# КРИПТОАНАЛИЗ ПО ИЗВЕСТНЫМ ОТКРЫТЫМ ТЕКСТАМ ГОМОМОРФНОЙ КРИПТОСИСТЕМЫ ДОМИНГО-ФЕРРЕ

А.В.Трепачева

Южный Федеральный Университет

4 декабря 2014 г.

# Содержание

# Гомоморфное шифрование

- **Гомоморфные криптосистемы** позволяют проводить вычисления программ над зашифрованными данными.
- Результат вычислений над шифртекстами является шифровкой результата вычислений над соответствующими исходными (незашифровнными) данными.

# Модель вычислений и гомоморфное шифрование

- *Исходные данные – элементы некоторого кольца $\mathcal{M}$ с операциями $+, *$, шифртексты – элементы кольца $\mathcal{C}$ с операциями $+_C, *_C$*
- **Программа $\mathbb{P}$, которую нужно вычислить над вектором данных $(a_1, ..., a_n), a_i \in \mathcal{M}$ – набор полиномов:**

$$\mathbf{f_j}(x_1, ..., x_n) =$$
$$\sum_{\{i_1,...,i_t\}\in\{1,...,n\}} f^j_{i_1,...,i_t} * x_{i_1} * ... * x_{i_k}, f^j_{i_1,...,i_t} \in \mathcal{M}, j = 1..m$$

- **Вычисление программы:**
  $b_j \in \mathcal{M} \longleftarrow \mathbf{f_j}(a_1, ..., a_n), j = 1..m.$
- Тогда криптосистема гомоморфна, если для $\forall \mathbf{x}, \mathbf{y} \in \mathcal{M}$:
  $\mathbf{D(E(x) +_C E(y)) = x + y, D(E(x) *_C E(y)) = x * y}$, где $\mathbf{E, D}$ – функции зашифрования и расшифрования.

# Где нужно гомоморфное шифрование?

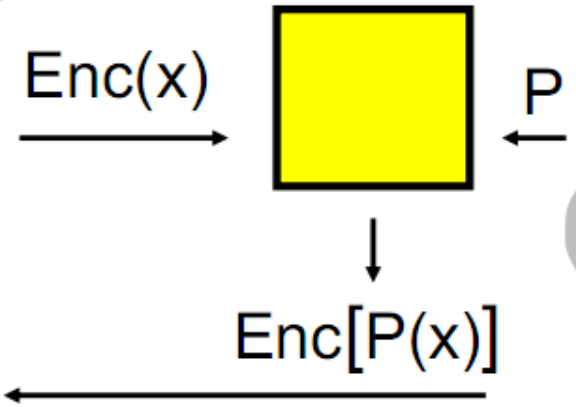
**Потребность в гомоморфном шифровании возникает в случае, когда вычисления над приватными данными проводит Вычислитель, которому Владелец данных не доверяет.**

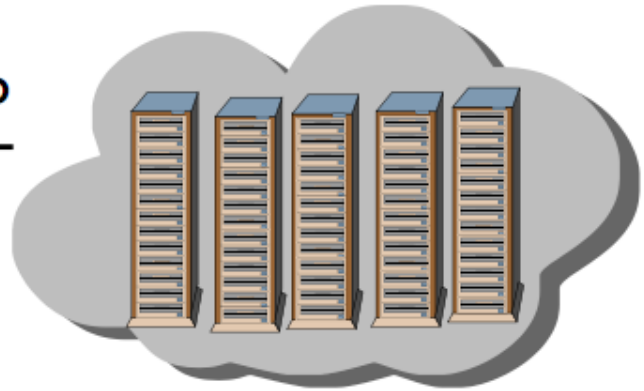
*Такая ситуация возникает, например:*

- *В Облачных сервисах.*
- *При передаче данных по Беспроводным Децентрализованным Сетям Связи (Mobile Ad hoc Network, MANET).*

# Гомоморфное шифрование и Облачные вычисления

**Клиент хочет делегировать вычисление облачному серверу, однако при этом он не желает, чтобы его входные данные попали на сервер в открытом виде.**
**Поэтому нужна криптосистема, которая позволила бы провести вычисления над шифртекстами с последующей возможностью извлечь за приемлемое время из результирующей шифровки результат нужных вычислений над открытыми данными.**



Клиент
(Вход: x)

Облачный сервер
(Программа: P)

# Цель работы

- **В данной работе уточняется степень защищенности гомоморфной криптосистемы Доминго-Ферре против атаки по известным открытым текстам.**
- **Почему анализ криптосистемы Доминго-Ферре представляет интерес?**

*Эту криптосистему можно эффективно использовать в некоторых приложениях (например её используют для защиты данных в Mobile Ad hoc Networks).*
*Однако, шифруя с её помощью данные, нужно хорошо осознававть насколько она уязвима к некоторым атакам.*

# Симметричная гомоморфная криптосистема Доминго-Ферре

- *Открытый текст* $a$ – элемент кольца вычетов $\mathbb{Z}_{\mathbf{n}}$,

  $\mathbf{n} = \mathbf{p} \cdot \mathbf{q}$, где $\mathbf{p}, \mathbf{q}$ – большие простые числа такие, что $\mathbf{p} < \mathbf{q}$, $log_2(\mathbf{p}) \approx log_2(\mathbf{q})$ .
  $\mathbf{n}$ – публичное, а $\mathbf{p}, \mathbf{q}$ являются секретом.

- *Ключ* – $k = (k_p \in \mathbb{Z}_{\mathbf{p}} \setminus \{0\}, k_q \in \mathbb{Z}_{\mathbf{q}} \setminus \{0\})$.
- *Шифртекст* $c = \{c_p(x), c_q(x)\} \in \mathbb{Z}_{\mathbf{n}}[x] \times \mathbb{Z}_{\mathbf{n}}[x]$, где $c_p(0) = 0, c_q(0) = 0, deg(c_p(x)) = d, deg(c_q(x)) = d$, $d \in \mathbb{Z}_+$ – параметр.

  $c_p(k_p) \bmod \mathbf{p} = a_p \in \mathbb{Z}_{\mathbf{p}} (\equiv a (\mathrm{mod} \mathbf{p}))$
  $c_q(k_q) \bmod \mathbf{q} = a_q \in \mathbb{Z}_{\mathbf{q}} (\equiv a (\mathrm{mod} \mathbf{q}))$

- Тогда по *Китайской теореме об остатках*:
  $a = \mathbf{q} \cdot (\mathbf{q}^{-1} \bmod \mathbf{p}) \cdot a_p + \mathbf{p} \cdot (\mathbf{p}^{-1} \bmod \mathbf{q}) \cdot a_q$.

# Уточнение процедуры шифрования

**Шифрование**$(a \in \mathbb{Z}_{\mathbf{n}}, d \in \mathbb{Z}_+, \mathbf{p}, \mathbf{q}, k_p \in \mathbb{Z}_{\mathbf{p}} \setminus \{0\}, k_q \in \mathbb{Z}_{\mathbf{q}} \setminus \{0\})$

- $a \in \mathbb{Z}_{\mathbf{n}} \longrightarrow a'(x) = \sum_{i=1}^{d} a'_i \cdot x^i \in \mathbb{Z}_{\mathbf{n}}[x]$, где:

  **2)** $a'_d \xleftarrow{\$} \mathbb{Z}_{\mathbf{n}} \setminus \{0\}$

  **2)** $a'_i \xleftarrow{\$} \mathbb{Z}_{\mathbf{n}}, i = \overline{2, d-1}$ ($a'_i$ берутся по равномерному распределению над $\mathbb{Z}_{\mathbf{n}}$)

  **3)** $a'_1 := (a - \sum_{i=2}^{d} a'_i) \bmod \mathbf{n}$

  Тогда имеем:

  $$a \equiv \sum_{i=1}^{d} a'_i (\mathrm{mod}\, \mathbf{n})$$

- Шифртекст $c = \{c_p(x), c_q(x)\} \in \mathbb{Z}_{\mathbf{n}}[x] \times \mathbb{Z}_{\mathbf{n}}[x]$, где:

  $c_p(x) := a'(k_p^{-1} \cdot x) \bmod \mathbf{p}$, и $\Rightarrow c_p(k_p) \equiv a (\mathrm{mod}\, \mathbf{p})$

  $c_q(x) := a'(k_q^{-1} \cdot x) \bmod \mathbf{q}$ , и $\Rightarrow c_q(k_q) \equiv a (\mathrm{mod}\, \mathbf{q})$

**То есть на самом деле все коэффициенты $c_p(x) \in \mathbb{Z}_{\mathbf{n}}[x]$ принадлежат $\{0, ..., p-1\}$, коэффициенты $c_q(x) \in \mathbb{Z}_{\mathbf{n}}[x]$ принадлежат $\{0, ..., q-1\}$.**

# Где гомоморфизм?

Пусть даны $a_i \in \mathbb{Z}_n, i = 1, 2$ и их шифровки $c_i = \{c_{p,i}(x), c_{q,i}(x)\}\}, i = 1, 2$ на одном ключе $k = (k_p, k_q)$.

*По свойствам сравнений имеем:*

- **Сумма:** $c_+ = \{(c_{p,1}(x) + c_{p,2}(x)) \bmod n, (c_{q,1}(x) + c_{q,2}(x)) \bmod n\}$ шифрует $(a_1 + a_2) \bmod n$ на ключе $k$.
- **Произведение:** $c_* = \{(c_{p,1}(x) \cdot c_{p,2}(x)) \bmod n, (c_{q,1}(x) \cdot c_{q,2}(x)) \bmod n\}$ шифрует $(a_1 \cdot a_2) \bmod n$ на ключе $k$.

# Основное свойство секретного ключа

$$a \in \mathbb{Z}_n \longrightarrow c = \{c_p(x), c_q(x)\} \in \mathbb{Z}_{\mathbf{n}}[x] \times \mathbb{Z}_{\mathbf{n}}[x]$$

$$c_p(k_p) \bmod \mathbf{p} \equiv a (\mathrm{mod}\, \mathbf{p})$$

$$c_q(k_q) \bmod \mathbf{q} \equiv a (\mathrm{mod}\, \mathbf{q})$$

*То есть имеем:*

- $k_p$ – корень $\mathbf{f_p}(x) = c_p(x) - a \in \mathbb{Z}_{\mathbf{n}}[x]$ по модулю $p$.
- $k_q$ – корень $\mathbf{f_q}(x) = c_q(x) - a \in \mathbb{Z}_{\mathbf{n}}[x]$ по модулю $q$.
- Но $\mathbf{f_p}(k_p) \not\equiv a (\mathrm{mod}\, \mathbf{n})$, $\mathbf{f_q}(k_q) \not\equiv a (\mathrm{mod}\, \mathbf{n})$.

# План криптоанализа по известным открытым текстам

Пусть у криптоаналитика есть $\mathbf{t}$ пар:
$(a_i \in \mathbb{Z}_{\mathbf{n}}, c_i = \{c_{p,i}(x), c_{q,i}(x)\} \in \mathbb{Z}_{\mathbf{n}}[x] \times \mathbb{Z}_{\mathbf{n}}[x]), i = \overline{1, t}$, где $c_i$ шифрует $a_i$.

Причем все $c_i$ изготовлены на одном ключе $k = (k_p, k_q)$ и $\forall i : deg(c_{p,i}(x)) = d, deg(c_{q,i}(x)) = d$.

**Для того чтоб взломать криптосистему криптоаналитику нужно:**

- *Раскрыть факторизацию* $\mathbf{n}$, *т.е. найти* $\mathbf{p}, \mathbf{q}$.
- *Вычислить* $k_p$ *как общий корень* $\mathbf{f_{p,i}}(x) = c_{p,i}(x) - a_i$ *по модулю* $\mathbf{p}$.
- *Вычислить* $k_q$ *как общий корень* $\mathbf{f_{q,i}}(x) = c_{q,i}(x) - a_i$ *по модулю* $\mathbf{q}$.

# Известные результаты по криптоанализу

**Ранее в литературе был представлен результат состоящий в том, что для того, чтобы раскрыть $\mathbf{p}, \mathbf{q}$ и $k = (k_p, k_q)$ при знании $\mathbf{n} = \mathbf{p} \cdot \mathbf{q}$ криптоаналитику необходимо перехватить $\mathbf{t} \geq \mathbf{d} + 1$ пар (открытый текст, шифртекст), изготовленных на ключе $k$.**

# Существующий метод криптоанализа (вычисление $\mathbf{p}$)

Пусть $\mathbf{t} = \mathbf{d} + \mathbf{1}$, даны $\mathbf{f_{p,i}}(x) = c_{p,i}(x) - a_i = \sum_{j=1}^{d} c_{p,i,j} \cdot x^j - a_i \in \mathbb{Z}_{\mathbf{n}}[x]$, $\mathbf{i} = \mathbf{1}, .., \mathbf{d} + \mathbf{1}$.

$$\mathbf{A} = \begin{pmatrix} -a_1 & c_{p,1,1} & \cdots & c_{p,1,d} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{d+1} & c_{p,d+1,1} & \cdots & c_{p,d+1,d} \end{pmatrix} \quad (1)$$

- СЛАУ $(\mathbf{A}|\mathbf{0})$ имеет решение $(1, k_p, k_p^2, ..., k_p^d)$ по модулю $\mathbf{p} \Rightarrow$ $\mathbf{det}(\mathbf{A}) \bmod \mathbf{p} = \mathbf{0}$ и

  $\Rightarrow \mathbf{det}(\mathbf{A}) \bmod \mathbf{n} = \mathbf{p} \cdot \mathbf{k}$, $\mathbf{k} \in \{\mathbf{0}, ..., \mathbf{q} - \mathbf{1}\}$.

  **Если $\mathbf{k} \neq \mathbf{0}$, то НОД $(\mathbf{det}(\mathbf{A}) \bmod \mathbf{n}, \mathbf{n}) = \mathbf{p}$.**

- $\mathbf{k} = \mathbf{0} \iff \mathbf{det}(\mathbf{A}) \bmod \mathbf{q} = \mathbf{0}$.
- Если $\mathbf{A}$ – матрица с $\approx$ равномерно случайными элементами по модулю $\mathbf{q}$, то $\mathbf{Pr}(\mathbf{det}(\mathbf{A}) \bmod \mathbf{q} \neq \mathbf{0}) \approx \mathbf{1}$ (для большого $\mathbf{q}$).

  *Однако $\mathbf{A}$ будет таковой, если вероятностное распределение $\mathcal{D}$ на открытых текстах будет равномерным (см. 1-й столбец $\mathbf{A}$).*

# Существующий метод криптоанализа (вычисление $\mathbf{k_p}$)

Даны $\mathbf{f_{p,i}}(x) = c_{p,i}(x) - a_i = \sum_{j=1}^{d} c_{p,i,j} \cdot x^j - a_i \in \mathbb{Z}_\mathbf{n}[x]$, $\mathbf{i = 1, .., d + 1}$.

- $\mathbf{f_{p,i}}(k_p) \bmod \mathbf{p} = 0$ и $\Rightarrow$

$$\mathbf{f_{p,i}}(x) \equiv (x - k_p) \cdot \mathbf{g_i}(x) (\mathrm{mod}\, \mathbf{p}),$$

$\mathbf{g_i}(x) \in \mathbb{Z}_\mathbf{p}[x]$ – равномерно случайные.

- $\Rightarrow$ НОД $(\mathbf{f_{p,1}}(x), ..., \mathbf{f_{p,d+1}}(x)) \equiv x - k_p (\mathrm{mod}\, \mathbf{p})$ с вероятностью:

$$\mathbf{1 - \frac{1}{p^{d+1}} + \frac{p-1}{p^{(d+1)^2}}}.$$

# Результант полиномов

Для $\forall \mathbf{f}(x), \mathbf{g}(x) \in \mathbb{Z}_{\mathbf{n}}[x]$, $\mathbf{n} = \mathbf{p} \cdot \mathbf{q}$, можно составить матрицу Сильвестра $\mathbf{S} \in \mathbb{Z}_{\mathbf{n}}^{(\mathbf{d_1}+\mathbf{d_2})\times(\mathbf{d_1}+\mathbf{d_2})}$, где $\mathbf{deg(f)} = \mathbf{d_1}, \mathbf{deg(g)} = \mathbf{d_2}$:

$$\mathbf{S} = \begin{vmatrix} \mathbf{f_0} & \cdots & \mathbf{f_{d_1}} & 0 & 0 & .. & 0 \\ 0 & \mathbf{f_0} & \cdots & \mathbf{f_{d_1}} & 0 & .. & 0 \\ .. & .. & .. & .. & & & \\ 0 & .. & 0 & 0 & \mathbf{f_0} & .. & \mathbf{f_{d_1}} \\ \mathbf{g_0} & .. & \mathbf{g_{d_2}} & 0 & 0 & .. & 0 \\ 0 & \mathbf{g_0} & \cdots & \mathbf{g_{d_2}} & 0 & .. & 0 \\ \vdots & \vdots & \ddots & \vdots & & & \\ 0 & .. & 0 & 0 & \mathbf{g_0} & .. & \mathbf{g_{d_2}} \end{vmatrix} \tag{2}$$

**Результант $\mathbf{f(x), g(x)}$ – $\mathbf{Res(f, g)} := \mathbf{det(S)} \bmod \mathbf{n} \in \mathbb{Z}_{\mathbf{n}}$.**

**Если $\mathbf{f(x), g(x)}$ имеют общий корень по модулю n, то $\mathbf{Res(f, g)} = \mathbf{0}$.**

**Если $\mathbf{f(x), g(x)}$ имеют общий корень по модулю p или q, то $\mathbf{Res(f, g)} \equiv \mathbf{0}$ по модулю p или q.**

# Вычисление $p$ по двум парам

Дано:
$(a_i \in \mathbb{Z}_{\mathbf{n}}, c_i = \{c_{p,i}(x), c_{q,i}(x)\} \in \mathbb{Z}_{\mathbf{n}}[x] \times \mathbb{Z}_{\mathbf{n}}[x]), \mathbf{i} = \mathbf{1}, \mathbf{2}.$

$\mathbf{f_{p,1}}(x) = c_{p,1}(x) - a_1$, $\mathbf{f_{p,2}}(x) = c_{p,2}(x) - a_1 \in \mathbb{Z}_{\mathbf{n}}[x]$

- Так как $\mathbf{f_{p,1}}(k_p) \equiv 0 (\mathrm{mod}\, \mathbf{p})$ и $\mathbf{f_{p,2}}(k_p) \equiv 0 (\mathrm{mod}\, \mathbf{p})$, то

$$\mathcal{R} = \mathbf{Res}(\mathbf{f_{p,1}}(\mathbf{x}), \mathbf{f_{p,2}}(\mathbf{x})) \equiv \mathbf{0} (\mathrm{mod}\, \mathbf{p}).$$

- Тогда $\mathcal{R} = \mathbf{p} \cdot \mathbf{k}$, где $\mathbf{k} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}, ..., \mathbf{q} - \mathbf{1}\}$.
- Если $\mathcal{R} \neq \mathbf{0}$, то $\mathbf{p} = GCD(\mathbf{n}, \mathcal{R})$.
- $\mathcal{R} = 0 \iff \mathcal{R} \bmod \mathbf{q} = 0$ (по Китайской теореме об остатках).

# Какова вероятность, что $\mathcal{R} \bmod \mathbf{q} \neq \mathbf{0}$?

$$\mathbf{f_{p,i}}(x) = c_{p,i}(x) - a_i = \sum_{j=1}^{d} c_{p,i,j} \cdot x^j - a_i \in \mathbb{Z}_{\mathbf{n}}[x], \mathbf{i} = \mathbf{1}, \mathbf{2}$$

- Если предположить, что $\mathbf{f^*_{p,i}}(x) = \mathbf{f_{p,i}}(x) \bmod \mathbf{q}, \mathbf{i} = \mathbf{1}, \mathbf{2}$ – равномерно случайные полиномы $\in \mathbb{Z}_{\mathbf{q}}[x]$, то

$$Pr\{\mathcal{R} \bmod \mathbf{q} \neq \mathbf{0}\} = 1 - \frac{1}{\mathbf{q}}.$$

- Однако на самом деле $\mathbf{f^*_{p,i}}(x) = \sum_{j=0}^{d} \mathbf{f_{i,j}} \cdot x^j, \mathbf{i} = \mathbf{1}, \mathbf{2}$ не будут раномерно случайными, если вероятностное распределение $\mathcal{D}$ на пространстве открытых текстов $\mathbb{Z}_{\mathbf{n}}$ неравномерно.
- И даже если $\mathcal{D}$ равномерно, то $\mathbf{f^*_{p,i}}(x), \mathbf{i} = \mathbf{1}, \mathbf{2}$ строго говоря не будут равномерно случайными в $\mathbb{Z}_{\mathbf{q}}[x]$, поскольку в соответствии с процедурой шифрования: $0 < c_{p,i,j} < \mathbf{p}$.

  Так что: $\mathbf{f_{i,0}} \xleftarrow{\$} \{\mathbf{0}, ..., \mathbf{q} - \mathbf{1}\}$, $\mathbf{f_{i,j}} \xleftarrow{\$} \{\mathbf{0}, ..., \mathbf{p} - \mathbf{1}\}$ для $\mathbf{1} \leq \mathbf{j} \leq \mathbf{d}$.

# Практическая оценка вероятности найти $\mathbf{p}, \mathbf{q}$

Вероятностное распределение $\mathcal{D}$ на пространстве открытых текстов $\mathbb{Z}_{\mathbf{n}}$ полагалось равномерным.

$\mathbf{Pr}_1$ – практическая оценка вероятности, того, что $\mathcal{R} \bmod \mathbf{q} \neq \mathbf{0}$ (при этом для практической оценки вероятности поводилось $\approx 10^5$ итераций.)

$\mathbf{Pr}_2 = 1 - 1/\mathbf{q}$

Таблица: Для $d = 10$

| **n** | **p** | **q** | $\mathbf{Pr}_1$ | $\mathbf{Pr}_2$ |
|---|---|---|---|---|
| 6 | 2 | 3 | 0.67 | 0.67 |
| 35 | 5 | 7 | 0.86 | 0.86 |
| 91 | 7 | 13 | 0.92271 | 0.923 |
| 253 | 11 | 23 | 0.956 | 0.957 |
| 1517 | 37 | 41 | 0.97 | 0.97 |
| 3599 | 59 | 61 | 0.98 | 0.98 |
| 9991 | 97 | 103 | 0.99 | 0.991 |

# Практическая оценка вероятности найти $\mathbf{p}, \mathbf{q}$

Вероятностное распределение $\mathcal{D}$ на пространстве открытых текстов $\mathbb{Z}_{\mathbf{n}}$ полагалось равномерным.

$\mathbf{Pr}_1$ – практическая оценка вероятности, того, что $\mathcal{R} \bmod \mathbf{q} \neq \mathbf{0}$ (при этом для практической оценки вероятности поводилось $\approx 10^5$ итераций.)

$\mathbf{Pr}_2 = 1 - 1/\mathbf{q}$

Таблица: Для $d = 50$

| **n** | **p** | **q** | $\mathbf{Pr}_1$ | $\mathbf{Pr}_2$ |
|---|---|---|---|---|
| 15 | 3 | 5 | 0.8 | 0.8 |
| 221 | 13 | 17 | 0.92 | 0.94 |
| 1147 | 31 | 37 | 0.964 | 0.972 |
| 2173 | 41 | 53 | 0.999 | 0.999 |
| 13943 | 103 | 131 | 0.999 | 0.999 |

# Вычисление $k_p, k_q$

Даны: $\mathbf{f_{p,i}}(x) = c_{p,i}(x) - a_i, \mathbf{f_{q,i}}(x) = c_{q,i}(x) - a_i, \mathbf{i} = 1, 2$

- $\mathbf{f_{p,i}}(k_p) \bmod \mathbf{p} = 0, \mathbf{i} = 1, 2$ и $\Rightarrow$

$$\mathbf{f_{p,i}}(x) \equiv (x - k_p) \cdot \mathbf{g_{p,i}}(x) (\mathrm{mod} \mathbf{p}), \mathbf{i} = 1, 2,$$

$\mathbf{g_{p,i}}(x) \in \mathbb{Z}_{\mathbf{p}}[x]$ – равномерно случайные (*в соответствии с процедурой шифрования*).

- $\Rightarrow$ НОД $(\mathbf{g_{p,1}}(x), \mathbf{g_{p,2}}(x)) \equiv 1 (\mathrm{mod} \mathbf{p})$ с вероятностью $\mathbf{1 - 1/p}$.

- Итого НОД $(\mathbf{f_{p,1}}(x), \mathbf{f_{p,2}}(x)) \equiv x - k_p (\mathrm{mod} \mathbf{p})$ с вероятностью $\mathbf{1 - 1/p}$.
- Аналогично НОД $(\mathbf{f_{q,1}}(x), \mathbf{f_{q,2}}(x)) \equiv x - k_q (\mathrm{mod} \mathbf{q})$ с вероятностью $\mathbf{1 - 1/q}$.

# Оценка вероятности раскрыть $k_p$

$\mathbf{Pr}_1$ – практическая оценка вероятности, того, что НОД$(\mathbf{f_1}(\mathbf{x}), \mathbf{f_2}(\mathbf{x})) = 1$, где $\mathbf{f_1}(\mathbf{x}), \mathbf{f_2}(\mathbf{x})$ – равномерно случайные полиномы из $\mathbb{Z}_\mathbf{p}[x]$ (для практической оценки вероятности поводилось $\approx 10^5$ итераций.)

$\mathbf{Pr}_2 = 1 - 1/\mathbf{p}$

Таблица:

| $\mathbf{p}$ | $\mathbf{Pr}_1$ | $\mathbf{Pr}_2$ |
|---|---|---|
| 2 | 0.48 | 0.5 |
| 23 | 0.7 | 0.7 |
| 103 | 0.99 | 0.9902 |
| 3389 | 1 | 1 |

# Асимптотические оценки сложности криптоанализа

- Вычисление $\mathbf{p}, \mathbf{q}$ потребует не более, чем $\mathbf{O(d^3 \cdot \log_2^2(n))}$ операций по модулю $\mathbf{n}$.
- Вычисление $k_p$ потребует соответственно $\mathbf{O(d^2 \cdot \log_2^2(p))}$ операций по модулю $\mathbf{p}$.
- Вычисление $k_q$ потребует соответственно $\mathbf{O(d^2 \cdot \log_2^2(q))}$ операций по модулю $\mathbf{q}$.

# Время работы атаки

**T** – время затраченное на раскрытие $\mathbf{p}, \mathbf{q}$ и $k = (k_p, k_q)$
$\mathbf{log_2(n)} = 1024$, $\mathbf{log_2(p)} = 512$ $\mathbf{log_2(q)} = 512$

Таблица:

| **d** | **T** |
|---|---|
| 4 | 14 мсек |
| 8 | 38 мсек |
| 16 | 121 мсек |
| 32 | 460 мсек |
| 64 | 1.9 сек |
| 128 | 9.5 сек |
| 256 | 52 сек |
| 512 | 5 мин |
| 1024 | 22 мин |

**Для реализации использовись Qt 1.3.1 и библиотека NTL. Замеры времени проводились на ПК со следующими характеристиками: Quad Core Celerone 1,7 GHz with 4 GB**

# Время работы атаки

**T** – время затраченное на раскрытие $\mathbf{p}, \mathbf{q}$ и $k = (k_p, k_q)$.

$\mathbf{log_2(n)} = 2048$, $\mathbf{log_2(p)} = 1024$ $\mathbf{log_2(q)} = 1024$

Таблица:

| **d** | **T** |
|---|---|
| 4 | 39 мсек |
| 8 | 112 мсек |
| 16 | 387 мсек |
| 32 | 1.5 сек |
| 64 | 6 сек |
| 128 | 27 сек |
| 256 | 2 мин |
| 512 | 12 мин |
| 1024 | 50 мин |

# Заключение

- **Итак, мы получили, что с вероятностью $\approx 1$ криптосистему Доминго Ферре можно взломать при наличии только двух пар (открытый текст, шифртекст).**
- **Однако важно отметить, что как наша, так и предложенная ранее атаки будут гарантированно работать если вероятностное распределение $\mathcal{D}$ на открытых текстов равномерное.**
- **Если $\mathcal{D}$ такое, что $Pr(0)$ не пренебрежительно мала, то вероятность успеха криптоанализа сильно падает.**
- **В случае если $\mathcal{D}$ неравномерно, но при этом $Pr(0) << 1$, нужно допонительное исследование.**
- **В дальнейшем планируется провести более подробный криптоанализ криптосистемы Доминго Ферре только по шифртекстам**

Спасибо за внимание!