kRunde+1, 0 = kRunde, 0 ⨁ substituiert(kRunde, 63) ⨁ Rundenkonstante

kRunde+1, j = kRunde, j ⨁ kRunde, j-1

Runde => Vorrunde (bei der 1. also Initialschlüssel)

j => Index des Schlüssels (zw. 0 und 63)