CRYPTOLOGY

DOI: 10.20535/2411-1031.2018.6.1.153136
УДК [003.26+004.056.5]::512.77

ОЛЕКСАНДР ТЕЛІЖЕНКО

РОЗПОДІЛ РЕЗУЛЬТАТІВ ПОДІЛУ ТОЧКИ ГРУПИ ТОЧОК КРИВОЇ ЕДВАРДСА НА 4 ЗА СУМІЖНИМИ КЛАСАМИ

У сучасній криптології еліптичні криві в формі Едвардса (криві Едвардса) є перспективними для використання в асиметричних криптосистемах. Ці криві у порівнянні з відомими еліптичними кривими у канонічній формі мають ряд переваг, таких як швидкодія, універсальність закону додавання та наявність афінних координат нейтрального елемента (нуля) абелевої групи точок. Із симетрії точок кривих Едвардса відносно обох координатних осей випливають властивості цих кривих, які знайшли застосування в криптографії. На сьогодні криві Едвардса активно досліджуються у всьому світі, зокрема, вивчається можливість розробки нових стандартів цифрового підпису, що базуються на кривих Едвардса. Найбільш цікавими для практичного використання є криві Едвардса, у яких порядок дорівнює $4n$, де n – велике просте число. Стійкість цифрового підпису на кривих Едвардса базується на складності розв'язання задачі дискретного логарифмування у підгрупі групи точок еліптичної кривої. Саме перспектива використання кривих Едвардса для побудови нових стандартів цифрового підпису робить актуальним питання криптографічного аналізу таких криптосистем. Серед атак на криптосистеми, що базуються на задачі дискретного логарифмування, особливе місце займають спеціальні атаки, що використовують особливості самої циклічної групи, в якій розглядається ця задача. Тому при побудові такої криптосистеми необхідно дослідити структуру відповідної групи та її особливості. Однією із алгебраїчних задач, яка може бути корисною у криптографічному аналізі є представлення точок кривої Едвардса через ліві (праві) суміжні класи за підгрупами порядку 4 та максимального простого порядку n. Одним з алгоритмів криптографічного аналізу систем на кривих Едвардса є алгоритм поділу точки групи точок кривої Едвардса на чотири. Результати поділу тісно пов'язані із розбиттям групи точок кривої Едвардса за суміжними класами за підгрупами максимального простого порядку та порядку 4. Структура групи точок кривої Едвардса дозволяє однозначно визначати знаходження будь-якої точки цієї групи одночасно в двох суміжних класах за підгрупами максимального простого порядку та порядку 4. Наведений приклад розв'язання задачі дискретного логарифмування з використанням поділу точки на чотири і класифікація результатів поділу за суміжними класами для групи точок кривої Едвардса порядку 28 і 76.

Ключові слова: крива Едвардса, підгрупа, суміжний клас, циклічна група, генератор групи.

Постановка проблеми. На еліптичні криві, що використовуються для побудови алгоритму цифрового підпису, накладаються обмеження [1], щоб задача дискретного логарифмування мала лише експоненційні алгоритми розв'язку. Такі, як великий порядок поля або великий простий степінь розширення, наявність підгрупи великого простого поля, *MOV*-умова. При порушенні будь-якої з перелічених вимог цифровий підпис стає уразливим до атак. Однак, жоден з відомих типів криптографічних атак не використовує особливості структури групи точок еліптичних кривих за суміжними класами за підгрупами великого та малого порядків. Розбиття групи точок кривої Едвардса порядку $4n$ за суміжними класами має закономірності. Використовуючи алгоритм поділу точок кривої Едвардса на 4 отримуємо розміщення результатів зазначеного поділу за суміжними класами різних підгруп, що має важливе значення при розв'язанні задачі дискретного логарифмування [2].

Аналіз останніх досліджень і публікацій. Дослідження властивостей кривих Едвардса дозволяє стверджувати [2], [3], що ці криві можна використовувати для генерування цифрового підпису із достатнім на сьогодні рівнем стійкості [4] – [6]. Однак, алгоритм атаки спеціального типу, запропонований у цій роботі, направлений не на безпосередній розв'язок задачі дискретного логарифмування, а на алгоритм формування цифрового підпису. Такі алгоритми атаки нав'язування на системи цифрового підпису, що побудовані на кривих Едвардса, раніше не розглядалися.

Метою статті є розв'язання задачі дискретного логарифмування з використанням суміжних класів групи точок кривих Едвардса. Для досягнення сформованої мети виконано такі окремі завдання:

1. Навести структуру групи точок кривої Едвардса порядку $4n$ за суміжними класами.
2. Прокласифікувати точки групи точок кривої Едвардса за суміжними класами.
3. Показати зв'язок результатів поділу точки групи точок кривої Едвардса на 4 із суміжними класами.

Виклад основного матеріалу досліджень. Крива Едвардса E над простим полем F_p, де $p \neq 2$ [1] задається рівністю

$$E: x^2 + y^2 = 1 + dx^2 y^2,\ d \in F_p^*,\ d \notin Q_p, \tag{1}$$

де $x, y \in F_p$;

F_p^* – мультиплікативна група простого поля F_p;

Q_p – множина квадратичних лишків поля F_p.

На множині точок кривої Едвардса існує операція додавання, що визначається згідно з формулою:

$$\forall R, S \in E,\ R = (x_1, y_1),\ S = (x_2, y_2)$$

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

де $1 - dx_1 x_2 y_1 y_2 \neq 0,\ 1 + dx_1 x_2 y_1 y_2 \neq 0,\ \forall x_1, x_2, y_1, y_2 \in F_p^*$.

Відносно цієї операції множина E утворює циклічну групу, що породжується деякою точкою $G = (x, y) \in E,\ x, y \in F_p:\ E = < G >$. Точка G знаходиться, наприклад [6], з використанням стандартного алгоритму пошуку генератора циклічної групи.

Надалі будемо розглядати групи E порядку $4n$, де n – просте число. На практиці доцільно використовувати число n порядку $> 2^{163}$ [2].

Для будь-якої групи справедлива теорема Лагранжа [7].

Теорема 1. Нехай H – підгрупа групи E. Тоді група E розкладається на суміжні класи, що не перетинаються, за підгрупою H.

Крім того, за теоремою про властивості циклічної групи [7] в групі E існує єдина підгрупа M порядку 4 та єдина підгрупа H порядку n.

Теорема 2. Група E за суміжними класами за підгрупою максимального простого порядку H має розклад [8]:

$$E = H \cup (G + H) \cup (2G + H) \cup (3G + H), \tag{3}$$

де G – генератор групи E.

Теорема 3. Група E за суміжними класами за підгрупою M порядку 4 має розклад:

$$E = (H_1 + M) \cup (H_2 + M) ... \cup (H_n + M),$$

де $\{H_1, H_2, ..., H_n\} = H$.

Теорема 3 є наслідком теореми 1. При цьому унікальною є структура групи M порядку 4. В кожній групі точок кривої Едвардса існує чотири точки, які будемо називати точками малого порядку [6].

1. Точка $\boldsymbol{O} = (0,1)$ – єдина в групі E точка першого порядку.
2. Точка $\boldsymbol{D} = (0,–1)$ – єдина в групі E точка другого порядку.
3. Рівно дві точки четвертого порядку: $\boldsymbol{F} = (1,0)$ та $–\boldsymbol{F} = (–1,0)$.

Саме ці точки утворюють групу четвертого порядку M [6]:

$$M = \{O, D, F, -F\}.$$

Важлива властивість точок малого порядку, яка дозволяє спростити проведення криптографічного аналізу систем цифрового підпису на кривих Едвардса, полягає в особливості їх додавання до інших точок групи E згідно з формулою (2).

Якщо $P = (x, y) \in E$, то:

$$\begin{gathered}(x, y) + O = (x, y);\\ (x, y) + D = (-x, -y);\\ (x, y) + (-F) = (-y, x).\\ (x, y) + F = (y, -x)\end{gathered} \quad (4)$$

Розглянемо детальніше структуру групи точок кривої Едвардса E за суміжними класами за підгрупою M порядку 4 та підгрупою H максимального простого порядку n. Покажемо, що між точками поділу точок групи E на 4 та суміжними класами за підгрупами M та H існує взаємооднозначний зв'язок.

Теорема 4. Якщо точка G є генератором групи E, то група M має наступну структуру:

$$M = \{nG, 2nG, 3nG, 4nG\}. \quad (5)$$

Доведення: Точка D має порядок 2. Тобто $2D = O$. Точка G має порядок $4n$. Звідси випливає, що точка $2nG + 2nG = 4nG = O$. Тобто точка $2nG$ як і точка D має порядок 2. Оскільки точка порядку 2 є єдиною у групі E, то $D = 2G$.

Точки F та $-F$ мають порядок 4. Відповідно, точка nG має порядок 4: $nG + nG + nG + nG = O$ і точка $3nG$ має порядок 4: $3nG + 3nG + 3nG + 3nG = 12nG = O$. Звідси випливає, рівність множин $\{F, -F\} = \{nG, 3nG\}$.

Оскільки порядок точки G дорівнює $4n$, то відповідно маємо, що $O = 4nG$.

Теорему доведено.

Означення 1. Визначимо, що точка $P \in E$ є результатом поділу точки $Q \in E$ на 4, якщо $4P = Q$. Відповідно, визначимо, що точка Q ділиться на 4.

Теорема 5. Якщо точка $Q \in E$, $|E| = 4n$, де n – просте число, ділиться на 4, то результати поділу точки Q утворюють суміжний клас за підгрупою M порядку 4.

Доведення: Група точок кривої Едвардса є абелевою і циклічною, тобто $E = < G >$. Оскільки порядок групи точок кривої Едвардса дорівнює $4n$, то в цій групі існує єдина підгрупа H максимального простого порядку n та єдина підгрупа M порядку 4. Підгрупа H також є циклічною як підгрупа циклічної групи, тобто існує точка P, така, що $H = <P>$. Оскільки H має порядок n, то $H = \{P, 2P, \ldots, nP\}$. Оскільки E – циклічна група маємо, що $P = 4G$. Тобто $H = \{4G, 8G, ...4nG\}$. Звідси випливає, що точка $Q \in E$ ділиться на 4, тоді і тільки тоді, коли вона належить підгрупі H, а саме – це буде точка виду $4kG$, $k \in \{1, ..., n\}$. При цьому результатом поділу точки на чотири будуть 4 точки групи E, а саме:

$$T_k = \{kG, kG + nG, kG + 2nG, kG + 3nG\},\ k \in \{1, ..., n\}. \quad (6)$$

Підгрупа M групи E порядку 4 є єдиною та циклічною як підгрупа циклічної групи, і має структуру визначену в (5). Тоді з (1) випливає, що множини T_k будуть суміжними класами за підгрупою M.

Теорему доведено.

Приклад 1. Розглянемо криву Едвардса над полем $GF(17)$ з параметром $d = 8$. Порядок кривої у цьому випадку буде $28 = 4 \cdot 7$.

Використаємо як генератор групи точок кривої Едвардса точку $P = (2,9)$. Запишемо групу E у вигляді таблиці:

Таблиця 1 – Точки групи точок кривої Едвардса E,
що породжені генератором $P=(2,9)$

	O	P	$2P$	$3P$	$4P$	$5P$	$6P$
x	1	2	–8	–3	–5	–4	–9
y	0	9	4	5	3	8	2
	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$
x	0	9	4	5	3	8	–2
y	–1	–2	8	3	5	4	9
	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$
x	–1	–2	8	3	5	4	9
y	0	-9	–4	–5	–3	–8	2
	$21P$	$22P$	$23P$	$24P$	$25P$	$26P$	$27P$
x	0	–9	–4	–5	–3	–8	2
y	1	–2	–8	–3	–5	–4	–9

Підгрупа максимального порядку H для наведеного прикладу буде:

$$H=\{H_1,H_2,H_3,H_4,H_5,H_6,O\}=\{4P,8P,12P,16P,20P,24P,O\}.$$

Тобто

$$H=\{(-5,3),(9,-2),(8,4),(8,-4),(9,2),(-5,-3),(1,0)\}.$$

За цією підгрупою існує 4 класи суміжності (3):

$$H,G+H,2G+H,3G+H,$$

де G – генератор групи E.

Використаємо як генератор групи точку $G=11P=(3,5)$.

За цим генератором маємо 4 суміжні класи за підгрупою H:

$$H=\{4P,8P,12P,16P,20P,24P,O\}=\{(-5,3),(9,-2),(8,4),(8,-4),(9,2),(-5,-3),O\},$$

$$G+H=\{15P,19P,23P,27P,3P,7P,11P\}=$$

$$=\{(-2,-9),(4,-8),(-4,-8),(2,-9),(-3,5),(0,-1),(3,5)\},$$

$$2G+H=\{26P,2P,6P,10P,14P,18P,22P\}=$$

$$=\{(-8,-4),(-8,4),(-9,2),(5,3),(-1,0),(5,-3),(-9,-2)\},$$

$$3G+H=\{9P,13P,17P,21P,25P,P,5P\}=$$

$$=\{(4,8),(-2,9),(3,-5),(0,1),(-3,-5),(2,9),(-4,8)\}.$$

Також маємо 7 суміжних класів за підгрупою M:

$$M=\{7P,14P,21P,O\}=\{(0,-1),(-1,0),(0,1),(1,0)\},$$

$$H_1+M=\{11P,18P,25P,4P\}=\{(3,5),(5,-3),(-3,-5),(-5,3)\},$$

$$H_2+M=\{15P,22P,P,8P\}=\{(-2,-9),(-9,-2),(2,9),(9,-2)\},$$

$$H_3+M=\{19P,26P,5P,12P\}=\{(4,-8),(-8,-4),(-4,8),(8,4)\},$$

$$H_4+M=\{23P,2P,9P,16P\}=\{(-4,-8),(-8,4),(4,8),(8,-4)\},$$

$$H_5+M=\{27P,6P,13P,20P\}=\{(2,-9),(-9,2),(-2,9),(9,2)\},$$

$$H_6+M=\{3P,10P,17P,24P\}=\{(-3,5),(5,3),(3,-5),(-5,-3)\}.$$

З (4) випливає, що кожен із суміжних класів за підгрупою M складається з точок $\{(x,y),(-x,-y),(y,-x),(-y,x)\}$, де $(x,y)\in H$. І, відповідно, у кожному суміжному класі є точка, що ділиться на 4.

Розглянемо результати поділу точок підгрупи максимального простого порядку H на чотири.

Маємо розподіл результатів поділу за суміжними класами за підгрупою M:

$$H_1/4=\{P,8P,15P,22P\}=H_2+M,\ 4P/4=8P+M,$$

$$H_2/4=\{2P,9P,16P,23P\}=H_4+M,\ 8P/4=16P+M,$$

$$H_3/4=\{3P,10P,17P,24P\}=H_6+M,\ 12P/4=24P+M,$$
$$H_4/4=\{4P,11P,18P,25P\}=H_1+M,\ 16P/4=4P+M,$$
$$H_5/4=\{5P,12P,19P,26P\}=H_3+M,\ 20P/4=12P+M,$$
$$H_6/4=\{6P,13P,20P,27P\}=H_5+M,\ 24P/4=20P+M.$$

Тобто, $4kP/4=8kP+M$, де $k=\overline{1,6}$. Результатом поділу точки $4kP$ на 4 буде суміжний клас за елементом подвоєної точки $8kP$ за підгрупою M.

Водночас маємо, що точки $H_1/4=\{P,8P,15P,22P\}$ належать різним суміжним класам за підгрупами групи H: $P\in 3G+H$, $8P\in H$, $15P\in G+H$, $22P\in 2G+H$.

Точки $H_2/4=\{2P,9P,16P,23P\}$ – $2P\in 2G+H$, $9P\in 3G+H$, $16P\in H$, $23P\in G+H$.

Точки $H_3/4=\{3P,10P,17P,24P\}$ – $3P\in G+H$, $10P\in 2G+H$, $17P\in 3G+H$, $24P\in H$.

Точки $H_4/4=\{4P,11P,18P,25P\}$ – $4P\in H$, $11P\in G+H$, $18P\in 2G+H$, $25P\in 3G+H$.

Точки $H_5/4=\{5P,12P,19P,26P\}$ – $5P\in 3G+H$, $12P\in H$, $19P\in G+H$, $26P\in 2G+H$.

Точки $H_6/4=\{6P,13P,20P,27P\}$ – $6P\in 2G+H$, $13P\in 3G+H$, $20P\in H$, $27P\in G+H$.

Узагальнюючи отримані результати можна провести класифікацію групи точок кривої Едвардса порядку 4n за суміжними класами за підгрупами M та H.

Таблиця 2 – Точки групи точок кривої Едвардса E порядку 4n за суміжними класами за підгрупами M та H

	$H+nP$	$H+2nP$	$H+3nP$	H
M	nP	$2nP$	$3nP$	O
$M+4P$	$nP+4P$	$2nP+4P$	$3nP+4P$	$4P$
$M+8P$	$nP+8P$	$2nP+8P$	$3nP+8P$	$8P$
…	…	…	…	…
$M+4(n-1)P$	$nP+4(n-1)P$	$2nP+4(n-1)P$	$3nP+4(n-1)P$	$(n-1)P$

Приклад 2. Структура групи точок кривої Едвардса порядку n=76=19·4.

Таблиця 3 – Точки групи точок кривої Едвардса порядку 76 за суміжними класами за підгрупами порядку 4 та порядку 19

	1H	2H	3H	4H
1M	19P	38P	57P	O
2M	***23P***	***42P***	***61P***	***4P***
3M	27P	46P	65P	8P
4M	31P	50P	69P	12P
5M	***35P***	***54P***	***73P***	***16P***
6M	**39P**	**58P**	**P**	**20P**
7M	***43P***	***62P***	***5P***	***24P***
8M	***47P***	***66P***	***9P***	***28P***
9M	51P	70P	13P	32P
10M	***55P***	***74P***	***17P***	***36P***
11M	59P	2P	21P	40P
12M	***63P***	***6P***	***25P***	***44P***
13M	67P	10P	29P	48P

Продовження таблиці 3

14M	71P	14P	33P	52P
15M	75P	18P	37P	56P
16M	3P	22P	41P	60P
17M	***7P***	***26P***	***45P***	***64P***
18M	***11P***	***30P***	***49P***	***68P***
19M	15P	34P	53P	72P

У табл. 3 у стовпцях представлено суміжні класи iH, i=1,…4 за підгрупою порядку 19, а в рядках – суміжні класи jM, j=1,…,19 за підгрупою порядку 4. Генератор групи E потрапив у суміжні класи відповідно $3H$ та $6M$. Результат поділу точки групи E на 4, а це може бути тільки точка з групи H утворює один з суміжних класів jM. Таким чином потрапити до суміжного класу, що містить точку P шляхом поділу точки на 4 можна тільки з суміжних класів $2M$, $5M$, $7M$, $8M$, $10M$, $12M$, $17M$, $18M$. Разом із суміжним класом $6M$, де знаходиться точка P – це рівно половина суміжних класів без підгрупи M.

Наприклад, якщо треба з точки $49P$ потрапити у суміжний клас, де знаходиться точка P шляхом поділу точки на 4:

1. Точка $49P$ належить до класу $18M$. Знаходимо у цьому класі точку, що ділиться на 4. Це $68P$.
2. Після поділу на 4 точка $68P$ утворює суміжний клас $10M$. У цьому суміжному класі точка, що ділиться на 4 буде $36P$.
3. Після поділу на 4 точка $36P$ утворює суміжний клас $8M$. У цьому суміжному класі точка, що ділиться на 4 буде $28P$.
4. Після поділу на 4 точка $28P$ утворює суміжний клас $17M$. У цьому суміжному класі точка, що ділиться на 4 буде $64P$.
5. Після поділу на 4 точка $64P$ утворює суміжний клас $5M$. У цьому суміжному класі точка, що ділиться на 4 буде $16P$.
6. Після поділу на 4 точка $16P$ утворює суміжний клас $2M$. У цьому суміжному класі точка, що ділиться на 4 буде $4P$.
7. Після поділу на 4 точка $4P$ нарешті утворює суміжний клас $6M$.

У таблиці 3 за стовпцями суміжні класи за підгрупою H, а за рядками суміжні класи за підгрупою M.

З точки $49P$ можна потрапити до суміжного класу $6M$ шляхом множення точки на 4:

1. $49P \cdot 4 = 44P$. Потрапляємо до суміжного класу $12M$.
2. $44P \cdot 4 = 24P$. Потрапляємо до суміжного класу $7M$.
3. $24P \cdot 4 = 20P$. Потрапляємо до шуканого суміжного класу.

Структура суміжного класу $6M$ має наступну структуру: P, $P+nP$, $P+2nP$, $P+3nP$. Або якщо точка $P = (x,y)$, то інші точки суміжного класу будуть мати вид: $(-x, -y)$, $(y, -x)$, $(-y,x)$. Таким чином, потрапляючи до будь-якого суміжного класу jM можемо легко перевірити чи знаходиться в ньому точка P.

Висновки. Структура групи точок кривої Едвардса має важливе значення для визначення в якому суміжному класі за підгрупами порядку 4 та максимального простого порядку n одночасно знаходяться точки, що використовуються при формуванні цифрового підпису. У кожному суміжному класі за підгрупою порядку 4 існує точка, що ділиться на 4 та знаходиться одночасно також і у підгрупі максимального простого порядку n. Доведено, що розподіл точок кривої Едвардса після поділу точки на 4 за суміжними класами має специфічну структуру і представляє собою суміжний клас за підгрупою порядку 4. Показано на прикладах груп порядку 28 і 76 як ця властивість використовується для проведення криптографічного аналізу систем на кривих Едвардса. Отриманий теоретичний результат дозволяє в подальшому запропонувати спеціальний алгоритм розв’язку задачі дискретного логарифмування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Державний стандарт України. *ДСТУ 4145. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння*. Київ, Україна: Держстандарт України, 2003.

[2] А. В. Бессалов, *Эллиптические кривые в форме Эдвардса и криптография*. Киев, Україна: Политехника, 2017.

[3] H. M. Edwards, "A normal form for elliptic curves", *Bulletin of the American Mathematical Society*, vol. 44, no. 3, pp. 393-422, 2007.
doi: 10.1090/S0273-0979-07-01153-6.

[4] D. Bernstein, and T. Lange, "Faster addition and doubling on elliptic curves". in *Proc. International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, 2007, pp. 1-20.
doi: 10.1007/978-3-540-76900-2_3.

[5] А. Бессалов, А. Дихтенко, и Д. Третьяков, "Оценка реальной стойкости криптосистемы на кривой Эдвардса над расширениями малых полей", *Сучасний захист інформації*, № 2, с. 17-20, 2012.

[6] А. В. Бессалов, и А. А. Дихтенко, "Криптостойкие кривые Эдвардса над простыми полями", *Прикладная радиоэлектроника*, т. 12, № 2, с. 285-291, 2013.

[7] М. М. Глухов, В. П. Елизаров, и А. А. Нечаев, *Алгебра*. Москва, Российская Федерация: Гелиос-АРВ, 2003.

[8] Л. Ковальчук, А. Бессалов, та О. Беспалов, "Порівняний аналіз алгоритмів генерації базової точки на кривій Эдвардса", на *XVII Міжнародної науково-практичної конференції "Безпека інформації у інформаційно-телекомунікаційних системах"*, Київ, 2015, с. 32-33.

[9] О. Б. Теліженко, "Структура групи точок кривої Едвардса, що не містить точок восьмого порядку", *Математичне та комп'ютерне моделювання*, вип. 15, с. 239-243, 2017.

Стаття надійшла до редакції 04 березня 2018 року.

REFERENCE

[1] State standard of Ukraine. *DSTU 4145-2002. Information technologies. Cryptographic defence of information. Digital signature which is based on elliptic curves. Forming and verification*. Kyiv, Ukraine: State standard of Ukraine, 2003.

[2] A. V. Bessalov, *Elliptic curve in Edvards form and cryptography*. Kyiv, Ukraine: Politechnika, 2017.

[3] H. M. Edwards, "A normal form for elliptic curves", *Bulletin of the American Mathematical Society*, vol. 44, no. 3, pp. 393-422, 2007.
doi: 10.1090/S0273-0979-07-01153-6.

[4] D. Bernstein, and T. Lange, "Faster addition and doubling on elliptic curves". in *Proc. International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, 2007, pp. 1-20.
doi: 10.1007/978-3-540-76900-2_3.

[5] A. Bessalov, A. Dichtenko, and D. Tretiakov, "Estimate of real resistance of cryptosystem on Edwards curve over finite fields of small extension", *Modern information protection*, no. 2, pp. 17-20, 2012.

[6] A. V. Bessalov, and A. A. Dikhtenko, "Crypto resistant Edwards elliptic curves over finite fields", *Applied radioelectronics*, vol. 12, no. 2, pp. 285-291, 2013.

[7] M. M. Glukchov, V. P. Yelizarov, and A. A. Nechayev, *Algebra*. Moscow, Russia: Gelios-ARV, 2003.

[8] L. Kovalchuk, A. Bessalov, and O. Bespalov, “Comparative analysis of base point generation algorithms on Edwards curve”, in *Proc. XVII International conference “Information protection in information-telecommunication systems”*, Kyiv, 2015, pp. 32-33.
[9] O.B. Telizhenko, “Group structure of Edwards elliptic curve without points of order 8”, *Mathematical and computer modeling*, iss. 15, pp. 239-243, 2017.

АЛЕКСАНДР ТЕЛИЖЕНКО

РАСПРЕДЕЛЕНИЕ РЕЗУЛЬТАТОВ ДЕЛЕНИЯ ТОЧКИ ГРУППЫ ТОЧЕК КРИВОЙ ЭДВАРДСА НА 4 ПО СМЕЖНЫМ КЛАССАМ

В современной криптологии эллиптические кривые в форме Эдвардса (кривые Эдвардса) являются перспективными для использования в асимметричных криптосистемах. Эти кривые по сравнению с известными эллиптическими кривыми в канонической форме имеют ряд преимуществ, таких как быстродействие, универсальность закона сложения и наличие аффинных координат нейтрального элемента (нуля) абелевой групы точек. Из симметрии точек кривых Эдвардса относительно обоих координатных осей следуют свойства этих кривых, которые нашли применение в криптографии. На сегодня кривые Эдвардса активно исследуются во всем мире, в частности, изучается возможность разработки новых стандартов цифровой подписи, основанной на кривых Эдвардса. Наиболее интересными для практического использования являются кривые Эдвардса, у которых порядок равен $4n$, где n – большое простое число. Стойкость цифровой подписи на кривых Эдвардса основана на сложности решения задачи дискретного логарифмирования в подгруппе группы точек эллиптической кривой. Именно перспектива использования кривых Эдвардса для построения новых стандартов цифровой подписи делает актуальным вопрос криптографического анализа таких криптосистем. Среди атак на криптосистеми, основанных на задаче дискретного логарифмирования, особое место занимают специальные атаки, которые используют особенности самой циклической группы, в которой рассматривается эта задача. Поэтому при построении такой криптосистеми необходимо изучить структуру соответствующей группы и ее особенности. Одной из алгебраических задач, которая может быть полезной в криптографическом анализе является представление точек кривой Эдвардса через левые (правые) смежные классы по подгруппам порядка 4 и максимального простого порядка. Одним из алгоритмов криптографического анализа систем на кривых Эдвардса является алгоритм деления точки группы точек кривой Эдвардса на четыре. Результаты деления тесно связаны с разбиением группы точек кривой Эдвардса по смежным классам по подгруппам максимального простого порядка и порядка 4. Структура группы точек кривой Эдвардса позволяет однозначно определить местонахождение любой точки этой группы одновременно в двух смежных классах по подгруппам максимального простого порядка и порядка 4. Приведен пример решения задачи дискретного логарифмирования с использованием деления точки на четыре и классификация результатов деления по смежным классам для групп точек кривой Эдвардса порядка 28 и 76.

Ключевые слова: кривая Эдвардса, подгруппа, смежный класс, циклическая группа, генератор группы.

OLEKSANDR TELIZHENKO

DISTRIBUTING OF POINT DIVISION ON 4 RESULTS OFEDWARDS CURVE POINTS GROUP TO ADJACEMENT CLASSES

Elliptic curves in Edwards form are perspective for usage in modern asymmetric cryptosystems. Such curves have a series of advantages in compare with elliptic curves in canonical form, such as speed of addition, universality of addition law, existence of affine coordinates for neutral element of group of points. The fact that Edwards curves are symmetric in both variables involves some properties of such curves that are used in cryptogogy. These days Edwards curves

are actively investigates all over the world, for instance, the possibility is investigated to design new digital signature standards on Edwards curves. The most interesting for practical usage are Edwards curves which orders are equal to $4n$, where n is large prime number. The security of digital signature on Edwards curves is based on complication of DLP (Discrete logarithm problem) in subgroup of Edwards curve points. The usage of Edwards curve for new digital signature standards stipulates the actuality of cryptanalysis of such cryptosystems. The important place among attacks on DLP-based cryptosystems take special attacks that use the features of the cyclic group in which the DLP problem is considered. Because of this it is necessary to investigate the structure of the cyclic group and its features for cryptanalysis of such systems. One of the algebraic tasks which may be useful in cryptanalysis is representation of Edwards curve points by the pair of left (right) adjacent classes by subgroups of the order 4 and of the maximal prime order n. One of the algorithms for cryptographic analysis of the Edwards curve cryptosystems is the division of point of Edwards curve by four. Division results are tightly connected with the split of point groups of Edward curve by adjacent classes of subgoups of maximum prime order and of the order 4. Structure of the Edwards curve points group allows to determine definitively position of any point of this group, simultaneously in two adjacent classes of subgroups of maximum prime order or fourth order. Example is given of discrete logarithmic problem solution using division of point by four and classification of results of division by adjacent classes for point groups of Edwards curve of order twenty eight and seventy six.

Keywords: Edwards curve, subgroup, adjacent class, cyclic group, generator of group.

Олександр Борисович Теліженко, консультант, ООО “Verum Visum”, Київ, Україна.
ORCID: 0000-0002-5335-5767
E-mail: tel63@ukr.net.

Александр Борисович Телиженко, консультант, ООО Verum Visum, Киев, Украина.

Oleksandr Telizhenko, consultant, OOO Verum Visum, Kyiv, Ukraine.