***О.Коссак. Криптування з використанням еліптичної кривої Едвардса / О.Коссак, Я.Холявка // Вісник ТНТУ. — 2014. — Том 73. — № 1. — С.275-280. — (математичне моделювання. математика. фізика).***

*УДК 512.742.72*

**О. Коссак, канд. фіз.-мат. наук.; Я. Холявка, канд. фіз.-мат. наук**

*Львівський національний університет імені Івана Франка*

# КРИПТУВАННЯ З ВИКОРИСТАННЯМ ЕЛІПТИЧНОЇ КРИВОЇ ЕДВАРДСА

***Резюме.*** *Розглянуто криптографічну схему, що використовує протокол Діффі-Геллмана, застосований до кільця $Z_p$ та групи точок еліптичної кривої Едвардса. Ця схема описує алгоритм, який можна використовувати для закритого зв'язку при обміні даними по мережі загального користування і є безпечною, якщо забезпечена автентичність ключа. Запропонований алгоритм має достатній рівень безпеки при невеликих обчислювальних затратах.*

***Ключові слова****: еліптична крива Едвардса, протокол Діффі-Геллмана.*

**O. Kossak, Ya. Kholyavka**

# ENCRYPTION USING THE EDWARDS ELLIPTIC CURVE

***Summary.*** *We consider an encryption system based on the Diffie–Hellman protocol applied both to the ring $\mathbf{Z}_p$ and to the group of points on the Edwards elliptic curve. This protocol establishes a shared secret that can be used for secret communications while exchanging data over a public network and is secure only if the authenticity of the key is assured. The original implementation of the protocol uses the multiplicative group of integers modulo p, where p is a prime.*

*N. Koblitz and V. Miller discovered the Weierstrass elliptic curve cryptography in 1985. The elliptic curve cryptographic schemes are a public-key protocol and their security is based on the hardness of an elliptic curve discrete logarithmic problem. The algorithms are based on the properties of the group of rational points of a Weierstrass elliptic curve with high stability. This group can be used to develop a variety of elliptic curve cryptographic schemes including the digital signature, encryption and key exchange. Over the years, the use of such algorithms did not experience a significant drop in their resistance, although the resistance algorithms built on other groups, significantly decreased.*

*Many papers in recent years are devoted to the study of the cryptographic properties of Edwards elliptic curves: finding fast algorithms to perform batch operations used in cryptosystems constructed on the group of rational points of these curves, the construction of stable curves of this type. The principal attraction of the Edwards elliptic curve cryptography is that it offers sufficient security for a small enough prime p and for a small enough key size.*

*In the present paper we consider a new encryption algorithm using both to the Edwards elliptic curve over finite fields and to the ring $Z_p$, due to this the linear cryptanalysis is highly difficult. The algorithm proposed here provides sufficient security at sufficiently small computational expenses.*

***Key words:*** *Edwards elliptic curve, Diffie–Hellman protocol.*

**Вступ.** Протокол Діффі-Геллмана [1] є асиметричною схемою шифрування. Він полягає у створенні спільного шифроключа для криптування без обміну ним. Цей ключ створюють так: Аліса і Боб (традиційні імена в криптографії) незахищеним каналом зв'язку домовляються про параметри алгоритму: достатньо велике просте число $p$ і ціле число $g$, $2<g<p$. Надалі усі міркування та арифметичні дії будемо проводити над кільцем лишків $Z_p$, числами також будемо вважати елементи $Z_p$. Аліса вибирає відоме тільки їй число $a$ і передає Бобу обчислене нею число $g^a \pmod p$, а Боб вибирає (секретне) число $b$ і передає Алісі обчислене ним число $g^b \pmod p$. Вважається, що будь-хто може прочитати їх повідомлення, але не може змінити. Тепер Алісі потрібно обчислити $(g^b)^a \pmod p$, а Бобу – обчислити $(g^a)^b \pmod p$, і у них буде один і той же ключ $g^{ab} \pmod p$. Вказаний спосіб створення відомого тільки Алісі та Бобу спільного секретного ключа $g^{ab} \pmod p$ дає можливість уникнути важливої для симетричних схем шифрування проблеми обміну ключами. Стійкість такої криптосистеми пов'язана з

обчислювальною трудністю операції дискретного логарифмування – знаючи числа $p$, $g$ і $g^a \pmod p$, потрібно обчислити $a$.

В. Міллер і Н. Кобліц [2,3] запропонували замість $Z_p$ використовувати групу раціональних точок на еліптичній кривій Вейєрштрасса. Г. Едвардс [4] розглянув іншу нормальну форму еліптичної кривої, яку назвали нормальною формою Едвардса.

**Постановка проблеми.** Сучасні криптосхеми, побудовані на еліптичних кривих Вейєрштрасса, мають добру криптостійкість, але досить повільні за рахунок, зокрема, складної групової операції над раціональними точками цієї кривої [5]. Одним із важливих завдань є збільшення швидкодії такої криптосхеми без зменшення її криптостійкості. Для цього є кілька шляхів. Один із них – використання замість кривих Вейєрштрасса інших форм еліптичної кривої [6].

**Аналіз досліджень і публікацій.** Багато праць в останні роки присвячено дослідженню криптографічних властивостей еліптичних кривих Едвардса: знаходженню швидких алгоритмів виконання групових операцій [7], порівнянню швидкодії криптосистем, побудованих на групі раціональних точок таких кривих [8], побудові стійких кривих цього виду [9]. Проведені в цих публікаціях дослідження показують перспективність використання еліптичних кривих Едвардса для побудови алгоритмів криптування.

**Мета роботи** – розроблення алгоритму криптування при обміні повідомленнями, який використовує протокол Діффі-Геллмана, застосований до $Z_p$ і групи раціональних точок кривої Едвардса. Вважатимемо, що при обміні інформацією від імені абонента передають і отримують його повідомлення. Для гарантування цього використовують протоколи ідентифікації, цифрового підпису тощо.

**Постановка задачі та результати досліджень.** Будемо вважати, що $p$ – достатньо велике просте число (можна розглядати степені простих чисел [9]). Над кільцем $Z_p$ розглянемо еліптичну криву Едвардса $E$, задану в проективних координатах рівнянням (нормальна форма Едвардса)

$$(x^2 + y^2)z^2 = z^4 + dx^2y^2, \tag{1}$$

$d$ не є квадратом елемента $Z_p$. Якщо $x_0, y_0, z_0$ є елементами $Z_p$ і задовольняють рівняння (1), то $P_0 = (x_0 : y_0 : z_0)$ називають раціональною точкою еліптичної кривої $E$, а $x_0, y_0, z_0$ – проективними координатами $P_0$. У цій роботі ми будемо розглядати лише раціональні точки кривої $E$ та називатимемо їх точками кривої $E$.

На множині точок кривої (1) визначають операцію $\oplus$ [6,7]. Для довільної точки $P = (x : y : z)$ кривої $E$ покладемо $-P = (-x : y : z)$. Координати $-P$ задовольняють (1), тому $-P \in E$. Якщо $P_1 = (x_1 : y_1 : z_1)$ і $P_2 = (x_2 : y_2 : z_2)$ – різні точки еліптичної кривої $E$, заданої рівнянням (1), то $P_1 \oplus P_2$ визначимо як точку $P_3 = (x_3 : y_3 : z_3)$, де $(x_3 : y_3 : z_3)$ обчислимо так:

$$\begin{aligned} &A = z_1z_2,\ B = A^2,\ C = x_1x_2,\ K = y_1y_2,\ E = dCK,\ F = B - E,\ H = B + E,\\ &x_3 = AF((x_1 + y_1)(x_2 + y_2) - C - K),\ y_3 = AH(K - C),\ z_3 = FH. \end{aligned} \tag{2}$$

Відомо [4], що точки кривої (1) утворюють абелеву групу $G$ відносно операції $\oplus$, нейтральним елементом цієї групи є $(0:1:1)$, а протилежним елементу $P$ є елемент $-P$. Надалі операцію $\oplus$ будемо позначати через +, а також позначимо $2P = P + P$, $3P = 2P + P, \ldots, (k-1)P = (k-2)P + P$, де $k$ – порядок групи $G$.

У нашому випадку крива (1) задана над $Z_p$, тому група точок цієї кривої скінченна. Якщо ж крива Едвардса $E: x^2 + y^2 = 1 + dx^2y^2$ задана в афінних координатах над полем дійсних чисел $R$, то операцію додавання точок кривої визначають за формулами, які відповідають формулам (2), і вона має геометричну інтерпретацію [10]. На рисунку 1 схематично зображено знаходження точки $P_3$, $P_3=P_1+P_2$, для двох різних точок $P_1$ та $P_2$ кривої $E$ у нормальній формі Едвардса, $0<d<1$. Допоміжна крива $C$ проходить через точки $P_1$, $P_2$,(0,–1) та нескінченно віддалені точки, що відповідають точкам з проективними координатами $(1:0:0)$, $(0:1:0)$, і перетинає криву $E$ у точці – $P_3$. Для побудови $P_3$ потрібно знайти точку, симетричну $–P_3$ відносно осі $OY$.

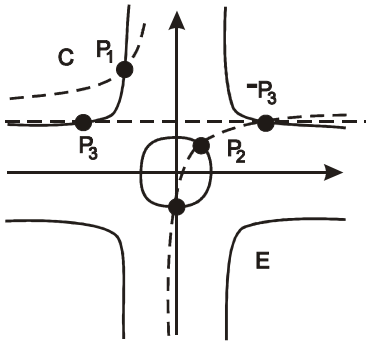


**Рисунок 1.** Геометрична інтерпретація групового закону над $\boldsymbol{R}$, $0<d<1$

**Figure 1.** Geometric interpretation of the group law over $R$ for $0<d<1$

На рисунку 2 схематично зображено знаходження суми (точки $P_3$) двох різних точок $P_1$ та $P_2$ кривої $E$ у нормальній формі Едвардса, $d<0$.

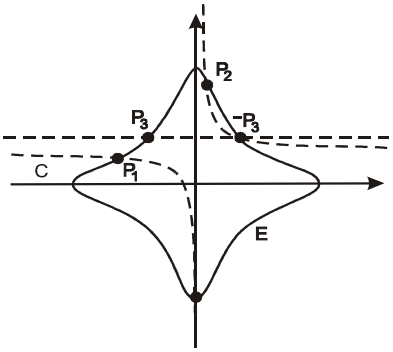


**Рисунок 2.** Геометрична інтерпретація групового закону над $R$, $d<0$

**Figure 2.** Geometric interpretation of the group law over $R$ for $d<0$

На рисунку 3 схематично зображено знаходження $P_1+P_2$ (точки $P_3$), $P_1 \neq P_2$, точок кривої $E$ у нормальній формі Едвардса, $d>1$.

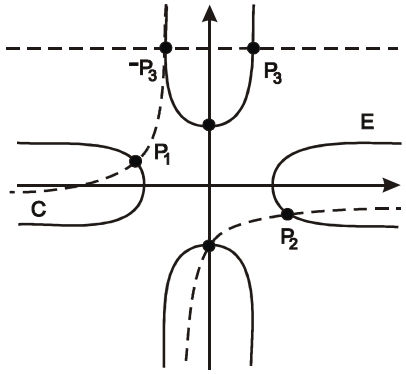


**Рисунок 3.** Геометрична інтерпретація групового закону над $R$, $d>1$

**Figure 3.** Geometric interpretation of the group law over $R$ for $d>1$

Щоб здійснити обмін закритими повідомленнями (за допомогою пропонованого тут протоколу) Аліса та Боб спочатку створюють секретний ключ. Для цього відкритими повідомленнями вони вибирають:

1) достатньо велике просте число $p$;

2) достатньо великого порядку криву $E: (x^2 + y^2)z^2 = z^4 + dx^2y^2$ над $Z_p$;

3) точку $C_0$ кривої $E$ також великого порядку;

4) випадкове число $g$, $g \in Z_p$, $g \neq 0, 1$;

5) число $n$ – довжину випадкової послідовності (можна використати одну або кілька таких послідовностей).

Так само відкритими повідомленнями Аліса та Боб домовляються про алфавітну таблицю, у якій кожному елементу потрібного для користування алфавіту ставлять у відповідність точку кривої $E$. Різним елементам алфавіту відповідають різні точки кривої $E$. Без обмеження загальності можна використати лише точки з $z_3 = 1$.

Після узгодження початкових даних:

1) Аліса генерує випадкові послідовності $\{\alpha_{i,j}\}$, $i = 1,2,3$, $j = 1,\ldots,n$, $\alpha_{i,j} \in \mathsf{Z}_p$, довжини $n$ (позначимо їх $(\alpha_1)$, $(\alpha_2)$ та $(\alpha_3)$ відповідно);

2) Боб генерує випадкові послідовності довжини $n$ $\{\beta_{i,j}\}$, $i = 1,2,3$, $j = 1,\ldots,n$, $\beta_{i,j} \in \mathsf{Z}_p$ (позначимо їх $(\beta_1)$, $(\beta_2)$ та $(\beta_3)$ відповідно);

3) Аліса обчислює послідовності $\{g^{\alpha_{i,j}}\}$, $\{\alpha_{3,j}C_0\}$, $i = 1,2$, $j = 1,\ldots,n$ (позначимо їх $(g^{\alpha_1})$, $(g^{\alpha_2})$ та $(\alpha_3 C_0)$ відповідно);

4) Боб обчислює послідовності $\{g^{\beta_{i,j}}\}$, $\{\beta_{3,j}C_0\}$, $i = 1,2$, $j = 1,\ldots,n$ (позначимо їх $(g^{\beta_1})$, $(g^{\beta_2})$ та $(\beta_3 C_0)$ відповідно).

Відкритими повідомленнями вони обмінюються послідовностями: Аліса надсилає Бобу $(g^{\alpha_1})$, $(g^{\alpha_2})$ та $(\alpha_3 C_0)$, а Боб надсилає Алісі $(g^{\beta_1})$, $(g^{\beta_2})$ та $(\beta_3 C_0)$. Отримавши повідомлення від Боба, Аліса обчислює послідовності $((g^{\beta_1})^{\alpha_1}) = \{(g^{\beta_{1,1}})^{\alpha_{1,1}}, (g^{\beta_{1,2}})^{\alpha_{1,2}}, \ldots, (g^{\beta_{1,n}})^{\alpha_{1,n}}\}$, $((g^{\beta_2})^{\alpha_2}) = \{(g^{\beta_{2,1}})^{\alpha_{2,1}}, (g^{\beta_{2,2}})^{\alpha_{2,2}}, \ldots, (g^{\beta_{2,n}})^{\alpha_{2,n}}\}$ та $(\alpha_3\beta_3 C_0) = \{\alpha_{3,1}\beta_{3,1}C_0, \alpha_{3,2}\beta_{3,2}C_0, \ldots, \alpha_{3,n}\beta_{3,n}C_0\}$. Так само Боб, отримавши повідомлення

від Аліси, обчислює послідовності $((g^{\alpha_1})^{\beta_1})$, $((g^{\alpha_2})^{\beta_2})$ та $(\beta_3\alpha_3C_0)$. Таким чином, Аліса і Боб після проведених обчислень мають ті ж самі послідовності (секретні ключі). Позначимо їх так: $(k_1)=(g^{\alpha_1\beta_1})$, $(k_2)=(g^{\alpha_2\beta_2})$, $(k_3)=(C)=(\alpha_3\beta_3C_0)$. Отже, в наших позначеннях $(k_1)=\{k_{1,j}\}_{j=1,\ldots,n}=\{g^{\alpha_{1,j}\beta_{1,j}}\}_{j=1,\ldots,n}$, $(k_2)=\{k_{2,j}\}_{j=1,\ldots,n}=\{g^{\alpha_{2,j}\beta_{2,j}}\}_{j=1,\ldots,n}$, $(k_3)=(C)=\{C_j\}_{j=1,\ldots,n}=\{C_j\}_{j=1,\ldots,n}=\{(c_{1,j},c_{2,j})\}_{j=1,\ldots,n}$.

Обчисливши секретний ключ, Аліса кількома перетвореннями повідомлення $M$ створює шифротекст $E(M)$:

1) записує повідомлення $M$ у цифровому форматі й отримує послідовність точок еліптичної кривої (1), яку позначимо $(M_1)$;

2) до отриманої послідовності $(M_1)=(x_1,y_1)=\{(x_{1,j},y_{1,j})\}_{j=1,\ldots,n}$ точок кривої $E$ додає послідовність $(k_3)$: $(M_2)=\{(x_{2,j}+c_{1,j},y_{2,j}+c_{2,j})\}_{j=1,\ldots,n}=(x_2,y_2)$;

3) до перших координат точок послідовності $(M_2)$ додає $(k_1)$, а до других координат додає $(k_2)$: $(M_3)=(x_3,y_3)=(x_2,y_2)+(k_1,k_2)=\{(x_{2,j},y_{2,j})\}_{j=1,\ldots,n}$.

Обчислена послідовність $E(M)=(M_3)$ є шифротекстом, який Аліса передає Бобу. Щоб прочитати повідомлення $M$, Боб над отриманою послідовністю $E(M)$ виконує у зворотному порядку перетворення, здійснені Алісою:

1) обчислює $(M_2)$: $(M_2)=E(M)-(k_1,k_2)$;

2) обчислює $(M_1)$: $(M_1)=(M_2)+(-C)$;

3) знайдену послідовність $(M_1)$ перетворює у текст $(M)$ відповідного алфавіту згідно зі встановленою алфавітною таблицею.

**Висновки.** Пропонований алгоритм криптування за допомогою протоколу Діффі-Геллмана для раціональних точок кривої Едвардса і кільця $Z_p$ має високу стійкість за рахунок послідовного використання цього протоколу до кожної зі вказаних структур. Еліптичні криві у нормальній формі Едвардса мають переваги над кривими у формі Вейєрштрасса за рахунок швидкодії та форми запису нейтрального елемента, а тому їх зручно використовувати у таких криптографічних протоколах.

Алгоритми, побудовані на властивостях групи раціональних точок еліптичної кривої, мають високу стійкість. За роки використання таких алгоритмів не відбулося помітного падіння їхньої стійкості, хоча стійкість алгоритмів, побудованих на інших групах, помітно зменшилася.

**Conclusions**. The proposed encryption algorithm based on the Diffie-Hellman protocol for rational points on the Edwards curve and the ring $Z_p$ is highly resistant due to consistent use of this protocol to each of these structures. The Edwards elliptic curves have the advantage over the Weierstrass curves by speed post and form of a neutral element, so they are useful in such cryptographic protocols.

The algorithms based on the properties of the group of rational points of an elliptic curve have high stability. Over the years, the use of such algorithms did not experience a significant drop in their resistance, although the resistance of algorithms built on other groups significantly decreased.

**Список використаної літератури**

1. Черепнев, М.А. Криптографические протоколы [Текст] / М.А.Черепнев – М.: Издательство мех.-мат. ф-та МГУ, 2006. – 69 с.
2. Miller, V.S. Use of Elliptic Curves in Cryptography / V.S. Miller // CRYPTO'85, LNCS. – 1986. –Vol. 218. – P. 417–426.
3. Koblitz, N. Elliptic Curve Cryptosystems / N. Koblitz // Math. Comp. – 1987. – Vol. 48. – P. 203–209.

4. Edwards, H.M. A normal form for elliptic curves / Edwards H. // Bull. Amer. Math. Soc. – 2007. – Vol. 44. – № 3. – P. 393–422.
5. Silverman, J.H. The Arithmetic of Elliptic Curves / J.H. Silverman – Springer-Verlag, New York, 1986. – 522 p.
6. Ashraf, M. On the Alternate Models of Elliptic Curves / M. Ashraf, B. B. Kirlar // International Journal of Information Security Science. – 2012. –Vol 1. – No 2. – P. 49–66.
7. Bernstein, D. J. Faster addition and doubling on elliptic curves / D. J. Bernstein, T. Lange // IST Programme under Contract IST–2002–507932 ECRYPT. – 2007. – P. 29–50.
8. Бессалов, А.В. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем [Текст] / А.В. Бессалов, А.А. Дихтенко, Д.Б. Третьяков // Сучасний захист інформації. – 2011. – №4. – С. 33–36.
9. Бессалов, А.В. Кривые Эдвардса почти простого порядка над расширениями малых простых полей [Текст] / А.В. Бессалов, А.И. Гурьянов, А.А. Дихтенко // Прикладная радиоэлектроника. – 2012. – Т. 11, №2. – С. 225–227.
10. Arenea, C. Faster Computation of the Tate Pairing/ C. Arenea, T. Lange, M. Naehrig, C. Ritzenthaler // Journal of Number Theory. – 2011. – Vol 131. – №5. – P. 842–857.

*Отримано 12.11.2013*