УДК 004.056.55

Р. Н. Квєтний, Є. О. Титарчук

АНАЛІЗ КРИПТОСТІЙКОСТІ ЧАСТКОВО ГОМОМОРФНОГО АЛГОРИТМУ ШИФРУВАННЯ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Вінницький національний технічний університет, м. Вінниця

Анотація. В роботі проведено аналіз криптографічної стійкості частково гомоморфного відносно операції додавання алгоритму шифрування на основі еліптичних кривих. Показано складність вирішення задачі дискретного логарифмування на еліптичній кривій при використанні ρ-методу Поларда. Наведено математичну модель, що визначає криптографічну стійкість базового асиметричного алгоритму шифрування на еліптичних кривих. Визначено математичну модель, що демонструє спрощення задачі дискретного логарифмування на еліптичній кривій при збільшенні кількості елементів гомоморфного додавання, відносно базового алгоритму асиметричного шифрування. Визначено криптографічну стійкість алгоритму частково гомоморфного шифрування на основі еліптичних кривих.

Ключові слова: Частково гомоморфне шифрування, Еліптичні криві, Криптостійкість, Алгоритм Поларда.

Аннотация. В роботе проведено анализ криптографической стойкости частично гомоморфного относительно операции суммирования алгоритма шифрования на основе эллиптических кривых. Показана сложность решения задачи дискретного логарифмирования на эллиптической кривой с использованием ρ-метода Поларда. Приведена математическая модель, которая определяет криптографическую стойкость базового асиметричного шифрования на эллиптических кривых. Определена математическая модель, которая демонстрирует упрощение задачи дискретного логарифмирования на эллиптической кривой при увеличении количества элементов гомоморфного суммирования относительно базового алгоритма ассиметрического шифрования. Определена криптографическая стойкость алгоритма частично гомоморфного шифрования на эллиптических кривых.

Ключевые слова: Частично гомоморфное шифрование, Гибридное шифрование, Алгоритм Поларда.

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: Partially homomorphic encryption, Elliptic curves, Cryptographically strong, Pollard's algorithm.

Вступ

Зазвичай, шифрування використовується як засіб для збереження даних конфіденційними та цілісними під час їх передачі іншим сторонам або зберігання. Практична більшість найбільш розповсюджених зараз схем шифрування використовуються у контексті операцій зчитування та запису інформації. Наприклад, такі алгоритми шифрування, як RSA, а також шифрування з використанням алгоритму обміну ключами Diffie-Hellman, створені для того, щоб дозволити сторонам шифрувати данні при потребі запису або передачі повідомлень, та дешифрувати їх при зчитуванні чи отриманні. Їх достатньо для простого застосування, такого як передача чи зберігання інформації, але більш значні переваги може надати можливість модифікації інформації без її розшифрування. Схеми шифрування, що дозволяють виконувати арифметичні операції з за-шифрованими текстами без їх розшифрування називаються гомоморфними. При цьому, отриманий результат після його дешифрування відповідає числу, що можна б було отримати при виконанні тих самих арифметичних дій над відкритими числами. Працююча схема гомоморфно-го шифрування отримала б широке застосування у хмарних технологіях комп'ютерних обчислень та зберігання інформації. Однак істотною проблемою існуючих схем гомоморфного шифрування є їх крайнє низька продуктивність. [1-3]

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 використання таких алгоритмів є відносно невеликою, їх швидкість значно вище ніж у повністю гомоморфних. Одним із можливих застосувань частково гомоморфних по операції додавання алгоритмів є електронні системи голосування з різними вага-ми де вони використовуються для створення протоколів анонімізації користувачів. Проте специфіка електронного голосування – значні напливи користувачів у короткі проміжки часу, вима-гають від алгоритму значної швидкодії. Тому є актуальною задача створення нового алгоритму частково гомоморфного шифрування, швидшого за аналогічні.

Частково гомоморфний алгоритм на основі еліптичних кривих має більшу швидкодію ніж добре відомий алгоритм Пайє. Алгоритм на основі еліптичних кривих є модифікацією звичайного асиметричного алгоритму Діффі-Геллмана на еліптичних кривих (ECDH), криптостійкість якого базується на складності вирішення задачі дискретного логарифмування в колі точок еліптичної кривої. [1]

Так як, результат гомоморфного додавання зашифрованих чисел містить додаткову інформацію про схему шифрування (сеансові ключі, суми зашифрованих точок еліптичної кривої) необхідно визначити

© Р. Н. Квєтний, Є. О. Титарчук, 2017

чи є алгоритм частково гомоморфного шифрування криптостійким. Тому, метою роботи є аналіз криптографічної стійкості частково гомоморфного алгоритму шифрування на основі еліптичних кривих.

Актуальність

На сьогоднішній день створено багато протоколів захисту інформацією користувачів, а також програм, що їх використовують. Проте дані протоколи використовуються лише у контексті операцій зчитування та запису інформації. Застосування гомоморфних алгоритмів шифрування дає можливість виконувати алгоритмічні операції з зашифрованим текстом без його попереднього дешифрування.

Одним із таких алгоритмів є частково гомоморфний алгоритм побудований на основі еліптичних кривих. Проте зміни що були внесені в оригінальний алгоритм асиметричного

шифрування могли зменшити його криптографічну стійкість. Тому є актуальною задача визначення криптографічної стійкості алгоритму гомоморфного шифрування на еліптичних кривих.

Мета

Метою роботи є аналіз криптографічної стійкості частково гомоморфного алгоритму шифрування на основі еліптичних кривих

Задачі

1. Визначити математичну модель криптографічної стійкості алгоритму асиметричного шифрування на еліптичних кривих.
2. Визначити вплив гомоморфного додавання, реалізованого в частково гомоморфному алгоритмі на результуючу криптографічну стійкість.

Розв'язання задач

Розглянемо кінцеве поле F_p, де p – просте число.

Задачею дискретного логарифмування (DLP) по основі $q \in F_p^*$ є знаходження для данного $p \in F_p^*$ такого цілого числа x, такого що $q^x = p$.

Задача дискретного логарифмування на еліптичній кривій (elliptic curve discrete logarithm problem, ECDLP) E(F_p) з основою $q \in E(F_p)$ полягає у знаходженні для даного $p \in E(F_p)$ такого цілого числа x, що $xq = p$ (якщо воно існує).

Найкращими з відомих на сьогоднішній день алгоритмів рішення ECDLP є метод «Великих та малих кроків» а також ρ-метод Поларда. Перевагою останнього є менший обсяг використання пам'яті та можливість розподілених обчислень. Алгоритм Поларда має складність $O(\sqrt{p})$ операцій складання в групі $\langle E(F_p, +)\rangle$. [3, 5, 7]

Визначимо оцінку складності алгоритму Поларда:

Нехай n, r – натуральні числа, $r^2 \geq n$ Покажемо, що для будь-якого цілого x можна вказати цілі числа s і t такі, що:

$$x \equiv sr + t(\mathrm{mod}\, n);\ 0 \leq s < r, 0 \leq t \leq\ r \tag{1}$$

Нехай, $0 \leq x < r$. Тоді $s = \frac{x}{r}\ ,\ t = x - sr$. Звідки можна побачити, що:

$$0 \leq s \leq \frac{x}{r} < \frac{n}{r} \leq r. \tag{2}$$

З іншого боку:

$$0 \leq s \leq \frac{x}{r} < s + 1 \tag{3}$$

Тому $sr \leq x < sr + r$, або $0 \leq x - sr = t < r$.

Теорема: Нехай $\langle E(F_p, +)\rangle$ – кінцева група точок еліптичної кривої над кінцевим полем F_p. Q, P- елементи цієї групи, n – порядок елемента P,

$$kP = Q \tag{4}$$

Тоді число k можна знайти виконавши не більше ніж $2\left(\sqrt{n} + \log_2 n\right) - 1$ операцій додавання в групі $\langle E(F_p, +)\rangle$. [3-5]

Доведення: Візьмемо $r = \sqrt{n} + 1$. Розглянемо ряди:

$$0 \cdot P = O;\ 1 \cdot P\ =\ G, 2 \cdot P, \dots, (r-1) \cdot P \tag{5}$$

та

$$Q, Q + \big(1 \cdot (-r)\big) \cdot P, Q \; + \; \big(2 \cdot (-r)\big) \cdot P, \dots, Q + ((r-1) \cdot (-r)) \cdot P \tag{6}$$

Можна помітити, що якщо рівняння $kG = Q$ (4) можна вирішити відносно k, то враховуючи, що $r^2 \geq n^2$, представимо k у вигляді:

$$k \equiv t + sr \pmod{n}, 0 \leq t < r. \tag{7}$$

де, n – порядок групи, отримаємо – $kP = (sr + t)P = Q$, якщо:

$$tP = Q + (-sr)P \tag{8}$$

тобто, коли знайдеться елемент другого ряду, що співпадає з деяким елементом першого ряду. [5]

При обчисленні елементів першого ряду, необхідно виконати не більше $r - 2$ складань в групі еліптичної кривої. Для обчислення $(-rG) = (n - r)G$ необхідно виконати не більше $2\log_2 n$ множень. Для обчислень елементів другого ряду необхідно виконати не більше $r - 1$ операцій додавання.

Таким чином, загальна кількість групових операції для знаходження натурального числа k не перевищує: [3-6]

$$2r - 3 + 2\log_2 n \leq 2\big(\sqrt{n} + \log_2 n\big) - 1. \tag{9}$$

Розгялнемо математичну модель алгоритму частково гомоморфного шифрування на еліптичних кривих:

$$\sum_{i=0}^{m} A_i' = (\sum_{i=0}^{m} k_i G \,, \sum_{i=0}^{m} (A_i + k_i P)) \tag{10}$$

Звідки можна виділити суму сеансових ключів шифрування, криптостійкіть якої визначає криптостійкість алгоритму шифрування:

$$\sum_{i=0}^{m} k_i G = Q \tag{11}$$

де, m – кількість доданків.

Так як, сеансові ключі алгоритму статистично непов'язані з приватним ключем шифрування, перехоплення усіх доданків не надасть додаткової переваги при знаходженні множників.

Можна побачити, що кількість операцій які необхідно виконати у найгіршому випадку скорочується на m (кількість виконаних операцій додавання):

$$r \leq \sqrt{n} + 1 - m \tag{12}$$

де, n – порядок групи точок еліптичної кривої ($n \gg m$)

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. E. Titarchuk. Usage of the hybrid encryption in a cloud instant messages exchange system / R. Kvyetnyy, O. Romanyuk, E. Titarchuk, K. Gromaszek, N. Mussabekov // Photonics Applica-tions in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2016, 100314S, September 28, 2016

2. Recommended elliptic curves for federal government use / National Institute of Standards and Technology // Maryland, U.S.A., – July 1999. – p. 8

3. Liam Morris. Analysis of Partially and Fully Homomorphic Encryption / Liam Morris // Rochester Institute of Technology, New York – 2013. – p. 5

4. S. D. Galbraith, P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem / Steven D. Galbraith, Pierrick Gaudry, Codes Cryptography – 2015

5. Лёвин В. Ю., Носов В. А. Анализ повышения криптографической сложности систем при переходе на эллиптические кривые // Интеллектуальные системы. Теория и приложения, 2014, № 2, ISSN 2075-9460. — 2008. — Т. 12, № 1-4. — С. 253–270.

6. Крендалл Р., Померанс К. Простые числа: Криптографические и вычислительные аспекты. Пер. с англ. / Под ред. В. Н. Чубарикова. – М.: УРСС: Книжный дом «Либроком», 2011. – 664 с.

7. R. P. Gallant. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphism / R. P. Gallant, R. J. Lambert, S. Vanstone // University of Waterloo, Canada – 2001.

Стаття надійшла: 25.04.2017.

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.

ДО ВІДОМА АВТОРІВ

Найновіші правила оформлення і подання статей знаходяться на сайті журналу **http://itce.vntu.edu.ua/index.php/itce/about/submissions#onlineSubmissions**