МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 004.056.55

Р. Н. Квєтний, Є. О. Титарчук

ХМАРНА СИСТЕМА ОБМІНУ ЕЛЕКТРОННИМИ ГРОШИМА НА ОСНОВІ АЛГОРИТМУ ЧАСТКОВО ГОМОМОРФНОГО ШИФРУВАННЯ

Вінницький національний технічний університет, м. Вінниця

Анотація. В даній роботі представлено хмарну модель обміну електронними грошима з централізованим сервером та системою забезпечення анонімності користувачів з використанням частково гомоморфного алгоритму шифрування. У порівнянні з поширеними у даний момент криптовалютами, представлений підхід на відміну від існуючих аналогів використовує централізований сервер та систему деперсоналізації користувачів на основі частково гомоморфного алгоритму шифрування на еліптичних кривих, що дозволяє забезпечити захист приватної інформації користувачів. Для забезпечення анонімності у запропонованій моделі планується використання частково гомоморфного алгоритму шифрування на еліптичних кривих.

Ключові слова: Електронні гроші, Частково гомоморфне шифрування, Хмарний сервіс.

Аннотация. В данной работе представлены облачную модель обмена электронными деньгами с централизованным сервером и системой обеспечения анонимности пользователей с использованием частично гомоморфного алгоритма шифрования. По сравнению с распространенными в данный момент криптовалютами, представленный подход в отличие от существующих аналогов использует централизованный сервер и систему деперсонализации пользователей на основе частично гомоморфного алгоритма шифрования на эллиптических кривых, позволяет обеспечить защиту частной информации пользователей. Для обеспечения анонимности в предложенной модели планируется использование частично гомоморфный алгоритм шифрования на основе эллиптических кривых.

Ключевые слова: Электронные деньги, Частично гомоморфное шифрование, Облачный сервис.

Abstract. The problem this article deals with is cryptographic analysis of partially homomorphic encryption scheme by addition based on elliptic curves. Complexity of solving elliptic curve discrete logarithm problem using Pollard's ρ-method is represented. Shown model determines the cryptographic stability of the basic asymmetric encryption based on the elliptic curves. A mathematical model that demonstrates the simplification of the problem of discrete logarithm on an elliptic curve with an increase in the number of elements of homomorphic summation with respect to the basic algorithm of asymmetric encryption is shown. The cryptographic stability of the partially homomorphic encryption algorithm on elliptic curves is determined.

Key words: Digital currency, partially homomorphic encryption, cloud service.

Вступ

Електронні гроші міцно закріпилися в нашому повсякденному житті. Цей вид грошей був введений для спрощення розрахунків у мережі Інтернет. Зараз їх використовують для оплати товарів та послуг, роботи віддалених робітників, переказів традиційних грошей, тощо.

Електронні гроші – відносно нова форма грошей. Їх історія бере початок з 50-х років XX сторіччя, коли записи банківських рахунків почали переносити з паперових носіїв інформації на електронні. Наступний етап розвитку електронних грошей стався у кінці 70-х, коли Девід Чаум, американський науковець у області криптографії, запропонував ідею «електронної готівки». Це стало можливим після створення перших систем електронного підпису. [1]

На відміну від популярних кредитних карток, новий вид грошей на той момент характеризувався анонімністю. Електронні гроші не враховувались на банківських рахунках клієнтів системи, а при проведенні платежу особисті дані платника не реєструвалися. Але, в той час електронні гроші ще не могли бути повноцінним засобом обміну, тобто у одержувача не було можливості здійснити за них розрахунки, він мав право лише отримати у обслуговуючого банку грошовий еквівалент електронних засобів.

З появою у 90-х роках чергового виду електронних грошей дана проблема частково була вирішена. Користувачі та постачальники товарів отримали можливість переводити засоби один одному без участі банків. В період швидкого розвитку Інтернет-технологій на межі сторіч в США, Євросоюзі та Японії було створено близько двадцяти платіжних Інтернет-систем. Але багато із них досить швидко перестали існувати, або ж збанкрутували, як наприклад, Beenz, Flooz, Goldmoney та інші.

В наш час електронні гроші поступово заміщують паперові, адже вони мають значну кількість переваг: зручність та доступність, економія часу; адже платежі відбуваються миттєво та можуть бути автоматизовані, зазвичай вимагають менше комісійних та дозволяють зберігати анонімність. Проте значними є і недоліки: ймовірність взлому, необхідність підключення до мережі, а також незахищеність – адже гарантом електронних грошей є лише емітент, держава ж не надає жодних гарантій і не несе жодної відповідальності.

Надзвичайний розвиток хмарних сервісів заставляє банки все частіше звертати увагу на можливість перенесення обчислювальних потужностей необхідних для сучасної банківської системи у «хмару». Проте небезпекою таких дій є відкриття фінансової інформації користувачів провайдеру хмарного сервісу. [2, 3]

Метою даної роботи є підвищення захищеності грошообміну шляхом створення хмарної моделі фінансової системи у якій користувачі та контролюючий орган зможуть зберігати рахунки та виконувати фінансові транзакції без розкриття особистої та фінансової інформації.

Задачі

1. Описати протокол захищених транзакцій між клієнтами банку при використанні публічного хмарного сервісу.
2. Показати можливість використання описаного протоколу для взаємодії між клієнтами різних банків.

Розв’язання задач

Мінімальна система необхідна для захищеної транзакції складається з наступних елементів:

- трьох користувачів системи, їх клієнтських додатків та рахунків у банківській службі;
- банку, його локального серверу та служби у хмарі.

Для захисту персональної інформації користувачів у протоколі транзакції пропонується використання частково гомоморфного відносно операції додавання алгоритму шифрування на основі еліптичних кривих. [3–5]

Робота системи складається з підготовчого етапу та сеансів здійснення захищених транзакцій – основного етапу.

На підготовчому етапі банківський сервер визначає для клієнтських додатків відкриті параметри схеми шифрування (параметри еліптичної кривої $E(a, b)$, точка-генератор G, що належить даній кривій, її порядок N_G, просте число (P_E) – модуль поля кривої), а також адреси абонентів (набір цілих чисел $a_0, a_1, \dots, a_m$). Для генерації чисел-адрес (a) серверу необхідно знати кількість людей (m), що мають рахунки у хмарному сервісі та максимальне число (n) коштів, що може бути збережено на одному рахунку. Тоді для визначення адреси можна скористатися формулою, що є ідентичною формулі для розрахунку ваги при голосуванні з різними вагами:

$$a_0 = 1 \tag{1}$$

$$a_i = a_{i-1} \cdot n + 1 \tag{2}$$

$$i = 1, 2, \dots, m \tag{3}$$

Спрощена діаграма сеансу транзакції показана на рисунку 1:

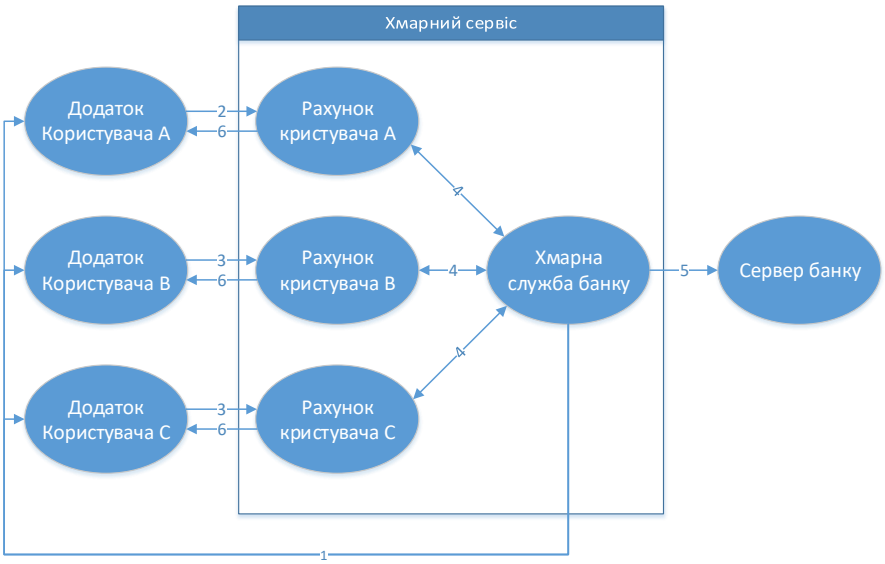

Рисунок 1 – Сеанс для здійснення захищеної транзакції

Після реєстрації користувача на локальному сервері банківської системи клієнт отримає персональний приватний ключ (p). Також локальний сервер банку генерує та повідомляє іншим учасникам системи публічний ключ алгоритму шифрування, точку (P_s).

Протокол здійснення захищеної транзакції включає в себе наступну послідовність дій:

1. Нотифікація клієнтів про можливість здійснення транзакції (1) – здійснюється хмарним сервісом з заданою періодичністю. Необхідна для інформування клієнтських додатків про початок сеансу передачі коштів.
2. Отримавши нотифікацію клієнтський доданок генерує приватні сеансові ключі шифрування. Для цього клієнтська програма генерує випадкове число ($k,\ a_m \cdot n + 1 < k < P_E$). Після генерації сеансового ключа клієнт повинен змінити свій спеціальний операційний рахунок (2) та (3). При цьому, якщо клієнт А хоче переказати кошти клієнту В, то він повинен зашифрувати кількість коштів, яку хоче перерахувати та число, що представляє адресанта. Коли користувач обирає одного з адресантів (a_0), а також суму для переказу (c_0), та перемножує їх між собою:

$$ac_0 = a_0 \cdot \mathrm{c}_0 \tag{4}$$

Клієнтська програма повинна відобразити результат у область еліптичної кривої (P_E). Це можна зробити помноживши значення варіанту на точку-генератор еліптичної кривої:

$$P_{ac} = ac_0 \cdot G \tag{5}$$

Отриману, у результаті попередньої дії, точку необхідно зашифрувати, використавши відкритий ключ системи, згенерований локальним сервером банку:

$$P'_{ac} = (kG, P_{ac} + kP_S) \tag{6}$$

Зашифрований результат клієнтська програма заносить на спеціальний операційний рахунок (2). Перша частина ($LP'_{ac} = kG$) даної пари – підказка, що дозволяє власнику відкритого ключа, використавши приватний ключ, виділити початкову точку з другої частини пари ($RP'_{ac} = P_{ac} + kP_S$).

3. Клієнти системи, що не бажають здійснювати фінансових операцій, також генерують сеансовий ключ, проте, зашифровують за допомогою нього число 0. Зашифрований результат так само, як і на попередньому кроці, розміщується на операційному рахунку (3).
4. На наступному етапі, банківська служба у хмарному сервісі гомоморфно додає зашифровані числа що знаходяться на операційних рахунках усіх клієнтів (4).

$$\sum_{i=0}^{m} A'_i = (\sum_{i=0}^{m} k_i G\,, \sum_{i=0}^{m} (P_{ac_i} + k_i P_s)) \tag{7}$$

5. Утворена сума передається на локальний сервер банку для перевірки та архівування здійснених транзакцій (5).
6. Кожний окремий клієнт визначається різною вагою в утвореній сумі. Тому для здійснення транзакції хмарному сервісу необхідно додати утворене число до окемих рахунків кожного з клієнтів (4).
7. Останній етап – розшифрування результату транзакції клієнтською програмою. Для отримання розшифрованої суми коштів на рахунку, сервер повинен помножити кожну з підказок на приватний ключ шифрування системи (p) та відняти результат від суми (S').

$$S = S' - \sum_{i=1}^{n} p \cdot RP'_{ac_i} \tag{8}$$

Якщо підставити значення S' та RP'_{ac} отримаємо розшифроване значення добутку адреси користувача на суму перерахованих коштів:

$$S = S' - \sum_{i=1}^{n} p \cdot k_i \cdot G = \sum_{i=1}^{n} (P_{ac_i} + k_i P_S) - \sum_{i=1}^{n} k_i P_S = \sum_{i=1}^{n} P_{ac_i} \quad (9)$$

Після отримання розшифрованого результату, необхідно відобразити його з області точок еліптичної кривої назад у область цілих чисел. Для цього хмарна служба повинна згенерувати перші h точок еліптичної кривої, де h:

$$h = n \cdot x \quad (10)$$

Після підстановки розшифрованої точки у отриману таблицю відповідності клієнт отримує кінцеву суму на рахунку, після здійснення транзакції.

Ускладненням системи є створення захищеної транзакції між двома сервісами у межах однієї або між різними хмарами. Приклад хмарних сервісів двох різних банків у межах однієї хмари показано на рисунку 2.

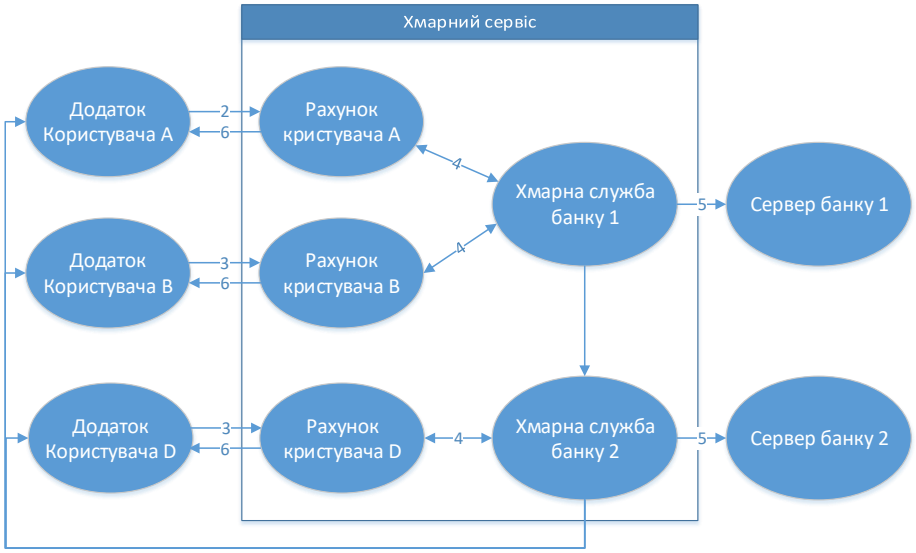

Рисунок 2 – Транзакція між двома хмарними службами

Особливістю такого підходу є об’єднання різних служб у спільну мережу з одночасною нотифікацією клієнтів. При встановленні зв’язку, клієнти відповідних банків інформуються про приєднання нових членів мережі та їх адреси.

Висновки

В роботі показано криптостійкість алгоритмів основаних на еліптичних кривих в залежності від порядку групи точок утвореної еліптичною кривою, при використанні алгоритму Поларда для знаходження приватного ключу шифрування. Алгоритм Поларда є одним з найшвидших алгоритмів розкладання чисел на множники в області точок еліптичної кривої і тому, фактично, визначає криптостійкість алгоритму частково гомоморфного шифрування на еліптичних кривих.

Встановлено, що криптостійкість частково гомоморфного алгоритму шифрування зменшується на кількість операцій гомоморфного додавання (m) відносно вихідного алгоритму ECDH, проте, так як порядок m значно менший n це не призводить до значної втрати криптографічної стійкості.

Список літератури

1. Chaum D. Blind signatures for untraceable payments / D. Chaum. — Santa Barbara : University of California, 1983.

2. Титарчук Є. О. Захист даних в хмарних технологіях комп'ютерних обчислень / Є. О. Титарчук // Pridneprovsky research journal. — 2014. — Vol. 5, No. 152. — P. 77–82.

3. Квєтний Р. Н. Використання частково гомоморфного алгоритму шифрування на еліптичних кривих у хмарній системі електронного голосування / Р. Н. Квєтний, Є. О. Титарчук // Оптико-електронні інформаційно-енергетичні технології. — 2016. — Vol. 32, No. 2. — P. 14–22.

4. Tebaa M. Homomorphic encryption applied to the cloud computing security / M. Tebaa, S. El Hajji, a El Ghazi // Proceedings of the World Congress on Engineering. — 2012. — Vol. 1. — P. 4–6.

5. Naehrig M. Can homomorphic encryption be practical? / M. Naehrig // ACM Computer and Communications Security. — 2011. — P. 113–124.

Стаття надійшла: 20.11.2017.

Відомості про авторів

Квєтний Роман Наумович — доктор технічних наук, професор, завідувач кафедра AIBT, Вінницький національний технічний університет, м. Вінниця.

Титарчук Євгеній Олександрович — аспірант, факультет комп'ютерних систем та автоматики, Вінницький національний технічний університет, м. Вінниця.