УДК 511, 003

Колеснікова О.О., Пірус Є.М., Рябухо О.М.

[1] *студентка 5 курсу фізико-математичного факультету, СДПУ*

[2] *старший викладач кафедри алгебри, СДПУ*

[3] *завідувач кафедри алгебри, СДПУ*

e-mail: pirus@ukr.net, rom.olena@gmail.com

РЕАЛІЗАЦІЯ ШИФРУ ЕЛЬ ГАМАЛЯ НА ЕЛІПТИЧНІЙ КРИВІЙ

В роботі описано застосування еліптичних кривих до задач криптографії, побудований приклад шифру Ель Гамаля на еліптичній кривій.

Ключові слова: *криптосистема, еліптична крива, проблема дискретного логарифмування.*

В останні десятиріччя еліптичні криві, і особливо над скінченими полями, знайшли найрізноманітніші і притому практичні застосування. Так, у теорії кодування вони використовуються для побудови різних класів кодів, які добре поєднують високу швидкість із хорошими коригуючими властивостями і для яких до того ж існують ефективні алгоритми кодування–декодування. А в криптографії спектр їх застосувань ще ширший. По–перше, саме з їх допомогою будуються найефективніші на сьогодні алгоритми тестування простоти і розкладу чисел на множники. По–друге, вони використовуються безпосередньо для побудови конкретних криптосистем.

Вперше криптографічні алгоритми в групах точок еліптичних кривих були запропоновані незалежно один від одного Н.Кобліцем і В.Міллером в 1986 році [1], [2]. Спочатку ці алгоритми видавалися вельми екзотичними і далекими від практичного вживання, але на початку дев'яностих років були отримані ряд теоретичних результатів, що доводять високу стійкість нових алгоритмів, стала ясною і можливість ефективного виконання операцій в цих групах.

Причин великого поширення криптосистем на еліптичних кривих кілька. По–перше, з кожною еліптичною кривою пов'язується певна абелева група, яка є близькою до циклічної. Це дозволяє будувати криптосистему, що спирається на проблему дискретного логарифма. Однак наявність на групі багатої додаткової структури призводить до експоненційної стійкості криптосистеми,

тоді як мультиплікативна група скінченного поля забезпечує лише субекспоненційну стійкість. По–друге, прогрес у розвитку техніки обчислень у групі точок еліптичної кривої призвів до того, що побудовані на них криптосистеми почали суттєво вигравати в своїх попередників у швидкості перетворення інформації. По–третє, можливості вибору серед еліптичних кривих — у порівнянні з вибором серед мультиплікативних груп полів — є незрівнянно більшими.

Означення 1. *Нехай $p > 3$ просте число. Еліптичною кривою $y^2 = x^3 + ax + b$ над $\mathbb{Z}_p$ є множина розв'язків $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ конгруенції*

$$y^2 \equiv x^3 + ax + b \ (mod\ p), \tag{1}$$

де $a, b \in \mathbb{Z}_p$ константи, такі, що $4a^3 + 27b^2 \not\equiv 0 (mod\, p)$, разом з виділеною точкою $\mathcal{O}$, так званою тачкою нескінченості.

Розв'язок 1 може слугувати для означення еліптичної кривої $GF(p^n)$ для простого числа $p > 3$. Еліптична крива над $GF(2^n)$ або $GF(3^n)$ визначається трохи іншим розв'язком.

На еліптичній кривій E можна побудувати абелеву групу. Для цього визначають відповідну операцію на її точках. Операцію зазвичай записують адитивно і визначають наступним чином: нехай $P = (x_1, y_1)$ і $Q = (x_2, y_2)$ будуть точками на кривій E. Якщо $x_2 = x_1$ та $y_2 = -y_1$, то $P + Q = \mathcal{O}$; в протилежному випадку $P + Q = (x_3, y_3)$, де

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_2) - y_1,$$

а також

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{де } P \neq Q; \\ \frac{3x_1^2 + a}{2y_1}, & \text{де } P = Q. \end{cases}$$

Нарешті визначмо $P + \mathcal{O} = \mathcal{O} + P = P \ \ \forall P \in E$.

Зауважимо, що протилежні елементи обчислити в цій групі дуже легко. Протилежним елементом для довільної точки $(x, y) \in E$ є точка $(x, -y)$.

Число точок які належать еліптичній кривій E над полем $\mathbb{Z}_p$ (p – просте число, $p > 3$) є наближенням до p. Докладніше, в твердженні Хассе йде мова про те, що число точок еліптичної кривої E, N, задовольняє нерівності

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}.$$

Більш докладніше обчислення величини N є важким однак існує розроблений Схофом ефективний алгоритм який виконує такі обчислення. (Термін "ефективний" тут означає час дії алгоритму який є поліпоміальним з-за $\log p$. Час дії алгоритму Схофа дорівнює $O((\log p)^8)$ бітових операцій, завдячуючи чому воно практично використано для простих чисел p з сотнями числових знаків).

Припустимо, що можемо обчислити N, далі хочемо знайти циклічну підгрупу групи E в якій проблема дискретного логарифма була б практично нерозв'язною.

Твердження 1. *Нехай E буде еліптичною кривою над $\mathbb{Z}_p$, де p – просте число та $p > 3$. В той же час існують цілі числа n_1 і n_2, такі, що E ізоморфне з $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Більш того, $n_2|n_1$ та $n_2|(p-1)$.*

Звідси випливає, що якщо зможемо знайти числа n_1 і n_2, то отримаємо циклічну підгрупу групи E ізоморфною з $\mathbb{Z}_{n_1}$, яка може потенційно слугувати основою криптографічної системи Ель Гамаля.

Звернемо увагу, що якщо $n_2 = 1$, то E – циклічна група. Подібно до того, що E є циклічною групою тоді, коли N – просте число або є добутком різних простих чисел.

Розглянемо приклад шифрування в системі Ель Гамаль з використанням еліптичної кривої.

В 1986р. Ель Гамаль запропонував алгоритм обчислення та перевірки цифрового підпису, стійкість якого грунтується на складності дискретного логарифмування в простому скінченному полі [3].

Для користувачей деякої мережі обирається спільна еліптична крива $E_p(a,b)$ і точка G на ній, така, що G, $[2]G$, $[3]G$, ... , $[q]G$ різні точки і $[q]G = \mathcal{O}$ для деякого простого числа q.

Кожен користувач U обирає число c_U, $0 < c_U < q$, яке зберігає як свій таємний ключ, і визначає точку на кривій $D_U = [c_U]G$, яка буде його відкритим ключем. Параметри кривої і список відкритих ключей передаються усім користувачам мережі.

Припустимо, користувач A бажає передати повідомлення користувачу B. Будемо вважати, що повідомлення представлено у вигляді числа $m < p$. робить наступне:

1) Обирає довільне число c_A, $0 < c_A < q$;

2) обчислює $R = [c_A]G$, $P = [c_A]D_B = (x,y)$;

3) шифрує $e = mx \mod p$;

4) посилає B шифротекст (R,e).

Користувач B після отримання (R,e):

1) обчислює $Q = [c_B]R = (x, y)$;
2) дешифрує $m' = ex^{-1} \mod p$.

Дамо обгрунтування протоколу. Для цього достатньо показати, що

$$[c_B]R = [c_B]([c_A]G) = [c_A]([c_B]G) = [c_A]D_B,$$

тобто $Q = P$. Тому $m' = m$.

Координата x точки Q залишається невідомою для супротивника, так як він не знає числа c_A. Противник може намагатися обчислити c_A із точки R, але для цього йому потрібно вирішити проблему дискретного логарифмування на кривій, що вважається неможливим.

Шифр Ель Гамаля на еліптичній кривій в середовищі MAPLE був реалізований для еліптичної кривої $y^2 = x^3 - 3 * x + 1000$ над полем Z_{31991}. Була обрана генеруюча точка $G = [0, 5585]$, а також таємні ключі $c_A = 523$, $c_B = 5103$. За допомогою ключа $c_A = 523$ повідомлення 30000 було перетворене в шрифтотекст $e = ((9767, 11500), 11685)$, який повинен дешифруватися за допомогою таємного ключа $c_B = 5103$.

Наведемо текст алгоритму в середовищі MAPLE

$> PaddQ := proc(x1, y1, x2, y2, p, a :: numeric)$
$> description"PaddQ";$
$> localk, x3, y3;$
$> if(x1 = x2)and(y2 + y1 mod p = 0)then$
$x3 := 0; y3 := 0; returnx3, y3$
$endif; if(x1 <> x2)then$
$> k := (y2 - y1)/(x2 - x1) mod p;$
$> x3 := k^2 - x1 - x2 mod p;$
$> y3 := k * (x1 - x3) - y1 mod p; returnx3, y3$
$> endif;$
$> if(y1 = y2)then$
$k := (3 * x1^2 + a)/(2 * y1);$
$x3 := k^2 - x1 - x2 mod p;$
$> y3 := k * (x1 - x3) - y1 mod p; returnx3, y3$
$> endif; endproc;$
$> PK := proc(x1, y1, k, p, a :: numeric)$
$> R := [0, 0];$
$> P[1] := x1;$
$> P[2] := y1;$
$> Q[1] := P[1];$
$> Q[2] := P[2];$

$> for i from 1 to k-1 do$
$> R := PaddQ(P[1], P[2], Q[1], Q[2], p, a) : Q := R$
$> enddo; return R[1], R[2]$
$> endproc; Warning, `R` is implicitly declared local to procedure `PK`$
$Warning, `P` is implicitly declared local to procedure `PK`$
$Warning, `Q` is implicitly declared local to procedure `PK`$
$Warning, `i` is implicitly declared local to procedure `PK`$
$Curve Y^2 = X^3 - 3 * X + 1000 p = 31991 N = 32089 G = [0, 5585]$
$> R := PK(0, 5585, 523, p, a);$
$> Db := PK(0, 5585, 5103, p, a);$
$> P := PK(Db[1], Db[2], 523, p, a);$
$> m := 30000;$
$> e := m * P[1] mod 31991;$
$> R, e;$
$> Q := PK(R[1], R[2], 5103, p, a);$
$> e;$
$> m1 := e * Q[1]^{-1} mod p;$

У зв'язку з невеликою (у порівнянні, наприклад, з RSA–шифром) довжиною ключа і малими вимогами до об'єму пам'яті свої перші застосування криптосистеми на еліптичних кривих знайшли в пластикових смарт-картах і мобільних телефонах. У багатьох країнах почали приймати нові національні стандарти цифрового підпису, що використовують криптосистеми на еліптичних кривих (США(2000) — FIPS 186-2, Росія(2001) — ГОСТ Р34.10-2001, Україна(2002) — ДСТУ 4145-2002).

Література

[1] *Koblitz N.* Eleptic curve cryptosystems. *Mathematics of Computation*, 48 (1987), 203–209.

[2] *Miller G.L.* Uses of eleptic curves in cryptography. *Lecture Notes in Computer Science*, 218 (1986), 417–426.

[3] *T. ElGamal.* A public key cryptosystem and a signature scheme based on discrete logaritms. IEEE *Transactions on Information Theory*, 31 (1985), 469–472.