

Sun setting on stream ciphers?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-02/2066.html>

From: Mok-Kong Shen (mok-kong.shen_at_t-online.de)

Date: 02/27/04

Date: Fri, 27 Feb 2004 18:54:26 +0100

In <http://www.eweek.com/article2/0.4149.1538027.00.asp> with the title 'RSA Panel: Cryptography Can't Foil Human Weakness' there is the following:

In perhaps the only actual discussion of cryptography, the Weizmann Institute's Shamir said the sun was setting on stream ciphers used to encode real-time data streams. Instead, the power of today's microprocessors could be used to encode data in blocks via block ciphers, which are more powerful but require a large amount of information to be buffered and then encoded.

Are stream ciphers really to go away in practice? What are the opinions of the group? Aren't there ongoing projects of stream cipher designs? (I suppose the issue might depend on the 'definition' of stream cipher and block cipher. Note that combinations of both types of techniques are possible and in fact could be advantageous in my humble view.)

M. K. Shen

<http://home.t-online.de/home/mok-kong.shen>