УДК 004.056.55

Ступень П. В.,
канд. техн. наук, доцент, Одеський національний політехнічний університет, м. Одеса, Україна
Соколов С. О.,
Одеський національний політехнічний університет, м. Одеса, Україна
Золкіна О. Ю.,
Одеський національний політехнічний університет, м. Одеса, Україна

ЗАСТОСУВАННЯ ГОМОМОРФНОГО ШИФРУВАННЯ ДЛЯ ЗАХИСТУ ЧИСЛОВИХ ДАНИХ У ХМАРНИХ СХОВИЩАХ

Хмарні сховища та хмарні сервіси, що дозволяють виконувати різні операції над даними відкрили багато можливостей для користувачів. Трудомісткі та складні обчислення, що потребують серйозних програмних та апаратних ресурсів, стали доступними для кожного, в будь-якій частині земної кулі, потрібен лише доступ в Інтернет. Проте існує і суттєвий недолік – незахищеність даних, що зберігаються та обчислюються у хмарних сервісах. Традиційні методи шифрування не дозволяють обробляти дані в зашифрованому вигляді, тому необхідно або повідомляти ключ шифрування хмарним сервісам, або зберігати дані в незашифрованому вигляді. В обох випадках не має гарантії, що ваші дані надійно захищені від несанкціонованого доступу. Для вирішення цієї проблеми існує гомоморфне шифрування даних, характерною особливістю якого є можливість виконувати будь-які математичні операції над зашифрованими даними.

Ключові слова: *хмарне сховище; гомоморфне шифрування; поліном першого порядку; ключ шифрування.*

Хмарні сховища – це програмно-апаратне забезпечення, доступне користувачеві через Інтернет у вигляді сервісу, що дозволяє використовувати зручний інтерфейс для віддаленого доступу до виділених ресурсів (обчислювальних ресурсів, програм і даних). На даний момент більшість хмарних інфраструктур розгорнуто на серверах датацентрів, використовуючи технології віртуалізації, що фактично дозволяє будь-якому користувачу використовувати обчислювальні потужності, абсолютно не замислюючись про технологічні аспекти. Завдяки цій особливості, хмарні обчислення широко використовуються в навчальній, науковій, комерційній та інших сферах діяльностях. Незважаючи на те, що такі системи отримали широке розповсюдження завдяки своїм особливостям, вони мають серйозний недолік, який стосується інформаційної безпеки. Часто виникає особливість обробки даних, що являє собою конфіденційну або комерційну таємницю. Для обробки цих даних, власнику необхідно передати та повідомити ці дані третій стороні, а це вже є суттєвим ризиком несанкціонованого доступу до таємної інформації. Саме для вирішення цієї проблеми ідеальним рішенням буде використання гомоморфного шифрування даних. На відміну від традиційного шифрування, воно дає можливість виконувати будь-яку обробку даних у зашифрованому вигляді [1].

25 червня 2009 року, аспірант Стенфордського університету і стажист IBM Крейг Гентрі запропонував модель повністю гомоморфного шифрування, яка дозволяла проводити глибоку обробку даних без їх попереднього розшифрування. В алгоритмі Крейга Гентрі виконуються властивості гомоморфності щодо як множення, так і складання. Тим самим дану модель можна використовувати в хмарних обчисленнях без обмежень. Передаючи дані в хмари, тобто в небезпечну, з точки зору конфіденційності, зону, можна не турбуватися про їх розголошення внаслідок несанкціонованого доступу. Але модель Крейга Гентрі виявилася занадто непрактичною. Зі збільшенням кількості операцій вироблених над зашифрованим текстом складність і розмір шифр-тексту збільшується з неймовірною швидкістю. І незважаючи на те, що за останні кілька років були зроблені покращення цієї моделі, вона все ще залишається теоретичною моделлю, яка не застосовується на практиці. Гомоморфне шифрування значно збільшує вимоги до обчислювальних ресурсів комп'ютера. За оцінкою самого Крейга Гентрі, наприклад, обробка пошукового запиту в Google у випадку, якщо текст гомоморфно зашифрований,

потребує приблизно в трильйон разів більше обчислень порівнюючи з незашифрованим текстом [2].

Для реалізації гомоморфного шифрування на практиці та спрощення і підвищення швидкості обробки зашифрованих числових даних доцільно використати метод, що базується на алгоритмі (рис. 1), основною ідеєю якого, є заміна числа, що підлягає шифруванню, на поліном першого порядку. Процес шифрування, обробки зашифрованих числових даних та розшифрування в загальному вигляді буде складатися з наступних кроків:

1. Користувач задає числа, над якими необхідно провести математичні операції, а також ключ шифрування, завдяки якому будуть зашифровані та розшифровані числові дані.

2. Після цього генеруються перші коефіцієнти поліномів, а потім на їх основі та враховуючи задані числа і ключ шифрування обчислюються другі коефіцієнти поліномів. Таким чином кожне число, що бажає зашифрувати користувач у зашифрованому вигляді є поліномом першого порядку з двома коефіцієнтами та одним невідомим – *x,* яке виступає в якості ключа шифрування.

3. Зашифровані числа, тобто – поліноми передаються обчислювачу, який виконує необхідні математичні операції над ними. Внаслідок цих операцій обчислювач отримує результат у вигляді поліному, який він повертає користувачеві.

4. Користувач підставляє свій ключ замість невідомого в отриманий поліном і таким чином розшифровує результат виконаних математичних операцій над заданими числами в зашифрованому вигляді.

Рис. 1. Алгоритм шифрування, обчислення та розшифрування числових даних

У приведеному нижче прикладі виконаємо чотири основні математичні операції: множення, ділення, додавання та віднімання над числами використовуючи гомоморфне шифрування, для підтвердження повної гомоморфності цього методу.

Припустимо, що у нас є 5 чисел, над якими необхідно виконати вище зазначені чотири основні математичні операції:

$y_1 = -4{,}8$; $y_2 = 6{,}7$; $y_3 = 11{,}46$; $y_4 = 3{,}62$; $y_5 = 8{,}22$

Але ці математичні операції буде виконувати обчислювач, і йому не повинно бути відомо значення цих чисел, тому їх потрібно гомоморфно зашифрувати. Для цього ми придумуємо ключ шифрування, за допомогою якого будуть зашифровані числа та розшифрований результат виконання операцій. Цей ключ повинен знати лише власник цих чисел. Наприклад, візьмемо ключ шифрування: $x = 3{,}14$. Зашифруємо наші числа, а для цього необхідно згенерувати перший коефіцієнт поліному, а потім за його допомогою розрахувати другий коефіцієнт поліному. Наприклад, перший коефіцієнт поліному: $a_1 = 2{,}74$, тоді за нижче зазначеною формулою (1) розрахуємо другий коефіцієнт поліному:

$$b_i = y_i - a_i \times x, \quad (1)$$

де b_i – другий коефіцієнт поліному;
y_i – число, що зашифровується;
a_i – перший коефіцієнт поліному;
x – ключ шифрування;
i – індекс.

$$b_1 = y_1 - a_1 \times x = -4{,}8 - 2{,}74 \times 3{,}14 \approx 13{,}4$$

Таким же чином згенеруємо та розрахуємо коефіцієнти поліномів для всіх чисел, та зведемо їх у таблицю (табл. 1).

Таблиця 1

Числа та відповідні коефіцієнти поліномів

Число	$y_1 = -4{,}8$	$y_2 = 6{,}7$	$y_3 = 11{,}46$	$y_4 = 3{,}62$	$y_5 = 8{,}22$
1-й коефіцієнт	$a_1 = 2{,}74$	$a_2 = -3{,}8$	$a_3 = 0{,}65$	$a_4 = -4{,}07$	$a_5 = -1{,}35$
2-й коефіцієнт	$b_1 = -13{,}4$	$b_2 = 18{,}63$	$b_3 = 9{,}42$	$b_4 = 16{,}4$	$b_5 = 12{,}46$

Зашифроване число буде мати вигляд полінома першого порядку: $a_i \times x + b_i$.

У ролі прикладу, нам необхідно отримати результат виконання наступних математичних операцій над числами:

$$\frac{y_1 * y_2 + y_3}{y_4 - y_5}$$

Для цього, передаємо обчислювачу зашифровані числа у вигляді поліномів першого порядку:

$$\frac{(a_1 * x + b_1) * (a_2 * x + b_2) + (a_3 * x + b_3)}{(a_4 * x + b_4) - (a_5 * x + b_5)} \quad (2)$$

Після чого обчислювач розкриває дужки, виконує необхідні математичні операції і повертає результат обчислення (3).

$$\frac{(2.74x + (-13.4)) * (-3.8x + 18.63) + (0.65x + 9.42)}{(-4.07x + 16.4) - (-1.35x + 12.46)} = \frac{-10.41x^2 + 102.62x - 240.22}{-2.72x + 3.94} = \quad (3)$$

$$= 3.83x - 32.18 + \frac{-113.43}{-2.72x + 3.94}$$

У повернутий результат обчислення (3), користувач підставляє ключ шифрування $\boldsymbol{x}$ і таким чином розшифровує результат (4):

$$3.83 * 3.14 - 32.18 + \frac{-113.43}{-2.72 * 3.14 + 3.94} \approx 4.5 \quad (4)$$

Перевіримо правильність отриманого результату над зашифрованими числами (5):

$$\frac{y_1 * y_2 + y_3}{y_4 - y_5} = \frac{-4.8 * 6.7 + 11.46}{3.62 - 8.22} = 4.5 \quad (5)$$

Оскільки результати (4) та (5) співпадають, то можна зробити висновок, що обчислення було виконано правильно, а також це є доказом того, що шифрування чисел методом їх заміни на поліном першого порядку є повністю гомоморфним методом шифрування.

З'ясуємо тепер на скільки буде відхилятись значення результату математичної операції (2) при відхиленні ключа шифрування x від свого значення, і чи виникає при цьому залежність. Для цього підставимо в результат математичної операції (3) ключі з деякими відхиленнями від істинного значення і отримані результати зведемо у таблицю (табл. 2).

Таблиця 2

Відхилення ключів шифрування та результату виконання математичної операції

№	**Істинне значення ключа: 3.14**			**Істинне значення результату: 4.5**		
	Ключ	**Відхилення ключа**	**Відхилення ключа, %**	**Результат**	**Відхилення результату**	**Відхилення результату, %**
1	3,142	0,002	0,064	4,48	0,02	0,44
2	3,136	0,004	0,127	4,54	0,04	0,89
3	3,133	0,007	0,223	4,58	0,08	1,78
4	3,149	0,009	0,287	4,40	0,1	2,22
5	3,10	0,04	1,27	4,94	0,44	9,8
6	3,2	0,06	1,91	3,89	0,61	13,6
7	3,06	0,08	2,55	5,42	0,92	20,4
8	3,24	0,1	3,18	3,51	0,99	22,0
9	3	0,14	4,46	6,19	1,69	37,6
10	3,44	0,3	9,56	1,94	2,56	56,9
11	2,59	0,55	17,5	14,3	9,8	218
12	4	0,86	27,4	– 0,52	5,02	112
13	1	2,14	68,2	– 121,3	125,8	2796
14	7	3,86	122,9	2,14	2,36	52,4
15	– 4	7,14	227,4	– 55,2	59,7	1327
16	13	9,86	314	21,2	16,7	371
17	– 20	23,14	737	– 110,7	115,2	2560
18	35	31,86	1015	103,1	98,6	2191
19	– 60	63,14	2011	– 262,7	267,2	5938
20	97	93,86	2989	339,8	335,3	7451
21	– 189	192,14	6119	– 756,3	759,4	16876
22	378	374,86	11938	1416	1413	31400
23	– 624	627,14	19973	– 2422	2425	53889
24	999	995,86	31715	3794	3791	84244

На основі отриманих даних (табл. 2) побудуємо графік (рис. 2), на якому зображена залежність відхилення результату та відхилення ключа шифрування від своїх істинних значень.

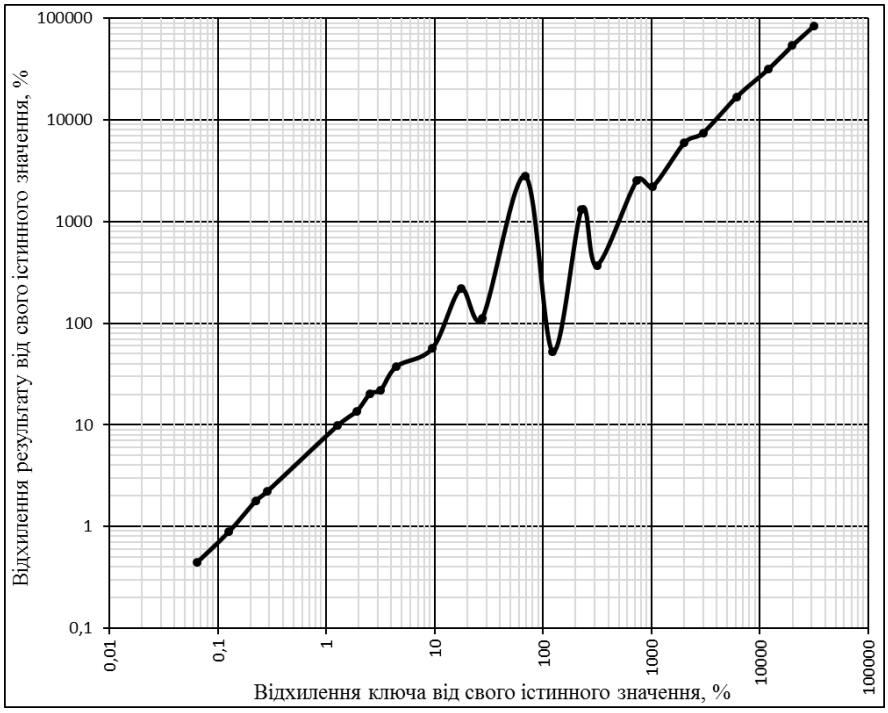

Рис. 2. Графік залежності відхилення результату та відхилення ключа шифрування

З таблиці (табл. 2) та графіку (рис. 2) видно, що залежності відхилення результату та відхилення ключа шифрування немає, проте в більшості випадків відхилення результату приблизно в 5–10 разів більше, ніж відхилення ключа шифрування. Підібрати ключ шифрування є майже неможливою задачею, оскільки він може приймати будь-яке числове значення.

Гомоморфне шифрування даних на основі методу заміни числа, що підлягає шифруванню, на поліном першого порядку – є достатньо простим у реалізації та використанні методом захисту та обробки зашифрованої інформації. Над зашифрованими даними можливо виконувати чотири найпростіші математичні дії, на основі яких можна побудувати математичні операції будь-якої складності. При використанні цього методу зашифровані дані надійно захищені, бо ключ шифрування може приймати будь-яке числове значення та відомий тільки власнику цих даних і передавати ключ третій стороні немає необхідності. Подальший розвиток та застосування гомоморфної криптографії буде активно направлено на зменшення трудомісткості та складності шифрування та розшифрування даних з метою його повноцінного використання на хмарних сховищах.

ЛІТЕРАТУРА

1. Schneier on Security [Електронний ресурс]. – Режим доступу : https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html.
2. Вікіпедія [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/.

Ступень П. В., Соколов С. А., Золкина О. Ю.,
Одесский национальный политехнический университет, г. Одесса, Украина

Применение гомоморфного шифрования для защиты числовых данных в облачных хранилищах

Облачные хранилища и облачные сервисы, позволяющие выполнять различные операции над данными, открыли много возможностей для пользователей. Трудоемкие и сложные вычисления, требующие серьезных программных и аппаратных ресурсов, стали доступными для каждого, в любой части земного шара, нужен только доступ в Интернет. Однако существует и существенный недостаток – незащищенность данных, которые хранятся и вычисляются в облачных сервисах. Традиционные методы шифрования не позволяют обрабатывать данные в зашифрованном виде, поэтому или сообщать ключ шифрования облачным сервисам, или хранить данные в незашифрованном виде. В обоих случаях нет гарантии, что ваши данные надёжно защищены от несанкционированного доступа. Для решения этой проблемы существует гомоморфное шифрование данных, характерной особенностью которого является возможность выполнять любые математические операции над зашифрованными данными.

Ключевые слова: *облачное хранилище; гомоморфное шифрование; полином первого порядка; ключ шифрования.*

Stupen P. V., Sokolov S. O., Zolkina O. Y.,
Odessa National Polytechnic University, Odessa, Ukraine

Application of homomorphic encryption to protect the numerical data in cloud storages

Cloud storages and cloud services that give an ability to perform various operations on the data have opened a lot of opportunities for users. Time-consuming and complex calculations that require serious hardware and software resources made available to everyone, anywhere in the world, you only need an access to the Internet. However, there is a significant disadvantage – no protection of data stored and calculated in the cloud services. Traditional methods of the encryption do not allow to process the data in encrypted form. To solve this problem, there is a homomorphic encryption, a characteristic feature of which, is the ability to perform any mathematical operations on encrypted data.

The purpose is the analysis of the possibility to apply the homomorphic encryption to process numerical data on cloud storages. On 25th of June in 2009 Craig Gentry for the first time proposed model of fully homomorphic encryption. In his conclusion, this encryption method does not currently applicable in practice, since it requires enormous computing resources. Therefore, to increase the speed of data processing and application of homomorphic encryption in practice was used the method of substitution of number on a polynomial of the first order. This method allows to perform any mathematical operations on encrypted numerical data. And this numerical data is being safely protected. This method can be used to protect the numerical data that is a confidential or a trade secret, when it is going to be transferred to a third party for processing.

Key words: *cloud storages; homomorphic encryption; a polynomial of the first order; the encryption key.*

 Дата надходження статті до редколегії 18.11.2015