УДК 681.3.06

ИССЛЕДОВАНИЕ АЛГОРИТМОВ РЕШЕНИЯ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМА НА ЭЛЛИПТИЧЕСКОЙ И ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВЫХ

С.И. Збитнев, В.Ю. Ковтун, Д.В. Шевченко, А.М. Гиневский

Исследуются алгоритмы решения дискретного логарифма эллиптический и гиперэллиптической кривых. Даются временные и пространственные оценки сложности алгоритмов. Проведена классификация алгоритмов в соответствии с условиями их применения. Определены эффективные алгоритмы криптоанализа криптопреобразований на эллиптических и гиперэллиптических кривых.

1. Введение

С ростом значимости информации в жизни человека, возникает потребность в обеспечении ее конфиденциальности. Одним из способов решения этой задачи является применение криптографических средств. Из работ [32-35, 37, 58] видно, что одним из наиболее перспективных направлений в современной криптографии в модели взаимного недоверия являются криптографические преобразования в группе точек эллиптической кривой (ЭК), а также криптопреобразования в якобиане классов дивизоров гиперэллиптической кривой (ГЭК) [38]. Для оценки стойкости криптосистем в группе точек ЭК и классах дивизоров ГЭК необходимо проанализировать сложность криптоаналитических преобразований при различных условиях и ограничениях использования. В основе приведенных криптопреобразований лежит проблема дискретного логарифмирования в группе чисел и полиномов поля (DLP), в группе точек эллиптической кривой (ECDLP) и в якобиане классов дивизоров гиперэллиптической кривой (HECDLP) соответственно.

Целью статьи является классификация многообразия алгоритмов решения DLP, ECDLP, HECDLP и для определения наиболее эффективных из них, а также накладываемых ограничений и условий применения известных криптопреобразований. Кроме того, исследуются возможность использования ГЭК, проводится сравнение стойкости используемых и перспективных криптопреобразований.

2. Классификация существующих методов решения DLP

Определим основные типы алгоритмов, которые будут рассмотрены ниже с точки зрения выполнимости и точности результата:

- Детерминированные/точные алгоритмы– алгоритмы, которые работают согласно стратегии поиска дающей точное решение;

- Вероятностные алгоритмы – алгоритмы, которые выбирают случайную стратегию поиска решения и не дающее точное решение;

- алгоритмы Монте-Карло – вероятностные алгоритмы, которые работаю до получения точного результата с заданной вероятностью решения или неправильного – в противном случае;

- Лас-Вегас алгоритмы – вероятностный алгоритм, который дает точное решение с заданной вероятностью или неизвестное решение.

Пусть даны групповые элементы g (генератор поля) и h, тогда под **решением DLP** будем понимать решение уравнения $h = g^l$ относительно l или доказательство того, что решения не существует. Необходимым условием является $h \in \langle g \rangle$, т.е. $l \in [0, \mathrm{ord}(g) - 1]$ и $h^{\mathrm{ord}(g)} = 1$, где $l, g, h \in GF(q)$, n - порядок элемента образующего группу $n = \mathrm{ord}(g)$, l - секретный ключ, h- открытый ключ.

В дальнейшем будем пользоваться обобщенным понятием задачи дискретного логарифма (DLP).

Различают «**стандартную DLP**» с известным порядком образующего элемента группы, в которой решение находится в интервале $[1, n]$, и с «**неизвестным порядком DLP».**

В [3] предложена классификация задач DLP на основе известной информации о решении, в соответствии с которой выделяют четыре типа задач:

1. С известным интервалом.
2. С известным весом Хемминга.
3. С решением лежащим в известном классе.
4. С известным распределением.

Недостатком подхода изложенного в [3] является узконаправленная применимость и невозможность ее применения к решению более широкого круга задач.

В связи с этим представляется целесообразным проведение более детальную классификацию всех алгоритмов решения DLP с учетом данных представленных в [3].

Учитывая результаты [3], а также введения в рассмотрение возможности дополнительной информации о решении, проведем следующую классификацию алгоритмов решения DLP, ECDLP, HECDLP.

В таблице 1 приведена сложность алгоритмов решения задачи DLP в поле.

Таблица 1.

№	Название алгоритмов	Поле	Сложность	Т
1	Обобщенное решето поля чисел [31, 35 annex D]	$GF(p)$	Требуется $O\left(\exp\left((64/9)^{1/3} + o(1)\right)(\ln p)^{1/3}(\ln\ln p)^{2/3}\right)$ групповых операций.	Д
2	Обобщенное решето поля чисел [35 annex D]	$GF(2^m)$	Требуется $O\left(\exp\left(1.587 m^{1/3}(\ln m)^{2/3}\right)\right)$ групповых операций.	Д
3	Алгоритм Adleman-Coppersmith [36, 55]	$GF(2^m)$	Требуется $O\left(\exp\left((c + o(1)) m^{1/3}(\log m)^{2/3}\right)\right)$ групповых операций, где $c \approx 1.4$.	Д

Пусть даны точки $P, Q \in E(GF(q))$, тогда **решением ECDLP** будем понимать решение уравнение $Q = lP$ относительно l или доказательстве, что решение не существует. Необходимым условием является $Q \in \langle P \rangle$, т.е. $l \in [0, \mathrm{ord}(P) - 1]$,

причем $\text{ord}(P)\cdot Q = O$, где P - базовая точка, образующая группу, n - порядок базовой точки $n = \text{ord}(P)$, l - секретный ключ, Q- открытый ключ, O - точка на бесконечности.

В таблице 2 приведены универсальные алгоритмы решения задачи DLP, которые могут быть применены к произвольному абелевому многообразию (DLP, ECDLP, HECDLP),.

Таблица 2.

№	Условие применения	Сложность	Т
Универсальные			
1. Алгоритм простого поиска (лобовой поиск, прямой перебор, грубой силы)			
1	над различными полями	Требуется $O(n)$ групповых операций [31].	Д
2. Алгоритм Pohling-Hellman [25]			
2	над различными полями	$O\left(p^{1/2}(\log n)^{O(1)}\right)$ групповых операций, где p - наибольший простой делитель n.	Д
3. Алгоритм больших и малых шагов (алгоритм Shanks'a)			
3	над различными полями	В классической реализации [3, 37] требуется $\sqrt{n} + 2\lfloor l/\sqrt{n} \rfloor + O\left(\log_2 \sqrt{n}\right)$ групповых операций.	Д
3.1. Известны ограничения решения			
1	если $l \geq \sqrt{n}$	Требуется $\lfloor \sqrt{n} \rfloor + \lfloor l/\sqrt{n} \rfloor + O\left(\log_2 \left(\sqrt{n}\right)\right)$ групповых операций, пространственная сложность $O(\sqrt{n})$ [3, 37, 62].	Д
2	неизвестен порядок, $k < l$	Требуется $O\left(\sqrt{n}\right)$ групповых операций, где k - принятая граница для l [3, 37, 62].	Д
3.2. Решение на отрезке			
1	решение на отрезке $[a, b]$	Требуется $\sqrt{n} + \lfloor (l-a)/\sqrt{n} \rfloor + O\left(\log\left(a\sqrt{n}\right)\right)$ групповых операций [3, 37, 62].	Д
2	решение на отрезке $[a, b]$	В классической реализации требуется, m малых шагов, $\lfloor (l-a)/m+1 \rfloor$ больших шагов, где $m = \lfloor \sqrt{b-a} \rfloor$, $n \in [a, b]$, $a < b$. Необходимо предвычислить $-aP$ и необходимо хранить в памяти m пар (jP, j) [23, 24, 62].	Д
3	решение на отрезке $[a, b]$, $a = 0$	Необходимо $m+1$ малых шагов, $\text{Ne}(l/2m)$ больших шагов. Предвычислить $2mP$, которое может быть получено как удвоение последнего малого шага mP и хранить в памяти $m+1$ пару (jP, j). Подход оптимален, если $m \approx \sqrt{E/2}$, где E - ожидаемое значение l, тогда требуется $\sqrt{2E}$ групповых операций (больших и малых шагов), т.е. сложность меньше на множитель $\sqrt{2}$, чем для случая 2 [23, 24, 62].	Д
4	решение на отрезке $[a, b]$, $a \neq 0$	Необходимо $m+1$ малых шагов, $\text{Ne}(l/2m)$ больших шагов. Хранить $2m+1$ малых шагов и предвычислить $aP, 2mP$. Подход оптимален, если $m \approx \sqrt{E}$, где E - ожидаемое значение $(l-a)$ [23, 24, 62].	Д

Продолжение таблицы 2.

№	Условие применения	Сложность	Т
5	поиск решения происходит от средины к краям отрезка $[a,b]$	Необходимо m малых шагов, $\lceil \lvert l-K \rvert / m \rceil$ больших шагов. Предвычислить KP, mP и хранить m пар (jP, j), где $K=(a+b)/2$, $m=\lfloor \sqrt{(b-a)/2} \rfloor$. Если l распределено симметрично относительно K и распределение $\lvert l-K \rvert$ - IHR распределение, то алгоритм оптимален, если $m \approx \sqrt{E}$, где E - ожидаемое значение $\lvert l-K \rvert$ и имеет ожидаемое время работы $2\sqrt{E}$ больших и малых шагов [23, 24, 62].	Д
3.3. Известен закон распределение решения			
1	равномерное распределение вероятности решения на отрезке $[a,b]$	Необходимо $\lfloor \sqrt{b-a} \rfloor /2$ больших шагов, $\lfloor \sqrt{b-a} \rfloor$ малых шагов. Возможно минимизировать среднее время, если работать с множеством малых шагов размером $\lfloor \sqrt{(b-a)/2} \rfloor$, которое требует в среднем $\lfloor \sqrt{(b-a)/2} \rfloor$ больших шагов и $\lfloor \sqrt{3(b-a)/2} \rfloor$ малых шагов [23, 24, 62].	Д
2	IHR распределение вероятности решения на отрезке $[a,b]$	Необходимо m больших и m малых шагов, где $m=Ne(\sqrt{E})$, E - ожидаемое значение $l-a$. Необходимо предвычислить $-aP$ и необходимо хранить в памяти m пар (jP, j). Distribution Increasing Hazard Rate (IHR) – распределение с увеличивающейся степенью риска, к ним относится: равномерное, нормальное, геометрическое распределения [23, 24, 62].	Д
3.4. Модификации			
3.4.1. Алгоритм Buchmann - Jacobson – Teske			
1	ГЭК и ЭК над различными полями	Основан на динамическом увеличением большого шага [3, 56] требует $4\lfloor \sqrt{l} \rfloor + O(\log_2 l)$ групповых операций, пространственная сложность $O(2\lfloor \sqrt{l} \rfloor)$.	Д
3.4.2.Алгоритм Terr'a (треугольный метод) с динамическим увеличением большого шага			
1	ГЭК и ЭК над различными полями	Основан на увеличении длины большого шага после каждого маленького. Требуется $O(2\lfloor \sqrt{2l+1/4} \rfloor)$ групповых операций, пространственная сложность $O(\lfloor \sqrt{2l+1/4} \rfloor)$ [3, 51, 62].	Д
2	решение на отрезке $[a,b]$	Требуется выполнить j малых шагов, j больших шагов, необходимо предвычислить aP, хранить $j+1$ пар (kP, k), где $j=Ne(\sqrt{2(l-a)+1/4})$, или без использования симметрии: $\sqrt{2(l-a)}$ малых шагов, $\sqrt{2(l-a)}$ больших шагов, хранить $\sqrt{2(l-a)}+1$ пар (jP, j), предвычислить значение aP [23, 24, 51, 62].	Д
3	поиск решения от начала до конца отрезка $[a,b]$, $a=0$	Необходимо $2\sqrt{\lceil l+1 \rceil}$ малых шагов, $\lfloor \sqrt{l+1} \rfloor$ больших шагов, удвоений $\lfloor \sqrt{l+1} \rfloor$. Хранить $\lfloor \sqrt{l+1} \rfloor$ пар (jP, j). Аналогичный подход может требовать выполнить $3\sqrt{\lceil l+1 \rceil}$ малых шагов, $\lfloor \sqrt{l+1} \rfloor$ больших шагов. Хранить $\lfloor \sqrt{l+1} \rfloor$ пар (jP, j) [23, 24, 51, 62].	Д

Продолжение таблицы 2.

№	Условие применения	Сложность	Т
4	поиска решения от начала до конца отрезка $[a,b]$, $a \neq 0$	Необходимо $2\sqrt{\lceil l+1 \rceil}$ малых шагов, $\lvert\sqrt{l+1}\rvert$ больших шагов, удвоений $\lvert\sqrt{l+1}\rvert$. Хранить $\lvert 2\sqrt{l+1}\rvert$ пар (jP, j). Аналогичный подход может требовать выполнить $3\sqrt{\lceil l+1 \rceil}$ малых шагов, $\lvert\sqrt{l+1}\rvert$ больших шагов. Хранить $\lvert 2\sqrt{l+1}\rvert$ пар (jP, j) [24, 51, 62].	Д
5	поиск решения происходит от средины к краям отрезка $[a,b]$	Необходимо $2j$ малых шагов, j больших шагов и предвычислить KP и хранить $j+1$ пар $((K+k)P, K+k)$, где $K=(a+b)/2$, $j=\mathrm{Ne}\left(\sqrt{2\lvert l-K\rvert+1/4}\right)$ [24, 51, 62].	Д
3.5. Распараллеленный алгоритм больших и малых шагов [3]			
1	ГЭК и ЭК над различными полями	На r процессорах с неограниченным и мгновенным доступом к памяти, уменьшение сложности происходит на множитель $\sqrt{r}$, алгоритм не дает линейного уменьшения сложности.	Д
4. Алгоритм ρ - Полларда			
1	ГЭК и ЭК над различными полями	Требуется $\sqrt{\pi n/2}+O(\log n)$ групповых операций [1, 3].	В
2.	ГЭК и ЭК над различными полями	С алгоритмом Brent'a. Требует $1.97\sqrt{n}$ групповых операций. Этот вариант имеет большую пространственную сложность, но меньше групповых операций, в сравнении с классическим [3, 52].	В
3	решение на отрезке $[a,b]$	Знание величины $l \bmod \lvert\sqrt{n}\rvert$ позволяет уменьшить сложность на множитель $\sqrt{\gcd(\lceil\sqrt{n}\rceil, n)}$, т.е. работая в группе с образующим элементом $F=\lvert\sqrt{n}\rvert P$, сложность не уменьшается, если n - простое. Требуется $O\left(\left(\sqrt{\pi n/2}+\log n\right)/\sqrt{\gcd(\lceil\sqrt{n}\rceil, n)}\right)$.	В
4	ГЭК и ЭК над различными полями	Алгоритм Teske с улучшенными случайными шагами, в количестве равном 20 [3, 53, 76]. Требует $1.26\sqrt{n}$ групповых операций.	В
5	ГЭК и ЭК над различными полями	Алгоритм Howitz-Venkatesan с улучшенными аддитивными, случайными шагами, в количестве равном *r*. [3, 57]. Основан на r-аддитивных, случайных шагах по r-регулярному графу Cayley над $\langle P\rangle$, который генерирован посредством r-случайными групповых элементов, тогда решение заключается в отыскании с помощью алгоритма ρ - Полларда не тривиальных циклов в графе Cayley. Число $r=const\cdot\log n$, а также при допущении о существовании t независимых хеш-функций для навигации по графу, $t=const\cdot\log^2 n$, сложность алгоритма составит $O\left(\left(\log^c n\right)\sqrt{n}\right)$ групповых операций, где c - небольшая константа.	В
6	ГЭК и ЭК над различными полями	Алгоритм Sattler, Schnorr с улучшенными случайными шагами в 8 раз [3, 50]. Сложность неизвестна.	В
4.1. Распараллеленный алгоритм ρ - Полларда			
1	ГЭК и ЭК над различными полями	Алгоритм Van Oorschot, Wiener [3, 17, 54]. Основан на методе отмеченных точек [39]. Требуется $O\left(\sqrt{\pi n}/(2r)+1/\Theta\right)$ групповых операций, пространственная сложность $\Theta\sqrt{\pi n/2}$, где Θ - доля отмеченных (отличающихся) точек.	В
2	ГЭК и ЭК над различными полями	Алгоритм Pollard'a [34]. Требуется $O\left(\sqrt{\pi n/2}/r\right)$ групповых операций.	В

Продолжение таблицы 2.

№	Условие применения	Сложность	Т
3	ГЭК и ЭК над различными полями	Алгоритм Brent'a [3, 49]. На r процессорах с неограниченным и мгновенным доступом к памяти требуется $O\left(\sqrt{\pi n/2r}\right)$, т.е. уменьшение сложности происходит на множитель $\sqrt{r}$, алгоритм не дает линейного уменьшения сложности.	В
		5. Алгоритм λ - Полларда	
1	решение принадлежит $[a, b]$	Требуется $3.3\sqrt{b-a}$ групповых операций или $2\sqrt{b-a}$ групповых операций, при двукратном увеличении памяти и двух процессорах, для применения стратегии инверсных точек. λ - метод быстрее ρ - метода, если $(b-a) < \mathrm{ord}(P)\cdot\pi/8$ и значение $l \in [\mathrm{ord}(P)\cdot\pi/8,\ \pi/8\ ]$ [3].	В
2	случайное распределение вероятности решения на отрезке $[a, b]$	Для распараллеленного алгоритма [3], сложность всегда ограничена величиной $O\left(3\sqrt{b-a}/r + 1/\Theta\right)$ групповых операций, где Θ - доля отмеченных точек.	В
3	стандартный ECDLP на отрезке $[a, b]$	Для нахождения решения с вероятностью $p = 0.9989$, требуется $4\sqrt{b-a}$ групповых операций.	В
		5.1. Распараллеленный алгоритм λ - Полларда	
1	ГЭК и ЭК над различными полями	Алгоритм Van Oorschot, Wiener [1, 3, 54]. Требуется $O\left(2\sqrt{b-a}/r + 1/\Theta\right)$ групповых операций, где r – количество процессоров, Θ - доля отмеченных точек.	В
2	ГЭК и ЭК над различными полями	Алгоритм Pollard'a [1, 3, 48]. Требуется $\sqrt{(b-a)/(uv)} + 1/\Theta$ групповых операций, где $\gcd(u, v) = 1$, $u \approx v \approx r/2$, $u + v \le r$, r - количество процессоров, Θ - доля отмеченных точек.	В
		6. Алгоритм множественного логарифмирования (R. Silverman – Stapleton) [31, 47]	
1	ГЭК и ЭК над различными полями	Если для заданной кривой и базовой точки уже была решена ECDLP за время t, тогда для решения ECDLP для той же кривой и базовой точки потребуется: во второй раз потребуется времени $\left(\sqrt{2}-1\right)t \approx 0.41t$; в третий раз потребуется времени $\left(\sqrt{3}-\sqrt{2}\right)t \approx 0.32t$; в четвертый раз потребуется времени $\left(\sqrt{4}-\sqrt{3}\right)t \approx 0.27t$; - в i раз потребуется времени $\left(\sqrt{i}-\sqrt{i-1}\right)t$.	В
		7. Алгоритм Index – calculus	
1	Для ЭК для кривых над любым полем	Алгоритм Kraitchik'a [27]. Не существует алгоритма для решения ECDLP на основе index-calculus алгоритма для решения DLP имеющего сложность меньшую или равную сложности атаки грубой силой $O(n)$.	В
2	Для ЭК для кривых над любым полем	Алгоритм Adleman, Western, Miller [32]. Не существует алгоритма для решения ECDLP на основе index-calculus алгоритма для решения DLP имеющего сложность меньшую или равную сложности атаки грубой силой $O(n)$.	В
		8. Алгоритм Xedni – calculus	
1	$E(GF(p))$, p - простое.	Предполагаемое [9, 12] асимптотическое время работы требует $O(p)$ групповых операций, что аналогично атаке грубой силы.	Д
		9. Алгоритм GenLog	
1	ГЭК и ЭК над различными полями	Алгоритм типа Las Vegas, основанный на угловой упаковке и покрытии [11]. Требуется $O\left(\sqrt{n}\right)$ групповых операций.	В

В таблице 3 приведены вычислительные и пространственные сложности алгоритмов решения ECDLP, с учетом специфических особенностей.

Таблица 3

№	Условие применения	Сложность	Т
10. Для аномальных эллиптических кривых (след отображения Frobenius'а равен 1)			
1	$E_{a,0}\left(GF\left(p^l\right)\right)$, $a \neq 0 \bmod p$, $l \equiv 1 \bmod 2$, $p \equiv 1 \bmod 4$	Модифицированный алгоритм ρ - Полларда [16]. Используют аддитивные шаги и отображение Frobenius $(x,y) \to \left(x^p, y^p\right)$, для понижения сложности на множитель $2\sqrt{l}$. Для варианта алгоритма Teske со сложностью $1.25\sqrt{n}$, имеем $0.625\sqrt{n/l}$. Для $p \equiv 3 \bmod 4$ применима MOV атака.	В
2	$E_{0,b}\left(GF\left(p^l\right)\right)$, $b \neq 0 \bmod p$, $l \equiv 1 \bmod 2$, $p \equiv 1 \bmod 3$	Модифицированный алгоритм ρ - Полларда [16]. Используются аддитивные шаги и отображение Frobenius'а $(x,y) \to \left(x^p, y^p\right)$, для понижения сложности на множитель $\sqrt{6l}$. Для варианта алгоритма Teske со сложностью $1.25\sqrt{n}$, имеем $0.208\sqrt{n/l}$. Для $p \equiv 2 \bmod 3$ применима MOV атака.	В
11. Алгоритм на основе MOV условия			
1	$E\left(GF\left(q\right)\right)$ - суперсингулярная кривая	Алгоритм Menezes – Okamoto – Vanstone на основе спаривания Weil'я [20]. Существует вероятностный полиномиальный алгоритм Miller'а перехода от ECDLP в $E\left(GF\left(q\right)\right)$ к DLP в подгруппе $GF\left(q^k\right)^*$ со сложностью $O\left(\ln q\right)$ групповых операций. Требуется $L[\alpha, x] = \exp\left((c+o(1))(\ln x)^{\alpha}(\ln\ln x)^{1-\alpha}\right)$ групповых операций, где $\alpha \in (0,\ 1)$, $o(1)$ - бесконечно малое число, которое стремится к нулю с ростом основания поля. Сложность субэкспоненциальная лишь для суперсингулярных кривых.	В
12. Алгоритм на основе FR условия			
1	$E\left(GF\left(q\right)\right)$, суперсингулярных кривых	Алгоритм Fray – Rück на основе спаривания Tate [21]. Существует переход от ECDLP $E\left(GF\left(q\right)\right)$ к DLP в подгруппе $GF\left(q^k\right)^*$. Требуется $L_q[\alpha, c] = \exp\left((c+o(1))(\log q)^{\alpha}(\log\log q)^{1-\alpha}\right)$ групповых операций, где $\alpha = 1/2$, для решения ECDLP в произвольном $GF\left(q\right)$. С другой стороны, при степени расширения $k < (\log q)^2$ решение ECDLP происходит посредством решета поля чисел и имеет туже сложность, но с $\alpha = 1/3$.	В
13. Алгоритм для кривых над композитным двоичным полем			
1	$E\left(GF\left(2^{tk}\right)\right)$, $m = tk$, $a, b \in \{0, 1\}$	Алгоритм Gallant - Lambert - Vanstone [15, 34], являющийся модификацией с использованием отображения Frobenius'а, распараллеленного алгоритма λ - Полларда требует $O\left(\sqrt{\pi n/t}/(2r)\right)$ групповых операций, где r - количество процессоров. В [8] даются рекомендации по уменьшению объема памяти для эффективной реализации распараллеленного λ - Полларда**.**	В
2	$E\left(GF\left(2^{tk}\right)\right)$	Алгоритм Wiener - Zuccherato с использованием стратегии инвертирования точек [3], являющийся модификацией алгоритма ρ - Полларда [45] требует $\sqrt{\pi n/2}$ групповых операций. Модификация состоит в использовании стратегии инверсных точек, т.е. каждой точке P ставится в соответствие ее инверсия $-P$. В результате чего, посредством отображения Frobenius'а точка P отображается в A, а точка $-P$ в точку $-A$. Требуется $O\left(\sqrt{\pi n}/2\right)$ групповых операций. Возможно расширение идеи, до m/k классов эквивалентности посредством отображения Frobenius'а, где $m = tk$, а не двух, как в [45], что приведет к понижению сложности до $\sqrt{\pi m/(2k)} = \sqrt{\pi t/2}$, групповых операций [46].	В

Продолжение таблицы 3

№	Условие применения	Сложность	Т
14. Алгоритм Semaev- Smart - Satoh - Araki для аномальных кривых над простым полем [13]			
1	$E(GF(p))$ - кривая со следом 1.	Алгоритму требуется полиномиальное количество операций для решения ECDLP любым из универсальных методов, например Pohlig-Hellman, т.к. происходит приведение ECDLP к DLP в аддитивной группе $F_p = \{0, \ldots, p-1\}$.	Д
15. Алгоритм Gaudry – Hess - Smart			
1	$E(K)$: 1. $t \equiv 1 \bmod 2$; 2. $m = t$; 3. $Tr_{K/F_2}(a) = 0$, $K = GF(q^t)$, $k = GF(2^k)$.	Алгоритм использует спуск Weil'я, для приведения ECDLP на $E(F_q)$ к HECDLP в подгруппу порядка $r \approx q^t$ якобиана $J_C(k)$ гиперэллиптической кривой $C(k)$ рода g. Согласно [7, 26], требуется - $O\left(q^{\frac{2g}{g+1}+e}\right)$ групповых операций для $q = 2^k$, K и фиксированных значениях $t \geq 4$, $q \to \infty$, т.е. для K имеем $O\left(2^{\frac{2kg}{g+1}+e}\right)$ групповых операций. Причем "магическое" число $m = \dim_{F_2}\left(\mathrm{Span}_{F_2}\left\{\left(1, b_i^{1/2}\right), i = \overline{0, t-1}\right\}\right)$, $1 \leq m < t$ в ограничениях Weil'я.	Д
2	$E(K)$, $q = 2^m$, $K = GF(q^n)$	Согласно [14]: 1. Пусть $m/2 \leq 2g/(g+1)$, тогда для решения DLP в $J_C(GF(F_q))$ пользуются алгоритмом ρ - Полларда, тогда общая сложность $O(g^2 q^{m/2} \log^2 q)$. 2. Пусть $m/2 > 2g/(g+1)$ и $g < 10$, тогда для решения DLP в $J_C(GF(F_q))$ пользуются алгоритмом Gaudry, тогда общая сложность $O(g^2 q \log^2 q(gq + g!))$ битовых операций при фиксированном g, требуется $O(q^{2+e})$ групповых операций; 3. Пусть $g \geq 10$, тогда для решения DLP в $J_C(GF(q))$ пользуются алгоритмом Enge-Gaudry, тогда общая сложность $O\left(\exp\left(\left(\sqrt{2} + o(1)\right)\sqrt{(g \log q)\log(g \log q)}\right)\right)$ операций. Атака считается удачной, если род g кривой C - достаточно мал, чтобы алгоритмы Gaudry или Enge-Gaudry были эффективнее алгоритма ρ - Полларда. Атака считается неудачной, если или q^g - слишком большое $q^g \geq 2^{1024}$, или $g = 1$, в этом случае $J_C(GF(q))$ отображается в $E(GF(q))$. В [60] показано, что неприменимость этой атаки не влечет за собой неприменимость методологии спуском Weil'я.	В
16. Алгоритм Galbraith – Hess – Smart			
1	$E(K)$, $q = 2^m$, $K = GF(q^n)$	Алгоритм [7, 73, 74, 75] использует спуск Weil'я и эффективный метод поиска изогенных эллиптических кривых над полями, с характеристикой отличной от 2, для уже взломанных, и является модификацией Hafner – McCurley [38] алгоритма и требует $O(q^{m/4+e})$ групповых операций. Причем в [74] используется алгоритм Enge-Gaudry для решения HECDLP.	В

Пусть дана гиперэллиптическая кривая $C(GF(q))$ рода g и приведенные дивизоры $D_1, D_2 \in J(GF(q))$, под **решением HCDLP** будем понимать решение уравнения $D_2 = lD_1$ относительно l или доказательстве, что решение не существует, где $J(GF(q)) = D^0/\mathrm{P}$ - якобиан, P - множество основных дивизоров, D^0 - множество дивизоров степени 0, n - порядок дивизора D_1, т.е. $n = \mathrm{ord}(D_1)$, l - секретный ключ, D_2- открытый ключ.

Наиболее удачным для решения HECDLP считается алгоритм Index-calculus. Некоторые идеи, при решении DLP, могут быть применимы и для вычисления HECDLP в якобиане $J_C(k)$ гиперэллиптической кривой C, рода g над полем $k = \mathbf{F}_q$ в мнимой квадратичной форме. Если род g значительно больше по сравнению с q, тогда субэкспоненциальное временем работы вероятностного алгоритма с известным $n = q^g$ обозначают $O(L_n[c])$, где $L_{q^g}[c] = \exp\left(\left(c + o(1)\sqrt{g \log q \log g \log q}\right)\right)$ для некоторой положительной константы c.

Для алгоритмов решения HECDLP предлагается рассмотреть три стратегии [38, 61]:

1. В основе первой стратегии лежит идея, предложенная Hafner'ом и McCurley'ом (HM) для ЗДЛ в полях мнимых квадратичных чисел. Напомним, что структура $J_C(k)$ якобиана кривой C, определяется как прямая сумма циклических подгрупп. Представления дивизоров D_1 и D_2 задается посредством прямой суммы циклических подгрупп, тогда решение DLP сводится к решению СЛУ, для найденных представлений дивизоров D_1 и D_2, составленной с использованием обобщенной китайской теоремы об остатках.

2. Вторая стратегия улучшает первую посредством дополнительных знаний $\#J_C(k)$. Предположение, что известен порядок $\#J_C(k)$, что позволяет заменить вычислительно сложное определение SNF, как в предыдущей стратегии, на решение системы линейных уравнений по модулю $\#J_C(k)$.

3. Гибридная стратегия. Предложена Vollmer в контексте поля квадратичных чисел [38], что может быть легко применимо к HECDLP. Эта стратегия является комбинацией двух предыдущих, с заменой вычислительно сложного вычисления SNF на решение системы линейных уравнений над целыми или если известен порядок группы, то по модулю $\#J_C(k)$. Этот метод может быть полезен, если существует метод генерации соотношений, который быстрее чем для генерации.

В таблице 3 приведем алгоритмы решения задачи HECDLP.

Таблица 3.

№	Условия применения	Сложность	Т
		1. Алгоритм Adleman - DeMarrais – Huang	
1	$C(GF(q))$, q - произвольное	Алгоритм Bauer'а [38, 10], в котором сделаны основные улучшения стратегии 1: 1. $J_C(k)$ сгенерирован всеми простыми дивизорами степени $\log_q L_{q^{2g+1}}[c]$, где c - положительное действительное число. 2. Вероятность того, что $D = \mathrm{div}(a, b)$ является t - гладким, равна вероятности того, что полином степени $\deg a$ над k может быть разложен на множители степени t. Bauer показал, что это предположение требует $O\left(L_{q^{2g+1}}[9/(16c)]\right)$ попыток разложения, при условии, что $\log q \le (2g+1)^{0.98}$. Общая сложность составляет $O\left(L_{q^{2g+1}}[c]\right)$, где $c = 3(l+1)/\left(4\sqrt{l}\right)$.	В

Продолжение таблицы 4

№	Условие применения	Сложность	Т
2	$C(GF(q))$, q - нечетное простое	Алгоритм основан на стратегии 1 и не требует знания $\#J_C(k)$. Требуется $O(L_{q^{2g+1}}[c])$ групповых операций если $\log q \le (2g+1)^{0.98}$ для $0 < c < 2.313$ [38, 10].	В
		2. Алгоритм Gaudry	
1	$C(GF(q))$, $g < 10$ - небольшое	Алгоритм основан на знании $\#J_C(k)$, что позволяет решать систему линейных уравнений по модулю $\#J_C(k)$, согласно стратегии 2. Требуется $O(g!qc_j) + O((g!q + gq^2)(c_n + c_{q,g})) + O(qc_q)$, групповых операций где $c_{q,g} = g\log q$, $c_q = \log q$, $c_j = g\log q$, $c_n = g\log q$, т.е. $O(gq^2 + g!q)$ групповых операций [10, 13]. Возможно уменьшение сложности за счет уменьшения размера базы разложения [26], при соотношении «годных» дивизоров $\frac{1}{l}$, время генерации соотношений увеличится на множитель l^g, но будет требоваться l раз меньше соотношений и сложность решения системы линейных уравнений уменьшится в l^2 раз. Оптимальным значение $l = O((q/g!)^{1/(g+1)})$ и сложность тогда $O\left(q^{\frac{2g}{g+1}+\varepsilon}\right)$ при $q \to \infty$.	В
2	$C(GF(q))$, $g < 10$ - небольшое	При наличии эффективно вычислимого нетривиального автоморфизма порядка m в $J_C(k)$, возможно понижение сложности алгоритма решения HECDLP на множитель $\sqrt{m}$, благодаря наличию m классам эквивалентности [16].	В
3	$C(GF(q))$, $g < 10$ - небольшое	Требуется $O(g^3q^2\log^2 q + g^2g!q\log^2 q)$ битовых операций, одна групповая операция согласно алгоритма Cantor'а требует $O(g^2\log^2 q)$ или же $O(gq^2 + qg!)$ групповых операций, при фиксированном g, требуется $O(q^{2g/(g+1)+e})$ групповых операций [13, 14, 38]. Алгоритм учитывает знание $\#J_C(k)$ для решения системы линейных уравнений по модулю $\#J_C(k)$. Алгоритм построен согласно стратегии 2. После построения базы разложения S (рассматриваются простые дивизоры степени 1), случайными шагами [3] предложенными Teske во множестве приведенных дивизоров эквивалентных $\alpha D_1 + \beta D_2$. Каждый 1-гладкий дивизор образует соотношение, остальная часть алгоритма аналогична алгоритму Bauer - Enge. Анализ [38] этого алгоритма показал, что его алгоритм становится эффективнее любого универсального алгоритма для $g > 4$. Т.е. лучше алгоритма Полларда, когда $n/2 > \frac{2g}{g+1}$ [13], но становится практически неприменимым при $g > 10$, сказывается $g!$.	В
		3. Алгоритм Enge	
1	$C(GF(q))$, q - произвольное, g - большое	Требуется $O\left(\exp\left(\frac{5\sqrt{3}}{2}\left(\sqrt{1+\frac{3}{\theta}}+\sqrt{\frac{3}{\theta}}\right)+o(1)\right)\sqrt{(g\log q)\log(g\log q)}\right)$ операций, где $g \ge \theta\log q$, θ - заданная положительная константа [4].	В

Продолжение таблицы 4

№	Условия применения	Сложность	Т
2	$C(GF(q))$, q - произвольное, g - большое	Этот алгоритм [38], как и алгоритм Flassenberg – Paulus, основан на стратегии Hafner – McCurley. Enge доказал, что база разложения образует $J_C(k)$ [42] и доказал необходимость t-гладкости простых дивизоров в ней. В дополнение, первым проиллюстрировал зависимость времени работы алгоритма от отношения g и $\log q$. Доказал, что если $g \geq \upsilon \log q$, тогда $n \in O\left(L_{q^g}\left\lfloor \rho + \frac{1}{\sqrt{\upsilon}} \right\rfloor\right)$ и количество итераций до отыскания соотношений $O\left(L_{q^g}\left\lfloor \frac{1}{2\rho} \right\rfloor\right)$, для решения системы линейных уравнений требуется $O\left(L_{q^g}[l\rho]\right)$, для генерации соотношений $O\left(L_{q^g}\left\lfloor 2\rho + \frac{2}{\sqrt{\upsilon}} + \frac{1}{2\rho} \right\rfloor\right)$. Для генерации одной случайной линейной комбинации элементов базы разложения. Положив $l = 4$ для решения системы линейных уравнений оптимальное значение для $\rho = 0{,}5\left(\sqrt{1 + \frac{1}{\sqrt{\upsilon}}} + \sqrt{\frac{1}{\sqrt{\upsilon}}}\right)$. Общая сложность $O\left(L_{q^g}[c]\right)$, где $c = 2\left(\sqrt{1 + \frac{1}{\sqrt{\upsilon}}} + \sqrt{\frac{1}{\sqrt{\upsilon}}}\right)$. Неприменим, если $q^g \approx 2^{1024}$.	
4. Алгоритм Enge-Gaudry			
1	$C(GF(q))$, q - произвольное, g - большое.	Алгоритм построен на основе стратегии 2. Алгоритм учитывает знание $\# J_C(k)$ и требует сохранения t-гладкости простых дивизоров. Является модификацией ρ - Полларда требует $O\left(\exp\left(\left(\sqrt{2} + o(1)\right)\sqrt{(g \log q)\log(g \log q)}\right)\right)$ групповых операций [7, 16, 18, 21].	В
2	$C(GF(q))$, q - произвольное, g - большое.	Согласно [29] требуется $O\left(\exp\left((1 + o(1))\sqrt{(2g+1)\log q \log((2g+1)\log q)}\right)\right)$ групповых операций.	В
3	$C(GF(q))$, q - произвольное, g - большое.	Требует $O\left(L_{q^g}[c]\right)$ групповых операций, $c = \sqrt{2}\left(\sqrt{1 + \frac{1}{2\upsilon}} + \sqrt{\frac{1}{2\upsilon}}\right)$, $g \geq \upsilon \log q$ для некоторой константы $\upsilon \geq 0$ [38].	В
5. Алгоритм Muller-Stein-Thiel			
1	$C(GF(q))$, q - нечетное простое	Алгоритм [38], использует инфраструктуру действительного квадратичного поля функций согласно стратегии 1 для поиска решения. В [40] рассматривается сведение HECDLP над полем нечетной характеристики и в [41] для четной характеристики, за полиномиальное время к DLP. Paulus - Ruck обобщили этот результат и показали, что HECDLP сводим за полиномиальное время к DLP над расширением поля, над которым задана кривая. В [42] показано, что при $\log q \leq 2g + 2$ и $n \in O\left(L_{q^{2g+1}}[\rho]\right)$, количество попыток для отыскания соотношений составляет $O\left(L_{q^{2g+1}}\left\lfloor \frac{1}{4\rho} \right\rfloor\right)$, для решения систему линейных уравнений требуется $O\left(L_{q^{2g+1}}[5\rho]\right)$ и для генерации соотношений требуется $O\left(L_{q^{2g+1}}\left\lfloor 2\rho + \frac{1}{4\rho} \right\rfloor\right)$. Требуется $m \in O\left(L_{q^{2g+1}}[\rho]\right)$ соотношений, сложность для вычисления случайной степени-произведения идеалов $O\left(L_{q^{2g+1}}[\rho]\right)$. Оптимальное значение $\rho = \frac{5}{2\sqrt{3}}$ и общая сложность составляет $O\left(L_{q^{2g+1}}[1.44]\right)$.	В
6. Алгоритм Galbraith – Hess – Smart			
	$C(GF(q))$, q - произвольное	Требуется $O\left(N \cdot L_{e^g}\left\lfloor \frac{1}{2}, 3.54\sqrt{\log q} \right\rfloor\right)$ групповых операций, при $g \to \infty$, $N = \deg_y C(x, y)$ [28].	В

Продолжение таблицы 4

№	Условия применения	Сложность	T
		7. Алгоритм Theriault	
	$C(GF(q))$, q - произвольное	Алгоритм [38] является улучшенной версией алгоритма Gaudry для небольшого рода кривой. Основан на нахождении оптимальной доли простых дивизоров степени 1, что позволило ему получить временную сложность $O\left(g^5 q^{2-2/(g+1)+\varepsilon}\right)$, второй вариант этого алгоритма основан на отслеживании следа дивизора, который полностью раскладывается над базой разложения исключая один дополнительный «большой простой» дивизор. Слияние варианта два с первым алгоритмом Theriault получен алгоритм со сложностью $O\left(g^5 q^{2-4/(2g+1)+\varepsilon}\right)$. Оба эти алгоритма асимптотически быстрее алгоритма Gaudry, т.к. $q > (g-1)!$, случае первого алгоритма и $q > (g-1)!/g$ для второго, более того, эти алгоритмы асимптотически быстрее универсального алгоритма для $g \geq 3$, т.е. гиперэллиптические кривые не являются криптографически стойкими, как считалось ранее.	B

Наряду с общеизвестными методами криптоанализа DLP существует ряд дополнительных методов, позволяющих уменьшить пространство возможных решений, которые следует рассмотреть, для решения DLP. К их числу относятся атаки, основанные на анализе побочных факторов [64-69]:

- времени отклика вычислительной системы [5, 6, 19, 43];
- потребляемой мощности [5, 6, 44, 63, 70-72];
- интенсивности излучения [5, 6].

Рассмотрение и учет данных методов играет важную роль при проведении криптоанализа в реальных криптосистемах. Отметим, эти методы учтены в нашей классификации.

Таким образом, проведенная классификация, в отличие от известных, позволяет производить комплексный анализ стойкости современных криптопреобразований, а также обеспечить адекватный выбор общесистемных параметров.

3. Сравнение DLP, ECDLP, HECDLP

Проведем оценку стойкости криптопреобразований DLP, ECDLP, HECDLP. Данную оценку стойкости криптопреобразований следует проводить при фиксированной длине ключа относительно стойкости к криптоанализу алгоритма AES.

Стойкость криптопреобразований, напрямую связанны с порядком группы, которая образуется базовым элементом:

- для криптографических преобразований в поле $GF(q)$, $q = 2^m$, известным наилучшим алгоритмом криптоанализа DLP является алгоритм А. 5, сложность которого, составляет $O\left(\exp\left((1.4 + o(1))m^{1/3}(\log m)^{2/3}\right)\right)$ групповых операций;

- для криптографических преобразований в группе точек эллиптической кривой, как и для гиперэллиптических кривых, рода $g = 1$, порядок равен $\#\{E(F_q)\} = O(4N^{1/2})$. Причем точка $P \in E(GF(q))$ должна иметь порядок $\mathrm{ord}(P) \approx q - 2\sqrt{q}$ [31]. Наилучшим универсальным алгоритмом криптоанализа является алгоритм А. 4.5, сложность которого составляет $O\left((\ln^c h)\sqrt{\pi\, h/2}\right)$

групповых операций, где h - наибольший простой делитель $\mathrm{ord}(P)$, c - небольшая константа [38];

- для криптографических преобразований в якобиане гиперэллиптической кривой порядок произвольного абелевого многообразия A над $GF(q)$ рода g, лежит в интервале $\left(q^{1/2}-1\right)^{2g} \le \# A(GF(q)) \le \left(q^{1/2}+1\right)^{2g}$, количество изогенных классов якобиановых многообразий рода g, чей порядок равен $\#J(F_q) = O(q^g) = O(N)$, соответственно равен $\#\{J(GF(q))\} = O(4gN^{1-1/2g})$ [59]. Приведенный дивизор D якобиана гиперэллиптической кривой $J_C(GF(q))$ рода g, имеет простой порядок $\mathrm{ord}(D) \approx q^g$ [12-14]. Сложность самого эффективного алгоритма криптоанализа составляет $O\left(g^5 q^{2-4/(2g+1)+\varepsilon}\right)$.

На основе приведенных данных в таблице 5 представлены необходимые размеры полей (длины ключей) для фиксированного уровня стойкости.

Таблица 5

Проблема	m_1	m_2	m_3	m_4	m_5
AES	-	-	(80)	128	256
DLP, $GF(2^m)$, A3	256	512	1024	3072	15360
ECDLP, $E(GF(2^m))$, A4.5	71	109	147	235	453
HECDLP, $g=2$, $C(GF(2^m))$, A7.1	26	42	58	95	186
HECDLP, $g=3$, $C(GF(2^m))$, A7.1	20	33	46	77	153
HECDLP, $g=4$, $C(GF(2^m))$, A7.1	17	29	41	69	139

Как видно из представленной таблицы, ГЭК обеспечивает соизмеримую стойкость с AES и ЭК при гораздо меньшей длине ключа. Преобразования в поле, при той же стойкости, требуют наибольшей длины ключа.

4. Выводы

Полученные результаты подтвердили тенденции в распространении использования ЭК и ГЭК над расширенным и простым полями.

Предложенная классификация алгоритмов криптоанализа позволяет производить комплексный анализ стойкости криптопреобразований и обеспечить адекватный выбор общесистемных параметров. Особенностью данной классификации является возможность учета побочных факторов имеющих место в реальных криптосистемах. Учет данных факторов позволяет существенно повысить стойкость к методам криптоанализа в действующих и перспективных системах.

Исследования, проведенные на основе предложенной классификации, показали, что дальнейшее развитие ассиметричной криптографии лежит в увеличении сложности кривой (рода). Так, наибольшей стойкостью к методам криптоанализа при одинаковом размере ключа обладает HECDLP $g=4$. Далее в порядке уменьшения сложности следуют: HECDLP $g=3$, HECDLP $g=2$, ECDLP, DLP. Таким образом, уменьшение размера поля открывает «новые

горизонты» для применения ГЭК, одним из которых являются мобильные и встраиваемые устройства в силу их сравнительно невысокого размера блока преобразования.

Литература

1. *E. Teske*. Computing discrete logarithms with the parallelized kangaroo method. Research Report CORR 01-01, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2001. 18 pages.

2. *A. Stein, E. Teske*. The parallelized pollard kangaroo method in real quadratic function fields.

3. *E. Teske*. Square-root algorithms for the discrete logarithm problem (a survey). Research Report CORR 01-07, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2001. 17 pages.

4. *A. Enge.* Computing discrete logarithms in high-genius hyperelliptic jacobians in provably subexponential time. Research Report CORR 99-04, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 1999. 17 pages.

5. *B. Möller*. Securing elliptic curve point multiplication against side-channel attacks.

6. *K. Okeya, K. Sakurai.* Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. Progress in cryptology – INDOCRYPT 2000 (2000), B.K. Roy, E. Okamoto, Eds., LNCS 19977, pp.178-190.

7. *M. Maurer, A. Menezes, E. Teske*. Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree. Research Report CORR 01-59, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2001. 42 pages.

8. *I. Semaev.* A reduction of the space for the parallelized Pollard lambda search on elliptic curves over prime finite fields and on anomalous binary elliptic curves. August 11, 2003.

9. *M.J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein, E. Teske*. Analysis of the Xedni calculus attack. Designs, Codes and Cryptography, 20, pp. 168-188, 2000.

10. *P. Gaudry*. An algorithm for solving the discrete log problem on hyperelliptic curves.

11. *M. Chateaneuf, A. C. H. Ling, D.R. Stinson*. Slope packing and coverings, and generic algorithms for the discrete logarithm. Research Report CORR 01-60, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2001. 12 pages.

12. *J.H. Silverman*. The Xedni calculus and the elliptic curve discrete logarithm problem. Designs, Codes and Cryptology, 20 (2000), 5-40. 13. *L. Wagner*. Algebro-geometric attack methods in elliptic curve cryptography. Honours thesis. 18.11.2002.

14. *A. Menezes, M. Qu*. Analysis of the Weil descent attack of Gaudry, Hess and Smart. Research Report CORR 00-48, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2000. 10 pages. Revised April 22, 2001.

15. *R. Galant, R. Lambert, S. Vanstone*. Improving the parallelized Pollard lambda search on binary anomalous curves. Mathemetics of computation, 69: 1699-1 705, 2000.

16. *I. Duursma, P. Gaudry, F. Morain*. Speeding up the discrete log computation on curves with automorphisms. Advances in cryptology-ASIACRYPT'99, LNCS 1716, pp. 103-121, Springer-Verlag, 1999.

17. *I. Duursma, P. Gaudry, F. Morain*. Joint work. Speeding up the discrete log computation on curves with automorphisms.

18. *A. Enge, P. Gaudry.* A general framework for subexponential discrete logarithms. LIX research report LIX/RR/00/04. June 23, 2000.

19. *M. Katagi, I. Kitamura, T. Akishita, T. Takagi.* A timing attack on hyperelliptic cryptosystems. Available at: http://eprint.iacr.org.

20. *A. Menezes, S. Vanstone.* Reducing elliptic curve logarithms to logarithms in a finite field. IEEE transactions on information theory, 39 (1993), 1639-1696.

21. *A. Miyaji, M. Nakabayashi, S. Takano*. New explicit conditions of elliptic curve traces for FR-reduction.

22. *A. Miyaji, M. Nakabayashi, S. Takano*. Characterization on elliptic curve traces under FR-reduction.

23. *S.R. Blackburn, E. Teske*. Baby-step giant-step for non-uniform distribution. Arithmetic number theory. Seminar ANTS-IV, LNCS 1838, pp. 153-168, Springer-Verlag, 2000.

24. *D.R. Stinson*. Some baby-step gaint-step algorithms for the low hamming weight discrete logarithm problem. Research Report CORR 99-07, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 1999. 13 pages.

25. *V. Shoup*. Lower bounds for discrete logarithms and related problems. Advances in Cryptology – EUROCRYPT'97, LNCS 1233, pp.256-266, 1997.

26. *P. Gaudry, F. Hess, N. P. Smart*. Constructive and destructive facets of Weil descent on elliptic curves.

27. *J.H. Silverman, J. Suzuki*. Elliptic Curve discrete logarithms and the index calculus.

28. *S.D. Galbraith, N. P. Smart*. A cryptographic application of Weil descent. Cryptography and coding, 7th IMA Conference, Springer-Verlag, LNCS 1746, pp. 191-200, 1999. The full version of the paper is HP Labs Technical report, HPL-1999-70. 29. *M. Jacobson, A. Menezes, A. Stein*. Solving elliptic curve discrete logarithm problems using Weil descent.

31. *D. Johnson, A. Menezes, S.Vanstone*. The Elliptic curve digital signature algorithm. Certicom research. Canada.

32. *V.S. Miller*. Use of elliptic curves in cryptology. Advances in Cryptology – Crypto'85, LNCS 218, 1986, Springer-Verlag, 417-426.

33. ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.

34. ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Key Transport Protocols, working draft, October 2000.

35. IEEE 1363, Standard Specifications for Public-Key Cryptography, 2000.

36. *E. Thome*. Computation of Discrete Logarithms in $F_{2^{607}}$. Laboratorie d'Informatique (LIX) Ecole polytechnique, Essen, France, 2001.

37. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

38. *M. Jacobson Jr, A. Menezes, A. Stein*. Hyperelliptic curves and cryptography.

39. *J.J. Quisquater, J. P. Delescaille.* How easy is collision search? Application to DES. Advances in Cryptology – EUROCRYPT'89, 1989.

40 *A.Stain*. Equivalences between elliptic curves and real quadratic congruence function fields. Journal de theorie des Nombres de Bordeaux, 9 (1997), pp.75-95.

41. *R. Zuccherato.* Equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2. Algorithmic number theory-ANTS-III, LNCS 1423, 1998, 621-638.

42. *V. Muller, A. Stein, C. Thiel.* Computing discrete logarithms in real quadratic congruence function fields of large genius, Mathematics of computation, 68 (1999), 807-822.

43. *P.C. Korcher.* Timing attack on implementation of Diffie-Helman, RSA, DSS, and other systems. Advances in Cryptology – Crypto'96, 1996, N. Koblitz, Ed., LNCS 1109, pp. 104-113.

44. *P.C. Korcher, J. Jaffe, B. Jun*, Differential power analisis. In Advances in Cryptology – Crypto'99 (1999), M. Wiener, Ed., LNCS 1666, pp. 388-397.

45. *M. Wiener, R. Zuccherato*. Faster attacks on elliptic curve cryptosystems. In Processing of SAC – Workshop on Selected Areas in Cryptography, LNCS 1556, pages 190-200. Springer, 1998.

46. *R. Galant, R. Lambert, S. Vanstone*. Improving the parallelized Pollard lambda search on binary anomalous curves. Mathematics of Computation, 69:1699-1705, 2000.

47. *R. Silverman, J. Stapleton.* Contribution to ANSI X9F1 working group, 1997.

48. *J.M. Pollard*. Kangaroos, Monopoly and discrete logarithms. Journal of Cryptology, 13: 437-447, 2000.

49. *R.P. Brent.* Parallel algorithms for integer factorization. In J. H. Loxton, Ed., Number theory and cryptography, vol. 154 of London Mathematical Society Lecture Note Series, Pages 26-37. Cambridge University Press, 1990.

50. *J. Sattler, C. P. Schnorr*. Generating random walks in groups. Ann.-Univ.-Sci.-Budapest.-Sect.Cpmut., 6:65-79, 1985.

51. *D.C. Terr*. A modification of Shanks' baby-step gaint-step algorithm. Mathematics of Computation. 69:767-773.

52. *R.P. Brent.* An improved Monte Carlo factorization algorithm. BIT, 20:176-184, 1980.

53. *E. Teske.* Speeding up Pollard's rho method for computing discrete algorithms. In Algorithmis Number Theory Seminar ANTIS-III, LNCS 1423, pp. 541-554. Springer-Verlag, 1998.

54. *P.C. van Oorschot, M. J. Wiener*. Parallel collision search with cryptoanalytic applications. Journal of Cryptology, 12:1-28, 1999.

55. *E. Thome*, Computing discrete logs in large characteristic 2 finite fields. Laboratorie d'Informatique (LIX) Ecole polytechnique, Essen, France, 25 September 2002.

56. *J. Buchmann, M.J. Jacobson, Jr., E. Teske*. On some computational problems in finite abelian groups. Mathematics of computation, 66: 1663-1687, 1997.

57. *J. Horwitz, R. Venkatesan*. Random Cayley graphs and discrete log. Preprint, 2000.

58. *J. Lopez, R. Dahab*. An overview of elliptic curve cryptography. 2000.

59. *J. Chao, N. Matsuda, S. Tsujii*. Efficient construction of secure hyperelliptic discrete logarithm problems.

60. *A. Menezes, M. Qu.* Analysis of the Weil descent attack of Gaudry, Hess and Smart. 2001, LNCS 2020.

61. *A.J. Menezes, Y. Wu, R.J. Zuccherrato*. An elementary introduction to hyperelliptic curves. Technical report CORR96-19, Department of combinatorics and optimization, University of Waterloo, Waterloo, Ontario, 1996. In: Koblitz, N.: Algebraic aspects of cryptography, Springer-Verlag, Berlin Heidelberg New York. 1998.

62. *A. Stein, E. Teske*. Optimized baby step-gaint step methods and applications to hyperelliptic function fields. Research Report CORR 01-62, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2001. 25 pages.

63. *E. Brier, C. Claver, F. Oliver*. Optimal statistical power analysis.

64. *O. Billet, M. Joye*. The Jacobi model of an elliptic curve and side-channel analysis.

65. *A. Bellezza*. Countermeasure against side-channel attacks for elliptic curve cryptosystems. 2001.

66. *W. Fischer, C. Giraud, E. W. Knudsen, J.-P. Seifert*. Parallel scalar multiplication on general elliptic curves over F_q hedged against non-differential side-channel attacks.

67. *D. Page*. Theoretical use of cache memory as a cryptoanalytic side-channel.

68. *B. Chevallier-Mames, M. Ciet, M. Joye*. Low-cost solutions for preventing simple side-channel analysis: side –channel atomicity. 2003.

69. *E. Smith, C. Gebotys*. SCA countermeasures for ECC over binary fields on a VLIW DSP core. Research Report CORR 03-06, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2003.

70. *N. Ebeid, M. Award Hasan.* Analysis of DPA countermeasures based on randomizing the binary algorithm. Research Report CORR 03-14, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2003.

71. *N. Ebeid, A. Hassan*. On randomizing private keys to counteract DPA attacks. Research Report CORR 03-11, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2003.

72. *K. Okeya, K. Sakurai*. A simple power attack on a randomized addition-substraction chains method for elliptic curve cryptosystems. IECES Trans. Fundamentals, vol. E86-A, No. 5, may 2003.

73. *S.D. Galbraith, F. Hess, N.P. Smart*. Extending the GHS Weil descent attack. Available: http://erpint.iacr.org

74. *E. Teske*. An elliptic curve trapdoor system. Research Report CORR 03-07, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2003.

75. *A. Menezes, E. Teske, A. Weng*. Weak fields for ECC. Research Report CORR 03-15, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 2003.

76. *E. Teske*. Better random walks for Pollard's rho method. Research Report CORR 98-52, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, 1998.

Збитнев Станислав Иванович, кандидат технических наук.
Преподаватель кафедры безопасности информационных технологий Национального технического университета радиоэлектроники, пр. Ленина 14, г. Харьков, Украина, 61166.
Круг научных интересов: Защита информационных технологий, криптопреобразования на алгебраических кривых.
e-mail: staszb@ukr.net
Ковтун Владислав Юрьевич.
Адъюнкт кафедры компьютерных систем Харьковского университета Воздушных Сил, ул. Сумская 77/79, г. Харьков, Украина, 61023.
Круг научных интересов: Защита информационных технологий, криптопреобразования на алгебраических кривых.
e-mail: vladislav.kovtun@gmail.com
Шевченко Денис Викторович.
Аспирант кафедры безопасности информационных технологий Национального технического университета радиоэлектроники, пр. Ленина 14, г. Харьков, Украина, 61166.
Круг научных интересов: Защита информационных технологий, криптопреобразования на алгебраических кривых.
e-mail: shevch_den@mail.ru
Гиневский Александр Михайлович, кандидат технических наук.
Старший научный сотрудник научно-исследовательской лаборатории кафедры компьютерных систем Харьковского университета Воздушных Сил, ул. Сумская 77/79, г. Харьков, Украина, 61023.
Круг научных интересов: Защита информационных технологий, криптопреобразования на алгебраических кривых.