Problem 8. «Bash-S3»

The sponge function Bash-f uses the permutation $S3$ that transforms a triple of 64-bit binary words a, b, c in the following way:

$$S3(a, b, c) = (b \vee \neg c \oplus a,\ \ a \vee c \oplus b,\ \ a \wedge b \oplus c).$$

Here $\neg$, $\wedge$, $\vee$, $\oplus$ denote the binary bitwise operations "NOT", "OR", "AND", "XOR" respectively. The operations are listed in descending order of priority. Let w^k also denote the cyclic shift of a 64-bit word w to the left by $k \in \{1, 2, \ldots, 63\}$ positions.

Alice wants to strengthen $S3$. She can add by XOR any input a, b, c or its cyclic shift to any output. She must use at least one cyclic shift and she cannot add two identical terms to the same output.

Help Alice to change $S3$ in such a way that a modified $S3$ will be still a permutation!

Remark 1. The descending order of operation priority means that, for example, in the expression $b \vee \neg c \oplus a$, we firstly calculate $\neg c$, then calculate $b \vee \neg c$, and after that the final result.

Remark 2. The modification

$$(b \vee \neg c \oplus a \oplus a^{11},\ \ a \vee c \oplus a^{7} \oplus c,\ \ a \wedge b \oplus b^{32})$$

is allowed but it does not satisfy the permutation condition.