Word Packing

Prof. Tzipora Halevi

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 $input = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$

- And let's assume our words are of length 4
- In this case we get after packing:

$$Key = \begin{bmatrix} 1\ 0\ 1\ 0\ 1\ 0 \\ 1\ 1\ 0\ 1\ 0\ 1 \\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1 \\ 1\ 0\ 0\ 1\ 1\ 0 \\ 1\ 1\ 0\ 0\ 1\ 1 \\ *\ *\ *\ *\ *\ * \\ *\ *\ *\ *\ *\ * \end{bmatrix}, \quad \text{where } K_{1,1} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, K_{1,2} = \begin{bmatrix} 1 \\ 1 \\ * \\ * \end{bmatrix}, \text{ etc.}$$

- We also get:

- $x_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \; x_2 = \begin{bmatrix} 0 \\ 1 \\ * \\ * \end{bmatrix}$

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 $X_i == 1$

- $Z_1 = (X_1 \mathbin{\&} 1) * K_{1,1} + \big((X_1 \gg 1) \mathbin{\&} 1\big) * K_{2,1} + \big((X_1 \gg 2) \mathbin{\&} 1\big) * K_{3,1} + \big((X_1 \gg 3) \mathbin{\&} 1\big) * K_{4,1} + (X_2 \mathbin{\&} 1) * K_{5,1} + \big((X_2 \gg 1) \mathbin{\&} 1\big) * K_{6,1}$

- The calculation of Z_2 is similar, but $K_{1,1}, K_{2,1}, \ldots K_{6,1}$ are replaced by $K_{1,2}, K_{2,2}, \ldots K_{6,2}$

- Please note that: $\mathbin{\&} = bitwise\ AND, \quad * = integer\ multiplication,$

- 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

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