Решетар Я. В.,
Національний університет "Львівська політехніка"

ПРОГРАМНО–АПАРАТНА РЕАЛІЗАЦІЯ АЛГОРИТМІВ БЛОКОВОГО ШИФРУВАННЯ ДСТУ ГОСТ 28147:2009 НА БАЗІ ПЛІС

Розвиток науки, передусім в галузі мікроелектроніки дає можливість розширювати базу для створення нових програмних та апаратних криптографічних засобів захисту інформації. Обмеженість обчислювальних ресурсів представлених платформ актуалізує дослідження ефективної реалізації криптографічних алгоритмів, розгляд їх архітектурних та структурних особливостей, пошук компромісу між затраченими ресурсами та продуктивністю. Особливо гостро визначена проблема стосується вітчизняної галузі, оскільки в Україні чинні власні стандарти криптографічного захисту інформації [1], дослідження реалізації яких на сучасних апаратних платформах потребує значно глибшого вивчення.

Сучасні реконфігураційні платформи, такі як *ПКВМ (FPGA)*, містять велику кількість логічних та арифметичних вентилів, таблиць відповідності, регістрів необхідних для реалізації основних компонентів алгоритму. Паралельність обчислень на рівні ітерацій досягається завдяки застосуванню декількох стратегій побудови архітектури шифру [2, 3]:

- ітеративної (iterative)*;*
- розгорнутого циклу (loop unrolling)*;*
- зовнішнього конвеєра (outer-round pipelining)*;*
- внутрішнього конвеєра (inner-round pipelining)*;*
- зовнішнього і внутрішнього конвеєра (inner- and outer-round pipelining).

Розглянемо детальніше основні компоненти алгоритму [1], з точки зору реалізації на базі ПКВМ:

Регістри N1 і N2. Відповідають внутрішній структурі ПКВМ (таблиці відповідності, тригери).

КЗП. Блок пам'яті, що зберігає один або декілька секретних ключів криптографічного перетворення. Функціонування блоку ОЗП (Distributed RAM) організується на базі таблиць відповідності, крім того більшість сучасних ПКВМ містять спеціальні високопродуктивні блоки пам'яті (Block RAM).

Суматор за модулем 2^{32} . Найпрацемісткіший компонент алгоритму, що реалізується у вигляді комбінаційної схеми на базі загальнодоступних ресурсів ПЛІС: таблиць відповідності, мультиплексорів, вентилів арифметичної логіки.

Таблиці заміни К1...К8 можуть бути виражені через логічні функції на основі таблиць відповідності або як блоки ПЗП на основі Distributed/Block RAM.

Регістр циклічного зсуву не використовує жодних додаткових ресурсів, оскільки є всього лиш відповідним з'єднанням сигналів на вході і на виході.

Регістр XOR, як і інші булеві функції ефективно реалізується на базі таблиць відповідності та вентилів арифметичної логіки.

Для дослідження реалізації ітеративної архітектури алгоритму, за допомогою програмного середовища *ISE WebPACK 10.1* було створено проект на мові опису апаратних компонентів *VHDL*. В якості базової платформи вибрано бюджетний пристрій *Spartan–3A (XC3S400A)*, фірми *Xilinx*, що поєднує помірну вартість з достатньою кількістю обчислювальних ресурсів загального призначення (400 000 еквівалентних вентилів).

Проект реалізує шифрувальний пристрій в режимі простої заміни, з наступним функціональним призначенням сигналів (див. рис.):

- шина вхідних даних (блоку) повідомлення ***plain_text***;
- шина, що визначає ключ перетворення ***key_addr***;
- тактуючий сигнал ***clk***;
- сигнал скиду ***rst***;
- сигнал, що визначає режим роботи шифратора (шиф-ня/дешиф-ня) ***cipher_mode***;
- шина вихідних даних (блоку) повідомлення ***cipher_text***.
-

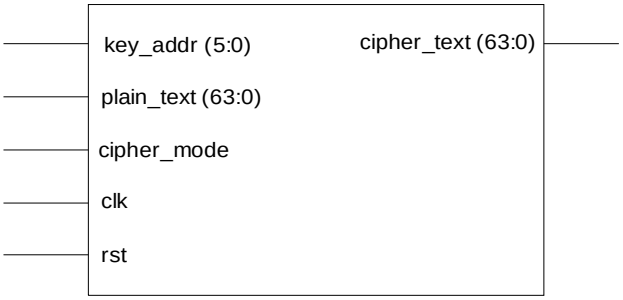

Рис. Інтерфейс схеми шифратора ДСТУ ГОСТ 28147:2009

Компоненти алгоритму реалізовані у вигляді структурних *VHDL*-блоків. Поряд з тим, заявлена платформа *XC3S400A* містить 20 блоків *ОЗП*, що дозволяє заощадити ресурси на реалізації *КЗП*. Зокрема в даному проекті був використаний готовий компонент *RAMB16BWE_S36* бібліотеки *UNISIM*, що задіює 1 блок *ОЗП*, сконфігурований для зберігання 512 слів довжиною 32 біти. Вибір відповідного раундового ключа здійснюється схемою управління, що реалізована в основній архітектурі проекту.

Для синтезу зовнішньої конвеєрної архітектури, були використані 32 компоненти (ядра) ітеративної структури. Після кожного спрацювання тактуючого сигналу ***clk***, сигнали з виходів компонентів подаються на входи наступних. Крім того, під час процедури ініціалізації (скидання сигналу ***rst***) ключ заноситься у 8 проміжних регістрів, дані з яких в подальшому паралельно використовуються для кожного структурного компоненту.

Таблиця.

Порівняльна характеристика реалізацій алгоритмів блокового шифрування.

Алгоритм	К-ть раундів	Режим роботи	Архітектура	Ресурси ПЛІС	Платформа	Період (макс. част.)	Прод.
ДСТУ ГОСТ 28147:2009 (проста заміна)	32	шифр/ де-шифр	ітератив-на	91 slice (2 %) 172 LUT (4-1) (2 %) 1 BRAM (18 кбіт) (5 %)	Spartan-3A (XC3S400A)	9,682 нс (103,3 МГц)	206,6 Мбіт/с
ДСТУ ГОСТ 28147:2009 (гамування зі зворотнім зв'язком)	32	шифр/ де-шифр	ітератив-на	145 slice (4 %) 243 LUT (4-1) (3 %) 1 BRAM (18 кбіт) (5 %)	Spartan-3A (XC3S400A)	9,342 нс (107 МГц)	214 Мбіт/с
ДСТУ ГОСТ 28147:2009 (проста заміна)	32	шифр/ де-шифр	зовнішня конвеєрна	2307 slice (64 %) 3088 LUT (4-1) (43 %) 1 BRAM (18 кбіт) (5 %)	Spartan-3A (XC3S400A)	7,715 нс (129,6 МГц)	8,29 Гбіт/с
DES [4]	16	шифр/ де-шифр	зовнішня конвеєрна	3328 LUT (4-1) (54 %) 960 flip-flops (54 %)	Spartan-2E (XC2S300E)	14,7 нс (68 МГц)	4,25 Гбіт/с
DES [5]	16	шифр/ де-шифр	конвеєрна (внут. і зовн.)	5036 LUT (4-1) (49 %)	Virtex-2 (XC2V1000)	4,219 нс (237 МГц)	15,1 Гбіт/с
AES–128 [6]	10	шифр/ де-шифр	конвеєрна (внут. і зовн.)	17,425 slice (43 %)	Spartan-3 (XC3S2000)	5,099 нс (196,1 МГц)	25,1 Гбіт/с

Висновки. Ітеративна структура криптографічних алгоритмів сприяє ефективній реалізації їх архітектури на базі *ПКВМ*. Виходячи з ресурсів конкретної платформи, комбінування внутрішніх і зовнішніх по відношенню до схеми проміжних регістрів дозволяє досягнути максимальної продуктивності [2, 3].

Встановлено, що в структурі алгоритмів ДСТУ ГОСТ 28147:2009 є компонент, що обмежує максимальну продуктивність реалізації в порівнянні з іншими алгоритмами. Тривалість періоду ~10 нс (див. табл.) визначається максимальною затримкою комбінаційної схеми ядра (раунду) алгоритму, з якої затримка 32-ох бітного арифметичного суматора складає ~7 нс. Застосування стратегії внутрішнього конвеєра з цієї причини виглядає неефективним, оскільки час проходження одного раунду таким чином, складатиме ~14 нс.

У представлених в порівняльній таблиці алгоритмах DES і AES основними компонентами є прості з точки зору апаратної реалізації компонен-

ти заміни, перестановки, суматори *XOR*, що й зумовлює їх перевагу в швидкодії. Поряд з тим ДСТУ ГОСТ 28147:2009 відзначається простотою реалізації схеми планування раундових ключів.

В особливих застосуваннях, максимальна потужність роботи шифрувального пристрою досягається розміщенням схеми кожного раунду на одній платформі (зовнішня конвеєрна архітектура). Зокрема таким чином при використанні 64 % ресурсів бюджетної платформи *Spartan–3A (XC3S400A)* було досянуто рівень швидкодії ~8 Гбіт/с.

Література:

1. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования : ДСТУ ГОСТ 28147:2009. — [Чинний від 2009-02-01]. — К. : Держспоживстандарт України, 2008. — 28 с. — (Національний стандарт України)
2. Cryptographic Algorithms on Reconfigurable Hardware / Rodriguez-Henriquez F., Saqib N. A., Díaz Pérez A., Koc C.K. — New York : Springer Science+Business Media, 2007. — 362 p. — ISBN: 978-0-387-33883-5.
3. Cryptographic Engineering / [editor Koc C.K]. — New York : Springer Science+Business Media, 2009. — 522 p. — ISBN: 978-0-387-71816-3.
4. Баркалов А.А. Реализация алгоритма шифрования DES на базе FPGA / Баркалов А. А., Красичков А. А., Кузьменко В.О. // Обчислювальна техніка та автоматизація: наукові праці ДНТУ. — Донецьк : ДонНТУ, 2009. — № 16(147). — С. 116—120.
5. Pasham V. Trimberger S. High-Speed DES and Triple DES Encryptor-Decryptor [Електронний ресурс] / Application Note: Virtex-E Family and Virtex-II Series (XAPP270), Xilinx, 2001. — Режим доступу : http://www.xilinx.com/support/documentation/application_notes/xapp 270.pdf.
6. Good T., Benaissa M. AES on FPGA from the Fastest to the Smallest / LNCS: Cryptographic Hardware and Embedded Systems — CHES 2005.— Berlin: Springer, 2005. — Vol. 3659. — P. 427—440.

Рижа Т. В., *аспірант.*
Хмельницький національний університет

УПРАВЛІННЯ ДЕБІТОРСЬКОЮ ЗАБОРГОВАНІСТЮ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Загальна криза неплатежів, яка охопила всі сфери національної економіки, негативно позначилась і на фінансовому стані вищих навчальних