## Pr = 1 due to the ladder switch $xu_0$ $xu_1$ $xu_2$ MC ( MC ) (PermuteNibbles) (PermuteNibbles) 15 | 12 | 13 | 14 → SB 2 3 R Shift 2 | 3 R Shift → 15 12 | 13 14 → SB -5 6 Shuffle 10 9 11 + SB Shuffle 10 9 11 -(SB) 7 8 9 10 11 Shuffle 6 5 4 7 + SB 8 9 10 | 11 Shuffle 6 5 4 -(SB) 13 | 14 L Shift 1 2 0 + SB 12 13 14 | 15 L Shift 1 2 3 0 · SB $s_0$ $S_1$ ( MC ) MC (PermuteNibbles) (PermuteNibbles) 3 ← R Shift 15 SB -2 3 R Shift 12 14 ← SB 5 11 SB -6 11 SB) 6 Shuffle Shuffle 11 7 SB -9 10 11 7 SB) 9 10 Shuffle 6 5 8 Shuffle 6 5 13 14 SB 14 L Shift 0 SB $xl_0$ $xl_1$ $xu_3$ $xu_4$ $xu_2$ MC ( MC ) (PermuteNibbles) (PermuteNibbles) R Shift 15 12 13 | 14 → SB R Shift 12 | 13 | 14 |→ SB 4 5 6 Shuffle 10 9 11 + SB 4 5 6 Shuffle 10 9 8 11 + SB 10 Shuffle + SB 10 11 Shuffle → SB 12 13 14 12 14 2 3 0 + SB 13 2 3 0 + SB L Shift $s_1$ $s_2$ $s_3$ MC (PermuteNibbles) MC (PermuteNibbles) 14 ← SB → 3 R Shift 15 12 13 | 14 **← SB** • R Shift 12 5 7 Shuffle 10 8 11 -(SB) Shuffle 11 -(SB) 7 7 9 10 SB) 11 Shuffle 6 5 4 -SB 9 10 | 11 Shuffle 6 5 13 | 14 15 L Shift 1 2 3 0 SB 12 14 15 L Shift 2 3 0 SB) $xl_1$ $xl_2$ $xl_3$ $xu_5$ $xu_4$ MC ( MC ) (PermuteNibbles) (PermuteNibbles) 1 R Shift 15 12 2 13 → SB R Shift 12 13 14 → SB → 5 5 Shuffle 10 9 11 → SB Shuffle 11 -(SB) 10 9 10 11 Shuffle 6 5 4 7 - SB 9 10 | 11 5 + SB Shuffle 4 12 L Shift · SB - SB $s_4$ $s_3$ MC (PermuteNibbles) MC (PermuteNibbles) 0 2 3 12 13 14 -(SB) 2 3 R Shift 12 | 13 | 14 **← SB** • 1 R Shift 7 10 11 **← SB** • 5 7 Shuffle 11 **← SB** • 5 6 Shuffle 6 9 11 Shuffle 5 7 -(SB) 9 10 | 11 Shuffle 7 -(SB)+ 4 5 13 | 14 15 L Shift 2 3 0 SB -12 13 14 | 15 L Shift 2 3 0 SB) $xl_3$ $xl_4$ $xl_5$