Сложность алгоритмов криптографической системы Эль–Гамаля и их эффективность

Вьонг Х.Б.
vuonghuubao@live.com

Зюбин С.А., Национальный исследовательский Томский политехнический университет

В статье приводиться оценку вычислительной сложности алгоритмов схем шифрования, дешифрования, расшифрования криптографической системы Эль-Гамаля на основе мультипликативных групп, предложенных в работах [1]. Оценка сложности алгоритмов, в которых используется метод быстрого возведения в степени [2]. Результат вычисления эффективности криптографической схемы показывает криптографическую схему на основе поля целых гауссовых чисел, что является лучшим.

Шифрсистема Эль-Гамаля была предложена в 1985 году и является фактически одним из вариантов метода выработки открытых ключей Диффи-Хеллмана. Криптографическая стойкость данной системы основана на сложности проблемы логарифмирования в мультипликативной группе конечного простого поля. Система Эль-Гамаля может быть обобщена для применения в любой конечной циклической группе G. Криптографическая стойкость такой обобщенной схемы определяется сложностью задачи логарифмирования в группе *G*. В качестве группы *G*, в работе [1] предложили мультипликативной группу $\mathbb{Z}^*_p, \mathbb{Z}[i]/<\beta>, \mathbb{Z}_2[x]/<h(x)>, \mathbb{Z}_p[x]/<x^2>$. В пункте 1, 2, 3, 4 приведен вычисление сложность алгоритмов соответственно для классической системы Эль-Гамаля,системы Эль-Гамаля в мультипликативной группе гауссовых чисел $\mathbb{Z}[i]/<\beta>$, системы Эль-Гамаля на группе фактора кольца $\mathbb{Z}_p[x]/<x^2>$, системы Эль-Гамаля в группе фактора кольца $\mathbb{Z}_2[x]/<h(x)>$. В результате определения сложности определяется эффективности данных протоколов, сделано сравнение и выводы этой работы.

Классическая схема Эль-Гамаля

Классическая схема Эль-Гамаля установлено в кольце целых чисел $\mathbb{Z}_p = 0,1,2,3,\dots,p-1$ при p большое простое число.

Описание алгоритмов классической схемы Эль-Гамаля

Реализация данной схемы представляет при передаче информации между А и Б. Сначала установлен открытый и секретный ключ, А использует следующий алгоритм:

Алгоритм 1. (Генерация ключа)

1. Генерация большого случайного простого числа p и вычисление $p-1$.
2. Нахождение одного порождающего элемента α в циклической группе $\mathbb{Z}^*_p$. Тогда $\mathbb{Z}^*_p = 1,\alpha,\alpha^2,\alpha^3,\dots,\alpha^{p-1}$.

3. Выбор случайного числа $a, 1 \le a \le p-2$ и вычисление $\alpha^a (\bmod p)$. Открытый ключ является (p, α, α^a) и секретный ключа a.
Для шифрования сообщения $m, m \in \mathbb{Z}_p^*$, Б использует следующий алгоритм:
Алгоритм 2. (Схема шифрования)
1. Получение открытый ключа из А (p, α, α^a).
2. Выбор случайного целого числа $k, 2 \le k \le p-2$, вычисление $\gamma \equiv \alpha^k (\bmod p)$ и $\delta \equiv m(\alpha^a)^k (\bmod p)$.
3. Отправление секретного сообщения (γ, δ).
Для дешифрования А использует следующий алгоритм:
Алгоритм 3. (Схема дешифрования)
1. Получение секретного сообщения (γ, δ), отправленного Б.
2. Используя секретный ключа a для вычисления $m = \gamma^{-a} \cdot \delta (\bmod p)$.
Алгоритм 4. (Схема расшифрования - полный перебор нахождения секретного ключа число а)
1. Вычисление $\alpha^2 (\bmod p); ....; \alpha^{p-2} (\bmod p)$
2. Сравнение с $\alpha^a (\bmod p)$

Вычислительная сложность алгоритмов классической схемы Эль-Гамаля

Алгоритм 2: Шифрование
1. Сообщение m
2. Выбрать случайно число $k, 2 \le k \le p-2$
3. Вычислить

$\gamma \equiv \alpha^k (\bmod\ p)$

$\delta \equiv m \cdot (\alpha^a)^k (\bmod\ p)$

Вычислить γ: количество умножений меньше или равно

$$2(\log_2 p + 1) \le 2(\log_2 (p-2) + 1)$$

Каждый раз умножения число разряд двоичных чисел увеличится 2 раза, самое большое число имеет $\log_2(p-2) \cdot \frac{(p-2)}{2}$ разрядов. Сложность вычисления γ

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2$$

Дальше делить с остатком по модулю p: $\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2$

Общая сложность определения

$$\gamma\$:\$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2 + \left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2$$

Вычислить $(\alpha^a)^k (\bmod p)$ аналогично вычислению γ общая сложность:

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2$$

Умножение $m\cdot(\alpha^a)^k$ имеет сложность: $[\log_2(p-1)]^2$

Деление с остатком модулю р двоичных чисел с количеством разрядов $2\cdot\log_2(p-1)$

Тогда сложность вычисления δ :

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+$$

$$+[\log_2(p-1)]^2+[2\cdot\log_2(p-1)]^2$$

Общая сложность алгоритм:

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+$$

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+$$

$$+[\log_2(p-1)]^2+[2\cdot\log_2(p-1)]^2=$$

$$=2[2\cdot\log_2(p-2)+3]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+5[\log_2(p-1)]^2$$

Алгоритм 3: Расшифрование

1. Вычислить $\gamma^{p-1-a}(\bmod p)$

Вычитание $p-1-a$: $\log_2(p-1)$

Вычисление γ^{p-1-a} аналогично как определение γ в алгоритме 1:

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2$$

2. Вычислить $m\equiv\gamma^{-a}\delta(\bmod p)$

$$[\log_2(p-1)]^2+[2\cdot\log_2(p-1)]^2=5[\log_2(p-1)]^2$$

Общая сложность алгоритма 3:

$$2[\log_2(p-2)+1]\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+\left[\log_2(p-2)\cdot\frac{(p-2)}{2}\right]^2+5[\log_2(p-1)]^2$$

Алгоритм 4: Дешифрование

Вычислить $\alpha^2(\bmod p);....;\alpha^{p-2}(\bmod p)$ и сравнение с $\alpha^a(\bmod p)$

1. Сравнение α с $\alpha^a(\bmod p)$: $\log_2(p-1)$

2. Вычислить $\alpha^2(\bmod p)$ и сравнение с $\alpha^a(\bmod p)$:

$$2[\log_2(p-1)]^2+\log_2(p-1)$$

3. Вычислить $\alpha^3(\bmod p)$ и сравнение с $\alpha^a(\bmod p)$ (число разряд α^2 уже $2\log_2(p-1)$

$$2\left[\log_2(p-1)\right]\cdot\left[2\cdot\log_2(p-1)\right]+\log_2(p-1)=2\cdot 2\cdot\left[\log_2(p-1)\right]^2+\log_2(p-1)$$

Аналогично для α^{p-2}

$$2\left[\log_2(p-1)\right]\cdot\left[(p-3)\cdot\log_2(p-1)\right]+\log_2(p-1)=2\cdot(p-3)\cdot\left[\log_2(p-1)\right]^2+\log_2(p-1)$$

Общая сложность определения a полным перебором:

$$2\left[\log_2(p-1)\right]^2\cdot\left(1+2+3+\ldots+(p-3)\right)+(p-2)\cdot\log_2(p-1)$$

Системы Эль-Гамаля в мультипликативной группе гауссовых чисел $\mathbb{Z}[i]/<\beta>$

Данная схема Эль-Гамаля установлено в мультипликативной группе гауссовых чисел $\mathbb{Z}[i]/<\beta>$ при β - простое число вида $4k+3$.

Описание алгоритмов схемы Эль-Гамаля в мультипликативной группе гауссовых чисел

Реализация данной схемы представляет при передаче информации между А и Б. Сначала установлен открытый и секретный ключ, А использует следующий алгоритм:

Алгоритм 1. (Генерация ключа)

1. Генерация большого случайного простого числа $\beta = p$ вида $4k+3$ и вычисление p^2-1.

2. Нахождение одного порождающего элемента θ в циклической группе G_β^*. Тогда $G_\beta = (a+bi)\,|\,0\le a\le p-1, 0\le b\le p-1$ и $G_\beta^* = 1,\theta,\theta^2,\theta^3,\ldots,\theta^{p^2-1}$.

3. Выбор случайного числа $a, 1\le a\le p^2-2$ и вычисление $\theta^a(\mathrm{mod}\,\beta)$. Открытый ключ является (p,θ,θ^a) и секретный ключа a.

Для шифрования сообщения $m, m\in G_\beta^*$, Б использует следующий алгоритм:

Алгоритм 2. (Схема шифрования)

1. Получение открытый ключа из A (p,θ,θ^a).

2. Выбор случайного целого числа $k, 2\le k\le p^2-2$, вычисление $\gamma\equiv\theta^k(\mathrm{mod}\,\beta)$ и $\delta\equiv m(\theta^a)^k(\mathrm{mod}\,\beta)$.

3. Отправление секретного сообщения (γ,δ).

Для дешифрования A использует следующий алгоритм:

Алгоритм 3. (Схема дешифрования)

1. Получение секретного сообщения (γ,δ), отправленного Б.

2. Используя секретный ключа a для вычисления $m=\gamma^{-a}\cdot\delta(\mathrm{mod}\,\beta)$.

Алгоритм 4. (Схема расшифрования - полный перебор нахождения секретного ключа a)

1. Вычисление $\theta^2(\mathrm{mod}\,\beta);\ldots;\theta^{p^2-2}(\mathrm{mod}\,\beta)$

2. Сравнение с $\theta\alpha^a(\mathrm{mod}\,\beta)$

Вычислительная сложность алгоритмов Системы Эль-Гамаля в мультипликативной группе гауссовых чисел $\mathbb{Z}[i]/<\beta>$

Алгоритм 2:

1. Сообщение m
2. Выбрать случайно число k, $k \le p^2 - 1$
3. Вычислить $\gamma \equiv \theta^k (\bmod\, \beta)$

Вычисление θ^k количество <u>умножений</u> меньше $2(\log_2 k + 1) \le 2(\log_2 (p^2 - 1) + 1)$

Умножение $(a + bi)(c + di) = ac - db + (bc + ad)i$ требует 4 умножения и 2 сложения

Сложность вычисление с учетом повышения разрядов число после каждого умножения.

Деление требует 6 <u>умножений</u>, 2 сложения, 2 деления.

$$2\left[\log_2(p^2-1)\right]\left\{4\left[\left(\log_2 p\right)\frac{p}{2}\right]^2 + 2\log_2 p \cdot \frac{p}{2}\right\}$$

Общая сложность вычисление γ

$$2\left[\log_2(p^2-1)\right]\left\{4\left[\left(\log_2 p\right)\frac{p}{2}\right]^2 + 2\log_2 p \cdot \frac{p}{2}\right\} + 6(p\log_2 p)^2 + 2p\log_2 p + 2((p+1)\log_2 p)^2 = 4\log_2(p^2-1$$

4. Вычислить $\delta \equiv m\left(\theta^a\right)^k (\bmod\ \beta)$

Вычисление $\left(\theta^a\right)^k (\bmod\ \beta)$ аналогично вычисления γ:

$$4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2 + \log_2 p \cdot \frac{p}{2}\right\} + 14\left(\log_2 p\right)^2 + 2\log_2 p$$

Умножение $m\left(\theta^a\right)^k (\bmod\ \beta)$:

$$4(\log_2 p)^2 + 2\log_2 p + 6(\log_2 p)^2 + 2\log_2 p + 2(2\log_2 p)^2 = 18(\log_2 p)^2 + 4\log_2 p$$

Общая сложность алгоритма

$$4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2 + \log_2 p \cdot \frac{p}{2}\right\} + 6(p\log_2 p)^2 + 2p\log_2 p +$$

$$2((p+1)\log_2 p)^2 + 4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2 + \log_2 p \cdot \frac{p}{2}\right\} + 14\left(\log_2 p\right)^2$$

$$+2\log_2 p + 18(\log_2 p)^2 + 4\log_2 p =$$

$$= 8\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2 + \log_2 p \cdot \frac{p}{2}\right\} + 6(p\log_2 p)^2$$

$$+2p\log_2 p + 2((p+1)\log_2 p)^2 + 32\left(\log_2 p\right)^2 + 6\log_2 p$$

Алгоритм 3: <u>Расшифрование</u>

1. Вычислить $\gamma^{p-1-a} (\bmod \beta)$

Вычисление $p - 1 - a : \log_2 p$

Вычисление $\gamma^{p-1-a}(\bmod \beta)$ аналогично вычислению γ :

$$4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2+\log_2 p\cdot\frac{p}{2}\right\}+6(p\log_2 p)^2+2p\log_2 p+2((p+1)\log_2 p)^2$$

2. Вычислить $\gamma^{-a}\delta(\bmod \beta)$ аналогично вычислению δ :

$$4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2+\log_2 p\cdot\frac{p}{2}\right\}+14\left(\log_2 p\right)^2+2\log_2 p+18(\log_2 p)^2+4\log_2 p=$$

$$=4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2+\log_2 p\cdot\frac{p}{2}\right\}+32\left(\log_2 p\right)^2+6\log_2 p$$

Общая сложность алгоритма:

$$4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2+\log_2 p\cdot\frac{p}{2}\right\}+6(p\log_2 p)^2+$$

$$2p\log_2 p+2((p+1)\log_2 p)^2+4\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2+\log_2 p\cdot\frac{p}{2}\right\}+$$

$$32\left(\log_2 p\right)^2+6\log_2 p=8\log_2(p^2-1)\left\{2\left[\left(\log_2 p\right)\frac{p}{2}\right]^2+\log_2 p\cdot\frac{p}{2}\right\}+$$

$$6(p\log_2 p)^2+2p\log_2 p+2((p+1)\log_2 p)^2+32\left(\log_2 p\right)^2+6\log_2 p$$

Алгоритм 4: Дешифрование

Вычислить $\theta^2(\bmod \beta);....;\theta^{p-2}(\bmod \beta)$ и сравнение с $\theta^a(\bmod \beta)$

1. Сравнение θ с $\theta^a(\bmod \beta)$: $2\log_2 p$

2. Вычислить $\theta^2(\bmod \beta)$ и сравнение с $\theta^a(\bmod \beta)$:

Вычислить θ^2 : $4(\log_2 p)^2+2(\log_2 p)$

Деление по модулю β : $4(\log_2 p)^2+2log_2 p+2(2\log_2 p)^2$

Сравнение: $2\log_2 p$

Общая сложность:

$$4(\log_2 p)^2+2(\log_2 p)+4(\log_2 p)^2+2log_2 p+2(2\log_2 p)^2+2\log_2 p=16(\log_2 p)^2+8(\log_2 p)$$

3. Вычислить $\theta^3(\bmod \beta)$ и сравнение с $\theta^a(\bmod \beta)$(число разряд θ^2 уже $2\log_2 p$)

Вычислить θ^3: $4(\log_2 p)^2\cdot 2+2(\log_2 p)\cdot 2$

Деление по модулю β : $4(\log_2 p)^2\cdot 2+2log_2 p\cdot 2+2(\log_2 p\cdot 4)^2$

Сравнение: $2\log_2 p$

$$\Rightarrow 4(\log_2 p)^2\cdot 2+2(\log_2 p)\cdot 2+4(\log_2 p)^2\cdot 2+2log_2 p\cdot 2+2(\log_2 p\cdot 4)^2+2\log_2 p$$

Аналогично для θ^{p^2-1}

$$4(\log_2 p)^2 \cdot (p^2-2) + 2(\log_2 p) \cdot (p^2-2) + 4(\log_2 p)^2 \cdot (p^2-2) + 2log_2 p \cdot (p^2-2)$$

$$+2(\log_2 p \cdot (2p^2-4))^2 + 2\log_2 p$$

Общая сложность определения а полным перебором:

$$4(\log_2 p)^2 \cdot \left[1+2+3+...+(p^2-2)\right] + 2(\log_2 p) \cdot \left[1+2+3+...+(p^2-2)\right] +$$

$$+4(\log_2 p)^2 \cdot (p^2-2) + 2log_2 p \cdot \left[1+2+3+...+(p^2-2)\right] +$$

$$+2\left\{\log_2 p \cdot 2\left[1+2+3+...+(p^2-2)\right]\right\}^2 + 2(p^2-1)\log_2 p$$

Системы Эль-Гамаля в группе фактора кольца $U\left(\mathbb{Z}_p[x]/<x^2>\right)$

Данная схема Эль-Гамаля установлено в группе фактора кольца $U\left(\mathbb{Z}_p[x]/<x^2>\right)$ при p большое простое число.

Описание алгоритмов схемы Эль-Гамаля в группе фактора кольца $U\left(\mathbb{Z}_p[x]/<x^2>\right)$

Реализация данной схемы представляет при передаче информации между А и Б. Сначала установлен открытый и секретный ключ, А использует следующий алгоритм:

Алгоритм 1. (Генерация ключа)

1. Генерация большого случайного простого числа p и вычисление $p(p-1)$.
2. Нахождение одного порождающего элемента $\alpha(x)$ в циклической группе $U\left(\mathbb{Z}_p[x]/<x^2>\right)$. Тогда $U\left(\mathbb{Z}_p[x]/<x^2>\right) = 1, \alpha(x), \alpha(x)^2, \alpha(x)^3, \ldots, \alpha(x)^{p^2-p-1}$.
3. Выбор случайного числа $a, 2 \le a \le p^2-p-1$ и вычисление $\alpha(x)^a (\bmod x^2)$.

Открытый ключ является $(p, \alpha(x), \alpha(x)^a)$ и секретный ключа a .

Для шифрования сообщения $m, m \in U\left(\mathbb{Z}_p[x]/<x^2>\right)$, Б использует следующий алгоритм:

Алгоритм 2. (Схема шифрования)

1. Получение открытый ключа из А $(p, \alpha(x), \alpha(x)^a)$.
2. Выбор случайного целого числа $k, 2 \le k \le p^2-p-1$, вычисление $\gamma \equiv \alpha(x)^k (\bmod x^2)$ и $\delta \equiv m(\alpha(x)^a)^k (\bmod x^2)$.
3. Отправление секретного сообщения (γ, δ) .

Для <u>дешифрования</u> А использует следующий алгоритм:

Алгоритм 3. (Схема <u>дешифрования</u>)

1. Получение секретного сообщения (γ, δ) , отправленного Б.
2. Используя секретный ключа a для вычисления $m = \gamma^{-a} \cdot \delta (\bmod x^2)$.

Алгоритм 4. (Схема <u>расшифрования</u> - полный перебор нахождения секретного ключа а)

1. Вычисление $\alpha(x)^2 (\bmod\ x^2); ....; \alpha(x)^{p^2-p-1} (\bmod\ x^2)$

2. Сравнение с $\alpha(x)^a(\operatorname{mod} x^2)$

Вычислительная сложность алгоритмов системы Эль-Гамаля в группе фактора кольца $U\left(\mathbb{Z}_p[x]/<x^2>\right)$

Алгоритм 2:

1. Сообщение m
2. Выбрать случайно число k, $2 \le k \le p^2 - p - 1$
3. Вычислить $\gamma \equiv \alpha(x)^k(\operatorname{mod} x^2)$

$\alpha(x) = a + bx$

$\alpha(x)^k = b^k + kab^{k-1}x$

Определение $b^k, b \le p-1, k \le p^2 - p - 1$

Количество умножений меньше $2(\log_2 k + 1) \le 2[\log_2(p^2 - p - 1) + 1]$

Самое большое число разрядов при вычисление b^k : $\frac{(p^2 - p - 1)}{2}\log_2(p-1)$

Сложность все умножений $2\left[(\log_2(p^2 - p - 1) + 1\right]\left[\frac{p^2 - p - 1}{2}\log_2(p-1)\right]^2$

Деление по модулю p: $\left[\log_2(p-1)\cdot\frac{p^2 - p - 1}{2}\right]^2$

Умножение kab^{k-1} имеет 3 умножения:

Умножение $ab^{k-1} : [\log_2(p-1)]^2$

Умножение $k\cdot(ab^{k-1})$: $\log_2(p^2 - p - 1)\cdot 2\log_2 p$

Общая сложность вычисления γ

$$2\left[(\log_2(p^2 - p - 1) + 1\right]\left[\frac{p^2 - p - 1}{2}\log_2(p-1)\right]^2 + \left[\log_2(p-1)\cdot\frac{p^2 - p - 1}{2}\right]^2$$

$$+[\log_2(p-1)]^2 + \log_2(p^2 - p - 1)\cdot 2\log_2 p$$

4. Вычислить $\delta \equiv m(x)(\alpha(x)^a)^k(\operatorname{mod} x^2)$

Вычислить $(a(x)^a)^k(\operatorname{mod} x^2)$ аналогично вычислению γ

$$2\left[(\log_2(p^2 - p - 1) + 1\right]\left[\frac{p^2 - p - 1}{2}\log_2(p-1)\right]^2 + \left[\log_2(p-1)\cdot\frac{p^2 - p - 1}{2}\right]^2 +$$

$$[\log_2(p-1)]^2 + \log_2(p^2 - p - 1)\cdot 2\log_2 p$$

Умножение

$m(x)(\alpha(x)^a)^k(\operatorname{mod} x^2)$

$(ax + b)(cx + d) = bd + (ad + bc)x$

требует

3 умножения: $3(\log_2(p-1))^2$

1 сложение: $2\log_2(p-1)$

2 деления по модулю p: $2(2\log_2(p-1))^2$

Общая сложность:

$$4\Big[(\log_2(p^2-p-1)+1\Big]\left[\frac{p^2-p-1}{2}\log_2(p-1)\right]^2+2\left[\log_2(p-1)\cdot\frac{p^2-p-1}{2}\right]^2+$$

$$2[\log_2(p-1)]^2+2\log_2(p^2-p-1)\cdot 2\log_2(p-1)+3(\log_2(p-1))^2+2\log_2(p-1)+$$

$$+2(2\log_2(p-1))^2=\Big[4(\log_2(p^2-p-1)+6\Big]\left[\frac{p^2-p-1}{2}\log_2(p-1)\right]^2+$$

$$+13[\log_2(p-1)]^2+2\log_2(p^2-p-1)\cdot 2\log_2(p-1)+2\log_2(p-1)$$

Алгоритм 3: <u>Разшифрование</u>

1. Вычислить p^2-p-a: $(\log_2 p)^2+2(2\log_2 p)$

$$2\Big[(\log_2(p^2-p-1)+1\Big]\left[\frac{p^2-p-1}{2}\log_2(p-1)\right]^2+\left[\log_2(p-1)\cdot\frac{p^2-p-1}{2}\right]^2+[\log_2(p-1)]^2$$

$$+\log_2(p^2-p-1)\cdot 2\log_2 p$$

Вычислить γ^{p^2-p-a} аналогично вычислению γ

2. Вычислить $\gamma^{-a}\delta(\bmod x^2)$: $3(\log_2(p-1))^2+2\log_2(p-1)+2(2\log_2(p-1))^2$

Общая сложность:

$$2\Big[(\log_2(p^2-p-1)+1\Big]\left[\frac{p^2-p-1}{2}\log_2(p-1)\right]^2+\left[\log_2(p-1)\cdot\frac{p^2-p-1}{2}\right]^2+$$

$$+[\log_2(p-1)]^2+\log_2(p^2-p-1)\cdot 2\log_2 p+3(\log_2(p-1))^2+2\log_2(p-1)+$$

$$+2(2\log_2(p-1))^2=\Big[2(\log_2(p^2-p-1)+3\Big]\left[\frac{p^2-p-1}{2}\log_2(p-1)\right]^2+$$

$$+12[\log_2(p-1)]^2+\log_2(p^2-p-1)\cdot 2\log_2 p+2\log_2(p-1)$$

Алгоритм 4: <u>Дешифрование</u>

Сравнение $\alpha(x)$ с $\alpha(x)^a$: $2\log_2(p-1)$

Вычислить $\alpha(x)^2$ и сравнение с $\alpha(x)^a$: $\alpha(x)^2=b^2+2abx$

Аналогично вычислить $\alpha(x)^k$ и сравнение с $\alpha(x)^a$: $\alpha(x)^k=b^k+kab^{k-1}x$

Принимаем что вычислить kab^{k-1}, k имеет максимальное число разряд: $\log_2(p^2-p-1)$

Тогда вычислить $\alpha(x)^k$ и сравнение с $\alpha(x)^a$: $\alpha(x)^k=b^k+kab^{k-1}x$ имеет сложность:

$$\big[(k-1)\log_2(p-1)\big]\log_2(p-1)+(2\log_2(p-1))\log_2(p^2-p-1)+[\log_2(p-1)]^2$$

Общая сложность

$$\sum_{k=1}^{p^2-p-1}\big[(k-1)\log_2(p-1)\big]\log_2(p-1)+\Big[(2\log_2(p-1))\log_2(p^2-p-1)+[\log_2(p-1)]^2\Big]\cdot(p^2-p-1)$$

Схема Эль-Гамаля и Эффективность схемы Эль-Гамаля

Классическая схема Эль-Гамаля	$\dfrac{\left[\log_2(p-1)\right]^2\cdot(p-2)\cdot(p-3)+(p-2)\cdot\log_2(p-1)}{p-1}\sim p\log_2 p\cdot(\log_2 p+1)$
В мультипликативной группе гауссовых чисел $\square[i]/<\beta>$	$\dfrac{2\log_2 p\cdot(p^2-1)^2+2(\log_2 p)^2\cdot\left[(p^2-1)(p^2-2)+(p^2-1)^2(p^2-2)^2+2(p^2\cdot\right.}{p^2-1}$
в группе фактора кольца $U\left(\square_p[x]/<x^2\right.$	$\dfrac{(p^2-p-1)\cdot\left[(2\log_2(p-1))\log_2(p^2-p-1)+[\log_2(p-1)]^2+[\log_2(p-1)]^2\right.}{p^2-p-1}$

Заключение

И так, в работе определена эффективности каждой из перечисленных схем Эль-Гамаля в разных групп. По результатам вычисления показывается, что схема Эль-Гамаля дает наибольшую эффективность является схемой в поле гауссовых целых чисел $\square[i]/<\beta>$.

Список литературы:

1. Nasser El-Kassar, Ramzi A. Haraty // ElGamal Public-key Cryptosystem in Multiplicative Groups of quotient Rings of Polynomials of Finite Fields, Comput. Sci. Inf. Syst. 2(1): 63-77 (2005)
2. Панкратова И.А. Теорико-числовые методы криптографии. – М.: ТГУ, 2009. - 120 с.

Характеристика положения тела спортсмена в безопорном положении с точки зрения биомеханических основ

Разуванова А.В.
visann@tpu.ru

Национальный исследовательский Томский политехнический университи

Много ли людей способно оторваться от земли и зависнуть на пару секунд в воздухе? Естественно никто в мире не считал количество умеющих прыгать в высоту или процент людей способных совершать акробатические элементы в воздухе. Однако не сложно предположить, что прыгнуть в длину с места сможет приблизительно три четверти здорового населения, а скрутить сальто или зависнуть над планкой при прыжке «фосбери – флоп» сможет уже, куда меньшая часть населения. Безопорное положение – это вызов для нормальной физиологии человека,