

Note: $x \boxminus y = (x - y) \bmod 1024$

$$f_1(x) = (x \ggg 7) \oplus (x \ggg 18) \oplus (x \gg 3)$$

$$f_2(x) = (x \ggg 17) \oplus (x \ggg 19) \oplus (x \gg 10)$$

$$g_1(x, y) = ((x \ggg 10) \oplus (y \ggg 23)) + Q[(x \oplus y) \bmod 1024]$$

$$g_2(x, y) = ((x \ggg 10) \oplus (y \ggg 23)) + P[(x \oplus y) \bmod 1024]$$

$$h_1(x) = Q[x_0] + Q[256 + x_1] + Q[512 + x_2] + Q[768 + x_3]$$

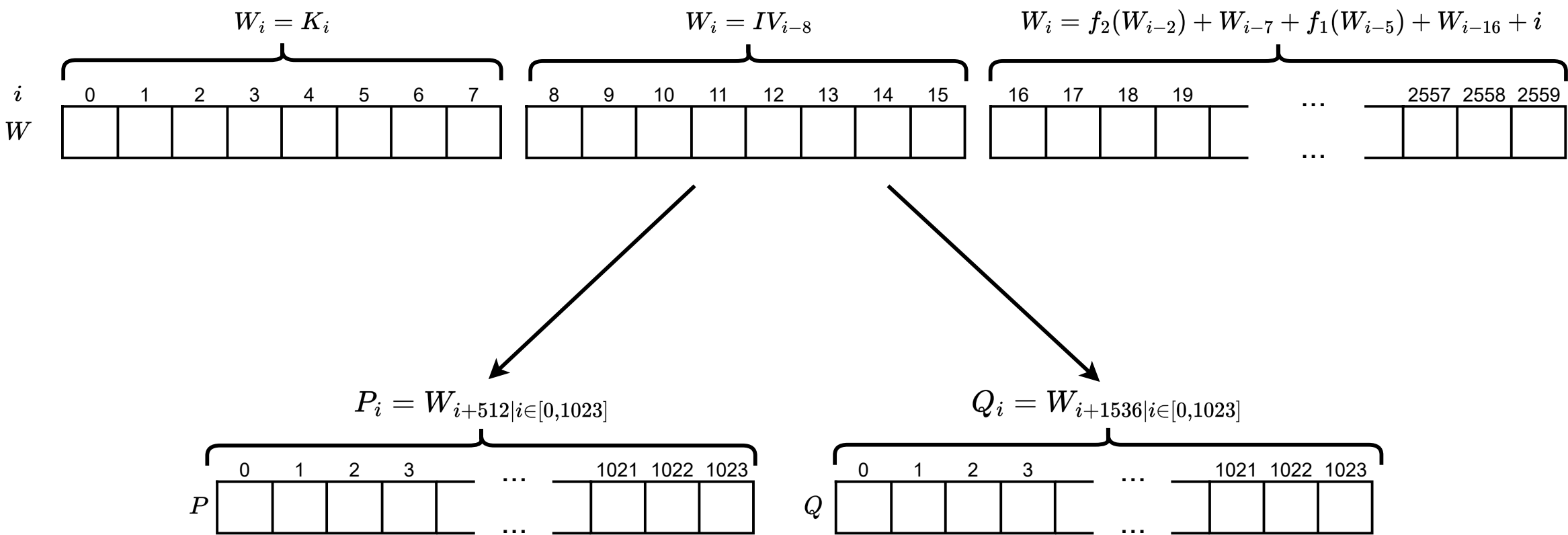
$$h_2(x) = P[x_0] + P[256 + x_1] + P[512 + x_2] + P[768 + x_3]$$

Initialization process

Key $K = K_0 K_1 K_2 \dots K_7$

Initialization vector $IV = IV_0 IV_1 IV_2 \dots IV_7$

\Rightarrow Array $W = W_0 W_1 W_2 \dots W_{2559}$



Keystream generation process

