

TABLE 9: Summary of the cube attack on 6-step MORUS-640-128.

Cube index	Involved secret variables $J$	Degree	Output bit	Time complexity
3, 4, 7, 15, 20, 24, 30, 31, 40, 43, 50, 60, 70, 79, 86, 89, 95, 96, 97, 102, 103, 106, 111, 116	1, 5, 7, 8, 26, 34, 36, 45, 46, 47, 48, 54, 58, 64, 84, 94, 105, 112, 117, 125	14	$s_{0,0}^{-10}[9]$	$2^{39.9}$
2, 6, 10, 29, 31, 32, 35, 40, 42, 51, 54, 66, 73, 78, 80, 85, 95, 100, 115, 118, 124, 126	4, 7, 13, 16, 18, 42, 57, 61, 73, 80, 83, 90, 96, 104, 108, 109, 112, 121	15	$s_{0,0}^{-10}[4]$	$2^{38.5}$
10, 12, 15, 22, 25, 26, 28, 44, 45, 54, 56, 59, 66, 67, 68, 74, 76, 80, 92, 96, 99, 103, 108, 127	1, 5, 7, 11, 21, 24, 39, 43, 54, 59, 77, 78, 82, 90, 95, 101, 116, 117, 126, 127	16	$s_{0,0}^{-10}[6]$	$2^{41.6}$
4, 26, 32, 33, 37, 49, 52, 54, 62, 67, 76, 79, 81, 85, 92, 102, 105, 106, 108, 124, 126	0, 1, 5, 11, 12, 15, 16, 18, 29, 31, 38, 40, 41, 42, 47, 50, 56, 59, 63, 64, 77, 82, 86, 94, 95, 101, 110, 120	15	$s_{0,0}^{-10}[1]$	$2^{39.9}$
13, 18, 25, 37, 38, 39, 46, 54, 56, 62, 70, 72, 76, 80, 85, 92, 96, 102, 105, 122, 125, 126	15, 16, 19, 21, 25, 34, 43, 49, 59, 69, 75, 84, 89, 98, 115, 121	12	$s_{0,0}^{-10}[4]$	$2^{35.4}$
13, 18, 25, 37, 38, 39, 46, 54, 56, 62, 70, 72, 76, 80, 85, 92, 96, 102, 105, 122, 125, 126	25, 33, 19, 73, 54, 1, 27, 42, 77, 103, 114, 16, 14, 52, 34, 8, 68, 36, 94, 123, 7, 24, 43, 56, 101	16	$s_{0,0}^{-10}[9]$	$2^{41.8}$
2, 21, 31, 36, 46, 49, 50, 52, 54, 55, 56, 72, 73, 76, 94, 95, 109, 111, 118, 123	7, 8, 22, 23, 31, 33, 40, 41, 45, 49, 54, 63, 69, 71, 73, 83, 92, 99, 111, 122, 124, 127	13	$s_{0,0}^{-10}[7]$	$2^{35.4}$
4, 7, 11, 14, 16, 18, 28, 29, 33, 41, 47, 53, 56, 64, 70, 88, 89, 95, 109, 111, 114, 119, 121	0, 5, 8, 13, 22, 23, 27, 34, 35, 39, 40, 43, 45, 46, 49, 64, 82, 84, 85, 94, 102, 104, 113, 117, 118, 124	15	$s_{0,0}^{-10}[9]$	$2^{41.1}$
1, 3, 8, 16, 26, 27, 36, 43, 60, 61, 66, 71, 75, 79, 85, 89, 92, 94, 101, 102, 106, 108, 118	7, 25, 27, 29, 33, 39, 44, 53, 58, 60, 62, 64, 71, 72, 76, 77, 88, 95, 99, 111, 112, 114, 116, 125	15	$s_{0,0}^{-10}[6]$	$2^{40.5}$
0, 2, 7, 8, 15, 20, 35, 40, 42, 45, 48, 55, 73, 76, 78, 89, 91, 110, 120, 122	4, 5, 7, 8, 23, 25, 27, 30, 33, 37, 44, 49, 53, 61, 62, 68, 72, 76, 77, 81, 100, 104, 107, 114, 127	12	$s_{0,0}^{-10}[6]$	$2^{34.2}$
0, 1, 10, 15, 23, 26, 33, 39, 66, 68, 73, 78, 84, 88, 94, 100, 101, 105, 111, 116, 119, 127	2, 8, 16, 18, 29, 31, 38, 40, 42, 46, 48, 50, 55, 60, 66, 76, 84, 85, 86, 89, 102, 106, 107, 108, 121	16	$s_{0,0}^{-10}[3]$	$2^{40.7}$
0, 16, 23, 26, 27, 28, 39, 41, 48, 67, 72, 79, 81, 82, 90, 92, 94, 99, 100, 110, 112, 123	1, 6, 7, 8, 25, 34, 36, 46, 48, 57, 62, 63, 70, 72, 81, 88, 89, 93, 94, 116, 117, 119, 127	15	$s_{0,0}^{-10}[9]$	$2^{39.6}$
3, 8, 10, 11, 14, 18, 20, 25, 33, 35, 37, 45, 50, 63, 78, 95, 101, 102, 110, 111, 116, 117, 118	1, 7, 15, 17, 21, 23, 27, 40, 48, 54, 57, 60, 64, 65, 86, 104, 105, 110, 111, 119, 127	14	$s_{0,0}^{-10}[1]$	$2^{37.5}$
5, 13, 22, 26, 30, 44, 48, 54, 65, 71, 81, 84, 85, 86, 87, 89, 94, 98, 106, 107	1, 6, 31, 32, 36, 45, 46, 49, 50, 51, 56, 68, 75, 78, 88, 90, 94, 103, 104, 113	12	$s_{0,0}^{-10}[5]$	$2^{34.8}$
2, 17, 18, 20, 28, 40, 41, 51, 52, 53, 63, 73, 75, 88, 94, 98, 110, 111, 113, 124, 125, 127	2, 16, 20, 35, 37, 48, 50, 52, 55, 58, 61, 74, 76, 77, 82, 84, 87, 97, 106	14	$s_{0,0}^{-10}[3]$	$2^{37.8}$
0, 1, 2, 6, 7, 9, 12, 18, 25, 28, 40, 44, 47, 61, 64, 67, 74, 82, 96, 116	9, 12, 19, 22, 24, 31, 52, 53, 55, 62, 73, 78, 93, 99, 101, 111, 118, 119	14	$s_{0,0}^{-10}[8]$	$2^{35.9}$
0, 11, 22, 29, 33, 47, 52, 55, 56, 62, 65, 71, 72, 80, 83, 90, 93, 99, 101, 102, 117, 120	1, 6, 9, 10, 14, 16, 18, 32, 42, 45, 51, 55, 59, 64, 65, 81, 82, 84, 87, 103, 106, 112, 122	15	$s_{0,0}^{-10}[2]$	$2^{39.3}$
12, 13, 18, 19, 22, 24, 50, 52, 55, 57, 61, 72, 77, 86, 90, 93, 94, 105, 112, 117, 118, 126	4, 6, 14, 21, 28, 34, 37, 41, 44, 45, 52, 60, 62, 73, 75, 79, 86, 88, 92, 95, 96, 98, 111, 115, 116, 126	15	$s_{0,0}^{-10}[7]$	$2^{41.4}$
3, 4, 6, 7, 17, 20, 21, 26, 31, 40, 41, 45, 53, 56, 60, 65, 66, 67, 68, 81, 82, 83, 90, 98, 103, 111, 115, 124	2, 3, 6, 8, 16, 22, 27, 33, 36, 55, 59, 63, 67, 78, 81, 91, 92, 97, 99, 104, 105, 106, 108, 110, 116	14	$s_{0,0}^{-10}[6]$	$2^{44.4}$
5, 7, 8, 18, 21, 27, 31, 36, 38, 43, 44, 47, 61, 77, 78, 79, 83, 87, 94, 99, 104, 110, 113, 118, 126	6, 8, 14, 23, 27, 32, 40, 56, 64, 72, 81, 87, 93, 96, 111, 116, 127	15	$s_{0,0}^{-10}[7]$	$2^{41.2}$
0, 11, 15, 20, 28, 42, 43, 48, 49, 51, 62, 66, 69, 71, 72, 79, 85, 89, 90, 105, 107, 114, 120	3, 4, 30, 33, 52, 60, 63, 67, 105, 112, 122, 123	12	$s_{0,0}^{-10}[72]$	$2^{36}$
2, 3, 6, 10, 12, 15, 18, 43, 44, 45, 47, 48, 55, 56, 63, 65, 77, 80, 82, 89, 98, 99, 109, 115, 126	7, 8, 12, 17, 22, 37, 71, 77, 89, 96, 100, 124	12	$s_{0,0}^{-10}[24]$	$2^{37}$
2, 5, 7, 10, 19, 22, 29, 41, 47, 48, 51, 53, 55, 58, 73, 78, 84, 100, 101, 102, 114, 115, 126	23, 25, 35, 40, 46, 56, 70, 74, 76, 81, 119	11	$s_{0,0}^{-10}[98]$	$2^{34}$
3, 4, 7, 15, 20, 24, 30, 31, 40, 43, 50, 60, 70, 79, 86, 89, 95, 96, 97, 102, 103, 106, 111, 116	1, 12, 19, 21, 39, 50, 58, 59, 66, 68, 73, 77, 78, 86, 90, 91, 96, 98, 105, 109, 116, 125	16	$s_{0,0}^{-10}[5]$	$2^{42.5}$