4.1 Computing $g(z) \mod z^2$

We denote $U_0(x) \equiv 1$ and $V_0(x) = v(x)$, and for $j = 0, 1, \ldots, \log n$ we denote $n_j = n/2^j$. We proceed in $m = \log n$ steps to compute the polynomials $U_j(x), V_j(x)$ ($j = 1, 2, \ldots, m$), such that the degrees of $U_j, V_j$ are at most $n_j - 1$, and moreover the polynomial $g_j(z) = \prod_{i=0}^{n_j-1} (V_j(\rho_i^{2^j}) - zU_j(\rho_i^{2^j}))$ has the same first two coefficients as $g(z)$. Namely,

$$g_j(z) \overset{\text{def}}{=} \prod_{i=0}^{n_j-1} \left( V_j(\rho_i^{2^j}) - zU_j(\rho_i^{2^j}) \right) = g(z) \pmod{z^2}.$$  \hfill (8)

Equation (8) holds for $j = 0$ by definition. Assume that we computed $U_j, V_j$ for some $j < m$ such that Equation (8) holds, and we show how to compute $U_{j+1}$ and $V_{j+1}$. From Equation (6) we know that $(\rho_{i+n_j/2})_{2^j} = -\rho_i^{2^j}$, so we can express $g_j$ as

$$g_j(z) = \prod_{i=0}^{n_j/2-1} \left( V_j(\rho_i^{2^j}) - zU_j(\rho_i^{2^j}) \right) \left( V_j(-\rho_i^{2^j}) - zU_j(-\rho_i^{2^j}) \right)$$

$$= \prod_{i=0}^{n_j/2-1} \left( V_j(\rho_i^{2^j})V_j(-\rho_i^{2^j}) - zU_j(-\rho_i^{2^j}) + U_j(-\rho_i^{2^j})V_j(\rho_i^{2^j}) \right) \pmod{z^2}$$

Denoting $f_{n_j}(x) \overset{\text{def}}{=} x^{n_j} + 1$ and observing that $\rho_i^{2^j}$ is a root of $f_{n_j}$ for all $i$, we next consider the polynomials:

$$A_j(x) \overset{\text{def}}{=} V_j(x)V_j(-x) \pmod{f_{n_j}(x)} \quad \text{(with coefficients } a_0, \ldots, a_{n_j-1})$$

$$B_j(x) \overset{\text{def}}{=} U_j(x)V_j(-x) + U_j(-x)V_j(x) \pmod{f_{n_j}(x)} \quad \text{(with coefficients } b_0, \ldots, b_{n_j-1})$$

and observe the following:

- Since $\rho_i^{2^j}$ is a root of $f_{n_j}$, then the reduction modulo $f_{n_j}$ makes no difference when evaluating $A_j, B_j$ on $\rho_i^{2^j}$. Namely we have $A_j(\rho_i^{2^j}) = V_j(\rho_i^{2^j})V_j(-\rho_i^{2^j})$ and similarly $B_j(\rho_i^{2^j}) = U_j(\rho_i^{2^j})V_j(-\rho_i^{2^j}) + U_j(-\rho_i^{2^j})V_j(\rho_i^{2^j})$ (for all $i$).

- The odd coefficients of $A_j, B_j$ are all zero. For $A_j$ this is because it is obtained as $V_j(x)V_j(-x)$ and for $B_j$ this is because it is obtained as $R_j(x) + R_j(-x)$ (with $R_j(x) = U_j(x)V_j(-x)$). The reduction modulo $f_{n_j}(x) = x^{n_j} + 1$ keeps the odd coefficients all zero, because $n_j$ is even.

We therefore set

$$U_{j+1}(x) \overset{\text{def}}{=} \sum_{t=0}^{n_j/2-1} b_{2^t} \cdot x^t, \quad \text{and} \quad V_{j+1}(x) \overset{\text{def}}{=} \sum_{t=0}^{n_j/2-1} a_{2^t} \cdot x^t,$$

so the second bullet above implies that $U_{j+1}(x^2) = B_j(x)$ and $V_{j+1}(x^2) = A_j(x)$ for all $x$. Combined with the first bullet, we have that

$$g_{j+1}(z) \overset{\text{def}}{=} \prod_{i=0}^{n_j/2-1} \left( V_{j+1}(\rho_i^{2^{j+1}}) - z \cdot U_{j+1}(\rho_i^{2^{j+1}}) \right)$$

$$= \prod_{i=0}^{n_j/2-1} \left( A_j(\rho_i^{2^j}) - z \cdot B_j(\rho_i^{2^j}) \right) \equiv g_j(z) \pmod{z^2}.$$  \hfill (mod $z^2$)

By the induction hypothesis we also have $g_j(z) = g(z)$ (mod $z^2$), so we get $g_{j+1}(z) = g(z)$ (mod $z^2$), as needed.
4.2 Recovering the scaled inverse $w$

Once we reach the last step above, we have two constant polynomials $U_m, V_m$ such that $g(z) = V_m - zU_m \pmod{z^2}$. It follows that $d = \text{resultant}(v, f_n) = V_m$, and the free term of the scaled inverse $w(x) = d \cdot (v^{-1}(x) \pmod{f_n(x)})$ is $w_0 = -U_m/n$.

We can now use the same technique to recover all the other coefficients of $w$: Note that since we work modulo $f_n(x) = x^n + 1$, then the coefficient $w_i$ is the free term of the scaled inverse of $x^i \cdot v \pmod{f_n}$.

In our case we only need to recover the first two coefficients, however, since we are only interested in the case where $w_1/w_0 = w_2/w_1 = \cdots = w_{n-1}/w_{n-2} = -w_0/w_{n-1} \pmod{d}$, where $d = \text{resultant}(v, f_n)$. After recovering $w_0, w_1$ and $d = \text{resultant}(v, f_n)$, we therefore compute the ratio $r = w_1/w_0 \pmod{d}$ and verify that $r^n = -1 \pmod{d}$. Then we recover as many coefficients of $w$ as we need (via $w_{i+1} = [w_i \cdot r]_d$), until we find one coefficient which is an odd integer, and that coefficient is the secret key.