

Re: Sun setting on stream ciphers?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-02/2110.html>

From: Lassi Hippeläinen (lassi.hippelainen_at_welho.compromised.invalid)

Date: 02/28/04

Date: Sat, 28 Feb 2004 16:15:23 +0200

Mok-Kong Shen wrote:

- >
- > *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.*

I disagree about two of those arguments.

First, whenever processors have gotten faster, the applications have consumed that speed ("Moore giveth, Gates taketh away"). If there aren't enough cycles to do block ciphering now, there won't be in near future either. And there are still those low power low bandwidth applications that have to play by the old rules anyway. So, IMHO there is a market for stream ciphers also in future.

Secondly, the block size isn't an issue. From the Quality of Service point of view, the most difficult application is Voice over IP. VoIP uses 20 octet packets, and needs low-jitter low-latency QoS. But 20 octets is still more than an AES block!

Stream ciphers are more efficient in terms of bandwidth, because they don't need padding bits. Anybody interested in developing a 160 bit block cipher for VoIP?

— Lassi

- > *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.*

Re: Sun setting on stream ciphers?

sci.crypt: Re: Sun setting on stream ciphers?

- > *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>