УДК 004.056.55

АНАЛІЗ СКЛАДНОСТІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК ЕК ЗАЛЕЖНО ВІД ОБРАНОГО БАЗИСУ

М.В. ЄСІНА, І.Д. ГОРБЕНКО

Розглядаються існуючі базиси представлень еліптичних кривих та їх використання під час виконання операцій у групах точок еліптичних кривих, а також швидкісні характеристики. Формуються пропозиції щодо використання базисів перетворень.

Ключові слова: базис, координати, криптографічні перетворення, складність.

Точки в групах точок ЕК можуть бути подані у декількох координатних базисах. Основними з них є: афінні координати, проективні координати, якобіанові координати, координати Чудновського (Chudnovsky Jacobian) та модифіковані якобіанові координати [6].

Рівняння ЕК над полем F_p дозволяє використовувати 5 найбільш відомих базисів, відомо також 3 базиси подання точок на ЕК над розширеним полем.

Змішані координати мають перевагу, яку легше побачити за наявності великої кількості базисів подання точок на ЕК. Тому з метою проведення подальшого порівняльного аналізу та вибору найбільш привабливих розглядатимемо більш детально базиси подання точок на ЕК над полем F_q.

Для подальшого порівняння складності операцій додавання та подвоєння визначимо змінні, які позначатимуть відповідні дії під час виконання операцій додавання та подвоєння точок: $t(B+B)$ та $t(2B)$ – додавання та подвоєння точок відповідно, B – координатний базис [5,6]; складність операцій додавання та подвоєння точок на кривій зазвичай виражається у:

– кількості множень – (M)
– піднесеннях до квадрата – (S)
– інверсіях – (I)

Операція додавання може ігноруватися в силу незначної складності [1, 2].

1. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В АФІННОМУ ПОДАННІ

Нехай рівняння еліптичної кривої E над F_p має вигляд (1).

$$E: y^2 = x^3 + ax + b\left(a,b \in F_p, 4a^3 + 27b^2 \neq 0\right). \quad (1)$$

Нехай також є точки $P_1 = (x_1, y_1) \in E\left(F_p\right)$ та $P_2 = (x_2, y_2) \in E\left(F_p\right)$. Тоді сумою двох точок P_1 та P_2 називається точка $P_3 \in E\left(F_p\right)$, така що $P_3 = P_1 + P_2 = (x_3, y_3)$. Якщо $P_1 \neq P_2$, то координати точки $P_3 = (x_3, y_3) = P_1 + P_2 = (x_1, y_1) + (x_2, y_2)$ визначаються з використанням формули (2) [4]

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \pmod p, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \pmod p, \end{aligned} \quad (2)$$

де $\lambda = (y_2 - y_1)/(x_2 - x_1) \pmod p$.

Якщо $P_1 = P_2$, то операцію $P_1 + P_2$ називають подвоєнням і вона обчислюється як $P_3 = (x_3, y_3) = 2P_1 = 2(x_1, y_1)$, причому [4]

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \pmod p, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \pmod p, \end{aligned} \quad (3)$$

де $\lambda = \left(3x_1^2 + a\right)/(2y_1) \pmod p$.

2. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ПРОЕКТИВНОМУ ПОДАННІ

Для проективних координат $x = X/Z$ та $y = Y/Z$, тому рівняння ЕК над F_p має вигляд (4).

$$E_P: Y^2 Z = X^3 + aXZ^2 + bZ^3 \pmod p. \quad (4)$$

Нехай є точки $P_1 = (X_1, Y_1, Z_1) \in E_P\left(F_p\right)$ та $P_2 = (X_2, Y_2, Z_2) \in E_P\left(F_p\right)$, тоді сумою двох точок P_1 та P_2 називається точка $P_3 \in E_P\left(F_p\right)$ така, що $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3)$. Якщо $P_1 \neq P_2$, то координати точки $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2 = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$ обчислюються як в [6]

$$\begin{aligned} X_3 &= vA \pmod p, \\ Y_3 &= u\left(v^2 X_1 Z_2 - A\right) - v^3 Y_1 Z_2 \pmod p, \\ Z_3 &= v^3 Z_1 Z_2 \pmod p \end{aligned} \quad (5)$$

де $u = Y_2 Z_1 - Y_1 Z_2 \pmod p$; $v = X_2 Z_1 - X_1 Z_2 \pmod p$; $A = u^2 Z_1 Z_2 - v^3 - 2v^2 X_1 Z_2 \pmod p$.

Якщо $P_1 = P_2$, то операцію $P_1 + P_2$ називають подвоєнням $P_3 = (X_3, Y_3, Z_3) = 2P_1 = 2(X_1, Y_1, Z_1)$, причому [5]

$$\begin{aligned} X_3 &= 2hs \pmod p, \\ Y_3 &= w(4B - h) - 8Y_1^2 s^2 \pmod p, \\ Z_3 &= 8s^3 \pmod p \end{aligned} \quad (6)$$

де $w = aZ_1^2 + 3X_1^2 \pmod p$; $s = Y_1 Z_1 \pmod p$; $B = X_1 Y_1 s \pmod p$; $h = w^2 - 8B \pmod p$.

3. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ЯКОБІАНОВИХ КООРДИНАТАХ

Для якобіанових координат $x = X/Z^2$ та $y = Y/Z^3$, тому рівняння ЕК над F_p має вигляд:

$$E_J: Y^2 = X^3 + aXZ^4 + bZ^6 \pmod p. \quad (7)$$

Нехай є точки $P_1=(X_1,Y_1,Z_1)\in E_J(F_p)$ та $P_2=(X_2,Y_2,Z_2)\in E_J(F_p)$, тоді сумою двох точок P_1 та P_2 називається точка $P_3\in E_J(F_p)$ така, що $P_3=P_1+P_2=(X_3,Y_3,Z_3)$. Якщо $P_1\neq P_2$, то координати точки $P_3=(X_3,Y_3,Z_3)=P_1+P_2=(X_1,Y_1,Z_1)+(X_2,Y_2,Z_2)$ обчислюються за правилом [5].

$$\begin{aligned}&X_3=-H^3-2U_1H^2+r^2\,(\mathrm{mod}\,p),\\&Y_3=-S_1H^3+r\left(U_1H^2-X_3\right)(\mathrm{mod}\,p),\\&Z_3=Z_1Z_2H\,(\mathrm{mod}\,p)\end{aligned}\qquad(8)$$

де $U_1=X_1Z_2^2\,(\mathrm{mod}\,p)$, $U_2=X_2Z_1^2\,(\mathrm{mod}\,p)$, $S_1=Y_1Z_2^3\,(\mathrm{mod}\,p)$, $S_2=Y_2Z_1^3\,(\mathrm{mod}\,p)$, $H=U_2-U_1\,(\mathrm{mod}\,p)$, $r=S_2-S_1\,(\mathrm{mod}\,p)$.

Якщо $P_1=P_2$, то операцію P_1+P_2 називають подвоєнням і $P_3=(X_3,Y_3,Z_3)=2P_1=2(X_1,Y_1,Z_1)$, причому

$$\begin{aligned}&X_3=T\,(\mathrm{mod}\,p),\\&Y_3=-8Y_1^4+M(S-T)(\mathrm{mod}\,p),\\&Z_3=2Y_1Z_1\,(\mathrm{mod}\,p)\end{aligned}\qquad(9)$$

де $S=4X_1Y_1^2\,(\mathrm{mod}\,p)$; $M=3X_1^2+aZ_1^4\,(\mathrm{mod}\,p)$; $T=-2S+M^2\,(\mathrm{mod}\,p)$.

4. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В КООРДИНАТАХ ЧУДНОВСЬКОГО

Для координат Чудновського $x=X/Z^2$ та $y=Y/Z^3$, тому рівняння ЕК над F_p має вигляд

$$E_{J^c}:Y^2=X^3+aXZ^4+bZ^6\,(\mathrm{mod}\,p),\qquad(10)$$

тобто співпадає з (7).

Нехай є точки $P_1=\left(X_1,Y_1,Z_1,Z_1^2,Z_1^3\right)\in E_{J^c}(F_p)$ та $P_2=\left(X_2,Y_2,Z_2,Z_2^2,Z_2^3\right)\in E_{J^c}(F_p)$, тоді сумою двох точок P_1 та P_2, називається точка $P_3\in E_{J^c}(F_p)$ така, що $P_3=P_1+P_2=\left(X_3,Y_3,Z_3,Z_3^2,Z_3^3\right)$. Якщо $P_1\neq P_2$, то координати точки

$$\begin{aligned}&P_3=\left(X_3,Y_3,Z_3,Z_3^2,Z_3^3\right)=P_1+P_2=\\&=\left(X_1,Y_1,Z_1,Z_1^2,Z_1^3\right)+\left(X_2,Y_2,Z_2,Z_2^2,Z_2^3\right)\end{aligned}$$

формуються так [6]:

$$\begin{aligned}&X_3=-H^3-2U_1H^2+r^2\,(\mathrm{mod}\,p),\\&Y_3=-S_1H^3+r\left(U_1H^2-X_3\right)(\mathrm{mod}\,p),\\&Z_3=Z_1Z_2H\,(\mathrm{mod}\,p),\\&Z_3^2=Z_3^2\,(\mathrm{mod}\,p),\\&Z_3^3=Z_3^3\,(\mathrm{mod}\,p),\end{aligned}\qquad(11)$$

де $U_1=X_1\left(Z_2^2\right)(\mathrm{mod}\,p)$; $U_2=X_2\left(Z_1^2\right)(\mathrm{mod}\,p)$; $S_1=Y_1\left(Z_2^3\right)(\mathrm{mod}\,p)$; $S_2=Y_2\left(Z_1^3\right)(\mathrm{mod}\,p)$; $H=U_2-U_1\,(\mathrm{mod}\,p)$; $r=S_2-S_1\,(\mathrm{mod}\,p)$.

Якщо $P_1=P_2$, то операцію P_1+P_2 називають подвоєнням і $P_3=\left(X_3,Y_3,Z_3,Z_3^2,Z_3^3\right)=2P_1=2\left(X_1,Y_1,Z_1,Z_1^2,Z_1^3\right)$, причому:

$$\begin{aligned}&X_3=T\,(\mathrm{mod}\,p),Y_3=-8Y_1^4+M(S-T)(\mathrm{mod}\,p),\\&Z_3=2Y_1Z_1\,(\mathrm{mod}\,p),Z_3^2=Z_3^2\,(\mathrm{mod}\,p),\\&Z_3^3=Z_3^3\,(\mathrm{mod}\,p),\end{aligned}\qquad(12)$$

де $S=4X_1Y_1^2\,(\mathrm{mod}\,p)$; $M=3X_1^2+a\left(Z_1^2\right)^2\,(\mathrm{mod}\,p)$; $T=-2S+M^2\,(\mathrm{mod}\,p)$.

5. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ У МОДИФІКОВАНИХ ЯКОБІАНОВИХ КООРДИНАТАХ

Для модифікованих якобіанових координат $x=X/Z^2$ та $y=Y/Z^3$, рівняння ЕК має вигляд

$$E_{J^m}:Y^2=X^3+aXZ^4+bZ^6\,(\mathrm{mod}\,p),\qquad(13)$$

тобто співпадає з (7, 10).

Нехай є дві точки $P_1=\left(X_1,Y_1,Z_1,aZ_1^4\right)\in E_{J^m}(F_p)$ та $P_2=\left(X_2,Y_2,Z_2,aZ_2^4\right)\in E_{J^m}(F_p)$, тоді сумою двох точок P_1 та P_2 називається точка $P_3\in E_{J^m}(F_p)$ така, що $P_3=P_1+P_2=\left(X_3,Y_3,Z_3,aZ_3^4\right)$.
Якщо $P_1\neq P_2$, то координати точки

$$\begin{aligned}&P_3=\left(X_3,Y_3,Z_3,aZ_3^4\right)=P_1+P_2=\\&=\left(X_1,Y_1,Z_1,aZ_1^4\right)+\left(X_2,Y_2,Z_2,aZ_2^4\right)\end{aligned}$$

формуються так [3]:

$$\begin{aligned}&X_3=-H^3-2U_1H^2+r^2\,(\mathrm{mod}\,p),\\&Y_3=-S_1H^3+r(U_1H^2-X_3)(\mathrm{mod}\,p),\\&Z_3=Z_1Z_2H\,(\mathrm{mod}\,p),aZ_3^4=aZ_3^4\,(\mathrm{mod}\,p),\end{aligned}\qquad(14)$$

де $U_1=X_1Z_2^2\,(\mathrm{mod}\,p)$; $U_2=X_2Z_1^2\,(\mathrm{mod}\,p)$; $S_1=Y_1Z_2^3\,(\mathrm{mod}\,p)$; $S_2=Y_2Z_1^3\,(\mathrm{mod}\,p)$; $H=U_2-U_1\,(\mathrm{mod}\,p)$; $r=S_2-S_1\,(\mathrm{mod}\,p)$.

Якщо $P_1=P_2$, то операцію P_1+P_2 називають подвоєнням та $P_3=\left(X_3,Y_3,Z_3,aZ_3^4\right)=2P_1=2\left(X_1,Y_1,Z_1,aZ_1^4\right)$, причому:

$$\begin{aligned}&X_3=T\,(\mathrm{mod}\,p),\\&Y_3=M(S-T)-U\,(\mathrm{mod}\,p),\\&Z_3=2Y_1Z_1\,(\mathrm{mod}\,p),\\&aZ_3^4=2U\left(aZ_1^4\right)(\mathrm{mod}\,p),\end{aligned}\qquad(15)$$

де $S=4X_1Y_1^2\,(\mathrm{mod}\,p)$, $U=8Y_1^4\,(\mathrm{mod}\,p)$, $M=3X_1^2+\left(aZ_1^4\right)(\mathrm{mod}\,p)$, $T=-2S+M^2\,(\mathrm{mod}\,p)$.

У таблиці 1 наведено основні співвідношення, які визначають складність перетворень у різних базисах.

Таблиця 1

Складність перетворення у різних базисах

Базис	Додавання
Афінний A	$t(A+A)=I+2M+S$
Проективний P	$t(P+P)=12M+2S$
Якобіанів J	$t(J+J)=12M+4S$
Чудновського J^C	$t(J^c+J^c)=11M+3S$
Модифікований Якобіанів J^m	$t(J^m+J^m)=13M+6S$
Базис	Подвоєння
Афінний A	$t(2A)=I+2M+2S$
Проективний P	$t(2P)=7M+5S$
Якобіанів J	$t(2J)=4M+6S$
Чудновського J^C	$t(2J^c)=5M+6S$
Модифікований Якобіанів J^m	$t(2J^m)=4M+4S$

У таблиці 2 наведено час, який затрачається на операцію складання та подвоєння у кожній системі координат.

Таблиця 2

Час, необхідний для виконання операції складання та подвоєння

Базис	$t(B+B)$	$t(2B)$
Афінний A	0.198 мс	0.209 мс
Проективний P	0.468 мс	0.245 мс
Якобіанів J	0.339 мс	0.186 мс
Чудновського J^C	0.260 мс	0.172 мс
Модифікований Якобіанів J^m	0.423 мс	0.137 мс

Як бачимо, на складання менше витрачається часу в афінному базисі, а на подвоєння – у модифікованому Якобіановому базисі. Найбільше часу на складання точок, а також на їх подвоєння потребує проективний базис. Тобто, якщо керуватися критерієм часу виконання операцій, то проективний базис можна відкинути як такий, що не задовольняє умову швидкодії.

У таблиці 3 наведено оцінку обчислювальної складності $t(X \to Y)$, необхідної для перетворення точки еліптичної кривої з однієї системи координат (X) до іншої (Y).

6. АНАЛІЗ СКЛАДНОСТІ КРИПТОПЕРЕТВОРЕНЬ ТА МОЖЛИВОСТІ ЇХ ЗМЕНШЕННЯ ЗА РАХУНОК КОМБІНАЦІЇ ПЕРЕТВОРЕНЬ У РІЗНИХ БАЗИСАХ

Просторова та часова складності криптоперетворень у групі точок еліптичних кривих залежать від базисів, що застосовуються при криптоперетвореннях, а також від конкретності реалізації криптопримітивів. Для кращої реалізації криптосистем необхідно мінімізувати складність перетворень за рахунок використання найкращого (можливо оптимального) базису.

Графіки складності додавання та подвоєння у групі точок ЕК в афінних та проективних координатах (в залежності від порядку розширеного поля m) наведені на рис. 1, 2 відповідно.

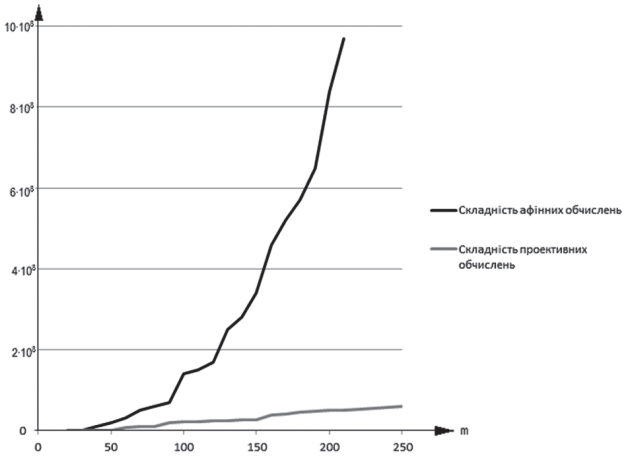

Рис. 1. Складність додавання у групі точок ЕК в афінних та проективних координатах

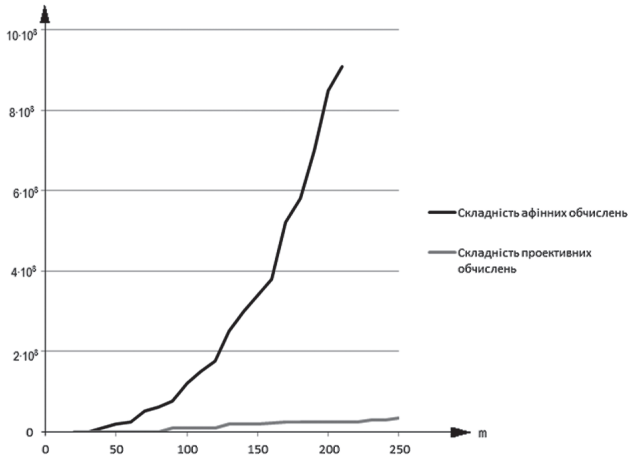

Рис. 2. Складність подвоєння у групі точок ЕК в афінних та проективних координатах

Таблиця 3

Оцінка обчислювальної складності

З/до	A	P	J	J^C	J^m
Афінний A	0	$2M$	$3M+S$	$3M+S$	$4M+2S$
Проективний P	$2M+I$	0	$2M+S$	$3M+S$	$3M+2S$
Якобіанів J	$3M+S+I$	$M+S+I$	0	$M+S$	$M+2S$
Чудновського J^C	$3M+S+I$	$M+S+I$	0	0	$M+S$
Модифікований Якобіанів J^m	$3M+S+I$	$M+S+I$	0	$M+S$	0

Складність додавання та подвоєння точок обчислена у числі тактів, необхідних для виконання операцій з довжиною чисел у m біт. Знаючи число тактів виконання операцій додавання та подвоєння, можна визначити час виконання кожної з операцій.

При додаванні та при подвоєнні складність обчислень більша в афінних координатах, а в проективних значно менше. Але водночас, проективні координати потребують більше часу на виконання операцій складання та подвоєння точок, ніж афінні, які взагалі є найшвидшими серед усіх інших базисів.

Зрештою, після різних перетворень приходять до афінних координат: наприклад, для максимального зменшення складності криптографічних перетворень у групі точок ЕК необхідно використовувати криптографічні перетворення в змішаних координатах з подальшим перетворенням в афінний базис. Це ще раз доводить швидкодію афінного базису.

Для побудови криптосистем на основі ЕК кращим є використання подання точок у модифікованих якобіанових координатах, оскільки вони забезпечують мінімізацію складності операції подвоєння точки на ЕК. Але при великій кількості одиниць у бінарному поданні множника необхідно використовувати більш збалансоване подання координат – якобіанове подання [6].

Використання одного координатного базису не завжди дозволяє досягнути максимальної продуктивності. Перспективним напрямком є використання змішаних координат.

У таблиці 4 наведено складності операцій додавання та подвоєння у випадку використання змішаних координат.

Таблиця 4

Складність операцій додавання та подвоєння під час використання змішаних координат

Подвоєння	
Операція	Часові витрати
$t(2P)$	$7M+5S$
$t(2J^c)$	$5M+6S$
$t(2J)$	$4M+6S$
$t(2J^m=J^c)$	$4M+5S$
$t(2J^m)$	$4M+4S$
$t(2A=J^c)$	$3M+5S$
$t(2J^m=J)$	$3M+4S$
$t(2A=J^m)$	$3M+4S$
$t(2A=J)$	$2M+4S$
$t(2A)$	$2M+2S+I$
Додавання	
Операція	Часові витрати
$t(J^m+J^m)$	$13M+6S$
$t(J^m+J^c=J^m)$	$12M+5S$
$t(J+J^c=J^m)$	$12M+5S$
$t(J+J)$	$12M+4S$
$t(P+P)$	$12M+2S$
$t(J^c+J^c=J^m)$	$11M+4S$
$t(J^c+J^c)$	$11M+3S$
$t(J^c+J=J)$	$11M+3S$
$t(J^c+J^c=J)$	$10M+2S$
$t(J+A=J^m)$	$9M+5S$
$t(J^m+A=J^m)$	$9M+5S$
$t(J^c+A=J^m)$	$8M+4S$
$t(J^c+A=J^c)$	$8M+3S$
$t(J+A=J)$	$8M+3S$
$t(J^m+A=J)$	$8M+3S$
$t(A+A=J^m)$	$5M+4S$
$t(A+A=J^c)$	$5M+3S$
$t(A+A)$	$2M+S+I$

ВИСНОВКИ

Аналіз таблиці 4 дозволяє визначити таке: для максимального зменшення складності криптографічних перетворень у групі точок ЕК необхідно використовувати криптографічні перетворення в змішаних координатах з подальшим перетворенням в афінний базис. Причому, вибір змішаних координат напряму залежить від алгоритму скалярного множення.

Література.

[1] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты та языке Си. Москва: «Триумф», 2002. – 797 с.

[2] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves. Part 2. Digital signatures.

[3] *Cohen H., Miyaji A., Ono T.* "Efficient elliptic curve exponentiation using mixed coordinates", Advanced in Cryptology, 1998.

[4] *Бондаренко М.Ф., Горбенко И.Д., Качко Е.Г., Свинарев А.В., Гриненко Т.А.* Сущность и результаты исследования свойств перспективных стандартов цифровой подписи X9.62-1998 и распределение ключей X9.63-199X на эллиптических кривых. // Радиотехника 114/2000. – С.15–24.

[5] *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Сложность операций в группах точек эллиптических кривых для криптограффических операций. // Радиотехника: Всеукр. межвед. науч-тех. сб 2001. Вып. 119. – С. 51–55.

[6] *Збитнев С.И.* Проективная геометрия – не все так гладко // Радиотехника: Всеукр. межвед. науч-тех. сб 2002. – Вып. 126. – С. 123–131.

Надійшла до редколегії 17.04.2013

Горбенко Іван Дмитрович, фото та відомості про автора див. на с. 201.

Єсіна Марина Віталіївна, студентка факультету комп'ютерних наук, кафедри Безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: криптографія, криптоаналіз та їх застосування з метою захисту інформації.

УДК 004.056.55

Анализ сложности криптографических преобразований в группе точек ЭК в зависимости от выбранного базиса / Есина М.В., Горбенко И.Д. // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 280–284.

Рассматриваются существующие базисы представлений эллиптических кривых и их использование при выполнении операций в группах точек эллиптических кривых, а также скоростные характеристики. Формулируются предложения, касающиеся базисов преобразований.

Ключевые слова: базис, координаты, криптографические преобразования, сложность.

Ил.: 2. Библиогр.: 6 назв.

UDC 004.056.55

Analyzing the complexity of cryptographic transformations in a group of points of elliptic curves according to a basis chosen / M.V. Yesina, I.D. Gorbenko / / Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 280–284.

Existing elliptic curves representation bases and their using in carrying out operations in groups of elliptic curves points are considered. Proposals for using transformation bases are formulated.

Keywords: basis, coordinates, cryptographic transformations, complexity.

Fig.: 2. Ref.: 6 items.