Летняя суперкомпьютерная академия – 2012

Лукция 1. Линейные системы над $\mathbb{F}_2$

Замарашкин Николай Леонидович

Институт вычислительной математики РАН

Линейные системы над $\mathbb{F}_2$

План цикла.

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения
   1.1 задача криптографии

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения
   - 1.1 задача криптографии
   - 1.2 построение кодов, исправляющих ошибки

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения
   - 1.1 задача криптографии
   - 1.2 построение кодов, исправляющих ошибки
2. Методы решения сверхбольших систем линейных уравнений над $\mathbb{F}_2$

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения
   - 1.1 задача криптографии
   - 1.2 построение кодов, исправляющих ошибки
2. Методы решения сверхбольших систем линейных уравнений над $\mathbb{F}_2$
   - 2.1 параллельные методы против параллельных реализаций

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения
   - 1.1 задача криптографии
   - 1.2 построение кодов, исправляющих ошибки
2. Методы решения сверхбольших систем линейных уравнений над $\mathbb{F}_2$
   - 2.1 параллельные методы против параллельных реализаций
   - 2.2 методы меньшей вычислительной сложности

Линейные системы над $\mathbb{F}_2$

План цикла.

1. Задачи большой вычислительной сложности "искусственного"происхождения
   - 1.1 задача криптографии
   - 1.2 построение кодов, исправляющих ошибки
2. Методы решения сверхбольших систем линейных уравнений над $\mathbb{F}_2$
   - 2.1 параллельные методы против параллельных реализаций
   - 2.2 методы меньшей вычислительной сложности
3. Параллельные вычисления при построении LDPC кодов

Линейные системы над $\mathbb{F}_2$

План лекции.

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   1.1 определим RSA шифр

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз
   - 1.4 проведем анализ свойств системы над $\mathbb{F}_2$

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз
   - 1.4 проведем анализ свойств системы над $\mathbb{F}_2$
2. Коды, исправляющие ошибки

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз
   - 1.4 проведем анализ свойств системы над $\mathbb{F}_2$
2. Коды, исправляющие ошибки
   - 2.1 определим математическое понятие канала

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз
   - 1.4 проведем анализ свойств системы над $\mathbb{F}_2$
2. Коды, исправляющие ошибки
   - 2.1 определим математическое понятие канала
   - 2.2 определим понятие линейного ECC кода

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз
   - 1.4 проведем анализ свойств системы над $\mathbb{F}_2$
2. Коды, исправляющие ошибки
   - 2.1 определим математическое понятие канала
   - 2.2 определим понятие линейного ECC кода
   - 2.3 опишем конструкцию LDPC кодов

Линейные системы над $\mathbb{F}_2$

План лекции.

1. Задача криптографии
   - 1.1 определим RSA шифр
   - 1.2 опишем метод факторных баз
   - 1.3 оценим сложность метода факторных баз
   - 1.4 проведем анализ свойств системы над $\mathbb{F}_2$
2. Коды, исправляющие ошибки
   - 2.1 определим математическое понятие канала
   - 2.2 определим понятие линейного ECC кода
   - 2.3 опишем конструкцию LDPC кодов
   - 2.4 сравним постановки задач криптографии и ECC (Error Correcting Codes)

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Будем исходить из того, что любая информация может быть представлена в виде конечного набора из 0 и 1 или, как принято говорить, конечным числом бит.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Будем исходить из того, что любая информация может быть представлена в виде конечного набора из 0 и 1 или, как принято говорить, конечным числом бит.

Предположим, что мы хотим передать некоторый конечный набор бит (передать сообщение) по открытому каналу, но сделать содержание сообщения труднодоступным для "чужих"и легкодоступным для "своих".

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Будем исходить из того, что любая информация может быть представлена в виде конечного набора из 0 и 1 или, как принято говорить, конечным числом бит.

Предположим, что мы хотим передать некоторый конечный набор бит (передать сообщение) по открытому каналу, но сделать содержание сообщения труднодоступным для "чужих"и легкодоступным для "своих".

Это задача криптографии.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Один из распространненных способов шифрования данных – RSA алгоритм (Riverst, Shamir, Adleman).

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Пусть n, p и q – натуральные числа, причем

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Пусть n, p и q – натуральные числа, причем

- $$n = p \cdot q \tag{1}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Пусть n, p и q – натуральные числа, причем

- $$n = p \cdot q \tag{1}$$
- p – большое простое число

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Пусть n, p и q – натуральные числа, причем

- $$n = p \cdot q \tag{1}$$

- p – большое простое число
- q – большое простое число

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Введение.

Пусть n, p и q – натуральные числа, причем

- $$n = p \cdot q \tag{1}$$

- p – большое простое число
- q – большое простое число
- $p \approx q \approx (p - q)$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Для кольца $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ сравнений по модулю n

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Для кольца $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ сравнений по модулю n определим подмножество обратимых элементов $\mathbb{Z}_n^*$:

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Для кольца $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ сравнений по модулю n определим подмножество обратимых элементов $\mathbb{Z}_n^*$:

$$a \in \mathbb{Z}_n^* \Longleftrightarrow a \cdot b = 1 \mod n, \tag{2}$$

для некоторого $b \in \mathbb{Z}_n$.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Для кольца $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ сравнений по модулю n определим подмножество обратимых элементов $\mathbb{Z}_n^*$:

$$a \in \mathbb{Z}_n^* \iff a \cdot b = 1 \mod n, \tag{2}$$

для некоторого $b \in \mathbb{Z}_n$.

Можно также говорить, что $\mathbb{Z}_n^*$ – множество, состоящее из чисел взаимно простых с n.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Theorem

$$\#\mathbb{Z}_n^* = (p-1)(q-1) \tag{3}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Theorem

$$\#\mathbb{Z}_n^* = (p-1)(q-1) \tag{3}$$

Доказательство.

- $\#\mathbb{Z}_n^* = \varphi(n)$, где $\varphi(\cdot)$ – функция Эйлера

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Theorem

$$\#\mathbb{Z}_n^* = (p-1)(q-1) \tag{3}$$

Доказательство.

- $\#\mathbb{Z}_n^* = \varphi(n)$, где $\varphi(\cdot)$ – функция Эйлера
- для взаимно простых a и b справедливо

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

(следствие, например, Китайской теоремы об остатках).

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Необходимые сведения.

Theorem

$$\#\mathbb{Z}_n^* = (p-1)(q-1) \tag{3}$$

Доказательство.

- $\#\mathbb{Z}_n^* = \varphi(n)$, где $\varphi(\cdot)$ – функция Эйлера
- для взаимно простых a и b справедливо

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

(следствие, например, Китайской теоремы об остатках).

- $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

$$n = p \cdot q$$

Алгоритм RSA:

1. выбирается случайное e, $e \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$,

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

$$n = p \cdot q$$

Алгоритм RSA:

1. выбирается случайное e, $e \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$,
2. находится d, $d \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$:

$$d \cdot e = 1 \mod ((p-1)\cdot(q-1))$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

$$n = p \cdot q$$

Алгоритм RSA:

1. выбирается случайное e, $e \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$,
2. находится d, $d \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$:

$$d \cdot e = 1 \mod ((p-1)\cdot(q-1))$$

3. нешифрованное сообщение x, $x \in \mathbb{Z}^*_n$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

$$n = p \cdot q$$

Алгоритм RSA:

1. выбирается случайное e, $e \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$,
2. находится d, $d \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$:

$$d \cdot e = 1 \mod ((p-1)\cdot(q-1))$$

3. нешифрованное сообщение x, $x \in \mathbb{Z}^*_n$
4. зашифрованное сообщение y: $y = x^e \mod n$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$y^d \mod n =$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$y^d \mod n = x^{e \cdot d} \mod n$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$\begin{aligned} y^d \mod n &= x^{e\cdot d} \mod n \\ &= x^{1+s\cdot(p-1)\cdot(q-1)} \mod n \end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$\begin{aligned} y^d \mod n &= x^{e\cdot d} \mod n \\ &= x^{1+s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot(p-1)\cdot(q-1)} \mod n \end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$\begin{aligned} y^d \mod n &= x^{e\cdot d} \mod n \\ &= x^{1+s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot\varphi(n)} \mod n \end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$\begin{aligned} y^d \mod n &= x^{e\cdot d} \mod n \\ &= x^{1+s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot\varphi(n)} \mod n \\ &= x, \end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Определение.

Итак, чтобы зашифровать сообщение, достаточно знать n и e, которые считаются общедоступными. В тоже время, чтобы восстанавливать сообщение, требуется знать недоступное d. Действительно,

$$\begin{aligned} y^d \mod n &= x^{e\cdot d} \mod n \\ &= x^{1+s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot(p-1)\cdot(q-1)} \mod n \\ &= x \cdot x^{s\cdot\varphi(n)} \mod n \\ &= x, \end{aligned}$$

где последнее равенство справедливо в силу малой теоремы Ферма.

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Это простые с вычислительной точки зрения задачи!

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Это простые с вычислительной точки зрения задачи!

Вопрос: трудно ли, зная n и e, найти d?

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Это простые с вычислительной точки зрения задачи!

Вопрос: трудно ли, зная n и e, найти d?

Ответ: легко, если знать p и q.

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Это простые с вычислительной точки зрения задачи!

Вопрос: трудно ли, зная n и e, найти d?

Ответ: легко, если знать p и q.

Вопрос: трудно ли, зная n, найти p и q?

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Это простые с вычислительной точки зрения задачи!

Вопрос: трудно ли, зная n и e, найти d?

Ответ: легко, если знать p и q.

Вопрос: трудно ли, зная n, найти p и q?

Ответ: опыт говорит, что это трудная задача!

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Считая параметры n, e и d заданными, приходим к следующим оценкам сложности:

- сложность шифрования $\leq \mathcal{O}(\log_2^3(n))$
- сложность восстановления $\leq \mathcal{O}(\log_2^3(n))$

Это простые с вычислительной точки зрения задачи!

Вопрос: трудно ли, зная n и e, найти d?

Ответ: легко, если знать p и q.

Вопрос: трудно ли, зная n, найти p и q?

Ответ: опыт говорит, что это трудная задача!

И ВСЁ ЖЕ ?!

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Способ 1. Перебрать все делители вплоть до $\sqrt{n}$.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Способ 1. Перебрать все делители вплоть до $\sqrt{n}$.
Сложность $\mathcal{O}(\sqrt{n} \cdot \log_2^2(n))$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Способ 1. Перебрать все делители вплоть до $\sqrt{n}$.
Сложность $\mathcal{O}(\sqrt{n} \cdot \log_2^2(n))$
Для n таких, что $\log_2 n = 300$ "затея"кажется бесперспективной.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Способ 1. Перебрать все делители вплоть до $\sqrt{n}$.
Сложность $\mathcal{O}(\sqrt{n} \cdot \log_2^2(n))$
Для n таких, что $\log_2 n = 300$ "затея"кажется бесперспективной. Действительно,

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Способ 1. Перебрать все делители вплоть до $\sqrt{n}$.
Сложность $\mathcal{O}(\sqrt{n} \cdot \log_2^2(n))$
Для n таких, что $\log_2 n = 300$ "затея"кажется бесперспективной. Действительно,

вычислительная сложность $\approx 2^{150} \cdot 300^2 \approx 10^{55}$ операций

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Способ 1. Перебрать все делители вплоть до $\sqrt{n}$.
Сложность $\mathcal{O}(\sqrt{n} \cdot \log_2^2(n))$
Для n таких, что $\log_2 n = 300$ "затея"кажется бесперспективной. Действительно,

вычислительная сложность $\approx 2^{150} \cdot 300^2 \approx 10^{55}$ операций

Способ 2. Метод факторных баз.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$n = pq$$

Сделаем элементарное наблюдение.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$n = pq$$

Сделаем элементарное наблюдение. Если целые x и y таковы, что

$$x^2 = y^2 \bmod(n),$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$n = pq$$

Сделаем элементарное наблюдение. Если целые x и y таковы, что

$$x^2 = y^2 \bmod(n),$$

то $pq|(x+y)(x-y)$.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$n = pq$$

Сделаем элементарное наблюдение. Если целые x и y таковы, что

$$x^2 = y^2 \bmod(n),$$

то $pq|(x+y)(x-y)$. Если дополнительно

$$x \neq y \mod n,$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$n = pq$$

Сделаем элементарное наблюдение. Если целые x и y таковы, что

$$x^2 = y^2 \bmod(n),$$

то $pq|(x+y)(x-y)$. Если дополнительно

$$x \neq y \mod n,$$

то

$$p = \gcd(n, x+y).$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Определение.

Пусть заданы n и $y < n$.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Определение.

Пусть заданы n и $y < n$.

Множество всех простых p_j чисел, меньших y, и, возможно, число -1 будем называть базой и писать $\mathcal{B}$.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Определение.

Пусть заданы n и $y < n$.

Множество всех простых p_j чисел, меньших y, и, возможно, число -1 будем называть базой и писать $\mathcal{B}$.

Число t такое, что

$$t^2 = \prod_j p_j^{\alpha_j} \mod n,$$

будем называть $\mathcal{B}$-числом.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Алгоритм факторных баз.

Дано n.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Алгоритм факторных баз.

Дано n.

1. задать y и базу $\mathcal{B}$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Алгоритм факторных баз.

Дано n.

1. задать y и базу $\mathcal{B}$
2. случайным образом выбирать t

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Алгоритм факторных баз.

Дано n.

1. задать y и базу $\mathcal{B}$
2. случайным образом выбирать t
3. проверять является t или нет $\mathcal{B}$-числом

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Алгоритм факторных баз.

Дано n.

1. задать y и базу $\mathcal{B}$
2. случайным образом выбирать t
3. проверять является t или нет $\mathcal{B}$-числом
4. найти таким образом $\#\mathcal{B} + 1$ различных $\mathcal{B}$-чисел

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Метод факторных баз.

Алгоритм факторных баз.

Дано n.

1. задать y и базу $\mathcal{B}$
2. случайным образом выбирать t
3. проверять является t или нет $\mathcal{B}$-числом
4. найти таким образом $\#\mathcal{B} + 1$ различных $\mathcal{B}$-чисел
5. решая линейную систему над $\mathbb{F}_2$ найти x и y:

$$x^2 = y^2 \mod n, \quad x \neq y \mod n.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть $n = 319$.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть $n = 319$. Фиксируем базу делителей:

- $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13\}, \quad \#\mathcal{B} = 7$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть $n = 319$. Фиксируем базу делителей:

- $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13\}, \quad \#\mathcal{B} = 7$

Случайным образом выбираем целые числа в интервале от 1 до 319.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть $n = 319$. Фиксируем базу делителей:

- $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13\}, \quad \#\mathcal{B} = 7$

Случайным образом выбираем целые числа в интервале от 1 до 319.

Пусть, например, первым "выпало"число 24.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть $n = 319$. Фиксируем базу делителей:

- $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13\}, \quad \#\mathcal{B} = 7$

Случайным образом выбираем целые числа в интервале от 1 до 319.
Пусть, например, первым "выпало"число 24.
Не сложно проверить, что остаток

$$24^2 \mod 319 = 257$$

в произведение чисел базы $\mathcal{B}$ не расскладывается.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть $n = 319$. Фиксируем базу делителей:

- $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13\}, \quad \#\mathcal{B} = 7$

Случайным образом выбираем целые числа в интервале от 1 до 319.

Пусть, например, первым "выпало"число 24.

Не сложно проверить, что остаток

$$24^2 \mod 319 = 257$$

в произведение чисел базы $\mathcal{B}$ не расскладывается.

24 не является $\mathcal{B}$-числом!

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть следующим "выпало"число 17.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть следующим "выпало"число 17. Прямыми вычислениями показываем, что

$$17^2 = -30 \mod 319 = -1 \cdot 2 \cdot 3 \cdot 5 \bmod(319).$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть следующим "выпало"число 17. Прямыми вычислениями показываем, что

$$17^2 = -30 \mod 319 = -1 \cdot 2 \cdot 3 \cdot 5 \bmod(319).$$

Следовательно, 17 – $\mathcal{B}$-число.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть следующим "выпало"число 17. Прямыми вычислениями показываем, что

$$17^2 = -30 \mod 319 = -1 \cdot 2 \cdot 3 \cdot 5 \bmod(319).$$

Следовательно, 17 – $\mathcal{B}$-число. Продолжаем случайную выборку $\mathcal{B}$-чисел, до тех пор пока не будет найдено $(\#\mathcal{B} + 1) = 8$ значений.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(n),$$

Пусть следующим "выпало"число 17. Прямыми вычислениями показываем, что

$$17^2 = -30 \mod 319 = -1 \cdot 2 \cdot 3 \cdot 5 \bmod(319).$$

Следовательно, 17 – $\mathcal{B}$-число. Продолжаем случайную выборку $\mathcal{B}$-чисел, до тех пор пока не будет найдено $(\#\mathcal{B} + 1) = 8$ значений. Будем считать, что в результате были найдены следующие $\mathcal{B}$-числа:

$$17, 18, 19, 25, 27, 33, 36, 22$$

Линейные системы над $\mathbb{F}_2$

1. Шифрование методом RSA

Выпишем разложения:

$$
\begin{aligned}
17^2 &= -1 \cdot 2 \cdot 3 \cdot 5 \mod 319 \\
18^2 &= 5 \mod 319 \\
19^2 &= 2 \cdot 3 \cdot 7 \mod 319 \\
25^2 &= -1 \cdot 13 \mod 319 \\
27^2 &= 7 \cdot 13 \mod 319 \\
33^2 &= 2^2 \cdot 3 \cdot 11 \mod 319 \\
36^2 &= 2^2 \cdot 5 \mod 319 \\
22^2 &= 3 \cdot 5 \cdot 11 \mod 319
\end{aligned}
$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$x^2 = y^2 \bmod(s),$$

Далее записываем произведение неизвестных степеней от квадратов

$$(17^2)^{\nu_1} \dots (22^2)^{\nu_8} = (-2 \cdot 3 \cdot 5)^{\nu_1} \dots (3 \cdot 5 \cdot 11)^{\nu_8} \mod 319,$$

и ищем такие ν_1, ν_2, ..., ν_7, ν_8, чтобы в правой части оказались квадраты простых чисел базы.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Эквивалентная система линейных уравнений

$$
\begin{array}{rcl}
(-1) & | & \nu_1 + \nu_4 = 0; \\
(2) & | & \nu_1 + \nu_3 + 2\nu_6 + 2\nu_7 = 0; \\
(3) & | & \nu_1 + \nu_3 + \nu_6 + \nu_8 = 0; \\
(5) & | & \nu_1 + \nu_2 + \nu_7 + \nu_8 = 0; \\
(7) & | & \nu_3 + \nu_5 = 0; \\
(11) & | & \nu_6 + \nu_8 = 0; \\
(13) & | & \nu_4 + \nu_5 = 0.
\end{array}
$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$
\begin{aligned}
x_1 + x_4 &= 0;\\
x_1 + x_3 &= 0;\\
x_1 + x_3 + x_6 + x_8 &= 0;\\
x_1 + x_2 + x_7 + x_8 &= 0;\\
x_3 + x_5 &= 0;\\
x_6 + x_8 &= 0;\\
x_4 + x_5 &= 0;
\end{aligned}
$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \\ \nu_4 \\ \nu_5 \\ \nu_6 \\ \nu_7 \\ \nu_8 \end{bmatrix} = 0.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \\ \nu_4 \\ \nu_5 \\ \nu_6 \\ \nu_7 \\ \nu_8 \end{bmatrix} = 0.$$

Эта система обязательно имеет нетривиальное решение! Почему?

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Действительно, в ядре матрицы, как минимум, два вектора

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{и} \quad \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Для первого вектора

$$\begin{aligned} (18^2 \cdot 36^2) &= 10^2 \mod 319 \\ (5 \cdot 5 \cdot 2^2) &= 10^2 \mod 319, \Rightarrow \\ 10^2 &= 10^2 \mod 319. \end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Взлом.

Для первого вектора

$$\begin{aligned} (18^2 \cdot 36^2) &= 10^2 \mod 319 \\ (5 \cdot 5 \cdot 2^2) &= 10^2 \mod 319, \Rightarrow \\ 10^2 &= 10^2 \mod 319. \end{aligned}$$

Для второго вектора

$$\begin{aligned} 112^2 &= 178^2 \mod 319 \\ 112 &\neq 178 \mod 319 \Rightarrow \end{aligned}$$

$$\gcd(319, 112 + 178) = 29 \Rightarrow 319 = 29 \cdot 11.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Какова сложность алгоритма факторных баз?

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Какова сложность алгоритма факторных баз?

Пусть n и y целые неотрицательные числа:

- $[\log_2(n)] = r$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Какова сложность алгоритма факторных баз?

Пусть n и y целые неотрицательные числа:

- $[\log_2(n)] = r$
- $[\log_2(y)] = s$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Какова сложность алгоритма факторных баз?

Пусть n и y целые неотрицательные числа:

- $[\log_2(n)] = r$
- $[\log_2(y)] = s$
- $u = \left[\frac{r}{s}\right]$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Какова сложность алгоритма факторных баз?

Пусть n и y целые неотрицательные числа:

- $[\log_2(n)] = r$
- $[\log_2(y)] = s$
- $u = \left[\frac{r}{s}\right]$

Пусть также $\Psi(n, y)$ – множество целых неотрицательных чисел, меньших n, которые не делятся ни на одно простое, большее y.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Наша ближайшая цель найти вероятность $\mathcal{P}(t \in \Psi(n, y))$ того, что случайное число t, меньшее заданного n, будет произведением простых чисел, меньших заданного y.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Наша ближайшая цель найти вероятность $\mathcal{P}(t \in \Psi(n, y))$ того, что случайное число t, меньшее заданного n, будет произведением простых чисел, меньших заданного y.

Рассмотрим базу $\mathcal{B} = \{2, 3, \cdots, p_s, \cdots, p_{\pi(y)}\}$, составленную из простых чисел, меньших y.

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Наша ближайшая цель найти вероятность $\mathcal{P}(t \in \Psi(n, y))$ того, что случайное число t, меньшее заданного n, будет произведением простых чисел, меньших заданного y.

Рассмотрим базу $\mathcal{B} = \{2, 3, \cdots, p_s, \cdots, p_{\pi(y)}\}$, составленную из простых чисел, меньших y.

Из закона простых чисел следует, что

$$\pi(y) \approx \frac{y}{\log_e(y)}.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Наша ближайшая цель найти вероятность $\mathcal{P}(t \in \Psi(n, y))$ того, что случайное число t, меньшее заданного n, будет произведением простых чисел, меньших заданного y.

Рассмотрим базу $\mathcal{B} = \{2, 3, \cdots, p_s, \cdots, p_{\pi(y)}\}$, составленную из простых чисел, меньших y.

Из закона простых чисел следует, что

$$\pi(y) \approx \frac{y}{\log_e(y)}.$$

Оценим количество целых чисел вида

$$\prod_{j=1}^{\pi(y)} p_j^{\alpha_j} \leq n,$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Наша ближайшая цель найти вероятность $\mathcal{P}(t \in \Psi(n, y))$ того, что случайное число t, меньшее заданного n, будет произведением простых чисел, меньших заданного y.

Рассмотрим базу $\mathcal{B} = \{2, 3, \cdots, p_s, \cdots, p_{\pi(y)}\}$, составленную из простых чисел, меньших y.

Из закона простых чисел следует, что

$$\pi(y) \approx \frac{y}{\log_e(y)}.$$

Оценим количество целых чисел вида

$$\prod_{j=1}^{\pi(y)} p_j^{\alpha_j} \leq n,$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\sum_{j=1}^{\pi(y)} \alpha_j \log_2(p_j) \leq \log_2(n), \Rightarrow$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\sum_{j=1}^{\pi(y)} \alpha_j \log_2(p_j) \leq \log_2(n), \Rightarrow$$

$$\sum_{j=1}^{\pi(y)} \alpha_j \leq \frac{\log_2(n)}{\log_2(y)}, \Rightarrow$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\sum_{j=1}^{\pi(y)} \alpha_j \log_2(p_j) \leq \log_2(n), \Rightarrow$$

$$\sum_{j=1}^{\pi(y)} \alpha_j \leq \frac{\log_2(n)}{\log_2(y)}, \Rightarrow$$

$$\sum_{j=1}^{\pi(y)} \alpha_j \leq u, \Rightarrow$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\sum_{j=1}^{\pi(y)} \alpha_j \log_2(p_j) \leq \log_2(n), \Rightarrow$$

$$\sum_{j=1}^{\pi(y)} \alpha_j \leq \frac{\log_2(n)}{\log_2(y)}, \Rightarrow$$

$$\sum_{j=1}^{\pi(y)} \alpha_j \leq u, \Rightarrow$$

$$\sum_{j=1}^{y} \alpha_j \leq u.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Из комбинаторики известно, что число таких α_j, что

$$\sum_{j=1}^{y} \alpha_j \leq u, \tag{4}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Из комбинаторики известно, что число таких α_j, что

$$\sum_{j=1}^{y} \alpha_j \leq u, \tag{4}$$

равно

$$\left(\begin{array}{c} u+y \\ y \end{array} \right) = \#\{\Psi(n, y)\},$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Из комбинаторики известно, что число таких α_j, что

$$\sum_{j=1}^{y} \alpha_j \leq u, \tag{4}$$

равно

$$\left(\begin{array}{c} u+y \\ y \end{array} \right) = \#\{\Psi(n,y)\},$$

а искомая вероятность

$$\mathcal{P}(t \in \Psi(n,y)) = \frac{\#\{\Psi(n,y)\}}{n} = \frac{\left(\begin{array}{c} u+y \\ y \end{array} \right)}{n}.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\log_2 \left(\left(\begin{array}{c} u+y \\ y \end{array} \right) / n \right)$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\log_2 \left(\left(\begin{array}{c} u+y \\ y \end{array} \right) / n \right)$$

$$= \log_2 \left(\begin{array}{c} u+y \\ y \end{array} \right) - \log_2(n)$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\log_2\left(\left(\begin{array}{c} u+y \\ y \end{array}\right)/n\right)$$

$$\begin{aligned} &= \log_2\left(\begin{array}{c} u+y \\ y \end{array}\right) - \log_2(n) \\ &= \log_2((u+y)!) - \log_2(u!) - \log_2(y!) - \log_2(n) \end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\log_2 \left(\binom{u+y}{y} / n \right)$$

$$\begin{aligned}
&= \log_2 \binom{u+y}{y} - \log_2(n) \\
&= \log_2((u+y)!) - \log_2(u!) - \log_2(y!) - \log_2(n) \\
&= (u+y)\log_2(u+y) - u\log_2(u) - y\log_2(y) - \log_2(n)
\end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\log_2 \left(\left(\begin{array}{c} u+y \\ y \end{array} \right) / n \right)$$

$$\begin{aligned}
&= \log_2 \left(\begin{array}{c} u+y \\ y \end{array} \right) - \log_2(n) \\
&= \log_2((u+y)!) - \log_2(u!) - \log_2(y!) - \log_2(n) \\
&= (u+y)\log_2(u+y) - u\log_2(u) - y\log_2(y) - \log_2(n) \\
&\approx y\log_2 y + u\log_2 y (= \log_2(n)) - \cdots
\end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\log_2\left(\left(\begin{array}{c} u+y \\ y \end{array}\right)/n\right)$$

$$\begin{aligned}
&= \log_2\left(\begin{array}{c} u+y \\ y \end{array}\right) - \log_2(n) \\
&= \log_2((u+y)!) - \log_2(u!) - \log_2(y!) - \log_2(n) \\
&= (u+y)\log_2(u+y) - u\log_2(u) - y\log_2(y) - \log_2(n) \\
&\approx y\log_2 y + u\log_2 y (= \log_2(n)) - \cdots \\
&= -u\log_2(u)
\end{aligned}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \binom{u+y}{y} / n \approx u^{-u}$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \binom{u+y}{y} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \begin{pmatrix} u+y \\ y \end{pmatrix} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы
   - выбор b_i кандидата $\rightarrow \mathcal{O}(r)$ (r – случайных бит)

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \binom{u+y}{y} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы
   - выбор b_i кандидата $\rightarrow \mathcal{O}(r)$ (r – случайных бит)
   - вычислить $b_i^2 \mod n \rightarrow \mathcal{O}(r^2)$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \binom{u+y}{y} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы
   - выбор b_i кандидата $\rightarrow \mathcal{O}(r)$ (r – случайных бит)
   - вычислить $b_i^2 \mod n \rightarrow \mathcal{O}(r^2)$
   - деление на элементы базы $\rightarrow \mathcal{O}(\pi(y) \cdot r \cdot s)$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \begin{pmatrix} u+y \\ y \end{pmatrix} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы
   - выбор b_i кандидата $\rightarrow \mathcal{O}(r)$ (r – случайных бит)
   - вычислить $b_i^2 \mod n \rightarrow \mathcal{O}(r^2)$
   - деление на элементы базы $\rightarrow \mathcal{O}(\pi(y) \cdot r \cdot s)$
   - полная сложность $\rightarrow \mathcal{O}\left(u^u \cdot (\pi(y) + 1) \cdot \pi(y) \cdot r \cdot s\right)$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \begin{pmatrix} u+y \\ y \end{pmatrix} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы
   - выбор b_i кандидата $\rightarrow \mathcal{O}(r)$ (r – случайных бит)
   - вычислить $b_i^2 \mod n \rightarrow \mathcal{O}(r^2)$
   - деление на элементы базы $\rightarrow \mathcal{O}(\pi(y) \cdot r \cdot s)$
   - полная сложность $\rightarrow \mathcal{O}\left(u^u \cdot (\pi(y) + 1) \cdot \pi(y) \cdot r \cdot s\right)$
2. решение линейной системы

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\mathcal{P}(t \in \Psi(n, y)) = \begin{pmatrix} u+y \\ y \end{pmatrix} / n \approx u^{-u}$$

Сложность всего алгоритма:

1. построение матрицы
   - выбор b_i кандидата $\rightarrow \mathcal{O}(r)$ (r – случайных бит)
   - вычислить $b_i^2 \mod n \rightarrow \mathcal{O}(r^2)$
   - деление на элементы базы $\rightarrow \mathcal{O}(\pi(y) \cdot r \cdot s)$
   - полная сложность $\rightarrow \mathcal{O}\left(u^u \cdot (\pi(y) + 1) \cdot \pi(y) \cdot r \cdot s\right)$
2. решение линейной системы
   - LU - метод $\rightarrow \mathcal{O}(y^3/s^3)$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Обе части алгоритма должны занимать одинаковое время. Следовательно,

$$\frac{r}{s}\log_2\left(\frac{r}{s}\right) \approx s \Rightarrow$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Обе части алгоритма должны занимать одинаковое время. Следовательно,

$$\frac{r}{s}\log_2\left(\frac{r}{s}\right) \approx s \Rightarrow$$

$$s^2 \approx r.$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Обе части алгоритма должны занимать одинаковое время. Следовательно,

$$\frac{r}{s}\log_2\left(\frac{r}{s}\right) \approx s \Rightarrow$$

$$s^2 \approx r.$$

Возвращаясь к примеру:

- $\log_2(n) = r = 300$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

Обе части алгоритма должны занимать одинаковое время. Следовательно,

$$\frac{r}{s}\log_2\left(\frac{r}{s}\right) \approx s \Rightarrow$$

$$s^2 \approx r.$$

Возвращаясь к примеру:

- $\log_2(n) = r = 300$
- $\log_2(y) = s = \sqrt{r} \approx 17$
- $u = \frac{\log_2(n)}{\log_2(y)} \approx 17 << y$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\left\{ \begin{array}{c} \text{вычислительная} \\ \text{сложность} \end{array} \right\} \approx 2 \cdot 2^{3 \cdot \sqrt{300}} = 2^{51} \approx 10^{18} \qquad (5)$$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Оценка сложности алгоритма.

$$\left\{ \begin{array}{c} \text{вычислительная} \\ \text{сложность} \end{array} \right\} \approx 2 \cdot 2^{3 \cdot \sqrt{300}} = 2^{51} \approx 10^{18} \qquad (5)$$

Вывод: это не страшное число!

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

1. каждая строка матрицы соответствует элементу $\mathcal{B}$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

1. каждая строка матрицы соответствует элементу $\mathcal{B}$
2. каждый столбец матрицы соответствует $\mathcal{B}$-числу

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

1. каждая строка матрицы соответствует элементу $\mathcal{B}$
2. каждый столбец матрицы соответствует $\mathcal{B}$-числу
3. число ненулевых элементов в столбце $\approx u$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

1. каждая строка матрицы соответствует элементу $\mathcal{B}$
2. каждый столбец матрицы соответствует $\mathcal{B}$-числу
3. число ненулевых элементов в столбце $\approx u$
4. за исключением первых строк число ненулевых элементов в строке $\approx u$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

1. каждая строка матрицы соответствует элементу $\mathcal{B}$
2. каждый столбец матрицы соответствует $\mathcal{B}$-числу
3. число ненулевых элементов в столбце $\approx \mathfrak{u}$
4. за исключением первых строк число ненулевых элементов в строке $\approx \mathfrak{u}$
5. кроме первых строк матрица разреженная

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для матрицы H справедливы следующие утверждения:

1. каждая строка матрицы соответствует элементу $\mathcal{B}$
2. каждый столбец матрицы соответствует $\mathcal{B}$-числу
3. число ненулевых элементов в столбце $\approx \mathfrak{u}$
4. за исключением первых строк число ненулевых элементов в строке $\approx \mathfrak{u}$
5. кроме первых строк матрица разреженная
6. ненулевые элементы матрицы "разбросаны"в случайном порядке

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для примера:

1. размер матрицы H: приблизительно $10^{18} \times 10^{18}$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для примера:

1. размер матрицы H: приблизительно $10^{18} \times 10^{18}$
2. число ненулевых элементов в строке и столбце: приблизительно 20

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для примера:

1. размер матрицы H: приблизительно $10^{18} \times 10^{18}$
2. число ненулевых элементов в строке и столбце: приблизительно 20
3. число ненулевых элементов: приблизительно $2 \cdot 10^{19}$

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для примера:

1. размер матрицы H: приблизительно $10^{18} \times 10^{18}$
2. число ненулевых элементов в строке и столбце: приблизительно 20
3. число ненулевых элементов: приблизительно $2 \cdot 10^{19}$
4. размер занимаемой памяти: приблизительно 10^{20} байт

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Свойства матрицы.

$$Hc = 0$$

Для примера:

1. размер матрицы H: приблизительно $10^{18} \times 10^{18}$
2. число ненулевых элементов в строке и столбце: приблизительно 20
3. число ненулевых элементов: приблизительно $2 \cdot 10^{19}$
4. размер занимаемой памяти: приблизительно 10^{20} байт

Вывод: пример все равно слишком сложен для метода факторных баз

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Особенности алгоритма.

Анализ алгоритма.

1. сложности построения и решения системы равны

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Особенности алгоритма.

Анализ алгоритма.

1. сложности построения и решения системы равны
2. построение системы – параллельный алгоритм

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Особенности алгоритма.

Анализ алгоритма.

1. сложности построения и решения системы равны
2. построение системы – параллельный алгоритм
3. решение системы – алгоритм с ограниченными параллельными свойствами

Линейные системы над $\mathbb{F}_2$

1. RSA шифр. Особенности алгоритма.

Анализ алгоритма.

1. сложности построения и решения системы равны
2. построение системы – параллельный алгоритм
3. решение системы – алгоритм с ограниченными параллельными свойствами

Вывод: необходимо строить эффективные методы решения больших и сверхбольших разреженных систем над $\mathbb{F}_2$