УКРАЇНА UKRAINE

П А Т Е Н Т

НА КОРИСНУ МОДЕЛЬ

№ 38400

СПОСІБ ВИЗНАЧЕННЯ СУМИ ДВОХ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ НАД ДВІЙКОВИМ РОЗШИРЕНИМ ПОЛЕМ У ПРОЕКТИВНИХ КООРДИНАТАХ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **12.01.2009.**

Голова Державного департаменту інтелектуальної власності М.В. Паладій

Міністерство освіти і науки України Державний департамент інтелектуальної власності № 1

(11) **38400**

(19) **UA**

(51) **МПК**
G06F 7/04 (2008.01)

(21) Номер заявки: **u 2008 10866**

(22) Дата подання заявки: **03.09.2008**

(24) Дата, з якої є чинними права на корисну модель: **12.01.2009**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **12.01.2009, Бюл. № 1**

(72) Винахідники:
Кузнецов Олександр Олександрович (UA),
Євсеєв Сергій Петрович (UA),
Ковтун Владислав Юрійович (UA),
Поляков Андрій Олександрович (UA),
Король Ольга Григорівна (UA)

(73) Власник:
Євсеєв Сергій Петрович,
вул.Ком.Корка,12,кв.212,
м.Харків, 61148, Україна

(54) Назва корисної моделі:

СПОСІБ ВИЗНАЧЕННЯ СУМИ ДВОХ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ НАД ДВІЙКОВИМ РОЗШИРЕНИМ ПОЛЕМ У ПРОЕКТИВНИХ КООРДИНАТАХ

(57) Формула корисної моделі:

Спосіб визначення суми двох точок еліптичної кривої над двійковим розширеним полем у проективних координатах, який полягає у виконанні процедури додавання двох точок, яка використовує послідовну дію пристроїв "добуток", "піднесення до квадрата" та "додавання" елементів двійкового розширеного поля згідно з алгоритмом додавання точок, а при обчисленні суми двох точок користуються проективними координатами, **який відрізняється** тим, що додатково включені тимчасові змінні, які зберігаються у відповідних пристроях, виконані над ними послідовні дії пристроїв "добуток", "піднесення до квадрата" та "додавання" елементів двійкового розширеного поля та відсутня залежність від параметра кривої.

Пронумеровано, прошито металевими
люверсами та скріплено печаткою
2 арк.
12.01.2009

Уповноважена особа

(підпис)

УКРАЇНА

(19) UA (11) 38400 (13) U

(51) МПК
G06F 7/04 (2008.01)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ ВИЗНАЧЕННЯ СУМИ ДВОХ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ НАД ДВІЙКОВИМ РОЗШИРЕНИМ ПОЛЕМ У ПРОЕКТИВНИХ КООРДИНАТАХ

(21) u200810866
(22) 03.09.2008
(24) 12.01.2009
(46) 12.01.2009, Бюл.№ 1, 2009 р.
(72) КУЗНЕЦОВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ, UA, ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ, UA, КОВТУН ВЛАДИСЛАВ ЮРІЙОВИЧ, UA, ПОЛЯКОВ АНДРІЙ ОЛЕКСАНДРОВИЧ, UA, КОРОЛЬ ОЛЬГА ГРИГОРІВНА, UA
(73) ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ, UA
(57) Спосіб визначення суми двох точок еліптичної кривої над двійковим розширеним полем у проективних координатах, який полягає у виконанні процедури додавання двох точок, яка використовує послідовну дію пристроїв "добуток", "піднесення до квадрата" та "додавання" елементів двійкового розширеного поля згідно з алгоритмом додавання точок, а при обчисленні суми двох точок користуються проективними координатами, який відрізняється тим, що додатково включені тимчасові змінні, які зберігаються у відповідних пристроях, виконані над ними послідовні дії пристроїв "добуток", "піднесення до квадрата" та "додавання" елементів двійкового розширеного поля та відсутня залежність від параметра кривої.

Запропонована корисна модель відноситься до автоматики й обчислювальної техніки і може бути використана системах криптографічного захисту інформації для розширення їх можливостей.

Відомий спосіб визначення суми двох точок еліптичної кривої над полем $GF(2^n)$ у проективних координатах Якобі [1], що ґрунтується на виконанні процедури додавання двох точок, яка використовує послідовну дію пристроїв „Добуток", „Піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, згідно алгоритму додавання точок, а при обчисленні суми двох точок користуються проективними координатами Якобі.

Проективній точці $(X:Y:Z)$, $Z\neq 0$, ставиться у відповідність точка з афінними координатами $(X/Z^2, Y/Z^3)$. Еліптична крива E над $GF(2^n)$, має вигляд

$$Y^2+XYZ=X^3+aX^2Z^2+bZ^6,$$

де $a,b \in GF(2^n)$ при $b\neq 0$.

Процедура додавання двох точок кривої у проективних координатах у випадку

$P_1(X_1:Y_1:Z_1)\neq P_2(X_2:Y_2:Z_2)$

виконується згідно виразів:

$$X_3 = A\cdot(A+Z_3)+B^2\cdot B+a\cdot Z_3^2;$$

$$Y_3=X_3\cdot(A+Z_3)+C^2\cdot(A\cdot X_2+B\cdot E);$$

$$Z_3=C\cdot Z_2$$

де

$$A = Y_1\cdot Z_2^3 + Y_2\cdot Z_1^3;$$

$$B = X_1\cdot Z_2^2 + X_2\cdot Z_1^2;$$

у випадку

$P_1(X_1:Y_1:Z_1)=P_2(X_2:Y_2:Z_2)$

й

$$P_1\left(X_1/Z_1^2, Y_1/Z_1^3\right)=P_2\left(X_2/Z_2^2, Y_2/Z_2^3\right)$$

процедура додавання виконується згідно виразів:

$$X_3=(X_1+c\cdot B)^4;$$

$$Y_3=A^2\cdot Z_3+X_3\cdot(Z_3+A+Y_1\cdot Z_1);$$

$$Z_3=X_1\cdot B,$$

де

$$A = X_1^2;$$

$$B = Z_1^2;$$

$$c = b^{\frac{1}{4}},$$

у випадку, коли одна з точок подана у проективних координатах, а інша у афінних координатах

$P_1(X_1:Y_1:Z_1)$,

$P_2(X_2:Y_2:1)$,

$$P_1\left(X_1/Z_1^2, Y_1/Z_1^3\right)\neq P_2\left(X_2/Z_2^2, Y_2/Z_2^3\right),$$

процедура додавання виконується згідно виразів:

(19) UA (11) 38400 (13) U

$X_3=a\cdot E+A\cdot(A+Z_3)+B^2\cdot B$;
$Y_3=X_3\cdot(A+Z_3)+E\cdot(X_2\cdot Y_1+D\cdot X_1)$;
$Z_3=B\cdot Z_1$,
де

$C=Z_1^2$;

$D=Y_2\cdot Z_1$;
$A=Y_1+C\cdot D$;
$B=X_1+X_2\cdot C$;

$E=Z_3^2$.

Недоліком цього способу є те, що додавання точок кривої залежить від параметру кривої a, що не дозволяє використовувати однакову процедуру додавання точок при використанні різних кривих, а також вимагає великої кількості операцій, що виконуються за допомогою послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, згідно алгоритму додавання точок.

Найбільш близьким по сукупності ознак до запропонованого технічним рішенням, обраним як прототип, є спосіб визначення суми двох точок еліптичної кривої над полем $GF(2^n)$ у проективних координатах Лопеса-Дахаба [2], що ґрунтується на виконанні процедури додавання двох точок, за допомогою послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $CF(2^n)$, згідно алгоритму додавання точок, а при обчисленні суми двох точок користуються проективними координатами Лопеса-Дахаба.

Проективній точці (X:Y:Z), $Z\neq 0$, ставиться у відповідність точка з афінними координатами $(X/Z, Y/Z^2)$. Еліптична крива E над $GF(2^n)$ має вигляд

$Y^2+XYZ=X^3Z+aX^2Z^2+bZ^4$,

де $a,b \in GF(2^n)$ при $b\neq 0$.

Процедура додавання двох точок кривої у проективних координатах у випадку

$P_1(X_1:Y_1:Z_1)\neq P_2(X_2:Y_2:Z_2)$

виконується згідно виразів:

$X_3=A^2+B^2\cdot(D+a\cdot C^2)+A\cdot D$;

$$Y_3 = Z_3\cdot\left(X_3+B^2\cdot Y_2Z_1^2\right)+A\cdot B\cdot\left(X_1Z_2\cdot Z_3+X_3\cdot B^2\right);$$

$Z_3=D^2$,
де

$$A = Y_1\cdot Z_2^2+Y_2\cdot Z_1^2;$$

$$B = X_1\cdot Z_2+X_2\cdot Z_1;$$

$C=Z_1\cdot Z_2$;
$D=B\cdot C$,
у випадку
$P_1(X_1:Y_1:Z_1) = P_2(X_2:Y_2:Z_2)$
й

$$P_1\left(X_1/Z_1, Y_1/Z_1^2\right) = P_2\left(X_2/Z_2, Y_2/Z_2^2\right)$$

процедура додавання виконується згідно виразів

$$X_3 = X_1^4 = b\cdot Z_1^4;$$

$$Y_3 = bZ_1^4\cdot Z_3+X_3\cdot\left(a\cdot Z_3+Y_1^2+bZ_1^4\right);$$

$$Z_3 = (X_1\cdot Z_1)_2.$$

у випадку, коли одна з точок подана у проективних координатах, а інша в афінних координатах

$P_1(X_1:Y_1:Z_1)$,
$P_2(X_2:Y_2:1)$,

$$P_1\left(X_1/Z_1, Y_1/Z_1^2\right)\neq P_2\left(X_2/Z_2, Y_2/Z_2^2\right).$$

процедура додавання виконується згідно виразів

$$X_3 = A^2+A\cdot C+(C+a\cdot Z_1^2)\cdot B^2;$$

$Y_3=(X_2\cdot Z_3+X_3)\cdot AC+(X_3+Y_2\cdot Z_3)\cdot Z_3$;
де

$$A = Y_1+Y_2\cdot Z_1^2;$$

$B=X_1+X_2\cdot Z_1$,
$C=Z_1\cdot B$.

Недоліком цього способу є те, що додавання точок кривої залежить від параметру кривої α, що не дозволяє використовувати однакову процедуру додавання точок при використанні різних кривих, а також вимагає великої кількості операцій, що виконуються за допомогою послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, згідно алгоритму додавання точок.

В основу корисної моделі поставлена задача створення способу визначення суми двох точок еліптичної кривої над полем $GF(2^n)$ у проективних координатах, який дозволив би звільнитися залежності від параметру кривої та виконувати меншу кількість операцій за допомогою послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $gGF(2^n)$, згідно алгоритму додавання точок.

Технічний результат, який може бути отриманий при здійснені винаходу полягає в можливості звільнитися від залежності параметру кривої a та зниження обчислювальної складності завдяки виконанню процедури додавання двох точок з меншою кількістю операцій за допомогою послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, згідно алгоритму додавання точок.

Сутність запропонованого способу визначення суми двох точок еліптичної кривої над двійковим розширеним полем у проективних координатах полягає в виконанні процедури додавання двох точок, за допомогою послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, згідно алгоритму додавання точок, а при обчисленні суми двох точок користуються проективними координатами, який відрізняється від способу-прототипу додатковим включенням тимчасових змінних, які зберігаються у відповідних пристроях, виконанням над ними послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$ та відсутністю залежності від параметру кривої a.

Процедуру додавання у випадку

$$P_1\left(X_1:Z_1:Y_1:Z_1^2\right)\neq P_2\left(X_2:Z_2:Y_2:Z_2^2\right)$$

виконують згідно виразів:
$X_3=D\cdot(G+J)+E\cdot(F+H)$;
$Y_3=A\cdot B\cdot(K\cdot D+X_3)+(F\cdot K^2+X_3\cdot Z_3)$;
$Z_3=K\cdot C$,

де
$D=X_1 \cdot Z_2$;
$E=X_2 \cdot Z_1$;
$F = Y_1 \cdot Z_2^2$;
$G = Y_2 \cdot Z_1^2$;
$A=D+E$;
$B=F+G$;
$C=Z_1 \cdot Z_2$;
$H=D^2$;
$J=E^2$;
$K=A^2=H+J$.
У випадках

$$P_1\left(X_1 : Z_1 : Y_1 : Z_1^2\right) = P_2\left(X_2 : Z_2 : Y_2 : Z_2^2\right)$$

й

$$P_1\left(X_1 / Z_1, Y_1 / Z_1^2\right) \neq P_2\left(X_2 / Z_2, Y_2 / Z_2^2\right)$$

процедуру додавання виконують згідно виразів:

$$X_3 = X_1^4 + b \cdot Z_1^4;$$

$$Y_3 = bZ_1^4 \cdot Z_3 + X_3 \cdot \left(a \cdot Z_3 + Y_1^2 + bZ_1^4\right);$$

$$Z_3 = X_1^2 \cdot Z_1^2.$$

Якщо одна з точок подана в проективних координатах, а інша в афінних:

$$P_1\left(X_1 : Z_1 : Y_1 : Z_1^2\right),$$

$$P_2(X_2 : Z_2 : 1 : 1),$$

$$P_1\left(X_1 / Z_1, Y_1 / Z_1^2\right) \neq P_2\left(X_2 / Z_2, Y_2 / Z_2^2\right),$$

то процедуру додавання виконують згідно виразів:
$X_3=X_1 \cdot (G+J)+E \cdot (Y_1+H)$;
$Y_3=A \cdot B \cdot (K \cdot X_1+X_3)+(F \cdot K^2+X_3 \cdot Z_3)$;
де
$Z_3=K \cdot X_1+X_3)$;
$G = Y_2 \cdot Z_1^2$;
$A=X_1+E$;
$B=Y_1+G$;
$H = X_1^2$;
$J=E^2$;
$K=A^2=H=J$.

У таблиці 1 наведено кількість пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, у порівнянні з відомим способом [1] та у порівнянні зі способом-прототипом [2]. У таблиці позначено: «^2» - кількість операцій піднесення до квадрату; «*» - кількість операцій добутку; «+» - кількість операцій додавання.

Таблиця 1

Порівняльна таблиця за кількістю операцій над елементами двійкового розширеного поля

Система координат	Загальне додавання			Загальне додавання (змішані координати)			Подвоєння		
	^2	*	+	^2	*	+	^2	*	+
Відомий спосіб [1]	5	15	8	3	11	8	5	5	4
Відомий спосіб-прототип [2]	6	15	8	4	10	8	6	5	4
Запропонований спосіб	5	13	9	4	10	9	5	5	4

Таким чином, за рахунок додаткового включення тимчасових змінних, які зберігаються у відповідних пристроях, виконанням над ними послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів поля $GF(2^n)$, вдається на [1] операцію піднесення до квадрату, 1 операцію добутку зменшити кількість виконуваних операцій з елементами поля $GF(2^n)$ та уникнути залежності від параметру кривої α.

На Фіг.. показана схема електрична структурна пристрою визначення двох точок еліптичної кривої над двійковим розширеним полем у проективних координатах запропонованим способом. Визначення двох точок еліптичної кривої виконується наступним чином.

Виконується обчислення тимчасової змінної D, яка дорівнює добутку координати X точки P_1, на координату Z точки P_2:
$D=X_1 \cdot Z_2$.

Виконується обчислення тимчасової змінної E, яка дорівнює добутку координати X точки P_2 на координату Z точки P_1:
$E=X_1 \cdot Z_2$. Виконується обчислення тимчасової змінної F, яка дорівнює добутку координати Y точки P_1 на квадрат координати Z точки P_2:

$$F = Y_1 \cdot Z_2^2.$$

Виконується обчислення тимчасової змінної G, яка дорівнює добутку координати Y точки P_2 на квадрат координати Z точки P_1:

$$G = Y_2 \cdot Z_1^2.$$

Виконується обчислення тимчасової змінної A, яка дорівнює сумі тимчасових змінних D та E:
$A=D+E$.

Виконується обчислення тимчасової змінної 5, яка дорівнює сумі тимчасових змінних F та G:
$B=F+G$.

Виконується обчислення тимчасової змінної C, як добуток Z координат точок:
$C=Z_1 \cdot Z_2$.

Виконується обчислення тимчасової змінної H, як квадрат тимчасової змінної D:
$H=D^2$.

Виконується обчислення тимчасової змінної J, як квадрат тимчасової змінної E:

$J=E^2$.

Виконується обчислення тимчасової змінної K, як сума тимчасової змінної Я та тимчасової змінної:

$K=A^2=H+J$.

Виконується обчислення Z координати результуючої точки P_3, як добуток тимчасової змінної K та тимчасової змінної C:

$Z_3=K\cdot C$.

Виконується обчислення X координати результуючої точки P_3, як сума добутку тимчасової змінної D на суму тимчасових змінних G та J, з добутком тимчасової змінної E на суму тимчасових змінних F та H:

$X_3=D\cdot(G+J)+E\cdot(F+H)$.

Виконується обчислення Y координати точки P_3, як сума добутків тимчасової змінної A, B з сумою X координати точки P^ з добутком тимчасових змінних K і D, та тимчасової змінної F з квадратом тимчасової змінної K, а також добутку X_3 на Z_3 координат результуючої точки P_3:

$Y_3=A\cdot B\cdot(K\cdot D+X_3)+F\cdot K^2+X_3\cdot Z_3)$.

Спосіб визначення суми двох точок еліптичної кривої над полем $GF(2^n)$ у проективних координатах у випадку $P_1 = P_2$ та

$$P_1\left(X_1/Z_1, Y_1/Z_1^2\right)=P_2\left(X_2/Z_2, Y_2/Z_2^2\right),$$

може бути реалізований у наступній послідовності. Виконується обчислення тимчасової змінної A, яка дорівнює квадрату координати X точки P_1:

$$A = X_1^2.$$

Виконується обчислення тимчасової змінної B, яка дорівнює квадрату координати Z точки $B = Z_1^2$.

Виконується обчислення тимчасової змінної C, яка дорівнює квадрату тимчасової змінної A:

$C=A^2$.

Виконується обчислення тимчасової змінної Z), яка дорівнює добутку квадрата тимчасової змінної B на коефіцієнт кривої b:

$D=b\cdot B^2$.

Виконується обчислення X координати результуючої точки P_3, як добуток тимчасової змінної A на B:

$Z_2=A\cdot B$.

Виконується обчислення X координати результуючої точки P_3, як сума тимчасової змінної C та D:

$X_3=C+D$.

Виконується обчислення Y координати точки P_3, як сума добутку Z координати точки P_3 на тимчасову змінну D, та добутку X координати точки P_3 на дужки, в дужках - сума добутку коефіцієнту кривої a на Z координати точки Д, квадрату У координати точки P_1 та тимчасової змінної D:

$Y_3=D\cdot Z_3+X_3\cdot(\alpha\cdot Z_3+Y_1^2+D)$.

Спосіб визначення суми двох точок еліптичної кривої над полем $GF(2^n)$ у проективних координатах у випадку, якщо одна з точок подана у проективних координатах, а інша у афінних координатах

$$P_1\left(X_1:Z_1:Y_1:Z_1^2\right),$$

$$P_2(X_2:Y_2:1:1),$$

$$P_1\left(X_1/Z_1, Y_1/Z_1^2\right)\neq P_2\left(X_2/Z_2, Y_2/Z_2^2\right),$$

може бути реалізований наступним чином. Виконується обчислення тимчасової змінної E, яка дорівнює добутку координати X точки P_2 та добутку координати Z точки P_1:

$E=X_2\cdot Z_1$.

Виконується обчислення тимчасової змінної G, яка дорівнює добутку координати X точки P, та координати Z точки P_1:

$E=X_2\cdot Z_1$.

Виконується обчислення тимчасової змінної A, яка дорівнює сумі тимчасової змінної E та координати X точки P_1:

$A=X_1+E$.

Виконується обчислення тимчасової змінної B, яка дорівнює сумі тимчасової змінної G та координати Y точки P_1.

$B=Y_1+G$.

Виконується обчислення тимчасової змінної Я, яка дорівнює квадрату координати X точки P_1 :

$Z_3 = K\cdot Z_1$.

Виконується обчислення тимчасової змінної J, яка дорівнює квадрату тимчасової змінної E:

$J=E^2$,

Виконується обчислення тимчасової змінної K, яка дорівнює сумі тимчасової змінної H та J:

$K=A^2=H+J$.

Виконується обчислення Z координати результуючої точки P_3, як добуток тимчасової змінної K та координати Z точки P_1:

$Z_3=A\cdot Z_1$.

Виконується обчислення X координати результуючої точки P_3, як сума добутків координати X точки P_1 з сумою тимчасових змінних G та J, та добутку тимчасової змінної E з сумою координати Y точки P_1 та тимчасової змінної H:

$X_3=X_1\cdot(G+J)+E\cdot(Y_1+H)$.

Виконується обчислення У координати точки P_3, як сума добутків тимчасової змінної A, B з сумою добутку тимчасової змінної K з координатою X точки P_1, та X координати точки P_3, та координати Y точки P_1 з квадратом тимчасової змінної K, а також добутку X_3 на Z_3 координат результуючої точки P_3:

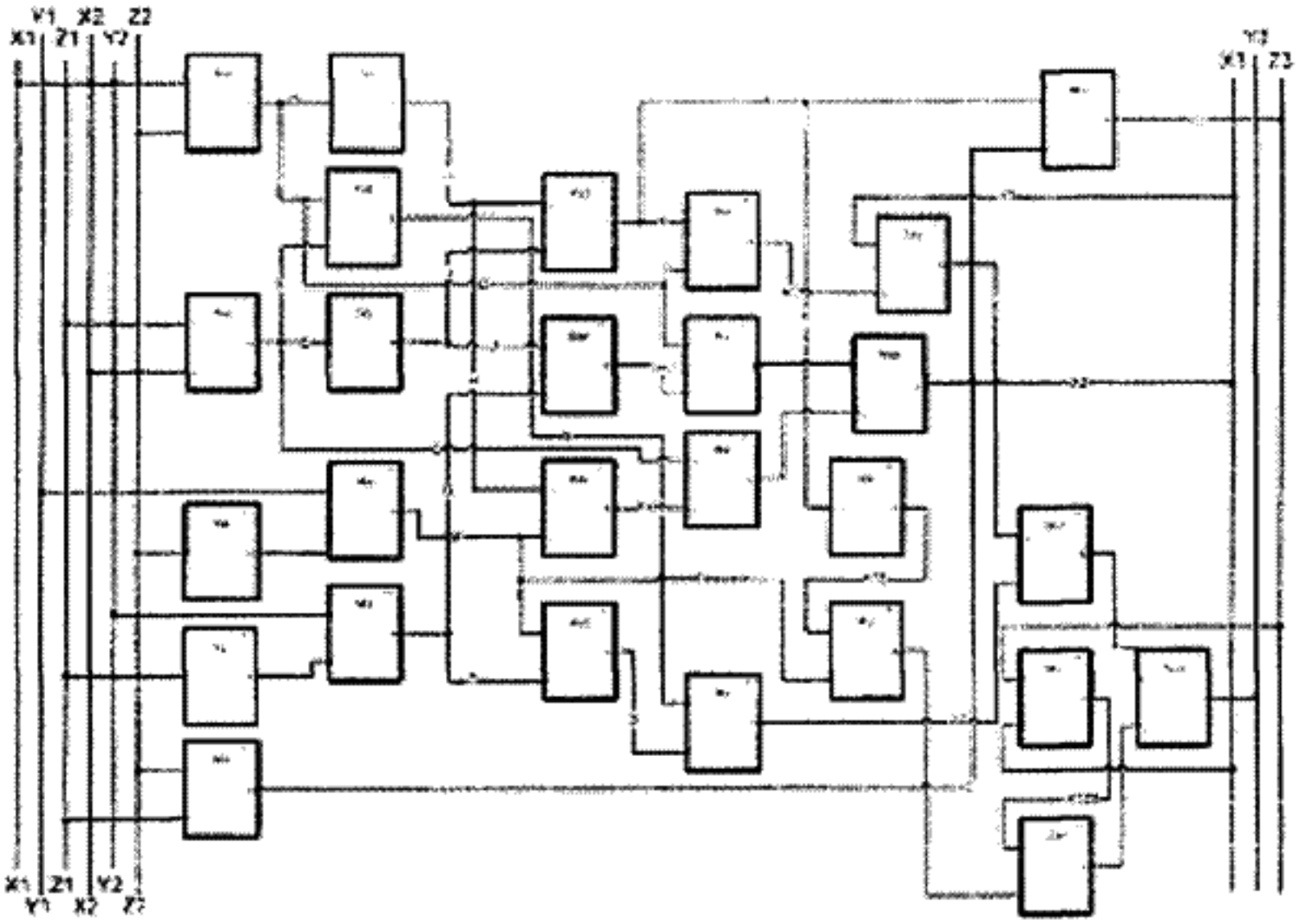
$Y_3=A\cdot B\cdot(K\cdot X_1+X_3)+(Y\cdot K^2+X_3\cdot Z_3)$.

Таким чином, за рахунок додаткового включення тимчасових змінних, які зберігаються у відповідних пристроях, виконанням над ними послідовної дії пристроїв „добуток", „піднесення до квадрату" та „додавання" елементів двійкового розширеного поля, вдається зменшити кількість виконуваних операцій з елементами двійкового розширеного поля та уникнути залежності від параметру кривої.

Джерела інформації:

1. D.V. Chudnovsky, G.V. Chudnovsky, Sequence of number generated by addition in formal group and new primal ity and factorization test, Advanced in Applied Math., 7 (1987), 385-434.

2. J. Lopez and R. Dahab, Improved algorithms for elliptic curve arithmetic's in $GF(2^n)$, Selected Areas in Cryptography -SAC'98, LNCS 1556, 1999, 201-212.



Фіг.

Комп'ютерна верстка Н. Лисенко Підписне Тираж 28 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601

Форма П12 (КМ)

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ
ДЕРЖАВНЕ ПІДПРИЄМСТВО
"УКРАЇНСЬКИЙ ІНСТИТУТ ПРОМИСЛОВОЇ ВЛАСНОСТІ"
(УКРПАТЕНТ)
ВІДДІЛЕННЯ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ РЕЄСТРАЦІЇ

вул. Глазунова, 1, м. Київ-42, 01601, Україна Тел.: (044) 494-05-68 www.sdip.gov.ua

26 СІЧ 2009 № 16377/11

Є всеєв С.П., вул. Ком. Корка, 12, кв. 212,
м. Харків, 61148, Україна

Стосовно видачі патенту України на корисну
модель № **38400**
заявка № u200810866 від 03.09.2008

Направляємо Вам патент України на корисну модель № **38400**

Збір за 1-й рік чинності патенту у розмірі 15,00 грн. (код - 13901) Вам необхідно сплатити до 12.05.2009р.

Розмір і порядок сплати зборів за підтримання чинності визначається Порядком сплати зборів за дії, пов'язані з охороною прав на об'єкти інтелектуальної власності, затвердженим Постановою Кабінету Міністрів України від 23 грудня 2004 року № 1716 із змінами і доповненнями, внесеними постановою Кабінету Міністрів України від 19 вересня 2007 року № 1148.

Сплата зборів за підтримання чинності наперед не передбачена.

Збір за кожний наступний рік сплачується відповідно до ст. 32 Закону "Про охорону прав на винаходи та корисні моделі" протягом останніх 4-х місяців поточного року дії.

Строк дії патенту відраховується від дати подання заявки.

УВАГА!

У зв'язку зі вступом України до Світової Організації Торгівлі з 16.05.2008 року розміри зборів змінилися згідно з Постановою Кабінету Міністрів України від 19 вересня 2007 року № 1148 "Про внесення змін до Порядку сплати зборів за дії, пов'язані з охороною прав на об'єкти інтелектуальної власності".

Реквізити для сплати зборів:

Отримувач:	**Призначення платежу:**
ДП "Український інститут промислової власності" код ЗКПО 31032378 АБ "Брокбізнесбанк" м.Київ Р/р 2600401457 МФО 300249	Збір 13901, підтримання чинності ПУ 38400 - 15,00 грн

Начальник Відділення **С.В. Лященко**