Word Packing

Word Packing

- Example: Input is 6 x 6 Toeplitz matrix, key is 6 x 1

- $Key = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$ and $input = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

- And let’s assume our words are of length 4
- In this case we get after packing:
- $Key = \begin{bmatrix} 1\,0\,1\,0\,1\,0 \\ 1\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,1 \\ 1\,0\,0\,1\,1\,0 \\ 1\,1\,0\,0\,1\,1 \\ *\,*\,*\,*\,*\,* \\ *\,*\,*\,*\,*\,* \end{bmatrix}$, where $K_{1,1} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, K_{1,2} = \begin{bmatrix} 1 \\ 1 \\ * \\ * \end{bmatrix}$, etc.

- We also get:
- $x_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, x_2 = \begin{bmatrix} 0 \\ 1 \\ * \\ * \end{bmatrix}$

We want to calculate: $Z = \begin{bmatrix} Z_1 \\ Z_2 \end{bmatrix} = K * X$

Therefore, we only need to use the columns K_i which have $X_i == 1$

- $Z_1 = (X_1 \,\&\, 1) * K_{4,1} \oplus \left((X_1 \gg 1)\&\, 1\right) * K_{3,1} \oplus \left((X_1 \gg 2)\&\, 1\right) * K_{2,1} \oplus \left((X_1 \gg 3)\&\, 1\right) * K_{1,1} \oplus \left((X_2 \gg 2)\&\, 1\right) * K_{6,1} \oplus \left((X_2 \gg 3) \,\&\, 1\right) \; * K_{5,1}$
- The calculation of Z_2 is similar, but $K_{1,1}, K_{2,1}, \dots K_{6,1}$ are replaced by $K_{1,2}, K_{2,2}, \dots K_{6,2}$

- Please note that: $\& = bitwise\ AND, \quad * = integer\ multiplication,$
- $\oplus = exlucisve\ or$ = (^) in C
- These are the C symbols for these

An alternative method

- An alternative implementation which does not require multiplication
  - the equation on the left can be replaced with the one on the right:

$$(X \,\&\, 1) * y = \big(-(\, x \,\&\, 1)\big) \,\&\, y$$

- Since

$$(x \,\&\, 1) = LSB\ of\ x \text{ and } \big(-(x \,\&\, 1\,)\big) = 0xFFFF$$

Multiplication mod 3

Multiplication

- Example: Input is 6 x 6 randomized matrix, output is 6 x 1
- $Randomized\ Matrix = \begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 0 & 2 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$ and $output = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

Multiplication

- Example: Input is 6 x 6 randomized matrix, output is 6 x 1

- $Randomized\ Matrix = \begin{bmatrix} 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0 \\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \end{bmatrix}$ and $output = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

- Add all the items that are multiplied by 1

Multiplication mod 3

- $m_1 = msb\ 1, l_1 = lsb\ 1$
- $m_2 = msb\ 2, l_2 = lsb\ 2$
- $m_1 l_1, m_2 l_2 = 2\ bit\ numbers\ mod\ 3, can\ only\ be: 0\ 0,\ \ 0\ 1,\ \ or\ 1\ 0$

- Now we need to add them mod 3

- In our example:
- $m_1 l_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix},\ m_3 l_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix},\ \ sum = \begin{vmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{vmatrix}$

Addition mod 3

- $\begin{matrix} m_1 & l_1 \\ m_2 & l_2 \end{matrix}.$
- $m_1 l_1 \ and \ m_2 l_2 \ can \ be$: 0 0, 0 1, or 1,0

- Bitwise addition mod 3:
- $L(m_1 l_1 + m_2 l_2) = (((\sim m_1)(\sim m_2))(l_1 \oplus l_2)) \mid (m_1 m_2 (\sim l_1)(\sim l_2))$
- $M(m_1 l_1 + m_2 l_2) = ((m_1 \oplus m_2)(\sim l_1 \mid \sim l_2)) \mid (\sim m_1 \sim m_2 \ l_1 \ l_2) \}$