A4. Cover sheet.

1. **NUSH MAC**

2. Message Authentication Codes. Proposed security level:

a) *High.* Security level equals to min(2**L, Q), where L is the MAC length (bits) and Q is the security level of NUSH Block, i.e. equals to 10**61 elementary operations with memory requirements for about 10**16 MACs or blocks of ciphertext. An elementary operation is equivalent to MAC computation, writing to (reading from) memory and comparison of MACs or an elementary operation in NUSH Block.

b) *Normal.* Security level equals to min(2**L, Q) , where L is the MAC length (bits) and Q is the security level of NUSH Block, i.e. equals to 10**22 elementary operations with memory requirements for about 10**16 MACs or blocks of ciphertext. An elementary operation is equivalent to MAC computation, writing to (reading from) memory and comparison of plaintext blocks.

Proposed environment: An eavesdropper knows all the details of the algorithm, can get and write down in memory at most as many as 10**16 different MACs or different pairs of plaintext-ciphertext blocks. He can also search through the memory in an efficient way such as a dichotomic search, lexicographic search etc.

3. Principal submitter: **LAN Crypto, Int.,**
Tel.: (7095) 288.5056, Fax: (7095) 288.5388,
22 Schepkina Str., Office 22, Moscow, RUSSIA, 129090,
e-mail: lanc@aha.ru; lancrypto@mtu-net.ru
www.lancrypto.com

4. Auxiliary submitters: NO

5. Algorithm inventors: Dr. Anatoly N. Lebedev, President, LAN Crypto, Int.,
Alexey A. Volchkov, President, «RusCrypto» Association.

6. Owner: **LAN Crypto, Int.**

7. _____ / Anatoly N. Lebedev, President, LAN Crypto, Int.

8. Point of contact: Anatoly Lebedev,
Tel.: (7095) 766.8026, 288.5056, 288.5388, fax: (7095) 288.5388, e-mail: lan@lancrypto.com, lanc@aha.ru