The Status of Stream Ciphers after the eSTREAM Project*

Bart Preneel

COSIC, K.U.Leuven, Belgium

ABSTRACT [1]

The eSTREAM project is a multi-year project within the ECRYPT Network of Excellence (http://www.ecrypt.eu.org/stream/). Launched in 2004, it is expected to come to a conclusion in April of 2008 with the publication of a portfolio of promising new stream cipher designs.

For many years stream ciphers of a dedicated design were seen as an important complement to block ciphers. While both stream and block ciphers provide what is termed *symmetric encryption*, where both the sender and the receiver of a protected message share the same key, they have different characteristics making them suitable for different applications. And while a block cipher could be used as a stream cipher, this was previously viewed as a second-best choice.

However the widespread adoption of the AES [1] —a trusted block cipher with excellent performance characteristics—has changed this. For the vast majority of applications one can just use the AES (in an appropriate way) with no need to look for alternatives. That said, there are two situations where a dedicated stream cipher might still hold an advantage: (1) in software applications requiring a very high encryption/decryption rate and (2) in hardware applications where physical resources, *e.g.* space or power, are severely restricted.

Over a three-year period, an initial set of 34 new stream cipher designs—submitted from around the world—has been gradually reduced to 16 finalist ciphers suitable for software or hardware implementation. All these finalists are superior to the AES in at least one significant way, and current indications are that the final portfolio will highlight some truly impressive algorithmic advances.

More than a dozen ECRYPT partners have actively contributed by sending in submissions and by performing security and performance evaluations in both software and hardware. The eSTREAM process has been advanced by four international workshops (each with more than hundred participants), hundreds of scientific research papers, and tens of thousands of on-line participants to the forum.

* Joint work with M.J.B. Robshaw, Orange Labs, Issy-les-Moulineaux, France

[1] This work has been supported by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

In this talk we will review the whole eSTREAM process, the parts that worked and those that didn't, and summarise the cryptographic lessons learnt along the way. We will explain how stream cipher design and analysis has been significantly advanced by eSTREAM during the past four years. Even better, it is gratifying to see the project extend its influence beyond stream ciphers as it impacts other aspects of cryptographic research in unexpected ways.

References

1. National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard, November 2001. Available via http://csrc.nist.gov/.