Algorithms and arithmetic operators for computing the η_T pairing in characteristic three

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

Algorithms and Arithmetic Operators for Computing the η_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 η_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, $v_i \in \mathbb{F}_{3^m}$, $0 \le i \le 2$. 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 overs $\mathbb{F}_{3^m}$ (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: $W = U \cdot V \in \mathbb{F}_{3^{3m}}$.

$a_0 \leftarrow u_0 + u_1$; $a_1 \leftarrow u_0 + u_2$; $a_2 \leftarrow bu1 + u_2$; (3A)
$a_3 \leftarrow v_0 + v_1$; $a_4 \leftarrow v_0 + v_2$; $a_5 \leftarrow v_1 + bv_2$; (3A)
$m_0 \leftarrow u_0 \cdot v_0$; $m_1 \leftarrow u_1 \cdot v_1$; $m_2 \leftarrow u_2 \cdot v_2$; (3M)
$m_3 \leftarrow a_0 \cdot a_3$; $m_4 \leftarrow a_1 \cdot a_4$; $m_5 \leftarrow a_2 \cdot a_5$; (3M)
$a_6 \leftarrow m_0 - m_1$; (1A)
$w_0 \leftarrow a_6 - m_2 + bm_5$ (2A)
if $b = 1$ **then**
  $w_1 \leftarrow -a_6 + m_3 + m_5$; (2A)
else
  $w_1 \leftarrow -m_0 + m_3 + m_5$; (2A)
end if
$w_2 \leftarrow -a_6 + m_4$; (1A)
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 $u_i \in \mathbb{F}_{3^m}$, $0 \le i \le 2$. $V = U^2$ 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: $V = U^2 \in \mathbb{F}_{3^{3m}}$.

$a_0 \leftarrow u_0 + u_1$; $a_1 \leftarrow a_0 + u_2$; (2A)
$m_0 \leftarrow u_0^2$; $m_1 \leftarrow u_0 \cdot u_1$; $m_2 \leftarrow u_1 \cdot u_2$; (3M)
$m_3 \leftarrow u_2^2$; $m_4 \leftarrow a_1^2$; (2M)
$a_2 \leftarrow m_1 + m_2$; (1A)
$v_0 \leftarrow m_0 - bm_2$; (1A)
$v_1 \leftarrow bm_3 - a_2$; (1A)
$v_2 \leftarrow m_4 + a_2 - m_0$; (2A)
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, $v_i \in \mathbb{F}_{3^m}$, $0 \le i \le 2$. 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:

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

Algorithm 3 Inversion over $\mathbb{F}_{3^{3m}}$.

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

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

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

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

$$\begin{aligned} v_0 &= u_0^3 + bu_2^3 + u_4^3, & v_1 &= -u_1^3 - bu_3^3 - u_5^3, \\ v_2 &= u_2^3 - bu_4^3, & v_3 &= -u_3^3 + bu_5^3, \\ v_4 &= u_4^3, & v_5 &= -u_5^3. \end{aligned}$$

As our unified operator computes $-u_5^3$ in one clock cycle, cubing over $\mathbb{F}_{3^{6m}}$ 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 $\mathbb{F}_{3^{6m}}$, 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 explicitely 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: $V = (-t^2 + u\sigma - t\rho - \rho^2)^3 \in \mathbb{F}_{3^{6m}}$.

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 $\mathbb{F}_{3^{6m}}$

A. General Algorithm

Elements of $\mathbb{F}_{3^{6m}}$ can be represented as degree-2 polynomials over $\mathbb{F}_{3^{2m}}$. Gorla *et al.* introduced an evaluation-interpolation scheme to perform multiplication over $\mathbb{F}_{3^{6m}}$ by means of five multiplications over $\mathbb{F}_{3^{2m}}$ [1]. Then, Karatsuba-Ofman's algorithm allows one to compute each multiplication over $\mathbb{F}_{3^{2m}}$ 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 $\mathbb{F}_{3^{6m}}$ involves 15 multiplications over $\mathbb{F}_{3^m}$ (Algorithm 5).

B. Multiplication by a Sparse Operand

The last multiplication over $\mathbb{F}_{3^{6m}}$ of the η_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 η_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 $\mathbb{F}_{3^{6m}}$ 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

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

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 $\mathbb{F}_{3^{6m}}$, 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 $\mathbb{F}_{3^{6m}}$ of the η_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 $\mathbb{F}_{3^m}$.

$r_0 \leftarrow u_0 + u_4$; $a_0 \leftarrow r_0 + u_2$; $a_{12} \leftarrow r_0 - u_2$; (3A)
$r_0 \leftarrow v_0 + v_4$; $a_3 \leftarrow r_0 + v_2$; $a_{15} \leftarrow r_0 - v_2$; (3A)
$r_0 \leftarrow u_0 - u_4$; $a_6 \leftarrow r_0 - u_3$; $a_{18} \leftarrow r_0 + u_3$; (3A)
$r_0 \leftarrow v_0 - v_4$; $a_9 \leftarrow r_0 - v_3$; $a_{21} \leftarrow r_0 + v_3$; (3A)
$r_0 \leftarrow u_1 + u_5$; $a_1 \leftarrow r_0 + u_3$; $a_{13} \leftarrow r_0 - u_3$; (3A)
$r_0 \leftarrow v_1 + v_5$; $a_4 \leftarrow r_0 + v_3$; $a_{16} \leftarrow r_0 - v_3$; (3A)
$r_0 \leftarrow u_1 - u_5$; $a_7 \leftarrow r_0 + u_2$; $a_{19} \leftarrow r_0 - u_2$; (3A)
$r_0 \leftarrow v_1 - v_5$; $a_{10} \leftarrow r_0 + v_2$; $a_{22} \leftarrow r_0 - v_2$; (3A)
$a_2 \leftarrow a_0 + a_1$; $a_5 \leftarrow a_3 + a_4$; $a_8 \leftarrow a_6 + a_7$; (3A)
$a_{11} \leftarrow a_9 + a_{10}$; $a_{14} \leftarrow a_{12} + a_{13}$; $a_{17} \leftarrow a_{15} + a_{16}$; (3A)
$a_{20} \leftarrow a_{18} + a_{19}$; $a_{23} \leftarrow a_{21} + a_{22}$; (2A)
$a_{24} \leftarrow u_4 + u_5$; $a_{25} \leftarrow v_4 + v_5$; (2A)
$m_0 \leftarrow a_0 \cdot a_3$; $m_1 \leftarrow a_2 \cdot a_5$; $m_2 \leftarrow a_1 \cdot a_4$; (3M)
$m_3 \leftarrow a_6 \cdot a_9$; $m_4 \leftarrow a_8 \cdot a_{11}$; $m_5 \leftarrow a_7 \cdot a_{10}$; (3M)
$m_6 \leftarrow a_{12} \cdot a_{15}$; $m_7 \leftarrow a_{14} \cdot a_{17}$; $m_8 \leftarrow a_{13} \cdot a_{16}$; (3M)
$m_9 \leftarrow a_{18} \cdot a_{21}$; $m_{10} \leftarrow a_{20} \cdot a_{23}$; $m_{11} \leftarrow a_{19} \cdot a_{22}$; (3M)
$m_{12} \leftarrow u_4 \cdot v_4$; $m_{13} \leftarrow a_{24} \cdot a_{25}$; $m_{14} \leftarrow u_5 \cdot v_5$; (3M)
if $b = 1$ **then**
  $t_0 \leftarrow m_0 + m_4 + m_{12}$; $t_1 \leftarrow m_2 + m_{10} + m_{14}$; (4A)
  $t_2 \leftarrow m_6 + m_{12}$; $t_3 \leftarrow -m_8 - m_{14}$; (2A)
  $t_4 \leftarrow m_7 + m_{13}$; $t_5 \leftarrow t_3 + m_2$; (2A)
  $t_6 \leftarrow t_2 - m_0$; $t_7 \leftarrow t_3 - m_2 + m_5 + m_{11}$; (4A)
  $t_8 \leftarrow t_2 + m_0 - m_3 - m_9$; (3A)
  $w_0 \leftarrow -t_0 + t_1 - m_3 + m_{11}$; (3A)
  $w_1 \leftarrow t_0 + t_1 - m_1 + m_5 + m_9 - m_{13}$; (5A)
  $w_2 \leftarrow t_5 + t_6$; (1A)
  $w_3 \leftarrow t_5 - t_6 + t_4 - m_1$; (3A)
  $w_4 \leftarrow t_7 + t_8$; (1A)
  $w_5 \leftarrow t_7 - t_8 + t_4 + m_1 - m_4 - m_{10}$; (5A)
else
  $t_0 \leftarrow m_4 + m_8 + m_{14}$; $t_1 \leftarrow m_6 + m_{12}$; (3A)
  $t_2 \leftarrow t_1 + m_{10}$; $t_3 \leftarrow m_2 + m_{14}$; (2A)
  $t_4 \leftarrow t_3 - m_8$; $t_5 \leftarrow -m_0 + m_6 - m_{12}$; (3A)
  $t_6 \leftarrow -t_3 + m_5 - m_8 + m_{11}$; (3A)
  $t_7 \leftarrow t_1 + m_0 - m_3 - m_9$; $t_8 \leftarrow m_1 + m_{13}$; (4A)
  $w_0 \leftarrow t_0 - t_2 + m_5 - m_9$; (3A)
  $w_1 \leftarrow t_0 + t_2 + m_3 - m_7 + m_{11} - m_{13}$; (5A)
  $w_2 \leftarrow t_4 + t_5$; (1A)
  $w_3 \leftarrow t_4 - t_5 - t_8 + m_7$; (3A)
  $w_4 \leftarrow t_6 + t_7$; (1A)
  $w_5 \leftarrow t_6 - t_7 + t_8 - m_4 + m_7 - m_{10}$; (5A)
end if
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 $\mathbb{F}_{3^m}$.

$a_0 \leftarrow u_0+u_2$; $a_{10} \leftarrow u_0-u_2$; (2A)
$r_1 \leftarrow v_0+v_4$; $a_2 \leftarrow r_1+v_2$; $a_{12} \leftarrow r_1-v_2$; (3A)
$r_0 \leftarrow v_0-v_4$; $a_7 \leftarrow r_0-v_3$; $a_{17} \leftarrow r_0+v_3$; (3A)
$r_2 \leftarrow v_1+v_5$; $a_3 \leftarrow r_2+v_3$; $a_{13} \leftarrow r_2-v_3$; (3A)
$a_5 \leftarrow u_1+u_2$; $a_{15} \leftarrow u_1-u_2$; (2A)
$r_0 \leftarrow v_1-v_5$; $a_8 \leftarrow r_0+v_2$; $a_{18} \leftarrow r_0-v_2$; (3A)
$a_1 \leftarrow a_0+u_1$; $a_4 \leftarrow a_2+a_3$; $a_6 \leftarrow u_0+a_5$; (3A)
$a_9 \leftarrow a_7+a_8$; $a_{11} \leftarrow a_{10}+u_1$; $a_{14} \leftarrow a_{12}+a_{13}$; (3A)
$a_{16} \leftarrow u_0+a_{15}$; $a_{19} \leftarrow a_{17}+a_{18}$; (2A)
$m_0 \leftarrow a_0\cdot a_2$; $m_1 \leftarrow a_1\cdot a_4$; $m_2 \leftarrow u_1\cdot a_3$; (3M)
$m_3 \leftarrow u_0\cdot a_7$; $m_4 \leftarrow a_6\cdot a_9$; $m_5 \leftarrow a_5\cdot a_8$; (3M)
$m_6 \leftarrow a_{10}\cdot a_{12}$; $m_7 \leftarrow a_{11}\cdot a_{14}$; $m_8 \leftarrow u_1\cdot a_{13}$; (3M)
$m_9 \leftarrow u_0\cdot a_{17}$; $m_{10} \leftarrow a_{16}\cdot a_{19}$; $m_{11} \leftarrow a_{15}\cdot a_{18}$; (3M)
if $b=1$ **then**
  $t_0 \leftarrow m_0+m_4$; $t_1 \leftarrow m_2+m_{10}$; (2A)
  $t_2 \leftarrow -m_8+m_2$; $t_3 \leftarrow m_6-m_0$; (2A)
  $t_4 \leftarrow -m_8-m_2+m_5+m_{11}$; (3A)
  $t_5 \leftarrow m_6+m_0-m_3-m_9$; (3A)
  $w_0 \leftarrow -t_0+t_1-m_3+m_{11}$; (3A)
  $w_1 \leftarrow t_0+t_1-m_1+m_5+m_9$; (4A)
  $w_2 \leftarrow t_2+t_3$; (1A)
  $w_3 \leftarrow t_2-t_3+m_7-m_1$; (3A)
  $w_4 \leftarrow t_4+t_5$; (1A)
  $w_5 \leftarrow t_4-t_5+m_7+m_1-m_4-m_{10}$; (5A)
else
  $t_0 \leftarrow m_4+m_8$; $t_1 \leftarrow m_6+m_{10}$; (2A)
  $t_2 \leftarrow m_2-m_8$; $t_3 \leftarrow -m_0+m_6$; (2A)
  $t_4 \leftarrow -m_2+m_5-m_8+m_{11}$; (3A)
  $t_5 \leftarrow m_6+m_0-m_3-m_9$; (3A)
  $w_0 \leftarrow t_0-t_1+m_5-m_9$; (3A)
  $w_1 \leftarrow t_0+t_1+m_3-m_7+m_{11}$; (4A)
  $w_2 \leftarrow t_2+t_3$; (1A)
  $w_3 \leftarrow t_2-t_3-m_1+m_7$; (3A)
  $w_4 \leftarrow t_4+t_5$; (1A)
  $w_5 \leftarrow t_4-t_5+m_1-m_4+m_7-m_{10}$; (5A)
end if
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: $W = U\cdot V \in \mathbb{F}_{3^{6m}}$.

$a_0 \leftarrow u_0+u_1$; $a_1 \leftarrow u_0+u_2$; $a_2 \leftarrow u_1+u_2$; (3A)
$a_3 \leftarrow v_0+v_1$; $a_4 \leftarrow v_0+v_2$; $a_5 \leftarrow v_1+v_2$; (3A)
$a_6 \leftarrow u_2+v_2$; (1A)
$m_1 \leftarrow u_0\cdot v_0$; $m_2 \leftarrow u_1\cdot v_1$; $m_3 \leftarrow u_2\cdot v_2$; (3M)
$m_4 \leftarrow a_0\cdot a_3$; $m_5 \leftarrow a_1\cdot a_4$; $m_6 \leftarrow a_2\cdot a_5$; (3M)
$w_0 \leftarrow m_1-m_2-ba_6$; (2A)
$w_1 \leftarrow m_4-m_1-m_2$; (2A)
$w_2 \leftarrow m_5-m_1-m_3-a_6+b$; (4A)
$w_3 \leftarrow m_6-m_2-m_3$; (2A)
$w_4 \leftarrow 1+m_3-u_0-v_0$; (3A)
$w_5 \leftarrow -u_1-v_1$; (1A)
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 η_T pairing calculation.

Input: $U = \lambda y_P t-\lambda y_Q\sigma-\lambda y_P\rho$ and $V = -t^2+y_Py_Q\sigma-t\rho-\rho^2$.
Output: $W = U\cdot V \in \mathbb{F}_{3^{6m}}$.

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