УДК 004.056.55

Роман Квєтний, Євгеній Титарчук (Вінниця, Україна)

Алгоритм частково гомоморфного шифрування на основі еліптичних кривих

Гомоморфне шифрування – це така форма шифрування, що дозволяє виконувати певні математичні дії з зашифрованими числами і отримувати зашифрований результат, що відповідає результату операцій, що були виконані з не зашифрованими числами.

Частково гомоморфними, на відміну від повністю гомоморфних, називають такі системи шифрування що здатні виконувати тільки одну з операцій – додавання або множення, над зашифрованим текстом. Хоча область застосування таких алгоритмів є невеликою (наприклад таємне голосування з різними вагами, деякі розподілені обчислення), проте значна перевага у продуктивності робить **актуальною** задачу створення стійких алгоритмів частково гомоморфного шифрування.

Постановка задачі. Необхідно створити систему шифрування що дасть змогу стороні А виконувати арифметичну дію додавання між зашифрованимистороною Б цілими числами, без їх розшифрування. Після отримання результату сторонаВповинна мати змогу розшифрувати результат, та отримати коректну суму.

Для **розв'язання задачі** використаємо систему Ель-Гамаля на еліптичних кривих. Відкритими параметрами системи є крива $E_p(a, b)$, її параметри, та точка-генератор, що належить цій кривій – G. Так як, дана система працює з точками, необхідно перевести кожне числоA, яке буде зашифровано, у область точок еліптичної кривої від 0 до максимального числаN_{max}, що можна отримати після виконання операції додавання. Таким чином перші N_{max} точок еліптичної кривої будуть відомі.

$$N \to N \cdot G = P_N$$

Нехай сторона Б хоче додати числа a та b, еквівалентами яких є точки на еліптичній кривій P_aта P_b. Для цього В генерує закритий ключ n та відкритий $P_n = nG$.

Сторона Б використовує публічний ключ P_nта обирає ціле число k (сеансовий ключ). Після цього шифрує кожне з чисел у вигляді пари точок:

$$G_{P_N} = (kG, P_N + kP_n)$$

Для додавання, сторона А, додає другі з точок у області еліптичної кривої $E_p(a, b)$:

$$G_{P_a} + G_{P_b} = (kG, P_a + kP_n + P_b + kP_n)$$

Результат додавання, та кількість точок M, що додавалась передається стороні В.

Після чого для розшифрування результату сторона В перемножує першу з точок результату на свій закритий ключ n та віднімає добуток від другої точки отриманого результату стільки раз, скільки операцій додавання виконувала сторона А, тобто Mраз.

$$S = P_a + kP_n + P_b + kP_n - kGn - kGn =$$
$$= P_a + P_b + knG + knG - knG - knG = P_a + P_b$$

Результат додавання Sставиться у відповідність цілому числу за таблицею, що була згенерована при відображенні чисел у точки еліптичної кривої.

Висновки.Запропонованочастково гомоморфний алгоритм шифрування з гомоморфністю по операції додавання на основі еліптичних кривих, що дозволяє зашифровувати, додавати, та розшифровувати числа різним сторонам процесу.

Література.

1. Титарчук Є.О. Захист даних в хмарних технологіях обчислень [Електронний ресурс]: XLII регіональна науково-технічна конференція м. Вінниці та області / Титарчук Є.О., Квєтний Р.Н. // ВНТУ. – 2014. – 1 с. – Режим доступу: www.conf.vntu.edu.ua/allvntu/2014/inaeksu/txt/Tytarchuk.pdf. – Назва з екрана.
2. Титарчук Є.О. Захист даних в хмарних технологіях комп'ютерних обчислень / Квєтний Р.Н., Титарчук Є.О. // Придніпровський науковий вісник. – 2014. – №5. – с. 77-82.
3. О.Н. Жданов.Методы и средствакриптографическойзащитыинформации / О.Н. Жданов. В.В. Золотарев // Красноярск – 2007. – с. 167