Генерическая сложность некоторых проблем криптографии

Александр Рыбалов

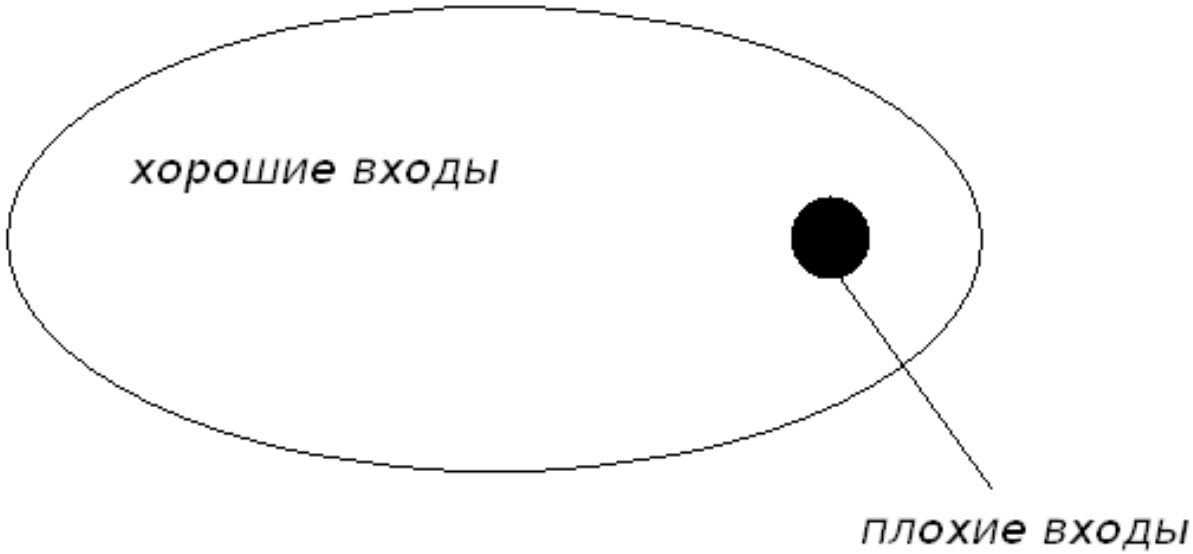
ОФ ИМ СО РАН, Омск

апрель, 2015

Классический подход

Алгоритм (быстро) работает на **всех** входах.

Генерический подход



Алгоритм быстро работает на **почти всех** входах и игнорирует плохие.

Асимптотическая плотность

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\mu(S) = \lim_{n \to \infty} \frac{|S \cap I_n|}{|I_n|}.$$

Асимптотическая плотность

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\mu(S) = \lim_{n \to \infty} \frac{|S \cap I_n|}{|I_n|}.$$

Замечание

$\frac{|S \cap I_n|}{|I_n|}$ – вероятность получить вход из S если мы генерируем входы размера n случайно и равномерно.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A} : I \to J \cup \{?\}$ называется генерическим, если

1. для любого $x \in I$ $\mathcal{A}(x)$ останавливается,
2. $\mu(\{x : \mathcal{A}(x) = ?\}) = 0$.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A} : I \to J \cup \{?\}$ называется генерическим, если

1. для любого $x \in I$ $\mathcal{A}(x)$ останавливается,
2. $\mu(\{x : \mathcal{A}(x) = ?\}) = 0$.

Определение

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если для любого $x \in I$

$$\mathcal{A}(x) \neq ? \Rightarrow f(x) = \mathcal{A}(x).$$

Криптографические проблемы

Криптографические проблемы

1. Проблема дискретного логарифма.

Криптографические проблемы

1. Проблема дискретного логарифма.
2. Проблема извлечения квадратного корня в группах вычетов.

Криптографические проблемы

1. Проблема дискретного логарифма.
2. Проблема извлечения квадратного корня в группах вычетов.
3. Проблема поиска изоморфизма графов.

Криптографические проблемы

1. Проблема дискретного логарифма.
2. Проблема извлечения квадратного корня в группах вычетов.
3. Проблема поиска изоморфизма графов.

Криптографические гипотезы

Для проблем 1-3 не существует полиномиальных (вероятностных) алгоритмов, решающих их для всех входов.

Что хочется доказать?

Теорема

Если для криптографической проблемы существует полиномиальный генерический алгоритм, то существует полиномиальный вероятностный алгоритм, решающий эту проблему **для всех** входов.

Что хочется доказать?

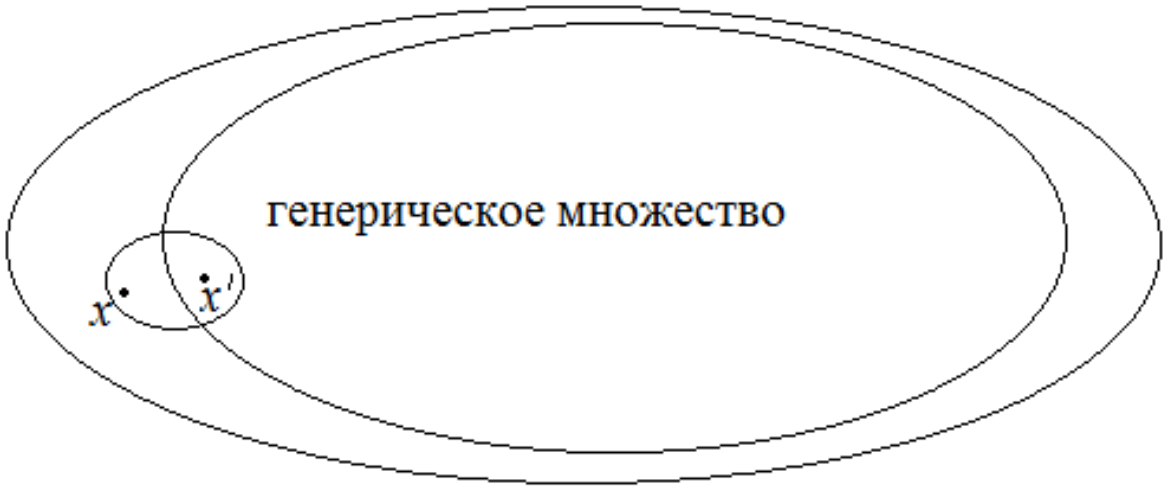
Теорема

Если для криптографической проблемы существует полиномиальный генерический алгоритм, то существует полиномиальный вероятностный алгоритм, решающий эту проблему **для всех** входов.

Следствие

Если криптографическая проблема трудноразрешима в классическом случае, то она трудноразрешима генерически.

Амплификация алгоритмических проблем



Проблема дискретного логарифма

Формулировка проблемы

$I = \{(a, g, p),\ p$ – простое, g – первообразный $GF(p)$, $a \in GF(p)^*\}$,

Вычислить функцию $dl : I \to \mathbb{N}$, определенную следующим образом:

$$dl(a, g, p) = x \Leftrightarrow g^x = a \text{ в } GF(p).$$

Проблема дискретного логарифма

Формулировка проблемы

$I = \{(a, g, p),\ p$ – простое, g – первообразный $GF(p)$, $a \in GF(p)^*\}$,
Вычислить функцию $dl : I \to \mathbb{N}$, определенную следующим образом:

$$dl(a, g, p) = x \Leftrightarrow g^x = a \text{ в } GF(p).$$

Приложения в криптографии

Протокол Диффи-Хеллмана, схема Эль-Гамаля, криптосистема Мэсси-Омуры.

Стратификация

Определение

Последовательность

$$\pi = \{(p_m, g_m),\ m \in \mathbb{N}, \text{где } p_m - \text{простое},$$

$$g_m - \text{первообразный в } GF(p_m)\}$$

экспоненциальная, если $2^m < p_m < 2^{m+1}$ для любого m.

Стратификация

Определение

Последовательность

$$\pi = \{(p_m, g_m),\ m \in \mathbb{N}, \text{где } p_m - \text{простое},$$

$$g_m - \text{первообразный в } GF(p_m)\}$$

экспоненциальная, если $2^m < p_m < 2^{m+1}$ для любого m.

Формулировка проблемы

$I_\pi = \{(a, g, p),\ (p, g) \in \pi,\ a \in GF(p)^*\}$,
Вычислить функцию $dl_\pi = dl|_{I_\pi}$.

Стратификация

Определение

Последовательность

$$\pi = \{(p_m, g_m),\ m \in \mathbb{N}, \text{где } p_m - \text{простое},$$

$$g_m - \text{первообразный в } GF(p_m)\}$$

экспоненциальная, если $2^m < p_m < 2^{m+1}$ для любого m.

Формулировка проблемы

$I_\pi = \{(a, g, p),\ (p, g) \in \pi,\ a \in GF(p)^*\}$,
Вычислить функцию $dl_\pi = dl|_{I_\pi}$.

Размер входа (a, g, p) – длина двоичной записи числа p.

Стратификация

Определение

Последовательность

$$\pi = \{(p_m, g_m),\ m \in \mathbb{N}, \text{где } p_m - \text{простое},$$

$$g_m - \text{первообразный в } GF(p_m)\}$$

экспоненциальная, если $2^m < p_m < 2^{m+1}$ для любого m.

Формулировка проблемы

$I_\pi = \{(a, g, p),\ (p, g) \in \pi,\ a \in GF(p)^*\}$,
Вычислить функцию $dl_\pi = dl|_{I_\pi}$.

Размер входа (a, g, p) – длина двоичной записи числа p.
Множество входов размера n: все тройки вида (a, g, p), где g, p – фиксированы, $a \in GF(p)^*$.

Проблема дискретного логарифма генерически трудна

Теорема

Если для вычисления dl не существует полиномиального вероятностного алгоритма, то найдется экспоненциальная последовательность π такая, что и для dl_π не существует полиномиального вероятностного алгоритма.

Проблема дискретного логарифма генерически трудна

Теорема

Если для вычисления dl не существует полиномиального вероятностного алгоритма, то найдется экспоненциальная последовательность π такая, что и для dl_π не существует полиномиального вероятностного алгоритма.

Теорема

Если для вычисления dl_π существует полиномиальный генерический алгоритм, то для dl_π существует полиномиальный вероятностный алгоритм, вычисляющий dl_π для всех входов.

Амплификация проблемы дискретного логарифма

$(a, g, p) \to (ag^k, g, p)$, где k – случайно и равновероятно сгенерированное число от 0 до $p - 2$.

Амплификация проблемы дискретного логарифма

$(a, g, p) \to (ag^k, g, p)$, где k – случайно и равновероятно сгенерированное число от 0 до $p - 2$.
$ag^k = g^x \Rightarrow a = g^{x-k}$.

Проблема извлечения корня в группах вычетов

Формулировка проблемы

$I = \{(a, m) : \ m = pq, p, q -$ простые, $a \in \mathbb{Z}/(m)\}$,
Вычислить функцию $sr : I \to \mathbb{N}$, определенную следующим образом:

$$sr(a, m) = \begin{cases} x, & \text{если } x^2 = a \text{ в } \mathbb{Z}/(m), \\ 0, & \text{иначе.} \end{cases}$$

Проблема извлечения корня в группах вычетов

Формулировка проблемы

$I = \{(a, m) : \ m = pq, p, q -$ простые, $a \in \mathbb{Z}/(m)\}$,
Вычислить функцию $sr : I \to \mathbb{N}$, определенную следующим образом:

$$sr(a, m) = \begin{cases} x, & \text{если } x^2 = a \text{ в } \mathbb{Z}/(m), \\ 0, & \text{иначе.} \end{cases}$$

Приложения в криптографии

Криптосистема Рабина.

Стратификация

Определение

Последовательность

$$\mu = \{m_k,\ k \in \mathbb{N}, \text{где } m_k - \text{произведение двух простых}\}$$

экспоненциальная, если $2^k < m_k < 2^{k+1}$ для любого k.

Определение

Последовательность

$$\mu = \{m_k,\ k \in \mathbb{N}, \text{где } m_k - \text{произведение двух простых}\}$$

экспоненциальная, если $2^k < m_k < 2^{k+1}$ для любого k.

Формулировка проблемы

$I_\mu = \{(a, m) :\ m \in \mu,\ a \in \mathbb{Z}/(m)\}$,
Вычислить функцию $sr_\mu = sr|_{I_\mu}$.

Стратификация

Определение

Последовательность

$$\mu = \{m_k,\ k \in \mathbb{N}, \text{где } m_k - \text{произведение двух простых}\}$$

экспоненциальная, если $2^k < m_k < 2^{k+1}$ для любого k.

Формулировка проблемы

$I_\mu = \{(a, m) :\ m \in \mu,\ a \in \mathbb{Z}/(m)\}$,
Вычислить функцию $sr_\mu = sr|_{I_\mu}$.

Размер входа (a, m) – длина двоичной записи числа m.

Стратификация

Определение

Последовательность

$$\mu = \{m_k,\ k \in \mathbb{N}, \text{где } m_k - \text{произведение двух простых}\}$$

экспоненциальная, если $2^k < m_k < 2^{k+1}$ для любого k.

Формулировка проблемы

$I_\mu = \{(a, m) :\ m \in \mu,\ a \in \mathbb{Z}/(m)\}$,
Вычислить функцию $sr_\mu = sr|_{I_\mu}$.

Размер входа (a, m) – длина двоичной записи числа m.
Множество входов размера n: все пары вида (a, m), где m – фиксировано, $a \in \mathbb{Z}/(m)$.

Проблема извлечения корня в группах вычетов генерически трудна

Теорема

Если для вычисления sr не существует полиномиального вероятностного алгоритма, то найдется экспоненциальная последовательность μ такая, что и для sr_μ не существует полиномиального вероятностного алгоритма.

Проблема извлечения корня в группах вычетов генерически трудна

Теорема

Если для вычисления sr не существует полиномиального вероятностного алгоритма, то найдется экспоненциальная последовательность μ такая, что и для sr_μ не существует полиномиального вероятностного алгоритма.

Теорема

Если для вычисления sr_μ существует полиномиальный генерический алгоритм, то для sr_μ существует полиномиальный вероятностный алгоритм, вычисляющий sr_μ для всех входов.

Амплификация проблемы извлечения корня в группах вычетов

$(a, m) \to (ab^2, m)$, где b – случайно и равновероятно сгенерированный элемент в $\mathbb{Z}/(m)$.

Амплификация проблемы извлечения корня в группах вычетов

$(a, m) \to (ab^2, m)$, где b – случайно и равновероятно сгенерированный элемент в $\mathbb{Z}/(m)$.
$ab^2 = x^2 \Rightarrow a = (xb^{-1})^2$.

Проблема поиска изоморфизма графов

Формулировка проблемы

$I = \{(G_1, G_2),\ G_1, G_2\ -$ изоморфные графы$\}$. Вычислить функцию $sgi : I \to S_1 \cup S_2 \cup \ldots S_n \cup \ldots$, определенную следующим образом:

$$sgi(G_1, G_2) = \text{перестановка вершин} - \text{изоморфизм } G_1 \text{ и } G_2.$$

Проблема поиска изоморфизма графов

Формулировка проблемы

$I = \{(G_1, G_2),\ G_1, G_2\ -$ изоморфные графы$\}$. Вычислить функцию $sgi : I \to S_1 \cup S_2 \cup \ldots S_n \cup \ldots$, определенную следующим образом:

$$sgi(G_1, G_2) = \text{перестановка вершин} - \text{изоморфизм } G_1 \text{ и } G_2.$$

Приложения в криптографии

Доказательство с нулевым разглашением (Шафи Гольдвассер, Сильвио Микали и Чарльз Реккоф, 1985).

Стратификация

Обозначение

Последовательность графов

$$\gamma = \{G_n,\ n \in \mathbb{N}, \text{где } G_n - \text{граф с } n \text{ вершинами}\}.$$

Стратификация

Обозначение

Последовательность графов

$$\gamma = \{G_n,\ n \in \mathbb{N}, \text{где } G_n - \text{граф с } n \text{ вершинами}\}.$$

Формулировка проблемы

$I_\gamma = \{(G_1, G_2) :\ G_2 \in \gamma\}$. Вычислить функцию $sgi_\gamma = sgi|_{I_\gamma}$.

Стратификация

Обозначение

Последовательность графов

$$\gamma = \{G_n,\ n \in \mathbb{N}, \text{где } G_n - \text{граф с } n \text{ вершинами}\}.$$

Формулировка проблемы

$I_\gamma = \{(G_1, G_2) :\ G_2 \in \gamma\}$. Вычислить функцию $sgi_\gamma = sgi|_{I_\gamma}$.

Размер входа (G_1, G_2) – число вершин G_2.

Стратификация

Обозначение

Последовательность графов

$$\gamma = \{G_n,\ n \in \mathbb{N}, \text{где } G_n - \text{граф с } n \text{ вершинами}\}.$$

Формулировка проблемы

$I_\gamma = \{(G_1, G_2) :\ G_2 \in \gamma\}$. Вычислить функцию $sgi_\gamma = sgi|_{I_\gamma}$.

Размер входа (G_1, G_2) – число вершин G_2. Множество входов размера n: все пары вида (G_1, G_2), где G_2 – фиксировано, G_1 – граф, изоморфный G_2.

Проблема поиска изоморфизма графов генерически трудна

Теорема

Если для вычисления sgi не существует полиномиального вероятностного алгоритма, то найдется последовательность графов γ такая, что и для sgi_γ не существует полиномиального вероятностного алгоритма.

Проблема поиска изоморфизма графов генерически трудна

Теорема

Если для вычисления sgi не существует полиномиального вероятностного алгоритма, то найдется последовательность графов γ такая, что и для sgi_γ не существует полиномиального вероятностного алгоритма.

Теорема

Если для вычисления sgi_γ существует полиномиальный генерический алгоритм, то для sgi_γ существует полиномиальный вероятностный алгоритм, вычисляющий sgi_γ для всех входов.

Амплификация проблемы поиска изоморфизма графов

$(G_1, G_2) \to (\pi(G_1), G_2)$, где π – случайно и равновероятно сгенерированная перестановка в S_n.

Амплификация проблемы поиска изоморфизма графов

$(G_1, G_2) \to (\pi(G_1), G_2)$, где π – случайно и равновероятно сгенерированная перестановка в S_n.
$\tau(\pi(G_1)) = G_2 \Rightarrow \chi = \tau\pi$.

Спасибо за внимание!