Mode Name: 2D-Encryption Mode (2DEM)

Principal submitter: Ahmed A. Belal

Telephone: (203) 543-9939

Organization: Department of Computer Science and Automatic Control, Faculty of Engineering, Alexandria University, Egypt.

Postal address: 35, Syria St., Roushdy, Alexandria, Egypt.

E-mail address: belala@usa.net

Auxiliary submitter: Moez A. Abdel-Gawad

Telephone: (203) 543-2482

Organization: Informatics Research Institute, Mubarak City for Scientific Research and Technological Applications, Egypt.

Postal address: 144, ElGiesh Road, Cleopatra, Alexandria, Egypt.

E-mail address: moezaabdelgawad@hotmail.com

Mode's Inventors/Developers: Ahmed A. Belal, Moez A. Abdel-Gawad

Mode's Owner: Ahmed A. Belal, Moez A. Abdel-Gawad

Here are estimates of the time and memory requirements of the 2D-Encryption Mode

Time Requirements

For a message of length $\mathtt{M}$ bits, and using an underlying block cipher of size n, the time required (using one processor) for the 2D-Encryption Mode to encrypt the message is:

$$t = 2 \cdot \frac{\mathtt{M}}{n} \cdot c + \tau \cdot \frac{\mathtt{M}}{n \cdot NSB} - \varepsilon \cdot (2 \cdot \frac{\mathtt{M}}{n} - 1)$$

where

c = the time required to do one encryption/decryption using the underlying block cipher,

τ = the time required to do the transpose operation

($\mathtt{M}/(n \cdot \mathrm{NSB})$ is the total # of 2D blocks in the message, and NSB = $n/8$ is chosen to let software implementations of the transposition be done in "no time", using appropriate coding for memory accesses; and hardware implementations do transpositions in very small time irrespective of the size of the input and the output), and

ε = the time required to calculate the encryption/decryption subkeys. These need not be calculated more than once for the whole message, so they are subtracted from the time t.

Typically, we have $c >> \tau$ and $c >> \varepsilon$, so $t \cong 2 \cdot \frac{\mathtt{M}}{n} \cdot c$

Memory Requirements

For a message of length $\mathtt{M}$ bits, and using an underlying block cipher of size n, the memory required (using one processor) for the 2D-Encryption Mode to encrypt the message is:

$$m = 2 \cdot \mathtt{M} + \mathtt{C} + w$$

where

C = the memory required for tables and subkeys of the underlying block cipher,

w = the memory required for BPR. This is usually the size of a processor word.

(BPR has a maximum value of $\mathtt{M}/(n^2/8)$)

$\mathtt{M}$ is multiplied by 2, as $\mathtt{M}$ bits are required to store the plaintext (as a maximum) and $\mathtt{M}$ bits are required (as a maximum) to hold the intermediate result (of the row-encryption phase), which is then replaced by the ciphertext (the result of the column-encryption phase).

$\mathtt{M}$ bits are the *maximum* required because 2D blocks could be encrypted independently, and so the actually required bits are the $n^2/8$ bits of the currently encrypted block.