

FIG. 1

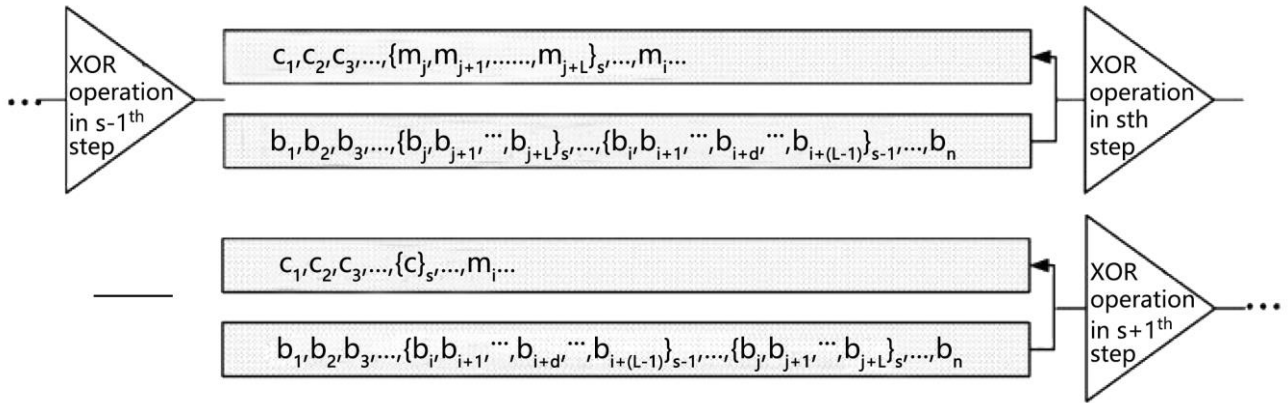


FIG. 2

where:

$$P_s = P(b_j) = P(S, b'_{s-1}) = P(S, (0 \times b_i b_{i+1} b_{i+2} \dots b_{i+d}))$$

$$L_s = p(b_{j+L}) - p(b_j) = L(S, b'_{s-1}) = L(S, (0 \times b_i b_{i+1} b_{i+2} \dots b_{i+d}))$$

$$F_s = F(S, b'_{s-1}) = F(0 \times b_i b_{i+1} b_{i+2} \dots b_{i+d})$$

$L-1$ refers to the length of the previous step

$0 \times b_i b_{i+1} b_{i+2} \dots b_{i+d}$ is the hexadecimal number carried by the calculation unit in the previous step

