ECRYPT

eSTREAM

Algorithms for the Next Round

http://www.ecrypt.eu.org/stream/

27 March 2007

Matt Robshaw
Bart Preneel

eSTREAM

- A multi-year project within ECRYPT to promote research into stream ciphers (2004-2008)
- The goal of eSTREAM is to arrive at a portfolio of promising stream ciphers
- We are particularly interested in two profiles
  - Good throughput in software
  - Compact and efficient implementation in hardware

eSTREAM Criteria

Security
Performance compared to the AES
Performance compared to other submissions
Justification and supporting analysis
Simplicity and flexibility
Completeness and clarity of design

ECRYPT

eSTREAM Panel

Steve Babbage	(VOD)	**Christophe de Cannière**	(INRIA)	**Anne Canteaut**	(INRIA)
Carlos Cid	(RHUL)	**Henri Gilbert**	(FTRD)	**Thomas Johansson**	(LUND)
Matthew Parker	(UiB)	**Christof Paar**	(RUB)	**Bart Preneel**	(KUL)
Vincent Rijmen	(IAIK)	**Matt Robshaw**	(FTRD)	**Hongjun Wu**	(KUL)

Phase 3 Ciphers

SW Phase 3	HW Phase 3
CryptMT	DECIM
DRAGON	Edon-80
HC-128 (-256)	F-FCSR
LEX	Grain
NLS (encrypt only)	MICKEY (-128)
Rabbit	MOUSTIQUE
Salsa20	POMARANCH
SOSEMANUK	Trivium

All algorithms are the most recent version

eSTREAM

- Short report to be available soon at

  www.ecrypt.eu.org/stream

- Next steps
  - Ongoing analysis and implementation
  - SASC 2008 in February/March 2008
  - We expect to announce the final portfolio in April/May 2008