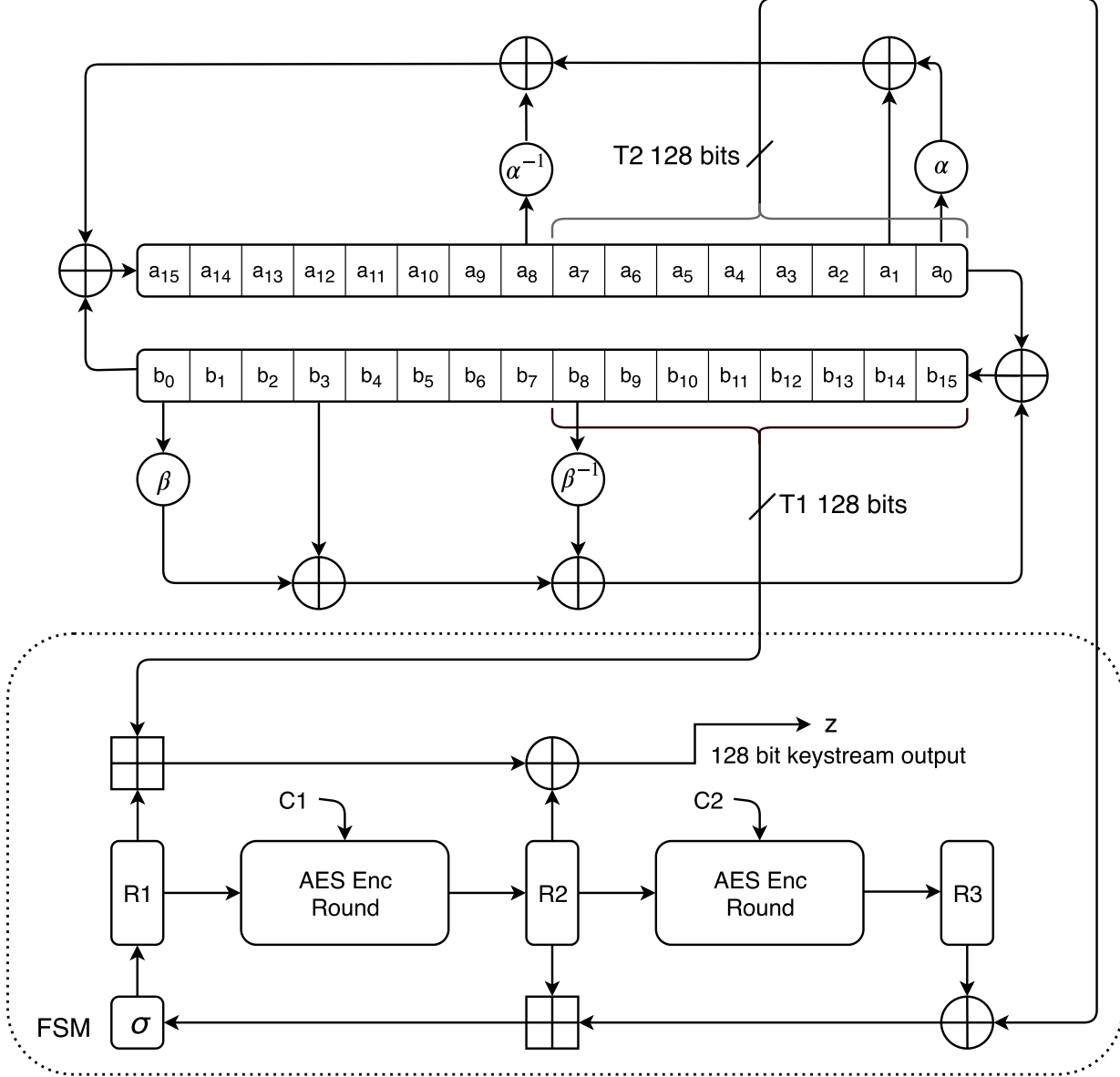


SNOW-V

$$g^A(x) = x^{16} + x^{15} + x^{12} + x^{11} + x^8 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$$

$$g^B(x) = x^{16} + x^{15} + x^{14} + x^{11} + x^8 + x^6 + x^5 + x + 1 \in \mathbb{F}_2[x].$$

When we consider these elements of $\mathbb{F}_{2^{16}}$ as words, the x^0 position will be the least significant bit in the word. Let $\alpha \in \mathbb{F}_{2^{16}}^A$ be a root of $g^A(x)$ and $\beta \in \mathbb{F}_{2^{16}}^B$ be a root of $g^B(x)$. At time $t \geq 0$ we denote the states of the LFSRs as $(a_{15}^{(t)}, a_{14}^{(t)}, \dots, a_1^{(t)}, a_0^{(t)})$, $a_i^{(t)} \in \mathbb{F}_{2^{16}}^A$ and $(b_{15}^{(t)}, b_{14}^{(t)}, \dots, b_1^{(t)}, b_0^{(t)})$, $b_i^{(t)} \in \mathbb{F}_{2^{16}}^B$ respectively for LFSR-A and LFSR-B. Referring to



Feedback relations:

$$T1_t, T2_{t+1}, T2_{t+2} \Rightarrow T2_{t+3}$$

$$T2_{t+1}T1_t, T1_{t+1} \Rightarrow T1_{t+2}$$

FSM relations:

$$R_{t+3}, R_{t+1}, R_t, T2_t$$

Output relations:

$$T1_t, R_{t+2}, R_{t+1}, z_t$$