М. А. Черепнев

О современных атаках на криптографические протоколы, построенные на эллиптических кривых

1 Спаривание Вейля

Обозначим $E[m]$ множество точек эллиптической кривой E над конечным полем $\mathbb{F}_q$, удовлетворяющих условию

$$[m]T = \overbrace{T + \cdots + T}^{m} = \Theta,$$

где Θ — бесконечно удалённая точка.

Согласно [1, III.3.5] дивизор $\sum n_P P$ является дивизором функции, то есть элемента поля $\mathbb{F}_q(x, y)$ тогда и только тогда, когда

$$\sum n_P = 0, \qquad \sum [n_P]P = \Theta.$$

Пусть $T \in E[m]$. Тогда существует рациональная функция $f \in \overline{\mathbb{F}}_q(x, y)$ с коэффициентами из алгебраического замыкания поля $\mathbb{F}_q$ такая, что дивизор

$$div(f) = mT - m\Theta.$$

Поскольку поле $\overline{\mathbb{F}}_q$ алгебраически замкнуто, то всегда найдётся такая точка $T' \in E$, что $[m]T' = T$. Так как отображение $[m]$ задаётся рациональной функцией, то эту точку можно построить, решив систему из двух уравнений: уравнения кривой и уравнения, выражающего первую координату точки T через координаты точки T', — а затем, в случае необходимости, перейти к алгебраическому сопряжению. Используя эту точку, построим дивизор, так же как и предыдущий, являющийся дивизором некоторой функции:

$$div(g) = \sum_{R \in E[m]} \big((T' + R) - R\big).$$

Поскольку $[m](T' + R) = T$, $[m]R = \Theta$ и показатель ветвления изогении, в данном случае $[m]$, равен степени её несепарабельности [1, III.4.10] (в случае $(m, q) = 1$ — единице по [1, III.5.4]), то в этом случае

$$f \circ [m] = g^m.$$

Можно рассуждать и по-другому: неразветвлённость отображения $[m]$ следует из [1, III.2.7] и того, что при $(m, q) = 1$ выполнено $deg[m] = \sharp E[m]$ [2, 4.73].

Теперь для фиксированной точки $S \in E[m]$ и произвольной точки $X \in E$ получим:

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

Из этого равенства следует, что $g(X + S) = g(X)\mu(X)$, $\mu(X)^m = 1$ в кольце $\overline{\mathbb{F}}_q[x, y]$ рациональных функций кривой. Так как $\overline{\mathbb{F}}_q[x, y]$ является областью целостности, то есть кольцом без делителей нуля, то в этом кольце выполнено: $\mu(X) = \mu$, $\mu^m = 1$. Таким образом определено отображение, называемое *спариванием Вейля*:

$$e_m : E[m] \times E[m] \to \text{подгруппа корней } m\text{-той степени из единицы в } \overline{\mathbb{F}_q}.$$

Такая подгруппа в $\mathbb{F}_{p^k}$, p — простое, существует, если

$$m \mid p^k - 1. \tag{1}$$

Данное отображение обладает рядом очень полезных свойств [1, III.8.1], среди которых:

- $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$,
- $e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$,
- $e_m(S, T) = e_m(T, S)^{-1}$,
- если для любого $S \in E[m]$: $e_m(S, T) = 1$, то $T = 0$,
- если $S \in E[mm'], T \in E[m]$, то $e_{mm'}(S, T) = e_m([m']S, T)$.

Таким образом, если на эллиптической кривой, определённой над полем $\mathbb{F}_p$ имеется группа точек порядка m, то отображение $e_m(\cdot, T)$, где $T \in E[m]$, переводит эту группу в подгруппу $\mathbb{F}^*_{p^k}$, где можно применять алгоритм дискретного логарифмирования с факторной базой и субэкспоненциальной оценкой трудоёмкости.

Для того чтобы этого избежать, необходимо, чтобы для выбранных $m, p = q$ условие (1) не выполнялось для $k = 1, \ldots, 131$. Параметр 131 взят из стандарта ГОСТ Р34.10-2012 и выбран из условия, что субэкспоненциальный алгоритм в $\mathbb{F}^*_{p^{131}}$ работает медленнее алгоритма Полларда в группе порядка m.

2 $(p-1)$-атаки

2.1 О связи между трудоёмкостями задач дискретного логарифмирования и Диффи—Хеллмана

Пусть используемая циклическая группа $\langle P\rangle$ точек кривой имеет простой порядок p. Пусть $p-1=\prod_{i=1}^{t} {q_i}^{\alpha_i}$. В стандарте ГОСТ Р34.10-2012 не указано никаких требований на это разложение, поэтому мы будем считать его имеющим общий вид. А именно, пусть

$$\psi(x,y)=\sharp\{1\leq n\leq x \mid \text{для любого } q\text{, простого делителя } n\text{, имеем } q<y\},$$

тогда при фиксированном $u\geq 3$, $x\geq 1$ [5, Теорема 3.1]

$$\psi(x,\sqrt[u]{x})\geq \frac{x}{u^{u(1+o(1))}}. \tag{2}$$

Таким образом, с вероятностью, равной константе, можно считать, что $q_i\leq \sqrt[u]{p}$ для фиксированного u.

Пусть по двум точкам Q,P на эллиптической кривой $E[\mathbb{F}_r]$ над полем $\mathbb{F}_r$ из простого r числа элементов, связанным равенством

$$Q=[n]P,$$

надо найти n, определённое по модулю $p=\operatorname{ord} P$. Обозначим трудоёмкость этой задачи $DLE(r,p)$, а трудоёмкость вычисления $[n_1n_2]P$ по паре $([n_1]P,[n_2]P)$ обозначим $DHE(r,p)$. Будем полагать, что эта последняя задача не проще одной операции на эллиптической кривой $E[\mathbb{F}_r]$. Символом log будем обозначать логарифм по некоторому фиксированному основанию, значение которого каждый раз будет некоторой эффективной абсолютной константой.

Теорема 1 ([13])

$$DLE(r,p)\leq DHE(r,p)\log p\sum_{i=1}^{t}{q_i}^{\alpha_i}.$$

В общем случае можно считать, что (см. [14])

$$DLE(r,p)\leq O(s(p)\log^2 p\,(DHE(r,p))^{s(p)}),$$

где $s(p)$ — длина наибольшей ветви дерева Пратта [4], для которой на сегодняшний день имеется только тривиальная оценка $s(p)\leq \log_2 p$ (см. некоторое развитие в статье [9]).

Доказанная теорема показывает, в частности, что на подгруппах точек простого порядка p на эллиптических кривых, удовлетворяющих стандарту ГОСТ Р34.10-2012, где $p-1$ раскладывается на «маленькие» простые множители, задачи Диффи—Хеллмана и дискретного логарифмирования полиномиально эквивалентны. Приведённые рассуждения потенциально ослабляют стандарт ГОСТ Р34.10-2012.

2.2 Атака при помощи обращения спаривания

Определение 1 ([3]) *Пусть G_1, G_2, G_T — циклические группы.* Спариванием *назовём отображение*

$$e : G_1 \times G_2 \to G_T.$$

Будем рассматривать билинейные относительно групповых операций невырожденные спаривания.

Пусть f_1, f_2, f_T — единичные элементы групп G_1, G_2, G_T соответственно. Тогда по определению $e(f_1, G_2) = e(G_1, f_2) = f_T$. Рассмотрим случай $|G_1| = |G_2| = |G_T| = p$ — простое. В этом случае невырожденность спаривания e эквивалентна существованию таких g_1, g_2, g_T — соответственно из множеств $G_1 \setminus f_1$, $G_2 \setminus f_2$, $G_T \setminus f_T$,— что $e(g_1, g_2) = g_T$. При этом для любых $h_1 \in G_1$, $h_T \in G_T$ существует $h_2 \in G_2$ и для любых $h_2 \in G_2$, $h_3 \in G_T$ существует $h_1 \in G_1$ такие, что $e(h_1, h_2) = h_T$.

Рассмотрим следующие задачи [3]:

$$\begin{aligned}
\text{FAPI-1:} &\quad D_1 \in G_1,\ z \in G_T \to D_2 \in G_2 : e(D_1, D_2) = z,\\
\text{FAPI-2:} &\quad D_2 \in G_2,\ z \in G_T \to D_1 \in G_1 : e(D_1, D_2) = z,\\
\text{GPI-2:} &\quad z \in G_T \to D_1 \in G_1, D_2 \in G_2 : e(D_1, D_2) = z.
\end{aligned}$$

Трудоёмкости решения этих задач обозначим соответственно I_1, I_2, I_T, соответствующие оракулы O_1, O_2, O_T, а трудоёмкость вычисления спаривания обозначим C. Ввиду предполагаемой простоты p и невырожденности спаривания, решение FAPI-i единственно. Обозначим $DH(G_i)$ трудоёмкость решения задачи Диффи—Хеллмана в группе G_i.

Теорема 2 ([3, Theorem 1])

$$DH(G_i) \le I_1 + I_2 + 2C, \quad i \in \{1, 2\}. \tag{3}$$

Для дальнейшего будет важен случай, когда G_2 конечная группа, вообще говоря, не простого порядка, но имеющая универсальную экспоненту, равную p.

Трудоёмкость решения задачи FAPI-2 в этом случае (нахождение хотя бы одного решения) будем обозначать $\tilde{I}_2$.

Аналогично доказательству теоремы 2 можно получить следующую оценку. Пусть (P, aP, bP) — элементы G_1, являющиеся входом для задачи Диффи—Хеллмана в группе G_1. Вычислим $z = e(aP, Q) = e(P, aQ)$ для случайного аргумента $Q \in G_2$ такого, что $z \neq f_T$. Вычисляем $O_1(P, z) = \tilde{Q}$ такое, что $e(P, \tilde{Q}) = e(aP, Q)$. Такое $\tilde{Q}$ существует, например $\tilde{Q} = aQ$. Вычислим $z' = e(bP, \tilde{Q}) = e(abP, Q)$. Вычисляем $O_2(z', Q) = abP$. Таким образом, имеем следующую оценку на трудоёмкость задачи Диффи—Хеллмана в группе G_1:

$$DH(G_1) \leq I_1 + \tilde{I}_2 + 2C, \quad i \in \{1, 2\}.$$

Применяя теорему 1, находим, что

$$DLE(r, p) \leq \log p \, (I_1 + \tilde{I}_2 + 2C) \sum_{i=1}^{t} q_i^{\alpha_i}.$$

Рассмотрим функцию $f_{s,Q}$ для произвольного целого s как функцию, определённую равенством

$$div(f_{s,Q}) = s(Q) - (sQ) - (s-1)(\infty). \tag{4}$$

Такая функция существует согласно [1, III.3.5]. В ряде случаев значение спаривания [10, 11] задаётся формулой

$$f_{s,Q}(D_2) = \prod_{P \in \operatorname{Supp} D_2} f_{s,Q}(P)^{v_P(D_2)}.$$

Пусть u — униформизующий параметр в бесконечности, а $v_\infty(f)$ — порядок функции f в бесконечности, тогда обозначим $lc_\infty(f) = (u^{-v_\infty(f)} f)(\infty)$. При этом будем обозначать $f^{norm} = (lc_\infty(f))^{-1} f$. Для получения однозначного определения $f_{s,Q}(D_2)$ заменим f на f^{norm}.

Значения вида $f_{s,Q}(D_2)$ и использующие их спаривания могут быть вычислены при помощи алгоритма Давенпорта [7] — Миллера [8] и его обобщений [2]. Этот алгоритм линеен относительно длины входа, поэтому трудоёмкость вычисления, например, спаривания Вейля будет $O(k \log r)$ операций в поле $\mathbb{F}_q$, $q = r^k$, или $O(k^3 \log^3 r)$ битовых операций.

Кроме того, пошаговые вычисления в алгоритме Миллера показывают, что спаривание Вейля является рациональной функцией степени не выше $8s^2$.

Пусть r — простое число, E — эллиптическая кривая, определённая над $\mathbb{F}_r$, и (∞) — бесконечно удалённая точка. Символом p обозначим большой простой

делитель числа $\sharp E(\mathbb{F}_r)$ — порядка группы $\mathbb{F}_r$-точек кривой $E(\mathbb{F}_r)$, а символом k — наименьший натуральный, для которого $p \mid r^k - 1$.

Пусть $P \in G_1 = E[p] \cap Ker(\pi_r - [1])$ и $Q \in G_2 = E[p] \cap Ker(\pi_r - [r])$. Для каждого целого s пусть $f_{s,Q}$ — рациональная функция на E с дивизором (4).

Пусть $s = r^i \pmod p$ для некоторого целого i. Пусть D — дивизор, эквивалентный $(P) - (\infty)$, носитель которого не пересекается с $\mathrm{Supp}(f_{s,Q})$. Тогда по [12, Theorem 1] (редуцированное) обобщённое спаривание Эйта

$$e(P,Q) = f_{s,Q}(D)^{\frac{r^k-1}{p}}, \quad f_{s,Q}(D) = \prod_{R \in \mathrm{Supp}\, D} f_{s,Q}(R)^{v_R(D)},$$

является невырожденным билинейным отображением $G_1 \times G_2$ в подгруппу корней p-й степени из единицы мультипликативной группы $\mathbb{F}_{r^k}^*$, если

$$\gamma_p(s^{\mathrm{ord}_p\, s} - 1) \le \gamma_p(r^k - 1), \tag{5}$$

где $\gamma_p(x)$ — степень вхождения p в x, а ord_p — порядок по модулю p.

Рассмотрим нередуцированное обобщённое спаривание Эйта

$$\tilde{e}(P,Q) = f_{s,Q}(D)$$

как отображение $G_1 \times E(\mathbb{F}_{r^k})$ в $\mathbb{F}_{r^k}^*/(\mathbb{F}_{r^k}^*)^p$. Это отображение корректно определено, так как $\tilde{e}([p]P, E(\mathbb{F}_{r^k})) \in (\mathbb{F}_{r^k}^*)^p$, то есть является единицей факторгруппы. $\tilde{e}(P,(\infty)) = 1$ по определению. Поскольку дивизор вида (4) при любом s является дивизором функции, то это отображение является гомоморфизмом. В случае выполнения условия (5) по теореме [12, Theorem 1] этот гомоморфизм также является невырожденным.

Если все возможные s велики, использование спаривания $f_{s,h,Q}(P)$ из работы [10] может быть эффективным.

Из алгоритма Миллера [8] получаем $f_{s,Q}(x,y)$ или $f_{s,(x,y)}(P)$ в виде рациональных функций

$$\frac{f_1(x,y)}{f_2(x,y)}, \quad deg_x(\frac{f_1}{f_2}),\ deg_y(\frac{f_1}{f_2}) \le 8s^2.$$

Для фиксированного $P \in G_1$ имеем $x, y \in \mathbb{F}_{r^k}$ и $f_1(x,y), f_2(x,y) \in \mathbb{F}_r(x,y)$. Для фиксированного $Q \in G_2$ имеем $x, y \in \mathbb{F}_r$ и $f_1(x,y), f_2(x,y) \in \mathbb{F}_{r^k}(x,y)$. Без ограничения общности будем пользоваться оценкой $deg_x f_i(x,y) = O(s^2)$, $deg_y f_i(x,y) = 1$.

В работе [16] обращение спаривания сводится к решению системы полиномов от нескольких переменных, степень которых есть минимальный вектор некоторой целочисленной решетки.

В результате эксперимента с пятизначными простыми малых векторов в таких решётках найти не удалось (координаты минимального вектора в основном пятизначные). Ситуация существенно не улучшилась при добавлении в рассматриваемую решётку векторов показателей, которые дают корни из единицы не очень большой степени, которые можно было бы потом перебрать.

Для решения поставленной задачи [13] воспользуемся нередуцированным обобщённым спариванием Эйта в случае, когда оно невырожденно. Значения этого спаривания лежат в факторгруппе $\mathbb{F}_{r^k}^*/(\mathbb{F}_{r^k}^*)^p$. Таким образом, обращение такого спаривания может быть сведено к решению уравнения

$$\frac{f_1(x,y)}{f_2(x,y)} = z(\tilde{z})^p, \quad \tilde{z} \in \mathbb{F}_{r^k}^*. \tag{6}$$

Для уменьшения степени в правой части этого уравнения рассмотрим i : $r^i \equiv s \pmod p$. Предположим, что s мало и выполнено условие (5). Пусть, кроме того, $t = \frac{r^i - s}{p}$, $(t, \frac{r^k-1}{p}) = 1$. Если это условие не выполняется, нужно рассмотреть удовлетворяющее этому условию $t = \frac{\sum \alpha_i r^i}{p} \in \mathbb{Z}$ с маленькими целыми значениями α_i (по модулю меньшими, чем s^2). Если считать вычеты $\sum \alpha_i r^i \pmod p$, а также $\frac{\sum \alpha_i r^i}{p} \pmod{\frac{r^k-1}{p}}$, при $\frac{\sum \alpha_i r^i}{p} \in \mathbb{Z}$, случайными, то с хорошей вероятностью это произойдёт при $(2s^2)^k > 2p \ln\ln \frac{r^k-1}{p}$, или при

$$s^k > p. \tag{7}$$

Вместо уравнения (6) будем рассматривать аналогичное:

$$\frac{f_1(x,y)}{f_2(x,y)} = z(\tilde{z})^{pt}, \quad \tilde{z} \in \mathbb{F}_{r^k}^*.$$

Поскольку $pt \equiv r^i - s \pmod{r^k - 1}$, получим

$$\frac{f_1(x,y)}{f_2(x,y)} = z(\tilde{z})^{r^i - s}. \tag{8}$$

В случае фиксированного Q имеем $x, y \in \mathbb{F}_r$ и $deg(\frac{f_1(x,y)}{f_2(x,y)}) = O(s^2)$.

Элемент $\tilde{z} \in \mathbb{F}_{r^k}$ может быть представлен в нормальном базисе [18]:

$$\tilde{z} = z_1\theta^{r^0} + z_2\theta^{r^1} + \cdots + z_k\theta^{r^{k-1}}, \quad z_i \in \mathbb{F}_r,$$

$$\tilde{z}^{r^i} = z_{1-i \pmod k}\theta^{r^0} + \cdots + z_{k-i \pmod k}\theta^{r^{k-1}}.$$

Произведение таких элементов может быть записано в той же форме с коэффициентами, являющимися квадратичными формами от исходных коэффициентов. Умножая на знаменатель, получим

$$\Phi(x, y, z_1, \ldots, z_k) = 0, \quad \Phi \in \mathbb{F}_{r^k}[x, y], \quad deg\Phi = O(s^2).$$

В случае $\sharp E(\mathbb{F}_r) = p$ любое решение системы, состоящей из этого уравнения и уравнения кривой, даёт точку, принадлежащую $\langle P \rangle$.

В случае фиксированного P, в (8) получим $x, y \in \mathbb{F}_{r^k}$, которые, как и выше, могут быть представлены в нормальном базисе:

$$x = x_1\theta^{r^0} + x_2\theta^{r^1} + \cdots + x_k\theta^{r^{k-1}}, \quad x_i \in \mathbb{F}_r,$$
$$y = y_1\theta^{r^0} + y_2\theta^{r^1} + \cdots + y_k\theta^{r^{k-1}}, \quad y_i \in \mathbb{F}_r.$$

Таким образом, в обоих случаях, представив z, $\tilde{z}$ и коэффициенты многочленов из $\mathbb{F}_{r^k}$ в нормальном базисе и собрав коэффициенты при θ^{r^i}, за $O(s^2k^2)$ арифметических операций в $\mathbb{F}_r$ можно представить уравнение (8) как систему из k уравнений степени $O(s^2)$ над $\mathbb{F}_r$ от $x, y, z_1, \ldots, z_k$ или $x_1, \ldots, x_k$; $y_1, \ldots, y_k$; $z_1, \ldots, z_k$, лежащих в $\mathbb{F}_r$. Уравнение кривой $y^2 = x^3 + \alpha x + \beta$ даст ещё одно или k уравнений над $\mathbb{F}_r$ соответственно. Общая система из этих уравнений может быть решена методами, использующими базис Грёбнера, или другими методами решения полиномиальных систем когда s, k невелики. Оценка трудоёмкости применения в этом случае (переменных больше, чем уравнений) алгоритма F_5 [20]

$$O(k(s^2)^{3 \cdot 3k}), \tag{9}$$

что, очевидно, является оценкой трудоёмкости всего алгоритма обращения спаривания.

Важно напомнить, что, как было замечено в [17], поскольку p простое, то из $d = \mathrm{ord}_p s$, $s \equiv r^i \pmod p$ следует, что p делит значение кругового многочлена $Q_d(s)$. Откуда $s \geq p^{\frac{1}{d}} \geq p^{\frac{1}{k}}$. При этом условие (7) выполняется, но при подстановке в (9) получается слишком большая оценка трудоёмкости. Однако, если рассматриваемая система полиномиальных уравнений не является полурегулярной (см. [21]), например как в случае HFE, она решается теми же алгоритмами намного быстрее.

В систему полиномиальных уравнений, которую мы предлагаем решать, можно включать уравнения, полученные из уравнений вида

$$\tilde{e}([m]P, Q) = z^m(\tilde{z}_1)^p, \quad \tilde{e}(P, [m]Q) = z^m(\tilde{z}_2)^p, \quad \tilde{z}_i \in \mathbb{F}^*_{r^k}.$$

Также отметим, что вместо нормального базиса можно использовать любой другой. Автоморфизм Фробениуса действует в этом базисе как некоторый линейный оператор.

Список литературы

[1] Silverman J. The Arithmetic of Elliptic Curves. Springer, 1986. $513 + xviii$ p.

[2] Cohen H., Frey G. et al. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall, 2006.

[3] Galbraith S., Hess F., Vercauteren F. Aspects of pairing invertion // IEEE Trans. on Information Theory. V. 54 (2008), issue 12. P. 5719–5728.

[4] Pratt V. Every prime has a succinct certificate // SIAM J. Comput. V. 4 (1975), no. 3. P. 214–220.

[5] Canfield E. R., Erdős P., Pomerance C. On a problem of Oppenheim concerning "Factorisatio Numerorum" // J. Number Theory. V. 17 (1983). P. 1–28.

[6] Selivanov B. I. On waiting time in the scheme random allocation of coloured particles // Discrete Math. Appl. V. 5 (1995), no. 1. P. 73–82.

[7] Davenport J. H. On the Integration of Algebraic Functions. LNCS, v. 102. Springer, 1979.

[8] Miller V. S. Short programs for functions on curves. Unpublished manuscript. 1986. `http://crypto.stanford.edu/miller/`

[9] Ford K., Konyagin S. V., Luca F. Prime chains and Pratt trees // Geom. Funct. Anal. V. 20 (2010). P. 1231–1258.

[10] Hess F. Pairing lattices // S. D. Galbraith, K. G. Paterson (eds). Pairing Based Cryptography (Pairing 2008). LNCS, v. 5209. Springer, 2008. P. 18–38.

[11] Hess F. A note on the Tate pairing of curves over finite fields // Arch. Math. (Basel). V. 82 (2004). P. 28–32.

[12] Chang-An Zhao, Fangguo Zhang and Jiwu Huang. A Note on the Ate Pairing // Cryptology ePrint Archive. Report 2007/247. `http://eprint.iacr.org/2007/247.pdf`

[13] Черепнёв М. А. Обращение спариваний для решения задачи дискретного логарифмирования // Фундаментальная и прикладная математика. Т. 18 (2013), вып. 4. С. 185–195.

[14] Cherepnev M. A. On the connection between discrete logarithms and the Diffie–Hellman problem // Discrete Math. V. 8 (1996), no. 3. P. 22–30.

[15] Vasilenko O. N. Number-Theoretic Algorithms in Cryptography. AMS, 2006. 328 p.

[16] Vercauteren F. The hidden root problem // S. D. Galbraith, K. G. Paterson (eds). Pairing Based Cryptography (Pairing 2008). LNCS, v. 5209. P. 89–99. Springer, 2008. http://eprint.iacr.org/2008/261.pdf

[17] Vercauteren F. Optimal pairings // IEEE Trans. on Information Theory. V. 56 (2010), no. 1. P. 455–461. http://eprint.iacr.org/2008/096.pdf

[18] Ван дер Варден Б. Л. Алгебра. М.: Наука, 1976. 648 с.

[19] Gradshteyn I. S., Ryzhik I. M. Tables of Integrals, Series, and Products. (6th ed.) Academic Press, 2000. P. 1111–1112.

[20] Faugère J. C., Din M. S., Verron T. On the complexity of computing Gröbner bases for quasi-homogeneous systems // ISSAC '13, June 26–29, 2013, Boston, Massachusetts, USA. P. 189–196.

[21] Bardet M., Faugère J. C., Salvy B. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$ // INRIA, rapport de recherche N 5049. Décembre 2003.