

$$C = \underbrace{0 \ 1 \ 2 \ 3 \ 4 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 0 \ 1 \ 2 \ 3 \ A \ B \ C \ D \ E \ F \ F \ F \ F \ F \ F \ F \ 0 \ 1 \ 2 \ 3 \ E \ F \ C \ D \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ A \ B}_{\left(0^5, 1^6, 2^6, 3^6, 4^6, 5^4, 6^3, 7^3, 8^3, 9^3, A^2, B^2, C^2, D^2, E^2, F^8\right)}$$

$S = 1$



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

0 1 2 3 4 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 4 0 1 2 3 A B C D...



1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15



$i = 2$

$s = 2$



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

0 1 2 3 4 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 4 0 1 2 3 A B C D...

2 1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15



$i = 3$

$S = 1$



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

0 1 2 3 4 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 4 0 1 2 3 A B C D...

2 1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15



$i = 3$

Diagram illustrating the A2 operation on a 64-bit input C . The input C is divided into four 16-bit segments. The first segment (bits 1-16) is processed by a function A (green) to produce the first 16 bits of the output $A2(C)$. The second segment (bits 17-32) is processed by a function B (blue) to produce the next 16 bits of the output. The third segment (bits 33-48) is processed by a function C (red) to produce the next 16 bits of the output. The fourth segment (bits 49-64) is processed by a function D (green) to produce the final 16 bits of the output. The output $A2(C)$ is shown as a 64-bit sequence with the first 16 bits being 0, the next 16 bits being 5, the next 16 bits being 4, and the final 16 bits being 7.