

map-
ping
 k
 (i,σ)
?
MAP-INT

σ ?
 σ =
 σ =
 Σ =
 $\{0,1\}$
 $start_k$

σ =
 σ ?
 k, r
 k
 $start_k$

if
 $r \bmod$
 γ =
0
then
re-
turn
0
else
re-
turn

1
if
 $r \bmod$
 γ =
0
then
re-
turn
1
else
re-
turn
0

p_k
 k
 i
 $y_{i-1}^k[k] \neq y_i^k[k]$

(1)

k
 $c[k]$
 u_k
 v_k
 $c[k]$
 p_k
 $\mathcal{O}(r)$
 r
 k
 u_k
 v_k
 $r \in$
 $\{0,\ldots,M-$
1}
 u_k
 v_k
 σ
 u_k
 v_k
 u_k
 v_k
 $y^5 = 00101111000000000000$

$c[5] =$
15
 y^5
 u_5
 v_5
 $i \neq$

0
 $u_k[i]$
 $v_k[i]$
 $\sigma =$
 σ =
 σ =
0 =

$u_k[i] =$
 $v_k[i] =$
0
 u_k
 v_k
 $uv_k| =$

r
 $i \in$
 $\{0,\ldots,r-$
1}
 $\sigma =$
0
 u_k
 v_k
 $i \in$
 $0,\ldots,r-1$