

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 a_0 and b_0 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.

Lab 7 Handwork

$a_0 = (1 \ 1 \ 0 \ 1 \ 0 \ 1)$
 $b_0 = (1 \ 1 \ 0 \ 0 \ 0 \ 1)$

1) $s=0 \quad t=0$

$$\left. \begin{array}{l} a_0 \cdot u = s \\ (1 \ 1 \ 0 \ 1 \ 0 \ 1) \cdot (0 \ 0 \ 0 \ 0 \ 0 \ 0) = \\ 0+0+0+0+0+0 = 0 = s \end{array} \right\} \begin{array}{l} b_0 \cdot u = t \\ (1 \ 1 \ 0 \ 0 \ 0 \ 1) \cdot (0 \ 0 \ 0 \ 0 \ 0 \ 0) = \\ 0+0+0+0+0+0 = 0 = t \end{array}$$

$u = (0, 0, 0, 0, 0, 0)$

2) $s=1 \quad t=1$

$$\left. \begin{array}{l} a_0 \cdot u = s \\ a_0 \cdot u = 1 \\ (1 \ 1 \ 0 \ 1 \ 0 \ 1) \cdot (0 \ 0 \ 0 \ 0 \ 0 \ 1) = \\ 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1 \end{array} \right\} \begin{array}{l} b_0 \cdot u = t \\ b_0 \cdot u = 1 \\ (1 \ 1 \ 0 \ 0 \ 0 \ 1) \cdot (0 \ 0 \ 0 \ 0 \ 0 \ 1) = \\ 0 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1 \end{array}$$

$u = (0 \ 0 \ 0 \ 0 \ 0 \ 1)$

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

$$a \oplus v = 5$$

$$a \oplus v = 1$$

$$b \oplus v = 4$$

$$b \oplus v = 0$$

$$(110101) \cdot (000100) = (110001) \cdot (000100) =$$

$$1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 0 = 1$$

$$1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 0 = 0$$

$$v = (000100)$$