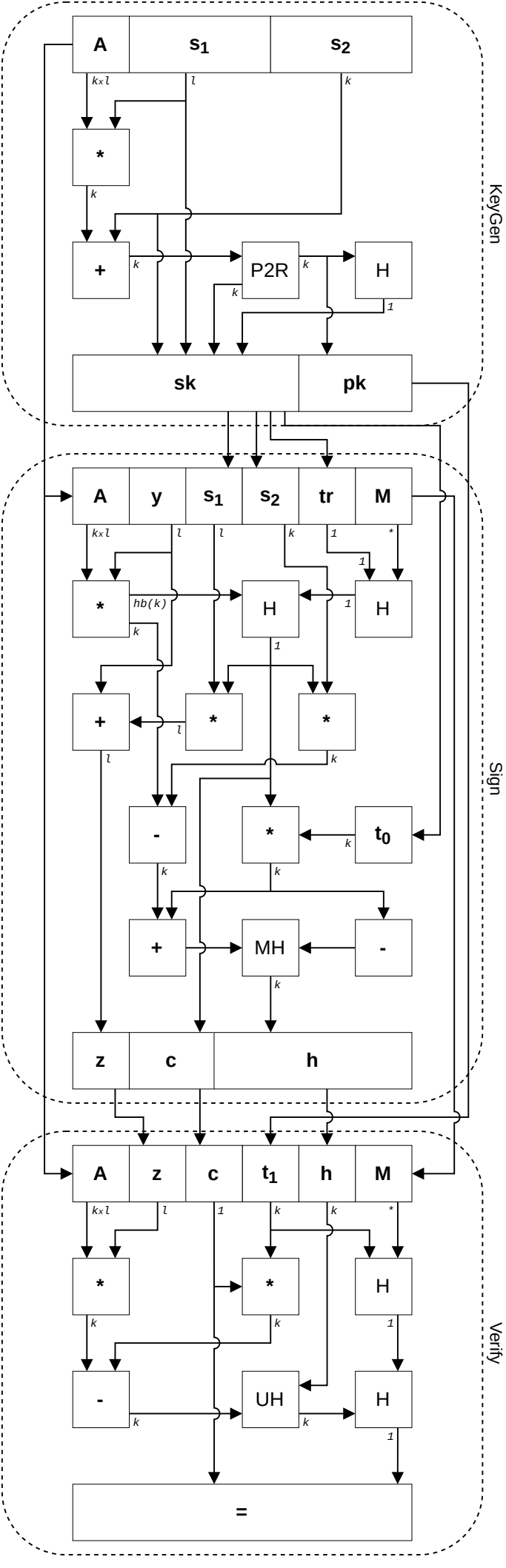
KeyGen
A
s1
s2
kxl
l
k
*
k
+
k
P2R
k
H
k
1
sk
pk
Sign
A
y
s1
s2
tr
M
kxl
l
l
k
1
*
1
*
hb(k)
k
H
1
H
1
+
l
*
*
l
k
-
*
t0
k
k
k
+
MH
-
k
z
c
h
Verify
A
z
c
t1
h
M
kxl
l
1
k
k
*
*
*
H
k
k
1
-
UH
H
k
k
1
=