УДК 004.056.55

Р. Н. Квєтний
Є. О. Титарчук

АНАЛІЗ КРИПТОСТІЙКОСТІ ЧАСТКОВО ГОМОМОРФНОГО АЛГОРИТМУ ШИФРУВАННЯ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Вінницький національний технічний університет

Анотація

В роботі проведено аналіз криптографічної стійкості частково гомоморфного відносно операції додавання алгоритму шифрування на основі еліптичних кривих. Математична модель, показана у статті, демонструє спрощення задачі дискретного логарифмування на еліптичній кривій при збільшенні кількості елементів гомоморфного додавання.

Ключові слова: частково гомоморфне шифрування, еліптичні криві, криптостійкість, алгоритм Полларда.

Abstract

The problem this article deals with is cryptographic analysis of partially homomorphic encryption scheme by addition based on elliptic curves. Shown in article mathematic model illustrate simplifying of discrete logarithm task with growing of count of members that take a part in homomorphic addition.

Keywords: partially homomorphic encryption, elliptic curves, cryptographically strong, Pollard's algorithm.

Вступ

Частково гомоморфний алгоритм на основі еліптичних кривих має більшу швидкодію ніж добре відомий алгоритм Пайє. Такі частково гомоморфні відносно додавання алгоритми шифрування знаходять застосування у спеціалізованих системах розподілених/хмарних обчислень та системах деперсоналізації користувачів. 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.

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

Результати дослідження

Криптостійкість алгоритму базується на важкості вирішення задачі дискретного логарифмування в колі еліптичної кривої (ECDLP) – знаходженні такого числа k для заданих точок еліптичної кривої $E(F_p) – G$ та Q, що $k \cdot G = Q$, де $G \in E(F_p)$, $Q \in E(F_p)$. [1]

Для вирішення цієї задачі скористаємося методом Поларда [2]. Розглянемо ряди:

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

та

$$Q, Q + \big(1 \cdot (-r)\big) \cdot G, Q\ +\ \big(2 \cdot (-r)\big) \cdot G, \dots, Q + ((r-1) \cdot (-r)) \cdot G$$

Якщо рівняння $kG = Q$ можна вирішити відносно k то представивши k у вигляді:

$$k \equiv (t + sr) \bmod n, 0 \le t \le r$$

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

$$tG = Q + (-sr)G$$

тобто, коли знайдеться елемент другого ряду, що співпадає з деяким елементом першого ряду. [1]

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: [1]

$$r \leq \sqrt{n}+1$$

В процесі гомоморфного шифрування маємо:

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

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

де, m – кількість доданків. Звідки можна побачити що сумма у лівій частині відповідає сумі рядів (1) а отже загальна кількість операцій:

$$r \leq \frac{\sqrt{n}+1}{m}$$

Висновки

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

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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.

2. 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.

Квєтний Роман Наумович — д-р. техн. наук, професор, завідувач кафедра AIBT, 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

Науковий керівник: ***Квєтний Роман Наумович*** — д-р. техн. наук, професор, завідувач кафедра AIBT, Вінницький національний технічний університет, м. Вінниця

Kvyetnyy Roman N. — Dr. Sc. (Eng.), Professor, Head of the Chair of Automation and Information Measuring Devices, Vinnytsia National Technical University, Vinnytsia, email : rkvetny@mail.ru

Titarchuk Eugene A. — postgraduate student, Chair of Automation and Information Measuring Devices, Vinnytsia National Technical University, Vinnytsia, email: etitarchuk@gmail.com

Supervisor: ***Kvyetnyy Roman N.*** — Dr. Sc. (Eng.), Professor, Head of the Chair of Automation and Information Measuring Devices, Vinnytsia National Technical University, Vinnytsia