A5. Cover sheet.

1. **NUSH Hash**

2. Collision-Resistant Hash functions. Proposed security level:

a) *High.* Security level equals to 2**(L/2) elementary operations, where L is the hash value length (bits), i.e. at least 2**256. An elementary operation is equivalent to hash computation, writing to (reading from) memory and comparison of hash values. Regular birthday attack.

b) *Normal.* Security level equals to 2**(L/2), where L is hash value length (bits), i.e. at least 2**128. An elementary operation is equivalent to hash value computation, writing to (reading from) memory and comparison of hash values.

Proposed environment: An eavesdropper knows all the details of the algorithm, can get and write down in memory as many as 2**(L/2) different hash values. 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