ISSN 2078–5097. Вісн. Львів. ун-ту. Сер. прикл. матем. та інф. 2015. Вип. 23. С. 82–88
Visnyk of the Lviv University. Series Appl. Math. and Informatics. Issue 23. P. 82–88

УДК 512.742.72

ОТ-ПРОТОКОЛ З ВИКОРИСТАННЯМ ЕЛІПТИЧНОЇ КРИВОЇ ЕДВАРДСА

О. Коссак, Я. Холявка

Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, 79000,
e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

Розглянуто ОТ-протокол, що використовує точки еліптичної кривої Едвардса.

Ключові слова: еліптичні криві, ОТ-протокол.

1. ВСТУП

Еліптичні криві як математичний апарат у криптографії розпочали вивчати В. Міллер і Н. Кобліц [1, 2]. Починаючи з 1986 р., значно розширились межі їхнього застосування, з'явилось багато криптографічних напрямів та областей, які використовують властивості різних видів еліптичних кривих над скінченими полями. Опишемо, як можна скористатись еліптичними кривими Едвардса в ОТ-протоколах.

Використання ОТ-протоколу (oblivious transfer protocol) запропонував М. Рабін [3]. У найпростішій версії такого протоколу відправник A (Alice) надсилає повідомлення отримувачу B (Bob) так, що B може прочитати це повідомлення з ймовірністю ½, а відправник A не знає, чи прочитав B надіслане повідомлення.

Надалі перша версія ОТ-протоколу була суттєво узагальнена та доповнена оригінальними математичними ідеями. Зокрема, в [4] описано ефективні інтерактивні та не інтерактивні m/n ОТ-протоколи. Такі протоколи можна впровадити в багатьох ситуаціях. Наприклад, A знає відповіді на оголошені заздалегідь питання, а B (один з користувачів) хоче отримати декілька з цих відповідей, але не розкривати, чи отримав він відповіді і на які питання. Зрозуміло, що поставленої мети можна досягти шляхом залучення третьої особи, яка буде приймати, зберігати та передавати інформацію (незалежний арбітр). ОТ-протокол створений для того, щоб уникнути залучення третьої сторони.

При користуванні ОТ-протоколом можливі різні види шахрайства. Пасивний шахрай дотримується усіх вимог протоколу, але намагається отримати більше інформації, ніж передбачено цим протоколом. Проти такого шахрайства можна забезпечити захист [5]. Активні шахраї подають спотворену інформацію, порушують умови протоколу тощо. Зазвичай при використанні ОТ-протоколів прийнято вважати, що кількість активних шахраїв не перевищує половини всіх учасників обміну інформацією.

Традиційно в ОТ-протоколах використовують математичні операції над Z_p. В [6] з'ясовано, як у таких протоколах можна використовувати групу цілих точок еліптичної кривої Вейєрштрасса. На практиці використовують криві, визначені стандартами FIPS (*Federal Information Processing Standards*).

Надалі розглянемо найпростішу ситуацію, коли відправник A за допомогою OT-протоколу, побудованого на підставі групи точок еліптичної кривої Едвардса з параметром *d*, має намір повідомити абоненту B деяку інформацію.

Наприклад, A хоче для подальшого спілкування використовувати еліптичну криву Едвардса з параметром d_1, яку назвемо основною. Знаючи параметр d_1, обмін інформацією можна проводити за допомогою асиметричної (або комбінованої) криптосистеми з використанням основної кривої Едвардса з параметром d_1. Крім зміни параметра еліптичної кривої, таким самим способом можна змінити і просте число *p* та працювати над іншим полем $\mathbb{Z}_p$.

Крім того, можна змінити й тип еліптичної кривої: замість кривої Едвардса в асиметричній криптосистемі використати еліптичну криву Вейєрштрасса, параметри якої передати за допомогою OT-протоколу з використанням кривої Едвардса.

Домовимось, що учасники обміну не використовують жодного шахрайства, а обмін повідомленнями відбувається відкритими каналами зв'язку без втручання сторонніх учасників: від імені абонента передають і отримують його повідомлення.

2. ГРУПА ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ ЕДВАРДСА

Еліптичною кривою у формі Едвардса [7–9] над полем *F*, характеристика якого відмінна від 2, називають криву *E*, яка в афінних координатах задається рівнянням

$$x^2 + y^2 = 1 + dx^2 y^2. \tag{1}$$

Тут параметр d є елементом поля F, $d^2 \neq 0, 1$. На множині точок кривої (1) можна визначити операцію +. Позначимо через $P_1 = (x_1, y_1)$ та $P_2 = (x_2, y_2)$ дві точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$, так:

$$\begin{cases} x_3 = \dfrac{x_1 y_2 + x_2 y_1}{1 + d x_1 y_1 x_2 y_2} \\ y_3 = \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 y_1 x_2 y_2}. \end{cases}$$

Точки кривої (1) утворюють абелеву групу *G* стосовно операції +, нейтральним елементом цієї групи є точка з координатами (0,1), а протилежним елементу $P = (x, y)$ є елемент $-P = (-x, y)$. Позначимо $2P = P + P$, $3P = 2P + P$, $4P = 3P + P$, …, $(k-1)P = (k-2)P + P$, де k – порядок групи *G*.

Уважаємо, що крива (1) задана над полем $\mathbb{Z}_p$, $p > 2$, тому група точок цієї кривої скінченна. Якщо ж крива Едвардса задана в афінних координатах над полем дійсних чисел $\boldsymbol{R}$, то операція додавання точок кривої має геометричну інтерпретацію [7]. На рис. 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, і перетинає криву *E* у точці $-P_3$. Для побудови P_3 потрібно знайти точку, симетричну $-P_3$ стосовно осі *OY*.

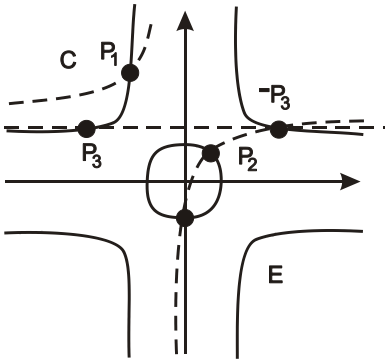

Рис. 1. Геометрична інтерпретація групового закону над $\boldsymbol{R}$, $0<d<1$

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

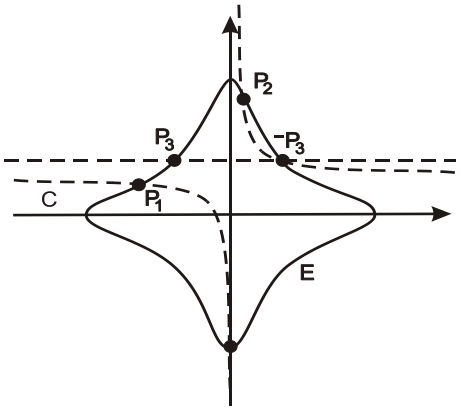

Рис. 2. Геометрична інтерпретація групового закону над $\boldsymbol{R}$, $d<0$

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

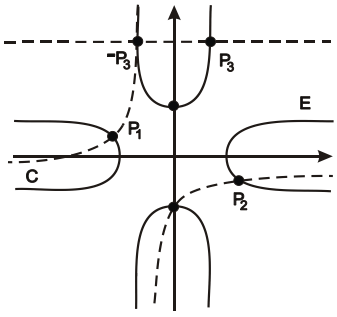

Рис. 3. Геометрична інтерпретація групового закону над $\boldsymbol{R}$, $d>1$

3. ОТ-ПРОТОКОЛ З ВИКОРИСТАННЯМ ГРУПИ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ ЕДВАРДСА

Опишемо ОТ-протокол з використанням кривої Едвардса, який відповідає протоколу, наведеному в [6].

3.1. ВІДКРИТА ІНФОРМАЦІЯ

Спочатку учасники A та B відкритими повідомленнями спільно вибирають такі параметри:

1) просте число p, $p > 2$;

2) еліптичну криву E над Z_p, $x^2 + y^2 = 1 + dx^2y^2$, d – параметр кривої Едвардса;

3) визначають взаємно однозначну відповідність між точками кривої E та деякими елементами Z_p;

4) вибирають довільний елемент a поля Z_p.

3.2. ПЕРЕДАЧА ПАРАМЕТРА ОСНОВНОЇ КРИВОЇ ЕДВАРДСА

Обидва учасники за відомим значенням a знаходять точку P на еліптичній кривій Едвардса з параметром d таку, що a є її першою координатою. Для цього потрібно розв'язати рівняння $a^2 + y^2 = 1 + da^2y^2$. Координату y точки $P(a, y)$ учасники визначають з точністю до знака та фіксують знайдені точки. Якщо учасник A вибрав точку P_A, а учасник B – точку P_B, то $P_A = P_B$ з ймовірністю ½. Кожен з учасників не знає, який вибір зробив інший.

Учасник A визначає параметр d_1 та хоче передати його учаснику B за допомогою ОТ-протоколу. Для цього A та B виконують такі дії:

1) A (згідно з окремо домовленого з B алгоритму) ставить у відповідність параметру d_1 точку K кривої E;

2) A обчислює d_1P_A та надсилає отриману точку до B;

3) B вибирає довільно відомі тільки йому число b та точку H кривої E;

4) B обчислює і надсилає до A три точки:

- bP_B;
- $bd_1P_A + H$;
- $b\,H$;

5) A обчислює дві точки:

- d_1bP_B;
- $Q = d_1(bd_1P_A + H - d_1bP_B)$.

Якщо $P_A = P_B$, то $Q = d_1H$. Позаяк $P_A = P_B$ з ймовірністю ½, то $Q = d_1H$ також з ймовірністю ½;

6) A надсилає до B:

- $d_1bP_B + Q$;
- $W = d_1bH + K$;

7) B обчислює точку d_1H: $d_1H = d_1bP_B + Q - bd_1P_A$;

8) якщо $P_A = P_B$, то B обчислює точку K: $K = W - bd_1H$.

Отже, якщо $P_A = P_B$, то B обчислить точку K. Знаючи цю точку, B отримає параметр d_1. Якщо ж точки P_A та P_B не збігаються, то знаходження точки K еквівалентне задачі обчислення дискретного логарифма.

Отже, учасник В отримав параметр d_1 та зможе надалі користуватись основною еліптичною кривою Едвардса для читання повідомлень від А. Учасник А не переконаний, чи збігаються P_A та P_B, тобто чи може В прочитати повідомлення.

4. ПРИКЛАД

Припустимо, що А хоче передати В значення параметра основної кривої Едвардса. Спочатку вони відкритими каналами зв'язку домовляються про вибір простого числа p та еліптичної кривої E. У прикладі достатньо використати малі числа, тому приймемо $p = 47$, E: $x^2 + y^2 = 1 + 11x^2y^2$. Крива E складається з точок (0, 1), (3, 7), (6, 9), (12, 12), (13, 21), (18, 19) та точок, утворених з них заміною (x,y) на (y,x) та x на $47 - x$, y на $47 - y$ у всіх можливих комбінаціях. Ці точки утворюють групу стосовно операції +, визначеної раніше.

Приймемо $a = 6$. Кожен з учасників обчислює точку на кривій E, першою координатою якої є a. Таких точок є дві: (6, 9) та (6, 38). В отримає параметр d_1, якщо обидва учасники виберуть ту саму точку. Будемо вважати, що $P_A = P_B = (6, 9)$. Жоден з учасників не знає про вибір іншого, тому вибрані точки збігатимуться з ймовірністю ½. Після вибору точок А та В виконують такі перетворення та обміни інформацією:

1) А вибирає параметр d_1, значення якого потрібно передати В. Нехай $d_1 = 3$. Згідно з відомим (заздалегідь визначеним) алгоритмом А ставить у відповідність вибраному параметру точку K кривої E. У нашому прикладі параметру d_1 поставимо у відповідність будь-яку точку кривої Е з першою координатою d_1: К = (3, 7);

2) А обчислює $d_1P_A = 3(6, 9) = (26, 34)$, та надсилає отриману точку до В;

3) В вибирає число b та точку H кривої E. Приймемо $b = 4$, H =(13, 21);

4) В обчислює три точки та надсилає отримані точки до А:

- $bP_B = 4(6, 9) = (41, 9)$;
- $bd_1P_A + H = 12(6,9) + (13, 21) = (7, 44)$;
- $bH = 4(13, 21) = (6, 38)$;

5) А обчислює точки:

- $d_1bP_B = (19, 18)$;
- $Q = d_1(bd_1P_A + H - d_1bP_B) = (44, 40)$;

6) А надсилає до В точки:

- $d_1bP_B + Q = (19, 18) + (44, 40) = (35, 12)$;
- $W = d_1bH + K = (35, 12)$;

7) В обчислює точку d_1H: $d_1H = d_1bP_B + Q - bd_1P_A = (35, 12) - (19, 18) = (44, 40)$;

8) В обчислює точку K: $K = W - bd_1H = (35, 12) - (28, 29) = (3, 7)$.

Отже, якщо $P_A = P_B$, то В отримає точку K, $K = (3, 7)$. Знаючи цю точку, В може визначити параметр d_1, прийнявши, що він дорівнює першій координаті знайденої точки.

Якщо точки P_A та P_B не збігаються, то цей алгоритм не дає змоги знайти точку K. Наведемо результати обчислень у випадку, коли $P_A = (6, 9)$, $P_B = (6, 38)$:

1а) $d_1 = 3$, К = (3, 7);

2а) А обчислює $d_1P_A = 3(6, 9) = (26, 34)$, та надсилає отриману точку до В;

3а) $b = 4$, H =(13, 21);

4а) В обчислює три точки та надсилає отримані точки до А:

- $bP_B = 4(6, 38) = (6, 9)$;
- $bd_1P_A + H = 12(6,9) + (13, 21) = (7, 44)$;

- $bH = 4(13, 21) = (6, 38)$;

5а) А обчислює точки:

- $d_1bP_B = (28, 18)$;
- $Q = d_1(bd_1P_A + H – d_1bP_B) = (35, 35)$;

6а) А надсилає до В точки:

- $d_1bP_B + Q = (28, 18) + (35, 35) = (7, 44)$;
- $W = d_1bH + K = (35, 12)$;

7а) В обчислює $d_1H = d_1bP_B + Q – bd_1P_A = (13, 21)$;

8а) В обчислює $W – bd_1H = (35, 12) – (6, 38) = (26, 13)$.

Обчислена у цьому випадку точка не збігається з точкою K та не визначає потрібного параметра d_1.

5. ВИСНОВКИ

Традиційно в криптографії використовують сертифіковані еліптичні криві Вейєрштрасса. В останні роки вийшло багато праць, у яких запропоновано використовувати в криптографічних протоколах інші типи еліптичних кривих, зокрема криві Едвардса. Такі криві мають деякі переваги [9, 10] і їхнє використання має великі перспективи. Ми розглянули один з найпростіших способів використання OT-протоколу, математичний апарат якого ґрунтується на властивостях групи точок еліптичної кривої Едвардса. В описаній ситуації криву Едвардса та точки на ній треба брати високого порядку. Просте число також потрібно брати достатньо велике. Різні протоколи мають різні вимоги до параметрів кривої, поля Z_p (деколи зручніше працювати над кільцем Z_n). Застосування еліптичних кривих Едвардса потребують подальшого вивчення та сертифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Miller V.S.* Use of Elliptic Curves in Cryptography / V.S. Miller // CRYPTO’85, LNCS. – 1986. –Vol. 218. – P. 417-426.
2. *Koblitz N.* Elliptic Curve Cryptosystems / N. Koblitz // Math. Comp. – 1987. – Vol. 48. – P. 203-209.
3. *Rabin M.O.* How to exchange secrets by oblivious transfer / M.O. Rabin//Technical Report Tech. Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
4. *Фролов А.Б.* Эффективные протоколы передачи комбинации сообщений с забыванием / А.Б. Фролов // Ползуновский вестник. – 2012. – № 2/1. – С. 129-133.
5. *Salomaa A.* Public-Key Cryptography / A. Salomaaю − Springer-Verlag, Berlin, 1996. – 285 p.
6. *Parakh A.* Oblivious transfer using elliptic curves / A. Parakh // Cryptologia. – 2007. – Vol. –31, № 2. – C. 125-132.
7. *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.
8. *Edwards H.* A normal form for elliptic curves / H. Edwards // Bull. Amer. Math. Soc. – 2007. – Vol. 44, № 3. – P. 393-422.

9. *Bernstein D.* Inverted Edwards coordinates / D. Bernstein, T. Lange // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium. – AAECC-17, Lecture Notes in Computer Science, Springer. – 2007. – Vol. 4851. – P. 20-27.
10. *Бессалов А.В.* Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем / А.В. Бессалов, А.А. Дихтенко, Д.Б. Третьяков // Сучасний захист інформації. – 2011. – № 4. – С. 33-36.
11. *Бессалов А.В.* Кривые Эдвардса почти простого порядка над расширениями малых простых полей / А.В. Бессалов, А.И. Гурьянов, А.А. Дихтенко // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2. – С. 225-227.

Стаття: надійшла до редколегії 02.09.2015
доопрацьована 14.10.2015
прийнята до друку 28.10.2015

OT-PROTOCOL USING EDWARDS ELLIPTIC CURVE

O. Kossak, Ya. Kholyavka

Ivan Franko National University of Lviv,
Universytetska Str., 1, Lviv, 79000,
e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

We propose OT-protocol using Edwards elliptic curve.

Key words: elliptic curves, OT-protocol.