УДК 681.3.06

Параметри криптосистеми на кривій Едвардса над розширеннями малих простих полів

Бессалов А.В., Діхтенко А.А., Яценко О.І.

Розглянуто можливість вдосконалення криптографічних систем на еліптичних кривих на базі кривих в 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 задовольняють стандартним криптографічним вимогам та можуть бути рекомендовані у майбутніх стандартах.

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.

The refinement possibility on elliptic curve cryptosystems on the basis of the Edwards curves is considered. The approach for an evaluation of Edwards's curve domain-parametres over of F_5 and F_7 field expansions is described. 28 gangs of parametres which satisfy standard cryptographic requirements are received. They can be recommended in the future standards.

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 в формі Едвардса дозволяє стверджувати, що на сьогоднішній день вони є найбільш 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.

Базуючись на результатах [2-6], в даній роботі приведений набір параметрів для реалізації криптографічної системи на кривій Едвардса над розширеннями поля малої характеристики. 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} таF_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]:

$$x^2 + y^2 = 1 + d\,x^2y^2, \qquad \text{де } d(1-d) \neq 0,\ d \neq A^2. \qquad (1)$$

З точністю до ізоморфізму [2-4] можна вважати різними криві, що задаються різними значеннями параметру d в 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 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 та значення $n = N_{Em}/4$.

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

F_p^m	m_b	$n = N_{Em}/4$
F_5^{181}	420	4D1E1043D31FB1CC9B562A717B3C43259476330974981C14F25E03 EACA14C7378C72BEB6F54DB72B8180B352DF12BA34CC023C219
F_5^{227}	527	21C529DD78FA571E196B3EBB0D20429C476A1848CAB5E0E8A12 1378DE187888F99D299F404EE4F9BC974D5035A62AC9F5E1E0DA 29A510B4012E23ECD15909A4B1065
F_7^{127}	356	5CAC4104D859A6DF582D5731211D9947A4AE9CFD1F4E3648997D 050DCE03624B891381F19AA1824CF98DE5637

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. Обчислення параметрів криптосистеми на кривій Едвардса над розширеннями малих полів.

Подальша реалізація рекомендованих у [5] кривих Едвардса над розширеннями полів F_5 та F_7представляє собою 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 $a = \frac{1-x^2}{1-3x^2}$. 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

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

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

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

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

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

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).

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

P(z) = $z^{181} + z^3 + z^2 + 3z + 3$ *x*=[020142034310022224101012221304140301432203243032241124434204012141101011240333421403412430442412314131110013401212233320143114004323232130032424012224444043224043044333224012421344] *y*=[332430012113102123101022332221434201344433301244110443241322234411431010032114420334344112412432431021014432304241344110320103214110041311411143304243313330304410134112442244300230 4]
P(z) = $z^{181} + z^3 + 4z^2 + 3z + 2$ *x*=[003221341120100121431033232411403230122241311323210244242401303214311143302311010034314220313344043333222032223224444241142331403042041122403444213444013134300433402034040130333024 3] *y*=[030430204201141033440121201004420123233110441401320234130413132430332314112324002304112100120314202043203010241004311331222434423031243233323200023131134221110113111233041334110303]

P(z) = $z^{181} + 2z^4 + z^3 + 2z^2 + 2$

x=[22004023004104340442013341242213300221442130010210021300001434240420343313030141104330144333413340343024321400343321440234041310321040123214244203012434102433433042423244012011300 2]

y=[32430013442442200430444314301132321021422011020423000330330433220042421231342032124423311220411110032130411310122130422024031020421040014411211413211034344204322324113020213312223 2]

P(z) = $z^{181} + 3z^4 + z^3 + 3z^2 + 3$

x=[01143320410224102443132333143404030230302121104140032234130212203213312414310110320022334001221240441441134200322420423343020343343324131140104122114122431314220110124242443242042]

y=[31141331400440010243444221440141143122241040233232242110412014430324133402033304240223121331201143242330021300003321131302000223144030224120300414144421111040002243104234311144333 1]

P(z) = $z^{181} + z^5 + z^3 + 2z + 2$

x=[23013124041144401400433102343011223012242120003242244333124304321034123423142234023344404023112002114430330430032412131320102424344001131144020142431404104220301020204141134412203 44]

y=[03343412304143114142243340110340412334204423313344234344244322332440313342314143401100301244143333402322114103421234414440033412103224020321000330424210301333024411013433424011041 12]

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=[23300430244024240011411404311222322143144001034021011033041411341434223343244331320024420121003143213443142041401330343204021100010240014442300301230420412441102224221444211340210 42]

P(z) = $z^{181} + z^5 + 3z^4 + 3z^3 + 3$ *x*=[430231143030042104122442004211031442233231212331100100323003341201344433331120310002101312011223223204122134310412131024210020010344000212342212231041402210200331004344113222024213] *y*=[220214013224431013231414442230343012344044044011300231414114122304314114433244421434202221124223200202333433331112244200141102141413131012110242032112333320144320241101012444220 32]
P(z) = $z^{181} + 2z^5 + 2z^3 + 4z + 2$ *x*=[213303120043101410430214113000223042401423430440104441233234204013241021021410012212131113130013010300034431014044244234032001424420410222124313100214302032044141310412102201001122 4] *y*=[333342223403012114404422142010023210021141130430442302023204431414313444410321233000203120022141222334233423040032120031121042103413314034213433320313204204142423432231111343131424]
P(z) = $z^{181} + 2z^5 + 2z^3 + 4z + 3$ *x*=[041004310220124400010323000323444403432134210112041043030341412422420242102402133113211112200032214301020314430023124230400401241320121003143044221313232340414001111113200242424002 4] *y*=[103300132311434420343104341031424340043124401420403234203202244214313030440040144030112014201104040324134020031112010040201101100101322211004030140442442444443041223413101210230300 2]

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

P(z) = $z^{227} + z^3 + 2z^2 + z + 2$ *x*=[200434204200342242421132330113311033122431404333242244010231330340440143341310142343240422122012144022221230022024030021341441000322330142321441233132042423021432414321221131340244221020101130123333102342434124103011001024411 2] *y*=[143314021300210304111310442344114031131013143133441204112044300113411410202331023320443333224142334442403242311333313133304320431140021013242301132431231300041404210042241140132201331324024442100212031201421440342020413001121 24]

$P(z) = z^{227} + z^3 + 3z^2 + z + 3$

x=[32022120111441122232431031402132303140404222314100233230131330211024433203113014314130344404113033202441041221121240132322400221034214041134421440442304133242320241034432414423310142023034010432303410314333344123110324133014444]

y=[00112021000033030304042014423344104401442204324420100123234211343220410234021302240342024043403011301404024011333412120213233004143221433103002232223043130244434012123110423031311012202442242303132014031113111234342422020044441]

$P(z) = z^{227} + z^4 + 2z^2 + z + 2$

x=[00130341131312012421212040140240313014202340431420010044200313404102301334141242324123210333142033414113314031314413000113222221440212004022430131433321234031143331414443402413000302044033411121214340141423243302210011124102 33]

y=[00314323301034220420433200330304332423230043240411103020101034122314222141341104433434122243404422030404334223334303034040424401041124242344400104324232112301300142220320443040141332230222013431233200332300420214144122220040011]

$P(z) = z^{227} + 2z^4 + 4z^3 + 2z + 3$

x=[04143040131323113313020330232044432241244230213432103410034144440332133244343322211040123402330342001204412122321224042112100334111230131020230020231203434301432043130111332211340014304442313402133004214343102220120140013043 12]

y=[42230343300243410212030123020242100011302124303210440141002443241020441144112034004242310442233112340411042343130421314112244031221111113214212420111422144013404042341302424143014134400303140332312122304404124120142141042421 12]

$P(z) = z^{227} + 3z^4 + 4z^3 + 2z + 2$

x=[42431120100132410101402123140402300013433034141124410421142232234430434120401121023214001134341202002213410434423032400123012013430200241103103223122442420240324142044104100240004233131420424303114010414324324130040420431221312]

y=[23232102342014112231203433413112230330443100403233204023040124003030212110124431223141434223110141130003014112014223414410344240443220114242140311242030003020022043303103223344013230202242002334432013101442113041341131031430241]

$P(z) = z^{227} + 4z^4 + 3z^2 + z + 3$

x=[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*=[02124203121121324411200224140411102320211132444243110341144403332421234003140123120411042423013102433344041411420133023011032234002004311410204030331144121303324243421324433013321002342231140131143200241114300100434123230304411]
y=[43424210212234423234101402131204120131221240003311022232424130102024343134034323320333441003124123322112414420123021202100333444011423323000043442110340122330042040310412322120443044300230112104222243003134330440302014342021402]

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полемF_7^{127}. Таблиця 4

P(z) = $z^{127} + 3z^2 + 2$ *x*=[46044006603145305201405123204222530031016222516201005661204244422522523363324113266525222005454623240563146654416124642102126 22] *y*=[13151463044055366051631435240114440055064050055036454015644623565455240161623205625064212024436215201514620643652053153153046 04]
P(z) = $z^{127} + 5z^2 + 4$ *x*=[03655433365210564341154620351326454535151161013652330566553051162552456414405421111444536306551655040562536036133665102265321 36] *y*=[13205354620266042601015444262135612041153411156022203232033334332456261531212132660656611400600631511244133355062142313264524 65]
P(z) = $z^{127} + 2z^2 + 2z + 4$ *x*=[64663156522464360424613322621061264325155146612546650340165526460656260605330601001241524365532112242546361653423243663533105 33] *y*=[05423004534624634645144346564106464142151303115465555340552214514542542415513632050154600544522051154153431552254401343230166 14]
P(z) = $z^{127} + 4z^2 + 2z + 2$ *x*=[15603613433453201456440343246134161662326116262564562611065413611640150064354520322441435430203152405222336106160316230450346

46] *y*=[22565136515404103214354614100102620424432610204434221505526520631610120103304131034135532442425021160020635604345330560532132 45]
P(z) = $z^{127} + 2z^3 + 6z^2 + 2$ *x*=[51023240025151200301513146555625112333514313425312615404624633363544464112402143231104546644562411633151664643345252622103224 22] *y*=[31454600364002230435316522200035653630653326336105534330260164362233640535132405012261153552256011436150150514123306045535553 05]
P(z) = $z^{127} + 4z^3 + 3z^2 + 4$ *x*=[03210446022155153061636044445346543554566532234021154266264643006553431621336330452354342330416321130233006510413516346512604 21] *y*=[64300456623431116662363540035340653523540016015004455565151346233035526466554026416010556405320333336331313606411310364566561 13]
P(z) = $z^{127} + 3z^5 + 2z^2 + 4$ *x*=[36055406325306300200206214002035336663512100445115122143126463204332523621131631331213106404601050301126451066240213540143631 16] *y*=[50233423240430140402550003602135502035055335033056621263204000533006200233160455153252603166106310405136105015023662236211266 16]
P(z) = $z^{127} + 6z^5 + 4z^2 + 2$ *x*=[26353632636554426243253135206500335243416466301121664533011056546414321023552562215414230302450116145060210041610544356156305 62] *y*=[40643203223163465324602451425033514603462453345412120546546124533500300436565341154401365365655613164664501220514626230031622 33]

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} 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.

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.

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. – 224с.

ПРЭ №2, 2013