Stream Cipher Design

Evaluation of the Stream Cipher Polar Bear

ERICSSON

KTH VETENSKAP OCH KONST

John Mattsson

Overview

- Introduction and background
  - eSTREAM
  - Polar Bear
- Purpose of the thesis
- Results
  - Weaknesses
  - Optimization
  - Enhancements
- End of eSTREAM's first phase
- Conclusion

Background

- There are two main types of symmetric encryption algorithms, *Block ciphers* and *Stream ciphers*.
- Stream ciphers are gaining popularity due to their efficiency, small footprint and bit-error robustness.
- Unfortunately, there is a lack of efficient and secure stream ciphers open to public use.

eSTREAM

- eSTREAM, *the ECRYPT Stream Cipher Project* is a multi-year effort to identify new stream ciphers that might become suitable for widespread adoption.
- Two Profiles
  - Profile I - Stream ciphers for software applications with high throughput requirements.
  - Profile II - Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption.

eSTREAM Timetable

November 2004	Call for Primitives
April 2005	The beginning of the first evaluation phase of eSTREAM. (34 candidates)
March 2006	The end of the first evaluation phase of eSTREAM. (25 candidates left)
⋮	⋮
July 2006	The beginning of the second evaluation phase of eSTREAM.
December 2006	Second classification
September 2007	The end of the second evaluation phase of eSTREAM.
January 2008	The final report of the eSTREAM.

Polar Bear

- Polar Bear is one of the 34 eSTREAM candidates. It borrows components from the ciphers RC4 and AES.
- It was created by Johan Håstad and Mats Näslund and claimed to be suitable for both profile I (software) and profile II (hardware)

Purpose

- The project aims at evaluating the security of the stream cipher Polar Bear, and look deeper at high speed implementations. The four main goals of the thesis are:
- Evaluation of Polar Bear security
- Evaluation with respect to statistical tests
- Optimized implementation
- Enhancements and tweaks.

Results

- Found that an erroneous ‘permutation’ resulted in that Polar Bear outputs the unencrypted message after a few million bytes.

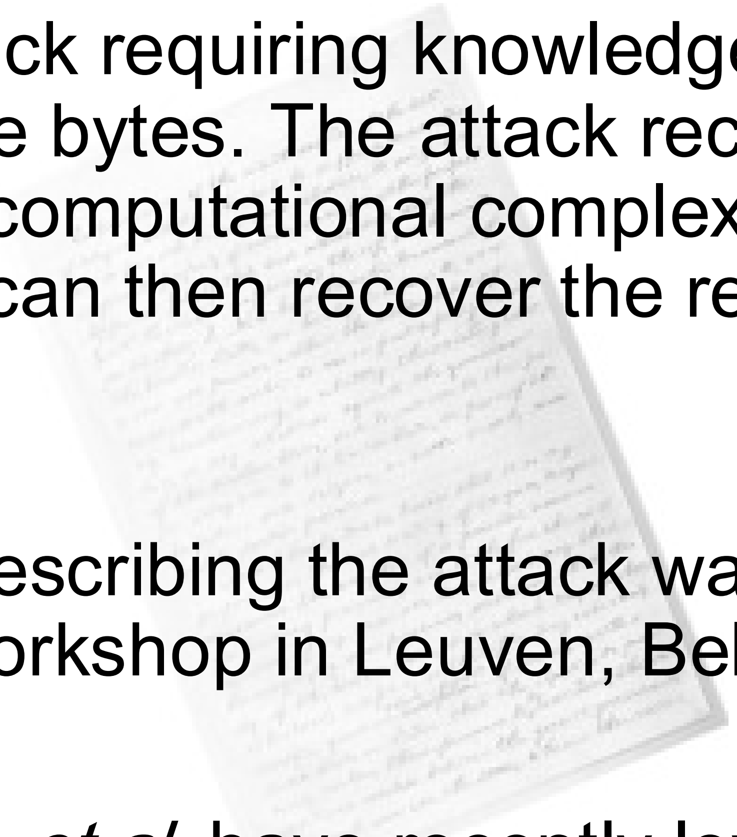
  As the Polar Bear documentation clearly states that is should be a permutation, this could be seen as a typo.

Results

- Found a attack requiring knowledge of the 24 first message bytes. The attack recovers the state with a computational complexity of O($2^{78.8}$). An attacker can then recover the rest of the message.

  The paper describing the attack was accepted to the SASC workshop in Leuven, Belgium.

  Hasanzadeh *et al* have recently lowered the time complexity to O($2^{57.4}$).



Results

- We have not found any other weaknesses in Polar Bear. Polar Bear seems resistant to all other known attacks.
- Polar Bear passes all the statistical tests in the NIST statistical test suite. It also passes new statistical tests that are tailored for stream ciphers and focuses on correlation.

Results

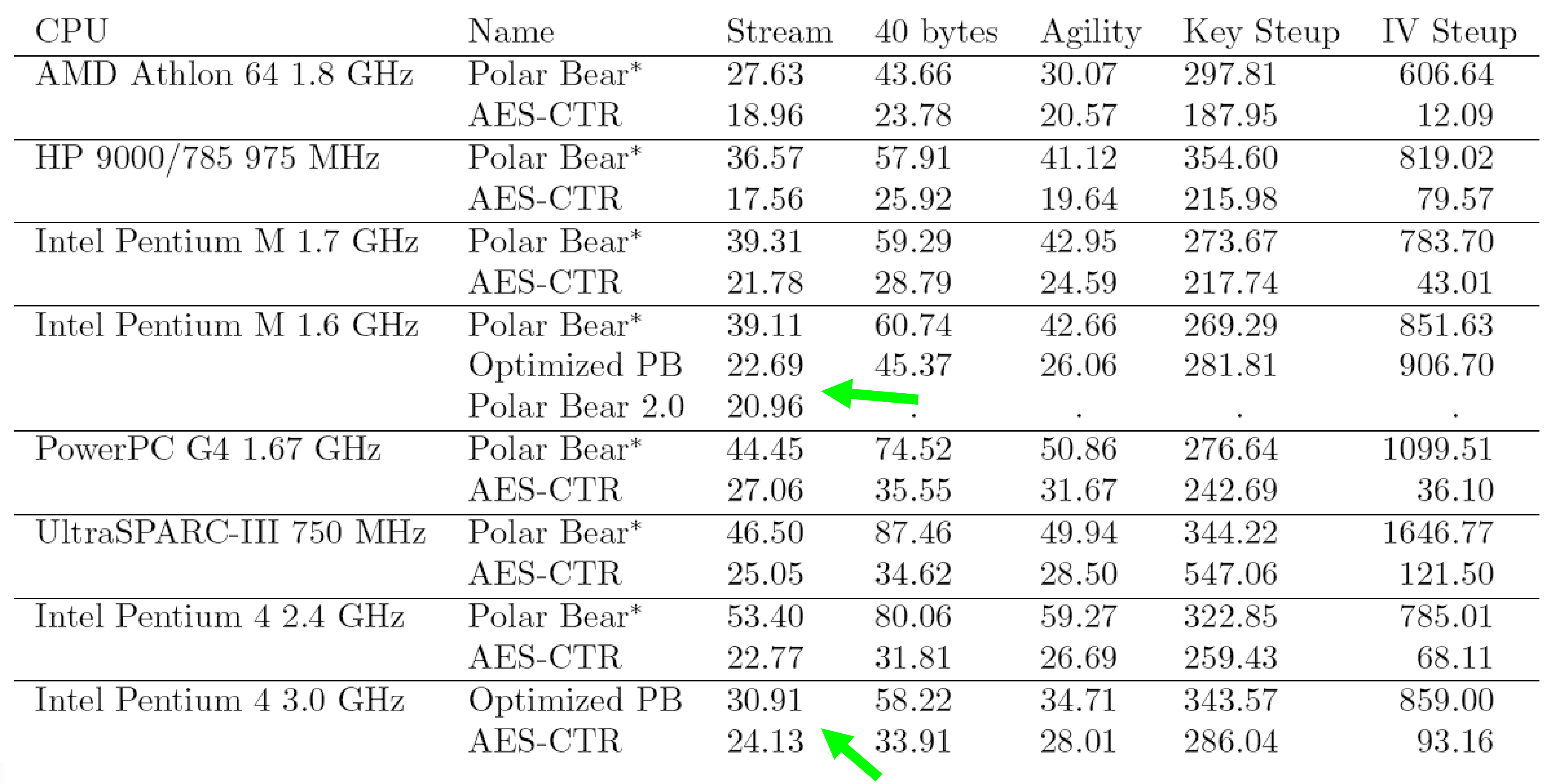
- We believe that Polar Bear can be made secure by adding a key-dependent pre-mixing of the D8 table in conjunction with the key schedule.

- Further tweaks strengthen the security and improves the performance on long streams.

These suggestions are part of a tweak that will be submitted to eSTREAM.

Polar Bear Software Performance

- Optimized the C implementation of Polar Bear.



CPU	Name	Stream	40 bytes	Agility	Key Steup	IV Steup
AMD Athlon 64 1.8 GHz	Polar Bear*	27.63	43.66	30.07	297.81	606.64
	AES-CTR	18.96	23.78	20.57	187.95	12.09
HP 9000/785 975 MHz	Polar Bear*	36.57	57.91	41.12	354.60	819.02
	AES-CTR	17.56	25.92	19.64	215.98	79.57
Intel Pentium M 1.7 GHz	Polar Bear*	39.31	59.29	42.95	273.67	783.70
	AES-CTR	21.78	28.79	24.59	217.74	43.01
Intel Pentium M 1.6 GHz	Polar Bear*	39.11	60.74	42.66	269.29	851.63
	Optimized PB	22.69	45.37	26.06	281.81	906.70
	Polar Bear 2.0	20.96	.	.	.	.
PowerPC G4 1.67 GHz	Polar Bear*	44.45	74.52	50.86	276.64	1099.51
	AES-CTR	27.06	35.55	31.67	242.69	36.10
UltraSPARC-III 750 MHz	Polar Bear*	46.50	87.46	49.94	344.22	1646.77
	AES-CTR	25.05	34.62	28.50	547.06	121.50
Intel Pentium 4 2.4 GHz	Polar Bear*	53.40	80.06	59.27	322.85	785.01
	AES-CTR	22.77	31.81	26.69	259.43	68.11
Intel Pentium 4 3.0 GHz	Optimized PB	30.91	58.22	34.71	343.57	859.00
	AES-CTR	24.13	33.91	28.01	286.04	93.16

eSTREAM – End of Phase 1

- Initial classification of algorithms into three categories.
  - Focus Phase 2 – Of particular interest.
  - Phase 2 – Are moved to the second phase.
  - Archived - No longer considered for the final portfolio.
- Main criteria are cryptanalysis and performance.
- No patented ciphers in the focus category.
- The deadline for final tweaks is June 30, 2006.
- A second classification towards the end of 2006.

Profile 1 – Software

Performance measured in cycles/byte on a Pentium 4

Focus Phase 2	v1	v2
DRAGON	12,27	
HC-256	4,96	
LEX	9,90	🟩
Phelix	5,56	
Py	3,74	
Salsa20	13,85	
SOSEMANUK	5,72	

Phase 2	v1	v2
ABC	3,43	4,15
CryptMT (pat.)	16,06	🟩
DICING	14,68	🟩
NLS	5,75	🟩
Polar Bear	30,90	
Rabbit (pat.)	7,71	
Yamb	16,50	

Archived	v1	v2	v3
F-FCSR	57,00	🟩	
Fubuki (pat.)	136,00	🟩	
Frogbit (pat.)	924,00		
Hermes8	170,00	🟩	
MAG	30,79	🟩	10,53
Mir-1	18,13		
POMARANCH	2040,00	🟩	
SSS	🟥		
TRBDK3 YAEA	🟩		

Reference	
AES-128-CTR	24,13
AES-256-CTR	33,09
RC4	11,00
SNOW 2.0	5,20

Profile 2 - Hardware

Focus Phase 2	v1	v2
Grain	🟥	🟩
MICKEY-128	🟩	
Phelix	🟩	
Trivium	🟩	

Phase 2	v1	v2
Achterbahn	🟥	🟩
DECIM	🟥	🟩
Edon80	🟩	
F-FCSR	🟥	🟩
Hermes8	🟥	🟩
LEX	🟥	🟩
MICKEY	🟩	
MOSQUITO	🟥	
NLS	🟥	🟩
Polar Bear	🟥	
POMARANCH	🟥	🟩
Rabbit (pat.)	🟩	
Salsa20	🟩	
SFINKS	🟥	
TSC-3	🟥	
VEST (pat.)	🟩	
WG	🟥	🟩
Yamb	🟥	
ZK-Crypt	🟥	🟩

Archived	v1	v2	v3
MAG	🟥	🟩	🟩
SSS	🟥		
TRBDK3 YAEA	🟩		

Summary

- Polar Bear was moved to the second phase.
- We believe that the tweak makes Polar Bear secure.
- The tweak makes Polar Bear faster on long stream.
- Polar Bear would need to get faster to have the required “significant performance advantage over the AES”.