```
GaX
                                                                                                                                                                                                                                                                                 GaXR
                                                                                   Ga
proc \mathsf{Gb}^{\pi}(1^k, f)
                                                                                                   proc \mathsf{Gb}^{\pi}(1^k, f)
                                                                                                                                                                                                      proc \mathsf{Gb}^{\pi}(1^k, f)
    (n, m, p, q, A, B, G, S, c) \leftarrow f
                                                                                                       (n, m, p, q, A, B, G, S, c) \leftarrow f

R \leftarrow \{0, 1\}^{k-1} \parallel 1
                                                                                                                                                                                                          (n, m, p, q, A, B, G, S, c) \leftarrow f

R \leftarrow \{0, 1\}^{k-1} \parallel 1
    for i \in PStates do
                                                                                                       for i \in PStates do
                                                                                                                                                                                                           for i \in PStates do
           t \twoheadleftarrow \{0,1\}
            \begin{array}{l} X_i^0[cid] \twoheadleftarrow \{0,1\}^{k-1} \parallel t \\ X_i^1[cid] \twoheadleftarrow \{0,1\}^{k-1} \parallel \bar{t} \end{array} 
                                                                                                              \begin{array}{l} X_i^0[0] \twoheadleftarrow \{0,1\}^k \\ X_i^1[0] \leftarrow X_i^0 \oplus R \end{array}
                                                                                                                                                                                                                 \begin{matrix} X_i^0[0] \twoheadleftarrow \{0,1\}^k \\ X_i^1[0] \leftarrow X_i^0 \oplus R \end{matrix}
                                                                                                        for cid \leftarrow Cycles do
                                                                                                                                                                                                           for cid \leftarrow Cycles do
    for cid \leftarrow Cycles do
                                                                                                              for i \in Inputs do
                                                                                                                                                                                                                 for i \in Inputs do
           for i \in Inputs \cup Gates do
                                                                                                                     X_i^0[cid] \leftarrow \{0,1\}^k

X_i^1[cid] \leftarrow X_i^0[cid] \oplus R
                                                                                                                                                                                                                        X_i^0[cid] \leftarrow \{0,1\}^k

X_i^1[cid] \leftarrow X_i^0[cid] \oplus R
                  t \leftarrow \{0,1\}
                  X_{i}^{0}[cid] \leftarrow \{0,1\}^{k-1} \parallel t

X_{i}^{1}[cid] \leftarrow \{0,1\}^{k-1} \parallel \bar{t}
                                                                                                              for g \in Gates do
                                                                                                                                                                                                                 \text{ for } g \in Gates \text{ do }
                                                                                                                                                                                                                        a \leftarrow A(g), \ b \leftarrow B(g), if G(g) = XOR then
                                                                                                                     a \leftarrow A(g), \ b \leftarrow B(g), if G(g) = XOR then
           for g \in Gates do
                   a \leftarrow A(g), \ b \leftarrow B(g)
                                                                                                                                                                                                                            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
                                                                                                                         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
                  for i \leftarrow 0 to 1, j \leftarrow 0 to 1 do
                         U \leftarrow X_a^i[cid], \ u \leftarrow lsb(U)
                                                                                                               else
                                                                                                                                                                                                                  else
                         V \leftarrow X_b^j[cid], \ v \leftarrow lsb(V)
                                                                                                                        \begin{array}{l} X_g^0[cid] \leftarrow \{0,1\}^k \\ X_g^1[cid] \leftarrow X_g^0[cid] \oplus R \end{array}
                                                                                                                                                                                                                            for u \leftarrow 0 to 1, v \leftarrow 0 to 1 do
                         r \leftarrow G(g)[i,j]
                                                                                                                                                                                                                                   i \leftarrow u \oplus lsb(X_a^0[cid])
                         T \leftarrow g \parallel cid
                                                                                                                         for i \leftarrow 0 to 1, j \leftarrow 0 to 1 do
                                                                                                                                                                                                                                   j \leftarrow v \oplus lsb(X_a^0[cid])
                         P[g, u, v][cid] \leftarrow \\ \mathbb{E}^{\pi}(U, V, T, X_g^r[cid])
                                                                                                                                                                                                                                   U \leftarrow X_a^i[cid]
                                                                                                                               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]
                                                                                                                                                                                                                                   V \leftarrow X_b^j[cid]
           \text{ for } i \in PStates \text{ do }
                                                                                                                                                                                                                                   r \leftarrow G(g)[i,j]
                  X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]
                                                                                                                               T \leftarrow g \parallel cid
                                                                                                                                                                                                                                   T \leftarrow g \parallel cid
                                                                                                                               P[g, u, v][cid] \leftarrow \\ \mathbb{E}^{\pi}(U, V, T, X_g^r[cid])
                                                                                                                                                                                                                                   if u = 0 and v = 0 then
                                                                                                                                                                                                                                       X_g^r[cid] \leftarrow
                                                                                                              for i \in PStates do
                                                                                                                                                                                                                                           \mathbb{E}^{\pi}(U,V,T,0^k)
                                                                                                                     X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]
                                                                                                                                                                                                                                       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])
                                                                                                                                                                                                          \begin{aligned} F &\leftarrow (n, m, p, q, A, B, P[Cycles]) \\ e &\leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles]) \end{aligned}
                                                                                                        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])
    d \leftarrow (lsb(X_{Outputs}^{0}[Cycles])
                                                                                                                                                                                                           d \leftarrow (lsb(X^0_{Outputs}[Cycles])
    return (F, e, d)
                                                                                                       return (F, e, d)
                                                                                                                                                                                                           return (F, e, d)
                                                                                   Ga
                                                                                                                                                                                  GaX
                                                                                                                                                                                                                                                                                 GaXR
\operatorname{proc} \operatorname{Ev}^{\pi}(F,X)
                                                                                                   proc Ev^{\pi}(F,X)
                                                                                                                                                                                                      proc Ev^{\pi}(F,X)
     (n, m, p, q, A, B, G, S, c) \leftarrow f
                                                                                                        (n, m, p, q, A, B, G, S, c) \leftarrow f
                                                                                                                                                                                                           (n, m, p, q, A, B, G, S, c) \leftarrow f
     (X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X
                                                                                                       (X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X for cid \leftarrow Cycles do
                                                                                                                                                                                                           (X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X
    for cid \leftarrow Cycles do
                                                                                                                                                                                                           \overrightarrow{\text{for }} cid \leftarrow \overrightarrow{Cycles} \ \text{do}
           for g \in Gates do
                                                                                                              \text{for } g \leftarrow Gates \text{ do}
                                                                                                                                                                                                                 for g \leftarrow Gates do
                                                                                                                    \begin{array}{l} g \\ \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) \end{array}
                 \begin{array}{l} 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) \end{array}
                                                                                                                                                                                                                       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
                  T \leftarrow g \parallel cid
                                                                                                                                                                                                                        T \leftarrow g \parallel cid
                                                                                                                         X_g[cid] \leftarrow U \oplus V
                   X_g[cid] \leftarrow
                                                                                                                                                                                                                         if G(g) = XOR then
                                                                                                                                                                                                                            X_g[cid] \leftarrow U \oplus V
                       \mathbb{D}^{\pi}(\dot{U}, V, T, P[g, u, v][cid])
                                                                                                                         T \leftarrow g \parallel cid
           for i \in PStatess do
                                                                                                                                                                                                                            u=0 and v=0 then
                                                                                                                         X_{g}[\overrightarrow{cid}] \leftarrow \mathbb{D}^{\pi}(U, V, T, P[g, u, v][\overrightarrow{cid}])
                                                                                                                                                                                                                            X_g[cid] \leftarrow
                  X_i[cid+1] \leftarrow X_{S(i)}[cid]
                                                                                                                                                                                                                                 \mathbb{E}^{\pi}(U, V, T, 0^k)
                                                                                                              for i \in PStatess do
                                                                                                                                                                                                                  else
                                                                                                                     X_i[cid+1] \leftarrow X_{S(i)}[cid]
                                                                                                                                                                                                                            X_g[cid] \leftarrow
                                                                                                                                                                                                                                 \mathbb{D}^{\pi}(U, V, T, P[g, a, b][cid])
                                                                                                                                                                                                                  for i \in PStatess do
                                                                                                                                                                                                            \begin{array}{c} X_i[cid+1] \leftarrow X_{S(i)}[cid] \\ \text{return} \ \ X_{Outputs}[0,\cdots,c-1] \end{array}
                                                                                                        return X_{Outputs}[0,\cdots,c-1]
    return X_{Outputs}[0,\cdots,c-1]
                                                                                                                                                          Ga, GaX, GaXR
                                                                                                                                                                                                                                                              Ga, GaX, GaXR
                                                        Ga, GaX, GaXR
                                                                                                   proc De(d, Y)
                                                                                                                                                                                                      \mathsf{proc}\ \mathsf{ev}(f,x)
proc En(e, x)
                                                                                                        (d_{Outputs}[Cycles]) \leftarrow d
     \begin{array}{l} (X_{PStates}^{\{0,1\}}[0],X_{Inputs}^{\{0,1\}}[Cycles]) \leftarrow e \\ (x_{Inputs}[Cycles]) \leftarrow x \\ \text{for } cid \in Cycles, i \in Inputs \text{ do} \end{array} 
                                                                                                                                                                                                           (n, m, p, q, A, B, G, S, c) \leftarrow f
                                                                                                        (Y_{Outputs}[Cycles]) \leftarrow Y
                                                                                                                                                                                                           w_{PState}[0] \leftarrow 0^p
                                                                                                        for cid \in Cycles, i \in Outputs do
                                                                                                                                                                                                           for cid \leftarrow Cycles do
                                                                                                              y_i[cid] \leftarrow lsb(Y_i[cid]) \oplus d_i[cid]
                                                                                                                                                                                                                 for q \leftarrow Gates do
           Y_i[cid] \leftarrow X_i^{x_i[cid]}[cid]
                                                                                                                                                                                                                        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
                                                                                                        return y \leftarrow (y_{Outputs}[Cycles])
                                                                                                                                                                                                           return y \leftarrow w_{Outputs}[Cycles]
          (X_{PStates}^{0}[0], Y_{Inputs}[Cycles])
```