

## Algorithms and arithmetic operators for computing the $\eta_T$ pairing in characteristic three

Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, Masaaki Shirase, Tsuyoshi Takagi

► **To cite this version:**

Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, Masaaki Shirase, et al.. Algorithms and arithmetic operators for computing the  $\eta_T$  pairing in characteristic three. IEEE Transactions on Computers, Institute of Electrical and Electronics Engineers, 2008, Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis, 57 (11), pp.1454-1468. <10.1109/TC.2008.103>. <inria-00423993>

**HAL Id: inria-00423993**

**<https://hal.inria.fr/inria-00423993>**

Submitted on 13 Oct 2009

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Algorithms and Arithmetic Operators for Computing the $\eta_T$ Pairing in Characteristic Three – Appendices

Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, Masaaki Shirase, and Tsuyoshi Takagi

We describe here how to implement the arithmetic operations over  $\mathbb{F}_{3^{2m}}$ ,  $\mathbb{F}_{3^{3m}}$ , and  $\mathbb{F}_{3^{6m}}$  involved in the  $\eta_T$  pairing calculation. In order to compute the number of operations over  $\mathbb{F}_{3^m}$ , we assume that the ALU is able to compute  $u \cdot v$ ,  $\pm u \pm v$  and  $\pm u^3$ , where  $u$  and  $v \in \mathbb{F}_{3^m}$ .

## I. MULTIPLICATION OVER $\mathbb{F}_{3^{2m}}$

Let  $U = u_0 + u_1\sigma$  and  $V = v_0 + v_1\sigma$ , where  $u_0, u_1, v_0$ , and  $v_1 \in \mathbb{F}_{3^m}$ . The product  $UV$  is carried out according to Karatsuba-Ofman's algorithm:

$$U \cdot V = (u_0v_0 - u_1v_1) + ((u_0 + u_1)(v_0 + v_1) - u_0v_0 - u_1v_1)\sigma.$$

It requires 3 multiplications and 5 additions over  $\mathbb{F}_{3^m}$ .

## II. MULTIPLICATION OVER $\mathbb{F}_{3^{3m}}$

Assume that  $U = u_0 + u_1\rho + u_2\rho^2$  and  $V = v_0 + v_1\rho + v_2\rho^2$ , where  $u_i, v_i \in \mathbb{F}_{3^m}$ ,  $0 \leq i \leq 2$ . The product  $W = U \cdot V$  is then given by

$$\begin{aligned} w_0 &= b(bu_1 + u_2)(v_1 + bv_2) + u_0v_0 - u_1v_1 - u_2v_2, \\ w_1 &= (u_0 + u_1)(v_0 + v_1) + (bu_1 + u_2)(v_1 + bv_2) \\ &\quad - u_0v_0 - (b+1)u_1v_1, \text{ and} \\ w_2 &= (u_0 + u_2)(v_0 + v_2) - u_0v_0 + u_1v_1. \end{aligned}$$

Multiplication over  $\mathbb{F}_{3^{3m}}$  involves 6 multiplications and 12 additions over  $\mathbb{F}_{3^m}$  (Algorithm 1).

---

### Algorithm 1 Multiplication over $\mathbb{F}_{3^{3m}}$ .

---

**Input:**  $U = u_0 + u_1\rho + u_2\rho^2$  and  $V = v_0 + v_1\rho + v_2\rho^2 \in \mathbb{F}_{3^{3m}}$ .

**Output:**  $W = U \cdot V \in \mathbb{F}_{3^{3m}}$ .

1.  $a_0 \leftarrow u_0 + u_1$ ;  $a_1 \leftarrow u_0 + u_2$ ;  $a_2 \leftarrow bu_1 + u_2$ ; (3A)
  2.  $a_3 \leftarrow v_0 + v_1$ ;  $a_4 \leftarrow v_0 + v_2$ ;  $a_5 \leftarrow v_1 + bv_2$ ; (3A)
  3.  $m_0 \leftarrow u_0 \cdot v_0$ ;  $m_1 \leftarrow u_1 \cdot v_1$ ;  $m_2 \leftarrow u_2 \cdot v_2$ ; (3M)
  4.  $m_3 \leftarrow a_0 \cdot a_3$ ;  $m_4 \leftarrow a_1 \cdot a_4$ ;  $m_5 \leftarrow a_2 \cdot a_5$ ; (3M)
  5.  $a_6 \leftarrow m_0 - m_1$ ; (1A)
  6.  $w_0 \leftarrow a_6 - m_2 + bm_5$  (2A)
  7. **if**  $b = 1$  **then**
  8.  $w_1 \leftarrow -a_6 + m_3 + m_5$ ; (2A)
  9. **else**
  10.  $w_1 \leftarrow -m_0 + m_3 + m_5$ ; (2A)
  11. **end if**
  12.  $w_2 \leftarrow -a_6 + m_4$ ; (1A)
  13. **return**  $w_0 + w_1\rho + w_2\rho^2$ ;
- 

## III. SQUARING OVER $\mathbb{F}_{3^{3m}}$

Let  $U = u_0 + u_1\rho + u_2\rho^2 \in \mathbb{F}_{3^{3m}}$ , with  $u_i \in \mathbb{F}_{3^m}$ ,  $0 \leq i \leq 2$ .  $V = U^2$  is given by

$$\begin{aligned} v_0 &= u_0^2 - bu_1u_2, \\ v_1 &= bu_2^2 - u_0u_1 - u_1u_2, \text{ and} \\ v_2 &= (u_0 + u_1) \cdot (u_0 + u_1 + u_2) - u_0^2 + u_0u_1 + u_1u_2. \end{aligned}$$

Thus, squaring over  $\mathbb{F}_{3^{3m}}$  requires 5 multiplications and 7 additions over  $\mathbb{F}_{3^m}$  (Algorithm 2).

---

### Algorithm 2 Squaring over $\mathbb{F}_{3^{3m}}$ .

---

**Input:**  $U = u_0 + u_1\rho + u_2\rho^2 \in \mathbb{F}_{3^{3m}}$ .

**Output:**  $V = U^2 \in \mathbb{F}_{3^{3m}}$ .

1.  $a_0 \leftarrow u_0 + u_1$ ;  $a_1 \leftarrow a_0 + u_2$ ; (2A)
  2.  $m_0 \leftarrow u_0^2$ ;  $m_1 \leftarrow u_0 \cdot u_1$ ;  $m_2 \leftarrow u_1 \cdot u_2$ ; (3M)
  3.  $m_3 \leftarrow u_2^2$ ;  $m_4 \leftarrow a_1^2$ ; (2M)
  4.  $a_2 \leftarrow m_1 + m_2$ ; (1A)
  5.  $v_0 \leftarrow m_0 - bm_2$ ; (1A)
  6.  $v_1 \leftarrow bm_3 - a_2$ ; (1A)
  7.  $v_2 \leftarrow m_4 + a_2 - m_0$ ; (2A)
  8. **return**  $v_0 + v_1\rho + v_2\rho^2$ ;
- 

## IV. INVERSION OVER $\mathbb{F}_{3^{3m}}$

Let  $V = v_0 + v_1\rho + v_2\rho^2 \in \mathbb{F}_{3^{3m}}$  be the multiplicative inverse of  $U = u_0 + u_1\rho + u_2\rho^2 \in \mathbb{F}_{3^{3m}}$ ,  $U \neq 0$ , where the  $u_i, v_i \in \mathbb{F}_{3^m}$ ,  $0 \leq i \leq 2$ . Since  $U \cdot V = 1$ , we obtain

$$\begin{cases} u_0v_0 + bu_2v_1 + bu_1v_2 = 1, \\ u_1v_0 + (u_0 + u_2)v_1 + (u_1 + bu_2)v_2 = 0, \\ u_2v_0 + u_1v_1 + (u_0 + u_2)v_2 = 0. \end{cases}$$

The solution of this system of equations is then given by

$$\begin{bmatrix} v_0 \\ v_1 \\ v_2 \end{bmatrix} = w^{-1} \begin{bmatrix} u_0^2 - (u_1^2 - u_2^2) - u_2(u_0 + bu_1) \\ bu_2^2 - u_0u_1 \\ u_1^2 - u_2^2 - u_0u_2 \end{bmatrix},$$

where  $w = u_0^2(u_0 - u_2) + u_1^2(-u_0 + bu_1) + u_2^2(-(-u_0 + bu_1) + u_2) \in \mathbb{F}_{3^m}$ . This operation involves 12 multiplications, 11 additions (or subtractions), and a single inversion over  $\mathbb{F}_{3^m}$  (Algorithm 3).

## V. CUBING OVER $\mathbb{F}_{3^{6m}}$

### A. General Algorithm

Let  $U = u_0 + u_1\sigma + u_2\rho + u_3\sigma\rho + u_4\rho^2 + u_5\sigma\rho^2 \in \mathbb{F}_{3^{6m}}$ .  $U^3 \in \mathbb{F}_{3^{6m}}$  is defined as follows:

$$U^3 = u_0^3 + u_1^3\sigma^3 + u_2^3\rho^3 + u_3^3(\sigma\rho)^3 + u_4^3(\rho^2)^3 + u_5^3(\sigma\rho^2)^3.$$

**Algorithm 3** Inversion over  $\mathbb{F}_{3^m}$ .**Input:**  $U = u_0 + u_1\rho + u_2\rho^2 \in \mathbb{F}_{3^m}$ ,  $U \neq 0$ .**Output:**  $V = U^{-1} \in \mathbb{F}_{3^m}$ .

1.  $a_0 \leftarrow u_0 + bu_1$ ;  $a_1 \leftarrow u_0 - u_2$ ; (2A)
2.  $a_2 \leftarrow -u_0 + u_1$ ;  $a_3 \leftarrow -a_2 + u_2$ ; (2A)
3.  $m_0 \leftarrow u_0^2$ ;  $m_1 \leftarrow u_1^2$ ;  $m_2 \leftarrow u_2^2$ ; (3M)
4.  $m_3 \leftarrow u_0 \cdot u_1$ ;  $m_4 \leftarrow u_0 \cdot u_2$ ;  $m_5 \leftarrow u_2 \cdot a_0$ ; (3M)
5.  $m_6 \leftarrow m_0 \cdot a_1$ ;  $m_7 \leftarrow m_1 \cdot a_2$ ;  $m_8 \leftarrow m_2 \cdot a_3$ ; (3M)
6.  $w \leftarrow m_6 + m_7 + m_8$ ; (2A)
7.  $i \leftarrow w^{-1}$ ; (1I)
8.  $a_4 \leftarrow m_1 - m_2$ ;  $a_5 \leftarrow -a_4 + m_0 - m_5$ ; (3A)
9.  $a_6 \leftarrow bm_2 - m_3$ ;  $a_7 \leftarrow a_4 - m_4$ ; (2A)
10.  $v_0 \leftarrow i \cdot a_5$ ;  $v_1 \leftarrow i \cdot a_6$ ;  $v_2 \leftarrow i \cdot a_7$ ; (3M)
11. **return**  $v_0 + v_1\rho + v_2\rho^2$ ;

Since

$$\begin{cases} \rho^3 & = \rho + b, \\ (\rho^2)^3 & = \rho^2 - b\rho + 1, \end{cases} \quad \begin{cases} \sigma^3 & = -\sigma, \\ (\sigma\rho)^3 & = -\sigma\rho - b\sigma, \\ (\sigma\rho^2)^3 & = -\sigma\rho^2 + b\sigma\rho - \sigma, \end{cases}$$

we obtain the following coefficients for  $V = U^3$ :

$$\begin{aligned} v_0 &= u_0^3 + bu_1^3 + u_2^3, & v_1 &= -u_1^3 - bu_2^3 - u_3^3, \\ v_2 &= u_2^3 - bu_4^3, & v_3 &= -u_3^3 + bu_5^3, \\ v_4 &= u_4^3, & v_5 &= -u_5^3. \end{aligned}$$

As our unified operator computes  $-u_5^3$  in one clock cycle, cubing over  $\mathbb{F}_{3^m}$  requires 6 cubings and 6 additions over  $\mathbb{F}_{3^m}$ .**B. Computation of  $(-t^2 + u\sigma - t\rho - \rho^2)^3$** Let  $U = -t^2 + u\sigma - t\rho - \rho^2$ . According to the previous formula for cubing over  $\mathbb{F}_{3^m}$ , we have

$$V = U^3 = v_0 + v_1\sigma + v_2\rho - \rho^2,$$

where

$$\begin{aligned} v_0 &= -t^6 - bt^3 - 1, \\ v_1 &= -u^3, \text{ and} \\ v_2 &= -t^3 + b. \end{aligned}$$

Therefore,  $U^3$  is as sparse as  $U$  and this specific cubing involves a single multiplication, 2 cubings, and 3 additions over  $\mathbb{F}_{3^m}$  (Algorithm 4).This operation is usually followed by a multiplication which is optimized to take advantage of  $v_4 = -1$  (see for instance Appendix VI-C). Thus, our coprocessor does not explicitly compute  $v_4 \leftarrow -1$ .**Algorithm 4** Computation of  $(-t^2 + u\sigma - t\rho - \rho^2)^3$ .**Input:**  $t$  and  $u \in \mathbb{F}_{3^m}$ .**Output:**  $V = (-t^2 + u\sigma - t\rho - \rho^2)^3 \in \mathbb{F}_{3^m}$ .

1.  $c_0 \leftarrow t^3$ ;  $c_1 \leftarrow -u^3$ ; (2C)
2.  $m_0 \leftarrow c_0^2$ ; (1M)
3.  $v_0 \leftarrow -m_0 - bc_0 - 1$ ; (2A)
4.  $v_1 \leftarrow c_1$ ;
5.  $v_2 \leftarrow b - c_0$ ; (1A)
6. **return**  $v_0 + v_1\sigma + v_2\rho - \rho^2$ ;

VI. MULTIPLICATION OVER  $\mathbb{F}_{3^m}$ **A. General Algorithm**

Elements of  $\mathbb{F}_{3^m}$  can be represented as degree-2 polynomials over  $\mathbb{F}_{3^m}$ . Gorla *et al.* introduced an evaluation-interpolation scheme to perform multiplication over  $\mathbb{F}_{3^m}$  by means of five multiplications over  $\mathbb{F}_{3^m}$  [1]. Then, Karatsuba-Ofman's algorithm allows one to compute each multiplication over  $\mathbb{F}_{3^m}$  by means of three multiplications over  $\mathbb{F}_{3^m}$  (see Appendix I). Thus, the scheme proposed by Gorla *et al.* to multiply two elements of  $\mathbb{F}_{3^m}$  involves 15 multiplications over  $\mathbb{F}_{3^m}$  (Algorithm 5).

**B. Multiplication by a Sparse Operand**

The last multiplication over  $\mathbb{F}_{3^m}$  of the  $\eta_T$  pairing algorithms is cheaper: it consists in computing the product  $(u_0 + u_1\sigma + u_2\rho) \cdot (v_0 + v_1\sigma + v_2\rho + v_3\sigma\rho + v_4\rho^2 + v_5\sigma\rho^2)$  and requires 12 multiplications and 51 additions over  $\mathbb{F}_{3^m}$  (Algorithm 6).

The first multiplication of the  $\eta_T$  pairing algorithms based on the reversed-loop approach also benefits from this optimization. Since

$$(u_0 + u_1\sigma + u_2\rho - \rho^2) \cdot V = (u_0 + u_1\sigma + u_2\rho) \cdot V - \rho^2 \cdot V, \quad (1)$$

it suffices to subtract  $\rho^2 V$  from the element of  $\mathbb{F}_{3^m}$  returned by Algorithm 6. Recall that  $\rho^3 = \rho + b$  and note that Algorithm 6 requires two intermediate variables  $r_1 = v_0 + v_4$  and  $r_2 = v_1 + v_5$ . We then have

$$\begin{aligned} -\rho^2 \cdot V &= -v_2b - bv_3\sigma - (v_2 + bv_4)\rho \\ &\quad - (v_3 + bv_5)\sigma\rho - (v_0 + v_4)\rho^2 - (v_1 + v_5)\sigma\rho^2 \\ &= -v_2b - bv_3\sigma - (v_2 + bv_4)\rho \\ &\quad - (v_3 + bv_5)\sigma\rho - r_1\rho^2 - r_2\sigma\rho^2. \end{aligned}$$

Therefore, subtracting  $\rho^2 \cdot V$  involves 8 additions over  $\mathbb{F}_{3^m}$  and the total cost of Equation (1) is 12 multiplications and 59 additions over  $\mathbb{F}_{3^m}$ .

**C. Computation of  $(u_0 + u_1\sigma + u_2\rho - \rho^2) \cdot (v_0 + v_1\sigma + v_2\rho - \rho^2)$** 

The multiplication of  $U = u_0 + u_1\sigma + u_2\rho - \rho^2$  by  $V = v_0 + v_1\sigma + v_2\rho - \rho^2$ , where both  $U$  and  $V$  are in  $\mathbb{F}_{3^m}$ , requires 6 multiplications and 21 additions over  $\mathbb{F}_{3^m}$  (Algorithm 7).

**D. Computation of  $(\lambda y_P t - \lambda y_Q \sigma - \lambda y_P \rho) \cdot (-t^2 + y_P y_Q \sigma - t\rho - \rho^2)$** 

We consider here the first multiplication over  $\mathbb{F}_{3^m}$  of the  $\eta_T$  pairing calculation based on the reversed-loop approach. Noting

$$\begin{aligned} W &= w_0 + w_1\sigma + w_2\rho + w_3\sigma\rho + w_4\rho^2 + w_5\sigma\rho^2 \\ &= (\lambda y_P t - \lambda y_Q \sigma - \lambda y_P \rho) \cdot (-t^2 + y_P y_Q \sigma - t\rho - \rho^2), \end{aligned}$$

we easily check that

$$\begin{aligned} w_0 &= -\lambda y_P t^3 + \lambda y_P y_Q^2 + b\lambda y_P, \\ w_1 &= \lambda y_P^2 y_Q t + \lambda y_Q t^2, \\ w_2 &= \lambda y_P, \\ w_3 &= \lambda y_Q t - \lambda y_P^2 y_Q, \\ w_4 &= 0, \text{ and} \\ w_5 &= \lambda y_Q. \end{aligned}$$

These equations involve a single cubing, 6 additions, and 6 multiplications over  $\mathbb{F}_{3^m}$ .

## REFERENCES

- [1] E. Gorla, C. Puttmann, and J. Shokrollahi, "Explicit formulas for efficient multiplication in  $\mathbb{F}_{3^6m}$ ," in *Selected Areas in Cryptography – SAC 2007*, ser. Lecture Notes in Computer Science, C. Adams, A. Miri, and M. Wiener, Eds., no. 4876. Springer, 2007, pp. 173–183.

**Algorithm 5** Multiplication over  $\mathbb{F}_{3^6m}$  [1].

**Input:**  $U, V \in \mathbb{F}_{3^6m}$  with  $U = u_0 + u_1\sigma + u_2\rho + u_3\sigma\rho + u_4\rho^2 + u_5\sigma\rho^2$  and  $V = v_0 + v_1\sigma + v_2\rho + v_3\sigma\rho + v_4\rho^2 + v_5\sigma\rho^2$ .

**Output:**  $W = U \cdot V$ . The algorithm requires 15 multiplications and 67 additions over  $\mathbb{F}_{3^m}$ .

1.  $r_0 \leftarrow u_0 + u_4; a_0 \leftarrow r_0 + u_2; a_{12} \leftarrow r_0 - u_2;$  (3A)
2.  $r_0 \leftarrow v_0 + v_4; a_3 \leftarrow r_0 + v_2; a_{15} \leftarrow r_0 - v_2;$  (3A)
3.  $r_0 \leftarrow u_0 - u_4; a_6 \leftarrow r_0 - u_3; a_{18} \leftarrow r_0 + u_3;$  (3A)
4.  $r_0 \leftarrow v_0 - v_4; a_9 \leftarrow r_0 - v_3; a_{21} \leftarrow r_0 + v_3;$  (3A)
5.  $r_0 \leftarrow u_1 + u_5; a_1 \leftarrow r_0 + u_3; a_{13} \leftarrow r_0 - u_3;$  (3A)
6.  $r_0 \leftarrow v_1 + v_5; a_4 \leftarrow r_0 + v_3; a_{16} \leftarrow r_0 - v_3;$  (3A)
7.  $r_0 \leftarrow u_1 - u_5; a_7 \leftarrow r_0 + u_2; a_{19} \leftarrow r_0 - u_2;$  (3A)
8.  $r_0 \leftarrow v_1 - v_5; a_{10} \leftarrow r_0 + v_2; a_{22} \leftarrow r_0 - v_2;$  (3A)
9.  $a_2 \leftarrow a_0 + a_1; a_5 \leftarrow a_3 + a_4; a_8 \leftarrow a_6 + a_7;$  (3A)
10.  $a_{11} \leftarrow a_9 + a_{10}; a_{14} \leftarrow a_{12} + a_{13}; a_{17} \leftarrow a_{15} + a_{16};$  (3A)
11.  $a_{20} \leftarrow a_{18} + a_{19}; a_{23} \leftarrow a_{21} + a_{22};$  (2A)
12.  $a_{24} \leftarrow u_4 + u_5; a_{25} \leftarrow v_4 + v_5;$  (2A)
13.  $m_0 \leftarrow a_0 \cdot a_3; m_1 \leftarrow a_2 \cdot a_5; m_2 \leftarrow a_1 \cdot a_4;$  (3M)
14.  $m_3 \leftarrow a_6 \cdot a_9; m_4 \leftarrow a_8 \cdot a_{11}; m_5 \leftarrow a_7 \cdot a_{10};$  (3M)
15.  $m_6 \leftarrow a_{12} \cdot a_{15}; m_7 \leftarrow a_{14} \cdot a_{17}; m_8 \leftarrow a_{13} \cdot a_{16};$  (3M)
16.  $m_9 \leftarrow a_{18} \cdot a_{21}; m_{10} \leftarrow a_{20} \cdot a_{23}; m_{11} \leftarrow a_{19} \cdot a_{22};$  (3M)
17.  $m_{12} \leftarrow u_4 \cdot v_4; m_{13} \leftarrow a_{24} \cdot a_{25}; m_{14} \leftarrow u_5 \cdot v_5;$  (3M)
18. **if**  $b = 1$  **then**
19.  $t_0 \leftarrow m_0 + m_4 + m_{12}; t_1 \leftarrow m_2 + m_{10} + m_{14};$  (4A)
20.  $t_2 \leftarrow m_6 + m_{12}; t_3 \leftarrow -m_8 - m_{14};$  (2A)
21.  $t_4 \leftarrow m_7 + m_{13}; t_5 \leftarrow t_3 + m_2;$  (2A)
22.  $t_6 \leftarrow t_2 - m_0; t_7 \leftarrow t_3 - m_2 + m_5 + m_{11};$  (4A)
23.  $t_8 \leftarrow t_2 + m_0 - m_3 - m_9;$  (3A)
24.  $w_0 \leftarrow -t_0 + t_1 - m_3 + m_{11};$  (3A)
25.  $w_1 \leftarrow t_0 + t_1 - m_1 + m_5 + m_9 - m_{13};$  (5A)
26.  $w_2 \leftarrow t_5 + t_6;$  (1A)
27.  $w_3 \leftarrow t_5 - t_6 + t_4 - m_1;$  (3A)
28.  $w_4 \leftarrow t_7 + t_8;$  (1A)
29.  $w_5 \leftarrow t_7 - t_8 + t_4 + m_1 - m_4 - m_{10};$  (5A)
30. **else**
31.  $t_0 \leftarrow m_4 + m_8 + m_{14}; t_1 \leftarrow m_6 + m_{12};$  (3A)
32.  $t_2 \leftarrow t_1 + m_{10}; t_3 \leftarrow m_2 + m_{14};$  (2A)
33.  $t_4 \leftarrow t_3 - m_8; t_5 \leftarrow -m_0 + m_6 - m_{12};$  (3A)
34.  $t_6 \leftarrow -t_3 + m_5 - m_8 + m_{11};$  (3A)
35.  $t_7 \leftarrow t_1 + m_0 - m_3 - m_9; t_8 \leftarrow m_1 + m_{13};$  (4A)
36.  $w_0 \leftarrow t_0 - t_2 + m_5 - m_9;$  (3A)
37.  $w_1 \leftarrow t_0 + t_2 + m_3 - m_7 + m_{11} - m_{13};$  (5A)
38.  $w_2 \leftarrow t_4 + t_5;$  (1A)
39.  $w_3 \leftarrow t_4 - t_5 - t_8 + m_7;$  (3A)
40.  $w_4 \leftarrow t_6 + t_7;$  (1A)
41.  $w_5 \leftarrow t_6 - t_7 + t_8 - m_4 + m_7 - m_{10};$  (5A)
42. **end if**
43. **return**  $w_0 + w_1\sigma + w_2\rho + w_3\sigma\rho + w_4\rho^2 + w_5\sigma\rho^2;$

---

**Algorithm 6** Computation of  $(u_0 + u_1\sigma + u_2\rho) \cdot (v_0 + v_1\sigma + v_2\rho + v_3\sigma\rho + v_4\rho^2 + v_5\sigma\rho^2)$ .

---

**Input:**  $U, V \in \mathbb{F}_{3^{6m}}$  with  $U = u_0 + u_1\sigma + u_2\rho$  and  $V = v_0 + v_1\sigma + v_2\rho + v_3\sigma\rho + v_4\rho^2 + v_5\sigma\rho^2$ .

**Output:**  $W = U \cdot V$ . The algorithm requires 12 multiplications and 51 additions over  $\mathbb{F}_{3^m}$ .

1.  $a_0 \leftarrow u_0 + u_2; a_{10} \leftarrow u_0 - u_2;$  (2A)
  2.  $r_1 \leftarrow v_0 + v_4; a_2 \leftarrow r_1 + v_2; a_{12} \leftarrow r_1 - v_2;$  (3A)
  3.  $r_0 \leftarrow v_0 - v_4; a_7 \leftarrow r_0 - v_3; a_{17} \leftarrow r_0 + v_3;$  (3A)
  4.  $r_2 \leftarrow v_1 + v_5; a_3 \leftarrow r_2 + v_3; a_{13} \leftarrow r_2 - v_3;$  (3A)
  5.  $a_5 \leftarrow u_1 + u_2; a_{15} \leftarrow u_1 - u_2;$  (2A)
  6.  $r_0 \leftarrow v_1 - v_5; a_8 \leftarrow r_0 + v_2; a_{18} \leftarrow r_0 - v_2;$  (3A)
  7.  $a_1 \leftarrow a_0 + u_1; a_4 \leftarrow a_2 + a_3; a_6 \leftarrow u_0 + a_5;$  (3A)
  8.  $a_9 \leftarrow a_7 + a_8; a_{11} \leftarrow a_{10} + u_1; a_{14} \leftarrow a_{12} + a_{13};$  (3A)
  9.  $a_{16} \leftarrow u_0 + a_{15}; a_{19} \leftarrow a_{17} + a_{18};$  (2A)
  10.  $m_0 \leftarrow a_0 \cdot a_2; m_1 \leftarrow a_1 \cdot a_4; m_2 \leftarrow u_1 \cdot a_3;$  (3M)
  11.  $m_3 \leftarrow u_0 \cdot a_7; m_4 \leftarrow a_6 \cdot a_9; m_5 \leftarrow a_5 \cdot a_8;$  (3M)
  12.  $m_6 \leftarrow a_{10} \cdot a_{12}; m_7 \leftarrow a_{11} \cdot a_{14}; m_8 \leftarrow u_1 \cdot a_{13};$  (3M)
  13.  $m_9 \leftarrow u_0 \cdot a_{17}; m_{10} \leftarrow a_{16} \cdot a_{19}; m_{11} \leftarrow a_{15} \cdot a_{18};$  (3M)
  14. **if**  $b = 1$  **then**
  15.  $t_0 \leftarrow m_0 + m_4; t_1 \leftarrow m_2 + m_{10};$  (2A)
  16.  $t_2 \leftarrow -m_8 + m_2; t_3 \leftarrow m_6 - m_0;$  (2A)
  17.  $t_4 \leftarrow -m_8 - m_2 + m_5 + m_{11};$  (3A)
  18.  $t_5 \leftarrow m_6 + m_0 - m_3 - m_9;$  (3A)
  19.  $w_0 \leftarrow -t_0 + t_1 - m_3 + m_{11};$  (3A)
  20.  $w_1 \leftarrow t_0 + t_1 - m_1 + m_5 + m_9;$  (4A)
  21.  $w_2 \leftarrow t_2 + t_3;$  (1A)
  22.  $w_3 \leftarrow t_2 - t_3 + m_7 - m_1;$  (3A)
  23.  $w_4 \leftarrow t_4 + t_5;$  (1A)
  24.  $w_5 \leftarrow t_4 - t_5 + m_7 + m_1 - m_4 - m_{10};$  (5A)
  25. **else**
  26.  $t_0 \leftarrow m_4 + m_8; t_1 \leftarrow m_6 + m_{10};$  (2A)
  27.  $t_2 \leftarrow m_2 - m_8; t_3 \leftarrow -m_0 + m_6;$  (2A)
  28.  $t_4 \leftarrow -m_2 + m_5 - m_8 + m_{11};$  (3A)
  29.  $t_5 \leftarrow m_6 + m_0 - m_3 - m_9;$  (3A)
  30.  $w_0 \leftarrow t_0 - t_1 + m_5 - m_9;$  (3A)
  31.  $w_1 \leftarrow t_0 + t_1 + m_3 - m_7 + m_{11};$  (4A)
  32.  $w_2 \leftarrow t_2 + t_3;$  (1A)
  33.  $w_3 \leftarrow t_2 - t_3 - m_1 + m_7;$  (3A)
  34.  $w_4 \leftarrow t_4 + t_5;$  (1A)
  35.  $w_5 \leftarrow t_4 - t_5 + m_1 - m_4 + m_7 - m_{10};$  (5A)
  36. **end if**
  37. **return**  $w_0 + w_1\sigma + w_2\rho + w_3\sigma\rho + w_4\rho^2 + w_5\sigma\rho^2;$
- 

---

**Algorithm 7** Computation of  $(u_0 + u_1\sigma + u_2\rho - \rho^2) \cdot (v_0 + v_1\sigma + v_2\rho - \rho^2)$ .

---

**Input:**  $U = (u_0 + u_1\sigma + u_2\rho - \rho^2)$  and  $V = v_0 + v_1\sigma + v_2\rho - \rho^2 \in \mathbb{F}_{3^{6m}}$ .

**Output:**  $W = U \cdot V \in \mathbb{F}_{3^{6m}}$ .

1.  $a_0 \leftarrow u_0 + u_1; a_1 \leftarrow u_0 + u_2; a_2 \leftarrow u_1 + u_2;$  (3A)
  2.  $a_3 \leftarrow v_0 + v_1; a_4 \leftarrow v_0 + v_2; a_5 \leftarrow v_1 + v_2;$  (3A)
  3.  $a_6 \leftarrow u_2 + v_2;$  (1A)
  4.  $m_1 \leftarrow u_0 \cdot v_0; m_2 \leftarrow u_1 \cdot v_1; m_3 \leftarrow u_2 \cdot v_2;$  (3M)
  5.  $m_4 \leftarrow a_0 \cdot a_3; m_5 \leftarrow a_1 \cdot a_4; m_6 \leftarrow a_2 \cdot a_5;$  (3M)
  6.  $w_0 \leftarrow m_1 - m_2 - ba_6;$  (2A)
  7.  $w_1 \leftarrow m_4 - m_1 - m_2;$  (2A)
  8.  $w_2 \leftarrow m_5 - m_1 - m_3 - a_6 + b;$  (4A)
  9.  $w_3 \leftarrow m_6 - m_2 - m_3;$  (2A)
  10.  $w_4 \leftarrow 1 + m_3 - u_0 - v_0;$  (3A)
  11.  $w_5 \leftarrow -u_1 - v_1;$  (1A)
  12. **return**  $w_0 + w_1\sigma + w_2\rho + w_3\sigma\rho + w_4\rho^2 + w_5\sigma\rho^2;$
- 

---

**Algorithm 8** First multiplication of the reversed-loop  $\eta_T$  pairing calculation.

---

**Input:**  $U = \lambda y_P t - \lambda y_Q \sigma - \lambda y_P \rho$  and  $V = -t^2 + y_P y_Q \sigma - t\rho - \rho^2$ .

**Output:**  $W = U \cdot V \in \mathbb{F}_{3^{6m}}$ .

1.  $m_0 \leftarrow y_Q \cdot t; m_1 \leftarrow y_P \cdot y_Q; m_2 \leftarrow y_P \cdot m_1;$  (3M)
  2.  $a_0 \leftarrow \lambda m_0 + \lambda m_2;$  (1A)
  3.  $c_0 \leftarrow t^3;$  (1C)
  4.  $m_3 \leftarrow a_0 \cdot t; m_4 \leftarrow y_P \cdot c_0; m_5 \leftarrow y_Q \cdot m_1;$  (3M)
  5.  $w_0 \leftarrow -\lambda m_4 + \lambda m_5 + b\lambda y_P;$  (2A)
  6.  $w_1 \leftarrow m_3;$  (1A)
  7.  $w_2 \leftarrow \lambda y_P;$  (1A)
  8.  $w_3 \leftarrow \lambda m_0 - \lambda m_2;$  (1A)
  9.  $w_5 \leftarrow \lambda y_Q;$  (1A)
  10. **return**  $w_0 + w_1\sigma + w_2\rho + w_3\sigma\rho + w_5\sigma\rho^2;$
-