The formulae were reverse engineered from the work of *The Weil Pairing on Elliptic Curves and Its Cryptographic Applications, Appendix D*, 2011. A.E. Aftuk.

Operations in $\mathbb{F}_{p^2}$, distortion parameter β, curve $E : y^2 = x^3 + 1$.

Multiplication of scalars $\mathrm{mul}_\beta(x, y)$:

$$
\begin{aligned}
&a \leftarrow x \bmod \beta \\
&b \leftarrow (x \bmod \beta^2) - a \\
&c \leftarrow y \bmod \beta \\
&d \leftarrow (y \bmod \beta^2) - c \\
&\textbf{return } (ac - bd) + \beta(ad + bc - bd) \bmod p
\end{aligned}
\tag{1}
$$

Power of scalars $\mathrm{pow}_\beta(x, y)$:

$$
\begin{aligned}
&r \leftarrow 1 \\
&\textbf{while } x > 0 \\
&\quad | \quad \textbf{if } x = 1 \bmod 2 \\
&\quad | \quad\quad | \quad r \leftarrow \mathrm{mul}_\beta(r, y) \\
&\quad | \quad y \leftarrow \mathrm{mul}_\beta(y, y) \\
&\quad | \quad x \leftarrow \left\lfloor \frac{x}{2} \right\rfloor \\
&\textbf{return } r
\end{aligned}
\tag{2}
$$

Inverse of scalar $\mathrm{inv}_\beta(x)$:

$$
\begin{aligned}
&a \leftarrow x \bmod \beta \\
&b \leftarrow (x \bmod \beta^2) - a \\
&\textbf{return } \frac{a - b}{a^2 - ab + b^2} - \beta \frac{b}{a^2 - ab + b^2} \bmod p
\end{aligned}
\tag{3}
$$

Sum of points on E $\mathrm{sum}_E(P, Q)$:

if $P =$ "O" **and** $Q =$ "O"
  | **return** "O"
if $P =$ "O"
  | **return** Q
and $Q =$ "O"
  | **return** P
$x1, y1 \leftarrow P$
$x2, y2 \leftarrow Q$
if $(x1 \bmod p) = (x2 \bmod p)$ **and** $(y1 \bmod p) = (-y2 \bmod p)$
  | **return** "O" (4)
if $(x1 \bmod p) = (x2 \bmod p)$
  | $\lambda \leftarrow \dfrac{3x1^2}{2y1} \bmod \beta^2 + \beta + 1$
else
  | $\lambda \leftarrow \dfrac{y1 - y2}{x1 - x2} \bmod \beta^2 + \beta + 1$
$x3 \leftarrow \lambda^2 - x1 - x2 \bmod \beta^2 + \beta + 1$
$x3 \leftarrow \lambda(x3 - x1) + y1 \bmod \beta^2 + \beta + 1$
return $\{x3, -y3 \bmod p\}$

Calculate $x \times P$ **using double-and-add method** $\mathrm{dadd}_E(x, P)$:

$R \leftarrow$ "O"
while $x > 0$
  | **if** $x = 1 \bmod 2$
  | | $r \leftarrow \mathrm{sum}_E(R, P)$ (5)
  | $P \leftarrow \mathrm{sum}_E(P, P)$
  | $x \leftarrow \left\lfloor \dfrac{x}{2} \right\rfloor$
return r

$\mathrm{H}(P, Q)$:

$$
\begin{array}{l}
x1, y1 \leftarrow P \\
x2, y2 \leftarrow Q \\
\textbf{if } (x1 \bmod p) = (x2 \bmod p) \textbf{ and } (y1 \bmod p) = (-y2 \bmod p) \\
\quad | \quad \textbf{return } x - x1 \bmod \beta^2 + \beta + 1 \\
\textbf{if } (x1 \bmod p) = (x2 \bmod p) \textbf{ and } (y1 \bmod p) = (y2 \bmod p) \\
\quad | \quad \lambda \leftarrow \dfrac{3x1^2}{2y1} \bmod \beta^2 + \beta + 1 \\
\quad | \quad \textbf{return } \dfrac{y - y1 - \lambda(x - x1)}{x + x1 + x2 - \lambda^2} \bmod \beta^2 + \beta + 1 \\
\textbf{if } (x1 \bmod p) \neq (x2 \bmod p) \\
\quad | \quad \lambda \leftarrow \dfrac{y2 - y1}{x2 - x1} \bmod \beta^2 + \beta + 1 \\
\quad | \quad \textbf{return } \dfrac{y - y1 - \lambda(x - x1)}{x + x1 + x2 - \lambda^2} \bmod \beta^2 + \beta + 1
\end{array}
\tag{6}
$$

Perform the Miller calculation $\mathrm{miller}_E(m, P, R)$:

$$
\begin{array}{l}
f \leftarrow 1 \\
T \leftarrow P \\
mlist \leftarrow \textbf{reversed}(\textbf{as\_binary}(m)) \\
\textbf{for } i \textbf{ in } \textbf{reversed}(\textbf{range}(\textbf{length}(mlist))) \\
\quad | \quad f \leftarrow f^2 \mathrm{H}(T, T) \bmod \beta^2 + \beta + 1 \\
\quad | \quad f \leftarrow \textbf{eval}(f, x = R[0], y = R[1]) \bmod \beta^2 + \beta + 1 \\
\quad | \quad T \leftarrow \mathrm{sum}_E(T, T) \\
\quad | \quad \textbf{if } mlist[i] = 1 \\
\quad | \quad \quad | \quad f \leftarrow f\mathrm{H}(T, P) \bmod \beta^2 + \beta + 1 \\
\quad | \quad \quad | \quad T \leftarrow \mathrm{sum}_E(T, P) \\
\quad | \quad \quad | \quad f \leftarrow \textbf{eval}(f, x = R[0], y = R[1]) \bmod \beta^2 + \beta + 1 \\
\textbf{return } f
\end{array}
\tag{7}
$$

Create a weil pairing $\text{pairing}_E(m, P, Q, S)$:

$$
\begin{aligned}
&nS \leftarrow \{S[0], -S[1]\} \bmod \beta^2 + \beta + 1 \\
&A \leftarrow \text{miller}_E(m, P, \text{sum}_E(Q, S)) \\
&B \leftarrow \text{miller}_E(m, P, S) \\
&C \leftarrow \text{miller}_E(m, Q, \text{sum}_E(P, nS)) \\
&D \leftarrow \text{miller}_E(m, Q, nS) \\
&WP \leftarrow \frac{AD}{BC} \bmod \beta^2 + \beta + 1 \\
&\textbf{return } \textbf{numerator}(WP) \times \text{inv}_\beta(\textbf{denominator}(WP)) \bmod \beta^2 + \beta + 1
\end{aligned}
\tag{8}
$$