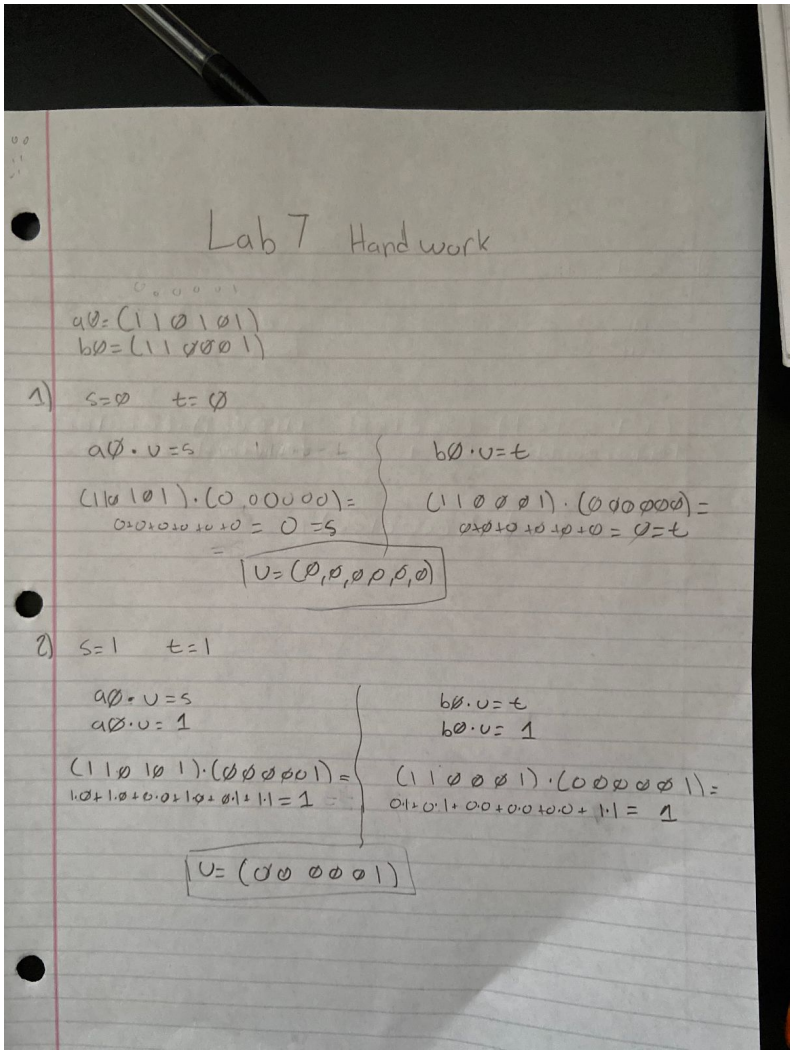
Report

For this lab, we are trying to find a random secret vector u such that a*u = s and b*u = t, where s and t are bits 0 1. Vectors a and b are fixed vectors provided in the book. The function secret_vector is a recursive function that generates a random vector u within GF(2) until a*u = s and b*u = t.

HandWork: Multiplying a0 and b0 vectors by a “random” u vector to produce the wanted s and t value. For the sake of the handwork and time, we used vectors that we knew would produce the solutions.



3) $s=1 \quad A=\emptyset$

$a\emptyset \cdot v = s$
$a\emptyset \cdot v = 1$

$b\emptyset \cdot v = t$
$b\emptyset \cdot v = \emptyset$

$(1\ 1\ \emptyset\ 1\ 0\ 1) \cdot (0\ 0\ 0\ 1\ 0\ \emptyset) =$
$1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 + \emptyset \cdot 0 + 1 \cdot \emptyset = 1$

$(1\ 1\ \emptyset\ \emptyset\ 0\ 1) \cdot (\emptyset\ 0\ 0\ 1\ 0\ \emptyset) =$
$1 \cdot \emptyset + 1 \cdot 0 + \emptyset \cdot 0 + \emptyset \cdot 1 + 0 \cdot 0 + 1 \cdot \emptyset = \emptyset$

$v = (0\ 0\ 0\ 1\ 0\ 0)$