УДК 512.772.7

ГРАНИЦЫ СБАЛАНСИРОВАННОЙ СТЕПЕНИ ВЛОЖЕНИЯ ДЛЯ КРИПТОГРАФИИ НА БИЛИНЕЙНЫХ СПАРИВАНИЯХ

С. А. Новоселов

Балтийский федеральный университет им. И. Канта, г. Калининград, Россия

Вводится формула для расчёта границ сбалансированной степени вложения гиперэллиптической кривой. Вычислены текущие границы для кривых рода 1–3. Для кривых с известными алгоритмами генерации, наименьшими ρ-значениями и степенями вложения от 1 до 10 вычислен диапазон значений, которому принадлежит уровень безопасности кривой.

Ключевые слова: *криптография, гиперэллиптические кривые, задача дискретного логарифмирования, билинейные спаривания, степень вложения.*

DOI 10.17223/20710410/32/5

ON BOUNDS FOR BALANCED EMBEDDING DEGREE

S. A. Novoselov

Immanuel Kant Baltic Federal University, Kaliningrad, Russia

E-mail: snovoselov@kantiana.ru

A generalized formula for calculating bounds for the balanced value of the hyperelliptic curve embedding degree is proved. Using this formula we give bounds for curves of genus 1–3 over finite fields with the small, medium and big characteristic. We also compute possible range of security level for curves with known generation methods, minimal ρ-value and embedding degrees $k = 1, 2, \ldots, 10$.

Keywords: *hyperelliptic curve cryptography, pairings, embedding degree, discrete logarithm problem.*

Введение

Криптография, основанная на билинейных спариваниях, — активно развивающаяся в настоящее время область исследований. Впервые билинейные спаривания были использованы в криптографии А. Менезесом, Т. Окамото и С. А. Ванстоуном для проведения атаки на суперсингулярные эллиптические кривые путём сведения дискретного логарифма на эллиптической кривой к дискретному логарифму в конечном поле [1], в котором существуют более эффективные алгоритмы вычисления дискретного логарифма. Данный метод подходит также и для других классов кривых, на которых возможно эффективное вычисление спариваний.

Позже в 2000 г. были предложены первые конструктивные приложения спариваний — схема цифровой подписи и схема распределения ключей [2], трёхсторонний протокол Диффи — Хеллмана [3]. После этого было разработано большое число криптосистем, основанных на спариваниях, среди которых выделяется IBE [4]. Обзор таких криптосистем можно найти в работе [5].

Безопасность и эффективность данных криптосистем зависит от двух параметров — степени вложения k и минимальной степени вложения k'. Степень вложения k определяет размер поля, над которым вычисляется билинейное спаривание; соответственно от данного параметра зависит скорость работы криптосистемы. Минимальная степень вложения k', введённая в работе [6], определяет минимальный размер поля, к которому сводится задача вычисления дискретного логарифма в якобиане кривой и, следовательно, является параметром, размер которого определяет безопасность криптосистемы. Эти параметры совпадают в случае, если кривая задана над простым конечным полем. Для случая непростого поля некоторые условия даны в работе [7]. Если параметры совпадают, то k является характеристикой безопасности кривой.

Степень вложения должна быть достаточно большой, чтобы сведение к конечному полю не позволяло решить проблему за меньшее время. С другой стороны, размер степени вложения влияет на эффективность вычисления функции спаривания, которая является основой для криптосистем на спариваниях, поэтому для построения эффективных криптосистем степень вложения должна быть как можно меньше. В связи с этим необходимо выбирать сбалансированное значение k — такое, что сложность решения задачи вычисления дискретного логарифма в якобиане гиперэллиптической кривой равна сложности решения задачи в конечном поле.

Для эллиптических кривых в работе [8] есть асимптотическая оценка, рассчитанная для актуальных по состоянию на 2008 г. алгоритмов дискретного логарифмирования в конечном поле со сложностью $\approx e^{(\ln q)^{1/3}}$. В связи с появлением принципиально новых методов дискретного логарифмирования в конечном поле [9, 10] эта оценка больше не является верной в общем случае.

Целью данной работы является вывод более общей формулы для оценки размера сбалансированного значения k для гиперэллиптических кривых, включающей в себя оценки других авторов как частный случай. Кроме того, проводится сравнение размера сбалансированного значения для разных кривых, различных комбинаций используемых алгоритмов решения задачи вычисления дискретного логарифма и разных типов конечных полей.

Работа организована следующим образом. П. 1 содержит основные определения, предварительные сведения и оценки других авторов для сбалансированной степени вложения. В п. 2 проводится обзор алгоритмов решения задачи вычисления дискретного логарифма в исследуемых группах с выбором наилучших на момент написания работы. Оценки сложности данных алгоритмов и значения констант в них используются для расчётов и вывода формул в последующих пунктах. В п. 3 выводятся общие формулы для расчёта границ сбалансированной степени вложения, позволяющие получить диапазон значений, которому она принадлежит. В п. 4 вводится понятие уровня безопасности, которое необходимо для сравнения кривых. Выводятся формулы для расчёта сбалансированной степени вложения, размеров групп и полей, необходимых для обеспечения заданного уровня безопасности. В п. 5 на основе предыдущих результатов выводится формула для вычисления диапазона уровней безопасности, которому принадлежит уровень безопасности заданной эллиптической или гиперэллиптической кривой с некоторой фиксированной степенью вложения. Кроме того, по выведенной формуле рассчитываются диапазоны уровней безопасности для кривых, предложенных в литературе для использования в криптографии на билинейных спариваниях, и выделяются классы кривых, небезопасные для использования в настоящее время.

1. Предварительные сведения

Определение 1. Пусть G_1, G_2, G_3 — группы порядка n. Билинейным спариванием называется отображение

$$e_n : G_1 \times G_2 \to G_3$$

со следующими свойствами:

1) билинейность:

$$\forall P \in G_1 \, \forall Q, R \in G_2 \ (e_n(P, Q + R) = e_n(P, Q)e_n(P, R)),$$
$$\forall P, R \in G_1 \, \forall Q \in G_2 \ (e_n(P + R, Q) = e_n(P, Q)e_n(R, Q));$$

2) невырожденность:

$$\forall P \in G_1 \setminus \{0\} \ \exists Q \in G_2 \ (e_n(P, Q) \neq 1),$$
$$\forall Q \in G_2 \setminus \{0\} \ \exists P \in G_1 \ (e_n(P, Q) \neq 1).$$

Пусть C — гиперэллиптическая кривая рода g; r — простое число, такое, что $r|\#Jac_C(\mathbb{F}_q)$.

Большинство билинейных спариваний являются модификациями спаривания Тейта — Лихтенбаума, которое определяется как невырожденное билинейное отображение:

$$Jac_C(\mathbb{F}_{q^k})[r] \times Jac_C(\mathbb{F}_{q^k})/rJac_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r.$$

Число k называется степенью вложения кривой C. Если r и q взаимно просты, то степень вложения определяется как наименьшее целое k, такое, что $r|q^k - 1$. Если q не взаимно просто с r, то имеем $r = p$, и подгруппа порядка r не подходит для криптографии на спариваниях, так как задача вычисления дискретного логарифма в $Jac_C(\mathbb{F}_{q^k})[p]$ решается за полиномиальное время от $\log q$ [11].

В [6] введён второй параметр безопасности k', который называется минимальной степенью вложения. Если $q = p^m$, то $k' = ord_r p/m \in \mathbb{Q}$. Этот параметр определяет минимальное поле вложения $\mathbb{F}_{q^{k'}}$, в котором содержится группа корней из единицы.

На практике спаривание вычисляется с помощью алгоритма Миллера [12] и его модификаций, которые имеют сложность $\mathrm{O}(\log r)$. Так как спаривание вычисляется над полем $\mathbb{F}_{q^k}$, сложность операции в котором $\mathrm{O}(k \log q)$, для эффективности вычислений k должно быть мало — асимптотически как полиномиальная функция от битового размера поля: $k = O((\log q)^{c_k})$.

Известно, что большая часть кривых имеет экспоненциальную степень вложения. Небольшую степень вложения имеют малые классы кривых, многие из которых специально подобраны для использования в криптосистемах на спариваниях. Обзор и методы построения таких кривых есть в работах [13, 14] и п. 5.5.

Так как с помощью спариваний дискретный логарифм в группе точек эллиптической кривой или в якобиане гиперэллиптической кривой сводится к дискретному логарифму в конечном поле, для безопасного использования криптосистем на спариваниях должно выполнятся неравенство

$$C_{DLP}(\mathbb{F}_{q^k}^{\times}) \geqslant C_{DLP}(Jac_C(F_q)),$$

где $C_{DLP}(G)$ — сложность решения дискретного логарифма в группе G. Вследствие того, что при увеличении k увеличивается время вычисления спаривания, для приложений необходимо, чтобы k было сбалансировано, т. е. выполнялось равенство

$$C_{DLP}(F_{q^k}^{\times}) \approx C_{DLP}(Jac_C(F_q)).$$

В случае эллиптических кривых в [8] есть оценка

$$k \approx \alpha(c,\rho)\left(\frac{\log r}{\log\log r}\right)^2, \tag{1}$$

где $\rho = \log q/\log r$; $\alpha \approx 1/100\rho$. Заметим, что эта оценка рассчитывалась для алгоритмов дискретного логарифмирования в конечном поле со сложностью $L_q(1/3, c)$.

В 2013 г. появилось улучшение метода исчисления индексов [9], на порядок уменьшающее сложность в случае малой характеристики с $L_q(1/3)$ до $L_q(1/4)$. Кроме того, появился новый теоретический квазиполиномиальный алгоритм [10]. Поэтому оценка k из формулы (1) больше не работает в общем случае.

2. Задача вычисления дискретного логарифма

2.1. Общий случай

Пусть G — аддитивная группа порядка n; g, h — элементы этой группы. Задача вычисления дискретного логарифма (ВДЛ) состоит в следующем: по паре (g, h) найти такое число l, что $h = lg$, если такое число существует. В случае мультипликативной группы задача формулируется аналогично.

В общем случае задача ВДЛ решается за время $\mathrm{O}(\sqrt{n})$ с помощью алгоритма Шенкса или ρ-метода Полларда [15]. Если $n = \prod\limits_i p_i^{e_i}$ — разложение порядка группы на простые множители, то задача решается за время $\mathrm{O}\left(\sum\limits_i e_i(\log n + \sqrt{p_i})\right) = \mathrm{O}(\max\sqrt{p_i})$ с помощью алгоритма Полига — Хеллмана [16]. Поэтому далее ограничимся случаем, когда порядок группы n — большое простое число, которое обозначим r; соответственно в данном случае сложность ВДЛ равна $\mathrm{O}(\sqrt{r})$.

2.2. Конечные поля

Пусть $\mathbb{F}_q$ — конечное поле; $q = p^m$; p — простое число.

В конечных полях существуют более эффективные алгоритмы решения задачи ВДЛ, основанные на методе исчисления индексов — метод решета числового поля (NFS), метод решета функционального поля (FFS) и их модификации. Сложность решения и выбор оптимального алгоритма зависят от соотношения между характеристикой p и степенью поля m. Для выражения сложности этих алгоритмов, а также соотношения между p и m используется L-нотация:

$$L_x(\alpha, c) = e^{(\ln x)^\alpha (\ln\ln x)^{1-\alpha}(c+\mathrm{o}(1))},$$

где $0 \leqslant \alpha \leqslant 1$; $c > 0$. При этом:

1) если $\alpha = 0$, то сложность полиномиальная от $\ln q$;
2) если $\alpha = 1$, то сложность экспоненциальная;
3) если $0 < \alpha < 1$, то сложность субэкспоненциальная.

Параметр α наиболее важен, так как он определяет состояние между экспоненциальной сложностью и полиномиальной. Поэтому часто используется сокращенный вариант записи $L_x(\alpha)$, при котором константа c опускается.

Обозначим соотношение между p и m как $p = L_{p^m}(l_p, c)$. Выделяют [17] три случая:

1) малая характеристика: $l_p \leqslant 1/3$;
2) средняя характеристика: $1/3 \leqslant l_p \leqslant 2/3$;
3) большая характеристика: $l_p \geqslant 2/3$.

В граничных случаях доступно несколько алгоритмов, и выбирается наилучший.

Малая характеристика

В случае малой характеристики наилучший алгоритм имеет сложность $L_q(1/4 + o(1), c)$ [9]. Существует также теоретический алгоритм [10], имеющий квазиполиномиальное время $2^{O((\log\log q)^2)}$, который, однако, имеет большой размер константы. Данные алгоритмы основаны на недоказанных формально гипотезах, но получили подтверждение при вычислениях дискретных логарифмов на практике [18, 19]. Поэтому в настоящее время поля малой характеристики считаются небезопасными для криптографии, основанной на дискретном логарифмировании. С историей вопроса можно ознакомиться в работе [20].

Средняя и большая характеристика

В случае средней характеристики наилучшие алгоритмы имеют сложность $L_q(1/3)$. Наиболее эффективные алгоритмы — MNFS [21] с константой $c = \left(8(9+4\sqrt{6})/15\right)^{1/3} \approx$ $\approx 2{,}156$ и exTNFS [22] с константой $c = \sqrt[3]{48/9} = 1{,}747$.

Для большой характеристики наилучший алгоритм — также MNFS [23] со сложностью в этом случае

$$L_q\left(\frac{1}{3}, \left(\frac{92+26\sqrt{13}}{27}\right)^{1/3}\right).$$

Информация по алгоритмам решения задачи ВДЛ в конечных полях приведена в табл. 1.

Таблица 1

Алгоритмы дискретного логарифмирования в конечных полях

Алгоритм	Характеристика	Сложность
BGJT [10]	Малая	$2^{O((\ln\ln q)^2)}$
Joux [9]	Малая	$L_q(1/4 + o(1), c)$
MNFS [21]	Средняя	$L_q(1/3, 2{,}156)$
exTNFS [22]	Средняя	$L_q(1/3, 1{,}747)$
MNFS [23]	Большая	$L_q(1/3, 1{,}901)$

2.3. Эллиптические кривые

Для эллиптических кривых в общем случае лучший алгоритм — ρ-метод Полларда, имеющий сложность $O(\sqrt{r})$. В специальных случаях возможно сведение проблемы к конечному полю [1, 24], изучаемое в данной работе, либо к кривым высокого рода с использованием спуска Вейля [25, 11]. Последний метод применим только для композитных полей с числом элементов $q = p^m$, где m — составное число. При этом в общем случае методы, основанные на спуске Вейля, не обязательно ведут к более эффективному решению задачи, но для использования кривых над композитными полями в криптографии необходимо доказывать неприменимость данной атаки. Поэтому обычно требуется, чтобы m было простым числом. Заметим, что спуск Вейля также применим и к более общему случаю гиперэллиптических кривых. Для некоторых классов эллиптических кривых доступен метод исчисления индексов [26] с асимптотической сложностью

$$2^{c\sqrt{\log q \log\log q}} = L_q(1/2, c\ln 2), \quad c \approx 1{,}69.$$

2.4. Гиперэллиптические кривые

Пусть C — гиперэллиптическая кривая рода g над полем $\mathbb{F}_q$, $G \subseteq Jac_C(\mathbb{F}_q)$ — подгруппа простого порядка r.

В общем случае задача дискретного логарифмирования на гиперэллиптических кривых может быть решена с помощью ρ-метода Полларда, имеющего сложность $\mathrm{O}(\sqrt{r})$. Однако для кривых рода $g \geqslant 3$ существуют более эффективные методы, основанные на методе исчисления индексов.

Кривые рода 2

Для кривых рода 2 в общем случае наилучший алгоритм — ρ-метод Полларда со сложностью $\mathrm{O}(\sqrt{r}) = O(q)$ (табл. 2). Поэтому гиперэллиптические кривые рода 2 и эллиптические кривые в настоящее время считаются наиболее подходящими для криптографии.

Таблица 2

Алгоритмы дискретного логарифмирования на гиперэллиптических кривых

Алгоритм	Род g	Сложность
ρ-метод Полларда	Любой	$L_r(1, 0{,}5)$
Semaev [26]	1	$L_r(1/2, 1{,}171)$
GTTD [27]	$g \geqslant 3$, $q > g!$	$L_r(1, (2-2/g)\rho/g)$
Enge — Gaudry [28]	$g > \mathrm{O}(\log q)$	$L_r(1/2, 1{,}414)$
Enge — Gaudry — Thome [29]	$g > \mathrm{O}(\log q)^2$	$L_r(1/3, 1{,}922)$

Кривые малого рода $g \geqslant 3$

В случае малого рода $g \geqslant 3$ существуют методы ВДЛ со сложностью $\tilde{\mathrm{O}}(q^{2-2/g})$, если $q > g!$ [27]. Заметим, что данный алгоритм зависит от ρ-значения — соотношения между размером якобиана и размером подгруппы — и превосходит ρ-метод Полларда только при $\rho < g^2/(4(g-1))$.

Кривые большого рода

Если род g достаточно большой по сравнению с q, то задача решается за субэкспоненциальное время от q^g с помощью метода исчисления индексов.

Теорема 1 (Enge — Gaudry [28]). Предположим, что $g > \vartheta \log(q)$, где ϑ — константа. Тогда существует алгоритм, который решает задачу ВДЛ на гиперэллиптических кривых за время $\mathrm{O}(L_{q^g}(1/2, c(\vartheta)))$, где q, g, ϑ стремятся к бесконечности, а $c(\vartheta)$ — функция, стремящаяся к $\sqrt{2}$.

3. Сбалансированное значение k

Пусть C — гиперэллиптическая кривая рода g над полем $\mathbb{F}_q$, $G \subseteq Jac_C(\mathbb{F}_q)$ — подгруппа простого порядка r.

Теорема 2 (Хассе — Вейль). Имеет место неравенство

$$\left(q^{1/2} - 1\right)^{2g} \leqslant |Jac_C(\mathbb{F}_q)| \leqslant \left(q^{1/2} + 1\right)^{2g}.$$

Поэтому $r \approx q^g$ при $q \to \infty$. Обозначим и зафиксируем $\rho = g \log q / \log r$. Это значение измеряет отношение между размером подгруппы, выбранной для криптосистемы, и размером якобиана кривой. Заметим, что $\rho \geqslant 1$. Для построения криптосистем на

практике это значение должно быть мало, чтобы уменьшить расходы на операции в группе.

Если $(r, q) = 1$, то степень вложения определяется как минимальное k, такое, что $r|q^k - 1$. Поэтому выполняется

Утверждение 1. Пусть C — гиперэллиптическая кривая рода g над полем $\mathbb{F}_q$; G — подгруппа Якобиана кривой простого порядка r; $(r, q) = 1$; k — степень вложения; $\rho = g \log q / \log r$. Тогда выполняется следующее неравенство:

$$k > g/\rho.$$

Доказательство. Так как $r|q^k - 1$, то $q^k - 1 \geqslant r$. Значит, $q^k > r$, $k > \log r / \log q = g/\rho$. ■

Аналогично можно доказать утверждение для минимальной степени вложения: $k' > g/\rho$.

Обозначим $L_{q^k}(\alpha, c_1)$ и $L_r(\beta, c_2)$ — сложности решения задачи дискретного логарифмирования в конечном поле и в подгруппе якобиана кривой соответственно.

В случае эллиптических кривых в [12, 30] указывается $k < \ln^2 q$ как необходимое условие для субэкспоненциальности (от $\ln q$) проблемы ВДЛ в конечном поле $\mathbb{F}_{q^k}$. Это условие верно для алгоритмов с $\alpha = 1/3$. Обобщая условие на случай произвольного $\alpha \in (0, 1)$, получаем

$$k < (\ln q)^{1/\alpha - 1}.$$

В случае гиперэллиптических кривых необходимо учитывать, что $r \approx q^{g/\rho}$. Заметим, что при $k = (g/\rho)^{1/\alpha} (\ln q)^{1/\alpha - 1} = (g/\rho)(\ln r)^{1/\alpha - 1}$ имеем

$$L_{q^k}(\alpha, c_1) = L_r(1, \alpha^{\alpha - 1} c_1)^{(\ln \ln r)^{1-\alpha}},$$

что больше $L_r(\beta, c_2)$ для любого β. Соответственно сбалансированное значение k ограничено следующим образом:

$$\frac{g}{\rho} < k < \frac{g}{\rho} (\ln r)^{1/\alpha - 1}. \tag{2}$$

Следовательно, $k = (g/\rho)(\ln r)^{c_k}$ для некоторого $0 < c_k < 1/\alpha - 1$. Таким образом, чтобы гарантировать стойкость кривой к MOV/FR-атаке, достаточно выбрать кривую со степенью вложения $k \geqslant (g/\rho)(\ln r)^{1/\alpha - 1}$. Для большинства кривых это условие выполняется, так как k в общем случае имеет размер, близкий к r.

Заметим, что на практике в настоящее время $\alpha = 1/3$ или $1/4$ для любых конечных полей [17]. Вследствие этого получаем гарантии безопасности криптосистемы при $k \geqslant (g/\rho)(\ln r)^2$ или $k \geqslant (g/\rho)(\ln r)^3$ соответственно. Однако кривые с такой степенью вложения не подходят для криптосистем на спариваниях, так как значения k слишком большие.

Для использования кривой в криптосистемах на спариваниях необходимо, чтобы сложности решения задачи вычисления дискретного логарифма в якобиане кривой и в конечном поле были сбалансированы:

$$L_{q^k}(\alpha, c_1) \approx L_r(\beta, c_2). \tag{3}$$

Заметим, что по свойствам L-нотации [31] для любых констант $c > 0$, a и δ выполняется $(\ln x)^a L_x(\delta, c) = L_x(\delta, c)$ и $L_x(\delta, c) L_x(\gamma, b) = L_x(\delta, c)$, если $\delta > \gamma$. Это связано

с тем, что $L_x(\delta, c)$ — сокращение для $L_x(\delta, c + \mathrm{o}(1))$ и множители $(\ln x)^a$ и $L_x(\gamma, b)$ при соответствующем преобразовании выражения попадают в $\mathrm{o}(1)$. При этом исходные константы c и δ не изменяются, меняется только константа в $\mathrm{o}(1)$.

Поэтому в оценках сложности $L_{q^k}(\alpha, c_1)$ и $L_r(\beta, c_2)$ решения задачи вычисления дискретного логарифма все временные затраты на вспомогательные операции, такие как операции в конечном поле, сложность сведения задачи к конечному полю и другие, попадают в $\mathrm{o}(1)$ и не влияют на константы c_1, c_2, α, β, если совокупное время их выполнения при работе алгоритма асимптотически не больше чем $L_{q^k}(\delta, c)$, $\delta < \alpha$, в первом случае и $L_r(\delta, c)$, $\delta < \beta$, — во втором. Если эти условия выполняются, то можно считать, что сложности $L_{q^k}(\alpha, c_1)$ и $L_r(\beta, c_2)$ выражены в битовых операциях, а не в операциях в поле $\mathbb{F}_{q^k}$ и якобиане кривой.

Покажем, что эти условия выполняются. Заметим, что групповая операция в якобиане кривой в общем случае вычисляется с помощью алгоритма Кантора [32] и его оптимизированных версий либо с помощью более быстрых явных формул при их наличии (например, если $g = 1$ или 2).

Утверждение 2 [33, § 2.6]. Если поле $\mathbb{F}_q$ имеет нечётную характеристику, то групповая операция в $Jac_C(\mathbb{F}_q)$ может быть вычислена за $17g^2 + \mathrm{O}(g)$ операций в поле $\mathbb{F}_q$. В случае чётной характеристики групповая операция может быть вычислена за $14g^2 + \mathrm{O}(g)$ операций.

Таким образом, операция в якобиане кривой имеет сложность $\mathrm{O}(g^2)$ операций в поле $\mathbb{F}_q$, или $\mathrm{O}(g^2(\log q)^2)$ битовых операций. Необходимо также учитывать затраты на выполнение сведения задачи ВДЛ к конечному полю. Общий алгоритм сведения для эллиптических кривых можно найти в [34, IX.9], для гиперэллиптических кривых — в [11].

Утверждение 3. Пусть C — гиперэллиптическая кривая рода g над полем $\mathbb{F}_q$; $G \subseteq Jac_C(\mathbb{F}_q)$; $|G| = r$ — простое число; k — степень вложения. Пусть $L_{q^k}(\alpha, c_1)$ — сложность решения задачи вычисления дискретного логарифма в поле $\mathbb{F}_{q^k}$, выраженная в операциях в этом поле. Тогда сведение задачи дискретного логарифмирования из якобиана кривой в конечное поле $\mathbb{F}_{q^k}$ имеет сложность $L_{q^k}(\alpha, c_1)$ битовых операций.

Доказательство. Покажем, что при выражении сложности в битовых операциях вспомогательные операции не влияют на константы α, c в выражении для сложности алгоритма вычисления дискретного логарифма в конечном поле. Кроме того, на эти константы также не оказывает влияния род кривой g.

Для сведения задачи ВДЛ к конечному полю необходимо вычислять функцию спаривания над полем $\mathbb{F}_{q^k}$, затем вычислять дискретный логарифм в этом поле за время $L_{q^k}(\alpha, c_1)$. При этом процесс может завершиться неудачей, если результатом вычисления спаривания будет элемент меньшего порядка, чем нужно. В этом случае выбирается другая случайная вспомогательная точка, и процесс повторяется. Ожидаемое число попыток для успешного применения атаки — $\mathrm{O}(\ln \ln r)$ [1]. Сложность операций в конечном поле $\mathbb{F}_{q^k}$ в общем случае — $\mathrm{O}((\ln q^k)^2)$ битовых операций.

Сложность вычисления спаривания — $\mathrm{O}(\ln r)$ операций в якобиане кривой $Jac_C(\mathbb{F}_q)$ [12; 24, Prop. 3.2]. Применяя утверждение 2, получаем сложность вычисления спаривания в битовых операциях $\mathrm{O}(g^2 \ln r (\ln q^k)^2)$. В итоге сложность атаки в битовых операциях составляет

$$(\mathrm{O}(g^2 \ln r) + L_{q^k}(\alpha, c_1))\mathrm{O}((\ln q^k)^2 \ln \ln r). \tag{4}$$

Заметим, что по теореме 2 имеем $r \leqslant (\sqrt{q} + 1)^{2g}$, то есть $r = \mathrm{O}(q^g)$. Кроме того, так как $k > g/\rho$, то $g = \mathrm{O}(k)$. Следовательно, $\ln r = \mathrm{O}(\ln q^k)$ и $\ln \ln r = \mathrm{O}(\ln \ln q^k)$. Поэтому

выражение (4) можно записать в виде

$$(\mathrm{O}(k^2 \ln q^k) + L_{q^k}(\alpha, c_1))\mathrm{O}((\ln q^k)^2 \ln\ln q^k). \tag{5}$$

Имеем

$$\mathrm{O}(k^2 \ln q^k) = \exp(\ln C + \ln k^2 + \ln\ln q^k) = \exp\left(\ln\ln q^k \left(\frac{2\ln k}{\ln\ln q + \ln k} + 1 + \mathrm{o}(1)\right)\right) =$$

$$= \exp\left(\ln\ln q^k \left(\frac{2}{\frac{\ln\ln q}{\ln k} + 1} + 1 + \mathrm{o}(1)\right)\right) = L_{q^k}(0, c)$$

для некоторой константы $c < 3$. Подставляя это выражение в (5), получаем

$$(L_{q^k}(0,c) + L_{q^k}(\alpha, c_1))\mathrm{O}((\ln q^k)^2 \ln\ln q^k) = L_{q^k}(\alpha, c_1)\mathrm{O}((\ln q^k)^2 \ln\ln q^k) = L_{q^k}(\alpha, c_1).$$

Утверждение доказано. ■

Аналогично можно записать в битовых операциях сложность $L_r(\beta, c_2)$, выраженную в операциях в якобиане кривой над полем $\mathbb{F}_q$:

$$L_r(\beta, c_2)\mathrm{O}(g^2 \ln^2 q) = L_r(\beta, c_2)\mathrm{O}((\rho \ln r)^2) = L_r(\beta, c_2).$$

Таким образом, условие (3) можно записать не в приближённом, а в точном виде:

$$L_{q^k}(\alpha, c_1) = L_r(\beta, c_2),$$

предполагая, что сложности выражены в битовых операциях, а все вспомогательные операции попадают в o(1).

Введём теперь более точную границу для сбалансированного значения k.

Теорема 3. Пусть C — гиперэллиптическая кривая рода g над полем $\mathbb{F}_q$; $G \subseteq Jac_C(\mathbb{F})$; $|G| = r$ и r — простое число; $L_{q^k}(\alpha, c_1)$ — сложность решения задачи ВДЛ в конечном поле; $L_r(\beta, c_2)$ — сложность решения задачи ВДЛ в группе G. Тогда если $\beta < 1$ или $\beta = 1$ и $\dfrac{c_2 + \mathrm{o}(1)}{c_1 + \mathrm{o}(1)} < \left(\dfrac{1}{\alpha} - \left(\dfrac{1}{\alpha} - 1\right)\dfrac{\ln\ln\ln r}{\ln\ln r}\right)^{1-\alpha}$, то для сбалансированной степени вложения выполняется неравенство

$$\frac{g}{\rho} < k < \frac{g}{\rho}\left(\frac{\ln r}{\ln\ln r}\right)^{1/\alpha - 1}. \tag{6}$$

Доказательство. Подставляя $k = \dfrac{g}{\rho}\left(\dfrac{\ln r}{\ln\ln r}\right)^{1/\alpha-1}$ и $\ln q = \dfrac{\rho}{g}\ln r$ в $L_{q^k}(\alpha, c_1)$, получаем

$$e^{(c_1 + \mathrm{o}(1))\ln r\left(1/\alpha - (1/\alpha - 1)\frac{\ln\ln\ln r}{\ln\ln r}\right)^{1-\alpha}} = L_r\left(1, (c_1 + \mathrm{o}(1))\left(\frac{1}{\alpha} - \mathrm{o}(1)\right)^{1-\alpha}\right).$$

Это выражение превосходит $L_r(\beta, c_2)$, только если $\beta < 1$ или $\beta = 1$ и $\dfrac{c_2 + \mathrm{o}(1)}{c_1 + \mathrm{o}(1)} < (1/\alpha - \mathrm{o}(1))^{1-\alpha}$. ■

При $\alpha = 0$ или $\beta = 0$ кривая считается непригодной для криптографии, так как задача ВДЛ в этом случае имеет полиномиальную сложность. При $\alpha > \beta$ сложность

решения задачи в конечном поле асимптотически выше, и в этом случае для построения криптосистем лучше подходят конечные поля, так как вычисления в них проще при меньшей, в данном случае, необходимой длине ключа.

Следующая теорема позволяет вычислить асимптотические границы для величины k, при которых уровни безопасности в якобиане кривой и конечном поле сбалансированы.

Теорема 4. Пусть C — гиперэллиптическая кривая рода g и $L_{q^k}(\alpha, c_1), 0 < \alpha < 1$, $L_r(\beta, c_2), \alpha \leqslant \beta \leqslant 1$, — сложности решения задачи ВДЛ в конечном поле $\mathbb{F}_{q^k}$ и подгруппе простого порядка r якобиана кривой $Jac_C(\mathbb{F}_q)$ соответственно. Тогда уровни безопасности сбалансированы при

$$k = \frac{g}{\rho}\left(\frac{\ln r}{\ln\ln r}\right)^{\beta/\alpha-1} c,$$

где c — некоторая константа, такая, что

$$\alpha^{1/\alpha-1}\left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha} < c < \left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}. \tag{7}$$

Если выполняется неравенство (6) из теоремы 3, то имеет место

$$\left(\frac{\alpha}{1-(1-\alpha)\dfrac{\ln\ln\ln r}{\ln\ln r}}\right)^{1/\alpha-1}\left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha} < c < \left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}. \tag{8}$$

Доказательство. Раскрывая условие $L_{q^k}(\alpha, c_1) = L_r(\beta, c_2)$, получаем

$$e^{(\ln q^k)^\alpha(\ln\ln q^k)^{1-\alpha}(c_1+\mathrm{o}(1))} = e^{(\ln r)^\beta(\ln\ln r)^{1-\beta}(c_2+\mathrm{o}(1))}.$$

Выразим из этого выражения k:

$$(\ln q^k)^\alpha(\ln\ln q^k)^{1-\alpha}(c_1+\mathrm{o}(1)) = (\ln r)^\beta(\ln\ln r)^{1-\beta}(c_2+\mathrm{o}(1)),$$
$$k^\alpha(\ln q)^\alpha(\ln\log q+\ln k)^{1-\alpha}(c_1+\mathrm{o}(1)) = (\ln r)^\beta(\ln\ln r)^{1-\beta}(c_2+\mathrm{o}(1)),$$
$$k = \left(\frac{(\ln r)^\beta(\ln\ln r)^{1-\beta}(c_2+\mathrm{o}(1))}{(\ln q)^\alpha(\ln\ln q+\ln k)^{1-\alpha}(c_1+\mathrm{o}(1))}\right)^{1/\alpha} = \left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}\frac{(\ln r)^{\beta/\alpha}(\ln\ln r)^{(1-\beta)/\alpha}}{\ln q(\ln\ln q+\ln k)^{1/\alpha-1}}.$$

Так как $\ln q = \rho\ln r/g$, то

$$k = \left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}\frac{g}{\rho}\frac{(\ln r)^{\beta/\alpha-1}(\ln\ln r)^{(1-\beta)/\alpha}}{(\ln\ln q+\ln k)^{1/\alpha-1}}.$$

Из неравенства (2) имеем $k = \dfrac{g}{\rho}(\ln r)^{c_k}$, поэтому $\ln\ln q + \ln k = (c_k+1)\ln\ln r$. Следовательно, получаем

$$k = \left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}\left(\frac{1}{c_k+1}\right)^{1/\alpha-1}\frac{g}{\rho}\left(\frac{\ln r}{\ln\ln r}\right)^{\beta/\alpha-1}.$$

Так как $0 < c_k < 1/\alpha - 1$, получаем

$$\alpha^{1/\alpha-1} < \left(\frac{1}{c_k+1}\right)^{1/\alpha-1} < 1.$$

Если выполняется неравенство (6), то на величину c_k можно наложить дополнительные ограничения. Имеем $k = \dfrac{g}{\rho}\left(\dfrac{\ln r}{\ln\ln r}\right)^{c'_k}$ для некоторой величины c'_k, $0 < c'_k < 1/\alpha - 1$. Так как $(\ln r)^{c_k} = \dfrac{\ln r}{\ln\ln r}$, получаем

$$c_k = c'_k\left(1 - \frac{\ln\ln\ln r}{\ln\ln r}\right) < \left(\frac{1}{\alpha} - 1\right)\left(1 - \frac{\ln\ln\ln r}{\ln\ln r}\right).$$

Отсюда следует, что

$$\left(\frac{1}{c_k+1}\right)^{1/\alpha-1} > \left(\frac{1}{\left(\dfrac{1}{\alpha}-1\right)\left(1-\dfrac{\ln\ln\ln r}{\ln\ln r}\right)+1}\right)^{1/\alpha-1} = \left(\frac{\alpha}{1-(1-\alpha)\dfrac{\ln\ln\ln r}{\ln\ln r}}\right)^{1/\alpha-1}.$$

Теорема доказана. ■

Выражение $\dfrac{\ln\ln\ln r}{\ln\ln r}$ в неравенстве (8) при $r \to \infty$ стремится к нулю и соответственно всё выражение стремится к $\alpha^{1/\alpha-1}$, т. е. к выражению в неравенстве (7).

В криптографии используются значения $2^{80} < r < 2^{10240}$, что означает

$$0{,}246 < \frac{\ln\ln\ln r}{\ln\ln r} < 0{,}346.$$

Следовательно,

$$\left(\frac{\alpha}{0{,}246\alpha+0{,}753}\right)^{1/\alpha-1} < \left(\frac{\alpha}{1-(1-\alpha)\dfrac{\ln\ln\ln r}{\ln\ln r}}\right)^{1/\alpha-1} < \left(\frac{\alpha}{0{,}346\alpha+0{,}653}\right)^{1/\alpha-1}.$$

Для $\alpha = 1/3$ получаем

$$0{,}159 < \left(\frac{\alpha}{1-(1-\alpha)\dfrac{\ln\ln\ln r}{\ln\ln r}}\right)^{1/\alpha-1} < 0{,}187,$$

что больше, чем $\alpha^{1/\alpha-1} \approx 0{,}111$, и значит, граница (8) точнее.

Теорема 4 позволяет вычислить границы для сбалансированного значения k с точностью до бесконечно малых величин. Соответственно кривая со степенью вложения

$$k = \left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}\frac{g}{\rho}\left(\frac{\ln r}{\ln\ln r}\right)^{\beta/\alpha-1}$$

является стойкой к MOV/FR-атаке. В то же время если

$$k < \alpha^{1/\alpha-1}\left(\frac{c_2+\mathrm{o}(1)}{c_1+\mathrm{o}(1)}\right)^{1/\alpha}\frac{g}{\rho}\left(\frac{\ln r}{\ln\ln r}\right)^{\beta/\alpha-1},$$

то уровень безопасности на кривой меньше, чем в конечном поле, и такая кривая небезопасна для использования в криптосистемах на спариваниях. Сбалансированное значение находится среди промежуточных значений.

4. Уровень безопасности

Определение 2. Группа G обладает уровнем безопасности l, если для решения задачи ВДЛ в этой группе требуется 2^l битовых операций.

Для обеспечения одного и того же уровня безопасности в различных группах может требоваться разный размер группы; группы с меньшим требуемым размером имеют преимущество. Для выбора безопасного размера группы, удовлетворяющего заданному уровню безопасности, могут использоваться рекомендации NIST [35]. Расчёт степеней вложения на основе этих данных есть в работе [14]. В общем случае, для асимптотической оценки размера группы, необходимого для обеспечения уровня безопасности l, докажем следующую теорему.

Теорема 5. Пусть G — группа порядка n и сложность решения задачи ВДЛ в битовых операциях выражается в виде $L_n(\alpha, c)$, где $0 \leqslant \alpha \leqslant 1$; $c > 0$. Тогда размер группы $\lg n$, необходимый для обеспечения уровня безопасности l, равен

$$s_l(\alpha, c) = \begin{cases} e^{l \ln 2/(c+\mathrm{o}(1))-\ln\ln 2}, & \alpha = 0, \\ l^{1/\alpha}(\ln l)^{-(1-\alpha)/\alpha}\dfrac{(\ln 2)^{1/\alpha-1}}{(c+\mathrm{o}(1))^{1/\alpha}}\left(\dfrac{\alpha}{1-\mathrm{o}(1)}\right)^{(1-\alpha)/\alpha}, & 0 < \alpha < 1, \\ \dfrac{l}{c+\mathrm{o}(1)}, & \alpha = 1. \end{cases}$$

Доказательство.

1) $\ln^c n = 2^l$, $\ln n = e^{l\,\ln 2/(c+\mathrm{o}(1))}$.

2) Последовательно запишем:

$$(\ln n)^\alpha (\ln\ln n)^{1-\alpha}(c+\mathrm{o}(1)) = l\ln 2,$$

$$(\ln n)^{\alpha/(1-\alpha)}\ln\ln n = \left(\frac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)},$$

$$e^{\frac{\alpha}{1-\alpha}\ln\ln n}\left(\frac{\alpha}{1-\alpha}\ln\ln n\right) = \frac{\alpha}{1-\alpha}\left(\frac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)},$$

$$\frac{\alpha}{1-\alpha}\ln\ln n = W\left(\frac{\alpha}{1-\alpha}\left(\frac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)}\right),$$

где W — функция Ламберта. Далее, имеем

$$\ln n = \exp\left(\frac{1-\alpha}{\alpha}W\left(\frac{\alpha}{1-\alpha}\left(\frac{l\ln 2}{c+o(1)}\right)^{1/(1-\alpha)}\right)\right).$$

По определению W-функции $e^{W(x)} = x/W(x)$. Кроме того,

$$W(x) = \ln x - \ln\ln x + \mathrm{o}(1) = \ln x\left(1 - \frac{\ln\ln x}{\ln x} + \mathrm{o}(1)\right) = \ln(x)(1-\mathrm{o}(1)).$$

Соответственно получаем

$$\ln n = \left(\frac{\dfrac{\alpha}{1-\alpha}\left(\dfrac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)}}{W\left(\dfrac{\zeta}{1-\alpha}\left(\dfrac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)}\right)}\right)^{(1-\alpha)/\alpha} =$$

$$= \left(\frac{\frac{\alpha}{1-\alpha}\left(\frac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)}}{\ln\left(\frac{\alpha}{1-\alpha}\left(\frac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)}\right)(1-\mathrm{o}(1))} \right)^{(1-\alpha)/\alpha} = l^{1/\alpha}\left(\frac{\ln 2}{c+\mathrm{o}(1)}\right)^{1/\alpha}\left(\frac{\alpha}{1-\alpha}\right)^{(1-\alpha)/\alpha} \times$$

$$\times \left(\left(\ln\frac{\alpha}{1-\alpha} + \frac{1}{1-\alpha}\ln l + \frac{1}{1-\alpha}\ln\left(\frac{\ln 2}{c+\mathrm{o}(1)}\right)\right)(1-\mathrm{o}(1))\right)^{-(1-\alpha)/\alpha} =$$

$$= l^{1/\alpha}(\ln l)^{-(1-\alpha)/\alpha}\left(\frac{\ln 2}{c+\mathrm{o}(1)}\right)^{1/\alpha}\left(\frac{\alpha}{1-\mathrm{o}(1)}\right)^{(1-\alpha)/\alpha}.$$

3) $n^{c+\mathrm{o}(1)} = 2^l$, $\ln n = l\ln 2/(c+\mathrm{o}(1))$.

Для определения размера группы в виде $\lg n$ необходимо поделить все полученные величины на $\ln 2$. ■

Значение $s_l(\alpha, c)$ при $0 < \alpha < 1$ получено аппроксимацией W-функции Ламберта с использованием только первых двух членов разложения функции в ряд и отбрасыванием остальных. Эту функцию можно вычислить с произвольной точностью [36]. Методы для вычисления W-функции есть в составе многих систем компьютерной алгебры, например Maxima или PARI/GP. Поэтому значение $s_l(\alpha, c)$ при $0 < \alpha < 1$ более точно можно вычислить по формуле

$$s_l(\alpha, c) = \exp\left(\frac{1-\alpha}{\alpha}W\left(\frac{\alpha}{1-\alpha}\left(\frac{l\ln 2}{c+\mathrm{o}(1)}\right)^{1/(1-\alpha)}\right) - \ln\ln 2\right). \tag{9}$$

Следствие 1. Пусть C — гиперэллиптическая кривая рода g над полем $\mathbb{F}_q$; l — уровень безопасности; G — подгруппа порядка r якобиана кривой $Jac_C(\mathbb{F}_q)$; $\rho = g\ln q/\ln r$ — константа. Предположим, что сложность решения задачи ВДЛ в группе G выражается в виде $L_r(\alpha, c)$ битовых операций. Тогда размер поля $\lg q$, необходимый для обеспечения уровня безопасности l, равен $\dfrac{\rho}{g}s_l(\alpha, c)$.

В случае квазиполиномиальной сложности решения задачи ВДЛ имеет место

Утверждение 4. Пусть сложность решения задачи ВДЛ в группе G порядка n квазиполиномиальна — $2^{\mathrm{O}((\ln\ln n)^c)}$. Тогда размер группы $\lg n$, необходимый для обеспечения уровня безопасности l, равен $e^{\mathrm{O}(l^{1/c})}$.

Табл. 3 содержит необходимые размеры групп для обеспечения уровня безопасности l. Значения, обозначенные $l_1(G)$, рассчитаны по теореме 5 и утверждению 4; $l_2(G)$ обозначает размер группы G, найденный, где применимо, по более точной формуле (9). При этом значение ρ считалось равным 1; сложность алгоритмов взята из табл. 1 и 2.

Размер базового поля, требуемый для обеспечения уровня безопасности l, вычисленный по следствию 1, приведён в табл. 4; используемые сокращения: ЭК — эллиптическая кривая; ГЭК — гиперэллиптическая кривая.

При вычислении функции спаривания выполняются операции в поле $\mathbb{F}_{q^k}$; в общем случае чем больше это поле, тем ниже эффективность вычисления функции спаривания. Размер поля также можно вычислить по теореме 5 либо использовать следующее эквивалентное утверждение.

Утверждение 5. Пусть C — ГЭК рода g над полем $\mathbb{F}_q$, k — её степень вложения, $L_{q^k}(\alpha, c_1)$ и $L_r(\beta, c_2)$ — сложности решения задачи ВДЛ в конечном поле $\mathbb{F}_{q^k}$ и якобиане кривой $Jac_C(\mathbb{F}_q)$ соответственно, причём $0 < \alpha \leqslant \beta$. Если уровни безопасности

Таблица 3

Размеры групп для обеспечения уровня безопасности l

Группа G	Алгоритм	Размер группы, $l_1(G)$	Размер группы, $l_2(G)$
Любая	Pollard	$2\,l$	—
$E(\mathbb{F}_q)$, специальная	Semaev	$0{,}252\,l^2/\ln l$	$1{,}44\exp(W(0{,}350\,l^2))$
$Jac_C(\mathbb{F}_q)$, $g > O(\ln q)$	EG	$0{,}173\,l^2/\ln l$	$1{,}44\exp(W(0{,}240\,l^2))$
$Jac_C(\mathbb{F}_q)$, $g > \mathrm{O}(\ln^2 q)$	EGT	$0{,}007\,l^3/\ln^2 l$	$1{,}44\exp(2W(0{,}108\,l^{3/2}))$
$Jac_C(\mathbb{F}_q)$, $g = 3$	GTTD	$2{,}250\,l$	—
$Jac_C(\mathbb{F}_q)$, $g = 4$	GTTD	$2{,}666\,l$	—
$Jac_C(\mathbb{F}_q)$, $g = 5$	GTTD	$3{,}125\,l$	—
$\mathbb{F}_q^\times$, малое p	Joux [9]	$0{,}005\,l^4/(c^4\ln^3 l)$	$1{,}44\exp(3W(0{,}204\,l^{4/3})/c^{4/3})$
$\mathbb{F}_q^\times$, малое p	BGJT [10]	$\exp(\mathrm{O}(\sqrt{l}))$	—
$\mathbb{F}_q^\times$, среднее p	exTNFS	$0{,}010\,l^3/\ln^2 l$	$1{,}44\exp(2W(0{,}124\,l^{3/2}))$
$\mathbb{F}_q^\times$, большое p	MNFS [23]	$0{,}007\,l^3/\ln^2 l$	$1{,}44\exp(2W(0{,}110\,l^{3/2}))$

Таблица 4

Размеры базового поля ГЭК для уровня безопасности l

Кривая C	Алгоритм	Размер поля, $\lg q$
ЭК	Pollard	$2l$
ЭК, специальная	Semaev	$0{,}252\,l^2/\ln l$
ГЭК рода 2	Pollard	l
ГЭК рода 3	GTTD	$0{,}75\,l$
ГЭК рода 4	GTTD	$0{,}666\,l$
ГЭК рода 5	GTTD	$0{,}625\,l$

в якобиане кривой и поле $\mathbb{F}_{q^k}$ сбалансированы, то размер расширенного поля $\ln q^k$ равен

$$\frac{(\ln r)^{\beta/\alpha}}{(\ln\ln r)^{\beta/\alpha-1}}c,$$

где c — константа из теоремы 4.

В [13] для балансирования уровней безопасности в случае эллиптических кривых используется следующий метод. Фиксируется безопасный размер подгруппы точек эллиптической кривой b_1 и безопасный размер конечного поля b_2, затем для балансирования уровней безопасности используется соотношение $b_2/b_1 = \rho k$. В случае гиперэллиптических кривых необходимо учитывать род кривой, и соотношение принимает следующий вид: $b_2/b_1 = (\rho/g)k$.

Для получения значений b_1, b_2 могут использоваться рекомендации из [35, 37] или их можно приближенно вычислить, используя теорему 5. В последнем случае получаем

$$k = \frac{g}{\rho}\frac{s_l(\alpha, c_1)}{s_l(\beta, c_2)}.$$

Для расчёта границ сбалансированной степени вложения для заданного уровня безопасности l используем формулу из теоремы 4 с подстановкой вместо $\ln r$ требуемого размера группы для данной кривой из табл. 3. Для удобства значения k и q^k представлены в виде $al^{\lambda_1}\ln^{\lambda_2} l = \mathrm{O}(l^{\lambda_1}\ln^{\lambda_2} l) = \tilde{\mathrm{O}}(l^{\lambda_1})$, где a, λ_1, λ_2 — константы. Члены меньших порядков опускаются. Расчёт этих констант для различных полей и сбалансированного значения k представлен в табл. 5.

Заметим, что в случае малой характеристики существует теоретический квазиполиномиальный алгоритм. Из утверждения 4 следует, что в этом случае размер группы, необходимый для обеспечения безопасности, растёт экспоненциально от l. В то же время, по утверждению авторов алгоритма [10], константа в оценке сложности алгоритма большая и поэтому на практике он неприменим. Для табл. 5 были выбраны практические алгоритмы, но необходимо учитывать, что безопасность в полях малой характеристики остаётся под вопросом.

Таблица 5

Сбалансированная степень вложения для различных ГЭК и полей

g	ρ	p	Алгоритмы	Степень вложения, k			Размер поля $\mathbb{F}_{q^k}$		
				a	λ_1	λ_2	a	λ_1	λ_2
1	1	2	Joux [9] / Semaev [26]	0,0025 – 0,1648	2	−2	0,0006 – 0,0416	4	−3
		Малое	Joux [9] / Pollard	0,0026 – 0,1665	3	−3	0,0052 – 0,3330	4	−3
		Среднее	ExTNFS / Pollard	0,0050 – 0,0450	2	−2	0,0100 – 0,0901	3	−2
		Большое	MNFS / Pollard	0,0038 – 0,0349	2	−2	0,0077 – 0,0699	3	−2
	2	Малое	Joux [9] / Pollard	0,0013 – 0,0832	3	−3	0,0052 – 0,3330	4	−3
		Среднее	ExTNFS / Pollard	0,0025 – 0,0225	2	−2	0,0100 – 0,0901	3	−2
		Большое	MNFS / Pollard	0,0019 – 0,0174	2	−2	0,0077 – 0,0699	3	−2
2	1	Малое	Joux [9] / Pollard	0,0052 – 0,3330	3	−3	0,0052 – 0,3330	4	−3
		Среднее	ExTNFS / Pollard	0,0100 – 0,0901	2	−2	0,0100 – 0,0901	3	−2
		Большое	MNFS / Pollard	0,0077 – 0,0699	2	−2	0,0077 – 0,0699	3	−2
	2	Малое	Joux [9] / Pollard	0,0026 – 0,1665	3	−3	0,0052 – 0,3330	4	−3
		Среднее	ExTNFS / Pollard	0,0050 – 0,0450	2	−2	0,0100 – 0,0901	3	−2
		Большое	MNFS / Pollard	0,0038 – 0,0349	2	−2	0,0077 – 0,0699	3	−2
3	1	Малое	Joux [9] / GTTD [27]	0,0069 – 0,4440	3	−3	0,0052 – 0,3330	4	−3
		Среднее	ExTNFS / GTTD [27]	0,0133 – 0,1201	2	−2	0,0100 – 0,0901	3	−2
		Большое	MNFS / GTTD [27]	0,0103 – 0,0932	2	−2	0,0077 – 0,0699	3	−2
	2	Малое	Joux [9] / Pollard	0,0039 – 0,2497	3	−3	0,0052 – 0,3330	4	−3
		Среднее	ExTNFS / Pollard	0,0075 – 0,0675	2	−2	0,0100 – 0,0901	3	−2
		Большое	MNFS / Pollard	0,0058 – 0,0524	2	−2	0,0077 – 0,0699	3	−2

5. Сравнение кривых

Пусть l — некоторый фиксированный уровень безопасности. При сравнении учитываются следующие параметры — размер группы, размер базового поля, размер расширенного поля и сбалансированная степень вложения.

5.1. Размер группы

От размера группы зависит скорость вычисления спаривания, так как алгоритм Миллера, используемый для вычисления спаривания, в общем случае имеет сложность $\mathrm{O}(\log r)$.

Размер группы, необходимый для обеспечения уровня безопасности l, зависит от используемого алгоритма решения задачи ВДЛ в данной группе. Расчёт требуемых размеров групп представлен в табл. 3. Эллиптические кривые и гиперэллиптические кривые рода 2 имеют преимущество перед кривыми больших родов, так как требуют меньший размер группы.

5.2. Размер базового поля

Кривые больших родов позволяют использовать меньший размер базового поля (см. табл. 4). Размер поля влияет на эффективность вычислений в якобиане кривой и на размер параметров и ключей криптосистемы. Однако, как замечено в [38], существуют методы сжатия точек эллиптической кривой, позволяющие достичь размеров

параметров, аналогичных гиперэллиптическим кривым рода 2. Для кривых рода $g \geqslant 2$ подобные методы не разработаны.

5.3. Сложность группового закона

Для эллиптических кривых и гиперэллиптических кривых рода 2 существуют быстрые явные формулы для вычисления группового закона. В общем случае чем больше род кривой, тем сложнее групповой закон на кривой. Для кривых рода $g > 2$ по утверждению 2 сложность вычисления группового закона растёт как $\mathrm{O}(g^2)$ операций в базовом поле или $\mathrm{O}(g^2 \log^2 q)$ битовых операций.

С другой стороны, кривые большего рода требуют меньший размер базового поля для обеспечения аналогичного уровня безопасности (см. табл. 4).

5.4. Размер расширенного поля

Сбалансированная степень вложения определяет размер расширенного поля, над которым вычисляется функция спаривания (см. табл. 5). В общем случае чем больше это поле, тем менее эффективно вычисляется функция спаривания. Однако существуют методы, позволяющие минимизировать необходимое число операций в поле при вычислении спаривания. Кроме того, эффективность вычисления функции спаривания может быть улучшена с помощью использования кручений (кривых, изоморфных данной над $\overline{F}_q$) при их наличии.

5.5. Алгоритмы генерации и ограничения на параметры

Так как для случайно выбранной эллиптической или гиперэллиптической кривой вероятность того, что её степень вложения мала, незначительна, кривые, подходящие для использования в криптографии на билинейных спариваниях, требуют специальных алгоритмов построения. Исключение составляют суперсингулярные кривые, которые всегда имеют малую степень вложения для любого рода (для эллиптических кривых $k \leqslant 6$ [1], для кривых больших родов границы рассчитаны в работе [39]).

Алгоритмы генерации наиболее разработаны для эллиптических кривых, в меньшей степени — для ГЭК рода 2, в отдельных случаях — для рода 3 и практически полностью не разработаны для рода 4 и больше. Классификация эллиптических кривых, подходящих для использования в криптографии на билинейных спариваниях, а также методы генерации таких кривых есть в [13]. Для сравнения из данной работы были выбраны кривые с наименьшими значениями ρ (см. [13, Table 8.2]).

В случае суперсингулярных эллиптических кривых возможны только степени вложения $k = 1, 2, 3, 4, 6$, причём значения $k = 4$ и 6 возможны только в случае $p = 2$ и 3 соответственно. Известно также, что при $k = 1$ минимальное ρ-значение равно 2.

В случае обычных эллиптических кривых существует несколько семейств кривых, подходящих для криптографии на спариваниях, — MNT-кривые, кривые Кокса — Пинча и др. Алгоритмы генерации таких кривых позволяют строить кривые с произвольной степенью вложения.

Хороший обзор методов генерации гиперэллиптических кривых для криптографии на билинейных спариваниях приведён в [14]. В отличие от эллиптических кривых, в настоящее время не разработаны методы генерации, позволяющие получать ГЭК со значением $\rho < 2$.

В случае ГЭК рода 2 первый алгоритм для генерации обычных ГЭК рода 2 с произвольной степенью вложения предложен Фриманом [40]. Алгоритм основан на обобщении метода Кокса — Пинча и позволяет генерировать кривые с $\rho \approx 8$. Позже было предложено обобщение метода Брезинга — Венга [41], позволяющее в частных случаях получать кривые с меньшим ρ-значением.

В случае кривых с разделённым якобианом существуют методы [42 – 45] для генерации кривых с $\rho \approx 4$. В частных случаях для определённых значений k возможны меньшие ρ-значения; например, в [45] для $k = 3, 4, 6, 12$ получены кривые с $\rho \approx 2$.

Суперсингулярные гиперэллиптические кривые рода 2 имеют степень вложения $k \leqslant 12$. При этом степень вложения $k = 12$ возможна только для кривой над полем характеристики 2, а степень вложения $k = 4$ — только для характеристики 3. Суперсингулярные кривые в настоящее время являются единственным известным классом ГЭК рода 2, для которых достигается значение $\rho \approx 1$.

В случае кривых рода 3 в работах [46, 41] предложены методы, позволяющие получить кривые в отдельных случаях с $\rho \approx 12$ при $k = 7$, $\rho \approx 15$ при $k = 9, 18$, $\rho \approx 8$ при $k = 13$.

5.6. Диапазон уровней безопасности и результаты

Если степень вложения k кривой C фиксирована, то, начиная с некоторого уровня безопасности l, эта степень становится меньше сбалансированного значения k, а такая кривая — непригодной для криптографии с уровнем безопасности больше l.

Для расчёта такого значения l введём следующий метод. Сначала сбалансированное значение k выражается в виде $al^{\lambda_1}(\ln l)^{\lambda_2}$. Значения $(a, \lambda_1, \lambda_2)$ можно брать из табл. 5 либо вычислять, используя теоремы 4 и 5. Далее, из равенства $k = al^{\lambda_1}(\ln l)^{\lambda_2}$ выражаем l и получаем формулу

$$l = \exp\left(\frac{\lambda_2}{\lambda_1} W\left(\frac{\lambda_1}{\lambda_2}\left(\frac{k}{a}\right)^{1/\lambda_2}\right)\right).$$

В настоящее время для криптографии требуется $r > 2^{160}$ и в общем случае все алгоритмы ВДЛ в якобиане кривых экспоненциальны, поэтому введём следующую более точную теорему для данного частного случая.

Теорема 6. Пусть C — ГЭК рода 2; $G \subseteq Jac_C(\mathbb{F}_q)$ — подгруппа простого порядка $r > e^e$; k — степень вложения кривой; $L_{q^k}(\alpha, c_1), L_r(\beta, c_2)$ — сложности решения задачи ВДЛ в конечном поле $\mathbb{F}_{q^k}$ и группе G соответственно. Тогда если $\beta = 1$, то кривая удовлетворяет уровню безопасности

$$l = \frac{c_2}{\ln 2}\frac{W_-(d)}{d},$$

где $d = -(gc/k\rho)^{\alpha/(\beta-\alpha)}$ и c — константа из теоремы 3.

Доказательство. По теореме 3 получаем сбалансированную степень вложения

$$k = \frac{g}{\rho} c \left(\frac{\ln r}{\ln\ln r}\right)^{\beta/\alpha-1}.$$

Выразим из данного выражения $\ln r$:

$$\frac{k\rho}{gc} = (\ln r)^{\beta/\alpha-1}(\ln\ln r)^{-(\beta/\alpha-1)} = e^{(\beta/\alpha-1)\ln\ln r}(\ln\ln r)^{-(\beta/\alpha-1)} = \left(e^{-\ln\ln r}\ln\ln r\right)^{-(\beta/\alpha-1)},$$

$$-\left(\frac{gc}{k\rho}\right)^{1/(\beta/\alpha-1)} = e^{-\ln\ln r}(-\ln\ln r), \quad \ln\ln r = -W(d), \quad \ln r = e^{-W(d)} = \frac{W(d)}{d}.$$

Здесь W-функция Ламберта определяется как решение уравнения $We^W = x$. На интервале $(-1/e, 0)$ уравнение имеет два вещественных решения, одно возрастает от -1 до 0 при $d \to 0$ и обозначается W_+; второе стремится к $-\infty$ при $d \to 0$.

Для W_+ имеем $1 < (W_+(d))/d < e$, то есть получаем $1 < \ln r < e$, что противоречит условию $r > e^e$. Поэтому остаётся решение W_-, и $\ln r = (W_-(d))/d$. Применяя теорему 5 для $\beta = 1$, получаем

$$l = \frac{c_2}{\ln 2} \ln r = \frac{c_2}{\ln 2} \frac{W_-(d)}{d}.$$

Теорема доказана. ■

Для сравнения были выбраны кривые со степенями вложения $1 \leqslant k \leqslant 10$ по следующим правилам:

1) для кривой или семейства кривых должны быть известны алгоритмы генерации и явные примеры построения, которые указываются в графе «Источник»;
2) выбираются кривые с минимальным ρ-значением среди всех кривых с одинаковой степенью вложения, родом и полем;
3) в случае, если ρ-значения совпадают, выбирается любая из кривых;
4) если требуются дополнительные ограничения или кривая имеет специальный вид, то дополнительно указываются кривые с минимальным ρ-значением без ограничений, а кривая помечается знаком «+»;
5) указываются кривые, уровень безопасности которых не удовлетворяет современным требованиям [47, 48] ($l < 80$). В этом случае кривая помечается знаком «*».

Результаты представлены в табл. 6; диапазон уровней безопасности рассчитан по теореме 6.

Заключение

В работе введена формула (теорема 4) для оценки границ сбалансированного значения степени вложения гиперэллиптических кривых.

Для гиперэллиптических кривых рода 1–3 вычислены текущие границы сбалансированной степени вложения для различных полей (табл. 5). Кривые со степенями вложения, выходящими за эти границы, либо не безопасны, либо их степень вложения превосходит необходимую для заданного уровня безопасности.

Для кривых с известными алгоритмами генерации выбраны семейства с наименьшими ρ-значениями и произведены вычисления диапазона уровней безопасности, которому они могут соответствовать (табл. 6), что позволило определить некоторые кривые, небезопасные для использования в настоящее время.

Таблица 6

Уровни безопасности для гиперэллиптических кривых

k	Кривая C	g	ρ	p	Источники	l
1	ЭК, полная	1	2	Среднее	[13, § 6.6]	23–98
1	ЭК, полная	1	2	Большое	[13, § 6.6]	27–115
2	ЭК, суперсингулярная	1	1	Среднее	[13, § 3.2]	23–98
2	ЭК, суперсингулярная	1	1	Большое	[13, § 3.2]	27–115
2	ГЭК, обычная$^+$	2	3	Большое	[45, Table 1]	36–147
2	ГЭК, обычная	2	8,135	Большое	[40, Ex. 1]	69–271
3	ЭК, суперсингулярная	1	1	Среднее	[13, § 3.3]	30–126
3	ЭК, суперсингулярная	1	1	Большое	[13, § 3.3]	36–147
3	ГЭК, обычная$^+$	2	2	Большое	[45, Ex. 24]	36–147
4	ЭК, полная	1	1,5	Среднее	[13, § 6.9]	48–193
4	ЭК, полная	1	1,5	Большое	[13, § 6.9]	57–225
4	ЭК, суперсингулярная*	1	1	2	[13, § 3.4]	6–48
4	ЭК, суперсингулярная*	1	2	2	[13, § 3.4]	9–65
4	ГЭК, суперсингулярная*	2	1	3	[14, § 3.4]	3–35
4	ГЭК, обычная$^+$	2	2	Большое	[45, Ex. 24]	43–176
4	ГЭК, обычная	2	8,139	Большое	[40, Ex. 4]	108–410
5	ЭК, полная	1	1,5	Среднее	[13, § 6.6]	56–221
5	ЭК, полная	1	1,5	Большое	[13, § 6.6]	66–258
5	ГЭК, обычная$^+$	2	3	Большое	[45, Table 1]	66–258
5	ГЭК, обычная	2	4	Большое	[41, 5.2]	79–307
6	ЭК, суперсингулярная*	1	1	3	[13, § 3.5]	7–57
6	ЭК, суперсингулярная*	1	2	3	[13, § 3.5]	11–77
6	ЭК, Скотта — Баретто	1	1,25	Среднее	[13, § 6.16]	56–221
6	ЭК, Скотта — Баретто	1	1,25	Большое	[13, § 6.16]	66–258
6	ГЭК, суперсингулярная*	2	1	Большое	[14, § 3.4]	5–42
6	ГЭК, обычная$^+$	2	2	Большое	[45, Ex. 24]	57–225
6	ГЭК, обычная	2	7,5	Большое	[41, Table 1]	132–497
7	ЭК, циклотомическая	1	1,33	Среднее	[13, § 6.20]	64–252
7	ЭК, циклотомическая	1	1,33	Большое	[13, § 6.20]	75–294
7	ГЭК, обычная$^+$	2	2,5	Большое	[45, Table 1]	73–283
7	ГЭК, обычная	3	12	Большое	[41, 5.7]	151–565
8	ЭК, полная	1	1,25	Среднее	[13, § 6.6]	67–263
8	ЭК, полная	1	1,25	Большое	[13, § 6.6]	79–307
8	ГЭК, обычная$^+$	2	3	Большое	[45, Ex. 25]	89–342
8	ГЭК, обычная	2	7,5	Большое	[41, Table 1]	157–589
9	ЭК, полная	1	1,33	Среднее	[13, § 6.6]	75–293
9	ЭК, полная	1	1,33	Большое	[13, § 6.6]	89–341
9	ГЭК, обычная$^+$	2	2,33	Большое	[45, Table 1]	81-315
9	ГЭК, обычная	3	15	Большое	[41, 5.7]	202–747
10	ЭК, полная	1	1,5	Среднее	[13, § 6.5]	87–336
10	ЭК, полная	1	1,5	Большое	[13, § 6.5]	102–391
10	ГЭК, обычная$^+$	2	3	Большое	[43, Th. 4]	102–391
10	ГЭК, обычная	2	6	Большое	[41, 5.4]	157–589

ЛИТЕРАТУРА

1. *Menezes A., Okamoto T., and Vanstone S. A.* Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Trans. Inform. Theory. 1993. V. 39. No. 5. P. 1639–1646.
2. *Sakai R., Ohgishi K., and Kasahara M.* Cryptosystems Based on Pairing. Okinawa, Japan, 2000.
3. *Joux A.* A one round protocol for tripartite Diffie — Hellman // ANTS-IV. LNCS. 2000. V. 1838. P. 385–393.

4. *Boneh D. and Franklin M. K.* Identity-based encryption from the Weil pairing // CRYPTO 2001. LNCS. 2001. V. 2139. P. 213–229.
5. *Paterson K. G.* Cryptography from pairings // Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005. P. 215–252.
6. *Hitt L.* On the minimal embedding field // LNCS. 2007. V. 4575. P. 294–301.
7. *Benger N., Charlemagne M., and Freeman D. M.* On the security of pairing-friendly Abelian varieties over non-prime fields // LNCS. 2009. V. 5671. P. 52–65.
8. *Galbraith S. D., Hess F., and Vercauteren F.* Aspects of pairing inversion // IEEE Trans. Inform. Theory. 2008. V. 54. No. 12. P. 5719–5728.
9. *Joux A.* A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic // LNCS. 2014. V. 8282. P. 355–379.
10. *Barbulescu R., Gaudry P., Joux A., and Thomé E.* A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic // LNCS. 2014. V. 8441. P. 1–16.
11. *Frey G. and Lange T.* Transfer of discrete logarithms // Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2005. P. 529–545.
12. *Miller V. S.* The Weil pairing, and its efficient calculation // J. Cryptology. 2004. V. 17. No. 4. P. 235–261.
13. *Freeman D., Scott M., and Teske E.* A taxonomy of pairing-friendly elliptic curves // J. Cryptology. 2010. V. 23. No. 2. P. 224–280.
14. *Balakrishnan J., Belding J., Chisholm S., et al.* Pairings on hyperelliptic curves. `http://arxiv.org/abs/0908.373`. 2009.
15. *Pollard J. M.* Monte Carlo methods for index computation (mod p) // Math. Comput. 1978. V. 78. No. 147. P. 918–924.
16. *Pohlig S. C. and Hellman M. E.* An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.) // IEEE Trans. Inform. Theory. 1978. V. 24. No. 1. P. 106–110.
17. *Joux A., Odlyzko A., and Pierrot C.* The past, evolving present, and future of the discrete logarithm // Open Problems in Mathematics and Computational Science. Springer International Publishing, 2014. P. 5–36.
18. *Adj G., Menezes A., Oliveira T., and Rodríguez-Henríquez F.* Computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ using Magma // LNCS. 2015. V. 9061. P. 3–22.
19. *Adj G., Menezes A., Oliveira T., and Rodríguez-Henríquez F.* Weakness of $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ for discrete logarithm cryptography // Finite Fields and Their Applications. 2015. V. 32. P. 148–170.
20. *Joux A. and Pierrot C.* Technical history of discrete logarithms in small characteristic finite fields — The road from subexponential to quasi-polynomial complexity // Des. Codes Cryptography. 2016. V. 78. No. 1. P. 73–85
21. *Pierrot C.* The multiple Number Field Sieve with conjugation and generalized Joux — Lercier methods // LNCS. 2015. V. 2056. P. 156–170.
22. *Kim T. and Barbulescu R.* Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case. Cryptology ePrint Archive, Report 2015/1027. `http://ia.cr/2015/1027`.
23. *Pierrot C. and Barbulescu R.* The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields. Cryptology ePrint Archive, Report 2014/147. `http://ia.cr/2014/147`.
24. *Frey G. and Rück H. G.* A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves // Math. Comput. 1994. V. 62. No. 206. P. 865–874.

25. *Gaudry P., Hess F., and Smart N. P.* Constructive and destructive facets of Weil descent on elliptic curves // J. Cryptology. 2002. V. 15. No. 1. P. 19–46.
26. *Semaev I. A.* New algorithm for the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, Report 2015/310. `http://ia.cr/2015/310`.
27. *Gaudry P., Thomé E., Thériault N., and Diem C.* A double large prime variation for small genus hyperelliptic index calculus // Math. Comput. 2007. V. 76. No. 257. P. 475–492.
28. *Enge A. and Gaudry P.* A general framework for subexponential discrete logarithm algorithms // Acta Arith. 2000. V. 102. P. 83–103.
29. *Enge A., Gaudry P., and Thomé E.* An $L(1/3)$ discrete logarithm algorithm for low degree curves // J. Cryptology. 2011. V. 24. No. 1. P. 24–41.
30. *Menezes A.* The elliptic curve logarithm problem // Elliptic Curve Public Key Cryptosystems. Boston: Springer US, 1993. P. 61–81.
31. *Lenstra A. K. L* Notation // Encyclopedia of Cryptography and Security. Springer, 2011. P. 709–710.
32. *Cantor D. G.* Computing in the Jacobian of a hyperelliptic curve // Math. Comput. 1987. V. 48. No. 177. P. 95–101.
33. *Jacobson M., Menezes A., and Stein A.* Hyperelliptic curves and cryptography // Fields Institute Communications. 2004. V. 41. P. 255–282.
34. *Galbraith S.* Pairings // Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005. P. 183–212.
35. `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf` — NIST. Recommendation for Key Management, Part 1: General. 2016.
36. *Corless R. M., Gonnet G. H., Hare D. E. G., et al.* On the Lambert W function // Adv. Comput. Math. 1996. V. 5. No. 1. P. 329–359.
37. `http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf` — ECRYPT II. Yearly Report on Algorithms and Keysizes. 2012.
38. *Galbraith S. D., Hess F., and Vercauteren F.* Hyperelliptic pairings // LNCS. 2007. V. 4575. P. 108–131.
39. *Galbraith S. D.* Supersingular curves in cryptography // LNCS. 2001. V. 2248. P. 495–513.
40. *Freeman D.* Constructing pairing-friendly genus 2 curves with ordinary Jacobians // LNCS. 2007. V. 4575. P. 152–176.
41. *Freeman D.* A Generalized Brezing — Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties. Cryptology ePrint Archive, Report 2008/155. `http://ia.cr/2008/155`.
42. *Kawazoe M. and Takahashi T.* Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$ // LNCS. 2008. V. 5209. P. 164–177.
43. *Kachisa E. J.* Generating more Kawazoe — Takahashi genus 2 pairing-friendly hyperelliptic curves // LNCS. 2010. V. 6487. P. 312–326.
44. *Freeman D. M. and Satoh T.* Constructing pairing-friendly hyperelliptic curves using Weil restriction // J. Number Theory. 2011. V. 131. No. 5. P. 959–983.
45. *Drylo R.* Constructing pairing-friendly genus 2 curves with split Jacobian // LNCS. 2012. V. 7668. P. 431–453.
46. *Freeman D., Stevenhagen P., and Streng M.* Abelian varieties with prescribed embedding degree // LNCS. 2008. V. 5011. P. 60–73.
47. *Lenstra A. K. and Verheul E. R.* Selecting cryptographic key sizes // J. Cryptology. 2001. V. 14. P. 255–293.
48. `www.keylength.com` — BlueKrypt: Cryptgraphic Key Length Recommendation. 2016.

REFERENCES

1. *Menezes A., Okamoto T., and Vanstone S. A.* Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory. 1993, vol. 39, no. 5, pp. 1639–1646.
2. *Sakai R., Ohgishi K., and Kasahara M.* Cryptosystems Based on Pairing. Okinawa, Japan, 2000.
3. *Joux A.* A one round protocol for tripartite Diffie — Hellman. ANTS-IV, LNCS, 2000, vol. 1838, pp. 385–393.
4. *Boneh D. and Franklin M. K.* Identity-based encryption from the Weil pairing. CRYPTO 2001, LNCS, 2001, vol. 2139, pp. 213–229.
5. *Paterson K. G.* Cryptography from pairings. Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005, pp. 215–252.
6. *Hitt L.* On the minimal embedding field. LNCS, 2007, vol. 4575, pp. 294–301.
7. *Benger N., Charlemagne M., and Freeman D. M.* On the security of pairing-friendly Abelian varieties over non-prime fields. LNCS, 2009, vol. 5671, pp. 52–65.
8. *Galbraith S. D., Hess F., and Vercauteren F.* Aspects of pairing inversion. IEEE Trans. Inform. Theory. 2008, vol. 54, no. 12, pp. 5719–5728.
9. *Joux A.* A new index calculus algorithm with complexity $L(1/4+\mathrm{o}(1))$ in small characteristic. LNCS, 2014, vol. 8282, pp. 355–379.
10. *Barbulescu R., Gaudry P., Joux A., and Thomé E.* A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. LNCS, 2014, vol. 8441, pp. 1–16.
11. *Frey G. and Lange T.* Transfer of discrete logarithms. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2005, pp. 529–545.
12. *Miller vol. S.* The Weil pairing, and its efficient calculation. J. Cryptology, 2004, vol. 17, no. 4, pp. 235–261.
13. *Freeman D., Scott M., and Teske E.* A taxonomy of pairing-friendly elliptic curves. J. Cryptology, 2010, vol. 23, no. 2, pp. 224–280.
14. *Balakrishnan J., Belding J., Chisholm S., et al.* Pairings on hyperelliptic curves. `http://arxiv.org/abs/0908.373`, 2009.
15. *Pollard J. M.* Monte Carlo methods for index computation $\pmod p$. Math. Comput., 1978, vol. 78, no. 147, pp. 918–924.
16. *Pohlig S. C. and Hellman M. E.* An improved algorithm for computing logarithms over $\mathrm{GF}(p)$ and its cryptographic significance (Corresp.). IEEE Trans. Inform. Theory, 1978, vol. 24, no. 1, pp. 106–110.
17. *Joux A., Odlyzko A., and Pierrot C.* The past, evolving present, and future of the discrete logarithm. Open Problems in Mathematics and Computational Science. Springer International Publishing, 2014, pp. 5–36.
18. *Adj G., Menezes A., Oliveira T., and Rodríguez-Henríquez F.* Computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ using Magma. LNCS, 2015, vol. 9061. pp. 3–22.
19. *Adj G., Menezes A., Oliveira T., and Rodríguez-Henríquez F.* Weakness of $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ for discrete logarithm cryptography. Finite Fields and Their Applications, 2015, vol. 32, pp. 148–170.
20. *Joux A. and Pierrot C.* Technical history of discrete logarithms in small characteristic finite fields — The road from subexponential to quasi-polynomial complexity. Des. Codes Cryptography, 2016, vol. 78, no. 1, pp. 73–85
21. *Pierrot C.* The multiple Number Field Sieve with conjugation and generalized Joux — Lercier methods. LNCS, 2015, vol. 2056, pp. 156–170.

22. *Kim T. and Barbulescu R.* Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case. Cryptology ePrint Archive, Report 2015/1027. http://ia.cr/2015/1027.
23. *Pierrot C. and Barbulescu R.* The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields. Cryptology ePrint Archive, Report 2014/147. http://ia.cr/2014/147.
24. *Frey G. and Rück H. G.* A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comput., 1994, vol. 62, no. 206, pp. 865–874.
25. *Gaudry P., Hess F., and Smart N. P.* Constructive and destructive facets of Weil descent on elliptic curves. J. Cryptology, 2002, vol. 15, no. 1, pp. 19–46.
26. *Semaev I. A.* New algorithm for the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, Report 2015/310. http://ia.cr/2015/310.
27. *Gaudry P., Thomé E., Thériault N., and Diem C.* A double large prime variation for small genus hyperelliptic index calculus. Math. Comput., 2007, vol. 76, no. 257, pp. 475–492.
28. *Enge A. and Gaudry P.* A general framework for subexponential discrete logarithm algorithms. Acta Arith., 2000, vol. 102, pp. 83–103.
29. *Enge A., Gaudry P., and Thomé E.* An $L(1/3)$ discrete logarithm algorithm for low degree curves. J. Cryptology, 2011, vol. 24, no. 1, pp. 24–41.
30. *Menezes A.* The elliptic curve logarithm problem. Elliptic Curve Public Key Cryptosystems. Boston: Springer US, 1993, pp. 61–81.
31. *Lenstra A. K.* L Notation. Encyclopedia of Cryptography and Security. Springer, 2011, pp. 709–710.
32. *Cantor D. G.* Computing in the Jacobian of a hyperelliptic curve. Math. Comput., 1987, vol. 48, no. 177, pp. 95–101.
33. *Jacobson M., Menezes A., and Stein A.* Hyperelliptic curves and cryptography. Fields Institute Communications, 2004, vol. 41, pp. 255–282.
34. *Galbraith S.* Pairings. Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005, pp. 183–212.
35. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf — NIST. Recommendation for Key Management, Part 1: General. 2016.
36. *Corless R. M., Gonnet G. H., Hare D. E. G., et al.* On the Lambert W function. Adv. Comput. Math., 1996, vol. 5, no. 1, pp. 329–359.
37. http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf — ECRYPT II. Yearly Report on Algorithms and Keysizes, 2012.
38. *Galbraith S. D., Hess F., and Vercauteren F.* Hyperelliptic pairings. LNCS, 2007, vol. 4575, pp. 108–131.
39. *Galbraith S. D.* Supersingular curves in cryptography. LNCS, 2001, vol. 2248, pp. 495–513.
40. *Freeman D.* Constructing pairing-friendly genus 2 curves with ordinary Jacobians. LNCS, 2007, vol. 4575, pp. 152–176.
41. *Freeman D.* A Generalized Brezing — Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties. Cryptology ePrint Archive, Report 2008/155. http://ia.cr/2008/155.
42. *Kawazoe M. and Takahashi T.* Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$. LNCS, 2008, vol. 5209, pp. 164–177.
43. *Kachisa E. J.* Generating more Kawazoe — Takahashi genus 2 pairing-friendly hyperelliptic curves. LNCS, 2010, vol. 6487, pp. 312–326.
44. *Freeman D. M. and Satoh T.* Constructing pairing-friendly hyperelliptic curves using Weil restriction. J. Number Theory, 2011, vol. 131, no. 5, pp. 959–983.

45. *Drylo R.* Constructing pairing-friendly genus 2 curves with split Jacobian. LNCS, 2012, vol. 7668, pp. 431–453.
46. *Freeman D., Stevenhagen P., and Streng M.* Abelian varieties with prescribed embedding degree. LNCS, 2008, vol. 5011, pp. 60–73.
47. *Lenstra A. K. and Verheul E. R.* Selecting cryptographic key sizes. J. Cryptology, 2001, vol. 14, pp. 255–293.
48. `www.keylength.com` — BlueKrypt: Cryptgraphic Key Length Recommendation, 2016.