eSTREAM Update

FSE 2006 Rump Session

M. Robshaw

16.03.06

eSTREAM

- A multi-year project within ECRYPT NoE
  - ECRYPT has >30 academic/industry partners
- The goal of eSTREAM:
  - To try and identify a portfolio of promising stream ciphers
- Along the way:
  - To promote a greater understanding of stream cipher design and analysis

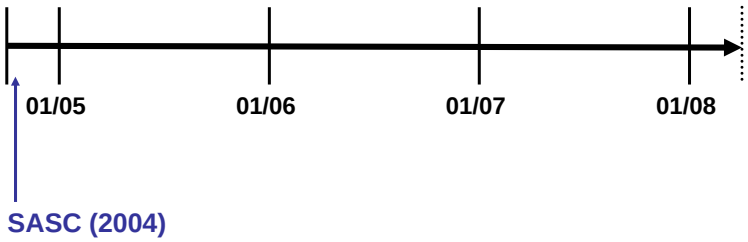
eSTREAM

- While it bears similarities to the AES-effort, there are some important differences
  - eSTREAM is not a standardisation effort
  - We offer the designers more flexibility with regards to "tweaking"
    - We don't want to miss out on good design ideas because of an easily avoided flaw

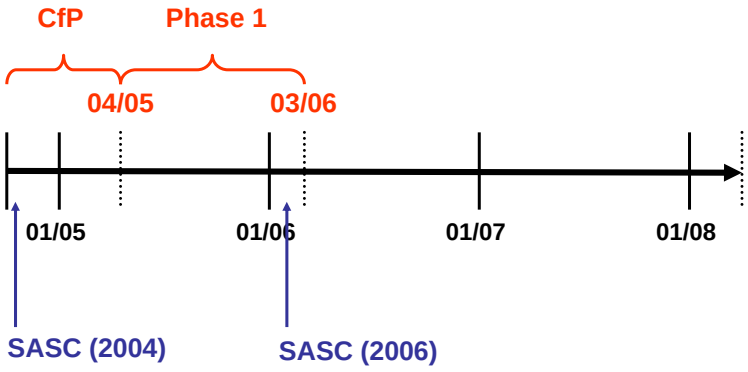
Two eSTREAM Profiles

1. Good SW throughput
2. Good HW implementation characteristics

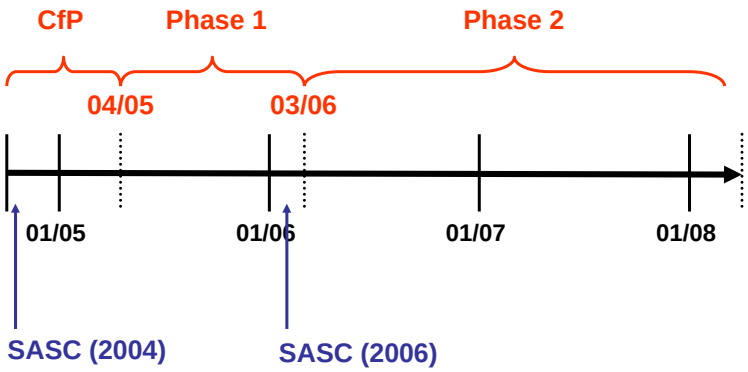
Timeline



Timeline



Timeline



eSTREAM – Phase 1

- There has been much cryptanalysis
- Considerable effort on SW and HW evaluations

Evaluation Criteria

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

eSTREAM – Phase 2

- Focus evaluation efforts on more promising candidates
- We aim to post an initial classification of the Phase 1 candidates next week

eSTREAM – Phase 2

- There will be a SW and a HW list:
  - The same cipher can appear in both lists

eSTREAM – Phase 2

- There will be a SW and a HW list:
  - The same cipher can appear in both lists
- In each list, a proposal will be classified as:

"Phase 1 candidate"	
"Phase 2 candidate"	
"Focus candidate"	

eSTREAM – Phase 2

- There will be a SW and a HW list:
  - The same cipher can appear in both lists
- In each list, a proposal will be classified as:

"Phase 1 candidate"	*Ciphers with shortcomings*
"Phase 2 candidate"	*Promising ciphers*
"Focus candidate"	*Very interesting proposals*

eSTREAM – Phase 2

- While we anticipate more opportunities for tweaking, these may be limited after a time
  - Cryptanalysis requires some stability
- We expect to revisit the classification of proposals as work continues
  - Ciphers may move between different classes

More information …

- Plan to post details on Phase 2 next week
- Reports, notes, cipher descriptions, code, and a discussion forum are all available via:

www.ecrypt.eu.org