УДК 681.3.06

ПАРАМЕТРИ КРИПТОСИСТЕМИ НА КРИВІЙ ЕДВАРДСА НАД РОЗШИРЕННЯМИ МАЛИХ ПРОСТИХ ПОЛІВ

А.В. БЕССАЛОВ, А.А. ДІХТЕНКО, О.І. ЯЦЕНКО

Розглянуто можливість удосконалення криптографічних систем на еліптичних кривих на базі кривих у формі Едвардса. Описаний підхід для обчислення загальносистемних параметрів криптосистеми на кривій Едвардса над розширеннями полів F_5 та F_7. Отримано 28 наборів параметрів, що відповідають стандартним криптографічним вимогам та можуть бути рекомендовані у майбутніх стандартах.

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

ВСТУП

Криптосистеми на еліптичних кривих є основою більшості сучасних стандартів та протоколів шифрування. Паралельно із дослідженнями щодо можливих атак на еліптичні криптосистеми не менш інтенсивно відбувається процес пошуку шляхів можливого вдосконалення таких систем. Роботи [2–6] присвячені дослідженню та аналізу властивостей нормальної форми (або форми Едвардса) еліптичної кривої, які можуть бути цікаві з точки зору криптографії. Аналіз складності групової операції для кривих у формі Едвардса дозволяє стверджувати, що на сьогоднішній день вони є найбільш продуктивними, порівняно з іншими відомими формами еліптичних кривих [2, 3]. У роботі [4] розглянуто перетворення канонічної еліптичної кривої в ізоморфну криву Едвардса, наведено умови, за яких порядок кривої Едвардса має найменший кофактор 4. Оскільки криві Едвардса не стандартизовані, відкритою залишається задача пошуку кривих, прийнятних до криптографії. В роботі [5] запропонований один із можливих шляхів розв'язання цієї задачі, а саме пошук кривих Едвардса над розширеннями полів малої характеристики, а в [6] наданий аналіз щодо складності задачі дискретного логарифмування на кривій Едвардса над розширенням малих полів.

Базуючись на результатах [2–6], у даній роботі наведений набір параметрів для реалізації криптографічної системи на кривій Едвардса над розширеннями поля малої характеристики. В результаті отримано набори з 28 примітивних поліномів та відповідних до них генераторів групи точок кривої Едвардса над полями F_5^{181}, F_5^{277} та F_7^{127}.

1. ПОРЯДКИ КРИВИХ ЕДВАРДСА НАД РОЗШИРЕННЯМИ ПОЛІВ МАЛОЇ ХАРАКТЕРИСТИКИ, ПРИЙНЯТНІ ДЛЯ КРИПТОГРАФІЇ

Крива Едвардса над кінцевим полем F_p^m характеристики $p > 3$ в афінній системі координат визначається рівнянням [1, 2]:

$$x^2 + y^2 = 1 + dx^2y^2,$$

де $d(1 - d) \neq 0$,

$$d \neq A^2. \qquad (1)$$

З точністю до ізоморфізму [2–4] можна вважати різними криві, що задаються різними значеннями параметру d у рівнянні (1), причому d має бути квадратичним нелишком в полі F_p^m. Будь-яка така крива має 4 обов'язкові точки:

$O = (0, 1]$ – нуль адитивної групи точок,

$D = (0, -1)$ – єдину точку другого порядку,

$\pm P = (\pm 1, 0)$ – точки четвертого порядку.

Отже, характерною властивістю кривих вигляду (1) є те, що їх порядок кратний 4. Формули додавання двох точок кривої Едвардса мають вигляд [1, 2]:

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

Закон додавання є повним і визначений для будь-яких двох точок (x_1, y_1), (x_2, y_2), якщо d – квадратичний нелишок у полі F_p^m [2].

У роботі [5] детально розглянуто один із можливих способів знаходження кривих Едвардса вигляду (1), в межах прийнятних криптографічних значень параметрів. Ідея полягає у знаходженні кривої Едвардса мінімального порядку 4 над полем F_p малої характеристики та подальшому розширенні поля з метою відбору простих степенів розширення m, за яких знайдена крива над полем F_p^m має майже просте значення порядку $N_{Em} = 4n$ (де n – просте). В [5] отримано три розширених поля характеристики $p = 5$ або $p = 7$, для яких крива $x^2 + y^2 = 1 + 3x^2y^2$ має псевдопросте значення порядку, що відповідає стандартним вимогам до порядку генератора криптосистеми. Отримані поля наведені в таблиці 1 відповідно до величини поля в бітах та значення $n = N_{Em}/4$.

Слід зауважити, що арифметичні операції в полях малої характеристики та їх розширеннях, як правило, виконуються більш ефективно порівняно з простими полями великої характеристики [5]. Крім того, криві з малим значенням параметру $d = 3$ дають можливість зменшити складність операції додавання різних точок на 1U – одну польову операцію множення на параметр кривої [2, 4], оскільки множення на 3 замінюється триразовим додаванням у полі (тобто практично безкоштовною операцією).

Таблиця 1

Розширення полів характеристики $p = 5$ та $p = 7$ та відповідні прості порядки підгрупи точок кривої $x^2 + y^2 = 1 + 3x^2y^2$

F_p^m	m_b	$n = N_{Em}/4$
F_5^{181}	420	4D1E1043D31FB1CC9B562A717B3C43259476330974981C14F25E03EACA14C7378C72BEB6F54DB 72B8180B352DF12BA34CC023C219
F_5^{227}	527	21C529DD78FA571E196B3EBB0D20429C476A1848CAB5E0E8A121378DE187888F99D299F404EE 4F9B-C974D5035A62AC9F5E1E0DA29A510B4012E23ECD15909A4B1065
F_7^{127}	356	5CAC4104D859A6DF582D5731211D9947A4AE9CFD1F4E3648997D050DCE03624B891381F19AA 1824CF98DE5637

2. ОБЧИСЛЕННЯ ПАРАМЕТРІВ КРИПТОСИСТЕМИ НА КРИВІЙ ЕДВАРДСА НАД РОЗШИРЕННЯМИ МАЛИХ ПОЛІВ

Подальша реалізація рекомендованих у [5] кривих Едвардса над розширеннями полів F_5 та F_7 становить два послідовних етапи:

– пошук примітивних поліномів $P(z)$ для полів F_5^{181}, F_5^{277}, F_7^{127} та побудова відповідної арифметики цих полів;

– обчислення генератора абелевої групи точок кривої згідно з визначеною арифметикою полів F_5^{181}, F_5^{277} та F_7^{127}.

Таким чином, за допомогою прикладної програми був отриманий ряд примітивних поліномів вказаних полів, серед яких ми обрали поліноми найменшої ваги. (Слід зазначити, що для випадку поля F_7^{127} існують примітивні поліноми найменшої можливої ваги – тобто триноми). У загальному випадку точками кривої будуть пари (x, y) елементів поля F_p^m, для яких виконується рівність (1). Щоб отримати генератори підгруп точок досліджуваної кривої Едвардса $x^2 + y^2 = 1 + 3x^2y^2$, вибираємо випадкову координату x з елементів відповідного поля та обчислюємо значення $a = \dfrac{1 - x^2}{1 - 3x^2}$. Визначення квадратного кореня з елементу a в розширеному полі робиться за допомогою експоненціювання [4].

У випадку полів характеристики 5:

$$q = 5^{181} \equiv 5 \bmod 8$$

або

$$q = 5^{227} \equiv 5 \bmod 8.$$

У мультиплікативній групі поля F_q, якщо $a = y^2$ – квадратичний лишок, маємо елементи підгрупи F_5^*:

$$a^{\frac{q-1}{2}} = 1,$$

$$a^{\frac{q-1}{4}} = \pm 1 = \delta,\ \delta^{\frac{1}{2}} = \pm 2.$$

Тоді

$$a = \delta a \cdot a^{\frac{q-1}{4}} = \delta \cdot a^{\frac{q+3}{4}} \Rightarrow y = \delta^{\frac{1}{2}} \cdot a^{\frac{q+3}{8}}.$$

Для поля характеристики 7: $q = 7^{127} \equiv 3 \bmod 4$.

Аналогічно, оскільки $a = y^2$ – квадратичний лишок, маємо:

$$a^{\frac{q-1}{2}} = 1,\ a^{\frac{q-1}{2}} a = a^{\frac{q+1}{2}} = a,\ \Rightarrow\ y = a^{\frac{q+1}{4}}.$$

Таким чином отримаємо пару (x, y), що задовольняє рівності $x^2 + y^2 = 1 + 3x^2y^2$, значить точка $Q = (x, y)$ належить до кривої Едвардса. Помноживши Q на величину n з таблиці1, можемо отримати точку нуль $O = (0, 1)$, точку $D = (0, -1)$ другого порядку або точки $\pm P$ четвертого порядку. В першому випадку генератором G підгрупи точок кривої Едвардса буде власне точка $G = Q = (x, y)$, в інших – генератор G визначається як $G = 2Q$ або $G = 4Q$ відповідно. Результати обчислень, а саме, примітивні поліноми та генератори підгрупи точок кривої $x^2 + y^2 = 1 + 3x^2y^2$ для відповідних полів, наведені в таблицях 2–4 (молодші степені векторів – зліва).

ВИСНОВКИ

З практичної точки зору питання щодо реальних оцінок швидкодії криптосистеми на кривій Едвардса над розширеннями малих полів залишається відкритим. Однак теоретичні дослідження дозволяють стверджувати, що параметри, надані в таблицях 2–4, забезпечать максимальну продуктивність криптосистеми при заданій стійкості.

Отримані параметри можна розглядати як еквівалентні відносно продуктивності при однаковому рівні стійкості системи. Виключення складає випадок поля F_7^{127}: для цього поля знайдено два примітивних поліноми ваги 3,тому відповідна арифметика поля є більш прийнятною порівняно з арифметикою, що побудована відповідно до поліномів більшої ваги. Незначна втрата стійкості [6] криптосистеми на кривій Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полями F_5^{181}, F_5^{227} та F_7^{127}, складає 4 біта в кожному з трьох випадків та є незначною порівняно з величинами відповідних полів у бітах.

У цілому вважаємо, що отримані параметри можна рекомендувати в ході побудови продуктивних криптосистем та розробки проектів майбутніх стандартів та протоколів.

Література

[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.

Таблиця 2

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_5^{181}

P(z) = $z^{181} + z^3 + z^2 + 3z + 3$ *x*=[020142034310022224101012221304140301432203243032241124434204012141101011240333421403412430442412314131110013401212233320143114004323232130032424012224444043224043044333224012421344 3] *y*=[332430012113102123101022332221434201344433301244110443241322234411431010032114420334344112412432431021014432304242413441103201032141100413114111433042433133303044101341124422443002304]
P(z) = $z^{181} + z^3 + 4z^2 + 3z + 2$ *x*=[003221341120100121431033232411403230122241311323210244242401303214311143302311010034314220313344043333222032223222444424114233140304204112240344421344401313430043340203404013033302433] *y*=[030430204201141033440121201004420123233110441401320234130413132430332314112324002304112100120314202043203010241004311331222434423031243233323200023131134221110113111233041334110303]
P(z) = $z^{181} + 2z^4 + z^3 + 2z^2 + 2$ *x*=[220040230041043404420133412422133002214421300102100213000014342404203433130301411043301443334133403430243214003433214402340413103210401232142442030124341024334330424232440120113002] *y*=[324300134424422004304443143011323210214220110204230003303304332200424212313420321244233112204111100321304111301221304220240310204210400144112114132110343442043222324113020213312223 2]
P(z) = $z^{181} + 3z^4 + z^3 + 3z^2 + 3$ *x*=[011433204102241024431323333143404030230302121104140032234130212203213312414310110320022334001221240441441134200322420423343020343343324131140104122114122431314220110124242443242042] *y*=[311413314004400102434442214401411431222410402332322421104120144303241334020333042402231213312011432423300213000033211313020000223144030224120300414144421111040002243104234311144333 1]
P(z) = $z^{181} + z^5 + z^3 + 2z + 2$ *x*=[230131240411444014004331023430112230122412200032422443331243043210341234231422340233444040231120021144303304300324121313201024243440011311440201424314041042203010202041413442203 44] *y*=[033434123041431141422433401103404123342044233133442343442443223324403133423141434011003012441433334023221141034212344144400334121032240203210003304242103013330244110134334240110411 2]
P(z) = $z^{181} + z^5 + z^3 + 2z + 3$ *x*=[033331143444211324403301130103313221202030422040211300031102241223241112323041432130114324303210400034023343134041203141411102033013423121332040144331022011214142131032100202332 33] *y*=[224433021012423102133424420211322011420114010032223220143234001020013040323402413104011423002000431000143241344412311141324132443100130433141322430110132124031133311233110111321222 2]
P(z) = $z^{181} + z^5 + 2z^4 + 3z^3 + 2$ x=[401313203242141100414140341402132031340204211010304301304433000241303202204322333210310143001114430042433302110323403441142111010403133420102301120222303041212423022004240014014144 2] y=[233004302440242400114114043112223221431440010340210110330414113414342233432443313200244201210031432134431420414013303432040211000102400144423003012304204124411022242214442113402104 2]
P(z) = $z^{181} + z^5 + 3z^4 + 3z^3 + 3$ *x*=[430231143030042104122442004211031442233231212331100100323003341201344433331120310002101312011223223204122134310412131024210020010344000212342212231041402210200331004344113222024213] *y*=[220214013224431013231414442230343012344044044401130023141411412230431411443324442143420222112422320020233343333111224420014110214141313101211024203211233332014432024110101244422032]
P(z) = $z^{181} + 2z^5 + 2z^3 + 4z + 2$ *x*=[213303120043101410430241413000223042401423430440104441233234204013241021021410012212131113130013010300034431014044244234032001424420410222124313100214302032044141310412102201011224] *y*=[333342223403012114404422142010023210021141130430442302023204431414313444410321233000203120022141222334233342304003212003112104210341331403421343332031320420414242343223111134313142 4]
P(z) = $z^{181} + 2z^5 + 2z^3 + 4z + 3$ *x*=[041004310220124400010323000323444403432134210112041043030341412422420242102402133113211112200032214301020314430023124230400401241320121003143044221313232340414001111113200242424002 4] *y*=[103300132311434420343104341031424340043124401420403234203202244214313030440040144030112014201104040324134020031111201004020110110010132221100403014044244244444304122341310121023030 02]

Таблиця 3

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_5^{277}

P(z) = $z^{227} + z^3 + 2z^2 + z + 2$ *x*=[200434204200342242421132330113311033122431404333242244010231330340440143341310142343240422122201214402222123002202403002134144100032233014232144123313204242302143241432122113134024422102010113012333310234243412410301100 10244112] *y*=[143314021300210304111310442344114031131013143133441204112044300113411410202331023320443333224142334442403242311333313133304320431140021013242301132431231300041404210042241140132201331324024442100212031201421440342020413 00112124]
P(z) = $z^{227} + z^3 + 3z^2 + z + 3$ *x*=[320221201114411222324310314021323031404042223141002332301313302110244332031130143141303444041130332024410412 2112124013232240022103421404113442144044230413324232024103443241442331014202303401043230341031433334412311032413 3014444] *y*=[001120210000330303040420144233441044014422043244201001232342113432204102340213022403420240434030113014040240 1133341212021323300414322143310300223222304313024443401212311042303131101220244224230313201403111311112343424220 20044441]

$P(z) = z^{227} + z^4 + 2z^2 + z + 2$ x=[00130341131312012421212040140240313014202340431420010044200313404102301334141242324123210333142033414113314031314413000113222221440212004022430131433321234031143331414443402413000302044033411121214340141423243302210011112410233] y=[00314323301034220420433200330304332423230043240411103020101034122314222141341104433434122243404422030404334223334303034040424401041124242344400104324232112301300142220320443040141332230222013431233200332300420214144122220040011]
$P(z) = z^{227} + 2z^4 + 4z^3 + 2z + 3$ x=[04143040131323211331302033023204443224124423021343210341003414444033213324434332221104012340233034200120441212232122404211210033411123013102023002023120343430143204313011133221134001430444231340213300421434310222012014001304312] y=[42230343300243410212030123020242100011302124303210440141002443241020441144112034004242310442233112340411042343130421314112244031221111113214212420111422144013404042341302424143014134400303140332312122304404124120142141042421121]
$P(z) = z^{227} + 3z^4 + 4z^3 + 2z + 2$ x=[42431120100132410101402123140402300013433034141124410421142232234430434120401121023214001134341202002213410434423032400123012013430200241103103223122442420240324142044104100240004233131420424303114010414324324130040420431221312] y=[23232102342014112231203433413112230330443100403233204023040124003030212110124431223141434223110141130003014112014223414410344240443220114242140311242030003020022043303103223344013230202242002334432013101442113041341131031430241]
$P(z) = z^{227} + 4z^4 + 3z^2 + z + 3$ x=[24303342131044231204240342011032222001302212422341124300210304133423242121230234243044432440011442411134133222320440240412311313044320002023232102241443012142241224120334231443021114444001103101414044000330333300223133121322424401] y=[40102210133011344034021002421020034141420303101421331324144221410320010321143014134030033032023410234330304043201320120331223210303032224341221323003143110234311212444143243044203323123423114230014324124313042224402203031310 1]
$P(z) = z^{227} + z^6 + 2z^3 + 3z + 2$ x=[41343412343120121333342000313130332230423131402141143200010243111304221133241011324424303433302322122022133330013424344010021424442231123133242042124241242443220044410131214232130224333204101014144141323112113143340440320304] y=[42341340241244422300440440242221330212001312412041114221331204134443000440111002000141312344244104034224311222404020431110333441012014033401031100020212130201021122122401244121014312434301430040141131032043411000444241002004334]
$P(z) = z^{227} + z^6 + 3z^3 + z + 3$ x=[13400344332022344142410331300231134012343032440040214210314334144342412302243033102032000413012112033000441311241321003432332023102404143423331401224000000004034103413012121121022041011430241031402142103120443432423412343041442 2] y=[02103340414110114412303311341210031003243303104322111303243324030244003103023104232420221234332223111020343134121220432022130433000121203432010320110330301331233132010120324403142341310220200300141314144212422121234042041232021]
$P(z) = z^{227} + 2z^6 + z^4 + 2z^2 + 2$ x=[32430432204441144130401211141034021102003130444001114011304301313433441123000142403411000400241433323230400134043303013343004030211413131231430001030022322410141340242404322113122423244222040423221042213312140403221123420220143] y=[10420433333004020211302010113111131024121232430033304242243030003102014401040010430212034430124413432331321310232423322241243123140220131422102112422100014203040212131300001014434224221141411234112422113200341203313003133043313]
$P(z) = z^{227} + 2z^6 + 3z^4 + 4z^2 + 3$ x=[02124203121121324411200224140411102320211132444243110341144403332421234003140123120411042423013102433344041411420133023011103223400200431141020403033114412130332424342132443301332100234223114013114320024111430010043412323030441] y=[43424210212234423234101402131204120131221240003311022232424130102024343134034323320333441003124123322112410 2012302120210033344401142332300004344211034012233004204031041232212044304430023011210422224300313433044030201434202140 2]

Таблиця 4

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем $F_7{}^{127}$

$P(z) = z^{127} + 3z^2 + 2$ x=[46044006603145305201405123204222530031016222516201005661204244422522523363324113266525222005454623240563146654441612464210212622] y=[13151463044055366051631435240114440055064050055036454015644623565455240161623205625064212024436215201514620643652053153153046 04]
$P(z) = z^{127} + 5z^2 + 4$ x=[03655433365210564341154620351326454535151161013652330566553051162552456414405421111444536306551655040562536036133666510226532136] y=[13205354620266042601015444262135612041153411156022203232033334332456261531212132660656611400600631511244133355062142313264524 65]
$P(z) = z^{127} + 2z^2 + 2z + 4$ x=[64663156522464360424613322621061264325155146612546650340165526460656260605330601001241524365532112242546361653423243663533105 33]
y=[05423004534624634645144346564106464142151303115465555340552214514542542415513632050154600544522051154153431552254401341 6]

$P(z) = z^{127} + 4z^2 + 2z + 2$ x=[156036134334532014564403432461341616623261162625645626110654136116401500643545203224414354302031524052223361061603162304503464 6] y=[225651365154041032143546141001026204244326102044342215055265206316101201033041310341355324424250211600206356043453306053213245]
$P(z) = z^{127} + 2z^3 + 6z^2 + 2$ x=[510232400251512003015131465556251123335143134253126154046246333635444641124021432311045466445624116331516646433452526221032242 2] y=[314546003640022304353165222000356536306533263361055343302601643622336405351324050122611535522560114361501505141233060455355555305]
$P(z) = z^{127} + 4z^3 + 3z^2 + 4$ x=[032104460221551530616360444453465435545665322340211542662646430065534316213363304523543423304163211302330065104135163465126042 1] y=[643004566234311166623635400353406535235400160150044555651513462330355264665540264160105564053203333363313136064113103645665611 3]
$P(z) = z^{127} + 3z^5 + 2z^2 + 4$ x=[360554063253063002002062140020353366635121004451151221431264632043325236211316313312131064046010503011264510662402135401436311 6] y=[502334232404301404025500036021355020350553350330566212632040005330062002331604551532526031661063104051361050150236622362112661 6]
$P(z) = z^{127} + 6z^5 + 4z^2 + 2$ x=[263536326365544262432531352065003352434164663011216645330110565464143210235525622154142303024501161450602100416105443561563056 2] y=[406432032231634653246024514250335146034624533454121205465461245335003004365653411544013653656556131646645012205146262300316223 3]

[3] 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.

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

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

[6] Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Оценка реальной стойкости криптосистемы на кривой Едвардса нарасширениями малых полей. Сучасний захист інформації, №2, 2012. – С. 17–20.

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

Надійшла до редколегії 29.03.2013

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри ММЗІ ФТІ НТУУ «КПІ». Наукові інтереси: криптографія, теорія коригуючого кодування.

Діхтенко Аліса Анатоліївна, аспірант кафедри теорії пружності та обчислювальної математики Донецького національного університету. Наукові інтереси: асиметрична криптографія.

Яценко Олександр Іванович, консорціум ЄДАПС, КП ОТІ, системний програміст відділу криптографічного захисту інформації. Наукові інтереси: криптографія, теорія алгоритмів, програмування.

УДК 681.3.06

Параметры криптосистемы на кривой Едвардса над расширениями малых простых полей / А.В. Бессалов, А.А. Дихтенко, О.И. Яценко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 273–277.

Рассмотрена возможность совершенствования криптосистем на эллиптических кривых на базе кривых, представленных в форме Эдвардса. Описан подход для вычисления общесистемных параметров криптосистемы на кривой Эдвардса над расширениями полей F_5 и F_7. Получено 28 наборов параметров, которые удовлетворяют стандартным криптографическим требованиям и могут быть рекомендованы в будущих стандартах.

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

Табл.: 4. Библиогр.: 7 назв.

UDC 681.3.06

Parameters of cryptosystems on the Edwards curve above expansions of small simple fields / A.V. Bessalov, A.A. Dihtenko, O.I. Yatsenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 273–277.

The improvement possibility of elliptic curve cryptosystems on the basis of the Edwards curves is considered. An approach for evaluating Edwards's curve system-wide-parametres over F_5 and F_7 ffield expansions is described. 28 sets of parametres which satisfy standard cryptographic requirements are obtained. They can be recommended in future standards.

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

Tab.: 4. Ref.:7 items.