УДК: 004.056.55: 003.26

Онацький О.В.
Онацкий А.В.
Onatskiy A.V.

ПРОТОКОЛ РОЗПОДІЛУ КЛЮЧІВ НА ЕЛІПТИЧНИХ КРИВИХ

ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

THE PROTOCOL OF DISTRIBUTION OF KEYS ON ELLIPTIC CURVES

Анотація. Запропонований протокол розподілу ключів на еліптичних кривих, що дозволяє шляхом передавання відкритих повідомлень сформувати у кожного користувача секретний ключ.

Аннотация. Предложен протокол распределения ключей на эллиптических кривых, позволяющий путем передачи открытых сообщений сформировать у каждого пользователя секретный ключ.

Summary. The protocol of distribution of keys on the elliptic curves is offered, allowing by transfer of open messages to create at each user a confidential key.

Будь-яка криптографічна система заснована на використанні криптографічних ключів. У симетричній криптосистемі відправник і одержувач повідомлення використовує один секретний ключ. В асиметричних криптосистемах для зашифровування й розшифровування використовуються різні ключі. Проблема розподілу ключів у криптосистемі є одним з найбільш важливих завдань. У сучасній криптографії завдання керування ключами вирішується за допомогою криптографічних протоколів, основою яких є генерація й розподіл ключів між користувачами. Для реалізації завдання створення загального секретного ключа розроблені й застосовуються у різній стадії складності самостійні алгоритми, протоколи, які реалізовані на основі перетворень у полях Галуа [1, 2]. Розвиток методів і засобів криптоаналізу таких криптосистем змушує збільшувати розміри загальносистемних параметрів і ключів, внаслідок чого збільшується складність виконання базових операцій у полях. Однак вирішення даного питання може бути досягнуте за рахунок створення загального ключа в групах точок еліптичних кривих над полем Галуа $GF(p)$ [3 … 5].

Метою даної статті є розробка криптографічного протоколу розподілу ключів на еліптичних кривих.

Криптосистеми на еліптичних кривих [3, 4] належать до класу криптосистем з відкритим ключем. Їхня безпека, як правило, базується на складності розв'язування задачі дискретного логарифмування в групі точок еліптичної кривої над скінченним полем [5]. Цим зумовлено їхню потужну криптостійкість порівняно з іншими алгоритмами. Еліптичні криві – математичний об'єкт, який може бути визначено над яким завгодно полем. У криптографії зазвичай використовуються скінченні поля. Дослідження показали [5], що криптосистеми на основі еліптичних кривих перевершують інші системи з відкритим ключем за двома важливими параметрами: ступенем захищеності з розрахунку на кожен біт ключа та швидкодією програмної й апаратної реалізацій. Це пояснюється тим, що для обчислення обернених функцій на еліптичних кривих відомі лише алгоритми з експоненційним зростанням трудомісткості, тоді як для звичайних систем запропоновано субекспоненційні методи. У результаті рівень стійкості, який досягається, скажемо, в RSA при використанні 1024-бітових ключів, у системах на еліптичних кривих реалізовується при розмірі ключів 163 біт, що забезпечує простішу як програмну, так і апаратну реалізацію.

У криптосистемах на еліптичних кривих використовується рівняння $y^2 \equiv (x^3 + ax + b) \bmod p$, де $a, b \in GF(p)$, $(4a^3 + 27b^2) \bmod p \neq 0$, $p > 3$ – просте [3]. Множина $E_p(a, b)$ складається з усіх точок (x, y), $x \geq 0$, $p > y$, які задовольняють рівнянню $y^2 \equiv (x^3 + ax + b) \bmod p$, й точки в нескінченності O. Для точок на еліптичній кривій вводиться операція додавання, яка відіграє таку саму роль, що й операція множення у криптосистемах RSA та Ель-Гамаля. Визначену над точками з $E(GF(p))$ операцію додавання алгебрично може бути описано таким чином:

1. $P + O = O + P = P$.

2. Якщо $P = (x, y)$, тоді $P + (x, -y) = O$. Точка $(x, -y)$ є від'ємним значенням точки P і позначається $-P$. Зазначимо, що $(x, -y)$ лежить на еліптичній кривій і належить до $E_p(a, b)$.

3. Якщо $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ визначається згідно з правилами

$$x_3 \equiv (\lambda^2 - x_1 - x_2) \bmod p;$$
$$y_3 \equiv [\lambda (x_1 - x_3) - y_1] \bmod p,$$

де

$$\lambda \equiv \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \pmod p, & \text{çà} \quad P \neq Q; \\ \dfrac{3x_1^2 + a}{2y_1} \pmod p, & \text{çà} \quad P = Q. \end{cases}$$

Число λ – кутовий коефіцієнт січної, проведеної через точки $P = (x_1, y_1)$ та $Q = (x_2, y_2)$. За $P = Q$ січна перетворюється на дотичну, чим і пояснюється наявність двох формул для обчислення λ.

За допомогою описаних вище правил додавання можна обчислити точку kP для будь-якого цілого числа k і будь-якої точки P еліптичної кривої. Проте розв'язок зворотного завдання – знаходження числа k за відомими точками P і kP – є важковирішальною проблемою. Дану задачу називають проблемою дискретного логарифма еліптичної кривої ECDLP (Elliptic Curve Discrete Logarithm Problem). Вирішення проблеми ECDLP [5] є більш складним, ніж вирішення проблеми дискретного логарифмування (знаходження числа x за заданим числом $y \equiv g^x \bmod p$ при відомих основи g і модуля p), на яких базуються RSA-подібні асиметричні криптосистеми. Складність вирішення проблеми ECDLP обумовлена ресурсомісткістю операцій додавання й дублювання точок, за допомогою яких обчислюється kP, як видно з наведених вище формул. Звідси випливає можливість застосування більш коротких ключів. Існує кілька реалізацій криптоалгоритмів на базі еліптичних кривих, які стандартизовано в IEEE P1363, ДСТУ 4145–2002, ГОСТ Р 34.10–2001.

В якості ключа класичної криптосистеми можна використовувати невідому стороннім (секретну) випадкову точку $(x, y) \neq O$ групи точок еліптичної кривої $E_p(a, b)$, якщо домовитись, як конвертувати її в натуральне число, наприклад, одну з координат, скажемо, x вважати подвійним записом натурального числа.

Для отримання такої секретної точки на двох терміналах відкритого каналу зв'язку можна використовувати модифікацію протоколу Діффі–Хеллмана – ECDH (Elliptic Curve Diffie–Hellman), який поданий на рис. 1 [6].

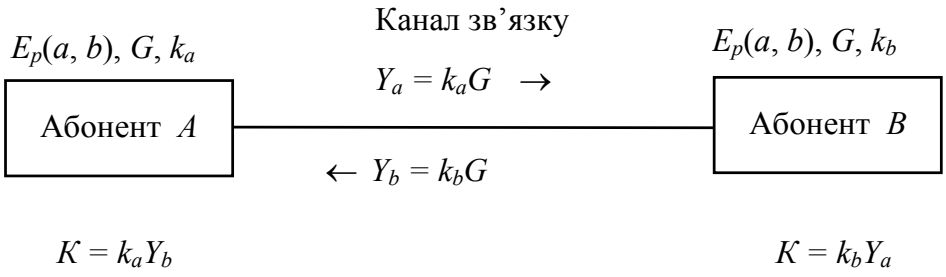

Рисунок 1 – Протокол Діффі–Хеллмана на еліптичних кривих

Припустимо, що E – еліптична крива і G – попередньо погоджена й опублікована точка цієї кривої. Абонент A вибирає, зберігаючи в секреті, випадкове число k_a (секретний ключ A), обчислює координати точки k_aG (свою «половинку» ключа) і пересилає абонентові B. Аналогічно B вибирає секретний ключ k_b, обчислює й пересилає абонентові A «половинку» k_bG ключа. Загальним ключем є точка k_ak_bG. Абонент A обчислює її, помножуючи на свій секретний ключ k_a на «половинку» ключа, обчислену B, а B обчислює цю ж точку, помножуючи повідомлення, яке отримане від A, на свій секретний ключ k_b. Через те, що група точок еліптичної кривої абелева, результат не залежить від порядку обчислення, отже, A і B мають координати секретної точки $k_a(k_bG) = k_b(k_aG) = k_ak_bG = (x, y)$ і можуть використовувати x як ключ симетричної криптосистеми (за умови достатності довжини цього подвійного запису, що залежить від порядку поля, над яким побудована еліптична крива, і за умови, що секретні ключі k_a та k_b були обрані як випадкові або як криптографічні стійкі псевдовипадкові числа). Тепер A і B мають однакові копії пошукової секретної точки еліптичної кривої. Проблема, яка стоїть перед зловмисником, який має намір дізнатися про секретний ключ, полягає в обчисленні k_ak_bG за відомими $G, k_aG, k_bG,$ але за невідомими k_a, k_b.

Приклад 1. Нехай $E_{751}(-1, 188)$; $G = (1, 375)$; $p = 751$, що відповідає кривій $y^2 = x^3 - x + 188$. Припустимо, що користувач A вибирає число $k_a = 297$, знаходить

$$Y_a = k_aG = 297(1, 375) = (341, 389)$$

і пересилає Y_a абонентові B. Аналогічно B вибирає секретний ключ $k_b = 539$, обчислює

$$Y_b = k_bG = 539(1, 375) = (325, 728)$$

і пересилає Y_b абонентові A.

Користувачі A і B обчислюють

$$K = k_aY_b = 297(325, 728) = (624, 295),$$
$$K = k_bY_a = 539(341, 389) = (624, 295).$$

Сторони A і B мають координати секретної точки $(x, y) = (624, 295)$ і можуть використовувати $x = 624$ або $y = 295$ у якості ключа симетричної криптосистеми.

Розглянутий протокол має також недоліки, а саме, якась третя особа C – зловмисник (противник) може взяти на себе функції посередника в передаванні повідомлень між двома абонентами й заволодіти секретним ключем. Дійсно, якщо A і B взаємодіють по протоколу Діффі–Хеллмана, то зловмисник C, перехопивши передавання відкритого ключа k_aG абонента A, передасть абонентові B свій відкритий ключ k_cG, абонент B передасть C свій відкритий ключ k_bG, після чого B і C будуть мати загальний закритий ключ $(k_ck_b)G$. Далі, якщо C передасть свій відкритий ключ також абонентові A, то C і A будуть мати загальний секретний ключ $(k_ck_a)G$. При добре замаскованих діях зловмисника легальні абоненти A і B не будуть знати, що є посередник, який, отримуючи повідомлення одного абонента, здатний його розшифровувати й знову зашифровувати з використанням іншого закритого ключа.

Протокол Діффі–Хеллмана є уразливим для атаки противника всередині (man-in-the-middle attack). Атака на протокол, за якої противник, підміняючи повідомлення в каналі, імітує дії кожної сторони (рис. 2).

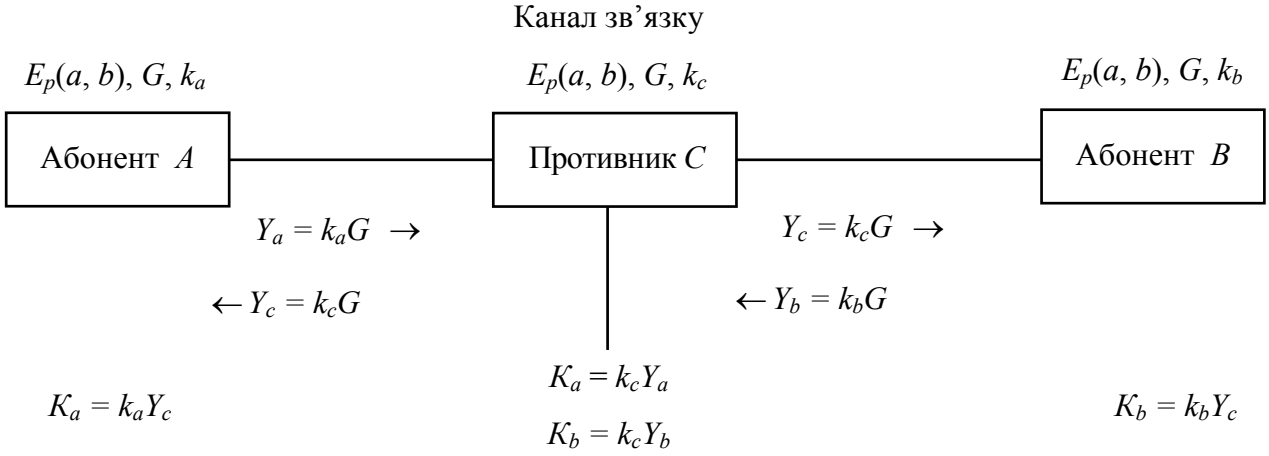

Рисунок 2 – Реалізації атаки противника всередині

Для запобігання таким діям зловмисника необхідна автентифікація (авторизація) цих короткочасних ключів k_aG та k_bG (ключів одноразового використання), для чого використовуються опубліковані довготривалі ключі d_aG та d_bG (ключі багаторазового використання). При цьому короткочасний відкритий ключ зв'язується з довготривалим і тому противник, що не має довготривалого ключа (не зареєстрованого на сервері, де такі ключі зберігаються), не зможе стати посередником комунікацій між двома абонентами.

Розглянемо протокол розподілу ключів Менезеса–Кью–Венстоуна (ECMQV – Elliptic Curve Menezes–Qu–Vanstone), який усуває атаку противника всередині (рис. 3) [7].

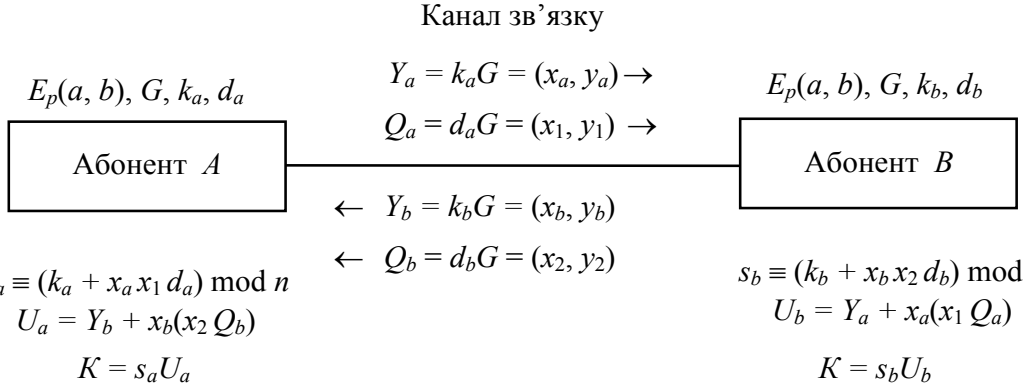

Рисунок 3 – Протокол Менезеса–Кью–Венстоуна на еліптичних кривих

Абоненти A і B мають у своєму розпорядженні точку G еліптичної кривої, над якою й здійснюються всі обчислення. Крім того, вони знають довготривалі й короткочасні ключі один одного. Відкриті ключі абонента B

$$Q_b = d_bG = (x_2, y_2),$$
$$Y_b = k_bG = (x_b, y_b)$$

відомі абонентові A, а відкриті ключі абонента A

$$Q_a = d_aG = (x_1, y_1),$$
$$Y_a = k_aG = (x_a, y_a)$$

відомі абонентові B.

Розглянемо опис і обґрунтування протоколу з використанням, як модульної арифметики, так і циклічної властивості еліптичної кривої. Протоколом передбачається три етапи, симетрично виконуваних кожною зі сторін.

На першому етапі A і B обчислюють відповідно до числа

$$s_a \equiv (k_a + x_a x_1 d_a) \bmod n,$$
$$s_b \equiv (k_b + x_b x_2 d_b) \bmod n,$$

(при цьому вони використовують свої секретні дані k_a, d_a й k_b, d_b відповідно, а також інтерпретуються як числа координати точок еліптичної кривої).

На другому етапі абоненти A і B обчислюють точки еліптичної кривої

$$U_a = Y_b + x_b(x_2 Q_b);$$
$$U_b = Y_a + x_a(x_1 Q_a).$$

На третьому абоненти обчислюють загальну для них точку еліптичної кривої

$$K = s_aU_a = s_bU_b.$$

Абоненти A і B мають у своєму розпорядженні секретну точку K еліптичної кривої, координати якої можуть бути використані для побудови бінарного коду секретного ключа симетричної системи.

Приклад 2. Нехай E_{751} $E_{751}(-1, 188)$; $G = (1, 375)$; $p = 751$; $727G = O$, що відповідає кривій $y^2 = x^3 - x + 188$. Абоненти A і B використовують ключі одноразового використання $k_a = 327$, $k_b = 619$ та ключі багаторазового використання $d_a = 191$ і $d_b = 713$.

Визначаємо відкриті ключі абонентів A і B:

$$Y_a = 327(1, 375) = (354, 153);$$
$$Q_a = 191(1, 375) = (604, 541);$$
$$Y_b = 619(1, 375) = (391, 564);$$
$$Q_b = 713(1, 375) = (734, 552).$$

Обчислюємо числа

$$s_a \equiv (327 + 354 \cdot 604 \cdot 191) \bmod 727 \equiv 685;$$
$$s_b \equiv (619 + 391 \cdot 734 \cdot 713) \bmod 727 \equiv 105.$$

Обчислюємо точки еліптичної кривої

$U_a = (391, 564) + 391 \cdot 734(734, 552) = (391, 564) + (227, 677) = (251, 695)$;

$U_b = (354, 153) + 354 \cdot 604(604, 541) = (354, 153) + (331, 367) = (198, 322)$.

Обчислюємо загальну точку еліптичної кривої

$$K = 685(251, 695) = 105(198, 322) = (339, 353).$$

У статті пропонується новий протокол розподілу ключів, що дозволяє шляхом передавання відкритих повідомлень сформувати у кожного користувача секретний ключ (рис. 4).

Рисунок 4 – Протокол розподілу ключів на еліптичних кривих

Нехай $E_p(a, b)$ – еліптична крива, відома учасникам інформаційного процесу; p – просте число; q – простий дільник числа $p - 1$; α – елементи поля Z_p порядку q. Числа q, α є секретними й відомі учасникам даного протоколу.

Сторона A вибирає випадкове число k_a, а сторона B – випадкове число k_b таким чином, щоб виконувалися умови $1 < k_a < n$ і $1 < k_b < n$.

Сторона A обчислює відкритий ключ Y_a і значення γ_a, які передає абонентові B по незахищеному каналу зв'язку. Сторона B обчислює відкритий ключ Y_b і значення γ_b, які передає абонентові A.

Після обміну відкритими ключами Y_a, Y_b і значеннями γ_a, γ_b сторони обчислюють значення секретного ключа K:

$$K = k_a Y_b + \alpha_1 \gamma_b \text{ – сторона } A;$$
$$K = k_b Y_a + \alpha_2 \gamma_a \text{ – сторона } B.$$

Приклад 3. Нехай $E_p(0, -4)$; $G = (1, 29)$; $241G = O$; $p = 211$; $q = 7$; $\alpha_1 = 58$; $\alpha_2 = 123$. Абонент A вибирає випадкове число $k_a = 72$, а користувач B – випадкове число $k_b = 53$.

Абонент A обчислює значення Y_a і γ_a

$$Y_a = 72(2, 2) = (120, 180),$$
$$\gamma_a = 58(2, 2) = (78, 3).$$

Абонент B обчислює значення Y_b і γ_b

$$Y_b = 53(2, 2) = (99, 180),$$
$$\gamma_b = 123(2, 2) = (104, 190).$$

Сторони обчислюють значення секретного ключа K:

$$K = 72(99, 180) + 58(104, 190) = (185, 199);$$
$$K = 53(120, 180) + 123(78, 3) = (185, 199).$$

Важливою перевагою запропонованого протоколу є те, що він дозволяє обійтися без захищеного каналу для передавання ключів та усуває атаку противника всередині. Однак необхідно мати гарантію того, що користувач A отримує відкритий ключ саме від користувача B, і навпаки. Ця проблема вирішується за допомогою сертифікатів відкритих ключів, створених і розповсюджених центрами сертифікації CA (Certification Authority) у рамках інфраструктури керування відкритими ключами PKI (Public Key Infrastructure), або використання протоколів ідентифікації.

Таким чином, у даній статті на основі аналізу протоколів Elliptic Curve Diffie–Hellman та Elliptic Curve Menezes–Qu–Vanstone, запропоновано новий протокол розподілу ключів на еліптичних кривих, що дозволяє шляхом передавання відкритих повідомлень сформувати у кожного користувача секретний ключ. До основних напрямів подальших досліджень слід віднести оцінку обчислювальної складності, а також криптографічної стійкості запропонованого протоколу.

Література

1. *Харченко В.К.* Некоммутативная теория Галуа / Харченко В.К. – Новосибирск.: Научная книга, 1996. – 372 с.
2. *Чеботарев Н.Г.* Основы теории Галуа / Чеботарев Н.Г. – М.: КомКнига, 2006. – 152 с.
3. *Болотов А.А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / Болотов А.А., Гашков С.Б., Фролов А.Б. – М.: КомКнига, 2006. – 328 с.
4. *Болотов А.А.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / Болотов А.А., Гашков С.Б., Фролов А.Б. – М.: КомКнига, 2006. – 280 с.
5. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии / Василенко О.Н. – М.: МЦНМО, 2003. – 328 с.
6. NIST, Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March, 2006. – 114 p.
7. Hankerson D. Guide to Elliptic Curve Cryptography / Hankerson D., Menezes A., Vanstone S.A. – Springer-Verlag, 2004. – 358 p.