Noname manuscript No.
(will be inserted by the editor)

Optimized reversible quantum circuits for $\mathbb{F}_{2^8}$ multiplication

José L. Imaña

Received: date / Accepted: date

1 Acknowledgement

This work has been supported by the Spanish MINECO and CM under grants S2018/TCS-4423 and RTI2018-093684-B-I00.

José L. Imaña
Department of Computer Architecture and Automation, Faculty of Physics, Complutense University, 28040 Madrid, Spain
Tel.: +34-91-3944384
Fax: +34-91-3944687
E-mail: jluimana@ucm.es
ORCID-iD: 0000-0002-4220-4111

Abstract Quantum computers represent a serious threat to the safety of modern encryption standards. Within symmetric cryptography, *Advanced Encryption Standard* (AES) is believed to be quantum resistant if the key sizes are large enough. Arithmetic operations in AES are performed over the binary field $\mathbb{F}_{2^m}$ generated by an irreducible pentanomial of degree $m = 8$ using polynomial basis (PB) representation. Multiplication over $\mathbb{F}_{2^m}$ is the most complex and important arithmetic operation, so efficient implementations are highly desired. A number of quantum circuits realizing $\mathbb{F}_{2^m}$ multiplication have been proposed, where the number of qubits, the number of quantum gates and the depth of the circuit are mainly considered as optimization objectives. In this work, optimized reversible quantum circuits for $\mathbb{F}_{2^8}$ multiplication using PB generated by two irreducible pentanomials are presented. The proposed reversible multipliers require the minimum number of qubits and CNOT gates, and the minimum depth among similar $\mathbb{F}_{2^8}$ multipliers found in the literature.

Keywords Quantum computing · reversible circuit · optimization · finite field arithmetic · multiplier · cryptography

2 Introduction

Quantum computing has become an import research field due to its ability to solve efficiently complex problems in comparison with classical solutions. Shor's algorithm for computing discrete logarithms is an example of the threat for asymmetric cryptography [17]. For symmetric cryptography, Grover's algorithm [6] can reduce the brute force attack time to its square root. However, symmetric encryption is believed to be quantum resistant if the key sizes are large enough (for example, the *Advanced Encryption Standard* AES-256 is still considered extremely secure). In order to actually implement such attacks, reversible circuits only consisting of reversible gates have to be described and afterwards mapped to quantum circuits. Quantum circuits for AES block cipher have been proposed in [5], [3], where the estimated quantum resources were studied. For quantum realizations, the number of qubits, the number of quantum gates and the depth of the circuit are mainly considered as optimization objectives.

Multiplication is a fundamental operation in both classical and quantum computing. Integer multiplication has to be performed in quantum computation in order to carry out Shor's algorithm for factoring integers [17], so optimized implementations of reversible circuits for integer multiplication are required. Important research has been done in this context. For instance, constant-optimized quantum circuits for modular multiplication and exponentiation were given in [11], and improved reversible circuits for integer multiplication were proposed in [14], where Karatsuba's recursive method was used. Together with integer multiplication, binary extension field $\mathbb{F}_{2^m}$ multiplication is also of fundamental interest.

Finite field $\mathbb{F}_{2^m}$ is very important due to its use in several important applications such as cryptography and digital signal processing. Specifically, arith-

metic operations in AES are performed over the binary field $\mathbb{F}_{2^m}$ generated by an irreducible pentanomial with degree $m = 8$ using polynomial basis representation. Among arithmetic operations over $\mathbb{F}_{2^m}$, *multiplication* is considered the most important one, so efficient implementations are highly desired. Many different approaches have been proposed to perform $\mathbb{F}_{2^m}$ multiplication. The complexity of the multiplier mainly depends on the representation basis and on the generating irreducible polynomial $f(y)$ selected for the binary field [15]. *Polynomial basis* (PB) is the most widely used for representation, and irreducible trinomials or pentanomials are usually considered. PB multiplication requires a multiplication of polynomials followed by a reduction modulo an irreducible polynomial. These two steps can be combined together using a *product matrix* [15], [16]. In [9], a PB multiplication method based on the decomposition of a product matrix was given. This method defines functions $\mathbf{S_i}$ and $\mathbf{T_i}$ given by the sum of product terms, where the coefficients of the product of two elements can be computed as the sum of these functions. This method was applied in [8] to *type I irreducible pentanomials* $f(y) = y^m + y^{n+2} + y^{n+1} + y + 1$, and in [7] to *type II irreducible pentanomials* $f(y) = y^m + y^{n+2} + y^{n+1} + y^n + 1$.

In this paper, optimized reversible quantum circuits for $\mathbb{F}_{2^8}$ multiplication using PB are presented, where the binary field is generated by the *type I irreducible pentanomial* $f(y) = y^8+y^4+y^3+y+1$ and by the *type II irreducible pentanomial* $f(y) = y^8+y^4+y^3+y^2+1$. Finite field $\mathbb{F}_{2^8}$ is especially important because it is used in AES [1], [4]. The proposed reversible multipliers require the minimum number of qubits and CNOT gates, and the minimum depth among similar $\mathbb{F}_{2^8}$ multipliers found in the literature.

3 Background

Let $f(y) = \sum_{i=0}^{m} f_i y^i$ be an irreducible polynomial of degree m over $\mathbb{F}_2$. Any element A of the binary finite field $\mathbb{F}_{2^m}$ can be represented in the PB $\{1, x, \ldots, x^{m-1}\}$, where x is a root of $f(y)$, as $A = \sum_{i=0}^{m-1} a_i x^i$, with $a_i \in \mathbb{F}_2$. In [9], a PB multiplication method defined functions $\mathbf{S_i}$ and $\mathbf{T_i}$ given by the sum of terms $x_k = (a_k b_k)$ and $z_i^j = (a_i b_j + a_j b_i)$, where $a_i, b_i \in \mathbb{F}_2$ are the coefficients of two field elements A and B, respectively. The product $C = A \cdot B \mod f(y)$ can then be computed as the sum of these functions. The expressions for $\mathbf{S_i}$ $(1 \leq i \leq m)$ and $\mathbf{T_i}$ $(0 \leq i \leq m-2)$ with $\varsigma = \lfloor \frac{i}{2} \rfloor$ and $\gamma = \left(\lceil \frac{m}{2} \rceil + \lfloor \frac{i}{2} \rfloor \right)$, are given in (1)

$$\mathbf{S_i} = x_\varsigma + \sum_{h=0}^{\varsigma-1} z_h^{i-h-1}, \qquad \mathbf{T_i} = x_\gamma + \sum_{j=1}^{\eta-(i+1)} z_{i+j}^{m-j} \tag{1}$$

where $x_\varsigma = a_\varsigma b_\varsigma$ only appears for i *odd* and x_γ only appears when m and i are *even* or when m and i are *odd*. In this case, $\eta = \gamma$. Otherwise, the term x_γ does not appear and the value of $\eta = \left(\lceil \frac{m}{2} \rceil + \lceil \frac{i}{2} \rceil \right)$. The method proposed in [9] was based on the introduction of a *product matrix* that can

be decomposed in a sum of matrices depending on the generating irreducible polynomial selected for the field $\mathbb{F}_{2^m}$, in such a way that the product can be computed as $\underline{c} = \mathbf{M} \cdot \underline{b}$, where $\underline{c} = (c_0, \ldots, c_{m-1})^T$ and $\underline{b} = (b_0, \ldots, b_{m-1})^T$ are the coefficients of C and B, respectively, and where $\mathbf{M}$ is a $m \times m$ matrix whose elements are additions of the coefficients a_i of the operand A. The application of this method in [8] to *irreducible pentanomials* $f(y) = y^m + y^{k_3} + y^{k_2} + y^{k_1} + 1$ showed that the matrix $\mathbf{M}$ can be decomposed into the sum of matrices given in (2) where $\tau_i = \lceil \frac{m-1}{m-k_i} \rceil$ and k_i is the power of y corresponding to the non null coefficient f_{k_i} of the pentanomial.

$$\mathbf{M} = \mathbf{M_0} + \sum_{j=1}^{3} \left(\sum_{i=1}^{\tau_j} \mathbf{M_i^j} + \sum_{p=1, p \neq j}^{3} \sum_{i=1}^{\tau_j - 1} \mathbf{M_i^{p,j}} \right) \tag{2}$$

$\mathbf{M_0}$ is given in (3), where a_i's are the coefficients of A in $\mathbb{F}_{2^m}$. It can be observed that the product $\mathbf{M_0} \cdot \underline{b}$ corresponds with the addition of $\mathbf{S_i}$ and $\mathbf{T_i}$ terms given in (1). Furthermore, it was proven in [8] that the products $\mathbf{M_i^j} \cdot \underline{b}$ and $\mathbf{M_i^{p,j}} \cdot \underline{b}$ correspond with $\mathbf{T_i}$ expressions given in (1). It must also be noted that the matrix $\mathbf{M_0}$ always appears in the decomposition of $\mathbf{M}$ for any field $\mathbb{F}_{2^m}$, so the product $\mathbf{M_0} \cdot \underline{b}$ (and therefore the addition of the corresponding $\mathbf{S_i}$ and $\mathbf{T_i}$ terms) is common to any irreducible polynomial selected for $\mathbb{F}_{2^m}$.

$$\mathbf{M_0} = \begin{pmatrix} a_0 & a_{m-1} & a_{m-2} & \cdots & a_1 \\ a_1 & a_0 & a_{m-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & a_{m-2} & a_{m-3} & \cdots & a_0 \end{pmatrix} \tag{3}$$

Finite field $\mathbb{F}_{2^8}$ is especially important because it is used in AES. Using the expressions given in (1), the functions $\mathbf{S_i}$ and $\mathbf{T_i}$ for $\mathbb{F}_{2^8}$ are $\mathbf{S_1} = x_0 = a_0 b_0$, $\mathbf{S_2} = z_0^1 = (a_0 b_1 + a_1 b_0)$, $\mathbf{S_3} = x_1 + z_0^2 = a_1 b_1 + (a_0 b_2 + a_2 b_0)$, $\mathbf{S_4} = z_0^3 + z_1^2 = (a_0 b_3 + a_3 b_0) + (a_1 b_2 + a_2 b_1)$, $\mathbf{S_5} = x_2 + z_0^4 + z_1^3 = a_2 b_2 + (a_0 b_4 + a_4 b_0) + (a_1 b_3 + a_3 b_1)$, $\mathbf{S_6} = z_0^5 + z_1^4 + z_2^3 = (a_0 b_5 + a_5 b_0) + (a_1 b_4 + a_4 b_1) + (a_2 b_3 + a_3 b_2)$, $\mathbf{S_7} = x_3 + z_0^6 + z_1^5 + z_2^4 = a_3 b_3 + (a_0 b_6 + a_6 b_0) + (a_1 b_5 + a_5 b_1) + (a_2 b_4 + a_4 b_2)$, $\mathbf{S_8} = z_0^7 + z_1^6 + z_2^5 + z_3^4 = (a_0 b_7 + a_7 b_0) + (a_1 b_6 + a_6 b_1) + (a_2 b_5 + a_5 b_2) + (a_3 b_4 + a_4 b_3)$, and $\mathbf{T_0} = x_4 + z_1^7 + z_2^6 + z_3^5 = a_4 b_4 + (a_1 b_7 + a_7 b_1) + (a_2 b_6 + a_6 b_2) + (a_3 b_5 + a_5 b_3)$, $\mathbf{T_1} = z_2^7 + z_3^6 + z_4^5 = (a_2 b_7 + a_7 b_2) + (a_3 b_6 + a_6 b_3) + (a_4 b_5 + a_5 b_4)$, $\mathbf{T_2} = x_5 + z_3^7 + z_4^6 = a_5 b_5 + (a_3 b_7 + a_7 b_3) + (a_4 b_6 + a_6 b_4)$, $\mathbf{T_3} = z_4^7 + z_5^6 = (a_4 b_7 + a_7 b_4) + (a_5 b_6 + a_6 b_5)$, $\mathbf{T_4} = x_6 + z_5^7 = a_6 b_6 + (a_5 b_7 + a_7 b_5)$, $\mathbf{T_5} = z_6^7 = (a_6 b_7 + a_7 b_6)$, $\mathbf{T_6} = x_7 = a_7 b_7$, where additions and products are implemented with XOR and AND gates, respectively. It must be noted that the above functions are valid for any irreducible polynomial generating the binary field $\mathbb{F}_{2^8}$ and that the product of two field elements can be computed as sums of these functions.

In quantum computing, a *quantum gate* is a basic quantum circuit operating on a number of quantum bits (*qubits*). Quantum gates are *reversible* (i.e., there exists a *one-to-one* mapping from the inputs to the outputs and viceversa) and require an equal number of input and output qubits. In order to

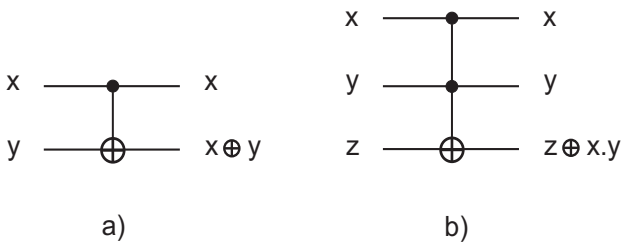

Fig. 1 a) CNOT gate, b) Toffoli gate

perform the product over $\mathbb{F}_{2^m}$, reversible gates for addition and multiplication are needed. The CNOT (controlled-NOT or Feynman) gate is equivalent to the $\mathbb{F}_2$ addition (XOR) and maps the two qubits x and y as $(x, y) \rightarrow (x, x \oplus y)$. The Toffoli gate is equivalent to the $\mathbb{F}_2$ multiplication (AND) and maps the three qubits x, y and z as $(x, y, z) \rightarrow (x, y, z \oplus xy)$. Figure 1 shows CNOT and Toffoli gates. For CNOT gate in Figure 1, x is the *control* line and y is the *target* line, while that for Toffoli gate, x, y are *control* lines and z is the *target* line. A line which is not target nor control line but is used in implementing a reversible circuit is termed an *ancillary* line. Classical computing can be performed using only reversible gates. For example, Toffoli gate can implement any Boolean function, often having to use ancilla bits. Reversible gates can be mapped to equivalent quantum circuits, so that quantum circuits can perform all operations accomplished by classical circuits. For quantum realizations, the major optimization objectives have been the number of lines (qubits) and the number of quantum gates. However, the *depth* of a quantum circuit is also of fundamental importance. This metrics considers the gates of the circuit that can concurrently be applied in order to reduce the execution time of the circuit [2]. Two consecutive quantum gates can be applied *concurrently* if the lines used by each gate (both control and target lines) are disjoint. Given a quantum circuit with q quantum gates, if the circuit can be partitioned into $d \leq q$ subcircuits whose gates can be applied *concurrently*, then the minimum d is refer as the *depth* of the quantum circuit [2].

4 Reversible multiplier for $\mathbb{F}_{2^8}$ generated by *type I irreducible pentanomial*

Type I irreducible pentanomials were defined in [15] as $f(y) = y^m + y^{n+1} + y^n + y + 1$, where $2 \leq n \leq \lceil \frac{m}{2} \rceil - 1$. These pentanomials are important due to their abundance and their use in many important applications (such as AES). Based on [8] and using the $\mathbf{S_i}$ and $\mathbf{T_i}$ terms given in Background section for $\mathbb{F}_{2^8}$, Table 1 shows the coefficients of the product $C = A \cdot B \bmod f(y)$, with $A, B \in \mathbb{F}_{2^8}$, for the type I irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y + 1$, where the expression of a coefficient c_i is computed by the addition of $\mathbf{S_i}$ and $\mathbf{T_i}$ terms given in its row.

Table 1 Coefficients c_i of the product for $f(y) = y^8 + y^4 + y^3 + y + 1$.

c_0	$\mathbf{S_1}$	$\mathbf{T_0}$	$\mathbf{T_4}$			$\mathbf{T_5}$					
c_1	$\mathbf{S_2}$	$\mathbf{T_1}$	$\mathbf{T_5}$			$\mathbf{T_6}$			$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$
c_2	$\mathbf{S_3}$	$\mathbf{T_2}$	$\mathbf{T_6}$						$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$
c_3	$\mathbf{S_4}$	$\mathbf{T_3}$				$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$	$\mathbf{T_2}$	$\mathbf{T_6}$	
c_4	$\mathbf{S_5}$	$\mathbf{T_4}$	$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$	$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$	$\mathbf{T_3}$		
c_5	$\mathbf{S_6}$	$\mathbf{T_5}$	$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$	$\mathbf{T_2}$	$\mathbf{T_6}$		$\mathbf{T_4}$		
c_6	$\mathbf{S_7}$	$\mathbf{T_6}$	$\mathbf{T_2}$	$\mathbf{T_6}$		$\mathbf{T_3}$			$\mathbf{T_5}$		
c_7	$\mathbf{S_8}$		$\mathbf{T_3}$			$\mathbf{T_4}$			$\mathbf{T_6}$		

Using the expressions presented in Table 1, the new reversible multiplier for $\mathbb{F}_{2^8}$ generated by the type I irreducible pentanomial is given by the concatenation of Figure 2, Figure 3 and Figure 4. This multiplier is implemented with Toffoli and CNOT gates. The number of lines (qubits) needed for the overall implementation of the multiplier is 24: eight lines for the coefficients of operand A, eight lines for the coefficients of operand B and eight lines, initialized to 0, that will be used in Figure 3 for the addition of $\mathbf{T_i}$ terms and in Figure 4 for the implementation of the coefficients of the product C.

Figure 2 shows the circuit implementing terms $\mathbf{T_i}$, $i = 0, \ldots, 6$, given in Background section, where only Toffoli gates are used. Figure 3 shows the implementation of the addition of $\mathbf{T_i}$ terms given in Table 1, where $\mathbf{p_0} = (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5})$, $\mathbf{p_1} = (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6}) + (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5})$, $\mathbf{p_2} = (\mathbf{T_2} + \mathbf{T_6}) + (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$, $\mathbf{p_3} = \mathbf{T_3} + (\mathbf{T_2} + \mathbf{T_6}) + (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5})$, $\mathbf{p_4} = (\mathbf{T_3} + \mathbf{T_4}) + (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5}) + (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$, $\mathbf{p_5} = (\mathbf{T_4} + \mathbf{T_5}) + (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6}) + (\mathbf{T_2} + \mathbf{T_6})$, $\mathbf{p_6} = (\mathbf{T_5} + \mathbf{T_6}) + \mathbf{T_3} + (\mathbf{T_2} + \mathbf{T_6})$ and $\mathbf{p_7} = \mathbf{T_6} + (\mathbf{T_3} + \mathbf{T_4})$. In Figure 3 (where only CNOT gates are used), the repeated additions that can be found in Table 1 among different coefficients are used for the implementation. These repeated additions correspond with the above given parenthesized expressions $(\mathbf{T_2} + \mathbf{T_6})$, $(\mathbf{T_5} + \mathbf{T_6})$, $(\mathbf{T_4} + \mathbf{T_5})$, $(\mathbf{T_3} + \mathbf{T_4})$, $(\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5})$ and $(\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$, that can be shared for the construction of $\mathbf{p_i}$ terms. It must be noted that the two-terms parenthesized additions $(\mathbf{T_2} + \mathbf{T_6})$, $(\mathbf{T_5} + \mathbf{T_6})$, $(\mathbf{T_4} + \mathbf{T_5})$ and $(\mathbf{T_3} + \mathbf{T_4})$ can be found in Table 1 for coefficients c_2, c_1, c_0 and c_7, respectively, and that they are used for the construction of the three-terms expressions $(\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5})$ and $(\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$. For this reason, parenthesized expressions are firstly implemented with CNOT gates in Figure 3 (starting with two-terms additions) in order to be used for the implementation of $\mathbf{p_i}$'s. Furthermore, $\mathbf{p_i}$ terms are computed by combining different $\mathbf{T_i}$ and $\mathbf{p_i}$ terms. For example, the term $\mathbf{p_0} = (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5})$ is used for the computation of the coefficients c_0, c_1, c_3 and c_4. As it can be observed in Figure 3, $\mathbf{p_0}$ is also combined with $(\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$ in $\mathbf{p_1}$ in order to compute c_1 and c_4. Finally, Figure 4 shows the circuit implementing terms $\mathbf{S_i}$, $i = 1, \ldots, 8$, given in Background section, that are summed with $\mathbf{p_i}$ terms computed in Figure 3. In Figure 4 only Toffoli gates are used.

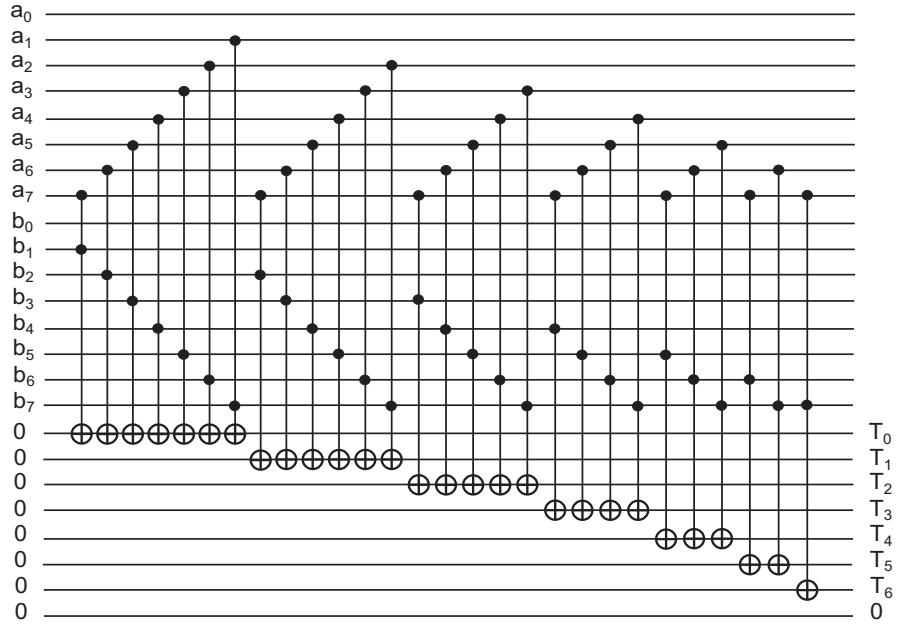

Fig. 2 Reversible implementation of $\mathbf{T_i}$ terms

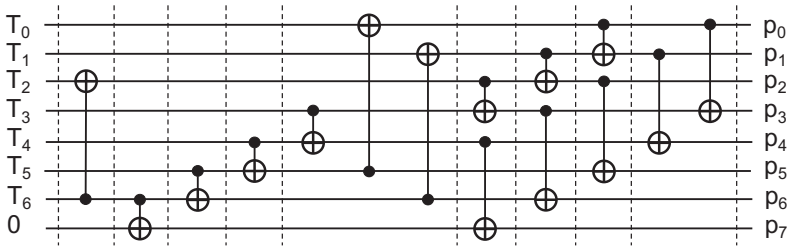

Fig. 3 Reversible implementation of $\mathbf{p_i}$ terms for Type I irreducible pentanomial

4.1 Depth and resource estimates

It can be observed that the new reversible multiplier given in Figures 2, 3 and 4 is implemented with 64 Toffoli (28 for the implementation of $\mathbf{T_i}$ terms, and 36 for $\mathbf{S_i}$ terms) and 15 CNOT gates (for $\mathbf{p_i}$ terms). Furthermore, the total number of qubits needed for the proposed multiplier is 24 (without ancillary lines).

With respect to the depth of the multiplier, circuits given in Figures 2 and 4 have depths 28 and 36, respectively, because the lines used by all consecutive Toffoli gates are not disjoint and therefore can not be applied concurrently. However, reversible circuit given in Figure 3 presents several consecutive CNOT gates that can be applied concurrently. Concurrent gates in Figure 3

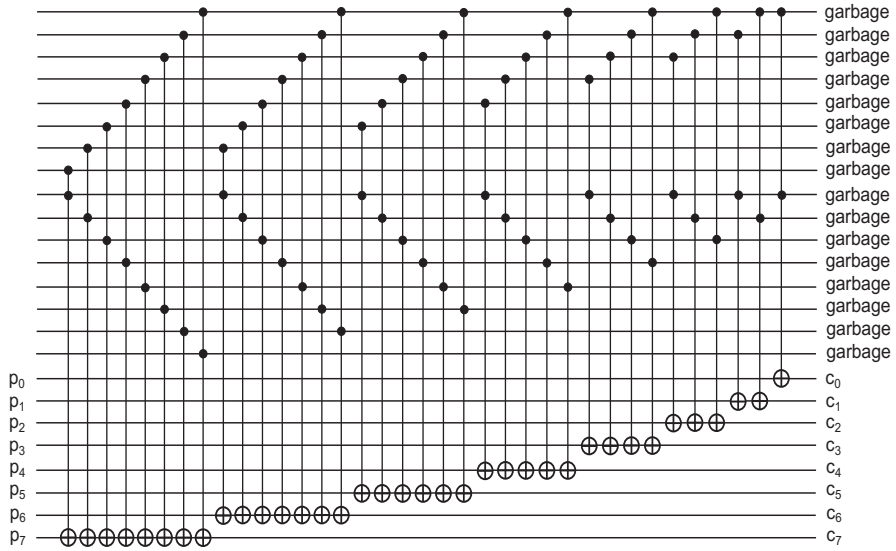

Fig. 4 Reversible implementation of $\mathbf{S_i}$ terms and coefficients of the product

are represented within two consecutive vertical dotted lines, in such a way that for the implementation of $\mathbf{p_i}$ terms there are 3, 2, 2, 2 and 2 consecutive gates that can be applied concurrently. Therefore, the depth of circuit given in Figure 3 is 9. Finally, the total depth of the reversible type I multiplier here proposed is 73.

As previously stated, the construction of the reversible circuits implementing $\mathbf{T_i}$ and $\mathbf{S_i}$ terms given in Figure 2 and Figure 4 makes that all consecutive Toffoli gates can not be concurrent. However, a new reversible construction can be done in such a way that several Toffoli gates can be applied concurrently in order to implement $\mathbf{T_i}$ and $\mathbf{S_i}$ terms with a reduced depth and without increasing the use of resources. The new reversible circuits for the implementation of $\mathbf{T_i}$ and $\mathbf{S_i}$ terms are given in Figure 5 and Figure 6, respectively, where concurrent gates are represented within two consecutive vertical dotted lines. These new circuits present a depth of 9 for $\mathbf{T_i}$ terms and 10 for $\mathbf{S_i}$ terms. Therefore, the total depth of the new reversible concurrent multiplier for $\mathbb{F}_{2^8}$ generated by the type I irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y + 1$ and given by the concatenation of Figure 5, Figure 3 and Figure 6 is 9 + 9 + 10 = 28.

5 Reversible multiplier for $\mathbb{F}_{2^8}$ generated by *type II irreducible pentanomial*

Type II irreducible pentanomials were defined in [16] as $f(y) = y^m + y^{n+2} + y^{n+1} + y^n + 1$, where $2 \leq n \leq \lceil \frac{m}{2} \rceil - 1$. These pentanomials are also abundant.

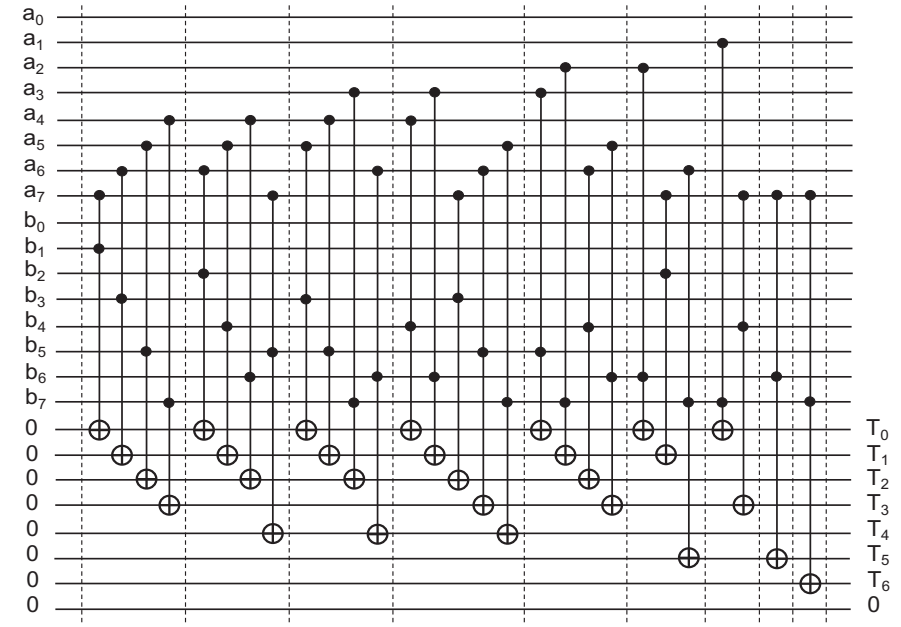

Fig. 5 New concurrent implementation of $\mathbf{T_i}$ terms

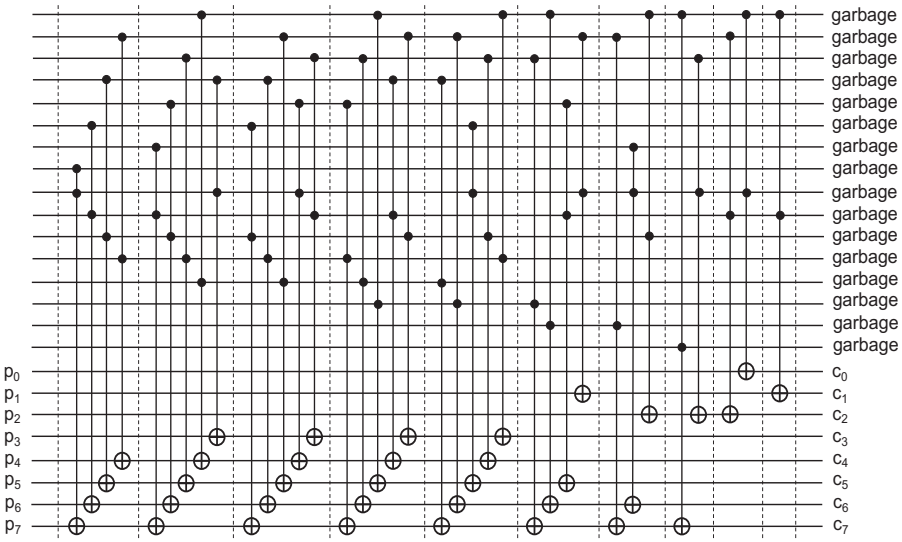

Fig. 6 New concurrent implementation of $\mathbf{S_i}$ terms and coefficients of the product

Table 2 Coefficients c_i of the product for $f(y) = y^8 + y^4 + y^3 + y^2 + 1$.

c_0	$\mathbf{S_1}$	$\mathbf{T_0}$	$\mathbf{T_4}$				$\mathbf{T_5}$				$\mathbf{T_6}$			
c_1	$\mathbf{S_2}$	$\mathbf{T_1}$	$\mathbf{T_5}$				$\mathbf{T_6}$							
c_2	$\mathbf{S_3}$	$\mathbf{T_2}$	$\mathbf{T_6}$								$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$	$\mathbf{T_6}$
c_3	$\mathbf{S_4}$	$\mathbf{T_3}$					$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$	$\mathbf{T_6}$	$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$	
c_4	$\mathbf{S_5}$	$\mathbf{T_4}$	$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$	$\mathbf{T_6}$	$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$		$\mathbf{T_2}$	$\mathbf{T_6}$		
c_5	$\mathbf{S_6}$	$\mathbf{T_5}$	$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$		$\mathbf{T_2}$	$\mathbf{T_6}$			$\mathbf{T_3}$			
c_6	$\mathbf{S_7}$	$\mathbf{T_6}$	$\mathbf{T_2}$	$\mathbf{T_6}$			$\mathbf{T_3}$				$\mathbf{T_4}$			
c_7	$\mathbf{S_8}$		$\mathbf{T_3}$				$\mathbf{T_4}$				$\mathbf{T_5}$			

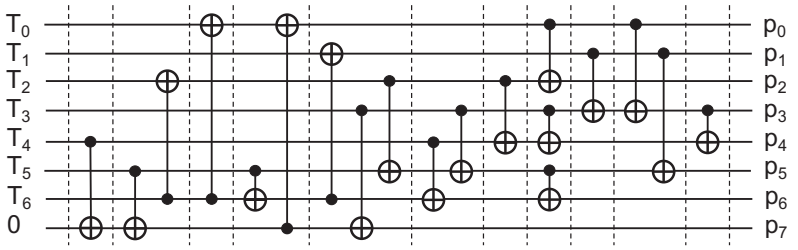

Fig. 7 Reversible implementation of $\mathbf{p_i}$ terms for type II irreducible pentanomial

Furthermore, all five binary fields recommended by NIST for ECDSA can be constructed using such irreducible pentanomials.

Using the work in [7] and $\mathbf{S_i}$ and $\mathbf{T_i}$ terms given in Background section for $\mathbb{F}_{2^8}$, Table 2 shows the coefficients of the product $C = A \cdot B \bmod f(y)$, with $A, B \in \mathbb{F}_{2^8}$, for the irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y^2 + 1$, where the expression of a coefficient c_i is computed by the addition of $\mathbf{S_i}$ and $\mathbf{T_i}$ terms given in its row.

Using the expressions presented in Table 2, the new reversible multiplier for $\mathbb{F}_{2^8}$ generated by the type II irreducible pentanomial is given by the concatenation of Figure 2, Figure 7 and Figure 4. This multiplier is implemented with Toffoli and CNOT gates. The number of qubits needed for the implementation of the multiplier is 24: eight lines for the coefficients of operand A, eight lines for the coefficients of B and eight lines, initialized to 0, that will be used in Figure 7 for the addition of $\mathbf{T_i}$ terms and in Figure 4 for the implementation of the product C.

As in the type I pentanomial, Figure 2 implements terms $\mathbf{T_i}$, $i = 0, \ldots, 6$, where only Toffoli gates are used. Figure 7 shows the implementation of the addition of $\mathbf{T_i}$ terms given in Table 2, where $\mathbf{p_0} = (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6})$, $\mathbf{p_1} = (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$, $\mathbf{p_2} = (\mathbf{T_2} + \mathbf{T_6}) + (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6})$, $\mathbf{p_3} = \mathbf{T_3} + (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6}) + (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$, $\mathbf{p_4} = \mathbf{T_4} + (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6}) + (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6}) + (\mathbf{T_2} + \mathbf{T_6})$, $\mathbf{p_5} = \mathbf{T_5} + (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6}) + (\mathbf{T_2} + \mathbf{T_6}) + \mathbf{T_3}$, $\mathbf{p_6} = \mathbf{T_6} + (\mathbf{T_2} + \mathbf{T_6}) + \mathbf{T_3} + \mathbf{T_4}$ and $\mathbf{p_7} = \mathbf{T_3} + (\mathbf{T_4} + \mathbf{T_5})$. In Figure 7 (where only CNOT gates are used), the repeated additions that can be found in Table 2 among different coefficients are used for the implementation. These repeated additions correspond with the above given parenthesized expressions $(\mathbf{T_2} + \mathbf{T_6})$, $(\mathbf{T_4} + \mathbf{T_5})$, $(\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$ and $(\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6})$, that can be

Table 3 Reduced coefficients c_i of the product for $f(y) = y^8 + y^4 + y^3 + y^2 + 1$.

c_0	$\mathbf{S_1}$	$\mathbf{T_0}$	$\mathbf{T_4}$	$\mathbf{T_5}$	$\mathbf{T_6}$
c_1	$\mathbf{S_2}$	$\mathbf{T_1}$	$\mathbf{T_5}$	$\mathbf{T_6}$	
c_2	$\mathbf{S_3}$	$\mathbf{T_0}$	$\mathbf{T_2}$	$\mathbf{T_4}$	$\mathbf{T_5}$
c_3	$\mathbf{S_4}$	$\mathbf{T_0}$	$\mathbf{T_1}$	$\mathbf{T_3}$	$\mathbf{T_4}$
c_4	$\mathbf{S_5}$	$\mathbf{T_0}$	$\mathbf{T_1}$	$\mathbf{T_2}$	$\mathbf{T_6}$
c_5	$\mathbf{S_6}$	$\mathbf{T_1}$	$\mathbf{T_2}$	$\mathbf{T_3}$	
c_6	$\mathbf{S_7}$	$\mathbf{T_2}$	$\mathbf{T_3}$	$\mathbf{T_4}$	
c_7	$\mathbf{S_8}$	$\mathbf{T_3}$	$\mathbf{T_4}$	$\mathbf{T_5}$	

shared for the construction of $\mathbf{p_i}$ terms. It must be noted that the two-terms parenthesized additions $(\mathbf{T_2} + \mathbf{T_6})$ and $(\mathbf{T_4} + \mathbf{T_5})$ can be found in Table 2 for coefficients c_2 and c_0, respectively. However, two-terms additions $(\mathbf{T_0} + \mathbf{T_6})$ and $(\mathbf{T_5} + \mathbf{T_6})$ can also be found for c_0 and c_1, respectively, that are used for the construction of the three- and four-terms parenthesized expressions $(\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$ and $(\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6})$. For this reason, parenthesized additions are firstly implemented with CNOT gates in Figure 7 (starting with the above two-terms additions) in order to be used for the implementation of $\mathbf{p_i}$'s. Furthermore, $\mathbf{p_i}$ terms are computed by combining different $\mathbf{T_i}$ and $\mathbf{p_i}$ terms. For example, the term $\mathbf{p_0} = (\mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6})$ is used for the computation of the coefficients c_0, c_2, c_3 and c_4. As it can be observed in Figure 7, $\mathbf{p_0}$ is also combined with $\mathbf{p_1} = (\mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6})$ in order to compute c_3 and c_4. Finally, as in the type I pentanomial, Figure 4 implements terms $\mathbf{S_i}$, $i = 1, \ldots, 8$, that are summed with $\mathbf{p_i}$ terms computed in Figure 7. In Figure 4 only Toffoli gates are used.

In order to reduce the complexity of the reversible multiplier using type II pentanomial, it can be observed that in Table 2, there are several $\mathbf{T_i}$ terms that can be cancelled in some coefficients (from c_2 to c_6) because they appear twice. The reduced expressions of the coefficients obtained from this simplification are shown in Table 3. For example, the coefficient c_4 of the product is given by $c_4 = \mathbf{S_5} + \cancel{\mathbf{T_4}} + \mathbf{T_0} + \cancel{\mathbf{T_4}} + \cancel{\mathbf{T_5}} + \cancel{\mathbf{T_6}} + \mathbf{T_1} + \cancel{\mathbf{T_5}} + \cancel{\mathbf{T_6}} + \mathbf{T_2} + \mathbf{T_6} = \mathbf{S_5} + \mathbf{T_0} + \mathbf{T_1} + \mathbf{T_2} + \mathbf{T_6}$, where additions are implemented with XOR gates.

Using the reduced expressions presented in Table 3, a new reversible multiplier for $\mathbb{F}_{2^8}$ generated by the type II irreducible pentanomial with reduced complexity is given by the concatenation of Figure 2, Figure 8 and Figure 9. This multiplier is implemented with Toffoli and CNOT gates. As in the previous implementation, the number of qubits needed for the overall implementation of the multiplier is 24.

Figure 2 implements $\mathbf{T_i}$ terms, $i = 0, \ldots, 6$, using only Toffoli gates. Figure 8 shows the implementation with CNOT gates of the addition of $\mathbf{T_i}$ terms given in Table 3, where $\mathbf{p_0} = \mathbf{T_0} + \mathbf{T_4} + \mathbf{T_5} + \mathbf{T_6}$, $\mathbf{p_1} = \mathbf{T_1} + \mathbf{T_5} + \mathbf{T_6}$, $\mathbf{p_2} = \mathbf{T_0} + \mathbf{T_2} + \mathbf{T_4} + \mathbf{T_5}$, $\mathbf{p_3} = \mathbf{T_0} + \mathbf{T_1} + \mathbf{T_3} + \mathbf{T_4}$, $\mathbf{p_4} = \mathbf{T_0} + \mathbf{T_1} + \mathbf{T_2} + \mathbf{T_6}$, $\mathbf{p_5} = \mathbf{T_1} + \mathbf{T_2} + \mathbf{T_3}$, $\mathbf{p_6} = \mathbf{T_2} + \mathbf{T_3} + \mathbf{T_4}$ and $\mathbf{p_7} = \mathbf{T_3} + \mathbf{T_4} + \mathbf{T_5}$. In Figure 8, some of the repeated additions that can be found in Table 3 among different coefficients are used for the implementation. For example, the addition $\mathbf{T_4} + \mathbf{T_5}$ (implemented with the first two CNOT gates in Figure 8) is used for the computation of terms $\mathbf{p_0}$, $\mathbf{p_2}$ and $\mathbf{p_7}$ (and, therefore, for the computation

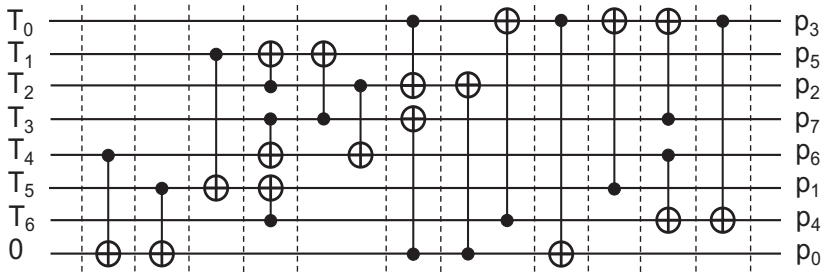

Fig. 8 Reduced reversible implementation of $\mathbf{p_i}$ terms for type II irreducible pentanomial

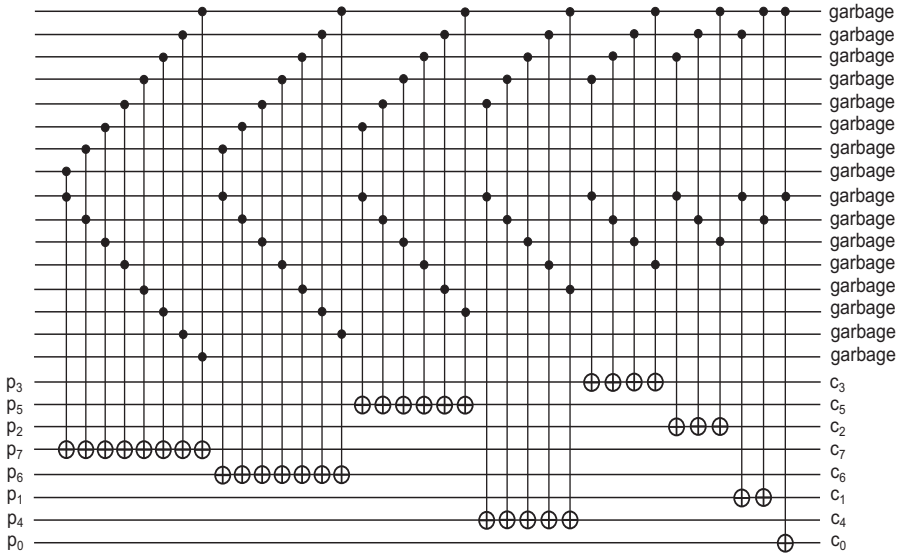

Fig. 9 Reversible implementation of $\mathbf{S_i}$ terms and coefficients of the product for type II irreducible pentanomial

of the coefficients of the product c_0, c_2 and c_7). In the same way, two-terms additions $\mathbf{T_1}+\mathbf{T_5}$, $\mathbf{T_1}+\mathbf{T_2}$ and $\mathbf{T_3}+\mathbf{T_4}$ (also implemented firstly with CNOT gates in Figure 8) can also be found in Table 3 and used for the implementation of $\mathbf{p_1}$, $\mathbf{p_5}$ and $\mathbf{p_6}$ terms, respectively. Furthermore, $\mathbf{p_i}$ terms are computed by combining different $\mathbf{T_i}$ and $\mathbf{p_i}$ terms. As an example, $\mathbf{p_4} = \mathbf{T_6} + \mathbf{p_6} + \mathbf{p_3} = \mathbf{T_6} + (\mathbf{T_2} + \cancel{\mathbf{T_3}} + \cancel{\mathbf{T_4}}) + (\mathbf{T_0} + \mathbf{T_1} + \cancel{\mathbf{T_3}} + \cancel{\mathbf{T_4}}) = \mathbf{T_0} + \mathbf{T_1} + \mathbf{T_2} + \mathbf{T_6}$. Finally, Figure 9 shows the circuit implementing terms $\mathbf{S_i}$, $i = 1, \ldots, 8$, that are summed with $\mathbf{p_i}$ terms computed in Figure 8. It can be observed that Figure 9, that only uses Toffoli gates, is equivalent to Figure 4 with a reordering of the $\mathbf{p_i}$ terms and the output coefficients.

5.1 Depth and resource estimates

It can be observed that the new reversible multiplier given by the concatenation of Figure 2, Figure 7 and Figure 4 is implemented with 64 Toffoli (28 for the implementation of $\mathbf{T_i}$ terms, and 36 for $\mathbf{S_i}$ terms) and 19 CNOT gates (for $\mathbf{p_i}$ terms). Furthermore, the total number of qubits needed for the proposed multiplier is 24 (without ancillary lines).

As in type I multiplier and in order to reduce the depth, reversible circuits given in Figure 5 and Figure 6, where several Toffoli gates are concurrently applied for the implementation of $\mathbf{T_i}$ and $\mathbf{S_i}$ terms, can be used. These concurrent reversible circuits present a depth of 9 for $\mathbf{T_i}$ terms and 10 for $\mathbf{S_i}$ terms. Reversible circuit given in Figure 7 presents several consecutive CNOT gates that can be applied concurrently. Concurrent gates in Figure 7 are represented within two consecutive vertical dotted lines, in such a way that for the implementation of $\mathbf{p_i}$ terms there are 2, 2, 3, 2, 3 and 2 consecutive gates that can be applied concurrently. Therefore, the depth of circuit given in Figure 7 is 11. Finally, the total depth of this first reversible concurrent multiplier proposed for $\mathbb{F}_{2^8}$ generated by the type II irreducible pentanomial $f(y) = y^8+y^4+y^3+y+1$ and given by the concatenation of Figure 5, Figure 7 and Figure 6 is 9 + 11 + 10 = 30.

The second reduced reversible multiplier proposed in Table 3 given by the concatenation of Figure 2, Figure 8 and Figure 9 is implemented with 64 Toffoli (28 for the $\mathbf{T_i}$ and 36 for $\mathbf{S_i}$ terms) and 17 CNOT gates (for $\mathbf{p_i}$ terms), with 24 qubits (without ancillas).

Reversible circuit given in Figure 8 for the implementation of $\mathbf{p_i}$ terms presents 3, 2, 2, 2 and 2 consecutive gates that can be applied concurrently, and its depth is 11. In a similar way as for type I and previous type II multipliers, concurrent circuits for the implementation of $\mathbf{T_i}$ and $\mathbf{S_i}$ terms can be used. Therefore, the total depth of this second reduced reversible concurrent multiplier proposed for $\mathbb{F}_{2^8}$ generated by the type II irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y + 1$ and given by the concatenation of Figure 5 (new reversible implementation of $\mathbf{T_i}$ terms with concurrent gates), Figure 8 and the concurrent implementation of Figure 9 (not given) is 9 + 11 + 10 = 30.

6 Comparison with other $\mathbb{F}_{2^8}$ reversible multipliers

6.1 Type I irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y + 1$

In Table 4, the resource counts and depth obtained by the multiplier here presented are compared with the multipliers given in [3] and [5], that are the unique reversible PB multipliers found in the literature over $\mathbb{F}_{2^8}$ generated by the type I irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y + 1$. The multiplier given in [3] is implemented with 64 Toffoli and 17 CNOT gates, the total number of qubits needed is 24 (no ancillas), and the depth of this multiplier is 67. The reversible multiplier given in [5], that is based on the design proposed

Table 4 Resource counts and depth for $\mathbb{F}_{2^8}$ reversible multipliers

	#Toffoli	#CNOT	#qubits	depth
$f(y) = y^8 + y^4 + y^3 + y + 1$				
[3]	64	17	24 (0 ancillas)	74
[5]	64	21	24 (0 ancillas)	68*
This Work	64	15	24 (0 ancillas)	28
$f(y) = y^8 + y^4 + y^3 + y^2 + 1$				
[10]	27	94	43 (19 ancillas)	n.a.
[13]	64	21	24 (0 ancillas)	43
This Work[1]	64	19	24 (0 ancillas)	30
This Work[2]	64	17	24 (0 ancillas)	30

n.a. = not available. * = maximum value.
[1] = First reversible implementation. [2] = Second reduced reversible implementation.

in [13], requires 64 Toffoli and 21 CNOT gates, with 24 qubits (no ancillas). The depth of the multiplier given in [5] is not supplied, although using [13], it could have a maximum depth of 68.

It can therefore be observed that the new reversible multiplier here proposed matches the number of qubits and Toffoli gates found in [3] and [5], and presents the lowest number of CNOT gates, with a reduction of 11.8% and 28.6% in comparison with the results found in [3] and [5], respectively. With respect to the depth of the reversible circuit, it is found that the multiplier here proposed presents the smallest depth, with a reduction of 58.2% and 58.9% in comparison with the multipliers given in [3] and [5], respectively.

It must be noted that the work in [13] also introduces a parallelized approach to determine the concurrency of quantum gates in order to reduce the depth of reversible multipliers. In [13], $\overrightarrow{e}$ and $\overrightarrow{d}$ computations (equivalent to the computations of $\mathbf{T_i}$ and $\mathbf{S_i}$ terms, respectively) present a depth of 13 and 15, respectively. Therefore, the reduction of depth of the reversible circuits implementing $\mathbf{T_i}$ and $\mathbf{S_i}$ terms here proposed is 30.8% and 33.3%, respectively, with respect to the work given in [13].

6.2 Type II irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y^2 + 1$

In Table 4, the resource counts and depth obtained by the two multipliers here presented are compared with the multipliers given in [13] and [10], that are the unique reversible PB multipliers found in the literature over $\mathbb{F}_{2^8}$ generated by the type II irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y^2 + 1$.

The multiplier given in [13] is implemented with 64 Toffoli and 21 CNOT gates, the total number of qubits needed is 24 (without ancillary lines), and the depth of this multiplier is 43. The work in [13] has been included into the *Reversible Logic Synthesis Benchmarks Page* given in [12]. The design given in [10] requires a reduced number of Toffoli gates (27) but needs an increased number of CNOT gates (94) and 43 qubits (including 19 ancillary lines). The depth of the reversible multiplier is not given in [10].

It can therefore be observed that the new reversible multipliers here proposed match the minimum number of qubits and the number Toffoli gates found in [13]. Furthermore, the two multipliers here proposed present the lowest number of CNOT gates. The second proposed implementation (with the reduced number of CNOT gates) exhibits a reduction of 19% with respect to the work in [13]. With respect to the depth of the reversible circuits, it is found that the multipliers here proposed present the smallest depth, with a reduction of 30.2% in comparison with the approach given in [13]. As previously stated with type I pentanomials, the work in [13] also introduces a parallelized approach to reduce the depth of the reversible multiplier. In [13], the equivalent computations of $\mathbf{T_i}$ and $\mathbf{S_i}$ terms present a depth of 13 and 15, respectively. Therefore, the reduction of depth of the circuits implementing $\mathbf{T_i}$ and $\mathbf{S_i}$ terms here proposed is 30.8% and 33.3%, respectively, with respect to [13].

With respect to the comparison with the work in [10], the reversible multipliers here proposed present an increase of 137% in the number of Toffoli gates. However, the second proposed multiplier presents a reduction of 82% in the number of CNOT gates and a reduction of 44.2% in the number of qubits needed with respect to [10].

7 Conclusion

In this paper, optimized reversible quantum circuits for $\mathbb{F}_{2^8}$ multiplication using PB generated by type I irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y + 1$ and type II irreducible pentanomial $f(y) = y^8 + y^4 + y^3 + y^2 + 1$ are presented. Binary field $\mathbb{F}_{2^8}$ is especially important because it is used in the *Advanced Encryption Standard* (AES). The proposed type I reversible multiplier requires the minimum number of qubits and Toffoli gates in comparison with similar reversible multipliers found in the literature. Furthermore, it requires the minimum number of CNOT gates and presents the smallest depth, with reductions of up to 28.6% and 58.9%, respectively, with respect to other results found in the literature for the same $\mathbb{F}_{2^8}$ multiplier. In this work, two reversible multipliers have also been proposed for $\mathbb{F}_{2^8}$ type II irreducible pentanomial that require the minimum number of qubits and the lowest number of CNOT gates, with a reduction of up to 19% in comparison with similar reversible multipliers found in the literature. With respect to the depth of the multipliers, the reversible circuits here proposed exhibit the smallest depth, with a reduction of up to 30.2% in comparison with other appoaches found in the literature for the same $\mathbb{F}_{2^8}$ multiplier.

References

1. Fips. advanced encryption standard (aes). National Institute of Standards and Technology (2001)
2. Abdessaied, N., Wille, R., Soeken, M., Drechsler, R.: Reducing the depth of quantum circuits using additional circuit lines. In: Intl. Conf. on Reversible Computation, vol. LNCS-7948, pp. 221–233 (2013)

3. Almazrooie, M., Samsudin, A., Abdullah, R., Mutter, K.: Quantum reversible circuit of aes-128. Quantum Inf. Process. **17**, 1–30 (2018)
4. Boyar, J., Peralta, R.: A new combinational logic minimization technique with applications to cryptology. In: SEA 2010, vol. LNCS 6049, pp. 178–189 (2010)
5. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: Applying grover's algorithm to aes: Quantum resource estimates. In: PQCrypto, vol. LNCS-9606, pp. 29–43 (2016)
6. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proc. 28th ACM Symp. Th. Computing, STOC, pp. 212–219 (1996)
7. Imaña, J.L.: Efficient polynomial basis multipliers for type-ii irreducible pentanomials. IEEE Trans. Circuits and Systems II-Express Briefs **59**, 795–799 (2012)
8. Imaña, J.L., Hermida, R., Tirado, F.: Low complexity bit-parallel multipliers based on a class of irreducible pentanomials. IEEE Trans. VLSI Systems **14**, 1388–1393 (2006)
9. Imaña, J.L., Sánchez, J.M., Tirado, F.: Bit-parallel finite field multipliers for irreducible trinomials. IEEE Trans. Comput. **55**, 520–533 (2006)
10. Kepley, S., Steinwandt, R.: Quantum circuits for f_{2^n}-multiplication with subquadratic gate count. Quantum Inf. Process. **14**, 2373–2386 (2015)
11. Markov, I.L., Saeedi, M.: Constant-optimized quantum circuits for modular multiplication and exponentiation. arXiv:1202.6614v3 pp. 1–29 (2015)
12. Maslov, D.: Reversible Logic Synthesis Benchmarks Page (2011). URL http://webhome.cs.uvic.ca/∼dmaslov/
13. Maslov, D., Mathew, J., Cheung, D., Pradhan, D.K.: On the design and optimization of a quantum polynomial-time attack on elliptic curve cryptography. arXiv:0710.1093v2 [quant-ph] (2009)
14. Parent, A., Roetteler, M., Mosca, M.: Improved reversible and quantum circuits for karatsuba-based integer multiplication. arXiv:1706.03419v1 pp. 1–16 (2017)
15. Reyhani-Masoleh, A., Hasan, M.A.: Low complexity bit parallel architectures for polynomial basis multiplication over gf(2^m). IEEE Trans. Comput. **53**, 945–959 (2004)
16. Rodríguez-Henríquez, F., Ç. K. Koç: Parallel multipliers based on special irreducible pentanomials. IEEE Trans. Comput. **52**, 1535–1542 (2003)
17. Shor, P.W.: Algorithms for quantum computation: discrete logarithm and factoring. In: Proc. FOCS'94, pp. 124–134 (1994)