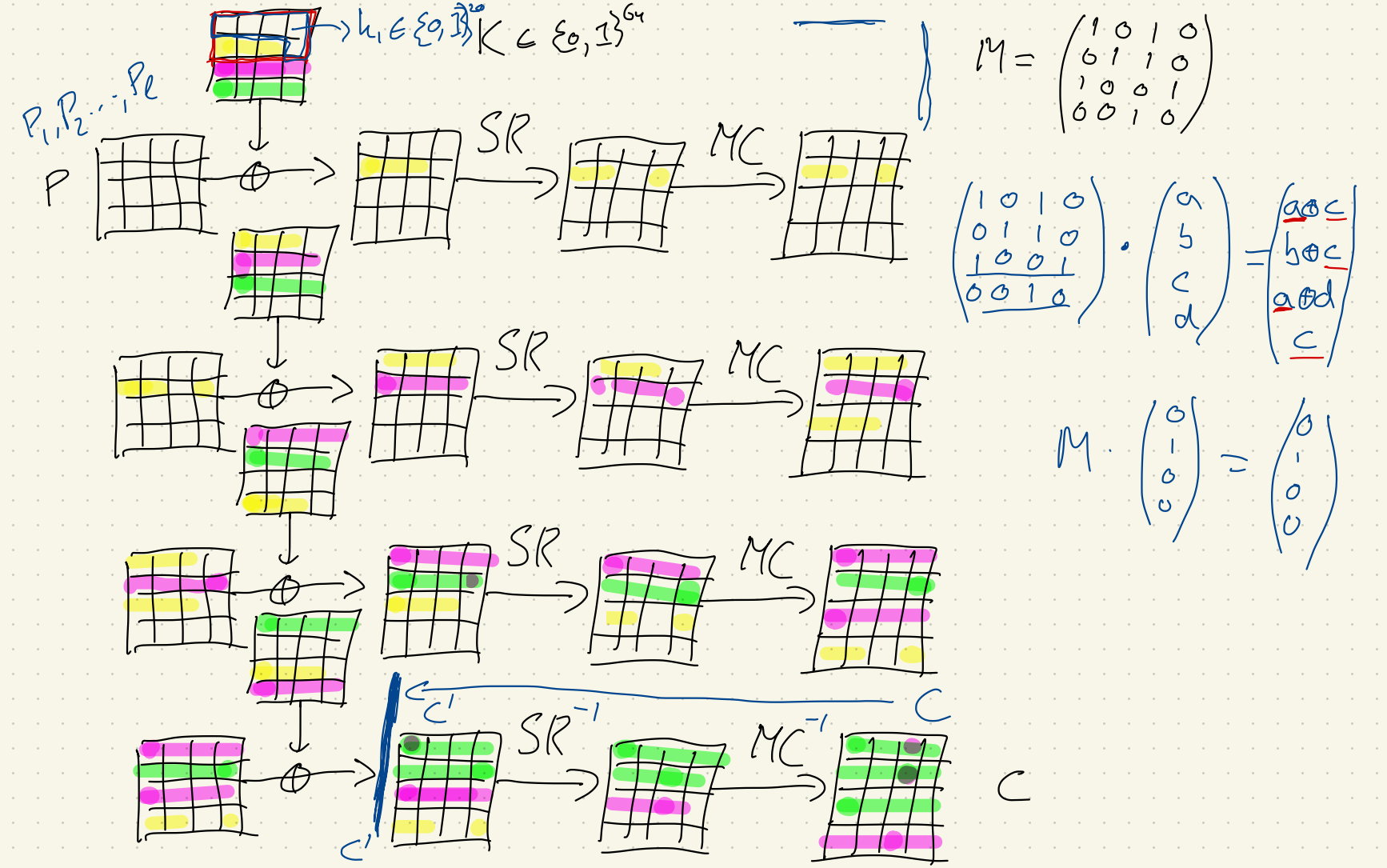
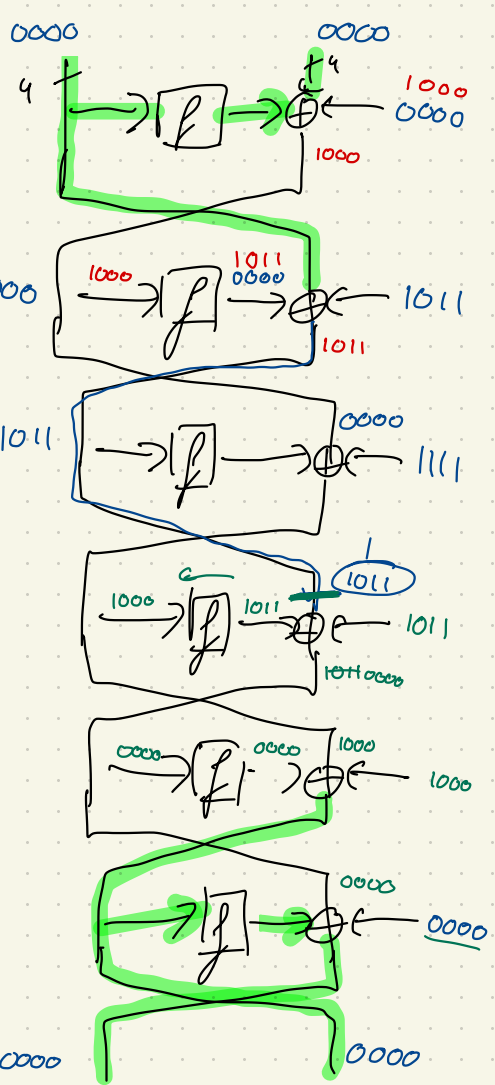
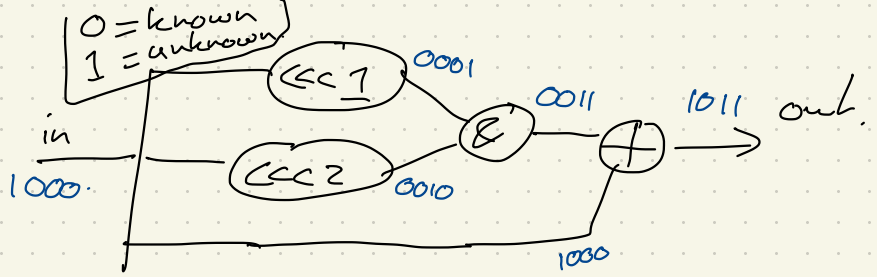
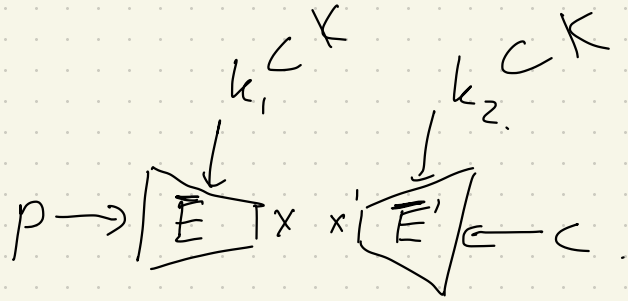

$k_i \in \{0,1\}^{32}$
$K \in \{0,1\}^{64}$
$P_1, P_2 \ldots, P_l$
P
SR
MC
SR
MC
SR
MC
C'
C
SR^{-1}
MC^{-1}
C'
C
$M = \begin{pmatrix} 1&0&1&0 \\ 0&1&1&0 \\ 1&0&0&1 \\ 0&0&1&0 \end{pmatrix}$
$\begin{pmatrix} 1&0&1&0 \\ 0&1&1&0 \\ 1&0&0&1 \\ 0&0&1&0 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \oplus c \\ b \oplus c \\ a \oplus d \\ c \end{pmatrix}$
$M \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$







$x \cap x' \neq \emptyset$

Phase 1

$H : X \to k_1$

for $k_1 \in K_1$:
  $x = []$
  for $p \in P$:
    $x \mathrel{+}= E_{k_1}(p)$
  $H[x] \to k_1$

Phase 2

for $k_2 \in K_2$:
  $x' = []$
  for $c \in C$
    $x' \mathrel{+}= E'_{k_2}(c)$
    if $x' \in H$:
      output $H[x']$, k_2 prob.