

Сложность алгоритмов криптографической системы Эль-Гамала и их эффективность

Вьонг Х.Б.
vuonghuubao@live.com

Зюбин С.А., Национальный исследовательский Томский политехнический университет

В статье приводится оценка вычислительной сложности алгоритмов схем шифрования, дешифрования, расшифрования криптографической системы Эль-Гамала 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-Гамала 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-Гамала 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 мультипликативную группу \mathbb{Z}_p^* , $\mathbb{Z}_2[x]/\langle h(x) \rangle$, $\mathbb{Z}_p[x]/\langle x^2 \rangle$. В пункте 1, 2, 3, 4 приведен вычисление сложности алгоритмов соответственно для классической системы Эль-Гамала, системы Эль-Гамала в мультипликативной группе гауссовых чисел $\mathbb{Z}[i]/\langle \beta \rangle$, системы Эль-Гамала на группе фактора кольца $\mathbb{Z}_p[x]/\langle x^2 \rangle$, системы Эль-Гамала в группе фактора кольца $\mathbb{Z}_2[x]/\langle h(x) \rangle$. В результате определения сложности определяется эффективности данных протоколов, сделано сравнение и выводы этой работы.

Классическая схема Эль-Гамала

Классическая схема Эль-Гамала 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-Гамала

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 $a, 1 \leq a \leq p-2$ и вычисление $\alpha^a \pmod{p}$. 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 $A(p, \alpha, \alpha^a)$.
2. Выбор случайного целого числа $k, 2 \leq k \leq p-2$, вычисление $\gamma \equiv \alpha^k \pmod{p}$ и $\delta \equiv m(\alpha^a)^k \pmod{p}$.
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 $m = \gamma^{-a} \cdot \delta \pmod{p}$.

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

1. Вычисление $\alpha^2 \pmod{p}; \dots; \alpha^{p-2} \pmod{p}$
2. Сравнение с $\alpha^a \pmod{p}$

Вычислительная сложность алгоритмов классической схемы Эль-Гамала

Алгоритм 2: Шифрование

1. Сообщение m
2. Выбрать случайно число $k, 2 \leq k \leq p-2$
3. Вычислить

$$\gamma \equiv \alpha^k \pmod{p}$$

$$\delta \equiv m \cdot (\alpha^a)^k \pmod{p}$$

Вычислить γ : количество умножений меньше или равно

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

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 $(\alpha^a)^k \pmod{p}$ 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 $m(\alpha^a)^k$ имеет сложность: $[\log_2(p-1)]^2$

Деление с остатком модулю p 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: Разшифрование

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 $\alpha^2(\bmod p); \dots; \alpha^{p-2}(\bmod p)$ 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

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

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

Аналогично для α^{p-2}

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

Общая сложность определения α полным перебором:

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

Системы Эль-Гамала в мультипликативной группе гауссовых чисел

$$\square [i] / < \beta >$$

Данная схема Эль-Гамала установлено в мультипликативной группе гауссовых чисел

$\square [i] / < \beta >$ при β - простое число вида $4k+3$.

Описание алгоритмов схемы Эль-Гамала 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 $G_\beta^* = (a+bi) \mid 0 \leq a \leq p-1, 0 \leq b \leq p-1$ и $G_\beta^* = 1, \theta, \theta^2, \theta^3, \dots, \theta^{p^2-1}$.

3. Выбор случайного числа $a, 1 \leq a \leq p^2-2$ и вычисление $\theta^a \pmod{\beta}$. 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 А (p, θ, θ^a) .

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

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 $m = \gamma^{-a} \cdot \delta \pmod{\beta}$.

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

1. Вычисление $\theta^2 \pmod{\beta}; \dots; \theta^{p^2-2} \pmod{\beta}$

2. Сравнение с $\theta \alpha^a \pmod{\beta}$

Вычислительная сложность алгоритмов Системы Эль-Гамалья в мультипликативной группе гауссовых чисел $\square [i] / < \beta >$

Алгоритм 2:

1. Сообщение m
2. Выбрать случайно число $k, k \leq p^2 - 1$
3. Вычислить $\gamma \equiv \theta^k \pmod{\beta}$

Вычисление θ^k количество умножений меньше $2(\log_2 k + 1) \leq 2(\log_2(p^2 - 1) + 1)$

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

Сложность вычисления с учетом повышения разрядов число после каждого умножения.

Деление требует 6 умножений, 2 сложения, 2 деления.

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

Общая сложность вычисления γ

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

4. Вычислить $\delta \equiv m(\theta^a)^k \pmod{\beta}$

Вычисление $(\theta^a)^k \pmod{\beta}$ аналогично вычисления γ :

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

Умножение $m(\theta^a)^k \pmod{\beta}$:

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

Общая сложность алгоритма

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

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

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

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

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

Алгоритм 3: Разшифрование

1. Вычислить $\gamma^{p-1-a} \pmod{\beta}$

Вычисление $p-1-a: \log_2 p$

Вычисление $\gamma^{p-1-a} \pmod{\beta}$ 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 $\gamma^{-a} \delta \pmod{\beta}$ аналогично вычислению δ :

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

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

Общая сложность алгоритма:

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

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

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

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

Алгоритм 4: Дешифрование

Вычислить $\theta^2 \pmod{\beta}; \dots; \theta^{p-2} \pmod{\beta}$ и сравнение с $\theta^i \pmod{\beta}$

1. Сравнение θ с $\theta^i \pmod{\beta}$: $2 \log_2 p$

2. Вычислить $\theta^2 \pmod{\beta}$ и сравнение с $\theta^i \pmod{\beta}$:

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

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

Сравнение: $2 \log_2 p$

Общая сложность:

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

3. Вычислить $\theta^3 \pmod{\beta}$ и сравнение с $\theta^i \pmod{\beta}$ (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 : $4(\log_2 p)^2 \cdot 2 + 2 \log_2 p \cdot 2 + 2(\log_2 p \cdot 4)^2$

Сравнение: $2 \log_2 p$

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

Аналогично для θ^{p^2-1}

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

Общая сложность определения a полным перебором:

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

Системы Эль-Гамала в группе фактора кольца $U(\mathbb{F}_p[x]/\langle x^2 \rangle)$

Данная схема Эль-Гамала установлено в группе фактора кольца $U(\mathbb{F}_p[x]/\langle x^2 \rangle)$ при p большое простое число.

Описание алгоритмов схемы Эль-Гамала в группе фактора кольца

$U(\mathbb{F}_p[x]/\langle x^2 \rangle)$

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 $U(\mathbb{F}_p[x]/\langle x^2 \rangle)$. Тогда $U(\mathbb{F}_p[x]/\langle x^2 \rangle) = 1, \alpha(x), \alpha(x)^2, \alpha(x)^3, \dots, \alpha(x)^{p^2-p-1}$.
3. Выбор случайного числа $a, 2 \leq a \leq p^2 - p - 1$ и вычисление $\alpha(x)^a \pmod{x^2}$.

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

Для шифрования сообщения $m, m \in U(\mathbb{F}_p[x]/\langle x^2 \rangle)$, 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 $k, 2 \leq k \leq p^2 - p - 1$, вычисление $\gamma \equiv \alpha(x)^k \pmod{x^2}$ и $\delta \equiv m(\alpha(x)^a)^k \pmod{x^2}$.
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 $m = \gamma^{-a} \cdot \delta \pmod{x^2}$.

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

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

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

Вычислительная сложность алгоритмов системы Эль-Гамала в группе фактора кольца $U(\mathbb{F}_p[x]/\langle x^2 \rangle)$

Алгоритм 2:

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

$$\alpha(x) = a + bx$$

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

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

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

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

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

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

Общая сложность вычисления γ

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

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

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

Вычислить $(\alpha(x)^a)^k \pmod{x^2}$ аналогично вычислению γ

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

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

Умножение

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

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

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:

$$4 \left[(\log_2(p^2 - p - 1) + 1) \left[\frac{p^2 - p - 1}{2} \log_2(p-1) \right]^2 + 2 \left[\log_2(p-1) \cdot \frac{p^2 - p - 1}{2} \right]^2 + \right. \\ \left. 2[\log_2(p-1)]^2 + 2 \log_2(p^2 - p - 1) \cdot 2 \log_2(p-1) + 3(\log_2(p-1))^2 + 2 \log_2(p-1) + \right. \\ \left. + 2(2 \log_2(p-1))^2 = \left[4(\log_2(p^2 - p - 1) + 6) \left[\frac{p^2 - p - 1}{2} \log_2(p-1) \right]^2 + \right. \right. \\ \left. \left. + 13[\log_2(p-1)]^2 + 2 \log_2(p^2 - p - 1) \cdot 2 \log_2(p-1) + 2 \log_2(p-1) \right] \right.$$

Алгоритм 3: Разшифрование

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

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

Вычислить $\gamma^{p^2 - p - a}$ аналогично вычислению γ

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

Общая сложность:

$$2 \left[(\log_2(p^2 - p - 1) + 1) \left[\frac{p^2 - p - 1}{2} \log_2(p-1) \right]^2 + \left[\log_2(p-1) \cdot \frac{p^2 - p - 1}{2} \right]^2 + \right. \\ \left. + [\log_2(p-1)]^2 + \log_2(p^2 - p - 1) \cdot 2 \log_2 p + 3(\log_2(p-1))^2 + 2 \log_2(p-1) + \right. \\ \left. + 2(2 \log_2(p-1))^2 = \left[2(\log_2(p^2 - p - 1) + 3) \left[\frac{p^2 - p - 1}{2} \log_2(p-1) \right]^2 + \right. \right. \\ \left. \left. + 12[\log_2(p-1)]^2 + \log_2(p^2 - p - 1) \cdot 2 \log_2 p + 2 \log_2(p-1) \right] \right.$$

Алгоритм 4: Дешифрование

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:

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

Общая сложность

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

Схема Эль-Гамала и Эффективность схемы Эль-Гамала

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

Заключение

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

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 университет

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,