступу. Сервер для голосування перевіряє його коректність у наступному порядку:

1. Перевіряє, чи не голосував користувач з таким ключем раніше. У випадку, якщо ключ зустрівся у базі даних сервера для голосування, сервер повертає клієнту повідомлення про неможливість повторного голосування.

2. Перевіряє, чи не вийшов термін дії токену. Якщо токен прострочений, сервер повертає клієнту повідомлення про необхідність повторної авторизації.

3. Перевіряє, чи відповідає хеш послідовність підпису. При невідповідності, або неправильності сертифікату керуючого сервера, сервер передає клієнту повідомлення про помилку та розриває з'єднання.

Після авторизації у керуючому сервері клієнтська програма крім ключу доступу отримує список варіантів відповідей ($a_0, a_1, \dots, a_m$), їх текстовий опис та відкриті параметри алгоритму шифрування – публічний ключ системи (P_S), та параметри еліптичної кривої. Числове значення кожного варіанту системи (вага) у даному випадку рівне 2 якщо користувач голосує за цей варіант і 1 якщо проти. Параметрами еліптичної кривої для алгоритму шифрування на еліптичних кривих є власне еліптична крива $E(a, b)$, точка-генератор G, що належить даній кривій, її порядок N_G, а також просте число (P_E) — модуль поля кривої.

Безпека, що забезпечується криптографічним підходом на основі еліптичних кривих залежить від того наскільки важкою для вирішення виявляється задача, визначення n за відомими nP та P. Цю задачу зазвичай називають проблемою логарифмування на еліптичній кривій. Криптостійкість при використанні ключу шифрування у 192 біти є співвідносною до криптостійкості алгоритму RSA з довжиною ключа 1024 біти [11].

Коли користувач обирає один з варіантів (a_V), клієнтська програма повинна відобразити число-вагу обраного варіанту (1 або 2) у область еліптичної кривої (P_V). Це можна зробити помноживши значення варіанту на точку-генератор еліптичної кривої:

$$P_V = a_V \cdot G \tag{2}$$

Отриману, у результаті попередньої дії, точку необхідно зашифрувати, використавши відкритий ключ системи, отриманий у керуючого серверу. Для цього клієнтська програма генерує випадкове число ($k,\ a_m \cdot n + 1 < k < P_E$) — сеансовий приватний ключ. В результаті шифрування отримаємо пару точок (P'_V) еліптичної кривої E.

$$P'_V = (kG, P_V + kP_S) \tag{3}$$

Перша частина ($LP'_V = kG$) даної пари — підказка, що дозволяє власнику відкритого ключа, використавши приватний ключ виділити початкову точку з другої частини пари ($RP'_V = P_V + kP_S$). Точку RP'_V необхідно гомоморфно додати до загального попереднього результату голосування (S'_{i-1}), що зберігається на сервері голосування. Сумування відбувається по кожному з варіантів окремо.

$$S'_i = S'_{i-1} + RP'_V \tag{4}$$

$$S' = \sum_{i=1}^{n} RP'_{V_i} \tag{5}$$

Процедура голосування виконується локально кожним з користувачів. Сума S' зберігається на кожному комп'ютеру виборчої ділянки до кінця голосування. Послідовність дій виглядає наступним чином:

1. Клієнтська програма робить запит до локального серверу виборчої дільниці, щоб отримати поточне значення голосування (S') по кожному з варіантів.

2. Локальний сервер ставить клієнта у чергу інших клієнтів, що зробили запит раніше.

3. Коли черга доходить до одного з клієнтів, локальний сервер передає йому поточне значення голосування (S'_{i-1}) по кожному з варіантів.

4. Клієнт додає до поточного значення зашифровану вагу свого вибору (RP'_V), та повертає його серверу разом з підказкою (LP'_V).

5. Клієнтська програма виводить на екран користувачу числа S'_i та S'_{i-1} по кожному з варіантів у вигляді QR-коду. Це забезпечить виборцю можливість перевірити правильність зарахування свого вибору по завершенню виборів.

6. Локальний сервер передає поточне значення іншим комп'ютерам дільниці.

Створення загальної суми варіантів виборів користувачів на клієнтській машині забезпечить неможливість дізнатись вибір користувача навіть після розкриття приватного паролю керуючого серверу по завершенню терміну голосування.

Отримання результатів

По завершенні терміну проведення голосування, керуючий сервер робить запит до серверу голосування для отримання загального результату. Сервер голосування у свою чергу опитує кожну з виборчих дільниць. Локальний сервер виборчої дільниці передає серверу голосування зашифровану суму S' по кожному з варіантів відповідей та список підказок LP'_{V_i}.

Для отримання розшифрованої суми ваг варіантів відповідей, сервер повинен помножити кожну з підказок на приватний ключ шифрування системи (p) та відняти результат від суми (S').

$$S = S' - \sum_{i=1}^{n} p \cdot RP'_{V_i} \tag{6}$$

Якщо підставити значення S' та RP'_V отримаємо розшифроване значення суми ваг варіантів голосування користувачів:

$$S = S' - \sum_{i=1}^{n} p \cdot k_i \cdot G = \sum_{i=1}^{n} (P_{V_i} + k_i P_S) - \sum_{i=1}^{n} k_i P_S = \sum_{i=1}^{n} P_{V_i} \tag{7}$$

Після отримання розшифрованого варіанту необхідно відобразити його з області точок еліптичної кривої, назад у область цілих чисел. Для цього сервер повинен згенерувати перші h точок еліптичної кривої, де h:

$$h = n \cdot x \tag{8}$$

Графік залежності часу генерації таблиці для зворотного відображення варіантів наведено нижче (.NET Framework 4.5.2, Windows 10, Intel i5-6600, 16Gb RAM, один потік):

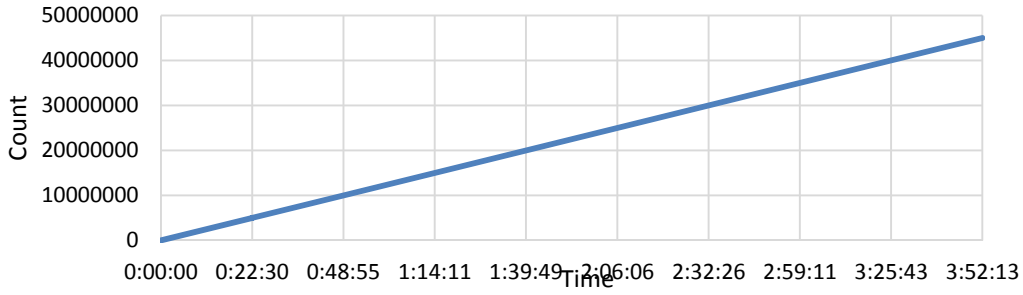

Рис. 2. Графік залежності часу генерованих точок кривої P-192 від їх кількості

Так як відповідь Ні (коли виборець не голосує) кодується як 1 та також додається до суми голосів, серверу необхідно виділити кількість голосів в залежності від загальної кількості проголосувавших (N):

$$\begin{cases} 2x + y = S \\ x + y = N \end{cases} \tag{9}$$

де x — кількість людей проголосувавших за варіант, а y — проти.

Відобразивши суму по кожному з варіантів сервер отримує можливість порівняти їх та визначити переможця. Також, за рахунок запиту сум голосів серверу виборчої дільниці, у системі закладена можливість оголошення результатів по кожній з виборчих дільниць окремо.

Для перевірки коректності врахування голосу виборцями, необхідно оприлюднити закритий ключ голосування. Тоді кожен з виборців може скористатись будь-яким стороннім додатком, що на основі QR коду виборця, опублікованого закритого ключа системи та формулами 2—8, дозволить визначити варіант голосування що був зарахований системою.

ПРИКЛАД

У країні відбуваються президентські вибори. Є 10 зареєстрованих кандидатів.

Відкритими параметрами системи є параметри еліптичної кривої та відкритий ключ шифрування. Для прикладу візьмемо криву рекомендовану NIST: P-192 [10]. Її параметри:

$P_E = 6277101735386680763835789423207666416083908700390324961279$
$\mathrm{N}_G = 6277101735386680763835789423176059013767194773182842284081$
$a = -3$
$\mathrm{b} = 64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1$
$G_x = 188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012$
$G_y = 07192b95ffc8da78631011ed6b24cdd573f977a11e794811$

Обираємо приватний ключ шифрування:

$$p = 26558562485896930961545096124999523125231866390682126703 02$$

Визначаємо публічний ключ шифрування:

$$P_{S_x} = 60821652769312232595326489580955408167281944077613682 8110$$

$$P_{S_y} = 61828810515884264324103412732571718009072543762181567883 21$$

Після авторизації виборець отримує 10 варіантів. Після вибору та підтвердження одного із них клієнтська програма генерує 10 сеансових приватних ключів. Так як у області точок еліптичної кривої не визначена операція множення на 0, коли користувач голосує за якийсь з варіантів він кодується числом 2 у іншому випадку 1 (G). Нехай користувач проголосував за кандидата 2. Нижче розглянемо розрахунки для данного варіанту:

$$P_V = 2 \cdot G = (399999758447622721422749120567434666825413022059161780 5041,$$
$$393304971859070169489986440622693545653200973184672562 4472)$$

Після цього клієнтська програма шифрує закодований варіант (формула 3):

$$k = 35782793466528962136602955574500835656097318224094201 2902$$
$$LP'_V = (795357982364963405413646088716125976512360924438263075286,$$
$$167056176734003039784452677192614981489824232024200154 23)$$
$$RP'_V = (211226749608942348047553842029750649675056947286142903 6778,$$
$$480059118818380457032782227662477066411540693317365140 1623)$$

Нехай, ще 2 користувачі проголосували за кандидата 2, а всього голосувало на дільниці — 4.

$$LP'_{V_2} = 667878581284661658342508811967788320832881571865134155 20,$$
$$224279297264644923359107977829886405691358670961288736 6458$$
$$LP'_{V_3} = 915141844835953377223754891253530479211895037475167102 998,$$
$$196738771542618596485641044602108155453230286447243761325 7$$
$$LP'_{V_4} = 921256860528940401031889437022407364662409130411953876 11,$$
$$106738425417917606003006631601455454146228731961393998947 1$$
$$S' = 343174819035923404931575176140671094075337769619945628866 1,$$
$$718280963812772129647538822576831429292268071782968039 0$$

Після голосування сервер повинен розшифрувати S':

$$S = S' - \sum n \cdot LP'_V =$$
$$= 146089920418721848344810353890431714350827256946844463108 0,$$
$$152642128106073454162929762441874157764139728522830311 2195$$

Для зворотного відображення результату в область цілих чисел сервер генерує таблицю використовуючи формулу 2:

Таблиця 1.

Відображення цілих чисел у точки кривої P-192

Ціле число	Точка еліптичної кривої
2	(399999758447622721422749120567434666825413022059161780504 1, 393304971859070169489986440622693545653200973184672562447 2)
3	(608076201759106617838712768394333228474851264596884403155 6, 402269644997423207968641799658339646784922321244328266592 2)
4	(476324331626881875534598951432701459412737898011928878033 0, 225765405429266235525376400650624698204129281057857635879)
5	(489064249585277214804708044296585782364311381902502112355 6, 350738748317137383541414263917240408625524540900945734122 1)
6	(293271579841376184475542449076347913266986549860590162099 0, 400613656917858942598542356363704449702347440242063691343 1)
7	(146089920418721848344810353890431714350827256946844463108 0, 152642128106073454162929762441874157764139728522830311219 5)

Після декодування S за допомогою таблиці 1 отримаємо число 7. Для того щоб дізнатись скільки виборців проголосувало за даний варіант скористаємось формулою 9:

$$\begin{cases} 2x + y = 7 \\ x + y = 4 \end{cases}$$
$$x = 3$$

Отже за варіант 2 проголосувало 3-є виборців.

ВИСНОВКИ

В даній роботі було представлено підхід до створення хмарного сервісу електронного голосування з використанням частково гомоморфного алгоритму шифрування для захисту принципів таємності вибору учасників. Наведено приклад роботи математичної моделі системи та час виконання затратної операції генерації таблиці кодування цілих чисел точками еліптичної кривої.

Перевагою даного підходу є неможливість відслідковування вибору користувачів на стороні хмарного сервісу навіть після завершення голосування та розкриття кількості виборів кожного окремого варіанту.

Таким чином, на відміну від існуючих аналогів, інформація про вибір окремої людини є недосяжною не тільки для сторонніх осіб, а і для власників обчислювальних ресурсів на яких працює система. А використання частково гомоморфного алгоритму шифрування на еліптичних кривих дозволяє досягти достатньої для функціонування системи швидкодії, коли час виконання операцій не впливає суттєво на процедуру голосування.

Окрім цього, система дозволяє кожному з бажаючих перевірити правильність врахування їх голосу після закінчення голосування та розкриття приватного ключа шифрування, за допомогою зручного QR коду. Це підвищує довіру виборців до системи та ускладнює їх підкуп.

СПИСОК ЛІТЕРАТУРИ

1. Титарчук Є. О. Використання гібридного шифрування в хмарних технологіях комп'ютерних обчислень [Електронний ресурс]: Sworld. — Режим доступу : http://www.sworld.com.ua/index.php/technical-sciences-314/informatics-computer-science-and-automation-314/23065-314-274. — Назва з екрана.
2. Титарчук Є. О. Захист даних в хмарних технологіях комп'ютерних обчислень [Електронний ресурс]: Захист даних в хмарних технологіях комп'ютерних обчислень // ВНТУ — ВНТУ. — Режим доступу : http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf. — Назва з екрану.
3. Шелудько Г. І. Електронне голосування як різновид виборчих Інформаційно-комунікативних технологій: Зарубіжний та вітчизняний / Шелудько Ганна Ігорівна // м. Київ, 2015 р.
4. Електронне голосування [Електрон. Ресурс]. — Режим доступу : http://uk.wikipedia.org/wiki/Електроннеголосування
5. Litan R. E. Law and Policy in the Age of Internet // Duke Law Journal. — 2001. — Vol. 50, № 4. — P. 145.
6. Пряма демократія Швейцарії у цифрову еру [Електронний ресурс]. — Режим доступу :

http://www.swissinfo.ch/rus/detail/content.html?cid=36670692&link=cto
7. Hacking fears jeopardise e-voting rollout [Електронний ресурс]. — Режим доступу : http://www.swissinfo.ch/directdemocracy/voting-with-a-click_hacking-fears-jeopardise-e-voting-rollout/41635672
8. Homomorphic encryption [Електронний ресурс]. — Режим доступу : https://en.wikipedia.org/wiki/Homomorphic_encryption
9. Elections in Brazil [Електронний ресурс]. — Режим доступу : https://en.wikipedia.org/wiki/Elections_in_Brazil#The_Brazilian_voting_machines
10. Recommended elliptic curves for federal government use / NIST — July 1999. — Режим доступу : http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf
11. O. N. Zdanov. Methods and tools of cryptographic information protection / O. N. Zdanov. V. V. Zolotarev // SibHau. — Krasnoyarsk — 2007. — p. 186

SPISOK LITERATURI

1. Titarchuk E. O. Vikoristannya gíbridnogo shifruvannya v khmarnikh tekhnologíyakh komp'yuternikh obchislen' [Yelektronniy resurs]: Sworld. — Rezhim dostupu: http://www.sworld.com.ua/index.php/technical-sciences-314/informatics-computer-science-and-automation-314/23065-314-274. — Nazva z yekrana.
2. Titarchuk Ê. O. Zakhist danikh v khmarnikh tekhnologíyakh komp'yuternikh obchislen' [Yelektronniy resurs]: Zakhist danikh v khmarnikh tekhnologíyakh komp'yuternikh obchislen' // VNTU — VNTU. — Rezhim dostupu: http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf. — Nazva z yekranu.
3. Shelud'ko G. Í. Yelektronne golosuvannya yak ríznovid viborchikh Ínformatsíyno-komunikativnikh tekhnologíy: Zarubízhniy ta vítchiznyaniy / Shelud'ko Ganna Ígorívna // m. Kiïv, 2015r
4. Yelektronne golosuvannya [Yelektron. Resurs]. — Rezhim dostupu: http://uk.wikipedia.org/wiki/Yelektronnegolosuvannya
5. Litan R. E. Law and Policy in the Age of Internet // Duke Law Journal. — 2001. — Vol. 50, № 4. — P. 145.
6. Ryama demokratíya Shveytsaríï u tsifrovu yeru [Yelektronniy resurs]. — Rezhim dostupu: http://www.swissinfo.ch/rus/detail/content.html?cid=36670692&link=cto
7. Hacking fears jeopardise e-voting rollout [Yelektronniy resurs]. — Rezhim dostupu: http://www.swissinfo.ch/directdemocracy/voting-with-a-click_hacking-fears-jeopardise-e-voting-rollout/41635672
8. Homomorphic encryption [Yelektronniy resurs]. — Rezhim dostupu: https://en.wikipedia.org/wiki/Homomorphic_encryption
9. Elections in Brazil [Yelektronniy resurs]. — Rezhim dostupu: https://en.wikipedia.org/wiki/Elections_in_Brazil#The_Brazilian_voting_machines
10. Recommended elliptic curves for federal government use / NIST – July 1999. — Rezhim dostupu: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf
11. O. N. Zdanov. Methods and tools of cryptographic information protection / O. N. Zdanov. V. V. Zolotarev // SibHau. — Krasnoyarsk — 2007. — p. 186

Надійшла до редакції 14.12.2016 р.

КВЄТНИЙ РОМАН НАУМОВИЧ — д-р техн. наук, професор, завідувач кафедри АІВТ, Вінницький національний технічний університет, м. Вінниця, e-mail: rkvetny@mail.ru.

ТИТАРЧУК ЄВГЕНІЙ ОЛЕКСАНДРОВИЧ — аспірант, факультет комп'ютерних систем та автоматики, Вінницький національний технічний університет, м. Вінниця, e-mail: etitarchuk@gmail.com.