

## Correlated Keystreams in Moustique

Emilia Käsper, Vincent Rijmen, Tor Bjørstad, Christian  
Rechberger, Matt Robshaw and Gautham Sekar

K.U. Leuven, ESAT-COSIC  
The Selmer Center, University of Bergen  
Graz University of Technology  
France Télécom Research and Development

Africacrypt 2008  
Casablanca, June 2008

# Background on eStream

- April 2005: Call for stream cipher primitives
- 34 submissions
- April 2007: 16 ciphers in “focus”
- May 2008: final portfolio, 8 ciphers

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

# eStream Portfolio

software	hardware
CryptMT	DECIM
Dragon	Edon80
HC	F-FCSR
LEX	Grain
NLS	Mickey
Rabbit	Moustique
Salsa20	Pomaranch
SOSEMANUK	Trivium

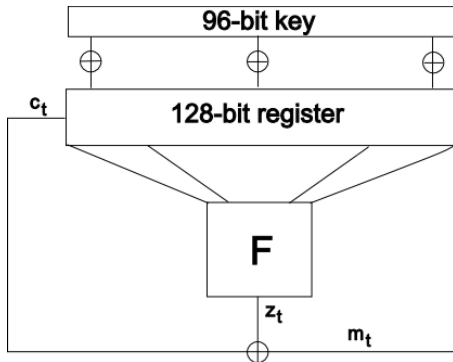
# eStream Portfolio

software	hardware
HC-128	F-FCSR-H v2 Grain v1 Mickey v2
Rabbit Salsa20/12 SOSEMANUK	Trivium

# Moustique factsheet

- Tweaked version of Mosquito
- hardware-oriented design, encryption bit-by-bit
- 96-bit key
- 128-bit state with nonlinear state update
- nonlinear output filter
- self-synchronization after 105 correctly received ciphertext bits

## Moustique: high-level structure

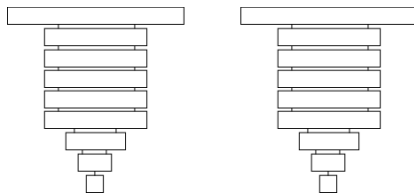


$$g(a, b, c, d) = a + b + c(d + 1) + 1$$

## Key ideas

- Differential cryptanalysis: find “related” internal states that give correlated output
- Related-key attack: use related keys to obtain such related states
- Distinguishing attack: observe output of two cipher copies running on related keys, detect correlation
- Divide-and-conquer: fast key recovery in related-key setting
- “Smarter” exhaustive search without related keys

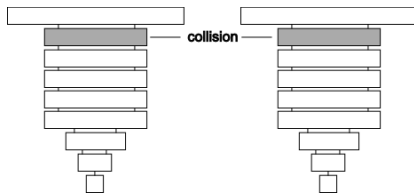
## Weaknesses in the filter function [JM06]



- First round of filtering compressing

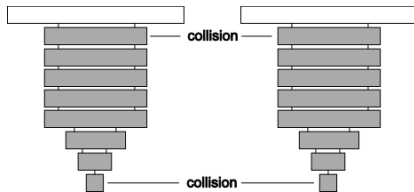


## Weaknesses in the filter function [JM06]



- First round of filtering compressing
- Diffusion in first round is weak—single-bit differences give collisions

## Weaknesses in the filter function [JM06]



- First round of filtering compressing
- Diffusion in first round is weak—single-bit differences give collisions
- Example: Two register states with only difference in bit  $x_{71}$  give coinciding outputs with probability  $3/4$ .

## Weaknesses in register update

- Each register bit  $x_i$  ( $1 \leq i \leq 88$ ) depends only on one key bit  $k_{i-1}$  and previous state bits  $x_1, \dots, x_{i-1}$
- Flipping key bit  $k_{70}$  flips  $x_{71}$

$$x_{71}^{(t+1)} = x_{70}^{(t)} + k_{70} + x_{67}^{(t)}(x_{69}^{(t)} + 1) + 1$$

## Weaknesses in register update

- Each register bit  $x_i$  ( $1 \leq i \leq 88$ ) depends only on one key bit  $k_{i-1}$  and previous state bits  $x_1, \dots, x_{i-1}$
- Flipping key bit  $k_{70}$  flips  $x_{71}$

$$x_{71}^{(t+1)} = x_{70}^{(t)} + k_{70} + x_{67}^{(t)}(x_{69}^{(t)} + 1) + 1$$

- Deterministic left-to-right difference propagation:

$$x_{72}^{(t+2)} = x_{71}^{(t+1)} + k_{71} + x_{67}^{(t+1)}(c^{(t+2)} + 1) + 1$$

$$x_{73}^{(t+2)} = x_{72}^{(t+1)} + k_{72} + x_{48}^{(t+1)} + x_{71}^{(t+1)}$$

## Weaknesses in register update

- Each register bit  $x_i$  ( $1 \leq i \leq 88$ ) depends only on one key bit  $k_{i-1}$  and previous state bits  $x_1, \dots, x_{i-1}$
- Flipping key bit  $k_{70}$  flips  $x_{71}$

$$x_{71}^{(t+1)} = x_{70}^{(t)} + k_{70} + x_{67}^{(t)}(x_{69}^{(t)} + 1) + 1$$

- Deterministic left-to-right difference propagation:

$$x_{72}^{(t+2)} = x_{71}^{(t+1)} + k_{71} + x_{67}^{(t+1)}(c^{(t+2)} + 1) + 1$$

$$x_{73}^{(t+2)} = x_{72}^{(t+1)} + k_{72} + x_{48}^{(t+1)} + x_{71}^{(t+1)}$$

- Flipping key bits  $k_{71}, k_{72}$  cancels difference

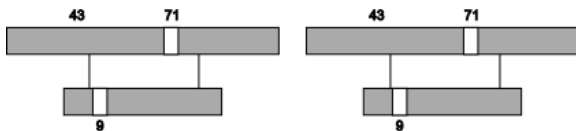
## Related-key distinguisher

- Correlated keystream from each pair  
 $k_0, k_1, \dots, k_{70}, k_{71}, k_{72}, \dots, k_{95}$   
 $k_0, k_1, \dots, k_{70} + 1, k_{71} + 1, k_{72} + 1, \dots, k_{95}$
- We found 8 more such related-key sets
- So: Each key has 8 related keys that produce correlated keystream for any ciphertext
- Bias 0.25 or in some cases stronger = keystream overlap  $\geq 75\%$

## Related-key key recovery

- Observe output from two related keys with  $x_{71}$  flipped
- Bit  $x_{71}$  affects filter output only in

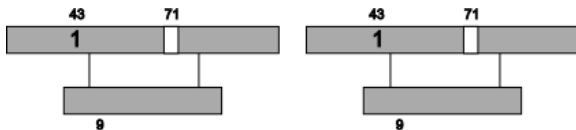
$$a_9 = x_{86} + x_{60} + x_{71}(x_{43} + 1) + 1$$



## Related-key key recovery

- Observe output from two related keys with  $x_{71}$  flipped
- Bit  $x_{71}$  affects filter output only in

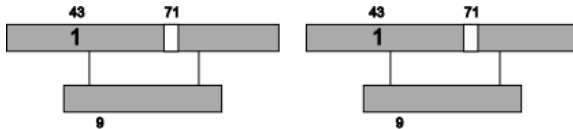
$$a_9 = x_{86} + x_{60} + x_{71}(x_{43} + 1) + 1$$



- $x_{43} = 1$  yields collision



## Divide-and-conquer approach



- Guessing 43 bits of the key allows to compute  $x_{43}$
- If  $x_{43} = 1$  but outputs differ, the guess was wrong.
- Repeat for a second related key at position  $x_{89}$ .
- With some fine-tuning, final attack complexity  $2^{38}$ .

## Relevance of Related-Key Properties

- Attack scenario unrealistic:
  - Attacker allowed to modify key—unreasonable assumption (?)
  - Proper key generation a must (e.g., key should not be increased as counter)
  - Freshness provided by IV-s
- ...but related-key properties show (first) weakness of design:
  - Stream cipher  $\approx$  PRNG
  - May be used in applications other than encryption
  - The case of Moustique: freshness of IV not applicable, as cipher “forgets” IV

## Smart exhaustive search

- Recall: each key has 8 related keys.
- Piling-Up Lemma—Key space partitioned into sets of 256 keys, bias within a set ranges from 0.25 to  $2^{-9}$
- Test only  $2^{88}$  keys—correlation with correct keystream will emerge.
- Trade-off: need longer keystream per candidate key (=more time).

## Smarter exhaustive search

- Two states with related keys differ in at most 8 bits
- With probability  $p = \frac{5}{8} \cdot \frac{1}{2^7}$ , these bits do not affect output
  - Test one key in a set of  $2^8$  keys
  - If 8 “check bits” neutral but output differs from known keystream, eliminate the set of  $2^8$  keys
- Need on average  $\frac{2}{p} \approx 410$  bits of keystream
- Complexity  $(105 + 410) \cdot 2^{88} \approx 2^{97}$  vs  $105 \cdot 2^{96} \approx 2^{103}$
- Speed-up factor 50, conjectured security 90 bits.

## Summary

- Moustique keyspace partitioned into sets of 256 keys that produce correlated output
- Related-key key recovery in  $2^{38}$  steps (96-bit key)
- Conjectured security in known keystream scenario  $2^{90}$
- Moustique eliminated from eSTREAM final portfolio
- How to design a secure self-synchronizing stream cipher?

Thank you! Questions?