УКРАЇНА UKRAINE

# ПАТЕНТ

## НА КОРИСНУ МОДЕЛЬ

## № 39675

**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 **10.03.2009.**

Голова Державного департаменту інтелектуальної власності М.В. Паладій

Міністерство освіти і науки України * Державний департамент інтелектуальної власності * № 1

(11) **39675**

(19) **UA**

(51) **МПК**
*G06F 7/04* **(2008.04)**

(21) Номер заявки: **u 2008 10864**

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

(24) Дата, з якої є чинними права на корисну модель: **10.03.2009**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **10.03.2009, Бюл. № 5**

(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, що виконують функції 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 включають тимчасові змінні, які зберігаються у відповідних пристроях, та виконують над ними послідовні дії пристроїв, що виконують функції добуток, піднесення до квадрата та додавання елементів двійкового розширеного поля.

Пронумеровано, прошито металевими
люверсами та скріплено печаткою
2 арк.
10.03.2009

Міністерство освіти і науки України * Державний департамент інтелектуальної власності * № 1

Уповноважена особа

(підпис)

УКРАЇНА

(19) UA (11) 39675 (13) U

(51) МПК
*G06F 7/04* (2008.04)

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)** u200810864
**(22)** 03.09.2008
**(24)** 10.03.2009
**(46)** 10.03.2009, Бюл.№ 5, 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, що виконують функції 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 включають тимчасові змінні, які зберігаються у відповідних пристроях, та виконують над ними послідовні дії пристроїв, що виконують функції добуток, піднесення до квадрата та додавання елементів двійкового розширеного поля.

1 2

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

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

де $\alpha, b\in GF(2^n)$ 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:

$X_3=A\cdot(A+Z_3)+B^2\cdot B+\alpha\cdot Z^2_3$;

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

$Z_3=C\cdot Z_2$,

де

$A=Y_1\cdot Z^3_2+Y_2\cdot Z^3_1$;

$B=X_1\cdot Z^2_2+X_2\cdot Z^2_1$;

у випадку

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

й

$P_1(X_1/Z^2_1, Y_1/Z^3_1)=P_2(X_2/Z^2_2, Y_2/Z^3_2)$

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

$A=X^2_1$;

$B=Z^2_1$;

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

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

$P_1(X_1:Y_1:Z_1)$,

$P_2(X_2:Y_2:1)$,

$P_1(X_1/Z^2_1, Y_1/Z^3_1)\neq P_2(X_2/Z_2{}^2, Y_2/Z^3_2)$,

процедура додавання виконується згідно виразів:

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

$Y_3=X_3\cdot(A+Z_3)+E\cdot(X_2\cdot Y_1+D\cdot X_1)$;

$Z_3=B\cdot Z_1$,

де

$C=Z^2_1$;

$D=Y_2\cdot Z_1$;

$A=Y_1+C\cdot D$;

$B=X_1+X_2\cdot C$;

$E=Z^2_3$.

(19) UA (11) 39675 (13) U

Недоліком цього способу є те, що додавання точок кривої 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 $GF(2^n)$, 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

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

де $\alpha, b\in GF(2^n)$ 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:

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

$Y_3=Z_3\cdot(X_3+B^2\cdot Y_2Z^2{}_1)+A\cdot B\cdot(X_1Z_2\cdot Z_3+X_3\cdot B^2);$

$Z_3=D^2,$

де

$A=Y_1\cdot Z^2{}_2+Y_2\cdot Z^2{}_1;$

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

$C=Z_1\cdot Z_2;$

$D=B\cdot C,$

у випадку

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

й

$P_1(X_1/Z_1, Y_1/Z^2{}_1)=P_2(X_2/Z_2, Y_2/Z^2{}_2)$

процедура додавання виконується згідно виразів

$X_3=X^4{}_1+b\cdot Z^4{}_1;$

$Y_3=bZ^4{}_1\cdot Z_3+X_3\cdot(a\cdot Z_3+Y^2{}_1+bZ^4{}_1);$

$Z_3=(X_1\cdot Z_1)^2,$

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

$P_1(X_1:Y_1:Z_1),$

$P_2(X_2:Y_2:1),$

$P_1(X_1/Z_1, Y_1/Z^2{}_1)\neq P_2(X_2/Z_2, Y_2/Z^2{}_2),$

процедура додавання виконується згідно виразів

$X_3=A^2+A\cdot C+(C+a\cdot Z^2{}_1)\cdot B^2;$

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

$Z_3=C^2,$

де

$A=Y_1+Y_2\cdot Z^2{}_1;$

$B=X_1+X_2\cdot Z_1,$

$C=Z_1\cdot B.$

Недоліком цього способу є те, що додавання точок кривої 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 виконувати меншу кількість операцій за допомогою послідовної дії пристроїв добуток, піднесення до квадрату та додавання елементів поля $GF(2^n)$, згідно алгоритму додавання точок.

Технічний результат, який може бути отриманий при здійснені корисної моделі полягає в отриманні можливості 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, та виконанням над ними послідовної дії пристроїв добуток, піднесення до квадрату та додавання елементів поля $GF(2^n)$.

Процедуру додавання у випадку

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

виконують згідно виразів:

$X_3=A^2+I+J+\alpha\cdot Z_3;$

$Y_3=X_3\cdot(I+Z_3)+J\cdot C\cdot(G\cdot F+H\cdot E);$

$Z_3=D^2,$

де

$A=E+F;$

$B=G+H;$

$C=Z_1\cdot Z_2;$

$D=B\cdot C;$

$E=Y_1\cdot Z^2{}_2;$

$F=Y_1\cdot Z^2{}_1;$

$G=X_1\cdot Z_2;$

$H=X_2\cdot Z_1;$

$I=A\cdot D;$

$J=B^2\cdot D.$

У випадках

$P_1(X_1:Y_1:Z_1:Z^2{}_1)=P_2(X_2:Y_2:Z_2:Z^2{}_2)$

й

$P_1(X_1/Z_1, Y_1/Z^2{}_1)=P_2(X_2/Z_2, Y_2/Z^2{}_2)$

процедуру додавання виконують згідно виразів:

$X_3=X^4{}_1+b\cdot Z^4{}_1;$

$Y_3=bZ^4{}_1\cdot Z_3+X_3\cdot(a\cdot Z_3+Y^2{}_1+bZ^4{}_1);$

$Z_3=X^2{}_1\cdot Z^2{}_1.$

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

$P_1(X_1:Y_1:Z_1:Z^2{}_1),$

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

$P_1(X_1/Z_1, Y_1/Z^2{}_1)\neq P_2(X_2/Z_2, Y_2/Z^2{}_2),$

то процедуру додавання виконують згідно виразів:

$X_3=A^2+D+C\cdot B^2+a\cdot Z_3;$

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

$Z_3=C^2$;
де
$A=Y_1+Y_2\cdot Z^2_1$;
$B=X_2+X_2\cdot Z_1$;
$C=Z_1\cdot B$;
$D=A\cdot C$.

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 | 4 | 14 | 8 | 4 | 10 | 8 | 5 | 5 | 4 |

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

На Фіг.1 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 E, яка дорівнює добутку координати Y точки $P_1$ на квадрат координати Z точки $P_2$:

$E=Y_1\cdot Z^2_2$.

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

$F=Y_2\cdot Z^2_1$.

Виконується обчислення тимчасової змінної G, яка дорівнює добутку координати X точки $P_2$ на координату Z точки $P_2$:

$G=X_1\cdot Z_2$.

Виконується обчислення тимчасової змінної H, яка дорівнює добутку координати X точки $P_2$ на координату Z точки $P_1$:

$H=X_2\cdot Z_1$.

Виконується обчислення тимчасової змінної A, яка дорівнює сумі тимчасових змінних E та F:

$A=E+F$.

Виконується обчислення тимчасової змінної B, яка дорівнює сумі тимчасових змінних G та H:

$B=G+H$.

Виконується обчислення тимчасової змінної C, як добуток Z координат точок:

$C=Z_1\cdot Z_2$.

Виконується обчислення тимчасової змінної D, як добуток тимчасових змінних B та C:

$D=B\cdot C$.

Виконується обчислення тимчасової змінної I, як добуток тимчасових змінних A та D:

$I=A\cdot D$.

Виконується обчислення тимчасової змінної J, як добуток квадрату тимчасової змінної B та тимчасової змінної D:

$J=B^2\cdot D$.

Виконується обчислення Z координати результуючої точки $P_3$, як квадрат тимчасової змінної D:

$Z_3=D^2$.

Виконується обчислення X координати результуючої точки $P_3$, як сума квадрату тимчасової змінної A з тимчасовими змінними I, J та добутку коефіцієнту кривої a на Z координату точки $P_3$:

$X_3=A^2+I+J+a\cdot Z_3$.

Виконується обчислення Y координати точки $P_3$, як сума добутку X координати точки $P_3$ на дужки, в дужках - сума тимчасової змінної I та Z координати точки $P_3$, та добутку тимчасових змінних J, C на дужки, в дужках - сума добутку тимчасових змінних G на F та добутку тимчасових змінних H на E:

$Y_3=X_3\cdot(I+Z_3)+J\cdot C\cdot(G\cdot F+H\cdot E)$.

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

$P_1(X_1/Z_1, Y_1/Z^2_1)=P_2(X_2/Z_2, Y_2/Z^2_2)$,

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

$A=X^2_1$.

Виконується обчислення тимчасової змінної B, яка дорівнює квадрату координати Z точки $P_1$:

$B=Z^2_1$.

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

$C=A^2$.

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

$D=b\cdot B^2$.

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

$Z_3=A\cdot B$.

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

$X_3=C+D$.

Виконується обчислення Y координати точки $_3$, як сума добутку Z координати точки $P_3$ на тимасову змінну D, та добутку X координати точки $P_3$ а дужки, в дужках - сума добутку коефіцієнту кривої a на Z координати точки $P_3$, квадрату Y координати точки $P_1$, та тимчасової змінної D:

$Y_3=D\cdot Z_3+X_3\cdot(a\cdot Z_3+Y^2_1+D)$.

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

$P_1(X_1:Y_1:Z_1:Z^2_1)$,

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

$P_1(X_1/Z_1,Y_1/Z^2_1)\neq P_2(X_2/Z_2,Y_2/Z^2_2)$,

може бути реалізований наступним чином. Виконується обчислення тимчасової змінної A, яка орівнює сумі координати Y точки $P_1$ та добутку оординати Y точки $P_2$ на квадрат координати Z очки $P_1$:

$A=Y_1+Y_2\cdot Z^2_1$.

Виконується обчислення тимчасової змінної B, ка дорівнює сумі координати X точки $P_1$ та координати Y точки $P_1$ та добутку координати X точки $_2$ на координату Z точки $P_1$:

$B=X_1+X_2\cdot Z_1$.

Виконується обчислення тимчасової змінної C, ка дорівнює добутку тимчасової змінної B на координату Z точки $P_1$:

$C=Z_1\cdot B$.

Виконується обчислення тимчасової змінної D, ка дорівнює добутку тимчасової змінної A на тимасову змінну C:

$D=A\cdot C$.

Виконується обчислення Z координати результуючої точки $P_3$, як квадрат тимчасової змінної C:

$Z_3=D^2$.

Виконується обчислення X координати результуючої точки $P_3$, як сума квадрату тимчасової змінної A, тимчасової змінної D, добутку тимчасової змінної C на квадрат тимчасової змінної B, та добутку коефіцієнту кривої $\alpha$ на Z координати точки $P_3$:

$X_1=A^2+D+C\cdot B^2+\alpha\cdot Z_3$.

Виконується обчислення Y координати точки $P_3$, як сума добутку Z координати точки $P_3$ на дужки, в дужках сума добутку тимчасової змінної D на X координату точки $P_3$, та добутку X координати точки $P_3$ на дужки, в дужках - сума тимчасової змінної D та Z координати точки $P_3$:

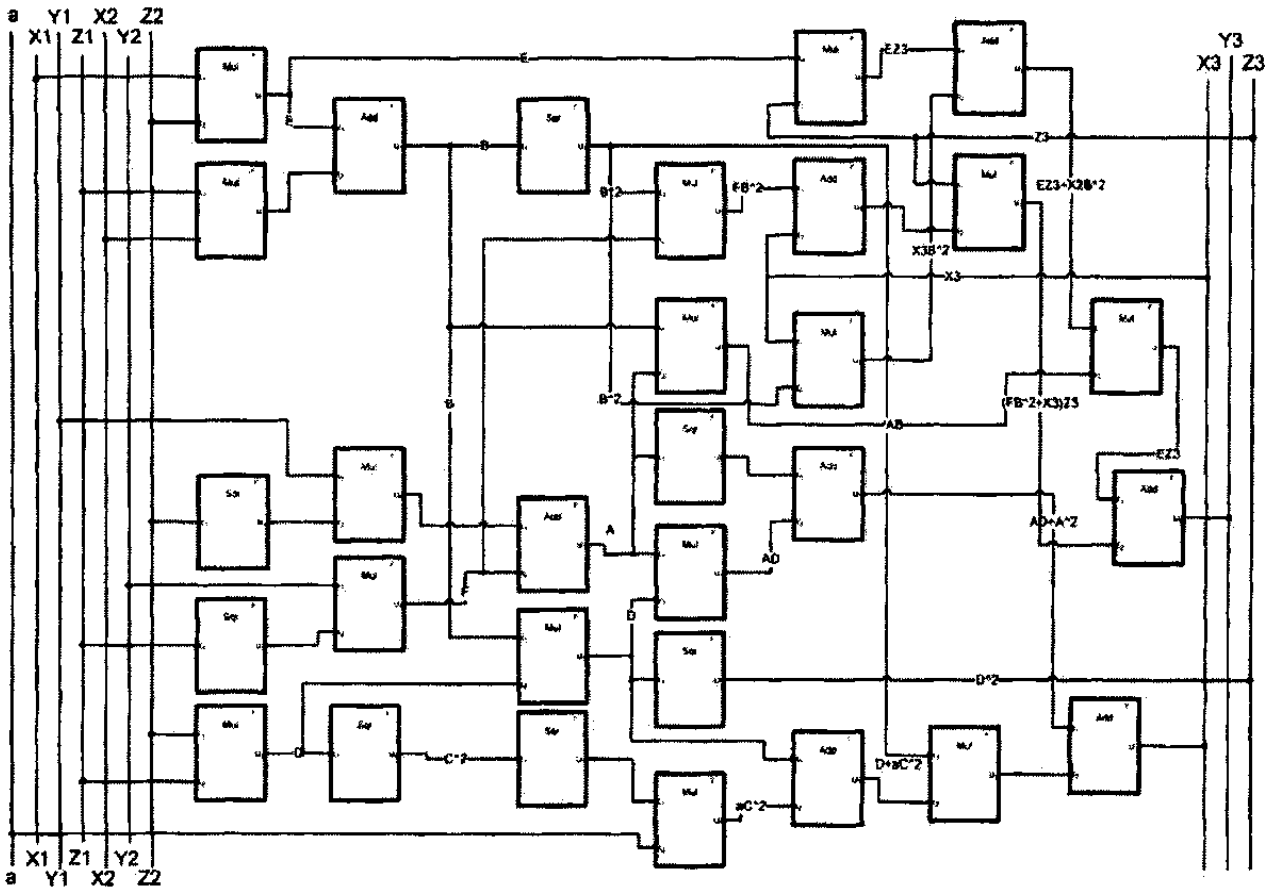
$Y_3=Z_3\cdot(X_2\cdot D+Y_2\cdot Z_3)+X_3\cdot(D+Z_3)$.

Таким чином, за рахунок додаткового включення тимчасових змінних, які зберігаються у відповідних пристроях, та 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.

Джерела інформації:

1. D.V. Chudnovsky, G.V. Chudnovsky, Sequence of number generated by addition in formal group and new primality 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 С.Литвиненко 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