

Jim,

I just wanted to make you aware that IBM will be submitting a minor "tweak" for our key expansion routine for MARS. The submission will be made either later tonight or tomorrow (5/15). The submission will contain the reason for the change, along with the justification. Essentially, we're retaining our key expansion routine, however instead of generating all 40 sub-keys at one time, we'll generate 10 sub-keys at a time. This will allow us to run more efficiently in limited-memory environments. Shai Halevi will be making the submission.

Nev Zunic

Internet: zunic@us.ibm.com

IBM Crypto Solutions

(914) 435-6949 (T/L 295)