УДК 638.322

К.т.н., доцент Тесленко О.К., магістрант Узерчук О.А.

Національний технічний університет України
«Київський політехнічний інститут»

ОПТИМІЗАЦІЯ СТРУКТУР ШВИДКОДІЮЧИХ БАГАТОРОЗРЯДНИХ СУМАТОРІВ ЗА ЗМІННИМ МОДУЛЕМ

Вступ

В Україні попит на методи і засоби захисту інформації збільшується з кожним днем. Виникла нагальна потреба використання криптографічних методів у приватному секторі. Сьогодні велика кількість інформації передається між ЕОМ звичайними лініями зв'язку. Тому вкрай потрібно розробляти нові криптографічні методи, програмне й апаратне забезпечення для гарантування таємності та цілісності закритої інформації.

Криптографія покликана обслуговувати потреби людства у дуже делікатній сфері – зберігання в таємниці конфіденційної інформації.

На теперішній час криптографія успішно використовується майже в усіх інформаційних системах – від електронної пошти до мобільного зв'язку, від баз даних до Інтернет. Без неї забезпечити потрібну ступінь конфіденційності в сучасному комп'ютерному світі вже неможливо. Крім цього за допомогою криптографії запобігають спробам шахрайства в системах електронної комерції, забезпечують законність фінансових угод. З часом її значення в навколишньому світі обіцяє стати ще більшим, і для цього у криптографії є необхідний потенціал.

Ніхто не в змозі забезпечити стовідсоткову гарантію безпеки. Проте криптографічний захист можна спроектувати так, щоб він міг протистояти атакам зловмисників до того моменту, коли інформація втрачає свою важливість, або стане простіше отримати бажану інформацію іншим шляхом. У криптографії вже давно винайдено високоефективні алгоритми і протоколи, необхідні для надійного захисту комп'ютерів та комп'ютерних мереж від електронного зламу. Ось чому в реальному житті криптографічні системи рідко зламуються винятково математичними методами. Адже конкретні реалізації криптографічного алгоритму або протоколу у вигляді працюючої програми або пристрою, як правило, можуть дуже відрізнятися по затратах та швидкодії.

Постановка задачі

Широке застосування модулярних операцій (операцій у залишках) в засобах захисту інформації з одного боку, і розвиток технології ПЛІС з іншого, актуалізує пошук ефективних апаратних реалізацій. Однією з базових операцій у залишках є операція додавання $(X+Y) \bmod P$ де X, Y та P цілі невід'ємні числа $X,Y<P$. На основі цієї операції реалізують операції $(X \times Y) \bmod P$ та $Y=A^X \bmod P$, де P – просте число, які застосовуються в значній кількості криптографічних перетворень, алгоритмів, протоколів, ЕЦП тощо. Запропонована реалізація операції додавання по змінному модулю [1] на основі логічної мережі - регулярної лінійної структури - одновимірному каскаді однотипних конструктивних модулів (ОКОКМ), де конструктивні модулі (КМ) та каскад в цілому є комбінаційними схемами. У КМ реалізується одна булева функція від 7 змінних для формування розряду результату і 4 булевих функції від 5 змінних для формування сигналів перенесення - по дві для кожного з напрямків - в сторону молодших і в сторону старших розрядів. Час T, необхідний для виконання операції додавання, пропорційний кількості n розрядів чисел X,Y,A та P- $T=n*t$, де t – затримка проходження сигналів через один КМ. Враховуючи, що реальні значення n становлять від декількох сотень до тисяч, затримка в виконанні операції може бути значною. Для суттєвого зменшення часу виконання операції додавання по змінному модулю в [2] була запропонована пірамідальна структура (рис.1) формування сигналів перенесення як в сторону молодших так і в сторону старших розрядів з використанням комбінаційної схеми асоціативної операції (КСАО) на 8 входів та 4 виходи, яка реалізує спеціально визначену асоціативну операції. Використання такої КСАО дозволяє забезпечити затримку виконання операції додавання по змінному модулю пропорційно log n.

Згідно з визначенням КМ та КСАО можна вважати, що складність реалізації та затримка сигналів цих пристроїв приблизно однакова. Тоді верхня оцінка затримки сигналу суматора з використанням КСАО складає:

$T_h = (m + log_2(n-m))t$

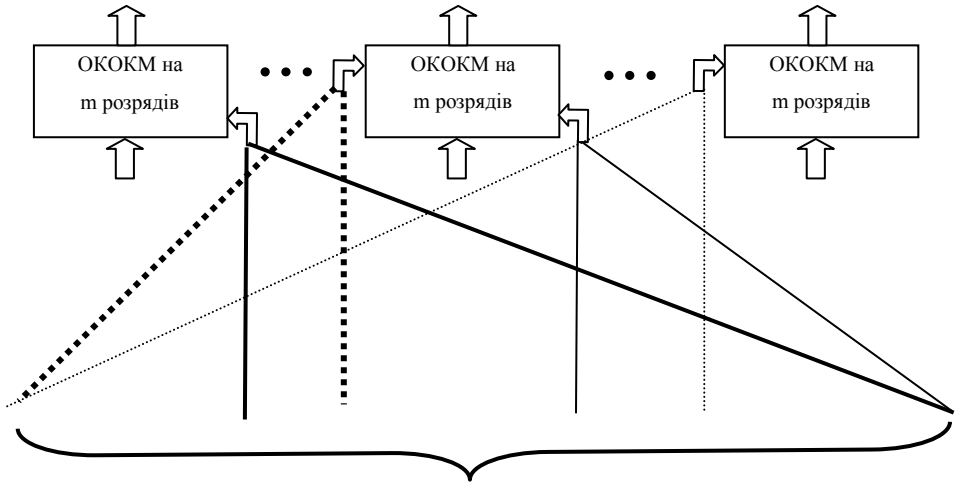
Верхня оцінка складності реалізації суматора за змінним модулем без використання КСАО - $C_h=c*n$, а з використанням КСАО:

$C_h=c*(n^2/m+n)$,

де c – складність реалізації КМ (КСАО).

Але наведена верхня оцінка складності не враховує можливість зменшення апаратних витрат за рахунок видалення КСАО які мають однакові вхідні сигнали. Тому постає задача створення алгоритму пошуку і видалення КСАО з однаковими вхідними сигналами. Ця задача може бути

вирішена шляхом розробки програмного забезпечення для моделювання всіх можливих «пірамідальних схем» і пошуку серед них оптимальної по апаратних витратах.



n-розрядні *X,Y,P (n >> m ≥ 1)*

Рис. 1. Пірамідальна структура формування сигналів переносу

Алгоритм оптимізації

Алгоритм забезпечує знаходження оптимального варіанту шляхом побудови та аналізу всіх можливих пірамідальних схем і знаходження серед них реалізації перенесень з найменшою кількістю елементів.

Кожен елемент моделі є структурою даних, в яку включено два списки - список всіх можливих варіантів пірамід від старших до молодших розрядів, і від молодших до старших. Піраміди представлені в такий спосіб: кожен елемент піраміди являє собою структуру даних з двох покажчиків, які вказують на елементи нижнього рівня. У разі відсутності елементів нижнього рівня – покажчик має нульове значення. Спочатку для кожного елемента моделі утворюється список всіх можливих пірамід, причому кількість рівнів піраміди не повинно перевищувати $r =]\log_2 q[$, де q– кількість входів піраміди. Піраміда будується таким чином: будується повна піраміда з $r =]\log_2 q[$ рівнів, далі з неї видаляються зайві для даного розряду елементи. Піраміди будуються для наступних розрядів вхідних даних (якщо розряди нумерувати з 0 до n-1): ((n-1,n-m-1),(n-1,n-2m-1),…,(n-1,n-jm-1),…,(n-1,m+1)) – в сторону молодших розрядів та ((0,m),(0,2m),…,(0,jm),…,(0,n-m-1)) – в сорону старших. Значення q пробігає ряд m,2m,3m,…як в сорону старших, так і в сторону молодших розрядів. При цьому існує багато варіантів видалення зайвих елементів і необхідно розглянути їх усі. Кількість варіантів визначається формулою (кількість

виборів з урахуванням порядку зайвих для даного розряду елементів з максимальної кількості елементів в пірамідальній структурі):

$$\frac{2^{r-1}!}{(2^{r-1}-2^{r}+q)!(2^{r}-q)!}$$

Далі виконується послідовний перебір всіх можливих комбінацій отриманих пірамід. У кожній комбінації виконується пошук надлишкових, які дублюють фрагменти, що мають однакові вихідні сигнали. Надлишкові фрагменти видаляються. Таким чином утворюється масив з усіх можливих комбінацій пірамідальних схем. Після чого з отриманого набору моделей пірамідальних схем виконується пошук оптимальних за апаратними витратами, що містять найменшу кількість елементів.

Результатом роботи програми, яка реалізує алгоритм, є текстовий файл з описом оптимальної за апаратними витратами схеми суматора для заданої кількості розрядів. За допомогою програми були одержані результати оптимізації структур суматорів, які подані в табл. 1, і які забезпечують результат значно кращий за верхню оцінку.

Таблиця 1. Результати оптимізації структур суматорів

$n\backslash m$	1		4		8		16	
	C_h	Оптим.	C_h	Оптим.	C_h	Оптим.	C_h	Оптим.
32	32	25	29	23	26	21	22	18
64	64	51	61	49	57	46	52	41
128	128	102	125	100	121	97	114	92
256	256	205	253	202	249	199	241	193
300	300	240	297	237	293	234	285	228
512	512	409	509	407	505	404	497	398
1024	1024	819	1021	817	1017	813	1017	813

В табл. 2 наведені значення оцінок затримки сигналів в суматорах при використанні КСАО в порівнянні з затримками по структурі, згідно з [1].

Висновки

Одержані результати дозволяють проводить оптимізацію структур суматорів зі змінним модулем по наступних напрямках:

- мінімізація апаратних витрат при заданій швидкості обчислень;

- мінімізацію затримки сигналів при заданій максимальній складності;
- формування оптимальної структури при заданому співвідношенні (швидкість)\(апаратні затрати);

Таблиця 2. Значення оцінок затримки сигналів

n\m	1		4		8		16	
	Без КСАО	Із КСАО	Без КСАО	Із КСАО	Без КСАО	Із КСАО	Без КСАО	Із КСАО
32	32t	6t	32t	9t	32t	13t	32t	20t
64	64t	7t	64t	10t	64t	14t	64t	22t
128	128t	8t	128t	11t	128t	15t	128t	23t
256	256t	9t	256t	12t	256t	16t	256t	24t
300	300t	10t	300t	13t	300t	17t	300t	25t
512	512t	11t	512t	13t	512t	17t	512t	25t
1024	1024t	11t	1024t	14t	1024t	18t	1024t	26t

Практичне значення отриманих результатів полягає у можливості їх застосування у спеціалізованих обчислювальних пристроях функціонального перетворення електронних документів, в системах несиметричних криптографічних перетворень, системах цифрового підпису та криптографічних протоколів типу SSL.

Література

1. *Тарасенко В.П.,. Тесленко О.К.* Реалізація основних арифметичних операцій над залишками на одномірних каскадах конструктивних модулів//Управляющие системы и машины, 2003. – № 3(185). – С.29-42.
2. *Тарасенко В.П., Тесленко А.К.* Быстродействующие многоразрядные сумматоры по переменному модулю//Материалы международной научно-практической конференции «Инфомационные технологии и информационная безопасность в науке, технике и образвании “ИНФОТЕХ-2007” СевНТУ, 2007. – С. 93-97.