Ga	GaX	GaXR
proc $Gb^\pi(1^k, f)$ $(n, m, p, q, A, B, G, S, c) \leftarrow f$	$\begin{array}{c} proc\;Gb^\pi(1^k,f) \\ (n,m,p,q,A,B,G,S,c) \leftarrow f \end{array}$	$\begin{array}{c} proc\;Gb^\pi(1^k,f) \\ (n,m,p,q,A,B,G,S,c) \leftarrow f \end{array}$
$\begin{array}{c} \text{for } i \in PStates \text{ do} \\ t \twoheadleftarrow \{0,1\} \end{array}$	$R \twoheadleftarrow \{0,1\}^{k-1} \parallel 1$ for $i \in PStates$ do	$R \leftarrow \{0,1\}^{k-1} \parallel 1$ for $i \in PStates$ do
$X_i^0[cid] \leftarrow \{0,1\}^{k-1} \parallel t$	$X_i^0[0] \leftarrow \{0,1\}^k$	$X_i^0[0] \leftarrow \{0,1\}^k$
$X_i^1[cid] \leftarrow \{0,1\}^{k-1} \parallel \bar{t}$ for $cid \leftarrow Cycles$ do	$X_i^1[0] \leftarrow X_i^0 \oplus R$ for $cid \leftarrow Cycles$ do	$X_i^1[0] \leftarrow X_i^0 \oplus R$ for $cid \leftarrow Cycles$ do
for $i \in Inputs \cup Gates$ do $t \leftarrow \{0, 1\}$	for $i \in Inputs$ do $X_i^0[cid] \twoheadleftarrow \{0,1\}^k$	for $i \in Inputs$ do $X_i^0[cid] \twoheadleftarrow \{0,1\}^k$
$X_i^0[cid] \leftarrow \{0,1\}^{k-1} \parallel t$	$X_i^1[cid] \leftarrow X_i^0[cid] \oplus R$	$X_i^1[cid] \leftarrow X_i^0[cid] \oplus R$
$X_i^1[cid] \leftarrow \{0,1\}^{k-1} \parallel \bar{t}$ for $g \in Gates$ do	for $g \in Gates$ do $a \leftarrow A(g), b \leftarrow B(g),$	for $g \in Gates$ do $a \leftarrow A(g), b \leftarrow B(g),$
$a \leftarrow A(g), \ b \leftarrow B(g)$ for $i \leftarrow 0$ to $1, \ j \leftarrow 0$ to 1 do	if $G(g) = XOR$ then $X_{a}^{0}[cid] \leftarrow X_{a}^{0}[cid] \oplus X_{b}^{0}[cid]$	if $G(g) = XOR$ then $X_g^0[cid] \leftarrow X_a^0[cid] \oplus X_b^0[cid]$
$U \leftarrow X_a^i[cid], \ u \leftarrow lsb(U)$	$X_g^1[cid] \leftarrow X_g^0[cid] \oplus R$	$X_g^1[cid] \leftarrow X_g^0[cid] \oplus R$ else
$V \leftarrow X_b^j[cid], \ v \leftarrow lsb(V)$ $r \leftarrow G(g)[i,j]$	$X_g^0[cid] \leftarrow \{0,1\}^k$	for $u \leftarrow 0$ to $1, \ v \leftarrow 0$ to 1 do $i \leftarrow u \oplus lsb(X_a^0[cid])$
$T \leftarrow g \parallel cid \\ P[g, u, v][cid] \leftarrow$	$X_g^1[cid] \leftarrow X_g^0[cid] \oplus R$ for $i \leftarrow 0$ to $1, \ j \leftarrow 0$ to 1 do	$j \leftarrow v \oplus lsb(X_a^0[cid])$
$\mathbb{E}^{\pi}(U,V,T,X_{g}^{r}[cid])$ for $i\in PStates$ do	$U \leftarrow X_a^i[cid], \ u \leftarrow lsb(U)$ $V \leftarrow X_b^j[cid], \ v \leftarrow lsb(V)$	$U \leftarrow X_a^i[cid]$ $V \leftarrow X_b^j[cid]$
$X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]$	$r \leftarrow G(g)[i,j]$ $T \leftarrow g \parallel cid$	$ r \leftarrow G(g)[i,j] $ $ T \leftarrow g \parallel cid $
- (/	$P[g, u, v][cid] \leftarrow \\ \mathbb{E}^{\pi}(U, V, T, X_q^r[cid])$	$\begin{array}{c c} x \leftarrow g \parallel ctu \\ \text{if } u = 0 \text{ and } v = 0 \text{ then} \\ X_q^r[cid] \leftarrow \end{array}$
	for $i \in PStates$ do	$\mathbb{E}^{\pi}(U, V, T, 0^k)$
	$X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]$	$X_g^{ar{r}}[cid] \leftarrow X_g^r[cid] \oplus R$ else
		$P[g, u, v][cid] \leftarrow \\ \mathbb{E}^{\pi}(U, V, T, X_q^r[cid])$
		for $i \in PStates$ do $X_i^{\{0,1\}}[cid+1] \leftarrow X_{S(i)}^{\{0,1\}}[cid]$
		$A_i = [ctu + 1] \leftarrow A_{S(i)} [ctu]$
$F \leftarrow (n, m, p, q, A, B, P[Cycles])$	$F \leftarrow (n, m, p, q, A, B, P[Cycles])$	$F \leftarrow (n, m, p, q, A, B, P[Cycles])$
$e \leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles])$ $d \leftarrow (lsb(X_{Outputs}^{0}[Cycles])$	$e \leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles])$ $d \leftarrow (lsb(X_{Outputs}^{\{0,1\}}[Cycles])$	$e \leftarrow (X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles])$ $d \leftarrow (lsb(X_{Outputs}^{0}[Cycles])$
return (F, e, d)	return (F, e, d)	return (F, e, d)
	GaX proc $\operatorname{Ev}^\pi(F,X)$	$\begin{array}{c c} & \mathbf{GaXR} \\ proc \ Ev^\pi(F,X) \end{array}$
$(n, m, p, q, A, B, G, S, c) \leftarrow f$ $(X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X$	$(n, m, p, q, A, B, G, S, c) \leftarrow f$ $(X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X$	$(n, m, p, q, A, B, G, S, c) \leftarrow f$ $(X_{PStates}[0], X_{Inputs}[Cycles]) \leftarrow X$
for $cid \leftarrow Cycles$ do for $g \in Gates$ do	for $cid \leftarrow Cycles$ do for $q \leftarrow Gates$ do	for $cid \leftarrow Cycles$ do
$a \leftarrow A(g), \ b \leftarrow B(g)$	$a \leftarrow A(g), \ b \leftarrow B(g)$	for $g \leftarrow Gates$ do $a \leftarrow A(g), b \leftarrow B(g)$
$U \leftarrow X_a[cid], \ u \leftarrow lsb(U)$ $V \leftarrow X_b[cid], \ v \leftarrow lsb(V)$	$U \leftarrow X_a[cid], \ u \leftarrow lsb(U) $ $V \leftarrow X_b[cid], \ v \leftarrow lsb(V)$	$U \leftarrow X_a[cid], \ u \leftarrow lsb(U)$ $V \leftarrow X_b[cid], \ v \leftarrow lsb(V)$
$T \leftarrow g \parallel cid \\ X_q[cid] \leftarrow$	if $G(g) = XOR$ then $X_g[cid] \leftarrow U \oplus V$	$T \leftarrow g \parallel cid$ if $G(g) = XOR$ then
$\overset{\widetilde{\mathbb{D}}^{\pi}}{(U,V,T,P[g,u,v][cid])}$ for $i\in PStatess$ do	else $T \leftarrow g \parallel cid$	$X_g[cid] \leftarrow U \oplus V$ u = 0 and $v = 0$ then
$X_i[cid+1] \leftarrow X_{S(i)}[cid]$	$X_g[cid] \leftarrow \mathbb{D}^{\pi}(U, V, T, P[g, u, v][cid])$	$X_g[cid] \leftarrow \mathbb{E}^{\pi}(U, V, T, 0^k)$
	for $i \in PStatess$ do $X_i[cid+1] \leftarrow X_{S(i)}[cid]$	else
	$2 I_{i}[ciu + 1] \sim 2 I_{S(i)}[ciu]$	$X_g[cid] \leftarrow \mathbb{D}^{\pi}(U, V, T, P[g, a, b][cid])$
	ration V [0 at	for $i \in PStatess$ do $X_i[cid+1] \leftarrow X_{S(i)}[cid]$
return $X_{Outputs}[0,\cdots,c-1]$	return $X_{Outputs}[0, \cdots, c-1]$ Ga, GaX, GaXR	return $X_{Outputs}[0,\cdots,c-1]$
Ga, GaX, GaXR proc $En(e,x)$	$proc\ De(d,Y)$	Ga, GaX, GaXR proc ev (f,x)
$(X_{PStates}^{\{0,1\}}[0], X_{Inputs}^{\{0,1\}}[Cycles]) \leftarrow e$ $(x_{Inputs}[Cycles]) \leftarrow x$	$(d_{Outputs}[Cycles]) \leftarrow d$ $(Y_{Outputs}[Cycles]) \leftarrow Y$ for side Cockes is Contracted to	$(n, m, p, q, A, B, G, S, c) \leftarrow f$ $w_{PState}[0] \leftarrow 0^{p}$
for $cid \in Cycles, i \in Inputs$ do	for $cid \in Cycles, i \in Outputs$ do $y_i[cid] \leftarrow lsb(Y_i[cid]) \oplus d_i[cid]$	for $cid \leftarrow Cycles$ do for $g \leftarrow Gates$ 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 $Y \leftarrow (X^0 [0] Y [Caroloo])$	return $y \leftarrow (y_{Outputs}[Cycles])$	
$(X_{PStates}^{0}[0], Y_{Inputs}[Cycles])$	(goulputs[Ogeles])	return $y \leftarrow w_{Outputs}[Cycles]$