УДК 004.056.5

Р. М. Пархоменко

АНАЛІЗ МОЖЛИВОСТІ ПІДВИШЕННЯ КРИПТОСТІЙКОСТІ АЛГОРИТМУ ШИФРУВАННЯ ЕЛЬ-ГАМАЛЯ

Вінницький національний технічний університет

Анотація

У даній статті запропоновано модифікації алгоритму шифрування Ель-Гамаля на основі матричних груп, виявлено недоліки даної модифікації та вроваджено її в підсистему шифрування.

Ключові слова: Ель-Гамаль, матричні групи, дискретне логарифмування, криптостійкість.

Abstract

This article proposes modifications of the El Gamal encryption algorithm based on matrix groups, identifies the shortcomings of this modification and embedded it in the encryption subsystem.

Keywords: El Gamal, matrix groups, discrete logarithm, cryptocurrency.

Вступ

Так як з кожним роком рівень розвитку сфери інформаційних технологій невпинно зростає, збільшується потужність комп'ютерних систем, то це дає можливість для підвищення швидкодії різного роду операцій, в тому числі й криптографічних. В цьому є безліч переваг: спрощення використання криптографічних засобів захисту інформації, збільшення швидкості передачі повідомлень та ін. Але це також дає зловмисникам більше можливостей для проведення різного роду атак та дешифрування перехоплених повідомлень та викрадених даних, отриманих в ході їх проведення. Цей факт змушує нас шукати нові алгоритми захисту цінної інформації та модифікації існуючих. Тому дослідження можливості підвищення стійкості та швидкодії алгоритмів ключового обміну інформації є досить актуальною задачею.

Результати дослідження

Схема Ель-Гамаля - асиметричний алгоритм шифрування, заснований на трудності обчислення дискретних логарифмів в кінцевому полі.

Розглядаючи проблему дескритного логарифмування можемо ввести поняття матричних груп в класичну схему Ель-Гамаля.

Застосування матричних груп в системі Ель-Гамаля обумовлено такими міркуваннями:

1). задача дискретного логарифмування є важко вирішуваною в

групах матриць;

2). матричні групи володіють багатою підгруповою структурою з огляду на те, що будь-яка кінцева група ізоморфна деякій підгрупі групи оборотних матриць.

Для розуміння даних концепцій модифікованого алгоритму покроково опишемо данну схему шифрування.

Алгоритм шифрування та розшифрування Ель-Гамаля на матричних групах складається з наступних кроків:

Генерація ключів:

Крок 1. Вибирається деяке велике просте число p і порядок групи n;

Крок 2. Вибирається елемент:

$$g \in GL_n(p, \mathbb{Z})$$ Формула 1

де $|g|$ - число великого порядку.

Крок 3. Вибирається деяке число α з проміжку $2 \leq a \leq |g| - 1$

Крок 4. Вираховується $y = g^a$.

Відкритим ключем шифрування буде ($GL_n(p,\mathbb{Z}), g, y$), а закритим a.

Алгоритм шифрування Ель-Гамаля на матричних групах:

Є деяке повідомлення в вигляді матриці $M \in GL_n(p,\mathbb{Z})$

Крок 1. Вибирається сеансовий ключ r з проміжку $2 \le a \le |g| - 1$.

Крок 2. Обчислюється

$$c = g^r$$ Формула 2

Крок 3. Обчислюється

$$b = M * y^r$$ Формула 3

Крок 4. Складається матриця $F_{n\times 2n}$, що є шифротекстом:

$$F = \begin{bmatrix} C_{11} \cdots & C_{1n} & b_{11} \cdots & b_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ C_{n1} \cdots & C_{nn} & b_{n1} \cdots & b_{nn} \end{bmatrix}$$ Формула 4

Алгоритм розшифрування Ель-Гамаля на матричних групах

Нехай є закритий ключ α і матриця:

$$F_{n\times 2n} = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{12n} \\ f_{21} & f_{22} & \cdots & f_{22n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & \cdots & f_{n2n} \end{bmatrix}$$ Формула5

Крок 1. Складаються матриці $C_{n\times n}$ і $b_{n\times n}$ з елементів матриці $F_{n\times 2n}$:

$$c = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{31} & f_{32} & \cdots & f_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & \cdots & f_{n2n} \end{bmatrix}$$ Формула 6

$$b = \begin{bmatrix} f_{1n+1} & f_{1n+2} & \cdots & f_{12n} \\ f_{2n+1} & f_{2n+2} & \cdots & f_{22n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{nn+1} & f_{nn+2} & \cdots & f_{n2n} \end{bmatrix}$$ Формула 7

Крок 2. Виходить вихідне повідомлення:

$$M' = b(c^a)^{-1}$$ Формула 8

Покажемо, що $M' = M$.

Так як $c = g^r$, $b = M * y^r$, то $M = \mathrm{b} * (\mathrm{c}^a)^{-1} = \mathrm{M} * g^{ar} * (g^{ar})^{-1} = M$.

Розглянемо на прикладі алгоритм шифрування і розшифрування Ель-Гамаля на матричних групах

Нехай n=2, p=61. Виберемо закритий ключ α = 37. Візьмемо в якості g_{2x2} матрицю:

$$g = \begin{pmatrix} 19 & 26 \\ 37 & 43 \end{pmatrix}$$

Тоді:

$$y_{2x2} = g^a = \begin{pmatrix} 20 & 14 \\ 34 & 47 \end{pmatrix}$$

Нехай повідомлення представлено у вигляді матриці:

$$M_{2\times2} = \begin{pmatrix} 57 & 37 \\ 4 & 28 \end{pmatrix}$$

Шифрування:

1). Вибираємо сеансовий ключ r = 29.

2). Обчислюємо c і b за формулами 2.6, 2.7 відповідно:

$$\mathrm{c} = \begin{pmatrix} 57 & 37 \\ 4 & 28 \end{pmatrix}$$

$$b = \begin{pmatrix} 50 & 40 \\ 17 & 51 \end{pmatrix}$$

3). Складаємо матрицю F:

$$F = \begin{pmatrix} 57 & 37 & 50 & 40 \\ 4 & 28 & 17 & 51 \end{pmatrix}$$

Дешифрування.

1). Складаємо матриці b_{2x2} і c_{2x2}з елементів матриці F_{2x2}

$$b = \begin{pmatrix} 50 & 40 \\ 17 & 51 \end{pmatrix}$$

$$\mathrm{c} = \begin{pmatrix} 57 & 37 \\ 4 & 28 \end{pmatrix}$$

2). Використовуючи секретний ключ, обчислюємо вихідне повідомлення:

$$M' = b(c^{37})^{-1} = \begin{pmatrix} 57 & 37 \\ 4 & 28 \end{pmatrix}$$

Класична реалізація схеми шифрування Ель-Гамаля спирається на використання мультиплікативних груп кінцевих полів простого порядку. Але розвиток технічних засобів зробило системи, що використовують традиційні ключі, більш уразливими. У зв'язку з цим особливо активно вивчаються способи, засновані на обчисленнях в спеціально підібраних групах. Та розроблено значну кількість методів які дозволяють обходити проблему дискретного логарифмування в мультиплікативних групах кінцевих полів простого порядку але всі ці методе не можуть бути перенесені на матричні групи описані вище.

Якщо ж спиратися на проблему дискретного логарифмування в матричних групах при побудові алгоритму шифрування , то в силу особливості групової операції (множення) при тій же довжині ключа, що і в кільці цілих чисел криптостійкість помітно підвищується.

Обчислювальна складність проблеми дискретного логарифмування порівнюється з запропонованою проблемою матричного дискретного логарифмування наступним чином:

Обчислювальна складність дискретного логарифмування $\mathrm{b} = \mathrm{a}^x \bmod \mathrm{p}$ може бути обрахована за наступною формулою:

$$T(a^x) = O(\log n) \qquad (2.9)$$

Де n - розмір відкритого повідомлення

Обчислювальна складність матричного дискретного логарифмування $B = \mathrm{A}^x \bmod \mathrm{p}$ може бути обрахована за наступною формулою:

$$T(A^x) = O(m^2 \log n)$$

Формула 9

Де n - розмір відкритого повідомлення, m - порядок матриці.

Якщо порівняти наведені вище формули, одразу видно, що математична складність алгоритму

який базується на проблемі матричного дискретного логарифмування бліша на m^2 .

Висновки

Розглянуто модифікацію алгоритму шифрування та розшифрування на основі класичної схеми Ель-Гамаля шляхом введення в нього поняття матричних груп. Дана модифікація дозволяє підвищити криптостійкість за рахунок того, що задача дискретного логарифмування є ще більш важко вирішуваною в групах матриць ніж при звичайному дискретному логарифмуванні. Ця особливість дає змогу зменшити довжину ключа без втрати криптостійкості. Але проведення обчислень над матрицями великих порядків суттєво зменшує швидкодію та продуктивність даного алгоритму.

Даний негативний момент змушує нас шукати методи підвищення швидкодії для описаного вище алгоритму, одним з яких може стати використання нейроних мереж.

.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ElGamal, T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms / T. ElGamal // IEEE Transactions on Information Theory. – 1985. – v. 31. – №4. – p.469–472

2. Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4):469–472, 1985.

3. Alan F. Karr, Xiaodong Lin, Ashish P. Sanil, and Jerome P. Reiter. Privacy-preserving analysis of vertically partitioned data using secure matrix products. Journal of Official Statistics, 25(1):125–138, 2009.

Пархоменко Руслан Михайлович – ст. гр. УБ-20м, Факультет менеджменту на інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: fm.yb16b.parhomenko@gmail.com.

Parkhomenko Ruslan M.. – Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: fm.yb16b.parhomenko@gmail.com.