www.ecrypt.eu.org

The eSTREAM Portfolio

Bart Preneel
COSIC, K.U.Leuven

eSTREAM

- A project within ECRYPT to promote research into the design and analysis of dedicated stream ciphers

- eSTREAM began in 2004 with a call for proposals
  - 34 submissions were received from around the world
  - Three phases of analysis and performance evaluation

- Candidates were intended to satisfy one of two profiles
  - High encryption rate in software
  - Implementation advantages in restricted hardware

eSTREAM Goal

- The goal of eSTREAM was a portfolio of promising new stream cipher designs
  - These will continue to receive cryptanalytic attention
  - When sufficiently mature, we anticipate proposals to be deployed and/or adopted in standards

eSTREAM Committee

Steve Babbage (Vodafone)

Anne Canteaut (INRIA)

Carlos Cid (Royal Holloway)

Christophe De Cannière (K.U.Leuven + ENS)

Henri Gilbert (Orange Labs)

Thomas Johansson (Univ. Lund)

Matthew Parker (Univ. Bergen)

Bart Preneel (K.U.Leuven)

Vincent Rijmen (K.U.Leuven + T.U. Graz)

Matt Robshaw (Orange Labs)

The eSTREAM Portfolio

- We prefer to avoid a direct comparison to the AES process or to SHA-3
  - We do not have the resources of NIST
  - Our goals are different: we are promoting research whereas NIST defines standards for the coming decades
- Consequently we have arrived at a broad portfolio

The eSTREAM Portfolio

Software	Hardware
HC-128	F-FCSR-H
Rabbit	Grain v1
Salsa20/12	MICKEY v2
Sosemanuk	Trivium

(In alphabetical order)

After the Portfolio

- A report will be available at

  www.estream.eu.org/stream

- We will continue to maintain the eSTREAM pages
  - Please continue to submit new results and analysis
  - The portfolio will be updated as required

- Finally: many thanks to **all** submitters, analysts, and implementers for their contributions to eSTREAM