УДК 681.3.06

КРИПТОСТОЙКИЕ КРИВЫЕ ЭДВАРДСА НАД ПРОСТЫМИ ПОЛЯМИ

А.В. БЕССАЛОВ, А.А. ДИХТЕНКО

Рассмотрена форма Эдвардса эллиптической кривой. Приведены явные формулы изоморфного преобразования канонической эллиптической кривой в кривую Эдвардса и обратно. Найдено 40 кривых в форме Эдвардса над простыми полями, приемлемых для криптографии, получены координаты генераторов криптосистем.

Ключевые слова: эллиптическая кривая, форма Эдвардса, простое поле, порядок кривой.

ВВЕДЕНИЕ

Среди различных форм представления эллиптических кривых особое место занимает кривая в форме Эдвардса, появившаяся в современной научной литературе сравнительно недавно [1, 2]. Обладая рядом замечательных свойств, кривые Эдвардса над конечными полями весьма перспективны в криптографии. Закон сложения для точек кривой Эдвардса обладает свойствами универсальности и полноты [2]. Более того, скалярное произведение для точек кривой Эдвардса вычисляется минимальным числом операций в поле по сравнению с другими известными представлениями эллиптических кривых [2, 4]. Несомненно, что кривые Эдвардса вызывают интерес при проектировании криптографических протоколов и будущих стандартов асимметричного шифрования.

Поиск кривых Эдвардса, приемлемых для криптографии, представляет собой нетривиальную задачу. Ключевым моментом в ней является расчет порядка кривой, заданной над конечным полем. В [6] для поиска кривых Эдвардса почти простого порядка предложен подход, в котором для найденных кривых над полями $\mathbf{F}_5$ и $\mathbf{F}_7$ с минимальным порядком 4 найдены кривые приемлемого порядка $4n$ в расширениях этих полей [6, 7]. В данной работе поставлена задача поиска кривых в форме Эдвардса с почти простым значением порядка над большими простыми полями. В первом разделе мы приводим общие сведения о кривых в форме Эдвардса над конечным полем. Второй раздел обозначает проблему определения порядка кривой в форме Эдвардса и кратко описывает возможные пути ее решения. В третьем разделе мы приводим 40 кривых Эдвардса над простыми полями $\mathbf{F}_p$ с модулями p длиной 192, 224, 256 и 384 бит [8]. Порядок $4n$ предложенных кривых содержит простой сомножитель n, сравнимый по величине с величиной соответствующего поля. Таким образом, найденные кривые удовлетворяют современным требованиям к порядку генератора криптосистемы и с успехом могут применяться на практике.

1. КРИВЫЕ В ФОРМЕ ЭДВАРДСА. ЗАКОН СЛОЖЕНИЯ ТОЧЕК КРИВОЙ

Пусть k – конечное поле ($char(k) \neq 2$). Кривая в форме Эдвардса над полем k задается уравнением в аффинных координатах [1–6]:

$$E: \quad x^2 + y^2 = 1 + dx^2y^2 . \qquad (1)$$

Далее будем рассматривать кривые Эдвардса с учетом ограничения на параметр кривой $d \neq A^2$ в поле k. Это гарантирует полноту закона сложения, заданного над точками кривой (1). Сумма двух точек с координатами (x_1, y_1), (x_2, y_2) определяется формулой

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right). \qquad (2)$$

Таким образом, если $d \neq A^2$ в поле k, то закон (2) корректен для произвольных точек (x_1, y_1), (x_2, y_2), включая совпадающие, обратные точки и точку $O = (0,1)$. Доказано [2], что знаменатели $1 + dx_1x_2y_1y_2 \neq 0$ и $1 - dx_1x_2y_1y_2 \neq 0$ при $\forall x_1, x_2, y_1, y_2 \in k$.

Легко видеть, что кривая (1) содержит как минимум четыре точки: нуль аддитивной группы точек O = (0, 1), точку 2-го порядка $D = (0, -1)$, точки 4-го порядка $\pm P = (\pm 1, 0)$. Отсюда следует, что любая кривая в форме Эдвардса имеет порядок, кратный четырем. В работе [2] доказано, что для любой кривой, записанной в форме (1), найдется изоморфная эллиптическая кривая в канонической форме над полем k. Однако, в известных стандартах шифрования на эллиптических кривых [8] не содержится кривых над простыми полями с кофактором 4 порядка. Это не позволяет преобразовать рекомендуемые современными стандартами кривые непосредственно в форму (1). В этой связи для криптографических приложений следует провести поиск кривых Эдвардса над простыми полями с приемлемым значением порядка $4n$.

2. ИЗОМОРФИЗМ МЕЖДУ КРИВОЙ В ФОРМЕ ЭДВАРДСА И КАНОНИЧЕСКОЙ КРИВОЙ. РАСЧЕТ ПОРЯДКА КРИВОЙ В ФОРМЕ ЭДВАРДСА

Для каждой кривой (1) в форме Эдвардса E найдется изоморфная ей кривая в форме Вейерштрасса W вида

$$W: \quad v^2 = u^3 + Au + B . \qquad (3)$$

Соответствующий изоморфизм между точками кривых E и W задается правилами [3]:

$$u=\frac{(5-d)+(1-5d)y}{12(1-y)},\ v=\frac{(1-d)+(1+y)}{4x(1-y)}, \quad (4)$$

при $x(y-1)\neq 0$.

Четыре точки пересечения с осями координат преобразуются следующим образом:

$$(x,y)=(0,1)\to(u,v)=O,$$

$$(x,y)=(0,-1)\to(u,v)=\left(\frac{1+d}{6},0\right) \text{ при } x=0. \quad (5)$$

$$(x,y)=(\pm 1,0)\to(u,v)=\left(\frac{5-d}{12},\pm\frac{1-d}{4}\right) \text{ при } y=\pm 1.$$

Коэффициенты кривой W выражаются через параметр кривой E следующим образом [3]:

$$A=-\frac{(1+14d+d^2)}{48},$$

$$B=-\frac{(1-33d-33d^2+d^3)}{864}. \quad (6)$$

Для обратного преобразования справедливо:

$$x=\frac{6u-(1+d)}{6v},\ y=\frac{12u+d-5}{12u+1-5d},$$

$$\text{при } 6v(12u+1-5d)\neq 0,$$

$$(u,v)=\left(\frac{1+d}{6},0\right)\to(x,y)=(0,-1), \text{ при } v=0, \quad (7)$$

$$(u,v)=O\to(x,y)=(0,1).$$

Одним из способов расчета порядка кривой Эдвардса является адаптация соответствующих методов нахождения порядка канонических эллиптических кривых (таких как алгоритмы Скуфа, SEA, Satoh). Используя соотношения (4)–(7), для кривых в форме Эдвардса, определяется последовательность полиномов деления [3], посредством которых может быть вычислен порядок рассматриваемой кривой Эдвардса. С другой стороны, подсчитать порядок кривой Эдвардса можно посредством изоморфного перехода к канонической форме с последующим нахождением порядка кривой по известным алгоритмам.

Второй сценарий был использован для поиска кривых над простыми полями, приведенных в разделе 3. Выбрав произвольно параметр $d\neq A^2$ в поле k и, используя формулы (6), получим изоморфную эллиптическую кривую в форме Вейерштрасса. Заметим, что при заданном ограничении на параметр d кривой, дискриминант изоморфной эллиптической кривой будет отрицательным и в кубик правой части уравнения (3) будет иметь единственный корень. Подсчитать порядок эллиптической кривой можно, например, по алгоритму SEA. Порядок N_E рассматриваемой кривой считаем приемлемым, если число $n=N_E/4$ простое, лежащее приблизительно в пределах 180–600 бит. Такая кривая может быть рекомендована к применению в криптопротоколах.

Для построения криптографической системы на полученной кривой Эдвардса необходимо определить генерирующую точку порядка n. Задавая произвольно координату x и вычисляя из уравнения кривой (1) значение y, получим произвольную точку Q кривой Эдвардса. Если $x\neq 0$ и $x\neq\pm 1$ (вероятность этого события ничтожно мала), порядок точки Q может быть равен $n=N_E/4$, $2n$ или $4n$. Тогда генератором криптосистемы будет точка Q, $2Q$ или $4Q$ соответственно.

3. КРИВЫЕ ЭДВАРДСА ПОЧТИ ПРОСТОГО ПОРЯДКА НАД ПРОСТЫМИ ПОЛЯМИ

В данном разделе мы рассматриваем простые поля с модулями

$$p_{192}=2^{192}-2^{64}-1,$$

$$p_{224}=2^{224}-2^{96}+1,$$

$$p_{256}=2^{256}-2^{224}+2^{192}+2^{96}-1,$$

$$p_{384}=2^{384}-2^{128}-2^{96}+2^{32}-1,$$

рекомендуемые стандартом FIPS – 186 – 2 – 2000 [8], и приводим перечень кривых в форме Эдвардса почти простого порядка $N_E=4n$ (n – простое) над каждым из полей. Данные изложены в таблицах 1–4. Наряду с этим, в таблицах также содержатся общесистемные параметры для реализации шифрования с помощью кривой Эдвардса, а именно, порядок $n=N_E/4$ и координаты (x_G,y_G) генератора криптосистемы для каждой кривой.

В каждой из приведенных ниже таблиц содержится по 10 кривых Эдвардса над соответствующим полем с параметрами d различной битовой длины. Порядок кривых сравним по длине с длиной рассматриваемого поля. Расчеты производились посредством прикладных программ, основанных на использовании функций библиотеки MIRACL.

ЗАКЛЮЧЕНИЕ

На сегодняшний день открытой остается задача адаптации алгоритмов вычисления порядка кривой для кривых в форме Эдвардса. Однако приемлемые кривые Эдвардса над простыми полями можно получить посредством трансформации кривой Эдвардса в изоморфную кривую в форме Вейерштрасса с последующим определением порядка кривой в форме Вейерштрасса.

Таким способом в данной работе получено 40 кривых Эдвардса над простыми полями с модулями p_{192}, p_{224}, p_{256}, p_{384}. Порядок кривых, приведенных в разделе 3, имеет минимально возможный кофактор, равный 4, и простой кофактор, сравнимый по длине с длиной соответствующего поля. Это делает возможным применение полученных кривых в практических приложениях. Благодаря выигрышу в быстродействии (в среднем в 1.5 раза [4]) и удобству программирования

Таблица 1

Кривые Эдвардса почти простого порядка над полем с модулем p_{192}

$p=$	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF
$d=$	28453E
$n=$	40000000000000000000000001AEAD1229D137F564D7FF6D5
$x_G=$	AE709D07B2D112CECD4A7AE103757F2C101D054ACB1A0F17
$y_G=$	8BDF8D5A994AAB1E1455889D28E29CA3EC68548D3F7CA32F
$d=$	6DBA6A
$n=$	3FFFFFFFFFFFFFFFFFFFFFFFEA75D4027230DD4DFFDB0455
$x_G=$	44F083BB00E51AD91A2743284D31F57EE5C84826FCC91F4B
$y_G=$	15FC16E5870524E0DBBE9EC8BB9F066C02A02B1978D4E029
$d=$	CE37DC
$n=$	400000000000000000000000002618428A483A133570834389
$x_G=$	508AEB91AB9A230C377BD82BDDBE5B75CD38CDF1DA407A3C
$y_G=$	6E12D78C595D0ECC1614BFD04616CE45D6BB7D8607BB2ED7
$d=$	111DB4A
$n=$	400000000000000000000000004F2EA0DD45656E7E6066E8C9
$x_G=$	1603A0943674DA7D8476608E764BA7A63DBEBE4D8E549165
$y_G=$	148D5DA4654152C9196699074374EE091FE789A0CC7EC60
$d=$	12CCB98
$n=$	400000000000000000000000006AF187D9A93890273705F7E9
$x_G=$	6AC4FE0FEF645CA5754BFB0BD05967A418FCCAAF20E473A9
$y_G=$	B2F122E8816B142765B0FABCD7834CDC2D1AAC7EA779750B
$d=$	BFFAB4397C01049E12A46027E7E14D7A666240E6831D926
$n=$	400000000000000000000000022F2FB1AD838D6680571D7BB
$x_G=$	B46D3402D2A7F4CE30C5AA7839B0CE8D957240684824C726
$y_G=$	F0B24C20880DE704123ADF2A44189480DDFFDEEAF002B238
$d=$	CAE5B27FA36F62C6EC5EEC6ABE086C2BFF6A9F029CE42C88
$n=$	3FFFFFFFFFFFFFFFFFFFFFFFBD410EA5F77DD3ECCBD0FC45
$x_G=$	72F6A4BADEB19F876258926630ECA22F1D9FEF34CE53440C
$y_G=$	852D88019C7A20987BEE784A9EC09FF213639E59A3C3A51E
$d=$	2FDE6BF890C01A5FEB8B8D976676DDAC8C3349FE0C89959A
$n=$	3FFFFFFFFFFFFFFFFFFFFFFFC9B03E26E57C1A34245E23ED
$x_G=$	F2FA1F9E30FDF9C5CD1E84D287CE5F2DE9283B077C2C83FA
$y_G=$	419A50AF660CBF77699FBECBF7181F7F15C0DCF31523171F
$d=$	83E48CF4C49FDDEF6E5D812D3FBD06054835C85D6DD283BC
$n=$	400000000000000000000000002640829409C3B60282409D8B
$x_G=$	5BCFE7F1248E5A43CDF179D95334FE45061F0ECB599020B2
$y_G=$	FDEB479483DB5D1743AE7496B9A32B5CF774B8D8CD13272F
$d=$	CFC522DAB7BE9E92FA78DDA10CE941CC7108A299FB4A79C9
$n=$	400000000000000000000000006B362B3138DB79B9866A5BD7
$x_G=$	BE321DFF94A4E7DA940394E9C9EC1F2BC4B29F93302BDA3B
$y_G=$	B5E1CE7F685CEFE82284E5027404FE6E8D3C11E7D37092F3

Таблица 2

Кривые Эдвардса почти простого порядка над полем с модулем p_{224}.

$p =$	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF000000000000000000000001
$d =$	3608425
$n =$	400000000000000000000000020BBEC47CEDB34DD05BCB6B7E619
$x_G =$	C448CA02660F57204FF1BDE2B5CC3E25606A7460399FEA3DA9A06383
$y_G =$	319117770D6FC7FE35F6A02905FE1F363156BD2E5B75BB89A64CAFAB
$d =$	42E5CF5
$n =$	400000000000000000000000070D1AD037FD1F2585B37C3CD8E75
$x_G =$	74E8DA9676A0AA64C73460EFBA56F04A5D69FB39DC03A0D53B9E99A9
$y_G =$	A70D758DE2B7CADCEED9D6315F44987AF89B9D1D3BB62B54574971D5
$d =$	148CD57
$n =$	400000000000000000000000001BE5276AAC300270278233024CF9
$x_G =$	EEA0CBD1BFB937E1C83C12E90200429DD3F74854256DA5E249B04A2B
$y_G =$	512F075B98B7281E07BDABF68CE2BF4A30200DB1A9029ABDAAAEDEEA
$d =$	2C4C61C
$n =$	400000000000000000000000000054547A5F0105F649731ECC684CF
$x_G =$	142954F6B9702D136634AD2F6574ED5CF24E2D7D8AEB0B855105451A
$y_G =$	6EB430B9BE6B0A78D41BCBCFC3A207D0A813C8AB052BFD23529D23E9
$d =$	2DD96A9
$n =$	400000000000000000000000000024E3FE6372F8DB77945FFF06024D
$x_G =$	C62E8C8EB908FFC6DAE6D79D335618D62855B9A14F49DF1DEE0A414E
$y_G =$	6955A4D991CFE25E6EE21B64FC61763C16634CA234222A0E752F4E85
$d =$	1968A1D7A81AF44243D0F60F186A519FB95BF7C2FE2C037798D70FE9
$n =$	400000000000000000000000000003FCA1753F6F54C2A869DC8C5DBD9
$x_G =$	6F39E721F18128534C6C0339A982011683D9676565CAFD942F8C7761
$y_G =$	2E5ECC135081FE6FF9E0F7020BBC7EFD9DFB18A47B81DB825FC26817
$d =$	60B4BE2A9399C390AA051FC8B4706856E1CE2A03791C1B5A2C88DD40
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFF5722B78ED1CA9B003572246F325
$x_G =$	60D6B139288C1B171E8FE28EC068130CABDA0A1A48C1DF7280A14211
$y_G =$	198E5F9E549D6C080CCCA7886E6BC880623B5AB1070CB62A81377BC0
$d =$	E3850F8A3D93759F172493E9339B29DB7D345BE57CFCDCE545EEB1DC
$n =$	400000000000000000000000000005B3B3E37B9EDE0A1B45BEC627F5B
$x_G =$	DB921A45CBF9979A3425F0556165DEF73ED6792034A9D9A5DC180FC9
$y_G =$	A3A87DA7A0307AD196B2CEC840C3E17147C570EBE9CC432DBF941CD7
$d =$	6E6607C2DCE3392468455ED0DBFBA5442AD87C7B8CE484C1B85D592
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFE623254CA68DF10B09B50D57327B
$x_G =$	96C7C00D85C8BB5B53F74E6EF38EFEEB458FE9434290046114E0E906
$y_G =$	A2410947B7C669193EC0B39001FC786B0558C3DBB6B64BC9677A7016
$d =$	2BFE721565BE78DE5DABD588BCE5E62C7127A0BEC33A2FF844E0B79D
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFCCA2B4C227A60815F6A6359225E9
$x_G =$	DA2B86A81DBF8B887D3A3552A26CF3679DC73C300998BD82EEC1F49C
$y_G =$	D817BCDA64B37A31B2A15975F472A18F8D226446D1473CB3FB38D7C

Таблица 3

Кривые Эдвардса почти простого порядка над полем с модулем p_{256}.

$p =$	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
$d =$	72A38
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFBA76FA29C30CC3AA4954B53EDBE54D75
$x_G =$	894F8283626AEE6848515DDDC3B8DBB3D5302DEE0EE75080D6753E4D39BA5AB2
$y_G =$	EA612346223F6480CBBAFA39DB95D54D21469DD3074A957EFDA4FD79FEB630B5
$d =$	2EBFA9
$n =$	3FFFFFFFC0000000400000000000000005EFF905BA96F95CE79513CBE0CC53D1F
$x_G =$	363D655BF3F221256F032FC791B06149C14ACFFD92B59C84D1D3B817A9E622D2
$y_G =$	A52438C53DDCA661685B1F235EF0F1D280A493C33153AD691097AEC67A62C564
$d =$	805294
$n =$	3FFFFFFFC000000040000000000000051814C8E8360B7C96A8419F38B8039F1
$x_G =$	EEBABE42482F67FECF7F9D2D49A4430372D7678CF7EDAB4B9184D42BD93F390C
$y_G =$	E2A059E8C776F46028BA9265E20C09A785ECEEFB162562DA2AF78BC412D2D3CC
$d =$	9855C9
$n =$	3FFFFFFFC000000040000000000000002C1564946E895DAE0EB7EB501C62C62F
$x_G =$	D139CE35F84CFA17E8ED28E083F07C708303AE788477118C5AFE86D313D443BD
$y_G =$	F5F4A5309EEA75820AEE714A8D99CD22CE2539E73D2C6688B8480E18F1D384D
$d =$	BE957B
$n =$	3FFFFFFFC000000040000000000000005DACD9D621DE8444CB5625A8193E1D81
$x_G =$	B1550150B88C76AEC1CD0B0EC2008D1D73D086A0FD63103A0875EF574F0FF113
$y_G =$	306021DA97347B1DA05C98CE858B5C69ED901187DB03F68C399B694003FACA96
$d =$	4A5084ABF5DFFAC393E29A8BF045F4AA94C80F55414AFDAB8517CE769130DC82
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFF9B91248CDD0CAF813BD0F8B9F32C892B
$x_G =$	96540A02F26ED385B606A7956E5BA33B8D5A9E47FCE718C752562E2F2A6891E2
$y_G =$	ACDE96C64793B77B72DC71EB12508AAC629C4CCAA281BF164B73030EF382D9DE
$d =$	340B9C82867CD106FA7E1B11E9415A1099BB48C9A28F3B21A77E70C20E528839
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFFBE08C2E4E3DDB90FBAB306B69633071
$x_G =$	490659C09655C82EECDC109AC5F29E85DC94882E30916E9F21273AFE9D1B01AC
$y_G =$	9BB0A4609F48A8029AD9014BE7184E36A120B5789799DE52F4E7D8D90386F786
$d =$	32BBA52848792541A79779B4CFFF035903D2112814334C1BE3556A670A9D73D1
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFFC0285F94E407693E8624559A0D329309
$x_G =$	9D39DB8088196DE49C37D787D64EEB9ECA6A762BE77D0FCBD0430DCCBB057C2E
$y_G =$	62ABD075DA7C26034514079E7B5000D4493BC4318C5A3E3856FAAB8724C5C0F5
$d =$	8884FA14412BC9B62B0C467262DA6BD8F529C01AAD09545B2A294D479B254B2F
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFC7D37AFE15BFD6994B8E6427BA368D27
$x_G =$	D5D245310DD89B88DFF59C2CAEC8DBE62000E53D0BB4051247B97DDF420158C
$y_G =$	444B435A604729B76A17E8F4B93A47DC62D7777C1B056DB727675D627CF749F1
$d =$	E49478138FFE7946F81C3AC55BBBE4D41B4DF660A3B118B0075676506425D9FA
$n =$	3FFFFFFFC000000040000000000000000300FC8D622E987518514DFF16654AAFB
$x_G =$	92967B57C8CAB56FBDE3C3B0568C336BE2FBBB875F3983281D38B173C80971B9
$y_G =$	F3270D7C8A827B913A0B10079555D7D2E3A1C64578A49A77A9C1E6B45C186E90

Таблица 4

Кривые Эдвардса почти простого порядка над полем с модулем p_{384}

$p =$	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFF0000000000000000FFFFFFFF
$d =$	12593A
$n =$	40000000000000000000000000000000000000000000000005063576B5A9A0C3A23E9510EA680650B4884E63A2968DD71
$x_G =$	1FC0E8E61F599813E376D11F7510D77F177C2F1CDE19FD14D63A2EC5EAD4D0DED1BD06676CCF365243BF3C0675A31B62
$y_G =$	F52B4FA352B257D7A102FA45C56A50CCBDB3DEC053D5610EDBD0188C11F321F28A43E2FC50395E4A8BD0029AE71D51AA
$d =$	46959A
$n =$	40000000000000000000000000000000000000000000000000C06E6B5CE557E3DDEC6844B3470B819A9E1C0ED5F348517
$x_G =$	4567EA938DECB2BC17F9ABDEDBD77AD188FEFD6E244FD8A12C95A365F9C241E13888506D9D1FB4F8F9B8AA49098C3DF0
$y_G =$	121D587D9CEDEB34DD331E150D9FB2A23B314A354411C4F4A5AFF18685F6EDA1D557EC99F830785420A4DAD15897814E
$d =$	5FD247
$n =$	4000000000000000000000000000000000000000000000000A6A021C752BB157244080A30D578824A05A3BFFF4E67575
$x_G =$	8947F1251392317F3C0E127F7D337B1EE67A120BC69B5E1D91B6C7DC004904C1D42013DE9F12176B6EB34AD5CAC2D485
$y_G =$	B934A355EC5F900123E5EFFDB74502E084A94E59BFDF80E2B0979D02F971F0FE93A4ECE5FFC82C34724A2063836DA847
$d =$	7B35A8
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF96861B6F4CC029EE5B29F5BE0649FA4B3A605D3EC2CFD8F
$x_G =$	712160E70ED57AEC69A66E55A3A285DBFA712F9ACF9B334AC881E5066E55A415BE5935881C7DF7AF90EF6558C380037
$y_G =$	F1FF700AB04A2CA0F40FD94F1E32F61A3D4638570A28EB07AD1D281DAAC0293B946205098F71AC9BEBC8616F1B1DD3E8
$d =$	9302CE
$n =$	400000000000000000000000000000000000000000000000422338834D697FC3149FC70C79239975452EA01F75E2B699
$x_G =$	E9FDD336AC467447D6DB0627563C181663797C6D87F8E66A3E61BE69E53F66CCC4847DF28A19235D9377F4A33FEE0F69
$y_G =$	CF9AC7F9EEB6528DF53C80BF02E3A83D07614F2708148B4F7F1907398DE79019256D32E535219D71F173DEAE9621716B
$d =$	4CCEDF781B3680122FCFC696374F2ACA57E8F7514293BDD81F5040F0858023ECD295E6835FC14021B1AFFAF8065139C9
$n =$	400000000000000000000000000000000000000000000000046824B5EE5BADD70EB246617456AD087BADECDA7CD2A6E81
$x_G =$	36AFEDFF2308CF4C2F2052B0BF3068F0B4EE9759729A40491EF5D5E75F23E74A6F8528D276E6C528F487DE35E71454CB
$y_G =$	94D6B53F630A6D41E4DD65CD195839CC24DE7B6A71C3DC0A814E379445C67C6604B8034F7C5580AC0FBE771FBA1E9E36
$d =$	3462B5F8DD2744C13ED8618BAFC853F60F83134B936F3DD2867562D1CEEA866E590D702CE8C11262193F077A798918DE
$n =$	400000000000000000000000000000000000000000000000339419162A90FA9A9CA9C0C12B231CF5D95CC5E241D18C0F
$x_G =$	387CCD92DDCF7203D579EC6D158AD3A4DBAB83BBA4E153FB130F380425FD9F73AABEE0F2BE3BCA53D9E1D798DB016F3C
$y_G =$	50E827613BC65DEC52FD123387279D4E9E27102CE6B9119DC656632ED043D3961C72EB7C67D690D970CC65DD2F7C5702
$d =$	941F6CCE649868BD59F335D3293FBB201E3C811ADE19779EEFD8FB21AC1A466377365A8763793A3B3BB2B6575D9893D1
$n =$	400000000000000000000000000000000000000000000000002E0E36DDDDC5D4EA80D339D03926CA39AE3A4739EF81A1C9
$x_G =$	647D270CE4CB1F9038EEE75ED9570A3360AC68DE443BE52D23A734966F813D690615BE4284BDD78CF89B4ED2D02BE08A
$y_G =$	32247232CFA0A712AE3B029B1DDF8C5FE86A78E5728CB4D4386026C21A92297C271C81294C7B9DC18E245F6D87706865
$d =$	584D94FEA391957947760106F180D57CFE8E85109656E4B0BF6FCBF69D62F9A649AEF53CDA9B9F3B2BB247DEB6AB0C70
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8C7F4A394F5C92E8C6FB2FD97B1657DF603DB9677EEE6DD9
$x_G =$	4CAFBA0D62C538B7CC74F8274978AF35C43E2360BA6606FD379086367898EFD57040629FD9AC9721D65BCB511603BA00
$y_G =$	E2C024B79576CC47776562F9203B166E1C8300AD5C7F4D0B04FE0DBAF92FEC3DD0E5CE1F93288308D2C5CFF5B24DEC9A
$d =$	A01FD8E4FCE20AF1A99E214FDFB6AB3CAB8FEBF45F18DA66000E104265E11B82D8499835148459978BB-8003DB7E1F5B6
$n =$	4000000000000000000000000000000000000000000000000025DABC64D5F4783A6399E3A6701B920E95AA760041BFFAD
$x_G =$	144C701104F4122AC3D09B9B212CD428F8B61993E202C74A02CC95EFAAE257E1FF7DCA3592A60A37E76BA94D-50213C7C
$y_G =$	1BF38FDE630B35DA3EEA40138E94574CF9BD4AF60779D792360252752EBAAAD36D1C31DD-9294586633178062BAA5AF0F

криптосистем кривые Эдвардса могут стать эффективной альтернативой каноническим эллиптическим кривым.

Литература

[1] Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.

[2] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[3] Moloney R., McGuire G. Two kinds of division polynomials for twisted Edwards curves. Applicable Algebrain Engineering, Communication and Computing, 2011. – PP. 321–345.

[4] Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, №4, 2011. – С. 33–36.

[5] Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника, вып. 167, 2011. – С. 203–208.

[6] Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей // Прикладная радиоэлектроника, том 11, №2, 2012. –С. 225–227.

[7] Бессалов А.В., Дихтенко А.А., Яценко А.И. Параметры криптосистемы на кривой Эдвардса над расширениями малых простых полей // Прикладная радиоэлектроника, том 12, № 2, 2013. – С. 93–97.

[8] Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224 с.

Поступила в редколлегию 25.04.2013

Бессалов Анатолий Владимирович, фото и сведения об авторе см. на стр. 277.

Дихтенко Алиса Анатольевна, фото и сведения об авторе см. на стр. 277.

УДК 681.3.06

Криптостійкі криві Едвардса над простими полями / Бессалов А.В. // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 285–291.

Розглянуто форму Едвардса еліптичної кривої. Наведено формули явного ізоморфного перетворення канонічної еліптичної кривої у криву Едвардса і навпаки. Знайдено 40 кривих у формі Едвардса, які прийнятні для криптографії, отримано координати генераторів криптосистем.

Ключові слова: еліптична крива, форма Едвардса, просте поле, порядок кривої.

Бібліогр.: 8 найм.

UDC 681.3.06

Cryptographically resistant Edwards curves over prime fields / Bessalov A.V., Dihtenko A.A. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 285–291.

The Edwards form of an elliptic curve is considered. Explicit formulas of isomorphic transformation of a canonical elliptic curve into Edwards's curve and inverse are given. 40 curves in the Edwards form over prime fields suitable to cryptography are discovered, coordinates of cryptosystem generators are obtained.

Keywords: elliptic curve, Edwards form, prime field, curve order.

Ref.: 8 items.