

$m + c$ blocks

$\mathcal{A}_{1,\dots,t}$

message
input

chaining
variable

$h_1^{\text{m.in}}$ $h_i^{\text{m.in}}$ $h_m^{\text{m.in}}$ $h_1^{\text{cv.in}}$ $h_i^{\text{cv.in}}$ $h_c^{\text{cv.in}}$

k blocks

$f^{(1)}$ $f^{(2)}$ $f^{(i)}$ $f^{(t)}$

h

$\mathcal{B}_{1,\dots,c}$

$h_1^{\text{cv.out}}$ $h_i^{\text{cv.out}}$ $h_c^{\text{cv.out}}$

output

c blocks