A2. Cover sheet.

1. **NUSH Stream**

2. Synchronous stream cipher. Proposed security level:

a) *High.* Complexity of a key reconstruction equals to 10**61 elementary operations with memory requirements for about 10**18 output keysteram bits. An elementary operation is equivalent to generation, writing to (reading from) memory and comparison of two output keystream blocks as long as necessary for key reconstruction..

b) *Normal.* Complexity of a key reconstruction equals to 10**22 elementary operations with memory requirements for about 10**18 output keystream bits. An elementary operation is equivalent to generation, writing to (reading from) memory and comparison of two output keystream blocks as long as necessary to reconstruct a key.

Proposed environment: An eavesdropper knows all the details of the algorithm, can get and write down in memory at most as many as 10**18 output keystream bits generated by the same key. 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