



initial round   any   nonzero   integral   key branch 1   key branch 2   active tweak