КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018
ISSN 2663 - 4023

УДК 681.3.06

Бессалов Анатолій Володимирович
доктор технічних наук, професор
професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID: 0000-0002-6967-5001
a.bessalov@gmail.com

РОЗРАХУНОК ПАРАМЕТРІВ КРИПТОСТІЙКОЇ КРИВІЙ ЕДВАРДСА НАД ПОЛЯМИ ХАРАКТЕРИСТИК 5 ТА 7

Анотація. Запропоновано метод пошуку криптостійких еліптичних кривих у формі Едвардса $x^2 + y^2 = 1 + dx^2y^2$ (де параметр $d -$ квадратичний не лишок у полі) над розширеними кінцевими полями $F_q, q = p^m$ малих характеристик $p \neq 2,3$. Для цих кривих виконується повнота закону додавання точок, тому вони називаються повними кривими Едвардса. На першому етапі над малими простими полями F_5 та F_7 знаходяться параметри d повних кривих Едвардса, які мають мінімальні порядки $N_{E1} = 4$. Для обох кривих отримуємо однакові значення параметрів $d = 3$, які є квадратичними не лишками у відповідних полях F_5 та F_7. Далі для обох кривих за рекурентною формулою обчислюються порядки $N_{Em} = 4n$ (де n – непарне) цих кривих над розширеними полями з простими степенями розширення m в межах відомих криптографічних стандартів (з еквівалентною бітовою довжиною модуля поля 200…600біт). Обчислені значення n тестуються на простоту. Відбираються розширення m, які забезпечують псевдопростий порядок кривої $4n$ з простим значенням n Це забезпечує найвищу крипто стійкість кривої при рішенні проблеми дискретного логарифму. В результаті над полями характеристики $p = 5$ отримано дві криві зі степенями розширення $m = 181$ та $m = 277$, а над полями характеристики $p = 7$ – одна крива зі степенем $m = 127$. Для них визначені відповідні великі прості значення n. Наступний етап – розрахунок інших загальносистемних параметрів криптографічних систем на базі повних кривих Едвардса. над полями характеристик 5 та 7. Арифметика розширених полів базується на незвідних примітивних поліномах $P(z)$ степені m. Виконано пошук та побудова таблиць поліномів $P(z)$ (по 10 різних поліномів для кожного значення m відповідно для значень характеристик $p = 5$ та $p = 7$). На базі кожного поліному згідно з розробленою методикою обчислені координати випадкової точки P кривої. Можливими порядками цієї точки є значення $4n, 2n$ або n Двократним подвоєнням цієї точки знаходяться координати x_G та y_G для 30 різних генераторів $G = 4P$ криптосистеми, які мають простий порядок n. Отримано набори параметрів, що задовольняють стандартним криптографічним вимогам та можуть бути рекомендовані у проектуємих криптосистемах.

Ключові слова: еліптична крива, крива Едвардса, параметр кривої, порядок кривої, порядок точки, розширене поле, незвідний поліном, характеристика поля, крипто стійкість.

1. ВСТУП

Запропонована в роботі [1] нормальна форма еліптичної кривої (форма Едвардса) була суттєво вдосконалено для криптографічних задач авторами [2] і пізніше отримала назву *повних кривих Едвардса.* Вони відрізняються повнотою та універсальністю законів складання точок, а також існуванням афінних координат нейтрального елементу групи точок кривої (заміст точці на нескінченності). Таки переваги повних кривих Едвардса створюють перспективи їх застосування в

криптографії. Роботи [2-6] присвячені дослідженню та аналізу властивостей кривих Едвардса, які можуть бути корисні в криптографічних протоколах. Аналіз складності групової операції для кривих в формі Едвардса дозволяє стверджувати, що на сьогоднішній день вони є найбільш швидкими і продуктивними, порівняно з іншими відомими формами еліптичних кривих [2, 3]. В роботі [4] розглянуто перетворення канонічної еліптичної кривої в ізоморфну криву Едвардса, наведені умови, при 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.

В даній роботі розглянуто методи розрахунку параметрів для реалізації криптографічної системи на кривій Едвардса над розширеннями поля малих характеристик 5 та 7. В результаті отримані 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}.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

2.1. РОЗРАХУНОК ПОРЯДКІВ КРИПТОСТІЙКИХ КРИВИХ ЕДВАРДСА НАД РОЗШИРЕННЯМИ ПОЛІВ ХАРАКТЕРИСТИК 5 ТА 7

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

$$x^2 + y^2 = 1 + d\,x^2y^2, \qquad d(1-d) \neq 0, \left(\frac{d}{p}\right) = -1, \tag{1}$$

де $\left(\frac{d}{p}\right)$ – символ Лежандра [7]. З точністю до ізоморфізму [2,4] можна вважати різними криві, що задаються різними значеннями параметру d в рівнянні (1), причому d має бути квадратичним нелишком в полі F_p. Будь-яка така крива має 4 обов'язкові точки:

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

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

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

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

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

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

В 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

ISSN 2663 - 4023

відбору простих степенів розширення m, при 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 задовольняє стандартним вимогам до порядку генератора криптосистеми. Отримані поля наведені в таблиці 1 відповідно до величини поля в бітах ($m_b = mlog_2p$) та значення $n = N_{Em}/4$.

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	4D1E1043D31FB1CC9B562A717B3C43259476330974981C14F25E03EACA14C7378C72BEB6F54DB72B8180B352DF12BA34CC023C219
F_5^{227}	527	21C529DD78FA571E196B3EBB0D20429C476A1848CAB5E0E8A121378DE187888F99D299F404EE4F9BC974D5035A62AC9F5E1E0DA29A510B4012E23ECD15909A4B1065
F_7^{127}	356	5CAC4104D859A6DF582D5731211D9947A4AE9CFD1F4E3648997D050DCE03624B891381F19AA1824CF98DE5637

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 зі 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 трикратним додаванням у полі (тобто практично безкоштовною операцією).

2.2. РОЗРАХУНОК ПАРАМЕТРІВ КРИПТОСИСТЕМИ НА КРИВІЙ ЕДВАРДСА НАД РОЗШИРЕННЯМИ ПОЛІВ ХАРАКТЕРИСТИК 5 ТА 7

Пошук рекомендованих у [5] повних кривих Едвардса над розширеннями полів F_5 та F_7 включає наступні етапи:

- пошук примітивних поліномів P(z) для полів F_5^{181}, F_5^{277},F_7^{127} та побудова відповідної арифметики цих полів;
- обчислення координат генератора абелевої групи точок кривої порядку n згідно з визначеною арифметикою полів F_5^{181}, F_5^{277} та F_7^{127}.

Таким чином, за допомогою прикладної програми був отрипманий 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 $a = \frac{1-x^2}{1-3x^2}$. Визначення квадратного кореня з елементу a в розширеному полі робиться за допомогою експоненціювання [4,7].

У випадку полів характеристики 5: $q = 5^{181} \equiv 5 \bmod 8$ або

ISSN 2663 - 4023

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

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

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

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

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

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

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

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 $\pm P = (\pm 1, 0)$ 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).

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 4]
y=[332430012113102123101022332221434201344433301244110443241322234411431010032114420334344112412432431021014432304241344110320103214110041311411143304243313330304410134112442244300230 4]
P(z) = $z^{181} + z^3 + 4z^2 + 3z + 2$ *x*=[003221341120100121431033232411403230122241311323210244242401303214311143302311010034314220313344043333222032222322444424114233140304204112240344421344401313430043340203404013033302 43]
y=[030430204201141033440121201004420123233110441401320234130413132430332314112324002304112100120314202043203010241004311331222434423031243233323200023131134221110113111233041334110303]
P(z) = $z^{181} + 2z^4 + z^3 + 2z^2 + 2$ *x*=[220040230041043404420133412422133002214421300102100213000014342404203433130301411043301443334133403430243214003433214402340413103210401232142442030124341024334330424232440120113002]
y=[324300134424422004304443143011323210214220110204230003303304332200424212313420321244233112204111100321304113101221304220240310204210400144112114132110343442043222324113020213312223 2]

$P(z) = z^{181} + 3z^4 + z^3 + 3z^2 + 3$ *x*=[01143320410224102443132333314340403023030212110414003223413021220321331241431011032002233400122124044144113420032242042334302034334332413114010412211412243131422011012424244324204 2] *y*=[31141331400440010243444221440141143122241040233232242110412014430324133402033304240223121331201143242330021300003321131302000223144030224120300414144421111040002243104234311144333 1]
$P(z) = z^{181} + z^5 + z^3 + 2z + 2$ *x*=[23013124041144401400433102343011223012242120003242244333124304321034123423142234023344404023112002114430330430032412131320102424344001131114402014243140410422030102020414113441220344] *y*=[03343412304143114142243340110340412334204423313344234344244322333244031334231414340110030124414333340232211410342123441444003341210322402032100033042421030133302441101343342401104112]
$P(z) = z^{181} + z^5 + z^3 + 2z + 3$ *x*=[03333114344421113244033011301033132212020304220402113000311022412232411123230414321301143243032104000340233431340412031414111020330134231213320401443310220112141421310321002023323 3] *y*=[22443302101242310213342442021132201142011401003222322014323400102001304032340241310401142300200043100014324134441231114132413244310013043314132243011013212403113331123311011321222 2]
$P(z) = z^{181} + z^5 + 2z^4 + 3z^3 + 2$ x=[40131320324214110041414034140213203134020421101030430130443300024130320220432233321031014300111443004243330211032340344114211101040313342010230112022230304121242302200424001401414 42] y=[23300430244024240011411404311222322143144001034021011033041411341422334324433132002442012100314321344314204140133034320402110001024001444230030123042041244110222422144421134021042]
$P(z) = z^{181} + z^5 + 3z^4 + 3z^3 + 3$ *x*=[43023114303004210412244200421103144223323121233110010032300334120134443333112031000210131201122322320412213431041213102421002001034400021234221223104140221020033100434411322202421 3] *y*=[22021401322443101323141444223034301234404404440113002314141141223043141144332444214342022211242232002023334333311122442001411021414131310121102420321123333201443202411010124442203 2]
$P(z) = z^{181} + 2z^5 + 2z^3 + 4z + 2$ *x*=[21330312004310141043021411300022304240142343044010444123323420401324102102141001221213111313001301030003443101404424423403200142442041022212431310021430203204414131041210220100112 24] *y*=[33334222340301211440442214201002321002114113043044230202320443141344441032123300020312002214122233423334230400321200311210421034133140342134333203132042041424234322311113431314 24]
$P(z) = z^{181} + 2z^5 + 2z^3 + 4z + 3$ *x*=[04100431022012440001032300032344440343213421011204104303034141242242024210240213311321111220003221430102031443002312423040040124132012100314304422131323234041400111111320024242400 24] *y*=[10330013231143442034310434103142434004312440142040323420320224421431303044004014403011201420110404032413402003111201004020110110010132221100403014044244244444304122341310121023030 02]

ISSN 2663 - 4023

Таблиця 3

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полемF_5^{277}.

P(z) = $z^{227} + z^3 + 2z^2 + z + 2$ *x*=[200434204200342242421132330113311033122431404333242244010231330340440143341310142343240422122012144022221230022024030021341441000322330142321441233132042423021432414321221131340244221020101130123333102342434124103011001024411 2]
P(z) = $z^{227} + z^3 + 3z^2 + z + 3$ *x*=[320221201114411222324310314021323031404042223141002332301313302110244332031130143141303444041130332024410412211212401323224002210342140411344214404423041332423202410344324144233101420230340104323034103143333441231103241330144 4]
P(z) = $z^{227} + z^4 + 2z^2 + z + 2$ *x*=[001303411313120124212120401402403130142023404314200100442003134041023013341412423241232103331420334141133140313144130001132222214402120040222430131433321234031143331414443402413000302044033411121214340141423243302210011124102 33]
P(z) = $z^{227} + 2z^4 + 4z^3 + 2z + 3$ *x*=[041430401313232113313020330232044432241244230213432103410034144440332133244343322211040123402330342001204412122321224042112100334111230131020230020231203434301432043130111332211340014304442313402133004214343102220120140013043 12]
P(z) = $z^{227} + 3z^4 + 4z^3 + 2z + 2$ *x*=[424311201001324101014021231404023000134330341411244104211422322344304341204011210232140011343412020022134104344230324001230120134302002411031032231224424202403241420441041002400042331314204243031140104143243241300404204312213 12]

$P(z) = z^{227} + 4z^4 + 3z^2 + z + 3$ *x*=[24303342131044231204240342011032222001302212422341124300210304133423242121230234243044432440011442411134133222320440241231131304432000202323210224144301214224122412033423144302111444400110310141404400033033330022313312132242401] *y*=[40102210133011344034021002421020034141420303101421331324144221410320010321143014134030033032023410234330304043201320120331223210303032224341221323003143110234311212444143243044203323123423114230014324124313042224402203031310 1]
$P(z) = z^{227} + z^6 + 2z^3 + 3z + 2$ *x*=[41343412343120121333342000313130332230423131402141143200010243111304221133241011324424303433302322122122022133330013424344010021424442231123133242042124241242443220044410131214232130224333204101014144141323112113143340440320304] *y*=[42341340241244422300440440242221330212001312412041114221331204134443000440111002000141312344244104034224311222404020431110333441012014033401031100020212130201021122122401244121014312434301430040141131032043411000444241002004334]
$P(z) = z^{227} + z^6 + 3z^3 + z + 3$ *x*=[13400344332022344142410331300231134012343032440040214210314334144342412302243033102032000413012112033000441311241321003432332023102404143423331401224000000040341034130121211210220410114302410314021421031204434324234123430414422] *y*=[02103340414110114412303311341210031003243303104322111303243324030244003103023104232420221234332223111020343134121220432022130433000121203432010320110330301331233132010120324403142341310220200300141314144212422121234042041232021]
$P(z) = z^{227} + 2z^6 + z^4 + 2z^2 + 2$ *x*=[32430432204441144130401211141034021102003130444001114011304301313433441123000142403411000400241433323230400134043303013343004030211413131231430001030022322410141340242404322113122423244222040423221042213312140403221123420220143] *y*=[10420433333004020211302010113111131024121232430033304242243030003102014401040010430212034430124413432331321310232423322241243123140220131422102112422100014203040212131300001014434224221141411234112422113200341203313003133044 24]
$P(z) = z^{227} + 2z^6 + 3z^4 + 4z^2 + 3$ *x*=[02124203121121324411200224140411102320211132444243110341144403332421234003140123120411042423013102433344041411420133023011103223400200431141020403033114412130332424342132443301332100234223114013114320024111430010043412323030441] *y*=[43424210212234423234101402131204120131221240003311022232424130102024343134034323320333441003124123322112414420123021202100333440114233230000434421103401223300420403104123221204430443002301121042222430031343304403020143420214 02]

ISSN 2663 - 4023

Таблиця 4

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полемF_7^{127}

P(z) = $z^{127} + 3z^2 + 2$ *x*=[460440066031453052014051232042225300310162225162010056612042444225225233633241132665252220054546232405631466544161246421021262 2] *y*=[131514630440553660516314352401144400550640500550364540156446235654552401616232056250642120244362152015146206436520531531530460 4]
P(z) = $z^{127} + 5z^2 + 4$ *x*=[036554333652105643411546203513264545351511610136523305665530511625524564144054211114445363065516550405625360361336651022653213 6] *y*=[132053546202660426010154442621356120411534111560222032320333343324562615312121326606566114006006315112441333550621423132645246 5]
P(z) = $z^{127} + 2z^2 + 2z + 4$ *x*=[646631565224643604246133226210612643251551466125466503401655264606562606053306010012415243655321122425463616534232436635331053 3] *y*=[054230045346246346451443465641064641421513031154655553405522145145425424155136320501546005445220511541534315522544013432301661 4]
P(z) = $z^{127} + 4z^2 + 2z + 2$ *x*=[156036134334532014564403432461341616623261162625645626110654136116401500643545203224414354302031524052223361061603162304503464 6] *y*=[225651365154041032143546141001026204244326102044342215055265206316101201033041310341355324424250211600206356043453305605321324 5]
P(z) = $z^{127} + 2z^3 + 6z^2 + 2$ *x*=[510232400251512003015131465556251123335143134253126154046246333635444641124021432311045466445624116331516646433452526221032242 2] *y*=[314546003640022304353165222000356536306533263361055343302601643622336405351324050122611535522560114361501505141233060455355530 5]
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*=[406432032231634653246024514250335146034624533454121205465461245350030043656534115440136536565561316466450122051462623003162233]

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

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 з виграшам порівняно з кривою у формі Вейерштрасса, близьким до 1.5 [4] .

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} таF_7^{127}, складає 4 біта в кожному з трьох випадків та є незначною порівняно з величинами відповідних полів в бітах.

В цілому вважаємо, що отримані параметри можна рекомендувати при побудові продуктивних криптосистем та розробці проектів майбутніх стандартів та протоколів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] H. M. Edwards, “A normal form for elliptic curves,” *Bulletin of the American Mathematical Society*, vol. 44, no. 3, pp. 393–422, Jul. 2007.

[2] Daniel J. Bernstein and Lange Tanja, “Faster addition and doubling on elliptic curves,” *IST-2002-507932 ECRYPT*, pp. 1–20, 2007.

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

[4] А. В. Бессалов, *Эллиптические кривые в форме Эдвардса и криптография*, Киев, «Политехника», 272 с., 2017.

[5] А. В. Бессалов, А. И. Гурьянов и А. А. Дихтенко, «Кривые Эдвардса почти простого порядка над расширениями малых простых полей», *Прикладная радиоэлектроника*, том 11, №2, сс. 225–227, 2012.

[6] А. В. Бессалов, А. А. Дихтенко и Д. Б. Третьяков, «Оценка реальной стойкости криптосистемы на кривой Едвардса над расширениями малых полей», *Сучасний захист інформації*, №2, сс. 17–20, 2012.

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

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (1), 2018
ISSN 2663 - 4023

UDC 681.3.06

Anatoliy V.Bessalov
Professor of the Department of Information and cyber security Professor of
Borys Grinchenko Kyiv University
OrcID: 0000-0002-6967-5001
a.bessalov17@gmail.com

CALCULATION OF PARAMETERS OF CRYPTIC CRIVIAE EDWARDS OVER THE FIELDS OF CHARACTERISTICS 5 AND 7

Abstract. The method of search of cryptographic strong elliptic curves in the Edwards form $x^2 + y^2 = 1 + dx^2y^2$ (where parameter d is non square in the field) over the extended finite fields $F_q, q = p^m$ of small characteristics $p \neq 2.3$ is proposed. For these curves is performed the completeness of the points addition law, so they are called as complete Edwards curve. In the first stage over a small prime fields F_5 and F_7 we find the parameters *d* of complete Edwards curves who have minimum orders $N_{E1} = 4$. For both curves we obtain the same values *d* = 3, which are non square in the fields F_5 and F_7. Next with help recurrent formulae for both curves we calculated the orders $N_{Em} = 4n$ (where *n* is odd) of these curves over the extended fields with prime degrees of extension *m* within known cryptographic standards (with the same bit-length field module 200 ... 600 bits). The calculated values *n* are tested on primelity. The extensions *m*, which provide a psevdoprime order 4*n* of curve with a prime value *n*, are selected. This provides the highest cryptographic stability of curve by the discrete logarithm problem solution. As a result, over the fields of the characteristic *p* = 5 we obtain two curves with degrees of expansion *m* = 181 and *m* = 277, and over the fields of the characteristic *p* = 7 one curve with the degree *m* = 127. For them, the corresponding large prime values of *n* are determined. The next stage is the calculation of other system-parameters of cryptographic systems based on complete Edwards curves. over the fields of characteristics 5 and 7. The arithmetic of extended fields is based on irreducible primitive polynomials *P* (*z*) of degree *m*. The search and construction of polynomial tables *P* (z) (for 10 different polynomials for each value *m*, respectively, for the values of the characteristics *p* = 5 and *p* = 7) has been performed. On the basis of each polynomial according to the developed method, the coordinates of the random point *P* of the curve are calculated. The possible order of this point is the value of 4n, 2n or n. The double doubling of this point is the coordinates x_G and y_G for 30 different generators *G* = 4*P* cryptosystems that have a prime order *n*. The set of parameters that satisfy the standard cryptographic requirements and can be recommended in projecting cryptosystems is obtained.

Keywords:elliptic curve, Edwards curve, curves parameter, curves order, points order, extended field, irreducible polynomial, field characteristic, cryptographic stability

REFERENCES

[1] H. M. Edwards, “A normal form for elliptic curves,” *Bulletin of the American Mathematical Society*, vol. 44, no. 3, pp. 393–422, Jul. 2007.
[2] Daniel J. Bernstein and Lange Tanja, “Faster addition and doubling on elliptic curves,” *IST-2002-507932 ECRYPT*, pp. 1–20, 2007.
[3] A. V. Bessalov, A. A. Dikhtenko and D. B. Tret'yakov, “Sravnitel'naya otsenka bystrodeistviya kanonicheskikh ellipticheskikh krivykh i krivykh v forme Edvardsa nad konechnym polem [A comparative estimate of the speed of canonical elliptic curves and curves in the Edwards form over a finite field],” *Suchasnyy zakhyst informatsiyi*, no. 4, pp. 33–36, 2011.
[4] A. V. Bessalov, *Ellipticheskie krivye v forme Edvardsa i kriptografiya* [*Elliptic curves in Edwards form and cryptography*], Kiev, «Politekhnika», 272 p., 2017.

[5] A. V. Bessalov, A. I. Gur'yanov and A. A. Dikhtenko, "Krivye Edvardsa pochti prostogo poryadka nad rasshireniyami malykh prostykh polei [Edwards curves of almost simple order over extensions of small prime fields]," *Prikladnaya radioelektronika*, tom 11, no. 2, pp. 225–227, 2012.

[6] A. V. Bessalov, A. A. Dikhtenko and D. B. Tret'yakov, "Otsenka real'noi stoikosti kriptosistemy na krivoi Edvardsa nad rasshireniyami malykh polei [An estimate of the real stability of a cryptosystem on the Edwards curve over extensions of small fields]," *Suchasnyy zakhyst informatsiyi*, no. 2, pp. 17–20, 2012.

[7] A. V. Bessalov and A. B. Telizhenko, *Kriptosistemy na ellipticheskikh krivykh: Ucheb. posobie* [*Cryptosystems on elliptical curves: A tutorial*], Kiev, IBC "Politekhnika," 224 p., 2004.