An Introduction to new Stream Cipher Designs

Ways of Turning Your Data into Line Noise

T. E. Bjørstad

The Selmer Center,
Department of Informatics
University of Bergen,
Norway

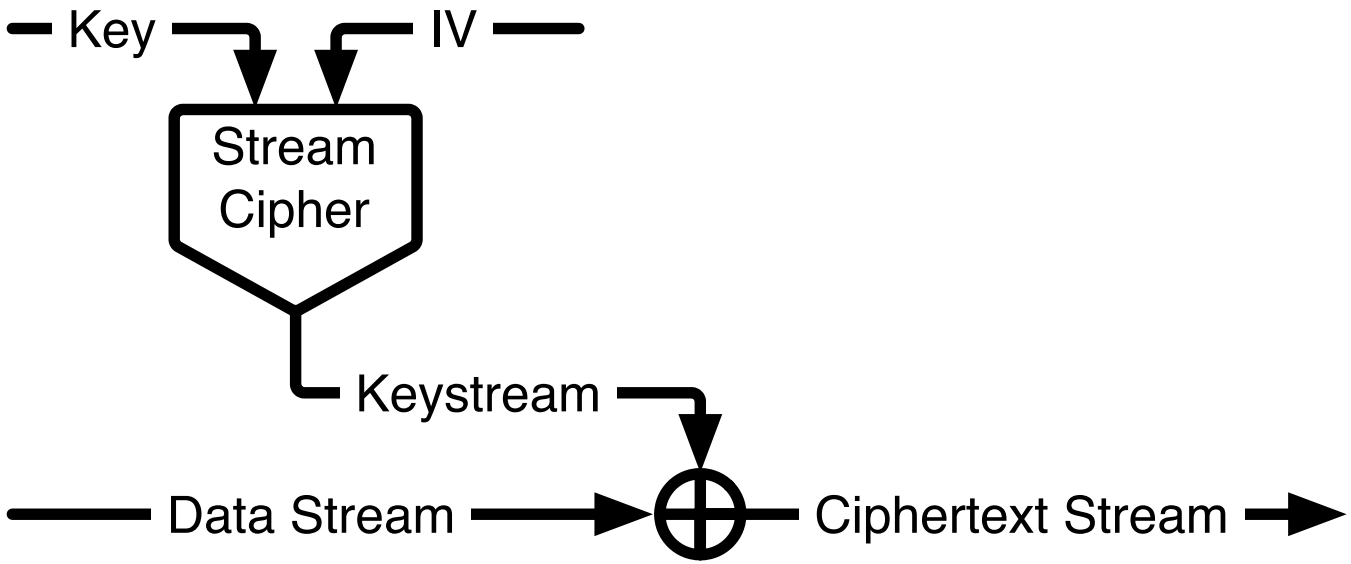
25th Chaos Communications Congress,
Berlin, Germany
2008-12-29

Outline

1. Background
   - Introduction to Stream Ciphers
   - Current State of the Art
2. The eSTREAM Project
   - What is eSTREAM?
   - Software Ciphers
     - HC-128
     - Rabbit
     - Salsa20/12
     - SOSEMANUK
   - Hardware ciphers
     - Grain v1
     - MICKEY 2.0
     - Trivium
3. Final words

What is a Stream Cipher?

- Block ciphers (such as AES) are keyed permutations on a fixed-length data block.
- Stream ciphers output a sequence of random-looking symbols, the keystream, which is combined with the data with a simple XOR.



What do we mean by “Security”?

- Usual assumption: attacker can choose IVs adaptively, knows the keystream produced.
- Resource usage: an attack should be more efficient (wrt. time, memory, money, etc.) than checking all possible keys.
- Main types of attack (informal):
  1. Distinguishing: Attacker is unable to distinguish keystream from a true random source.
  2. State recovery: Attacker is unable to recover the internal state of the cipher / the secret key.

On RC4

- RC4: By far the most widely used stream cipher.
- Used or supported in WEP, WPA, Bittorrent, SSL, Kerberos, ...
- Advantages: Very fast in software. Simple description. Can be implemented in a dozen lines of C.
- Disadvantages: Output can be distinguished from random. No specified IV-handling. Hard to use correctly. State is large (2048 bits). Not suitable for hardware.
- Saga of WEP and WPA – RC4 is dangerous.

On AES

- The Advanced Encryption Standard (FIPS 197).
- AES in Counter mode (AES-CTR) is a stream cipher.
- Advantages: It's the Standard. Everybody uses it. Secure. Reasonable resource requirements.
- Disadvantages: Bad for "biodiversity". Everybody wants to break it. One size fits all badly.

Other Stream Ciphers

- Lots of bad proprietary stream ciphers.
- A5/1 and A5/2 used in GSM . . . broken.
- E0 used in Bluetooth . . . broken.
- MIFARE Classic, KEELOQ . . . oh dear.
- EU project “NESSIE” (2000 – 2003):
  all six stream ciphers were successfully attacked.
- There is a demand for secure stream ciphers – but most real-world stream ciphers suck. :-(

eSTREAM

- ECRYPT – “European Network of Excellence for Cryptology” – EU-funded research project, 2004–2008.
- eSTREAM – the ECRYPT Stream Cipher Project.
- Goal: “identify new stream ciphers that might become suitable for widespread adoption”.
- Ciphers: “must be demonstrably superior to the AES in at least one significant aspect”.
- eSTREAM is not a formal standardisation process.

eSTREAM timetable

- Call for primitives: November 2004.
- Deadline for submissions: April 29, 2005.
- Received 34 submissions in 2 usage profiles

Profile 1 Software applications with high throughput requirements.
Profile 2 Hardware applications with restricted resources.

- About half were broken.
- Final portfolio selection: April 15, 2008.

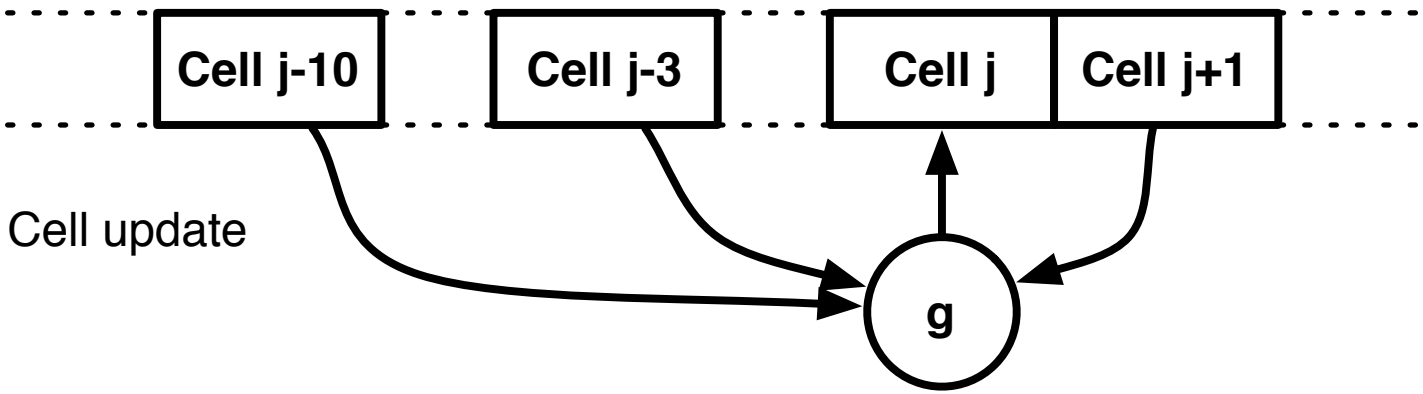
The Profile 1 ("Software") Ciphers

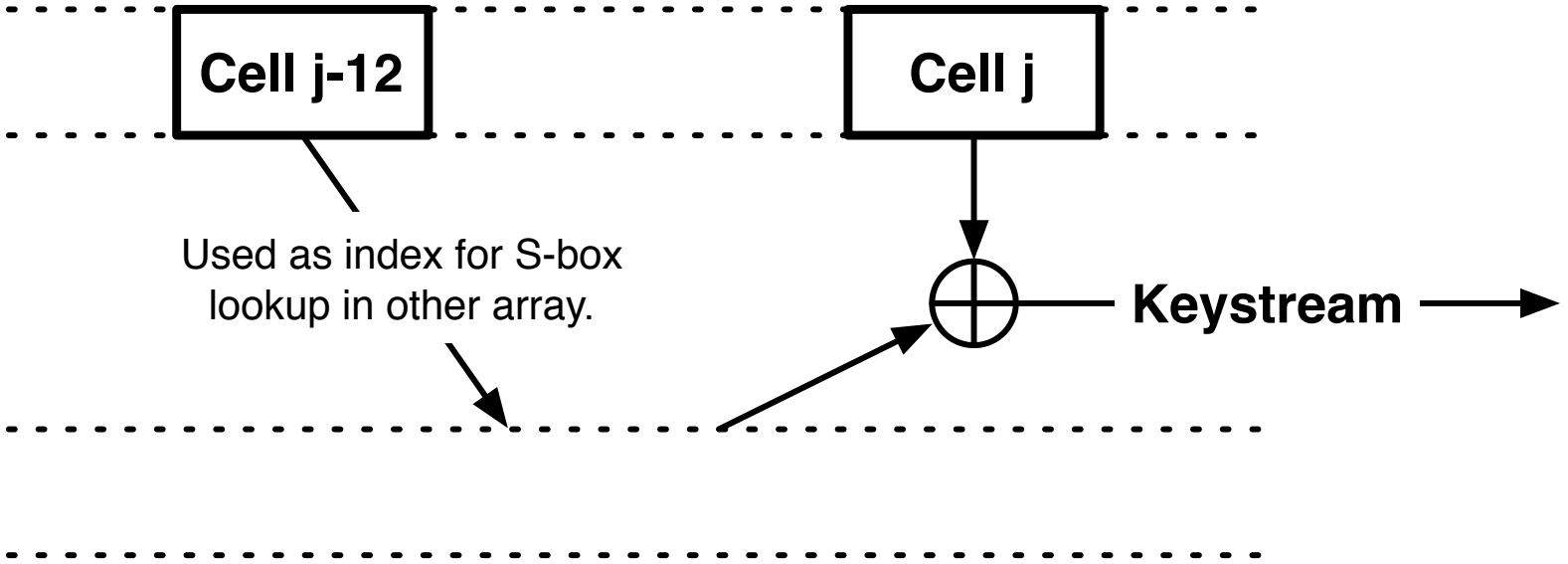
- Formal requirements for Profile 1:
  - Key length at least 128 bits.
  - IV length either 64 or 128 bits.
- The Profile 1 portfolio consists of four ciphers.
- HC-128 – designed by Wu.
- Rabbit – designed by Boesgaard et al.
- Salsa20/12 – designed by Bernstein.
- SOSEMANUK – designed by Berbain et al.

HC-128 (Specs)

- "HC" named after the author, "Hongyun's Cipher".
- Key length: 128 bits.
- IV length: 128 bits.
- State: 2x 512-word registers = 4 kilobytes.
- Output symbols: 32-bit words.
- Stream: Up to 2^{64} bits.
- Security: 128 bits.

HC-128 (Illustrated)





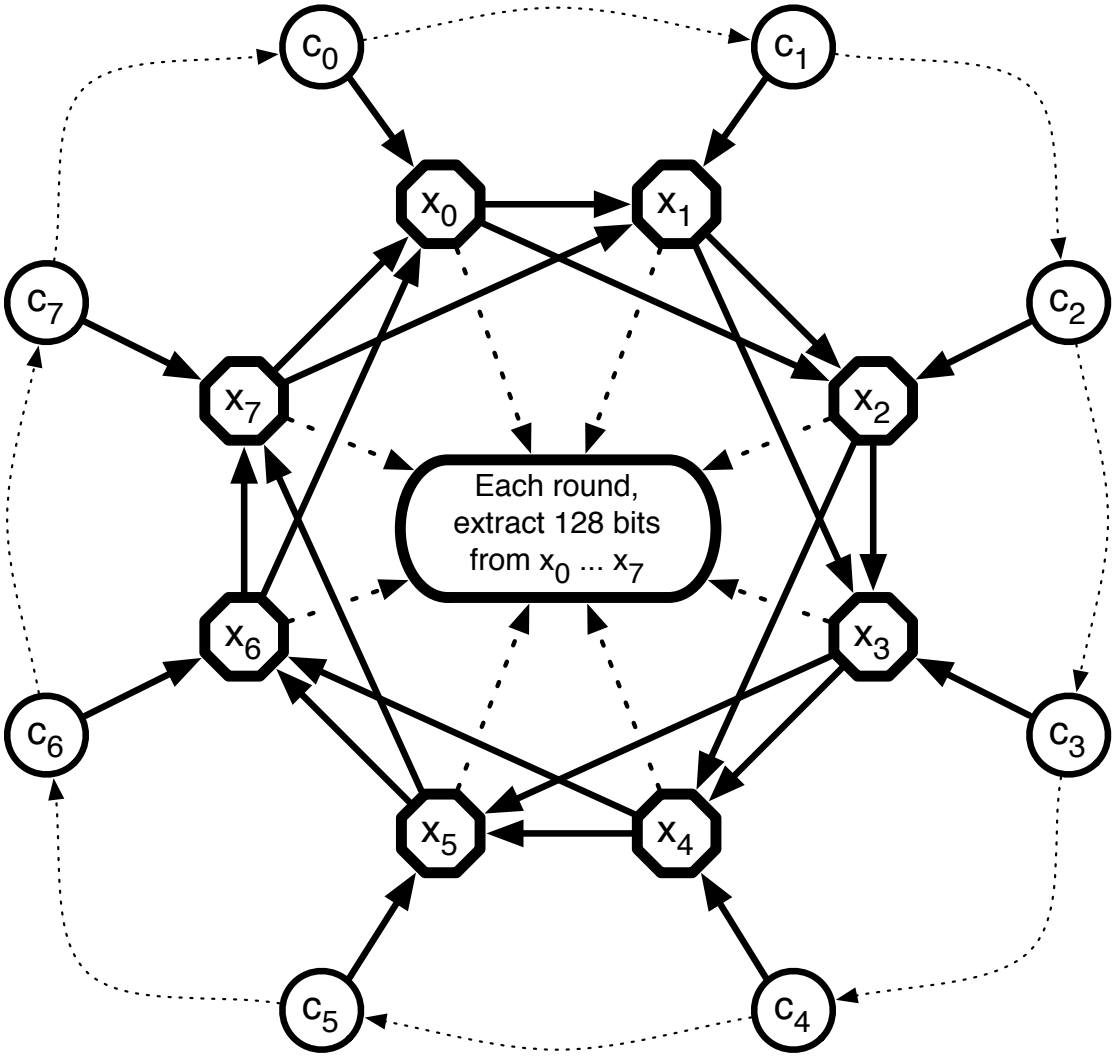
HC-128 (Notes)

- HC-128 is the eSTREAM that resembles RC4 the most. It reuses components from SHA-256.
- No regular attacks known. Cache timing (Zenner 2008)?
- The fastest eSTREAM for “long” streams (2-4 cycles/byte).
- AES-CTR runs at 15-30 CPB in the same setting (depending on platform).
- Horribly slow (> 500 cycles/byte) for short (40-byte) packets (AES: 18-26 CPB).
- Variant cipher HC-256 supports 256-bit keys.

Rabbit (Specs)

- Rabbit was designed by the Danish company Cryptico.
- Key length: 128 bits.
- IV length: 64 bits.
- State: 8 state words, 8 counter words, 1 carry bit = 513 bits (in practice 544 bits).
- Output: 128-bit blocks.
- Stream: Up to 2^{64} output blocks.
- Security: 128 bits.

Rabbit (Illustrated)



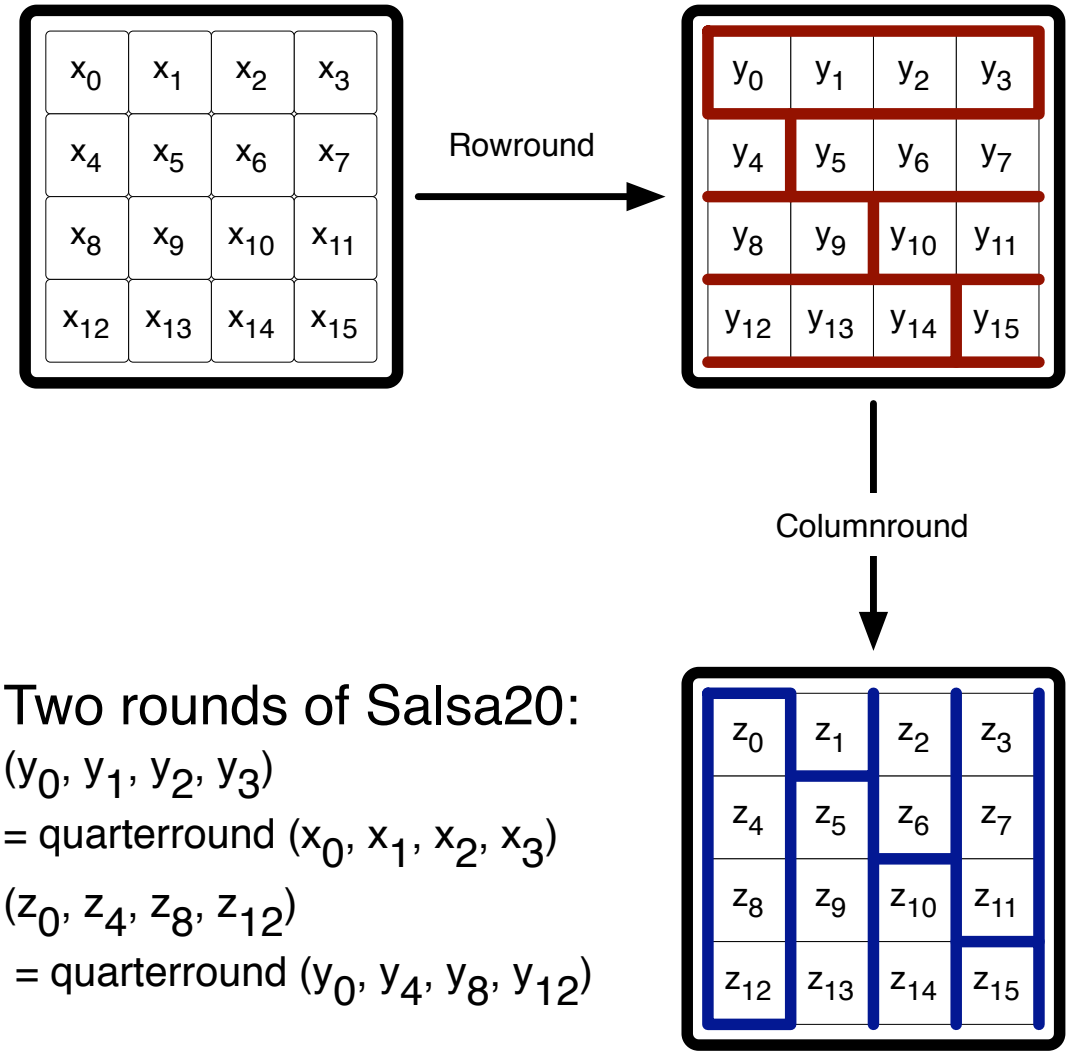
Rabbit (Notes)

- One of the oldest eSTREAMs, first published in early 2003.
- Simple symmetrical structure.
- The only portfolio cipher which had patent issues, but has always been free for noncommercial use.
- The cipher was released into the public domain by Cryptico in 2008, after eSTREAM ended.
- Rabbit is described in RFC 4503.
- About the same speed as AES on short packets, fast (2-10 cycles/byte) on long streams.

Salsa20/12 (Specs)

- I'm sure you all know who djb is. ;-)
- Key length: 256 bits.
- IV length: 64 bits.
- State: 4x4 matrix of words = 512 bits.
- Output: 512-bit blocks (entire state).
- Stream: At most 2^{64} blocks, due to the block counter.
- Security: 256 bits.

Salsa20/12 (Illustrated)



Two rounds of Salsa20:

(y_0, y_1, y_2, y_3)
= quarterround (x_0, x_1, x_2, x_3)

(z_0, z_4, z_8, z_{12})
= quarterround (y_0, y_4, y_8, y_{12})

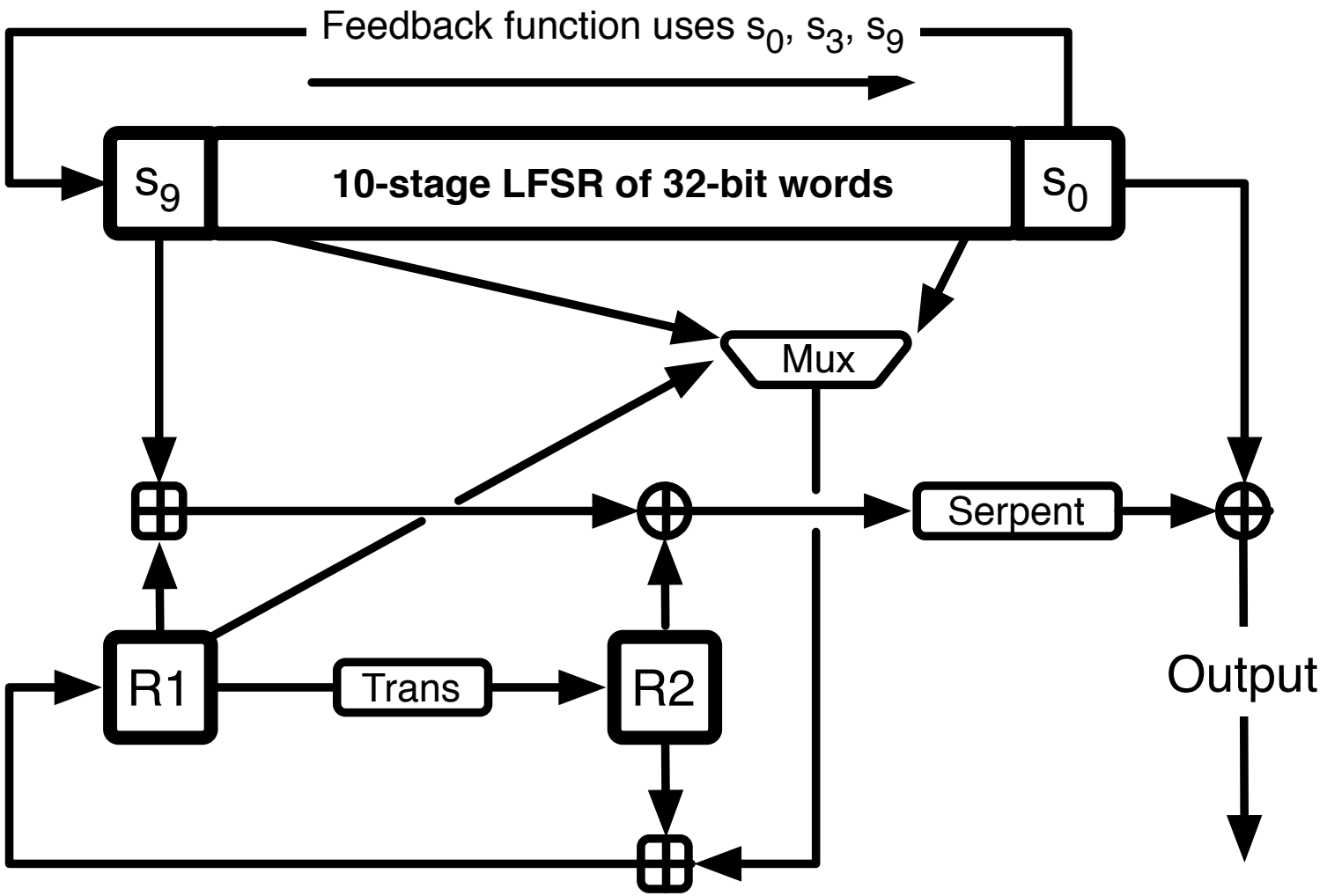
Salsa20/12 (Notes)

- Quarterround function: simple ADD-ROL-XOR.
- Salsa20 is basically a hash function in counter mode.
- Easy to describe, analyse, implement.
- djb has a good track record with respect to security.
- Salsa20/x has x rounds. “Full” version is Salsa20/20.
- Best attack is on 8 rounds (i.e. Salsa20/8).
- Slightly faster than AES on short packets;
  2.5-8 cycles/byte for long streams.
- Variant: ChaCha, proposed in early 2008.

SOSEMANUK (Specs)

- "SOSEMANUK" means "snowsnake" in the Cree language.
- Key length: 128 - 256 bits.
- IV length: 128 bits.
- State: 10 word LFSR and 2 words of FSM = 384 bits.
- Stream: (not specified)
- Output: one 128-bit block every 4 steps.
- Security: $\geq$ 128 bits.

SOSEMANUK (Illustrated)



SOSEMANUK (Notes)

- The cipher reuses parts of previous ciphers; notably the stream cipher SNOW 2.0 and the block cipher SERPENT.
- While SOSEMANUK supports key lengths up to 256 bits, the designers only claim 128-bit security.
- The best known attack (on the 256-bit version) takes on the order of 2^{224} steps.
- Performance: 3.5 - 8 cycles/byte for long streams, slower than AES-CTR on 40-byte packets.

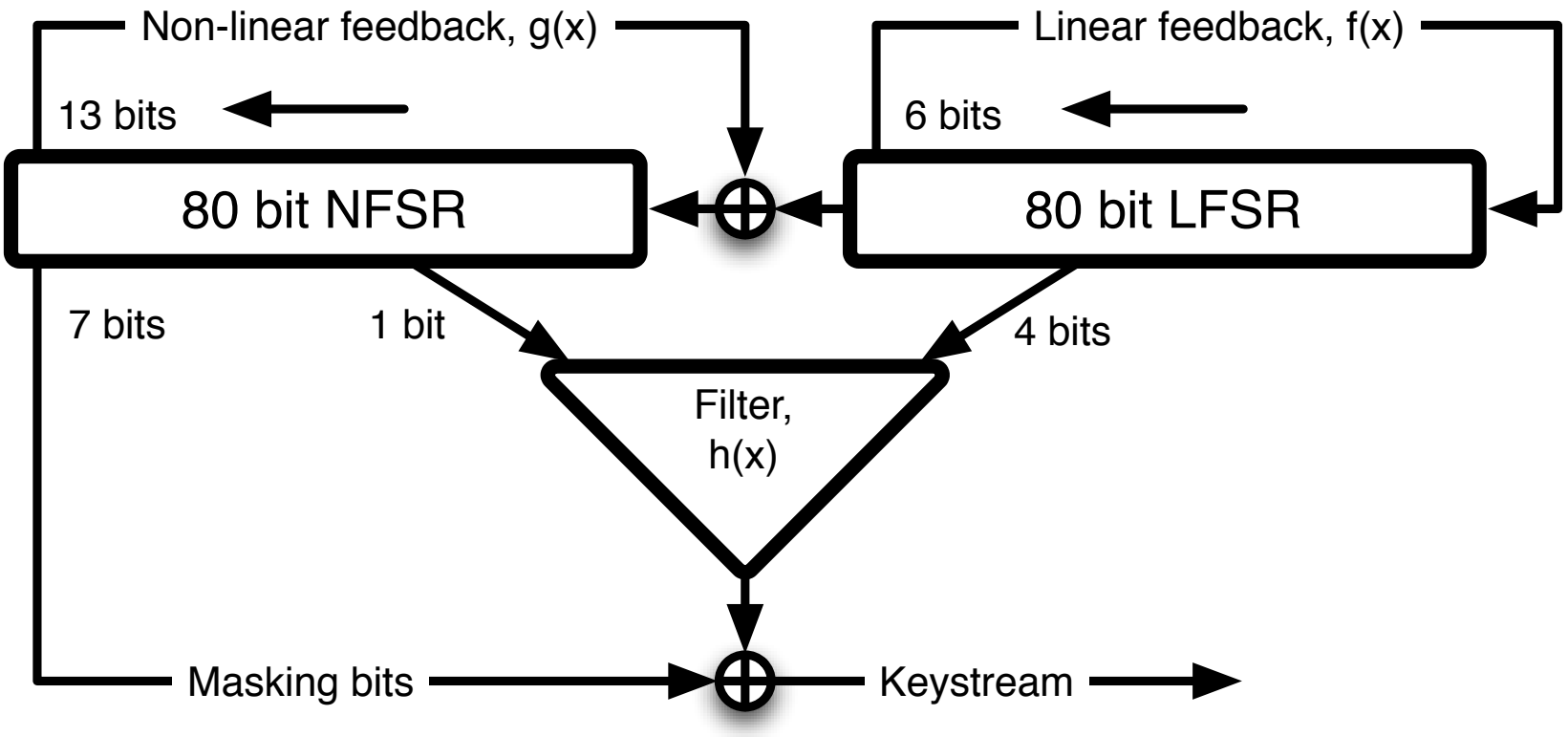
The Profile 2 ("Hardware") Ciphers

- Formal requirements for Profile 2:
  - Key length at least 80 bits.
  - IV length either 32 or 64 bits.
- The Profile 2 portfolio consists of three ciphers.
- Grain – designed by Hell et al.
- MICKEY – designed by Babbage and Dodd.
- Trivium – designed by De Cannère and Preneel.

Grain v1 (Specs)

- I have no idea where they got the name for this one.
- Key length: 80 bits.
- IV length: 64 bits.
- State: 2x 80-bit registers = 160 bits.
- Stream: (not specified)
- Output: 1 bit, can be unrolled for 16 steps.
- Security: 79 bits.

Grain v1 (Illustrated)



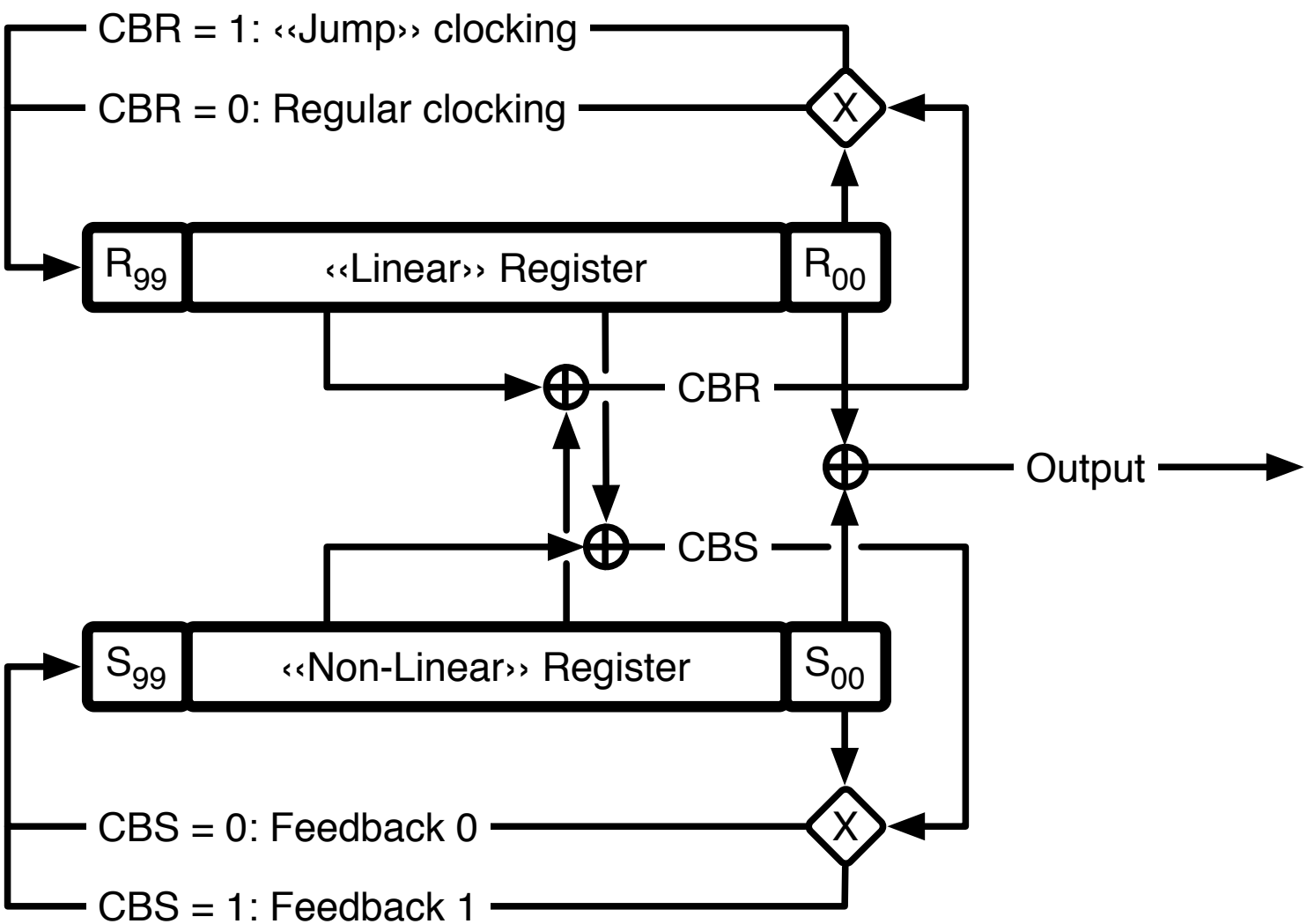
Grain v1 (Notes)

- The most compact hardware cipher, can be implemented in about 1300 NAND eq. gates.
- Fast in hardware, unrolling enables different tradeoffs.
- Security margin is extremely tight. Attacks on initialisation. Sliding property. Time/Memory tradeoff.
- Also a 128-bit version, Grain-128.

MICKEY 2.0 (Specs)

- Mutually Irregular Clocking KEYstream generator.
- Key length: 80 bits
- IV length: up to 80 bits
- State: 200 bits
- Stream: 2^{40} bits for 2^{40} unique IVs.
- Output: 1 bit.
- Security: 80 bits.

MICKEY 2.0 (Illustrated)



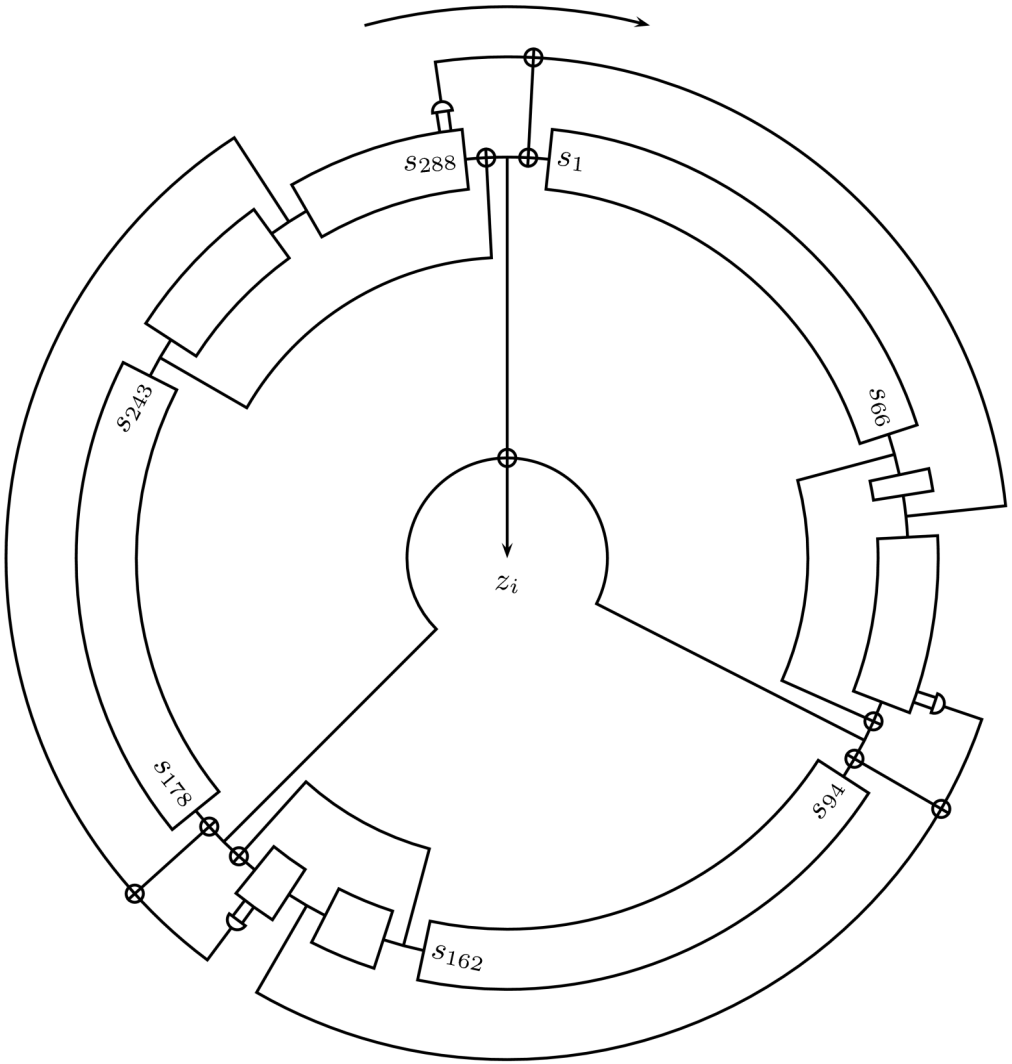
MICKEY 2.0 (Notes)

- Slower and larger than Grain and Trivium, more conservative design.
- Possible side channel issues as result of irregular clocking mechanism?
- Design is said to be clear and easy to implement.
- No known attacks that approach the complexity of bruteforcing the key.
- Variant MICKEY-128 supports longer keys.

Trivium (Specs)

- "Trivium" refers both to the cipher's structure, and its simplicity.
- Key length: 80 bits
- IV length: 80 bits
- State: 288 bits
- Stream: 2^{64} bits
- Output: 1 bit, can be unrolled for 64 steps.
- Security: 80 bits?

Trivium (Illustrated)



Trivium (Notes)

- The fastest Profile 2 cipher, but the largest state.
- Extremely simple description has made Trivium a prime target for almost everyone.
- Possibility of unrolling allows flexible tradeoffs.
- Maximov and Biryukov show that guess-and-determine attacks *almost* break the cipher.
- Dinur and Shamir break 735 (of 1152) initialisation rounds by cube attack, estimate that attack works for 1024 rounds.

On the Final Portfolio Cipher

- There used to be four Profile 2 ciphers in the portfolio.
- F-FCSR-H was recently broken by Hell and Johansson.
- Practical linearisation attack which breaks the cipher in minutes.
- The attack was published at ASIACRYPT 2008.
- The cipher was removed from the eSTREAM portfolio in September 2008.
- Whoops.

On Confidence and Future Attacks

- “Attacks never get worse, they only get better”.
- Confidence in security increases over time.
- Faith in security of AES remains much stronger.
- New attacks may not be practical, or depend on specific usage. Or not.
- Do Cube Attacks (Dinur and Shamir, CRYPTO 2008) apply to the hardware candidates?
- Use at own risk. ;-)

The NIST Hash Function Competition (SHA-3)

- The next big thing for cryptanalysts to play with.
- NIST wants to find a new hash function standard.
- Similar to the AES process (and eSTREAM).
- 64 submissions, 51 made it to the first evaluation round.
- Currently 17 of the proposals have been broken.
- Final decision expected in Q2 2012.

Summary

- eSTREAM has identified 7 new, promising stream ciphers.
- Ciphers offer various performance tradeoffs.
- All “better” than AES in some respect.

- Beware of future cryptanalysis – still very young ciphers.
- If in doubt, AES(-CTR) is still the safest choice. ;-)

Thank You!

Thanks for listening!
Any questions?

Further Reading


M. Robshaw and O. Billet (Eds.).
New Stream Cipher Designs – The eSTREAM Finalists.
LNCS 4986. Springer–Verlag, 2008.
http://www.ecrypt.eu.org/stream/


Stream-cipher timings (Software).
http://cr.yp.to/streamciphers/timings.html


The SHA-3 Zoo.
http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo