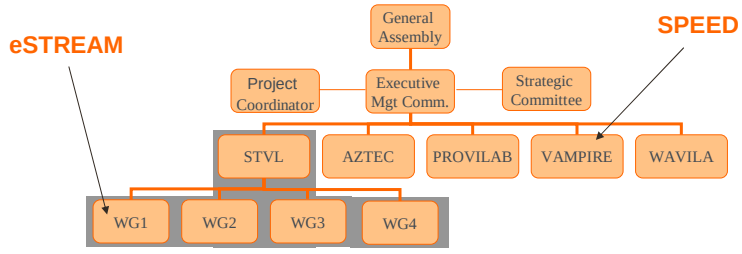
The eSTREAM Project

Matt Robshaw
Orange Labs

11.06.07

ECRYPT

- An EU Framework VI Network of Excellence
  - > 5 M€ over 4.5 years
  - More than 30 european institutions (academic and industry)
- ECRYPT activities are divided into Virtual Labs
  - Which in turn are divided into Working Groups



Cryptography (Overview!)

- Cryptographic algorithms often divided into two classes
  - Symmetric (secret-key) cryptography
    - Participants using secret-key cryptography share the same key material
  - Asymmetric (public-key) cryptography
    - Participants using public-key cryptography use different key material
- Symmetric encryption can be divided into two classes
  - Block ciphers
  - Stream ciphers

Stream Ciphers

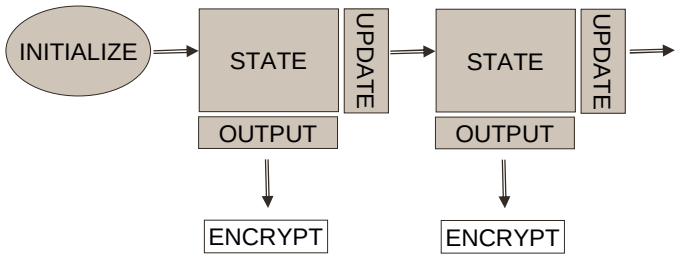
- Stream encryption relies on the generation of a "random looking" *keystream*
  - Encryption itself uses bitwise exclusive-or

```
01101001110001110011100001111010101010101   keystream
11101110111011101110111011101110111000001 00 plaintext
10000111001010011101011010010100010010100 01 ciphertext
```

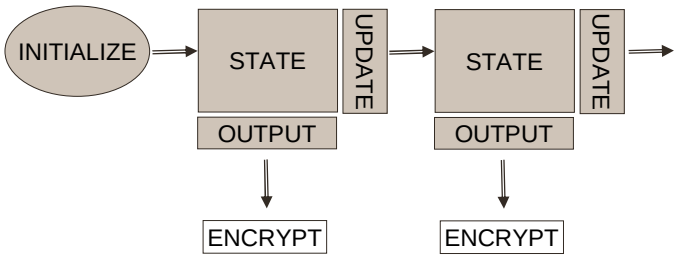
- Stream encryption offers some interesting properties
  - They offer an attractive link with perfect secrecy (Shannon)
  - No data buffering required
  - Attractive error handling and propagation (for some applications)
- How do we generate keystream ?

Stream Ciphers in a Nutshell

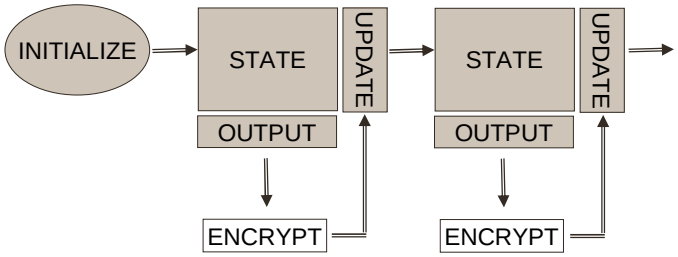
- Stream ciphers employ an evolving state
  - We sample the state to derive keystream



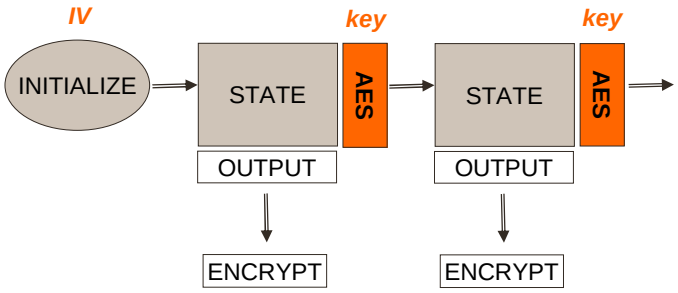
Stream Ciphers: Synchronous



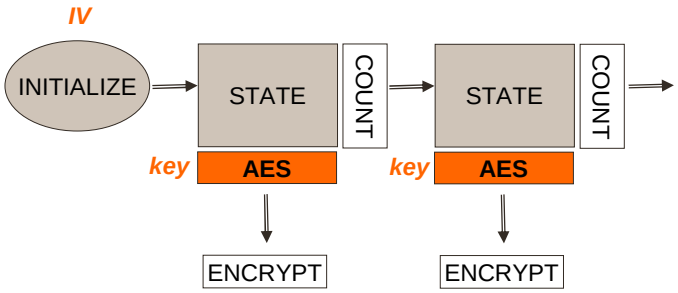
Stream Ciphers: Self-Synchronising



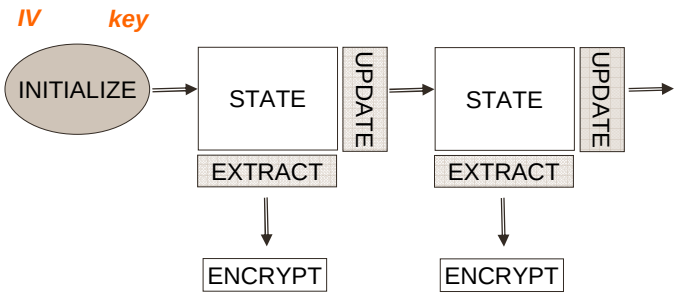
Stream Ciphers: OFB Mode



Stream Ciphers: Counter Mode



Stream Ciphers: Dedicated



Stream Ciphers (Past)

- Dedicated stream ciphers have an illustrious history
  - Dedicated stream ciphers have the reputation of being faster and more compact than block ciphers
  - Can (at times) be effectively analysed
    - LFSR-based stream ciphers have had a strong theoretical analytic framework since the 1950's
  - However, dedicated stream ciphers don't always have the best security reputation

Stream Ciphers (Present)

- Dedicated stream ciphers are widely used
  - GSM, TLS + some hiccups, *e.g.* 802.11
- The issue is not "do we need stream ciphers" but "do we need stream ciphers of dedicated design"?
- There are very few established dedicated stream ciphers
  - RC4, SNOW 2.0
  - Attempts to change this haven't been successful; *e.g.* NESSIE

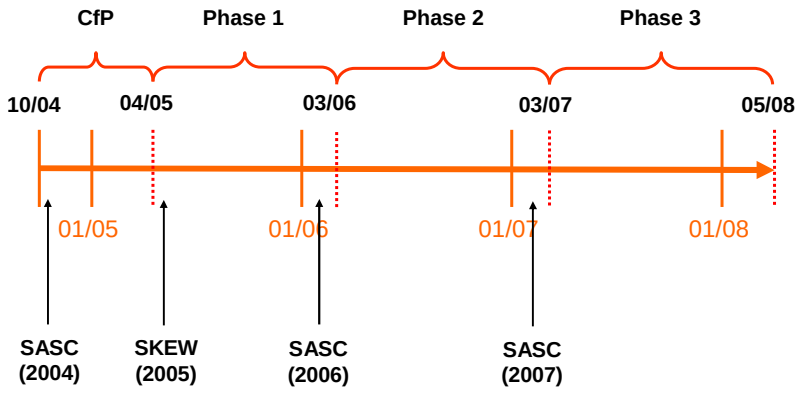
SASC 2004

- eSTREAM was launched with a workshop in October 2004 in Brugge
- A variety of stream cipher proposals and industry position papers were presented
- From this the scope of eSTREAM was established
- *Call for Proposals* was devised

What is eSTREAM?

- eSTREAM is a collaborative research effort
  - We (in ECRYPT) manage the eSTREAM process
  - We do not analyze or assess candidates
- Our focus is the research community
- eSTREAM is not a standardization body
  - However, the results of eSTREAM might be taken up by standardisation bodies or industry

eSTREAM Timeline



Submission Requirements

- Very modest submission requirements
  - Proposals had to be received by April 30, 2005
- Submissions had to be either fast in software or resource-friendly in hardware

	key	IV	tag (optional)
Profile 1	128	64 or 128	32, 64, 96, or 128
Profile 2	80	32 or 64	32 or 64

- Designers required to give an IP statement

The eSTREAM Submissions

- There were 34 submissions
  - 32 synchronous and 2 self-synchronising
  - 7 submissions offered encryption + authentication
- 74% submissions from outside ECRYPT

Europe	57%	**Asia**	16%	**N. America**	14%	**Oceania**	13%

The eSTREAM Submissions

PROFILE I	PROFILE I+II	PROFILE II
ABC	F-FCSR	Achterbahn
CryptMT	Hermes8	DECIM
DICING	LEX	Edon-80
DRAGON	MAG	Grain
FROGBIT	NLS	MICKEY (128)
HC-256	Phelix	MOSQUITO
Mir-1	Polar Bear	SFINKS
Py	POMARANCH	Trivium
Salsa20	Rabbit	TSC-3
SOSEMANUK	SSS	VEST
	TRBDK3 YAEA	WG
	Yamb	ZK-Crypt

Phase 1 Cryptanalysis

PROFILE I	PROFILE I+II	PROFILE II
ABC	F-FCSR	Achterbahn
CryptMT	Hermes8	DECIM
DICING	LEX	Edon-80
DRAGON	MAG	Grain
FROGBIT	NLS	MICKEY (128)
HC-256	Phelix	MOSQUITO
Mir-1	Polar Bear	SFINKS
Py	POMARANCH	Trivium
Salsa20	Rabbit	TSC-3
SOSEMANUK	SSS	VEST
	TRBDK3 YAEA	WG
	Yamb	ZK-Crypt

Phase 1 Lessons

- #1: The half-life of new stream ciphers is one year
- #2: Self-synchronizing stream ciphers are hard to design

For Phase 2 – Trying Something New

- Tweaking
  - The goal was to get better algorithms for the later stages
  - The AES process allowed (minor) tweaks for the finalists but we allowed all designers (even those of broken designs) to tweak
  - An administrative nightmare
- Focus ciphers
  - We were very conscious of the limited time - we hoped to guide the direction of some cryptanalytic attention
  - Trying to avoid the LHF problem (*low hanging fruit*)

- Software

Phase 1 Submissions (SW)

PROFILE I	PROFILE I+II	
ABC	F-FCSR	
CryptMT	Hermes8	
DICING	LEX	
DRAGON	MAG	
FROGBIT	NLS	
HC-256	Phelix	
Mir-1	Polar Bear	
Py	POMARANCH	
Salsa20	Rabbit	
SOSEMANUK	SSS	
	TRBDK3 YAEA	
	Yamb	

Phase 2 Submissions (SW)

Focus Phase 2	Phase 2	Archived
DRAGON	**ABC**	F-FCSR
HC-256	**CryptMT**	FROGBIT
LEX	**DICING**	Fubuki
Phelix	**NLS**	Hermes8
Py	**Polar Bear**	MAG
Salsa20	**Rabbit**	Mir-1
SOSEMANUK		POMARANCH
		SSS
		TRBDK3 YAEA
		Yamb
(7)	(6)	(10)

- Hardware

Phase 1 Submissions (HW)

	PROFILE I+II	PROFILE II
	F-FCSR	Achterbahn
	Hermes8	DECIM
	LEX	Edon-80
	MAG	Grain
	NLS	MICKEY (128)
	Phelix	MOSQUITO
	Polar Bear	SFINKS
	POMARANCH	Trivium
	Rabbit	TSC-3
	SSS	VEST
	TRBDK3 YAEA	WG
	Yamb	ZK-Crypt

Phase 2 Submissions (HW)

Phase 2 Focus	Phase 2	Archived
Grain	**Achterbahn**	MAG
MICKEY-128	**DECIM**	SFINKS
Phelix	**Edon-80**	SSS
Trivium	**F-FCSR**	TRBDK3 YAEA
	Hermes8	Yamb
	LEX	
	MICKEY	
	MOUSTIQUE	
	NLS	
	Polar Bear	
	POMARANCH	
	Rabbit	
	Salsa20	
	TSC-4	
	VEST	
	WG	
	ZK-Crypt	
(4)	**(17)**	**(5)**

Phase 2 Lessons

- Tweaking helped!
  - At the start of Phase 2, the SW profile contained 13 ciphers
    - Cryptanalysis results were announced against 3
  - At the start of Phase 2, the HW profile contained 21 ciphers
    - Cryptanalysis results were announced against 4
- "Focus" ciphers didn't make much difference
- There is rarely a consistent view on "distinguishing" attacks

Moving into Phase 3

- The decision depended on many issues including …
  - Security
  - Performance in comparison to the AES
  - Performance in comparison to other submissions
  - Simplicity
- IP didn't have any role in the decision
- For hardware, the complicated implementation trade-offs led us to make a first cut on size

- Software

Phase 3 Submissions (SW)

Phase 3	Archived Phase 2	Archived
CryptMT v3	ABC	F-FCSR
DRAGON	DICING	FROGBIT
HC-128	Phelix	Fubuki
LEX v2	Polar Bear	Hermes8
NLS v2	Py	MAG
Rabbit		Mir-1
Salsa20		POMARANCH
SOSEMANUK		SSS
		TRBDK3 YAEA
		Yamb
(8)	(5)	(10)

- Hardware

Phase 3 Submissions (HW)

Phase 3	Archived Phase 2	Archived
DECIM v2	Achterbahn	MAG
Edon-80	Hermes8	SFINKS
F-FCSR-H v2	LEX	SSS
Grain v1	NLS	TRBDK3 YAEA
MICKEY v2	Phelix	Yamb
MOUSTIQUE	Polar Bear	
POMARANCH v3	Rabbit	
Trivium	Salsa20	
	TSC-4	
	VEST	
	WG	
	ZK-Crypt	
(8)	**(12)**	**(5)**

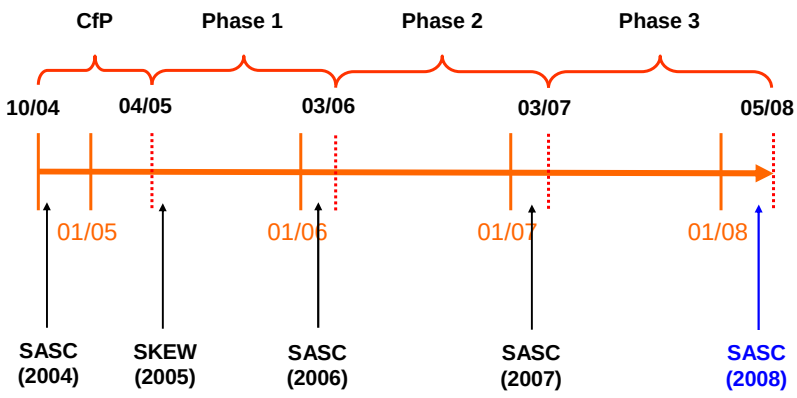
Phase 3 and the Final Stages

- As with the AES, there will probably be a concentration on peformance
  - Good for the attendees of SPEED
  - Hardware results will be the hardest to come by
- But we also really need cryptanalytic results!

The Committee

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

eSTREAM Timeline



Profile I Results (Phase 3)

- Example of some performance data
  - *e.g.* Intel Pentium M (1700MHz)

Salsa12 Salsa 8

	40 bytes	576 bytes	1500 bytes	IMIX	STREAM
HC-128	656.89	48.24	20.54	79.80	3.07
RC4	332.52	30.01	16.30	45.71	7.58
DRAGON	69.24	25.76	23.71	27.99	11.74
AES (counter)	**22.90**	**16.19**	**16.10**	**16.62**	**15.96**
Salsa20	29.01	11.91	12.22	13.20	11.71
LEX	20.07	10.73	9.90	11.07	9.41
SOSEMANUK	32.00	8.99	7.63	10.07	4.68
CryptMT v3.0	20.75	9.00	9.09	9.84	4.87
NLS v2	36.87	7.74	6.19	9.17	5.99
Rabbit	18.85	6.83	6.41	7.50	6.25
SNOW v2	23.34	5.80	5.28	6.88	4.75

Profile I Results (Phase 3)

- Example of some performance data
  - *e.g.* Intel Pentium M (1700MHz)

Salsa12 Salsa 8

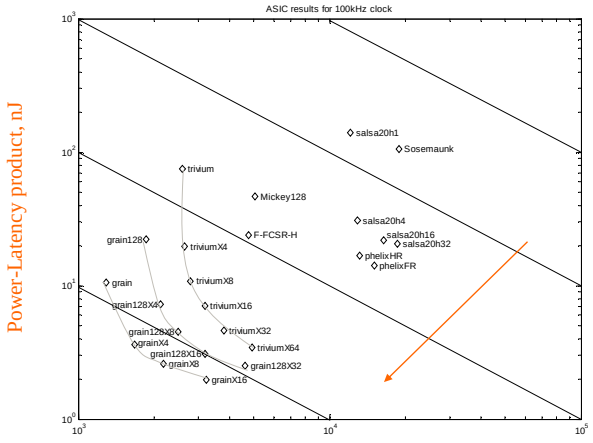
	40 bytes	576 bytes	1500 bytes	IMIX	STREAM
AES (counter)	**22.90**	**16.19**	**16.10**	**16.62**	**15.96**
DRAGON	69.24	25.76	23.71	27.99	11.74
Salsa20	29.01	11.91	12.22	13.20	11.71
LEX	20.07	10.73	9.90	11.07	9.41
RC4	332.52	30.01	16.30	45.71	7.58
Rabbit	18.85	6.83	6.41	7.50	6.25
NLS v2	36.87	7.74	6.19	9.17	5.99
CryptMT v3.0	20.75	9.00	9.09	9.84	4.87
SNOW v2	23.34	5.80	5.28	6.88	4.75
SOSEMANUK	32.00	8.99	7.63	10.07	4.68
HC-128	656.89	48.24	20.54	79.80	3.07

Profile II Results (Phase 3)

- Potential to be more compact than the AES
  - Ignores issues such as relative security levels and different speed optimisations
  - Some sample area results are given below, there may be smaller implementations while * denotes a crude estimate
  - Much more detail expected to become apparent in the final phase

SNOW 2.0	7000	**DECIM v2**	3000 *
RC4	≈12000	**Edon-80**	2900
AES	3600	**F-FCSR-H**	3200 *
		Grain v1	1300
		MICKEY v2	3400
		POMARANCH v3	3300 *
		Trivium	1500

Results of Good and Benaissa



Stream Ciphers – Alive or Dead?

- Still too early to say … but there is considerable interest!

	2005	2006	2007 (to 03/07)
Papers on-line	50 (+35)	60	37
Discussion posts	293	290	83
Web activity (page loads)	79,112	127,141	33,092
Web activity (unique visitors)	25,555	43,702	11,975
SASC Attendance	88	95	103

Conclusions

- eSTREAM has generated some new and provocative designs
- Signs are good for an interesting final portfolio !
- In terms of a research effort, real and lasting results have been gained
- Please feel free to contribute to eSTREAM!

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