УДК 681.3.06: 519.248.681

М.Ф. БОНДАРЕНКО, д-р. техн. наук, И.Д. ГОРБЕНКО, д-р. техн. наук,
Е.Г. КАЧКО, канд. техн. наук, А.В. СВИНАРЕВ, канд. техн. наук, Т.А. ГРИНЕНКО

СУЩНОСТЬ И РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ СВОЙСТВ ПЕРСПЕКТИВНЫХ СТАНДАРТОВ ЦИФРОВОЙ ПОДПИСИ X9.62-1998 И РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ X9.63-199X НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Введение

В 80-е годы были разработаны, а в 90-е нашли широкое распространение криптографические системы, построенные на использовании методов несимметричной криптографии. Основными из них являются методы, базирующиеся на использовании RSA, Эль-Гамаля и Диффи-Хеллмана криптоалгоритмов [1-4]. Практическое применение их было закреплено в стандартах, основными из них являются X-509, ISO-11166, X9.30, X9.42, ГОСТ 34.10-94, ГОСТ 34.310-95 и др. Эти системы были отнесены к классу вероятно-стойких или доказуемо-стойких, что объясняется тем, что доказательство их стойкости сводилось к доказательству сложности решения определенных математических задач при соответствующих значениях (размерах) общесистемных параметров. Так доказательство стойкости RSA систем сводилось в основном к доказательству сложности решения задач факторизации модуля преобразования N. Доказательство стойкости алгоритмов Эль-Гамаля и Диффи-Хелмана сводилось к доказательству сложности решения дискретного логарифмического уравнения. При этом по мере расширения применения указанных стандартов активизировались усилия по их взлому. Появились совершенно новые разделы математики, позволяющие существенно уменьшить вычислительную сложность решения указанных задач. Например, создание средств решения таких задач на основе общего решета числового поля в сочетании с применением мощных компьютеров сделало возможным взлом систем с параметрами, используемыми на практике. Иначе средства криптоанализа, в смысле математики и производительности криптоаналитических систем, развивались быстрее, чем изменялись версии средств цифровой подписи, направленного шифрования и распределение ключей.

Основным методом защиты стали изменения параметров, в смысле их увеличения, например, модулей преобразования. Так, в Эль-Гамаля и Диффи-Хеллмана системах длина модуля преобразования составляет порядка 1024 и более битов. Но при этом до такой же длины были увеличены длины ключей, как следствие увеличилась вычислительная сложность криптографических преобразований и уменьшилась скорость. В то же время все преобразования необходимо осуществлять все с возрастающими скоростями, как правило, в реальном масштабе времени. Разрешение указанного противоречия было найдено за счет реализации различных несимметричных преобразований на эллиптичных кривых в полях Галуа [4-38]. По существу в 90-е годы криптографы и криптоаналитики разрабатывали и исследовали стойкость криптоалгоритмов на эллиптичных кривых. К настоящему времени уже разработаны, прошли сертификацию и утверждены ряд стандартов. Прежде всего стандарт цифровой подписи X9.62-1998 [3] и стандарт распределения ключей X9.63-1999[4], а также черновые версии ИИЭР P1363/79 стандартных спецификаций для шифрования с открытыми ключами. Основными преимуществами этих стандартов является возможность уменьшения в 5 и более раз длин ключей и общесистемных параметров, большая степень увеличения сложности криптоанализа с ростом размеров общесистемных параметров, а также уменьшение вычислительной мощности всех преобразований. Все это, на наш взгляд, и предопределило переход, а по существу перевод существующих алгоритмов на вычисления на эллиптических кривых над полями Галуа.

1. Математические основы преобразований на эллиптических кривых в полях Галуа

Наиболее общее определение эллиптической кривой дает уравнение Вейерштрасса. Для конечного поля Галуа GF(q), где q>3 и есть простым числом, уравнение Вейерштрасса имеет вид

$$y^2 = x^3 + ax + b(\mathrm{mod}\, q), \tag{1}$$

где a и b есть целые числа над полем GF(q), но такие, что справедливо выражение

$$4a^3 + 27b^2 \neq 0(\mathrm{mod}\, q). \tag{2}$$

Для расширенного поля GF(2^m), уравнение Вейерштрасса имеет вид

$$y^2 + xy = x^3 + ax^2 + b(\mathrm{mod}\, f(x), q), \tag{3}$$

где a и b являются элементами поля GF(2^m), т.е. полиномами степени m над полем GF(2). Все вычисления в (3) производятся по двойному модулю (f(x),2), где f(x) примитивный полином степени m. При чем в сравнении (3) $b \neq 0$.

Эллиптичная кривая E над конечным полем GF(q) определяется множеством точек на плоскости P=(x_p, y_p),где x_p и y_p являются элементами поля GF(q). Элементы поля a $\in$GF(q) и b $\in$ GF(q) называются коэффициентами эллиптической кривой E. Составляющие точки P называются x_p - координатой точки P и y - координатой точки P.

Основной характеристикой эллиптической кривой есть ее порядок #E. Под порядком эллиптической кривой понимается число различных точек на E, включая точку O, который обозначается как

$$n = \#\, E(GF(q)). \tag{4}$$

При этом под разными мы понимаем точки, которые отличаются хотя бы одной координатой.

На эллиптической кривой введены операции сложения и скалярного умножения.

Операции сложения обладают следующими свойствами.

1. Сложения с нулем P+0=0+P=P, для всех точек P є E(GF(q)).
2. Для каждой точки P=(x_1, y_1), P $\in$ E(GF(q)) существует точка Q=(x_1,-y_1), Q $\in$ E(GF(q)), такая что

P+Q=0.

Точка Q называется обратным элементом и обозначается как (-P).

3.Если P=(x_1,y_1) $\in$ E(GF(q)), то

(x_1,y_1)+ (x_1,-y_1)=0.

4.Операция сложения двух точек.

Если P=(x_1,y_1) $\in$ E(GF(q)) и Q=(x_2,y_2) $\in$ E(GF(q)) и P$\neq$ 0, то R=P+Q=(x_3,y_3).

При этом, если q есть простое число, то

$$x_3 = (\lambda^2 - x_1 - x_2)(\mathrm{mod}\, q) \tag{5}$$

$$y_3 = (\lambda(x_2 - x_3) - y_1)(\mathrm{mod}\, q), \tag{6}$$

где

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}(\mathrm{mod}\, q), если P \neq Q (x_1 \neq x_2) \\ \dfrac{3x^2 + a}{2y_2}(\mathrm{mod}\, q), если P = Q (x_1 = x_2) \end{cases} \tag{7}$$

Если q=2^mто вместо 3 имеет место 3^1,а вместо 4 имеет место 4^1.

3^1.(x, y)+(x, x+y)=0 для всех (x, y) $\in$ E(GF(2^m)).

4^1.Если P=(x_1,y_1) $\in$ E(GF(2^m)) и Q=(x_2,y_2) E(GF(2^m)),

то

(x_3,y_3)=(x_1,y_1)+(x_2,y_2),

где

$$x_3 = (\lambda^2 + \lambda + x_1 + x_2 + a)(\mathrm{mod}\, f(x),2) \quad (8)$$

$$y_3 = (\lambda(x_1 + x_3) + x_3 + y_2)(\mathrm{mod}\, f(x),2) \quad (9)$$

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}(\mathrm{mod}\, f(x),2) \quad (10)$$

5.Скалярное умножение определяется для каждой точки E(GF(q)). Если точка P ∈ E(GF(q)), а ∈ N (а целое положительное), то скалярное умножение

$$a \times P = \underbrace{P + P + P + \ldots + P}_{a\ раз},$$

где операция (+) есть операция сложения на эллиптической кривой, определенная в 4 и 4[1].

2. Основные стандарты, применение, характеристика и возможности

Уже предварительный анализ соотношений (5)-(10) показывает, что выполнение операций сложения и скалярного умножения на эллиптической кривой требует значительных вычислительных ресурсов. При этом, очевидно, наибольшей вычислительной сложности требуют вычисления согласно выражению (7) и (9), решение этих задач ввиду значительной сложности, особой важности и необходимости требует отдельного рассмотрения.

К 1998 году разработаны и уже приняты в качестве рабочих версий следующие криптографические стандарты, которые построены на базе математического аппарата эллиптических кривых над простыми и расширенными полями Галуа (двоичными). Это цифровая подпись на эллиптических кривых X9.62-1998 и схемы управления ключами на эллиптических кривых X9.63-199X . По существу стандарт X9.62-1998 есть усовершенствование уже применяемого стандарта ANSI X9.30 часть 1, т.е. цифровой подписи DSA. Стандарт X9.63-199X есть усовершенствование применяемого стандарта ANSI X9.42-1996 управления ключами по схеме Диффи-Хеллмана.

Алгоритм DSA на эллиптических кривых (ECDSA) является аналогом DSA. В таблицах 1-8 устанавливаются соответствия по параметрам DSA и ECDSA.

В таблице 1 приведена информация о DSA и ECDSA.

Таблица 1

Группа	поле F_p*	$E(F_q)$
Группа элементов	Множество целых {1,2,...,p-1}	Точки (x,y), которые удовлетворяют уравнению ЭК, плюс точка бесконечности 0.
Операция в группе	Умножение по модулю p	Сложение точек на ЭК
Группа	поле F_p*	$E(F_q)$
Обозначения	Элементы: g, h Умножение: $g \times h$ Степень: g^a	Элементы: P, Q Сложение: $P + Q$ Умножение точек (так называемое скалярное умножение): aP
Проблема дискретного логарифма	Дано $g \in F_p^*$ и $h = g^x \bmod p$, Найти целое x.	Дано $P \in E(F_q)$ и $Q = aP$, найти целое a.

В таблице 2 указывается соответствие параметров DSA и ECDSA

Таблица 2

Характеристика	DSA Обозначения	ECDSA Обозначения
Порядок	q	n
Порождающий элемент	g	G
Личный ключ	x	d
Открытый ключ	y	Q

В таблице 3 перечислены параметры DSA и ECDSA

Таблица 3

Параметры	Параметры DSA	Параметры ECDSA
1. Общесистемные параметры	1. p и q - простые, q *делит* p-1.	1. E – ЭК над полем Fq.
2. Порождающий элемент	2. g – элемент порядка q в поле F_p*.	2. G точка порядка n в E(Fq).
3. Используемая группа	3. Используемая группа: $\{g^0, g^1, g^2, ..., g^{q-1}\}$.	3. Используемая группа: $\{0, G, 2G, ..., (n-1)G\}$.

В таблице 4 приведен алгоритм генерации ключей в DSA и ECDSA

Таблица 4

Параметр	Генерация ключей в DSA	Генерация ключей в ECDSA
1.Личный ключ x.	1. Выбрать случайное x в интервале [1, q-1].	1. Выбрать случайное целое d в интервале [1, n-1].
2.Открытый ключ.	2. Вычислить $y = g^x \bmod p$.	2. Вычислить $Q = dG$.
3.Ключи	3. Личный ключ x. Открытый ключ y.	3. Личный ключ d. Открытый ключ Q.

В таблице 5 приведен алгоритм выработки подписи в DSA и ECDSA

Таблица 5

DSA	ECDSA
1. Выбрать случайное целое k в интервале [1, q-1].	1. Выбрать случайное d в интервале [1, n-1].
2. Вычислить $g^k \bmod p$.	2. Вычислить $kG = (x_1, y_1)$.
3. Вычислить $r = (g^k \bmod p) \bmod q$.	3. Вычислить $r = x_1 \bmod n$.
4. Вычислить $e = H(M)$.	4. Вычислить $e = H(M)$.
5. Вычислить $s = k^{-1}(e + xr) \bmod q$.	5. Вычислить $s = k^{-1}(e+dr) \bmod n$.
6. Подпись для M - (r, s).	6. Подпись для M - (r, s).

В таблице 6 приведен алгоритм проверки подписи для DSA и ECDSA

Таблица 6

Проверка подписи для DSA	Проверка подписи для ECDSA
1. Вычислить h = $H(M)$.	1. Вычислить h= $H(M)$.
2. Вычислить $s^{-1} \bmod q$.	2. Вычислить $s^{-1} \bmod n$.
3. Вычислить $u_1 = hs^{-1} \bmod q$.	3. Вычислить $u_1 = hs^{-1} \bmod n$.
4. Вычислить $u_2 = rs^{-1} \bmod q$.	4. Вычислить $u_2 = rs^{-1} \bmod n$.
5. Вычислить $v' = g^{u1} y^{u2} \bmod p$.	5. Вычислить $u_1G + u_2Q = (x_1, y_1)$.

Продолжение таблицы 6

Проверка подписи для DSA	Проверка подписи для ECDSA
6. Вычислить $v = v' \bmod q$.	6. Вычислить $v = x_1 \bmod n$.
7. Принять подпись, если $v = r$.	7. Принять подпись, если $v = r$.

В таблице 7 переведена характеристика параметров X9.63-199X.

Таблица 7

Группа	*поле* F_p	$E(F_q)$
Группа элементов	Множество целых {1,2,...,p-1}	Точки (x,y), которые удовлетворяют уравнению ЭК
Операция в группе	Умножение по модулю p	Сложение точек
Обозначения	Элементы: g_1, g_2 Умножение: $g_1 \times g_2$ Степень: g^k	Элементы: P_1, P_2 Сложение: P_1+P_2 Умножение точек (так называемое скалярное умножение): kP
Проблема дискретного логарифма	Дано $g_1 \in F_p^*$ и $h = g_1^{\,k} \bmod p$, Найти целое k.	Дано $P_1 \in E(F_q)$ и $P_2 = kP_1$, найти целое k.
Диффи-Хеллмана проблема	Известны g^{k1}, $g^{k2} \in F_p^*$. Найти g^{k1k2}	Дано $P_1 \in E(F_q)$ и $P_2 = kP_1$, найти целое k_1k_2P.

В таблице 2 указывается соответствие параметров DSA и ECDSA

Таблица 8

X9.42	q	P	g	x	y	z	t
X9.63	n	#E(F_g)	G	d_s	Q_s	d_e	Q_e

3. Оценка криптостойкости

Пусть E - эллиптическая кривая над конечным полем Галуа F(q). Пусть G $\in$ E(F(q)) будет кратной порядку n, где n - простое число и $n \geq 2^{160}$.

Задачу дискретного логарифма эллиптической кривой (ДЛЭК) сформулируем таким образом: для заданных (известных E, G и открытого ключа Q $\in$ E (F(q)) необходимо найти целое число l, $0 \leq l \leq n-1$ такое, что

$$Q = \Omega = lG$$

при условии существования такого числа l.

Известно несколько методов (алгоритмов) решения дискретного логарифма эллиптической кривой. Лучшими на сегодняшний день алгоритмами являются методы семейства Полларда, в частности ρ-метод и λ-метод Полларда.

Показано, что ρ метод требует выполнения порядка

$$I_\rho = \sqrt{\frac{\pi n}{2}}$$

шагов, то есть обладает сложностью такого порядка. Каждый шаг, его сложность, является операцией суммирования на эллиптической кривой. Метод Полларда может быть распараллелен. В этом случае каждый из m-процессоров может выполнять часть I ρ операций (шагов), при m-процессорах.

$$\sqrt{\frac{\pi n}{2}} \Big/ m$$

Показано, что сложность λ-метода Полларда I_λ оценивается соотношением

$$I_\lambda = 2\sqrt{n}.$$

Он также может быть распараллелен. При m параллельных процессорах каждый из них должен выполнить

$$2\sqrt{n}/m$$

операции суммирования точки на эллиптической кривой.

Приведенные соотношения справедливы только для решения задач, исключая суперсингулярные и другие кривые. Запрет суперсингулярных кривых связан с тем, что существует метод эффективного сведения задачи дискретного логарифма на эллиптической кривой к задаче дискретного логарифма в конечном поле.

В 1998 г. было показано, что расчетная сложность лучших методов, например ρ метода может быть уменьшена в $\sqrt{2}$ раз. Для этого улучшенного метода ожидаемая сложность может оцениваться как

$$I_{\rho'} = \sqrt{\frac{\pi n}{4}}.$$

При распараллеливании имеем сложность на один из m процессоров

$$\sqrt{\pi n/4}/m.$$

Это касается эллиптических кривых над простым полем. Для расширенного поля $GF(2^l)$ на кривой порядка

$$E(F(2^{ld}))$$

может быть ускоренный в $\sqrt{2d}$ раз.

Пример. Пусть двоичная аномальная кривая E имеет вид

$$y^2 + xy = x^3 + x^2 + 1.$$

Для нее порядок кривой

$$\#E\left(F\left(2^{163}\right)\right) = 2n,$$

где n-простое 162 разрядное число.

Задача дискретного логарифма в $E(F(2^{163}))$ может быть решена с 2^{77} операций суммирования на эллиптической кривой. Для случайной кривой рассматриваемого вида оценивается величиной 2^{81} операций.

Для защиты от всех известных на сегодня вторжений необходимо, чтобы:

1. Порядок #E(F(q)) был кратным большому простому числу $n > 2^{160}$;
2. Выполнялось условие MOV.
3. Выполнялось условие аномальности.

MOV условие гарантирует, что эллиптическая кривая не поддается атакам с уменьшенной сложностью. Оно (условие) рассмотрено в [3].

Условие аномальности заключается в том, чтобы $\#E(F(q)) \neq q$, то есть порядок поля не должен совпадать с порядком кривой E.

4. Практические результаты криптоаналитических атак на эллиптические кривые

Очевидно все атаки на эллиптические кривые можно разделить на три вида: программные, аппаратные и программно-аппаратные.

Программные вторжения. Пусть одна MIPS машина выполняет $l = 4 \cdot 10^4$ сложений точек эллиптической кривой в секунду. Это достаточно высокий показатель. Так ASIC схема аппаратной реализации (прикладная специализированная интегральная схема) выполняет $4 \cdot 10^4$ операций на эллиптической кривой в поле $F(2^{155})$. При работе на частоте 40 Мгц в поле $F(2^{155})$ она выполняет 40 000 операций добавления точек на эллиптической кривой.

При таких условиях число операций добавления на эллиптической кривой 1 MIPS машиной определяется как

$$L = l \cdot t_{року} = \left(4 \cdot 10^4\right) \cdot (60 \cdot 60 \cdot 24 \cdot 365) = 1{,}15 \cdot 2^{40}.$$

В таблице 9 приведены необходимые значения мощности, которая необходима для вычисления одного дискретного логарифма для различных значений n. При этом считалось, что мощность криптоаналитической системы составляет $S = 4 \cdot 10^4$ добавлений на эллиптической кривой.

Таблица 9

Размер поля q (в разрядах)	Размер n эллиптической кривой (разрядов)	Значение $\sqrt{\frac{\pi n}{4}} = I_{\rho^0}$	L (MIPS-лет)
131	128	$1{,}64 \cdot 10^{19}$	$1{,}3 \cdot 10^7$
163	160	$1{,}07 \cdot 10^{24}$	$8{,}5 \cdot 10^{11}$
197	192	$7{,}05 \cdot 10^{28}$	$5{,}6 \cdot 10^{16}$
229	224	$4{,}62 \cdot 10^{33}$	$3{,}7 \cdot 10^{21}$
261	256	$3{,}03 \cdot 10^{38}$	$2{,}4 \cdot 10^{26}$
325	320	$1{,}30 \cdot 10^{48}$	$1{,}0 \cdot 10^{36}$
518	512	$1{,}03 \cdot 10^{77}$	$8{,}2 \cdot 10^{64}$
1032	1024	$1{,}19 \cdot 10^{144}$	$9{,}5 \cdot 10^{141}$

Значения L в таблице приведены для случая выполнения $4 \cdot 10^4$ операций сложения на кривой.

В [3] приведены данные, которые при использовании криптоаналитической системы из 10000 компьютеров, причем каждый из них имел мощность 1000 MIPS, то для $n = 2^{160}$ дискретный логарифм может быть вычислен за 85 тысяч лет.

По оценкам Одлизко [3], если для криптоанализа использовать 0,1% мировой мощности компьютеров, то в 2004 году можно выполнить на них 10^8 MIPS, а в 2014 году - $\left(10^{10} - 10^{11}\right)$ MIPS.

Отметим, что приведенные данные справедливы для случая использования методов Полларда. Однако, по-видимому, появятся новые математические методы решения задачи нахождения дискретного логарифма. Так уже было при решении задач факторизации RSA модулей и решения дискретного логарифма над простым полем. Тогда после освоения ρ и $(\rho - 1)$ методов Полларда появились методы кривых Ленстра, решето числового поля и общее решето числового поля, которые стали намного эффективнее по сравнению с методами Полларда.

Ван Ушрот и Вайнер [3] исследовали аппаратные вторжения и возможности построения специализированной криптоаналитической системы для решения дискретного логарифма на эллиптической кривой. Они получили интересный результат. Для $n = 10^{36} = 2^{120}$ система из 325000 компьютеров, цена которой составляет не меньше 10 миллионов долларов, нашла бы дискретный логарифм примерно за 35 дней.

5. Аспекты, связанные с нахождением ключа

В нашей постановке личным ключом является целое число l, $0 \le l \le n-1$ такое, что

$$Q = lG(\mathrm{mod}\, q)$$

Рассмотренные выше вторжения обеспечивают при рассмотренных условиях нахождение личного ключа l. При этом принимается, что системные параметры числовые значения точки G и модуля n известные криптоаналитику.

Мы здесь рассмотрим особенности λ метода Полларда. Пусть известна эллиптическая кривая E и базовая точка G. Пусть также время нахождения l, то есть решением дискретного логарифмического уравнения является t. Можно показать, что в этом случае ожидаемое время решения второго дискретного логарифмического уравнения (при тех же E, n и G) рассчитывается как

$$\left(\sqrt{2}-1\right)t = 0{,}41t.$$

Дальше решение третьего примера требует

$$\left(\sqrt{3}-\sqrt{2}\right)t \approx 0{,}32t.$$

Решение четвертого уравнения требует

$$\left(\sqrt{4}-\sqrt{3}\right)t = 0{,}27t$$

времени. И так далее.

Таким образом, при фиксированных значениях E, n, G решение следующих дискретных логарифмических уравнений все легче и легче.

Считается, что в ближайшее время число n (порядок используемой кривой) должно быть не меньше 150 битового числа для обеспечения краткосрочной защиты и не меньше чем 180 битовое число для среднесрочной защиты.

Необходимо отметить, что при использовании симметричных криптоалгоритмов длина ключа должна быть не меньше 75 бит. Надежная стойкость же может быть обеспечена при длине ключа не меньше 90 бит. Сегодня считается, что в 21 столетии длина симметричного ключа должна быть не меньше 128 бит.

Показано, что полный поиск K-битового ключа для симметричного криптоалгоритма примерно равняется сложности поиска согласно методам Полларда личного ключа на эллиптической кривой, порядок n которой равен 2k. В таблице 10 приведена расчетная сложность криптоанализа методов Полларда.

Таблица 10

n	$\sqrt{n}$	I_ρ (команд)	I_λ (команд)	I_{ρ_0} (команд)	I'_ρ (mipsолет)	I'_λ (mipsолет)	I'_{ρ_0} (mipsолет)
2^{128}	$2{,}42\cdot10^{19}(2^{64})$	$3{,}03\cdot10^{19}$	$4{,}84\cdot10^{19}$	$2{,}15\cdot10^{19}$	$0{,}97\cdot10^{6}$	$1{,}55\cdot10^{6}$	$0{,}69\cdot10^{6}$
2^{160}	$1{,}09\cdot10^{24}(2^{80})$	$1{,}36\cdot10^{24}$	$2{,}18\cdot10^{24}$	$0{,}97\cdot10^{24}$	$0{,}44\cdot10^{11}$	$0{,}69\cdot10^{11}$	$0{,}31\cdot10^{11}$
2^{198}	$7{,}76\cdot10^{28}(2^{96})$	$9{,}70\cdot10^{28}$	$1{,}55\cdot10^{29}$	$6{,}9\cdot10^{28}$	$3{,}10\cdot10^{15}$	$0{,}47\cdot10^{15}$	$2{,}21\cdot10^{15}$
2^{224}	$5{,}13\cdot10^{33}(2^{112})$	$6{,}41\cdot10^{33}$	$1{,}03\cdot10^{34}$	$4{,}56\cdot10^{33}$	$2{,}05\cdot10^{20}$	$0{,}33\cdot10^{21}$	$1{,}46\cdot10^{20}$
2^{256}	$3{,}39\cdot10^{38}(2^{128})$	$4{,}23\cdot10^{38}$	$6{,}78\cdot10^{38}$	$3{,}02\cdot10^{38}$	$1{,}35\cdot10^{25}$	$2{,}17\cdot10^{25}$	$0{,}97\cdot10^{25}$
2^{288}	$2{,}19\cdot10^{43}(2^{144})$	$2{,}74\cdot10^{43}$	$4{,}38\cdot10^{43}$	$1{,}95\cdot10^{43}$	$0{,}88\cdot10^{30}$	$1{,}470\cdot10^{30}$	$0{,}62\cdot10^{30}$
2^{320}	$1{,}44\cdot10^{48}(2^{160})$	$1{,}80\cdot10^{48}$	$2{,}88\cdot10^{48}$	$1{,}28\cdot10^{48}$	$0{,}57\cdot10^{35}$	$0{,}74\cdot10^{35}$	$0{,}41\cdot10^{35}$
2^{352}	$9{,}33\cdot10^{52}(2^{176})$	$1{,}17\cdot10^{53}$	$1{,}87\cdot10^{53}$	$8{,}30\cdot10^{52}$	$0{,}37\cdot10^{40}$	$0{,}60\cdot10^{40}$	$2{,}66\cdot10^{40}$
2^{384}	$6{,}17\cdot10^{57}(2^{192})$	$7{,}71\cdot10^{57}$	$1{,}22\cdot10^{58}$	$5{,}49\cdot10^{57}$	$2{,}46\cdot10^{44}$	$0{,}39\cdot10^{45}$	$1{,}75\cdot10^{44}$
2^{416}	$4{,}07\cdot10^{62}(2^{208})$	$5{,}09\cdot10^{62}$	$8{,}14\cdot10^{62}$	$3{,}62\cdot10^{62}$	$1{,}63\cdot10^{49}$	$2{,}6\cdot10^{49}$	$1{,}16\cdot10^{49}$

Продолжение таблицы 10

n	$\sqrt{n}$	I_ρ (команд)	I_λ (команд)	I_{ρ_0} (команд)	I_ρ' (mipsолет)	I_λ' (mipsолет)	I_{ρ_0}' (mipsолет)
2^{448}	$2{,}63\cdot10^{67}(2^{224})$	$3{,}29\cdot10^{67}$	$5{,}26\cdot10^{67}$	$2{,}34\cdot10^{67}$	$1{,}05\cdot10^{54}$	$1{,}68\cdot10^{54}$	$7{,}49\cdot10^{53}$
2^{512}	$1{,}15\cdot10^{77}(2^{256})$	$1{,}43\cdot10^{77}$	$2{,}30\cdot10^{77}$	$1{,}02\cdot10^{77}$	$0{,}46\cdot10^{64}$	$0{,}74\cdot10^{64}$	$0{,}33\cdot10^{64}$
2^{768}	$3{,}80\cdot10^{115}(2^{384})$	$4{,}75\cdot10^{115}$	$7{,}6\cdot10^{115}$	$3{,}38\cdot10^{115}$	$1{,}21\cdot10^{102}$	$25{,}43\cdot10^{102}$	$1{,}08\cdot10^{102}$
2^{1024}	$1{,}29\cdot10^{154}(2^{512})$	$1{,}61\cdot10^{154}$	$2{,}58\cdot10^{154}$	$1{,}15\cdot10^{154}$	$0{,}52\cdot10^{141}$	$0{,}83\cdot10^{141}$	$0{,}39\cdot10^{141}$

Заключение

Следует предположить, что в ближайшие несколько десятилетий получат распространение криптографические алгоритмы и протоколы, в основу построения которых будет положена математика эллиптических кривых в полях Галуа. Основными направлениями деятельности и исследований в Украине в этом направлении являются освоение и анализ существующих стандартов, реализация их на программной, программно-аппаратной или аппаратной основе, а также разработка или доработка стандартов в интересах Украины. Первоочередной задачей, на наш взгляд, является перевод Гост 34.310-95 на эллиптические кривые. Вместе с тем, следует ожидать, что алгоритмы, базирующиеся на эллиптических кривых, пройдут тот же эволюционный путь развития, применения и разочарований, которые мы видели в отношении RSA, Ель-Гамаля, Диффи-Хеллмана и других криптоалгоритмов.

Список литературы: **1.** *ANSI X9.30-1995*, Part 1: Public key cryptography using irreversible algorithms for the financial services industry: The Digital Signature Algorithm (Revised). **2.** *ANSI X9.30-1993*, Part 2: Public key cryptography using irreversible algorithms for the financial services industry: The Secure Hash Algorithm 1 (SHA-1) (Revised). **3.** *ANSI X9.62-1998:* Certificate Management. **4.** *ANSI X9.63-199x*: Elliptic curve key agreement and transport protocols, draft. **5.** *ANSI NWI:* Prime number generation, draft. **6.** *G. AGNEW, T. BETH, R. MULLIN AND S. VANSTONE,* Arithmetic operations in GF(2^m), Journal of Cryptology, 6 (1993), 3-13. **7.** *G. AGNEW, R. MULLIN AND S. VANSTONE,* An implementation of elliptic curve cryptosystems over F_{2155}, IEEE Journal on Selected Areas in Communications, 11 (1993), 804-813. **8.** *G. AGNEW, R. MULLIN, I. ONYSZCHUK AND S. VANSTONE,* An implementation for a fast public-key cryptosystem, Journal of Cryptology, 3 (1991), 63-79. **9.** *M. BLAZE, W. DIFFIE, R. RIVEST, B. SCHNEIER, T. SHIMOMURA, E. THOMPSON, AND M. WIENER,* Minimal key lengths for symmetric ciphers to provide adequate commercial security, January 1996. **10.** *E. BRICKELL, D. GORDON, K. MCCURLEY AND D. WILSON,* Fast Exponentiation with precomputation, Advances in Cryptology - EUROCRYPT '92 Lecture Notes in Computer Science, 658 (1993), Springer-Verlag, 200-207. **11.** *T. ELGAMAL,* A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31 (1985), 469-472. **12.** *R. GALLANT, R. LAMBERT, AND S. VANSTONE,* Improving the parallelized Pollard lambda search on binary anomalous curves, to appear in Mathematics of Computation. **13.** *ITU-T* Recommendation X.680, Information Technology - Abstract Syntax Notation One (ASN.1): Specification of Basic Notation (equivalent to ISO/IEC 8824-1). **14.** *ITU-T* Recommendation X.681, Information Technology - Abstract Syntax Notation One (ASN.1): Information Object Specification (equivalent to ISO/IEC 8824-2). **15.** *TU-T* Recommendation X.682, Information Technology - Abstract Syntax Notation One (ASN.1): Constraint Specification (equivalent to ISO/IEC 8824-3). **16.** *ITU-T* Recommendation X.683, Information Technology – Abstract Syntax Notation One (ASN.1): Parametrization of ASN.1 Specifications (equivalent to ISO/IEC 8824-4). **17.** *ITU-T* Recommendation X.690, Information Technology - ASN.1 Encoding Rules. Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) (equivalent to ISO/IEC 8825-1). **18.** *ITU-T* Recommendation X.691, Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER)

(equivalent to ISO/IEC 8825-2). **19.** *D. JUNGNICKEL,* Finite Fields: Structure and Arithmetics, B.I.-Wissenschaftsverlag, Mannheim, 1993. **20.** *D. KNUTH,* The Art of Computer Programming, volume 2, 2nd edition, 1981. **21.** *N. KOBLITZ,* Elliptic curve cryptosystems, Mathematics of Computation, 48 (1987), 203-209. **22.** *R. LERCIER,* Finding good random elliptic curves for cryptosystems defined over F_{2^n}, Advances in Cryptography - EUROCRYPT '97, Lecture Notes in Computer Science, 1233 (1997), Springer-Verlag, 379-392. **23.** *R. LERCIER AND F. MORAIN,* Counting the number of points on elliptic curves over finite fields: strategies and performances, Advances in Cryptology - EUROCRYPT '95, Lecture Notes in Computer Science, 921 (1995), Springer-Verlag, 79-94. **24.** *R. LIDL AND H. NIEDERREITER,* Finite Fields, Cambridge University Press, 1987. **25.** *R.J. MCELIECE,* Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987. **26.** *A. MENEZES,* Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993. **27.** *A. MENEZES, T. OKAMOTO AND S. VANSTONE,* Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory, 39 (1993), 1639-1646. **28.** *V MILLER,* Uses of elliptic curves in cryptography, Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, 218 (1986), Springer-Verlag, 417-426. **29.** *NATIONAL* INSTITUTE OF STANDARDS AND TECHNOLOGY, Secure Hash Standard (SHS), FIPS Publication 180, May 1993. **30.** *NATIONAL* INSTITUTE OF STANDARDS AND TECHNOLOGY, Digital Signature Standard, FIPS Publication 186, 1993. **31.** *A. ODLYZKO,* The Future of Integer Factorization, Cryptobytes, volume 1, number 2, summer 1995, 5-12. **32.** *P. VAN OORSCHOT AND M. WIENER,* Parallel Collision Search With Application To Hash Functions And Discrete Logarithms, in Proceedings of the 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, November 2-4, 1994, 210-218. **33.** *J. POLLARD,* Monte Carlo methods for index computation mod p, Mathematics of Computation, 32 (1978), 918-924. **34.** *R. SCHOOF,* Elliptic curves over finite fields and the computation of square roots mod p, Mathematics of Computation, 44 (1985), 483-494. **35.** *T. SATOH AND K. ARAKI,* Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, preprint, 1997. **36.** *N. SMART,* The discrete logarithm problem on elliptic curves of trace one, to appear in Journal of Cryptology. **37.** *S. VAUDENAY,* Hidden collisions on DSS, Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, 1109 (1996), Springer-Verlag, 83-88. **38.** *M. WIENER AND R. ZUCCHERATO,* Fast attacks on elliptic curve cryptosystems, to appear in Fifth Annual Workshop on Selected Areas in Cryptography – SAC '98, Lecture Notes in Computer Science, Springer-Verlag.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 15.03.2000