

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 КРИВОЇ 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 (замість 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]:

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

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]:

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right), \quad (2)$$

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

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 ( $m_b = m \log_2 p$ ) 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  $F_5^{181}$ ,  $F_5^{227}$ ,  $F_7^{127}$  та побудова відповідної арифметики цих полів;
- обчислення координат генератора абелевої групи точок кривої порядку  $n$  згідно з визначеною арифметикою полів  $F_5^{181}$ ,  $F_5^{227}$  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 триніми). 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:  $q = 5^{181} \equiv 5 \pmod{8}$  або



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

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

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

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:  $q = 7^{127} \equiv 3 \pmod{4}.$

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

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

Таким чином отримуємо 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 таблиці 1, 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  $F_5^{181}$ .**

$P(z) = z^{181} + z^3 + z^2 + 3z + 3$ $x=[020142034310022224101012221304140301432203243032241124434204012$ $1411010112403334214034124304424123141311100134012122333201431140043232$ $321300324240122244440432240430443332240124213444]$ $y=[332430012113102123101022332221434201344433301244110443241322234$ $4114310100321144203343441124124324310210144323042413441103201032141100$ $413114111433042433133303044101341124422443002304]$
$P(z) = z^{181} + z^3 + 4z^2 + 3z + 2$ $x=[003221341120100121431033232411403230122241311323210244242401303$ $214311143302311010034314220313344043332220322232244442411423314030420$ $411224034442134440131343004334020340401303330243]$ $y=[030430204201141033440121201004420123233110441401320234130413132$ $4303323141123240023041121001203142020432030102410043113312224344230312$ $43233323200023131134221110113111233041334110303]$
$P(z) = z^{181} + 2z^4 + z^3 + 2z^2 + 2$ $x=[220040230041043404420133412422133002214421300102100213000014342$ $4042034331303014110433014433341334034302432140034332144023404131032104$ $01232142442030124341024334330424232440120113002]$ $y=[324300134424422004304443143011323210214220110204230003303304332$ $2004242123134203212442331122041111003213041131012213042202403102042104$ $001441121141321103434420432223241130202133122232]$



$P(z) = z^{181} + 3z^4 + z^3 + 3z^2 + 3$ $x=[011433204102241024431323333143404030230302121104140032234130212203213312414310110320022334001221240441441134200322420423343020343343324131140104122114122431314220110124242443242042]$ $y=[311413314004400102434442214401411431222410402332322421104120144303241334020333042402231213312011432423300213000033211313020002231440302241203004141444211110400022431042343111443331]$
$P(z) = z^{181} + z^5 + z^3 + 2z + 2$ $x=[2301312404114440140043310234301122301224212000324224433312430432103412342314223402334440402311200211443033043003241213132010242434400113114402014243140410422030102020414113441220344]$ $y=[0334341230414311414224334011034041233420442331334423434424432233244031334231414340110030124414333340232211410342123441444003341210322402032100033042421030133302441101343342401104112]$
$P(z) = z^{181} + z^5 + z^3 + 2z + 3$ $x=[033331143444211132440330113010331322120203042204021130003110224122324111232304143213011432430321040003402334313404120314141110203301342312133204014433102201121414213103210020233233]$ $y=[2244330210124231021334244202113220114201140100322232201432340010200130403234024131040114230020004310001432413444123111413241324431001304331413224301101321240311333112331101113212222]$
$P(z) = z^{181} + z^5 + 2z^4 + 3z^3 + 2$ $x=[4013132032421411004141403414021320313402042110103043013044330002413032022043223332103101430011144300424333021103234034411421110104031334201023011202223030412124230220042400140141442]$ $y=[2330043024402424001141140431122232214314400103402101103304141134143422334324433132002442012100314321344314204140133034320402110001024001444230030123042041244110222422144421134021042]$
$P(z) = z^{181} + z^5 + 3z^4 + 3z^3 + 3$ $x=[430231143030042104122442004211031442233231212331100100323003341201344433331120310002101312011223223204122134310412131024210020010344000212342212231041402210200331004344113222024213]$ $y=[220214013224431013231414442230343012344044044401130023141411412230431411443324442143420222112422320020233343333111224420014110214141313101211024203211233332014432024110101244422032]$
$P(z) = z^{181} + 2z^5 + 2z^3 + 4z + 2$ $x=[2133031200431014104302141130002230424014234304401044412332342040132410210214100122121311131300130103000344310140442442340320014244204102221243131002143020320441413104121022010011224]$ $y=[3333422234030121144044221420100232100211411304304423020232044314143134444103212330002031200221412223342333423040032120031121042103413314034213433320313204204142423432231111343131424]$
$P(z) = z^{181} + 2z^5 + 2z^3 + 4z + 3$ $x=[0410043102201244000103230003234444034321342101120410430303414124224202421024021331132111122000322143010203144300231242304004012413201210031430442213132323404140011111132002424240024]$ $y=[1033001323114344203431043410314243400431244014204032342032022442143130304400401440301120142011040403241340200311120100402011011001013222110040301404424424444430412234131012102303002]$



Таблиця 3

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

$P(z) = z^{227} + z^3 + 2z^2 + z + 2$ $x=[20043420420034224242113233011331103312243140433324224401023133034044014334131014234324042212220121440222212300220240300213414410003223301423214412331320424230214324143212211313402442210201011301233331023424341241030110010244112]$ $y=[14331402130021030411131044234411403113101314313344120411204430011341141020233102332044333322414233444240324231133331313330432043114002101324230113243123130004140421004224114013220133132402444210021203120142144034202041300112124]$
$P(z) = z^{227} + z^3 + 3z^2 + z + 3$ $x=[3202212011144112223243103140213230314040422231410023323013133021102443320311301431413034440411303320244104122112124013232240022103421404113442144044230413324232024103443241442331014202303401043230341031433344123110324133014444]$ $y=[00112021000033030304042014423344104401442204324420100123234211343220410234021302240342024043403011301404024011333412120213233004143221433103002232223043130244434012123110423031311012202442242303132014031113111234342422020044441]$
$P(z) = z^{227} + z^4 + 2z^2 + z + 2$ $x=[00130341131312012421212040140240313014202340431420010044200313404102301334141242324123210333142033414113314031314413000113222221440212004022243013143332123403114333141444340241300030204403341112121434014142324330221001112410233]$ $y=[00314323301034220420433200330304332423230043240411103020101034122314222141341104433434122243404422030404334223334303034040424401041124242344400104324232112301300142220320443040141332230222013431233200332300420214144122220040011]$
$P(z) = z^{227} + 2z^4 + 4z^3 + 2z + 3$ $x=[04143040131323211331302033023204443224124423021343210341003414444033213324434332221104012340233034200120441212232122404211210033411123013102023002023120343430143204313011133221134001430444231340213300421434310222012014001304312]$ $y=[42230343300243410212030123020242100011302124303210440141002443241020441144112034004242310442233112340411042343130421314112244031221111113214212420111422144013404042341302424143014134400303140332312122230440412412014214104242112]$
$P(z) = z^{227} + 3z^4 + 4z^3 + 2z + 2$ $x=[4243112010013241010140212314040230001343303414112441042114223223443043412040112102321400113434120200221341043442303240012301201343020241103103223122442420240324142044104100240004233131420424303114010414324324130040420431221312]$ $y=[2323210234201411223120343341311223033044310040323320402304012403030212110124431223141434223110141130003014112014223414410344240443220114242140311242030003020022043303103223344013230202242002334432013101442113041341131031430241]$



$P(z) = z^{227} + 4z^4 + 3z^2 + z + 3$   
 $x=[243033421310442312042403420110322220013022124223411243002103041$   
 $334232421212302342430444324400114424111341332232044024123113130443200$   
 $0202323210224144301214224122412033423144302111444400110310141404400033$   
 $033330022313312132242401]$   
 $y=[401022101330113440340210024210200341414203031014213313241442214$   
 $1032001032114301413403003303202341023433030404320132012033122321030303$   
 $2224341221323003143110234311212444143243044203323123423114230014324124$   
 $3130422244022030313101]$

$P(z) = z^{227} + z^6 + 2z^3 + 3z + 2$   
 $x=[413434123431201213333420003131303322304231314021411432000102431$   
 $1130422113324101132442430343330232212212202213333001342434401002142444$   
 $2231123133242042124241242443220044410131214232130224333204101014144141$   
 $323112113143340440320304]$   
 $y=[423413402412444223004404402422213302120013124120411142213312041$   
 $3444300044011100200014131234424410403422431122240402043111033344101201$   
 $4033401031100020212130201021122122401244121014312434301430040141131032$   
 $043411000444241002004334]$

$P(z) = z^{227} + z^6 + 3z^3 + z + 3$   
 $x=[134003443320223441424103313002311340123430324400402142103143341$   
 $4434241230224303310203200041301211203300044131124132100343233202310240$   
 $414342333140122400000040341034130121211210220410114302410314021421031$   
 $204434324234123430414422]$   
 $y=[021033404141101144123033113412100310032433031043221113032433240$   
 $3024400310302310423242022123433222311102034313412122043202213043300012$   
 $1203432010320110330301331233132010120324403142341310220200300141314144$   
 $212422121234042041232021]$

$P(z) = z^{227} + 2z^6 + z^4 + 2z^2 + 2$   
 $x=[324304322044411441304012111410340211020031304440011140113043013$   
 $1343344112300014240341100040024143332323040013404330301334300403021141$   
 $3131231430001030022322410141340242404322113122423244222040423221042213$   
 $312140403221123420220143]$   
 $y=[104204333330040202113020101131111310241212324300333042422430300$   
 $0310201440104001043021203443012441343233132131023242332224124312314022$   
 $0131422102112422100014203040212131300001014434224221141411234112422113$   
 $20034120331300313304424]$

$P(z) = z^{227} + 2z^6 + 3z^4 + 4z^2 + 3$   
 $x=[021242031211213244112002241404111023202111324442431103411444033$   
 $3242123400314012312041104242301310243334404141142013302301110322340020$   
 $0431141020403033114412130332424342132443301332100234223114013114320024$   
 $111430010043412323030441]$   
 $y=[434242102122344232341014021312041201312212400033110222324241301$   
 $0202434313403432332033344100312412332211241442012302120210033344401142$   
 $3323000043442110340122330042040310412322120443044300230112104222243003$   
 $134330440302014342021402]$





Таблиця 4

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

$P(z) = z^{127} + 3z^2 + 2$ $x=[460440066031453052014051232042225300310162225162010056612042444$ $2252252336332411326652522200545462324056314665441612464210212622]$ $y=[131514630440553660516314352401144400550640500550364540156446235$ $6545524016162320562506421202443621520151462064365205315315304604]$
$P(z) = z^{127} + 5z^2 + 4$ $x=[036554333652105643411546203513264545351511610136523305665530511$ $6255245641440542111144453630655165504056253603613366510226532136]$ $y=[132053546202660426010154442621356120411534111560222032320333343$ $3245626153121213266065661140060063151124413335506214231326452465]$
$P(z) = z^{127} + 2z^2 + 2z + 4$ $x=[646631565224643604246133226210612643251551466125466503401655264$ $6065626060533060100124152436553211224254636165342324366353310533]$ $y=[054230045346246346451443465641064641421513031154655553405522145$ $1454254241551363205015460054452205115415343155225440134323016614]$
$P(z) = z^{127} + 4z^2 + 2z + 2$ $x=[156036134334532014564403432461341616623261162625645626110654136$ $1164015006435452032244143543020315240522233610616031623045034646]$ $y=[225651365154041032143546141001026204244326102044342215055265206$ $3161012010330413103413553244242502116002063560434533056053213245]$
$P(z) = z^{127} + 2z^3 + 6z^2 + 2$ $x=[510232400251512003015131465556251123335143134253126154046246333$ $6354446411240214323110454664456241163315166464334525262210322422]$ $y=[314546003640022304353165222000356536306533263361055343302601643$ $6223364053513240501226115355225601143615015051412330604553555305]$
$P(z) = z^{127} + 4z^3 + 3z^2 + 4$ $x=[032104460221551530616360444453465435545665322340211542662646430$ $0655343162133633045235434233041632113023300651041351634651260421]$ $y=[643004566234311166623635400353406535235400160150044555651513462$ $3303552646655402641601055640532033333633131360641131036456656113]$
$P(z) = z^{127} + 3z^5 + 2z^2 + 4$ $x=[360554063253063002002062140020353366635121004451151221431264632$ $0433252362113163133121310640460105030112645106624021354014363116]$ $y=[502334232404301404025500036021355020350553350330566212632040005$ $3300620023316045515325260316610631040513610501502366223621126616]$
$P(z) = z^{127} + 6z^5 + 4z^2 + 2$ $x=[263536326365544262432531352065003352434164663011216645330110565$ $4641432102355256221541423030245011614506021004161054435615630562]$ $y=[406432032231634653246024514250335146034624533454121205465461245$ $3350030043656534115440136536565561316466450122051462623003162233]$

### 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 вирашам 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  $F_5^{181}$ ,  $F_5^{227}$  та  $F_7^{127}$ , 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 Эдвардса 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.



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 primality. The extensions  $m$ , which provide a pseudoprime order  $4n$  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  $G = 4P$  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, «Politekhnik», 272 p., 2017.



- [5] A. V. Bessalov, A. I. Gur'yanov and A. A. Dikhtenko, "Krivye Edvardsa pochi 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 "Politekhnik," 224 p., 2004.