$$\tilde{L}_2 = (L_{21}, \ldots, L_{2n}), \quad L_{2k} : \mathbb{F}_q^m \to \mathbb{F}_q^m$$
$$L_{2k}(\underline{y}_k) = \underline{y}_k B_{2k}, \quad B_{2k} = (B_{ij}^k) \in \mathrm{M}_{m\times m}(\mathbb{F}_q), \quad |B_{2k}| \neq 0$$

$$L_3 = \rho \circ \tilde{L}_3 \circ \tilde{\pi}_2, \quad \tilde{L}_3 = (L_{31}, \ldots, L_{3n}),$$
$$L_{3k}(\underline{z}_k) = \underline{z}_k C_{3k}, \quad C_{3k} = (C_{ij}^k) \in \mathrm{M}_{n\times n}(\mathbb{F}_q), \quad |C_{3k}| \neq 0$$

$$A_1 \in \mathrm{M}_{m\times m}(\mathbb{Z}_{q^n-1}), \quad \gcd(|A_1|, q^n - 1) = 1$$
$$G_1 : (\mathbb{F}_{q^n})^m \to (\mathbb{F}_{q^n})^m, \quad G_1(u_1, \ldots, u_m) = (u_1^{a_{11}} \ldots u_m^{a_{1m}}, \ldots, u_1^{a_{m1}} \ldots u_m^{a_{mm}})$$

$$A_1^{-1} \in \mathrm{M}_{m\times m}(\mathbb{Z}_{q^n-1}), \quad (\mathbb{F}_{q^n} \setminus \{0\})^n$$

$$A_2 \in \mathrm{M}_{n\times n}(\mathbb{Z}_{q^m-1}), \quad \gcd(|A_2|, q^m - 1) = 1$$
$$G_2 : (\mathbb{F}_{q^m})^n \to (\mathbb{F}_{q^m})^n, \quad G_2(v_1, \ldots, v_n) = (v_1^{b_{11}} \ldots v_n^{b_{1n}}, \ldots, v_1^{b_{n1}} \ldots v_n^{b_{nn}})$$

$$F(x_1, \ldots, x_{nm}) = (z_1, \ldots, z_{mn}), \quad F_k(\underline{x}) \in \mathbb{F}_q[x_1, \ldots, x_{nm}]$$
$$DM : \mathbb{F}_q^N \to \mathbb{F}_q^{nm} \quad F^{-1}(\underline{z}) = L_1^{-1} \circ G_1^{-1} \circ L_2^{-1} \circ G_2^{-1} \circ L_3^{-1}(\underline{z})$$

$$\overline{x}_1, \ldots, \overline{x}_k \in \mathbb{F}_q^N, \quad \underline{x}_i = H(\overline{x}_i) \in \mathbb{F}_q^{nm}$$

$$\underline{z}_i, \quad (\underline{z}_i)_j = F_j(\underline{x}_i) = \sum_u f_{u,j} M_u(\underline{x}_i)$$

$$\underline{z} = DM(\overline{x}), \quad \underline{z} \in \mathbb{F}_q^{nm}$$

$$h_1 : \{1, \ldots, N\} \to \{1, \ldots, nm\}$$
$$s = \mathrm{sig}(\overline{z}) = (\overline{z}, \overline{x}, h_1)$$
$$\overline{y} = DM_B(\overline{x}), \quad \overline{z} = DM_A^{-1}(\overline{y})$$

$$HAS : \mathbb{F}_2^e \to \mathbb{F}_2^b, \quad q = 2^e \quad b < e \cdot N, \quad w = HAS(x)$$