Information Society Technologies

ECRYPT

Network of Excellence in Cryptology

DOES THE WORLD NEED NEW STREAM CIPHERS?

STEVE BABBAGE, VODAFONE

12TH AUGUST 2004

The world has standard block ciphers in AES and 3DES. But there is not even a de facto standard stream cipher: there is no dedicated[1] stream cipher that is suitable for most applications and has stood the test of time.

One of the headline activities of the ECRYPT consortium is to coordinate research effort to meet the world's requirements for really strong, really useful, de facto standard stream ciphers. But does the world need dedicated stream ciphers? Are there requirements, either today or plausibly in the future, for a stream cipher that cannot be met just by running AES in a suitable mode of operation?

Please help us to identify what the world's requirements for stream ciphers really are. Help us to meet future needs as you see them.

FUNCTIONAL CHARACTERISTICS OF A STREAM CIPHER

The functional characteristics of a stream cipher that we have identified are:

Parameter sizes	**Special functionality**
Secret key size	Transform plaintext to ciphertext by bitwise XOR? Or a more complex transformation on larger plaintext/ciphertext blocks?
IV size	Direct keystream access? (Generate the millionth keystream block efficiently without cycling through a million generator states)
Maximum output length	Other functionality combined with the stream cipher, e.g. an integrity mechanism?

Speed …	**… and size …**	**… on different platforms**
Initialisation time Re-initialisation time (same secret key, new IV) Throughput	Implementation size Power consumption	32-bit or 64-bit processor 8-bit processor Purpose built ASIC

[1] By a "dedicated stream cipher", we mean one that has been designed specifically as a stream cipher, rather than say a block cipher running in counter or output feedback mode.

QUESTIONS FOR YOU

Can you envisage a *plausible, real world* requirement for a stream cipher that cannot be met by using AES in a standard mode (e.g. Counter, OFB), because at least one of the following is true:

- on some desired platform, an AES mode cannot provide the required speed (of initialisation, re-initialisation or encryption) in a sufficiently small (size, power) implementation;
- the required parameter sizes are too big: it needs a bigger secret key than AES can support, or a bigger IV than standard AES modes can support, or it needs to generate more output than can be done securely with an AES mode.

If so, please indicate what sort of application you envisage, and why you believe an AES mode cannot meet it. (We are just asking for enough detail to motivate the stream cipher requirement — nothing more.)

Ideally, please also indicate whether the application you envisage would benefit from any of the "special functionality" shown under that heading in the table above.

Please send all feedback to the author:

Steve Babbage, Vodafone Group R&D
Vodafone House, The Connection, Newbury, Berkshire RG14 2FN, UK
Tel: +44 (0)1635 676209
Fax: +44 (0)1635 231776
Email: steve.babbage@vodafone.com

By default, we will assume that you are willing to have your feedback attributed to you, and we will give you credit when we refer to it. If you prefer it to be treated anonymously, please let us know and we will of course respect your wishes.

Please note that, if your feedback is to be taken into account when preparing input for the SASC conference (see below), it must be provided by the end of August 2004.

WHAT HAPPENS NEXT?

Your feedback will be used:

- by the ECRYPT consortium members (http://www.ecrypt.eu.org/) in planning future research activities (which may include calls for submissions from researchers outside the consortium);
- in particular, to prepare an input for the State of the Art in Stream Ciphers (SASC) conference in October 2004 (http://www.isg.rhul.ac.uk/research/projects/ecrypt/stvl/sasc.html).