УДК 004.382

В.С. ГЛУХОВ, М.В. НОГАЛЬ

Національний університет "Львівська політехніка", Україна

СПЕЦІАЛІЗОВАНИЙ ОДНОРОЗРЯДНИЙ ПРОЦЕСОР ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ГАРАНТОЗДАТНИХ СИСТЕМАХ

У статті досліджується можливість використання однорозрядного ядра спеціалізованого процесора в складі гарантоздатних апаратних засобів, що виконують операції над елементами полів Галуа GF(2^m), представленими у нормальному базисі, у відповідності до алгоритму цифрового підпису, який ґрунтується на еліптичних кривих (Elliptic Curve Digital Signature Algorithm (ECDSA)).

захист інформації, скінченні поля Галуа, нормальний базис, додавання і множення в полях Галуа, однорозрядний процесор

Вступ

Від комп'ютерних засобів інтегрованих систем керування завжди крім рішення основної задачі керування вимагалося виконання додаткової вимоги, а саме забезпечення надійності.

Поняття гарантоздатності виросло з поняття надійності і містить як характеристики традиційно надійних систем (власне показники надійності, показники готовності до роботи, характеристики безперервність роботи та інші), так і нові вимоги, які раніше до поняття надійності не входили, серед них – конфіденційність та цілісність, недоторканість. Їх виконання забезпечується використанням відповідних криптографічних засобів. Одним з засобів є використання цифрового підпису. В основі метода лежить використання полів Галуа GF(2^m) та обчислень над точками еліптичних кривих.

У даній роботі досліджується можливості використання у складі криптографічних засобів гарантоздатних систем однорозрядного ядра спеціалізованого процесора при проведенні обчислень над елементами поля GF(2^m) у нормальному базисі.

Аналіз публікацій і окреслення проблеми. Термін «надійність» в його сучасному розумінні набуває відтінку «довірчості», тобто мова в даному випадку йде про «довірчу надійність», що включає аспекти безпеки, класичної надійності (reliability), продуктивності і живучості в широкому діапазоні потенційних ризиків і погроз [1].

Концепція довірчої надійності практично збігається з тим, що у ряді англомовних джерел, що особливо мають відношення до американського Інституту інженерів по електротехніці і електроніці (IEEE), прийнято називати dependability («функціональна надійність» або «гарантоздатність», що забезпечує отримання достовірних результатів за наявності несправностей).

Основною теоретичною роботою в області гарантоздатних систем є спеціальний випуск журналу IEEE "Trans On Computers" 1986 р., під редакцією A.Avizienis і J.-C. Laprie [2], якими був сформульований принцип "Dependable computing" (гарантоздатних обчислень) як обчислень, стійких до відмов апаратних засобів і програмних засобів, тобто до відмов, обумовленим проявом їх дефектів, внесених при розробці і не виявлених при тестуванні. Сьогодні теорію гарантоздатнихсистем, сервісів і технологій розвиває науково-технічний центр "DeSSerT" (Dependable Systems, Services & Technologies) [3], який очолює доктор технічних наук, професор В.С. Харченко.

Система гарантоздатна, коли вона [4]:

- доступна (available) – готова для використ-

тання, коли нам потрібне це;

- надійна (reliable) – здатназабезпечити безперервність обслуговування, поки ми її використовуєм;
- безпечна (safe) – не має катастрофічного впливу на оточення;
- захищена (secure) – здатна зберегти конфіденційність (confidentity), забезпечувати недоторканість (integrity);
- ремонтопридатна (mintainability).

Гарантоздатну систему можна представити у вигляді дворівневої паралельної багатозадачної системи (рис. 1), структура якої збігається з узагальненою схемою функціонального контролю [5].

Важливу роль у забезпеченні гарантоздатності мають криптографічні засоби захисту інформації (рис. 2). Одним з них є методи отримання і перевірки цифрового підпису, стандартизовані на міжнародному [10] і вітчизняному [11] рівнях. В основі метода лежить використання полів Галуа $GF(2^m)$ та обчислень над точками еліптичних кривих. Однією з найскладніших операцій у таких полях є операція множення, відомий алгоритм Мессі-Омури для її рішення [6] та варіанти його практичного впровадження [7 – 9]. Недоліком алгоритму є великі апаратні витрати.

Рис. 1. Гарантоздатна система

Сам контрольний орган також має дворівневу структуру [7] (рис. 3).

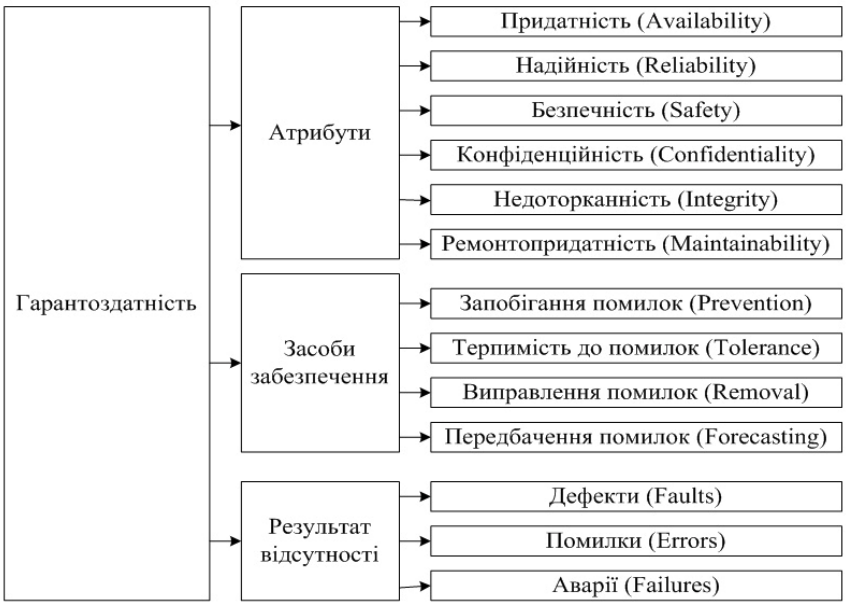

Рис. 2. Гарантоздатність

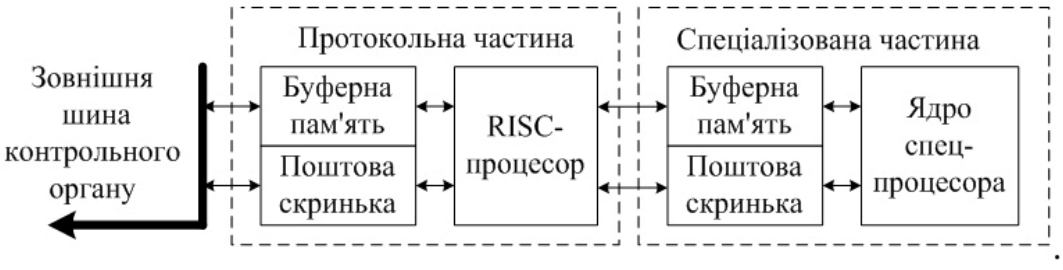

Рис. 3. Структура контрольного органу

Спеціалізована частина контрольного органу, що виконує операції над багаторозрядними елементами полів GF(2^m) у нормальному базисі вимагає великих апаратних витрат, тому актуальною є задача проектування і дослідження спеціалізованих структур з меншими апаратними витратами в порівнянні з відомими рішеннями.

Мета роботи. У даній роботі досліджується можливості використання однорозрядного ядра спеціалізованого процесора (рис. 4) при проведенні обчислень над елементами поля GF(2^m) у нормальному базисі.

Множення у нормальному базисі

Елементи $\left\{\theta, \theta^2, \theta^{2^2}, ..., \theta^{2^{m-1}}\right\}$ основного поля Галуа утворюють нормальний базис (θ – корінь полінома p, що утворює поле). Усі інші елементи основного поля Галуа можуть бути представлені у нормальному базисі у вигляді $a_0\theta + a_1\theta^2 + a_2\theta^{2^2} + ... + a_{m-1}\theta^{2^{m-1}}$, де a_i – двійкові розряди (i = 0, 1, …, m-1).

Додавання двох елементів у полі Галуа виконується як порозрядне додавання за модулем 2.

Під час множення двох елементів (x_N та y_N) поля Галуа у нормальному базисі (далі множення у нормальному базисі) потрібно виконати такі операції [10]:

- скласти систему рівнянь:

$$t = a_{0,0} + a_{0,1}t + a_{0,2}t^2 + ... + a_{0,m-1}t^{m-1} (\mathrm{mod}\ p(t));$$
$$t^2 = a_{1,0} + a_{1,1}t + a_{1,2}t^2 + ... + a_{1,m-1}t^{m-1} (\mathrm{mod}\ p(t));$$
$$t^4 = a_{2,0} + a_{2,1}t + a_{2,2}t^2 + ... + a_{2,m-1}t^{m-1} (\mathrm{mod}\ p(t));$$

……

$$t^{2^{m-1}} = a_{m-1,0} + a_{m-1,1}t + a_{m-1,2}t^2 + ...$$
$$+ a_{m-1,m-1}t^{m-1} (\mathrm{mod}\ p(t));$$

- з системи рівнянь утворити матрицю A з елементами $a_{i,j}$ (при правильно обраному поліномі, що утворює поле, детермінант матриці A $detA \neq 0$);
- у полі Галуа знайти матрицю B, обернену до A: $B=A^{-1}$, $detB \neq 0$.
- утворити допоміжну матрицю C, де c_i – коефіцієнти полінома $p(t) = t^m + c_{m-1}t^{m-1} + ...c_1t + c_0$, що утворює відповідне поле Галуа;

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,m-1} \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{m-1} \end{bmatrix};$$

- обчислити допоміжну матрицю $D = ACB$;
- з матриці D утворити помножувальну матрицю M, з елементами $\mu_{i,j} = d_{j-i,-i}$. Тоді старший розряд результату $r_{N(m\text{-}1)} = x_N * M * y_N^t$.

Наступні розряди результату ($r_{N(m\text{-}2)}$, …, $r_{N(0)}$) обчислюються за цією самою формулою, тільки замість самих векторів x_N та y_N використовуються їхні послідовні циклічні зсуви на один розряд вліво.

Нижче наведений фрагмент опису послідовності обчислення одного розряду результату $r_N(m\text{-}1) = x_N * M * y_N^t$ для примітивного полінома з p=173 при використанні правого зсуву, де позначено:

$x_N(i)$, $y_N(i)$, $s(i)$ – і-й розряд операндів x_N, y_N та проміжного результату;

o – вихід матриці (1 біт).

-- початок фрагменту обчислення:

$r_N(m\text{-}1) = x_N * M * y_N^t$

$s(172) <= y_N(172)$ *and* $(x_N(171))$;

$s(171) <= y_N(171)$ *and* $(x_N(172)$ *xor* $x_N(20))$;

...

$s(1) <= y_N(1)$ *and* $(x_N(70)$ *xor* $x_N(22))$;

$s(0) <= y_N(0)$ *and* $(x_N(21)$ *xor* $x_N(0))$;

$r_{N(m\text{-}1)} <= s(172)$ *xor* $s(171)$ *xor* ... *xor* $s(0)$;

-- кінець фрагменту.

Як видно, при виконанні множення доводиться обробляти окремі розряди двох багаторозрядних операндів. Це наштовхує на необхідність дослідження можливості використання однорозрядного

ядра спеціалізованого процесора (рис. 4) при проведенні обчислень над елементами поля GF(2^m) у нормальному базисі.

Ядро однорозрядного спеціалізованого процессора

Однорозрядний спеціалізований процесор має класичну RISC-архітектуру, його структура показана на рисунку 4. Він має в своему складі такі вузли: АЛП (виконує операції однорозрядного логічного додавання за модулем 2 XOR і однорозрядного логічного множення AND), регістровий файл (ззовні можна доступтись до 4-х регістрів по *m* розрядів, для внутрішніх команд є 4**m* днорозрядних регістрів по одному біту, 2 порти на читання і 1 на запис), лічильник команд, регістр інструкцій, пристрій керування. Система інструкцій дуже проста і складається лише з двох інструкцій, операндами для яких є регістри регістрового файлу:

and r1, *r*2, *r*3*;*

*xor r*1, *r*2, *r*3.

Ззовні процесор має шину даних , через яку можна .записати чи вичитати дані з регістрового файлу, а також шину для сигналів керування.

Розглянемо як буде виконуватись множення елементів в нормальному базисі поля Галуа. В пам'яті інструкцій міститься програма, яка буде виконувати обчислення одного розряду операції множення двох елементів в нормальному базисі поля Галуа. В регістровий файл записуємо операнди. Посилаємо сигнал про завантаження адреси початку програми в лічильник програм. Далі виконуються обчислення. Через певну кількість тактів отримаємо один розряд добутку. Процедуру повторюємо необхідну кількість раз. Результат обчислень вкінці можна вичитати з регістрового файлу.

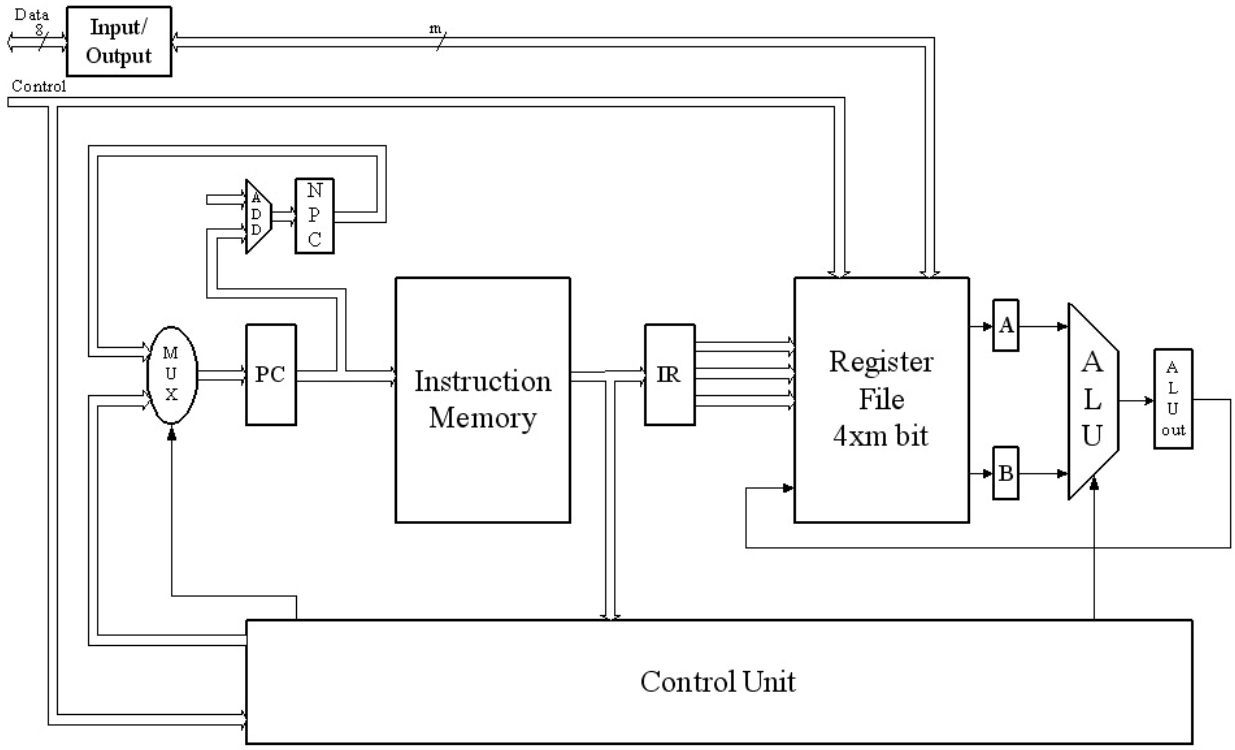

Рис. 4. Структура однорозрядного спеціалізованого процессора

Висновки

У статті проведено дослідження можливості використання однорозрядного ядра спеціалізованого процесора в складі гарантоздатних апаратних засобів, що виконують операції над елементами полів Галуа GF(2^m), представленими у нормальному базисі, у відповідності до алгоритму цифрового

підпису, який ґрунтується на еліптичних кривих (Elliptic Curve Digital Signature Algorithm (ECDSA)).

Наведено структуру гарантоздатної системи, а також структуру контрольного органу. Спеціалізована частина контрольного органу виконує операції над багаторозрядними елементами полів $GF(2^m)$ у нормальному базисі. Наведено структурну схему і опис спеціалізованого однорозрядного процесора, який проводить обчислення над елементами поля $GF(2^m)$ у нормальному базисі скінченного поля.

Література

1. Лашкарев Ю., Павлов Л., Лаврешин Г. Как обеспечить надежность банковских ИТС [Электронный ресурс]. – Режим доступа: http://www.bdm.ru/arhiv/2003/12/56-59.htm.

2. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Transactions on Dependable and Secure Computing, 2004. – Vol. 1. – P. 11-33.

3. Сайт DESSERT (Dependable Systems, Services & Technologies) [Электронный ресурс]. – Режим доступа: http:// stc-dessert.com.

4. Основи надійності цифрових систем: Підручник. Рекомендовано Міносвіти України // За ред. В.С. Харченка, В.Я. Жихарева. – Х.: ХАІ, 2004. – 573 с.

5. Локазюк В.М., Савченко Ю.Г. Надійність, контроль, діагностика і модернізація ПК: Посібник. За ред. В.М. Локазюка. К.: Академія, 2004. – С. 156.

6. Omura J. Massey J. Computational method and apparatus for finite field arithmetic. U.S. Patent Number 4,587,627. 1986. – P. 201.

7. Глухов В.С., Євтушенко К.С., Заіченко Н.В., Оліярник Б.О. Криптографічні засоби спеціалізованої бортової ЕОМ для бронетехніки // Вісник Хмельницького національного університету Хмельницький: Технічні науки, 2007. – № 2. – С. 29-33.

8. Глухов В., Заіченко Н., Оліярник Б. Шифропроцесор для бортових інформаційно-керуючих систем. Наукові нотатки. Міжвузівський збірник (за напрямком «Інженерна механіка»). Луцький державний технічний університет, Луцьк, 2007. – № 19. – С. 33-43.

9. Глухов В.С. Операційний пристрій для роботи з елементами поля Галуа, представленими у нормальній формі // Матеріали науково-технічної конференція ІППТ при НУ «Львівська політехніка». Львів, 2007. – С. 136.

10. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000.

11. ДСТУ 4145-2002. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння.

Надійшла до редакції 15.01.2008

Рецензент: д-р техн. наук, проф. О.М. Романкевич, Національний технічний університет України «КПІ», Київ.