Ga

proc $\mathsf{Gb}^{\pi}(1^k, f)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 for $i \in PStates$ do
  $t \twoheadleftarrow \{0,1\}$
  $X_i^0[cid] \twoheadleftarrow \{0,1\}^{k-1} \parallel t$
  $X_i^1[cid] \twoheadleftarrow \{0,1\}^{k-1} \parallel \bar{t}$
 for $cid \leftarrow Cycles$ do
  for $i \in Inputs \cup Gates$ do
   $t \twoheadleftarrow \{0,1\}$
   $X_i^0[cid] \twoheadleftarrow \{0,1\}^{k-1} \parallel t$
   $X_i^1[cid] \twoheadleftarrow \{0,1\}^{k-1} \parallel \bar{t}$
  for $g \in Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g)$
   for $i \leftarrow 0$ to $1,\ j \leftarrow 0$ to 1 do
    $U \leftarrow X_a^i[cid],\ u \leftarrow lsb(U)$
    $V \leftarrow X_b^j[cid],\ v \leftarrow lsb(V)$
    $r \leftarrow G(g)[i, j]$
    $T \leftarrow g \parallel cid$
    $P[g, u, v][cid] \leftarrow$
     $\mathbb{E}^{\pi}(U, V, T, X_g^r[cid])$
  for $i \in PStates$ do
   $X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]$

 $F \leftarrow (n, m, p, q, A, B, P[Cycles])$
 $e \leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles])$
 $d \leftarrow (lsb(X_{Outputs}^0[Cycles])$
 return (F, e, d)

Ga

proc $\mathsf{Ev}^{\pi}(F, X)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 $(X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X$
 for $cid \leftarrow Cycles$ do
  for $g \in Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g)$
   $U \leftarrow X_a[cid],\ u \leftarrow lsb(U)$
   $V \leftarrow X_b[cid],\ v \leftarrow lsb(V)$
   $T \leftarrow g \parallel cid$
   $X_g[cid] \leftarrow$
    $\mathbb{D}^{\pi}(U, V, T, P[g, u, v][cid])$
  for $i \in PStatess$ do
   $X_i[cid+1] \leftarrow X_{S(i)}[cid]$

 return $X_{Outputs}[0, \cdots, c-1]$

Ga, GaX, GaXR

proc $\mathsf{En}(e, x)$
 $(X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles]) \leftarrow e$
 $(x_{Inputs}[Cycles]) \leftarrow x$
 for $cid \in Cycles, i \in Inputs$ do
  $Y_i[cid] \leftarrow X_i^{x_i[cid]}[cid]$

 return $Y \leftarrow$
  $(X_{PStates}^0[0], Y_{Inputs}[Cycles])$

GaX

proc $\mathsf{Gb}^{\pi}(1^k, f)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 $R \twoheadleftarrow \{0,1\}^{k-1} \parallel 1$
 for $i \in PStates$ do
  $X_i^0[0] \twoheadleftarrow \{0,1\}^k$
  $X_i^1[0] \leftarrow X_i^0 \oplus R$
 for $cid \leftarrow Cycles$ do
  for $i \in Inputs$ do
   $X_i^0[cid] \twoheadleftarrow \{0,1\}^k$
   $X_i^1[cid] \leftarrow X_i^0[cid] \oplus R$
  for $g \in Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g),$
   if $G(g) = XOR$ then
    $X_g^0[cid] \leftarrow X_a^0[cid] \oplus X_b^0[cid]$
    $X_g^1[cid] \leftarrow X_g^0[cid] \oplus R$
   else
    $X_g^0[cid] \twoheadleftarrow \{0,1\}^k$
    $X_g^1[cid] \leftarrow X_g^0[cid] \oplus R$
    for $i \leftarrow 0$ to $1,\ j \leftarrow 0$ to 1 do
     $U \leftarrow X_a^i[cid],\ u \leftarrow lsb(U)$
     $V \leftarrow X_b^j[cid],\ v \leftarrow lsb(V)$
     $r \leftarrow G(g)[i, j]$
     $T \leftarrow g \parallel cid$
     $P[g, u, v][cid] \leftarrow$
      $\mathbb{E}^{\pi}(U, V, T, X_g^r[cid])$
  for $i \in PStates$ do
   $X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]$

 $F \leftarrow (n, m, p, q, A, B, P[Cycles])$
 $e \leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles])$
 $d \leftarrow (lsb(X_{Outputs}^0[Cycles])$
 return (F, e, d)

GaX

proc $\mathsf{Ev}^{\pi}(F, X)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 $(X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X$
 for $cid \leftarrow Cycles$ do
  for $g \leftarrow Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g)$
   $U \leftarrow X_a[cid],\ u \leftarrow lsb(U)$
   $V \leftarrow X_b[cid],\ v \leftarrow lsb(V)$
   if $G(g) = XOR$ then
    $X_g[cid] \leftarrow U \oplus V$
   else
    $T \leftarrow g \parallel cid$
    $X_g[cid] \leftarrow$
     $\mathbb{D}^{\pi}(U, V, T, P[g, u, v][cid])$
  for $i \in PStatess$ do
   $X_i[cid+1] \leftarrow X_{S(i)}[cid]$

 return $X_{Outputs}[0, \cdots, c-1]$

Ga, GaX, GaXR

proc $\mathsf{De}(d, Y)$
 $(d_{Outputs}[Cycles]) \leftarrow d$
 $(Y_{Outputs}[Cycles]) \leftarrow Y$
 for $cid \in Cycles, i \in Outputs$ do
  $y_i[cid] \leftarrow lsb(Y_i[cid]) \oplus d_i[cid]$

 return $y \leftarrow (y_{Outputs}[Cycles])$

GaXR

proc $\mathsf{Gb}^{\pi}(1^k, f)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 $R \twoheadleftarrow \{0,1\}^{k-1} \parallel 1$
 for $i \in PStates$ do
  $X_i^0[0] \twoheadleftarrow \{0,1\}^k$
  $X_i^1[0] \leftarrow X_i^0 \oplus R$
 for $cid \leftarrow Cycles$ do
  for $i \in Inputs$ do
   $X_i^0[cid] \twoheadleftarrow \{0,1\}^k$
   $X_i^1[cid] \leftarrow X_i^0[cid] \oplus R$
  for $g \in Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g),$
   if $G(g) = XOR$ then
    $X_g^0[cid] \leftarrow X_a^0[cid] \oplus X_b^0[cid]$
    $X_g^1[cid] \leftarrow X_g^0[cid] \oplus R$
   else
     for $u \leftarrow 0$ to $1,\ v \leftarrow 0$ to 1 do
      $i \leftarrow u \oplus lsb(X_a^0[cid])$
      $j \leftarrow v \oplus lsb(X_a^0[cid])$
      $U \leftarrow X_a^i[cid]$
      $V \leftarrow X_b^j[cid]$
      $r \leftarrow G(g)[i, j]$
      $T \leftarrow g \parallel cid$
      if $u = 0$ and $v = 0$ then
       $X_g^r[cid] \leftarrow$
        $\mathbb{E}^{\pi}(U, V, T, 0^k)$
       $X_g^{\bar{r}}[cid] \leftarrow X_g^r[cid] \oplus R$
      else
       $P[g, u, v][cid] \leftarrow$
        $\mathbb{E}^{\pi}(U, V, T, X_g^r[cid])$
  for $i \in PStates$ do
   $X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]$

 $F \leftarrow (n, m, p, q, A, B, P[Cycles])$
 $e \leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles])$
 $d \leftarrow (lsb(X_{Outputs}^0[Cycles])$
 return (F, e, d)

GaXR

proc $\mathsf{Ev}^{\pi}(F, X)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 $(X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X$
 for $cid \leftarrow Cycles$ do
  for $g \leftarrow Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g)$
   $U \leftarrow X_a[cid],\ u \leftarrow lsb(U)$
   $V \leftarrow X_b[cid],\ v \leftarrow lsb(V)$
   $T \leftarrow g \parallel cid$
   if $G(g) = XOR$ then
    $X_g[cid] \leftarrow U \oplus V$
    $u = 0$ and $v = 0$ then
    $X_g[cid] \leftarrow$
     $\mathbb{E}^{\pi}(U, V, T, 0^k)$
   else
    $X_g[cid] \leftarrow$
     $\mathbb{D}^{\pi}(U, V, T, P[g, a, b][cid])$
  for $i \in PStatess$ do
   $X_i[cid+1] \leftarrow X_{S(i)}[cid]$
 return $X_{Outputs}[0, \cdots, c-1]$

Ga, GaX, GaXR

proc $\mathsf{ev}(f, x)$
 $(n, m, p, q, A, B, G, S, c) \leftarrow f$
 $w_{PState}[0] \leftarrow 0^p$
 for $cid \leftarrow Cycles$ do
  for $g \leftarrow Gates$ do
   $a \leftarrow A(g),\ b \leftarrow B(g)$
   $w_g[cid] \leftarrow G(g)[w_a[cid], w_b[cid]]$
  for $i \in PState$ do
   $w_i[cid+1] \leftarrow w_{S(i)}[cid]$

 return $y \leftarrow w_{Outputs}[Cycles]$