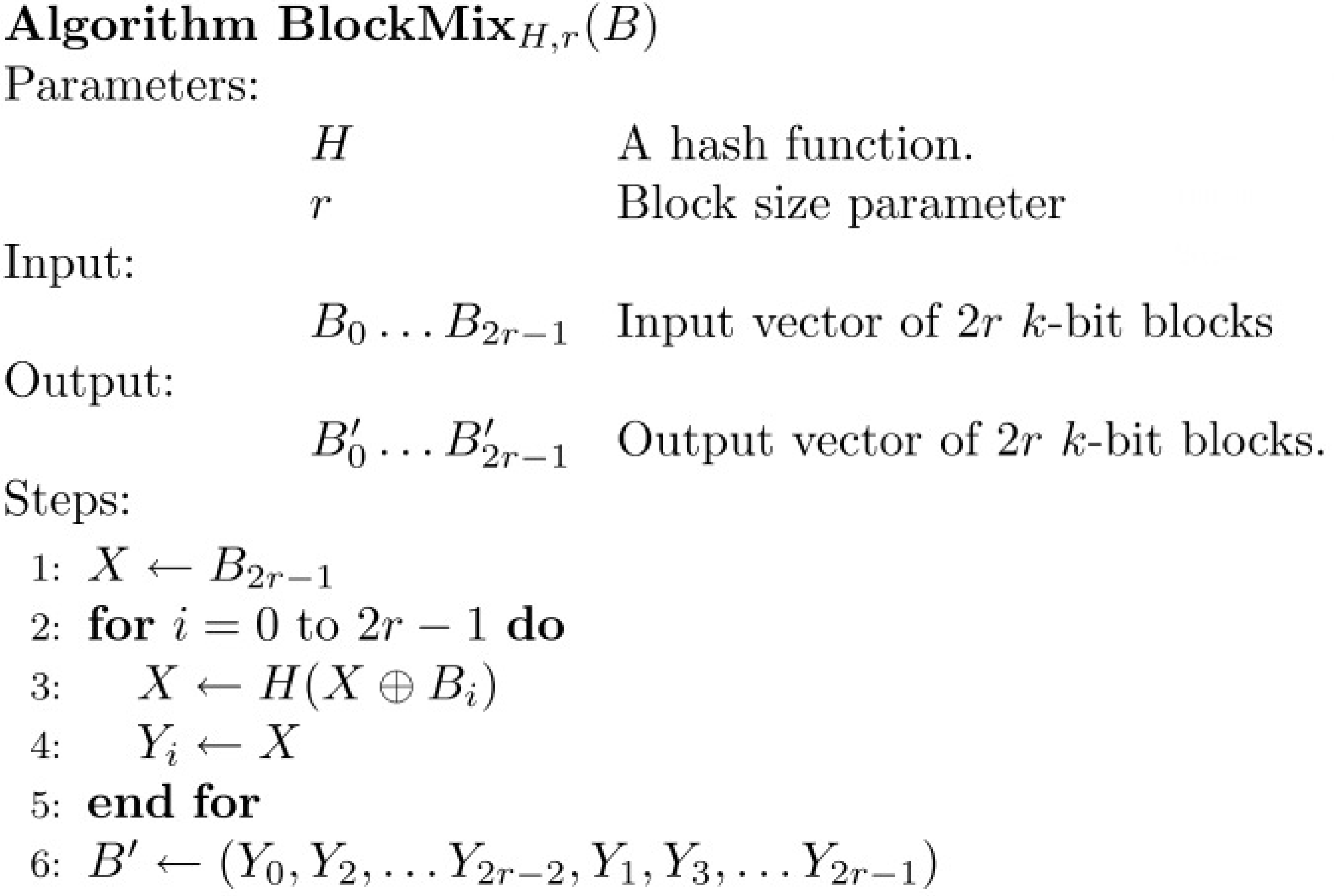

Algorithm BlockMix$_{H,r}(B)$

Parameters:

H	A hash function.
r	Block size parameter

Input:

$B_0 \ldots B_{2r-1}$	Input vector of $2r$ k-bit blocks

Output:

$B'_0 \ldots B'_{2r-1}$	Output vector of $2r$ k-bit blocks.

Steps:

```
$X \leftarrow B_{2r-1}$
for $i = 0$ to $2r - 1$ do
    $X \leftarrow H(X \oplus B_i)$
    $Y_i \leftarrow X$
end for
$B' \leftarrow (Y_0, Y_2, \ldots Y_{2r-2}, Y_1, Y_3, \ldots Y_{2r-1})$
```