УДК 681.3.06

КРИВА ЕДВАРДСА НАД КІЛЬЦЕМ ЛИШКІВ ЯК ДЕКАРТІВ ДОБУТОК КРИВИХ ЕДВАРДСА НАД СКІНЧЕНИМИ ПОЛЯМИ

О. Ю. БЕСПАЛОВ, Н. В. КУЧИНСЬКА

Розглядається крива, що є узагальненням кривої Едвардса над кільцем лишків; показано, що за певних умов множина її точок утворює групу відносно визначеної операції; ця група ізоморфна декартовому добутку відповідних кривих Едвардса над скінченими полями.

Ключові слова: еліптичні криві, еліптичні криві Едвардса, криптосистеми на еліптичних кривих, група точок еліптичної кривої.

ВСТУП

Еліптичні криві над кільцем лишків Z_n є цікавим об'єктом як з точки зору криптології, так і з точки зору алгебри. Особливістю таких кривих є подвійна можливість їх використання: як для побудови RSA-подібних криптосистем [1, 2], так і для криптоаналізу класичних криптосистем, що базуються на важкорозв'язуваності задачі факторизації, таких як криптосистеми RSA та Рабіна [3,4].

Вперше RSA-подібні еліптичні алгоритми були запропоновані у роботі [1], після чого тема продовжувала активно обговорюватися як у напрямку удосконалення таких криптосистем, наприклад, [2], так і у напрямку їх криптоаналізу [5,6]. Також вдосконалювались і алгоритми факторизації на еліптичних кривих, наприклад, [7,8].

Що стосується RSA-подібних криптосистем на еліптичних кривих, то їх основними перевагами є такі:

- для побудови такої криптосистеми можна використовувати еліптичні криві з довільними параметрами;
- можна будувати як алгоритми шифрування, так і цифрового підпису;
- можна будувати цифрові підписи довільної довжини, зокрема такої довжини, як і повідомлення;
- на відміну від класичної криптосистеми RSA, її еліптичний аналог є стійким до атаки гомоморфізмів;
- інструментарій, що використовується в ході побудови цих криптосистем, може бути використаний для побудови еліптичних аналогів ρ-методу Поларда.

З появою в 2007 році такої форми подання еліптичних кривих, як форма Едвардса [9–11], визначення закону точок додавання такої кривої та доведення ізоморфізму з кривою у формі Вейєрштрасса, було виявлено перспективність її застосування в криптографії. Особливими перевагами еліптичних кривих у формі Едвардса є:

- наявність одного параметра замість двох для кривої у формі Вайєрштрасса;
- відсутність точки на нескінченності, оскільки як нейтральний елемент групи точок кривої Едвардса використовується точка кривої зі скінченими координатами;
- вища швидкість виконання операції додавання та подвоєння точок порівняно з аналогічними операціями для кривих у формі Вайєрштрасса;
- однаковий закон додавання та подвоєння точок кривої, що унеможливлює проведення таймінгової та ємнісної атаки для відновлення бітового запису скаляру.

Тому природним є питання можливості застосування еліптичних кривих Едвардса у зазначених вище напрямках замість класичних еліптичних кривих у формі Вейєрштраса. При цьому слід зазначити, що перенесення криптосистем і методів з еліптичних кривих у формі Вейєрштраса на еліптичні криві у формі Едвардса не є тривіальним.

1. ОСНОВНІ РЕЗУЛЬТАТИ

Під час дослідження узагальнення кривої Едвардса над кільцями лишків Z_n виявилась ще одна її цікава властивість, яку також можна віднести до переваг кривої у формі Едвардса порівняно з кривою у формі Вейєрштрасса. Ця властивість полягає у тому, що, за певних умов, крива Едвардса над кільцем Z_n, де $n = p \cdot q$ (p, q – різні прості числа), утворює групу відносно "стандартної" операції додавання точок. Далі, ця група є ізоморфною декартовому добутку груп, утворених точками відповідних кривих Едвардса над полями F_p та F_q.

Властивості кривих Едвардса над простими полями досить добре вивчені, і, внаслідок зазначеного ізоморфізму, відповідні результати можна використати під час дослідження властивостей таких кривих над кільцями.

Зазначимо, що аналогічний ізоморфізм для кривих у формі Вайєрштрасса побудувати неможливо, внаслідок існування так званої "нескінченно віддаленої точки" кривої, в якої не існує афінних координат.

Результати цієї роботи саме і стосуються побудови ізоморфізму між зазначеними групами точок кри-

вих Едвардса. Ці результати можна застосовувати як для побудови відповідних криптосистем, так і для побудови аналогів методу Лєнстра [7].

Нехай $n \in Z$. Позначимо через $Q_n = \left\{ x \in Z_n^* \mid \exists y \in Z_n^* : x \equiv y (\mathrm{mod}\, n) \right\}$ множину всіх квадратичних лишків за модулем n і $\tilde{Q}_n = \left\{ x \in Z_n^* \mid x \notin Q_n \wedge \left(\frac{x}{n} \right) = 1) \right\}$ множину всіх псевдоквадратів за модулем n. Зазначимо, що якщо $n = p \cdot q$, де p, q – різні прості числа, то

$$\forall x \in Q_n \cup \tilde{Q}_n : \left(\frac{x}{n} \right) = \left(\frac{x}{p} \right) \left(\frac{x}{q} \right) = 1,$$

$$\forall x \notin Q_n \cup \tilde{Q}_n : \left(\frac{x}{n} \right) = -1.$$

Для будь-яких $n \in Z$ та $d \in Z_n^*$ позначимо

$$E_n = \left\{ (x, y) \in Z_n \times Z_n \mid x^2 + y^2 = 1 + dx^2 y^2) \right\}, \quad (1)$$

де операції додавання та множення виконуються за модулем n.

Якщо n – просте число, $d \in Z_n^* \setminus Q_n$, тоді (1) задає деяку криву Едвардса над простим скінченним полем F_n. Але в даній статті розглянемо більш загальний випадок – коли n є добутком двох різних простих чисел. Тому надалі p, q – різні прості числа, $n = p \cdot q$.

Мета даної роботи полягає в тому, щоб звести дослідження кривої E_n, визначеної в (1), до більш відомих та досліджених об'єктів – кривих Едвардса E_p та E_q над простими скінченими полями F_p та F_q, відповідно.

В цій роботі розглянемо найпростіший випадок, коли крива E_n не містить «особливих» точок (тобто точок з нескінченими координатами). Такі криві, згідно з [12], називатимемо повними кривими Едвардса. Авторами роботи буде показано, що в такому випадку E_n утворює групу відносно деякої операції додавання її точок та, більше того, ця група ізоморфна декартовому добутку груп, утвореному кривими Едвардса E_p та E_q.

На множині E_n, визначеній у (1), задамо операцію, яка співпадає зі стандартною операцією додавання точок кривої Едвардса [12], а саме

$$\forall (x_1, y_1), (x_2, y_2) \in E_n : (x_1, y_1) + (x_2, y_2) = (x_3, y_3),$$

де

$$x_3 = \frac{x_1 x_2 - y_1 y_2}{1 - d x_1 x_2 y_1 y_2}, \; y_3 = \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}. \quad (2)$$

Це так званий «модифікований універсальний закон додавання», визначений у [12]. Тут під операціями додавання та множення розуміємо відповідні операції за модулем n, а під операцією ділення – множення на обернений елемент за модулем n.

Сформулюємо відповідні результати у вигляді наступних лем, які доводять, що операція (2) задана коректно.

Для кривої E_n, визначеної в (1) та простого p, $p \mid n$, визначимо множину $\left(E_n\right) \mathrm{mod}\, p$, що є підмножиною $Z_p \times Z_p$, за таким правилом:

$$\left(E_n\right) \mathrm{mod}\, p = \left\{ \left(x \,\mathrm{mod}\, p, y \,\mathrm{mod}\, p \right) \mid (x, y) \in E_n \right\}. \quad (3)$$

Аналогічно, для кожної точки $P = (x, y) \in E_n$ визначимо точку

$$P \,\mathrm{mod}\, p = \left(x \,\mathrm{mod}\, p, y \,\mathrm{mod}\, p \right). \quad (4)$$

Лема 1. Множина $\left(E_n\right) \mathrm{mod}\, p$, визначена згідно з (3), співпадає з множиною точок еліптичної кривої E_p, визначеною в (1), де замість параметра d використовується $d \,\mathrm{mod}\, p$.

Доведення. Нехай $P = (x, y) \in E_n$, тоді $P \,\mathrm{mod}\, p \in \left(E_n\right) \mathrm{mod}\, p$.

Покажемо, що $P \,\mathrm{mod}\, p \in E_p$. Для цього достатньо довести, що для її координат $\left(x \,\mathrm{mod}\, p, y \,\mathrm{mod}\, p \right)$ виконується рівність (1):

$$\left(x \,\mathrm{mod}\, p \right)^2 + \left(y \,\mathrm{mod}\, p \right)^2 =$$

$$= 1 + \left(d \,\mathrm{mod}\, p \right) \left(x \,\mathrm{mod}\, p \right)^2 \left(y \,\mathrm{mod}\, p \right)^2, \quad (5)$$

де всі операції у лівій та правій частині виконуються за модулем числа p.

Оскільки $P = (x, y) \in E_n$, то відповідно до (1), виконується конгруенція

$$x^2 + y^2 = 1 + dx^2 y^2 \left(\mathrm{mod}\, n \right). \quad (6)$$

Але, оскільки $p \mid n$, то за властивістю конгруенцій [13,14]

$$x^2 + y^2 = 1 + dx^2 y^2 \left(\mathrm{mod}\, p \right),$$

що еквівалентно виконанню рівності (5), звідки і отримаємо $P \,\mathrm{mod}\, p \in E_p$.

Нехай тепер деяка точка $P' = (x', y') \in E_p$, тобто

$$\left(x' \right)^2 + \left(y' \right)^2 = 1 + \left(d \,\mathrm{mod}\, p \right) \left(x' \right)^2 \left(y' \right)^2 \left(\mathrm{mod}\, p \right). \quad (7)$$

Покажемо, що $P' \in E_n \bmod p$, тобто що

$$\exists P = (x, y) \in E_n : \begin{cases} x \bmod p = x'; \\ y \bmod p = y'. \end{cases}$$

Визначимо криву E_q згідно з (1) з параметром $d \pmod q$ та виберемо на ній довільну точку $P'' = (x'', y'') \in E_q$. Тоді для координат цієї точки виконується рівність

$$(x'')^2 + (y'')^2 = 1 + (d \bmod q)(x'')^2 (y'')^2, \quad (8)$$

де всі операції виконуються за $\bmod q$.

Тепер визначимо точку $P = (x, y)$ з таких умов:

$$\begin{cases} x = x' \pmod p; \\ x = x'' \pmod q, \end{cases} \qquad \begin{cases} y = y' \pmod p; \\ y = y'' \pmod q. \end{cases} \quad (9)$$

Для завершення доведення достатньо показати, що $P = (x, y) \in E_n$, тобто що для (x, y) виконується рівність (1).

Дійсно, з рівностей (7) та (8) отримуємо:

$$\begin{cases} x^2 + y^2 = 1 + dx^2 y^2 \pmod p; \\ x^2 + y^2 = 1 + dx^2 y^2 \pmod q, \end{cases}$$

звідки, за властивостями конгруенцій та, враховуючи, що НСД$(p, q) = 1$, отримаємо

$$x^2 + y^2 = 1 + dx^2 y^2 \pmod n,$$

тобто $P = (x, y) \in E_n$. Крім того, згідно з (9), $P \bmod p = (x \bmod p, y \bmod p) = P' = (x', y')$ і лему доведено.

Наступна Лема доводить, що за умови $d \in \tilde{Q}_n$ крива E_n не має особливих точок та операція на ній задана коректно.

Лема 2. Нехай $P = (x_1, y_1), Q = (x_2, y_2) \in E_n$, $n = p \cdot q$, де p, q - прості, $d \in \tilde{Q}_n$. Тоді:

1) $dx_1 x_2 y_1 y_2 \neq \pm 1 (\bmod n)$; (10)

2) множина E_n, задана співвідношенням (1), замкнена відносно операції, визначеної в (2).

Доведення. 1) Спершу зазначимо, що якщо $d \in \tilde{Q}_n$, то $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) = -1$. Дійсно, оскільки $d \in \tilde{Q}_n$, то $\left(\frac{d}{n}\right) = 1$, звідки $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right)$. Але при цьому рівність $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) = 1$ не може виконуватися, оскільки $d \notin Q_n$. Тому $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) = -1$.

У цьому випадку, очевидно, $d \bmod p \notin Q_p$, $d \bmod q \notin Q_q$, а, отже, згідно з [12]

$$\begin{cases} dx_1 x_2 y_1 y_2 \bmod p \neq \pm 1, \\ dx_1 x_2 y_1 y_2 \bmod q \neq \pm 1. \end{cases} \quad (11)$$

Доведемо, від супротивного, що тоді виконується і умова (10). Припустимо, що (10) не виконується. Тоді $\exists\, x_1, x_2, y_1, y_2$ такі, що $(x_1, y_1), (x_2, y_2) \in E_n$ та

$$dx_1 x_2 y_1 y_2 \equiv 1 (\bmod n) \text{ або } dx_1 x_2 y_1 y_2 \equiv -1 (\bmod n). \quad (12)$$

Але в цьому випадку виконуватиметься також одна з рівностей

$$(d \bmod p)(x_1 \bmod p)(x_2 \bmod p)(y_1 \bmod p)(y_2 \bmod p) \equiv$$

$$\equiv 1 (\bmod p)$$

або

$$(d \bmod p)(x_1 \bmod p)(x_2 \bmod p)(y_1 \bmod p)(y_2 \bmod p) \equiv$$

$$\equiv -1 (\bmod p). \quad (13)$$

За лемою 1, це, зокрема, означає, що на кривій E_p, яка задається згідно з (2) з параметром $d \bmod p$, існують такі точки $P = (x_1 \bmod p, y_1 \bmod p)$ та $Q = (x_2 \bmod p, y_2 \bmod p)$, для координат яких виконується одна з рівностей (13). Але, оскільки $d \in \tilde{Q}_n$, то як було зазначено раніше, $\left(\frac{d \bmod p}{p}\right) = \left(\frac{d}{p}\right) = -1$, і згідно з [12] існування точок P та Q, для координат яких виконується (13) у цьому випадку неможливе. Оскільки прийшли до суперечності, то перше твердження леми доведено.

2) Оскільки за умови $d \in \tilde{Q}_n$ криві Едвардса E_p та E_q, визначені відповідно до (1) з параметрами $d \bmod p$ та $d \bmod q$, утворюють групи (без особливих точок) відносно відповідних операцій, то їх декартовий добуток $E_p \times E_q$ з компонентними операціями є групою.

У пункті 1) цієї леми було показано, що вирази (2) є коректними у сенсі, що їх знаменники не перетворюються в 0. Тепер покажемо, що результатом операції (2) також є точка кривої E_n.

Нехай P, $Q \in E_n$. $P = (x_1, y_1)$ та $Q = (x_2, y_2)$. Позначимо, $Z = P + Q = (x_3, y_3)$, де x_3, y_3 визначено згідно з (3). Потрібно довести, що $Z \in E_n$, тобто, що для її координат (x_3, y_3) виконується рівняння (1).

Розглянемо відповідні точки

$$P_p = P \bmod p, \; Q_p = Q \bmod p,$$

$$P_q = P \bmod q\,,\quad Q_q = Q \bmod q\,.$$

За лемою 1, $P_p, Q_p \in E_p$ та $P_q, Q_q \in E_q$, де криві E_p та E_q задаються згідно з (1) з параметрами $d \bmod p$ та $d \bmod q$, відповідно.

За властивостями конгруенцій та за лемою 1,

$$P_p + Q_p = Z \bmod p = Z_p \in E_p\,,$$

$$P_q + Q_q = Z \bmod q = Z_q \in E_q\,.$$

Отже, для координат точок Z_p та Z_q виконується рівняння (1) з параметрами $d \bmod p$ та $d \bmod q$, відповідно. Але для їх координат також виконуються конгруенції

$$\begin{cases} x_3 \equiv x_3 \bmod p \pmod p; \\ y_3 \equiv y_3 \bmod p \pmod p; \\ x_3 \equiv x_3 \bmod q \pmod q; \\ y_3 \equiv y_3 \bmod q \pmod q; \\ d \equiv d \bmod p \pmod p; \\ d \equiv d \bmod q \pmod q. \end{cases}$$

Тому, за властивостями конгруенцій, також виконуватимуться конгруенції

$$\begin{cases} x_3^2 + y_3^2 = 1 + dx_3^2 y_3^2 \pmod p, \\ x_3^2 + y_3^2 = 1 + dx_3^2 y_3^2 \pmod q. \end{cases} \qquad (14)$$

Оскільки НСД $(p,q) = 1$, то з (14) випливає виконання конгруенції

$$x_3^2 + y_3^2 = 1 + dx_3^2 y_3^2 \pmod n\,,$$

тобто для точки $Z = (x_3, y_3)$ виконується рівність (1), звідки $Z \in E_n$.

Лему повністю доведено.

Тепер сформулюємо теорему про структуру алгебраїчної системи E_n з операцією, визначеною в (2).

Теорема 1. Нехай p, q – різні прості числа, $n = p \cdot q$, $d \in \tilde{Q}_n$. Тоді :

1) множина E_n з операцією (2) утворює абелеву групу;

2) $E_n \cong E_p \times E_q$, де E_p та E_q – криві Едвардса, визначені згідно з (1) з параметрами $d \bmod p$ та $d \bmod q$, відповідно.

Доведення. Як було зазначено раніше, з умови $d \in \tilde{Q}_n$ випливає $d \bmod p \notin Q_n$ та $d \bmod q \notin Q_q$, тому відповідні еліптичні криві E_p та E_q є повними кривими Едвардса [12]. Отже, E_p та E_q, відносно відповідних операцій (згідно з (2)) є абелевими групами, тому їх декартовий добуток $E_p \times E_q$ також є абелевою групою відносно відповідної (покомпонентної) операції. Побудуємо відображення $\phi : E_n \to E_p \times E_q$ таким чином:

$\forall P = (x, y) \in E_n$:

$$\phi(P) = \left(P \bmod p, P \bmod q\right) =$$

$$= \left(\left(x \bmod p, y \bmod p\right), \left(x \bmod q, y \bmod q\right)\right).$$

Для доведення теореми необхідно довести такі властивості цього відображення:

1) ϕ – бієкція;

2) $\forall P, Q \in E_n : \phi(P+Q) = \phi(P) + \phi(Q)$.

Доведемо бієктивність відображення ϕ. Нагадаємо, що згідно з лемою 1, криві $(E_n) \bmod p$ та $(E_n) \bmod q$ співпадають з кривими E_p та E_q, заданими згідно з (1). Покажемо, що для будь-якої пари точок $P_1 = (x_1, y_1) \in E_p$, $P_2 = (x_2, y_2) \in E_q$, $\exists! P = (x, y) \in E_n : \phi(P) = (P_1, P_2)$.

Обчислимо x та y за системами конгруенцій

$$\begin{cases} x \equiv x_1 \pmod p, \\ x \equiv x_2 \pmod q, \end{cases} \quad \begin{cases} y \equiv y_1 \pmod p, \\ y \equiv y_2 \pmod q. \end{cases} \qquad (15)$$

За китайською теоремою про лишки $\exists! x \in Z_n$ та $\exists! y \in Z_n$ для яких виконуються системи (15). Таким чином залишається зазначити, що за властивістю конгруенцій, для x та y справедлива рівність (1), де операції виконуються за модулем n. Звідси $P = (x, y) \in E_n$ і бієктивність відображення доведено.

Доведемо, що це відображення зберігає операцію. Для цього потрібно переконатись у виконанні рівності

$$\forall P, Q \in E_n : \phi(P+Q) = \phi(P) + \phi(Q)\,. \qquad (18)$$

За побудовою відображення ϕ, ліва частина рівності (18) дорівнює

$$\phi(P+Q) = \left(\left(P+Q\right) \pmod p, \left(P+Q\right) \pmod q\right) =$$

$$= \left(\frac{x_1 x_2 - y_1 y_2}{1 - dx_1 x_2 y_1 y_2} \pmod p, \frac{x_1 y_2 - x_2 y_1}{1 + dx_1 x_2 y_1 y_2} \pmod q \right) =$$

$$= \left(\frac{(x_1 \bmod p)(x_2 \bmod p) - (y_1 \bmod p)(y_2 \bmod p)}{1 - d(x_1 \bmod p)(x_2 \bmod p)(y_1 \bmod p)(y_2 \bmod p)} \pmod p, \right.$$

$$\left. \frac{(x_1 \bmod q)(y_2 \bmod q) - (x_2 \bmod q)(y_1 \bmod q)}{1 + d(x_1 \bmod q)(x_2 \bmod q)(y_1 \bmod pq)(y_2 \bmod q)} \pmod q \right) =$$

$$= \left(P \bmod p + Q \bmod p, P \bmod q + Q \bmod q\right) =$$

$$= \left(P \bmod p, P \bmod q\right) + \left(Q \bmod p, Q \bmod q\right) =$$

$$\phi(P) + \phi(Q),$$

і рівність (18) доведена.

ВИСНОВКИ

Таким чином, у роботі повністю описано структуру кривої Едвардса над кільцем лишків Z_n для випадку, коли проекції цієї кривої на поля Z_p та Z_q є повними кривими.

Зазначимо, що у випадку $d \notin \tilde{Q}_n$ проекції кривої E_n на вказані поля не будуть повними, там з'являться «особливі точки» [12], тобто точки з нескінченними координатами. Тому в цьому випадку ізоморфізм $E_n \cong E_p \times E_q$ не може бути доведений за аналогією до теореми 1. Тому наведене питання є темою подальших досліджень.

В даній роботі також показано, що множина точок кривої утворює групу відносно операції додавання точок, яка визначається подібно до операції на кривій Едвардса над F_p. Встановлено ізоморфізм групи точок кривої Едвардса над Z_n, де $n = p \cdot q$, а p, q – різні прості числа, декартовому добутку груп $Z_p \times Z_q$, утворених точками кривих Едвардса над відповідними полями. Ці результати дозволяють звести дослідження властивостей нового об'єкта – кривої E_n над кільцем Z_n, $n = p \cdot q$, до дослідження властивостей «проекцій» цієї кривої на Z_p та Z_q, які є досить добре дослідженими.

Детальніше про практичне значення отриманих тут результатів, а саме про їхнє застосування до методів факторизації, мова йтиме у наступних роботах. Зокрема, буде показано, що з їхнім використанням обґрунтування методу Лєнстра та оцінка часу його роботи виконується суттєво простіше, ніж це зроблено у [7,13].

Література

[1] *K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone*, "New Public-Key Schemes Based on Elliptic Curves over the Ring Zn", CRYPTO' 91 Abstracts, Santa Barbara, CA, pp. 6-1 to 6-7, August 11–15, 1991.

[2] *N. Demytko.* A new elliptic curve based analogue of RSA. In T. Helleseth, edit., Advances in Cryptology – EUROCRYPT '93 , vol.765 of Lect. Notes in Comp.Science, p.40–49. Springer-Verlag, 1994.

[3] *A.K. Lenstra and H.W. Lenstra,* Jnr. "Algorithms in Number theory", University of Chicago, Department of computer Science, Technical Report # 87-008, 1987.

[4] *D.M. Bressoud*, Factorisation and Primality Testing, Springer-Verlag, New York, 1989.

[5] *B.S. Kaliski* Jr. A chosen message attack on Demytko's elliptic curve cryptosystem. Journal of Cryptology, 10(1):71–72, 1997.

[6] *D. Bleichenbacher, M. Joye, J.-J. Quisquarter,* A new and optimal chosen-message attack on RSA-type cryptosystems, LNCS 1334, Proc. Information and Communications Security – ICICS'97, Springer-Verlag, (1997), pp.302-313.

[7] *H.W. Lenstra,* Jr. Factoring integers with elliptic curves. Annuals of Mathematics, 126: 649-673, 1987.

[8] *Беспалов О.Ю., Панасюк І.І.* Метод Лєнстра та особливості його застосування на кривих Едвардса. Перспективні напрями захисту інформації: матеріали третьої всеукраїнської наук.-пр.конф. – м.Одеса, 02-06 вересня 2017р. – Одеса:ОНАЗ, 2017. – с. 4-6

[9] *Edwards H.M.* A normal form for elliptic curves. Bulletin of the American Society, Volume 44, Number 3, July 2007, PP.393-422.

[10] *Bernstein D.J., Lange T.* Faster Addition and Doubling on Elliptic Curves. Advances in Cryptology - ASIACRYPT'2007 (Proc. 13th Int.Conf. On the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2-6, 2007). Lect. Notes Comp. Sci. V.4833, Berlin: Springer, 2007. P.29-50.

[11] *Bernstein Daniel J., Lange Tanja, Farashahi Reza Rezaeian.* Binary Edwards curves. Cryptographic hardware and embedded systems - CHES 2008, 10th international workshop, Washington, D.C.

[12] *Бессалов А.В.* Эллиптические кривые в форме Эдвардса в криптографии: монография. – Киев. Изд-во «Политехника», 2017.-272 с.

[13] *Коблиц Н.* Курс теории чисел и криптографии. – М.: Научное изд-во ТВП, 2001. – 254 с.

[14] *Ковальчук Л.В., Кучинська Н.В.* Теоретична криптологія-2: теорія чисел та її застосування в криптоаналізі. – Київ: ІСЗЗІ «КПІ ім. Ігоря Сікорського», 2016. – 106с.

Поступила в редколлегию 29.12.2017

Беспалов Олексій Юрійович, аспірант, Фізико-технічний інститут НТУУ КПІ ім. Ігоря Сікорського. Область наукових інтересів: алгебра, асиметрична криптологія, еліптичні криві, криві Едвардса, програмування, блокчейн, старт-контракти.

Кучинська Наталія Вікторівна, фото та відомості про автора див. на стор. 164.

УДК 681.3.06:006.354

Структура группы точек кривой Эдвардса над кольцом вычетов и ее применение в криптологии / А.Ю. Беспалов, Н.В. Кучинская, // Прикладная радиоэлектроника: науч.-техн. журнал. – 2017. – Том 16, № 3, 4 – С. 170–175.

Рассматривается эллиптическая кривая, которая является обобщением кривой Эдвардса над кольцом вычетов; в работе показано, что при определенных условиях, множество ее точек образует группу относительно определенной операции; данная группа изоморфна декортовому произведению соответствующих кривых Эдвардса над конечными полями.

Ключевые слова: эллиптические кривые, эллиптические кривые Эдвардса, криптосистемы на эллиптических кривых, группа точек эллиптической кривой.

Библиогр.: 14 наим.

UDC 681.3.06:006.354

Edwards curve group of points structure over a residue ring and its application in cryptology / O. Yu. Bespalov, N. V. Kuchinska // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 170–175.

The curve is considered which is the generation of Edward's curve over the residue ring. It is shown that under some conditions, the set of its points forms a group with respect to some definite operation. This group is isomorphic to the Decart product of correspondent Edward's curves over the prime fields.

Keywords: elliptic curves, Edwards elliptic curves, elliptic curve cryptosystems, group of elliptic curve points.

Ref.: 14 items.