Conference on Very Large Scale Integration (October 2008). – Rhodes, Greece. – P. 321-326. 4. Pande P.P., Grecu C., Jones M., Ivanov A., Saleh R. Performance Evaluation and Design Trade-Offs for Network-on-Chip Interconnect Architectures // IEEE TRANSACTIONS ON COMPUTERS, 2005, V. 54, № 8, p.1025-1040 5. Gebali F., Elmiligi H., Watheq El-Kharashi M. Networks-on-Chip: Theory and Practice.– Boca Raton (USA): CRC Press/Taylor and Francis Group LLC, 2009. – 307p. 6. Дунець Р.Б. Топології комп'ютерних систем. – Львів: ІППТ при НУ „Львівська політехніка", 2007. – 50 с. 7. Dally W., Towles B. Route packets, not wires: on-chip interconnection networks // Proceedings of the 38th annual Design Automation Conference (June 2001). – Las Vegas, USA. – P.684-689. 8. Bjerregaard T., Mahadevan S. A survey of research and practices of Network-on-chip // ACM Computing Surveys. – 2006. –Vol.38, 51. – P.1–51. 9. Дунець Б.Р. Базові архітектури пристроїв комутації пакетів з багатоканальною вхідною буферизацією Комп'ютерні технології друкарства. – Львів: Укр. акад. друкарства. – 2004. – №11. – С. 43–49. 10. Дунець Б.Р. Архітектура пристрою планування комутацією // Вісник Тернопільського державного технічного університету. – 2003. – Т. 8. – №4. – С. 85–91. 11. Jingcao Hu, Radu Marculescu, "Energy-Aware Communication and Task Scheduling for Network-on-Chip Architectures under Real-Time Constraints," date, vol. 1, pp.10234, Design, Automation and Test in Europe Conference and Exhibition Volume I (DATE'04), 2004. 12. Дунець Р.Б. Аналіз та синтез топологій комп'ютерних видавничо-поліграфічних систем: Монографія. – Львів: НВФ "Українські технології", 2003. – 192 с. 13. Дунець Р.Б. Визначення часу та маршрутів критичних шляхів топологій спеціалізованих комп'ютерних систем // Вісн. Хмельницького національного університету. – Хмельницький, 2007. – Т.1. – № 2. – С.70–74.

УДК 004.382

Р. Еліас
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ВБУДОВАНИЙ КОНТРОЛЬ СЕКЦІОНОВАНИХ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА GF(2^M)

Розглядається секціонований помножувач елементів полів Галуа GF(2^m). Помножувач обробляє 521-бітні елементи поля Галуа GF(2^{521}), представлені з використанням гауссівського нормального базису типу 2 і формує 521-бітний добуток порціями по 16 бітів. Якщо під час обчислення добутку виникає помилка, помножувач формує відповідну ознаку. Помножувач використовується в процесорах оброблення цифрових підписів, які ґрунтуються на використанні еліптичних кривих.

Scalable multiplier for Galois field GF(2^m) elements is examined. The multiplier processes presented with the use of type 2 Gaussian normal basis 521-bit Galois field GF(2^{521}) elements and forms 521-bit result by 16 bits portions. The multiplier forms the error sign in case error during the calculation. The multiplier is used in the processors for digital signatures which are based on the use of elliptic curves.

Вступ. На сучасному етапі математичною основою цифрових підписів є еліптичні криві. В одному з варіантів реалізації цифрових підписів оброблення точок еліптичних кривих відбувається за правилами оброблення елементів полів Галуа *GF*(2^m). Розрядність елементів поля *m* може сягати 2048 бітів. Апаратна реалізація помножувача для таких полів вимагає більш ніж мільйона транзисторів. Помножувачі можуть бути паралельними, послідовними та паралельно-послідовними – секціонованими. У роботах останніх років звертається увага на вбудовані методи виявлення

помилок у роботі послідовних помножувачів за допомогою цифрового контролю на парність (зіставлення кількості 1 серед бітів операндів та результатів). Вбудованому контролю секціонованих помножувачів, які поєднують переваги паралельних (більша швидкодія) та послідовних (менші апаратні витрати), приділялася менша увага. Тому задача проектування секціонованих помножувачів елементів полів Галуа $GF(2^m)$ з вузлами вбудованого контролю є важливою і актуальною. У цій роботі розглядається помножувач для поля Галуа $GF(2^{521})$, елементи якого представлені з використанням гауссівського нормального базису типу 2.

Огляд літератури, постановка проблеми. Математичною основою цифрових підписів є еліптичні криві та поля Галуа. Одним з варіантів представлення елементів поля Галуа $GF(2^m)$ є гауссівський нормальний базис типу 2 [5]. Для цього базису відомий послідовний помножувач Мессі–Омури [3], паралельний помножувач та паралельно-послідовний помножувач (секціонований) [1]. Методи вбудованого контролю результатів множення у нормальних базисах полів Галуа $GF(2^m)$ відомі з [4]. Для збільшення надійності роботи послідовного помножувача, який працює у нормальному базисі типу 2 у відповідно до стандарту [5], запропонована проста схема вбудованого контролю [2]. Водночас задача контролю роботи секціонованих помножувачів не розглядалася. Оскільки секціонований помножувач поєднує переваги послідовного (менші апаратні витрати) та паралельного (більша швидкодія) помножувачів, ця задача є актуальною і важливою.

Мета роботи. Метою роботи є розроблення принципів вбудованого контролю секціонованих помножувачів елементів полів Галуа $GF(2^m)$, представлених у гауссівському нормальному базисі типу 2, та схеми вбудованого контролю секціонованих помножувачів (на прикладі 521-бітного помножувача).

Математичні основи вбудованого контролю секціонованих помножувачів для GF(2^m)

Секціонований m-бітний помножувач формує m-бітний добуток R в $]m/n[=K$ секціях порціями по n біт ($k = 0, 1, \ldots, K-1$):

$$(r_{m-kn-1}, \ldots, r_0, r_{m-1}, \ldots, r_{m-n+r}) = (f(a_{m-kn}, \ldots, a_{m-1}, a_0, \ldots, a_{m-kn-1}; b_{m-kn}, \ldots, b_{m-1}, b_0, \ldots, b_{m-kn-1}), \ldots, f(a_{m-n+r+1}, \ldots, a_{m-1}, a_0, \ldots, a_{m-n+r}; b_{m-n+r+1}, \ldots, b_{m-1}, b_0, \ldots, b_{m-n+r})) \text{ [1].} \quad (1)$$

Ознака помилки E_R у роботі послідовного помножувача Мессі–Омури для гаусівського нормального базису типу 2 формується за формулою (2)

$$E_R = \sum_{i=0}^{m-1} (a_i b_i \oplus r_i), \quad (2)$$

де a_i, b_i – біти елементів поля A та B, r_i – біти результату R.

Модифікація формули (2) $E_R = \sum_{k=0}^{K-1} \sum_{i=0}^{n-1} (a_{kn+i} b_{kn+i} \oplus r_{kn+i}) = \sum_{k=0}^{K-1} e_k$ дає змогу ввести вузол вбудованого контролю до кожної секції помножувача. При цьому кожна секція разом з розрядами добутку повинна формувати часткову ознаку $e_k = \sum_{i=0}^{n-1} (a_{kn+i} b_{kn+i} \oplus r_{kn+i})$ помилки множення. Для отримання загальної ознаки множення необхідно провести додаткове згортання часткових ознак.

Реалізація секціонованого помножувача з вбудованим контролем

Схема вузла формування часткових ознак (рис. 1) та спосіб її під'єднання до послідовного помножувача (рис. 2) відомі з [2]. До складу вузла формування часткових ознак входять двовходові елементи І та виключне АБО (*XOR*), а також лічильний тригер (*T*-тригер), на якому накопичується ознака під час виконання множення.

Послідовний помножувач Мессі–Омури (рис. 2) складається з двох регістрів циклічного зсуву операндів *RGA* і *RGB* та помножувальної матриці *M*.

Секціонований помножувач з вузлами вбудованого контролю наведено на рис. 3. Помножувач (рис. 3) також складається з двох регістрів циклічного зсуву операндів *RGA* і *RGB*, 16-ти секцій $F1, \ldots, F16$, які працюють відповідно до формули (1), вузла згортання часткових ознак

помилки *Error Convolution* та регістрового файла результату множення *Our RG File*. Також до складу секціонованого помножувача входить вузол керування *Control Unit*, який блокує формування *i*-х розрядів добутку, коли $i < 0$, та їхніх часткових ознак помилок (*x* на (рис. 3)).

Функціональну схему вузла згортки часткових ознак наведено на рис. 4. Для прикладу 521-бітного помножувача вузол складається з 4-х каскадів елементів виключно АБО (*XOR*), розділених конвеєрними регістрами *Pipeline A, B, C*.

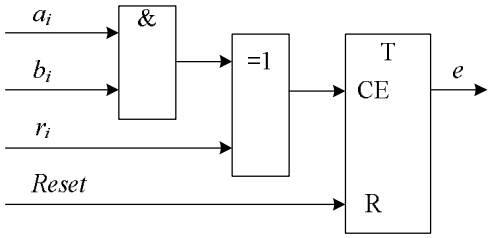

Рис. 1. Формувач часткових ознак помилки

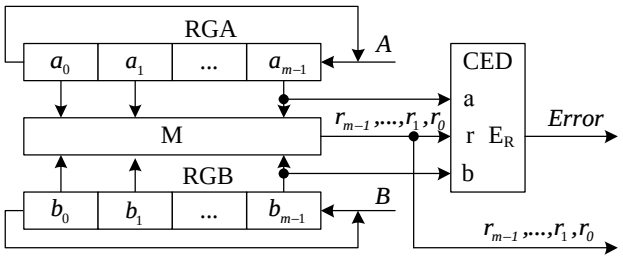

Рис. 2. Помножувач з вузлом виявленням помилок

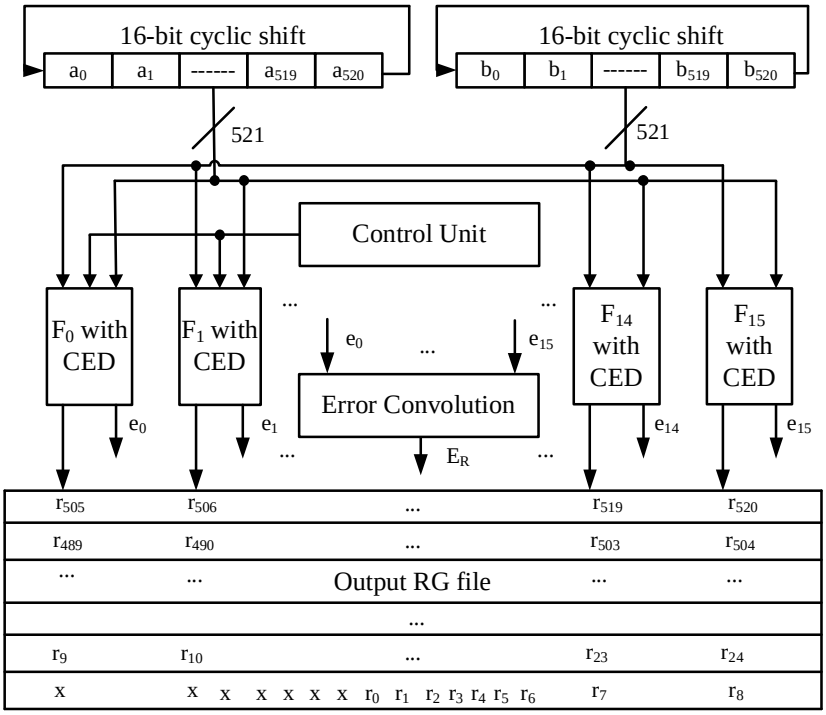

Рис. 3. Секціонований помножувач з вбудованим контролем

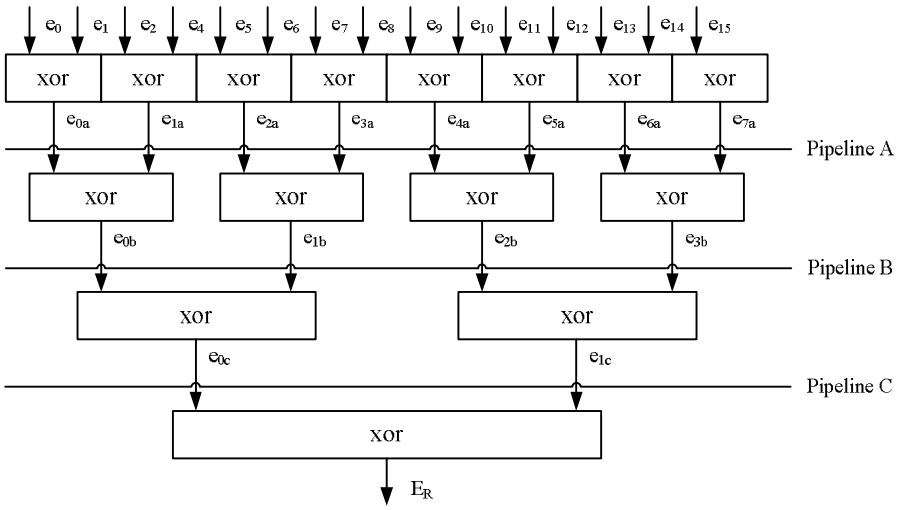

Рис. 4. Згортка часткових ознак помилок

Висновок. У роботі показано, що часткові ознаки помилки множення можуть формуватися безпосередньо секціями секціонованого помножувача елементів полів Галуа $GF(2^m)$, що обробляє елементи поля, представлені у гауссівському нормальному базисі типу 2. Для отримання узагальненої ознаки помилки необхідно згортати часткові ознаки. У роботі наведено функціональну схему секціонованого 521-бітного помножувача із вбудованим контролем. Вбудований контроль секціонованих помножувачів елементів полів Галуа $GF(2^m)$, що обробляє елементи поля, представлені у гауссівському нормальному базисі типу 2, може бути реалізований для інших, відмінних від 521 значень m.

1. Elias Rodrigue. Design of an Elliptic Curve Cryptography Using A Finite Field Multiplier in GF(2^{521}) // Вісник № 658 Нац. ун-ту "Львівська політехніка" "Комп'ютерні системи та мережі". – 2009. – С. 144 – 149. 2. Глухов В.С. Вбудований контроль множення в гауссівському нормальному базисі типу 2 полів Галуа GF(2^m) // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи 6(47). – Харків. ХАІ, 2010. – С. 255 – 259. 3. Omura J. and Massey J. Computational method and apparatus for finite field arithmetic. U.S. Patent Number 4,587,627, May 1986. 4. Chiou-Yng Lee, Chin-Chin Chen, Erl-Huei Lu. Concurrent error detection in bit-serial normal basis of GF(2^m). VLSI Test Technology Workshop. July 16-18, 2008, Tainan, Taiwan. 5. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003.