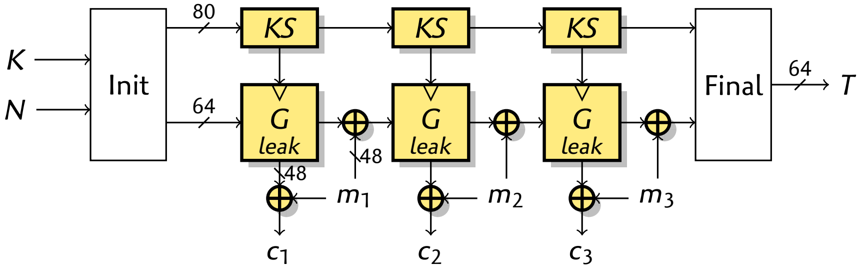
Cryptanalysis of LAC

Gaëtan Leurent

Inria, France

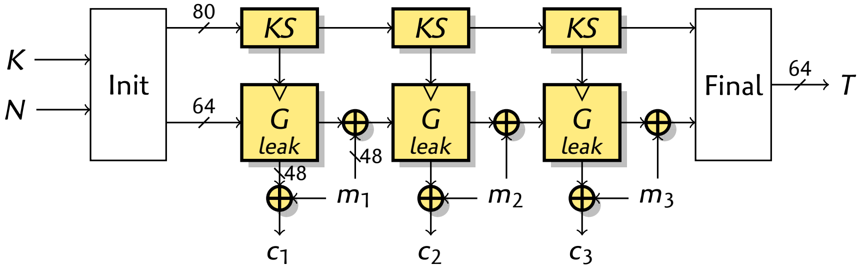
DIAC 2014

Description of LAC



- Designed by Chinese Academy of Science researchers
  - Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, Jian Zhang
- Follows the structure of ALE
  - *G* based on modified LBlock.
  - 80-bit key, 64-bit state, 48-bit leak

Description of LAC

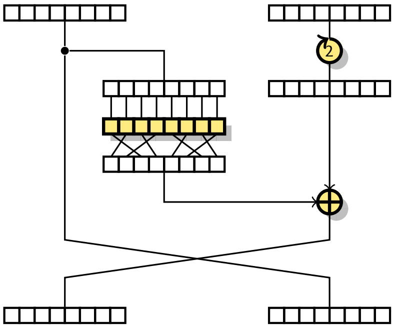


Security claims

- Confidentiality: 80 bits
- Authenticity: 64 bits

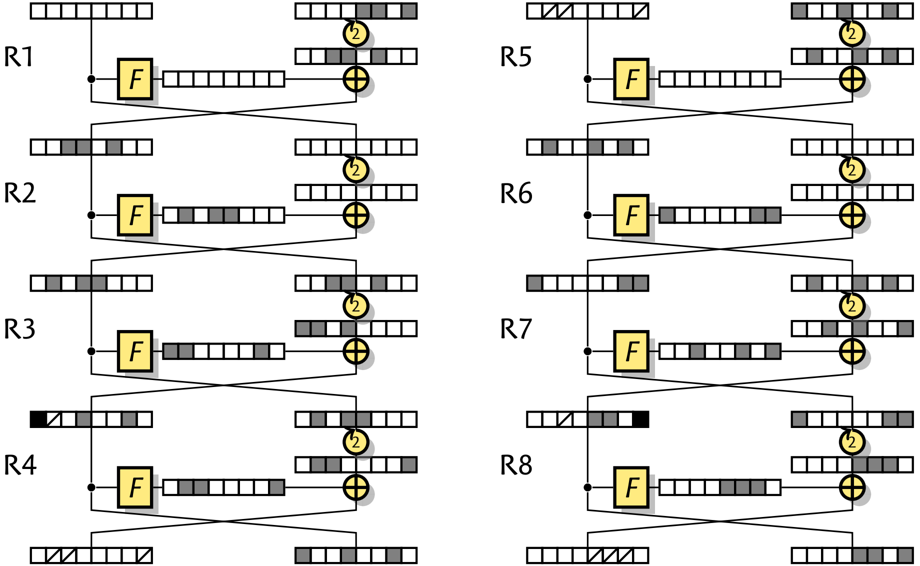
"any forgery attack with an unused tuple has a success probability at most 2^{-64}"

Inside LBlock-s

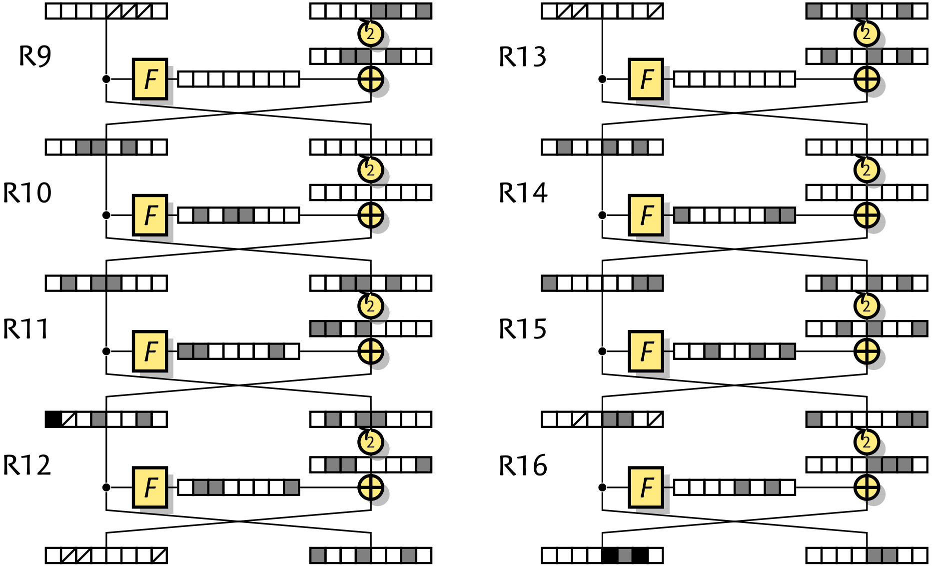


- Feistel structure
- 16 rounds
  - Key addition
  - Nibble S-box
  - Nibble permutation
- Best characteristics
  - 35 active Sboxes
  - Proba $\leq 2^{-70}$

Truncated differential characteristic



Truncated differential characteristic



Differential and characteristics

Differential $\alpha \rightsquigarrow \beta$

Characteristic $\alpha_0 \to \alpha_1 \to \cdots \alpha_n = \beta$

- Common assumption:
  A single characteristic dominates the differential
  - Modifying one step leads to significantly different characteristics
- Not necessarily true for byte-wise designs
  - Given a truncated characteristics, there are many instantiated characteristics with the same input/output difference.

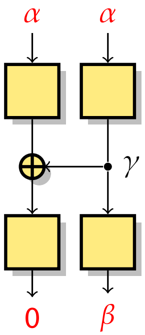
Differential and characteristics

Differential $\alpha \rightsquigarrow \beta$

Characteristic $\alpha_0 \to \alpha_1 \to \cdots \alpha_n = \beta$

- Common assumption:
  A single characteristic dominates the differential
  - Modifying one step leads to significantly different characteristics
- Not necessarily true for byte-wise designs
  - Given a truncated characteristics, there are many instantiated characteristics with the same input/output difference.

A simple example



- Fixed differential $(\alpha, \alpha) \to (0, \beta)$
- Many characteristics: all possible γ

$$\Pr\Big[(\alpha,\alpha) \to (0,\beta)\Big] = \sum_{\gamma} \Pr\Big[\alpha \to \gamma\Big]^2 \cdot \Pr\Big[\gamma \to \beta\Big]$$

- If S-box has a flat differential table, $\approx 2^n$ characteristics with probability $\approx 2^{-3n}$
- Can we evaluate the sum of all the characteristics following a truncated characteristic?

Computing aggregation

- Consider a fixed truncated characteristic D
  - D_i is the first i rounds of D
- $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following D
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right] \leq \Pr\left[\alpha \rightsquigarrow \beta\right]$

Computing $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$

1. Compute $\Pr[D_1 : \alpha \rightsquigarrow x]$ for all x following D_1
2. Compute $\Pr[D_i : \alpha \rightsquigarrow x]$ for all x following D_i iteratively:
   $\Pr[D_i : \alpha \rightsquigarrow x] = \sum_{x'} \Pr[D_{i-1} : \alpha \rightsquigarrow x'] \times \Pr[x' \rightsquigarrow x]$

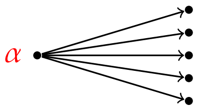
α

Computing aggregation

- Consider a fixed truncated characteristic D
  - D_i is the first i rounds of D
- $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following D
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right] \leq \Pr\left[\alpha \rightsquigarrow \beta\right]$

Computing $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$

1. Compute $\Pr[D_1 : \alpha \rightsquigarrow x]$ for all x following D_1
2. Compute $\Pr[D_i : \alpha \rightsquigarrow x]$ for all x following D_i iteratively:
   $\Pr[D_i : \alpha \rightsquigarrow x] = \sum_{x'} \Pr[D_{i-1} : \alpha \rightsquigarrow x'] \times \Pr[x' \rightsquigarrow x]$

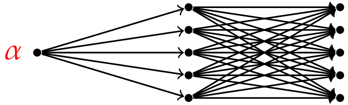


Computing aggregation

- Consider a fixed truncated characteristic D
  - D_i is the first i rounds of D
- $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following D
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right] \leq \Pr\left[\alpha \rightsquigarrow \beta\right]$

Computing $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$

1. Compute $\Pr\left[D_1 : \alpha \rightsquigarrow x\right]$ for all x following D_1
2. Compute $\Pr\left[D_i : \alpha \rightsquigarrow x\right]$ for all x following D_i iteratively:
   $\Pr\left[D_i : \alpha \rightsquigarrow x\right] = \sum_{x'} \Pr\left[D_{i-1} : \alpha \rightsquigarrow x'\right] \times \Pr[x' \rightsquigarrow x]$

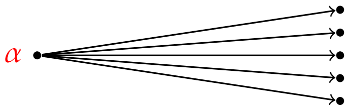


Computing aggregation

- Consider a fixed truncated characteristic D
  - D_i is the first i rounds of D
- $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following D
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right] \leq \Pr\left[\alpha \rightsquigarrow \beta\right]$

Computing $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$

1. Compute $\Pr\left[D_1 : \alpha \rightsquigarrow x\right]$ for all x following D_1
2. Compute $\Pr\left[D_i : \alpha \rightsquigarrow x\right]$ for all x following D_i iteratively:
   $\Pr\left[D_i : \alpha \rightsquigarrow x\right] = \sum_{x'} \Pr\left[D_{i-1} : \alpha \rightsquigarrow x'\right] \times \Pr[x' \rightsquigarrow x]$

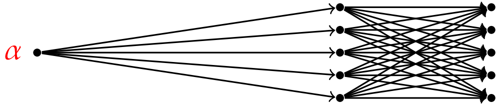


Computing aggregation

- Consider a fixed truncated characteristic D
  - D_i is the first i rounds of D
- $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following D
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right] \leq \Pr\left[\alpha \rightsquigarrow \beta\right]$

Computing $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$

1. Compute $\Pr\left[D_1 : \alpha \rightsquigarrow x\right]$ for all x following D_1
2. Compute $\Pr\left[D_i : \alpha \rightsquigarrow x\right]$ for all x following D_i iteratively:
   $\Pr\left[D_i : \alpha \rightsquigarrow x\right] = \sum_{x'} \Pr\left[D_{i-1} : \alpha \rightsquigarrow x'\right] \times \Pr[x' \rightsquigarrow x]$

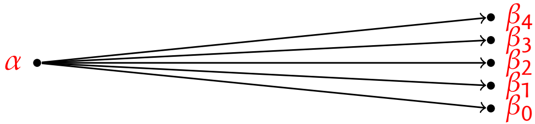


Computing aggregation

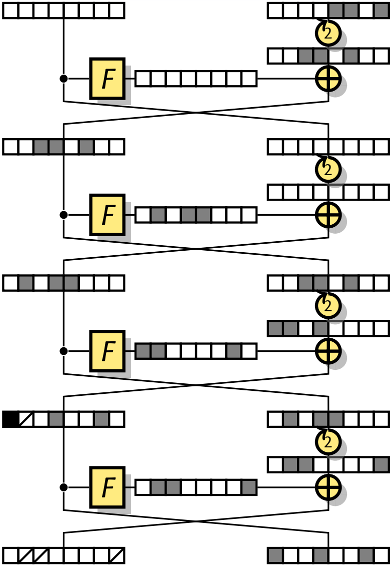
- Consider a fixed truncated characteristic D
  - D_i is the first i rounds of D
- $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following D
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right] \leq \Pr\left[\alpha \rightsquigarrow \beta\right]$

Computing $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$

1. Compute $\Pr[D_1 : \alpha \rightsquigarrow x]$ for all x following D_1
2. Compute $\Pr[D_i : \alpha \rightsquigarrow x]$ for all x following D_i iteratively:
   $\Pr[D_i : \alpha \rightsquigarrow x] = \sum_{x'} \Pr[D_{i-1} : \alpha \rightsquigarrow x'] \times \Pr[x' \rightsquigarrow x]$



Application to LAC



- At most 6 active nibbles
  - Storage 2^{24}
- At most 3 active Sboxes
  - At most 2^{9} transitions
  - Time 2^{37}

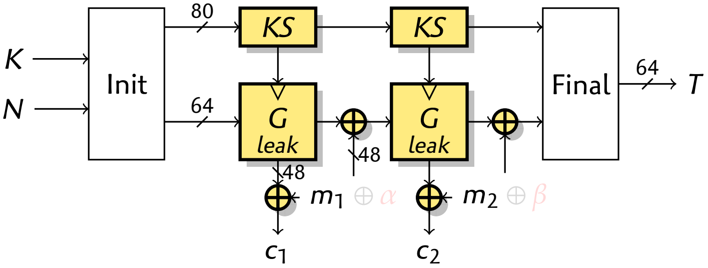
Results

17512 differentials with $p > 2^{-64}$

Best differentials found:

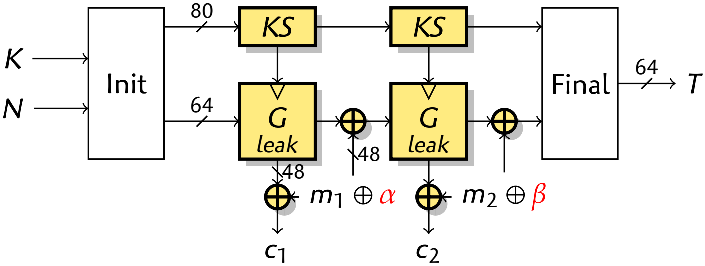
$p \geq 2^{-61.52}$

Forgery Attack



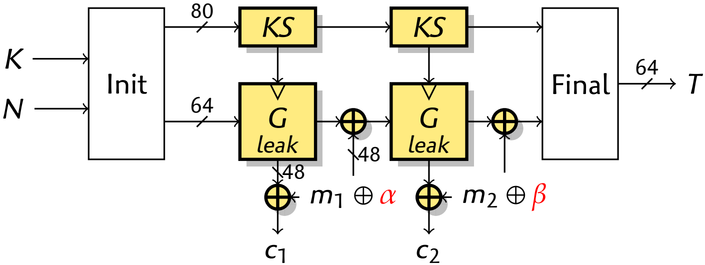
1. Get a valid message $(m_1 \parallel m_2, c_1 \parallel c_2, \tau)$
2. $(c_1 \oplus \alpha \parallel c_2 \oplus \beta, \tau)$ is a forge with probability $\geq 2^{-61.52}$
   - Corresponding plaintext: $m_1 \oplus \alpha \parallel m_2 \oplus \beta$, because the truncated characteristic doesn't affect the leak

Forgery Attack



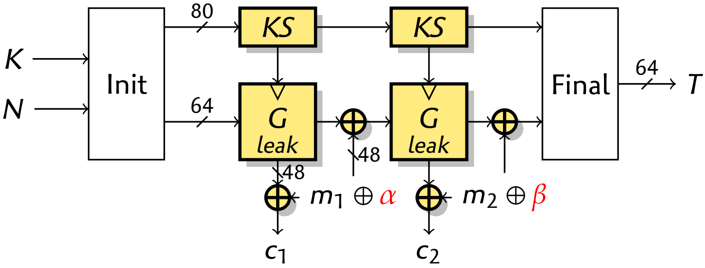
1. Get a valid message $(m_1 \parallel m_2, c_1 \parallel c_2, \tau)$
2. $(c_1 \oplus \alpha \parallel c_2 \oplus \beta, \tau)$ is a forge with probability $\geq 2^{-61.52}$
   - Corresponding plaintext: $m_1 \oplus \alpha \parallel m_2 \oplus \beta$,
     because the truncated characteristic doesn't affect the leak

Forgery Attack



1. Get a valid message $(m_1 \| m_2, c_1 \| c_2, \tau)$
2. $(c_1 \oplus \alpha \| c_2 \oplus \beta, \tau)$ is a forge with probability $\geq 2^{-61.52}$
   - Corresponding plaintext: $m_1 \oplus \alpha \| m_2 \oplus \beta$,
     because the truncated characteristic doesn't affect the leak

Forgery Attack



Is it an attack?

- Probability slightly lower than claimed for forgery ($2^{-61.52}$ *vs.* 2^{-64})
- Need new data to repeat...
  - Can use several differentials (17512 in this class)
  - Design limited to 2^{40} data

Cryptanalysis of Wheesht

Anne Canteaut Gaëtan Leurent

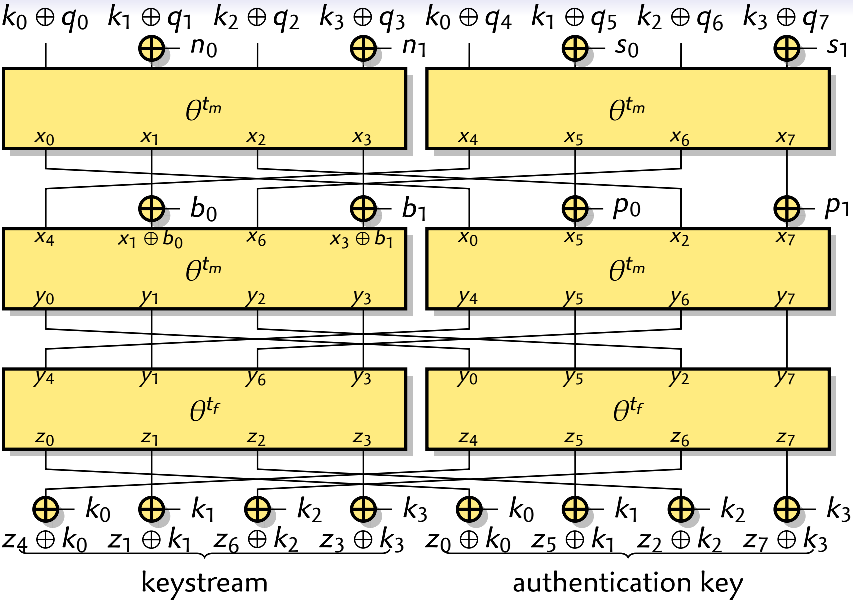
Inria, France

DIAC 2014

CAESAR candidate Wheesht

- Designed by Peter Maxwell
- 256-bit security
- ARX, 64-bit words
- Encryption: counter mode stream cipher
- Notations:
  - Encryption key k_i;
  - Constants q_i;
  - Public nonce n_i;
  - Secret nonce s_i;
  - Block counter b_i;
  - Extra parameters p_i;

Wheesht structure



Wheesht Analysis

Our results

1. Generic keystream distinguisher
   - Using 2^{71} data & time
2. Generic key recovery
   - Using 2^{197} data, 2^{192} time
3. Key recovery for Wheesht-3-1-256
   - Using 2^{10} data, 2^{200} time

Differential attack on the authentication by Samuel Neves

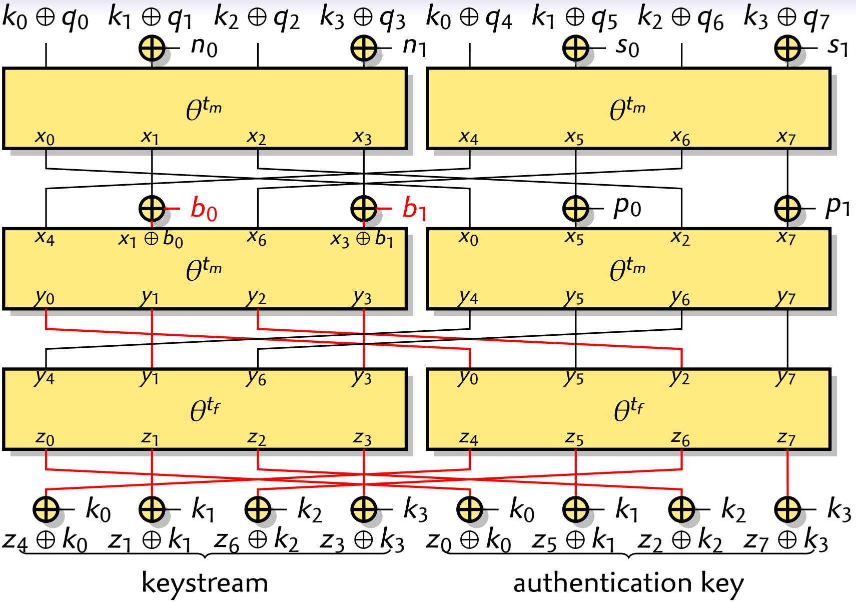
- Probability 1 differential
- Trivial forgeries

Wheesht Analysis

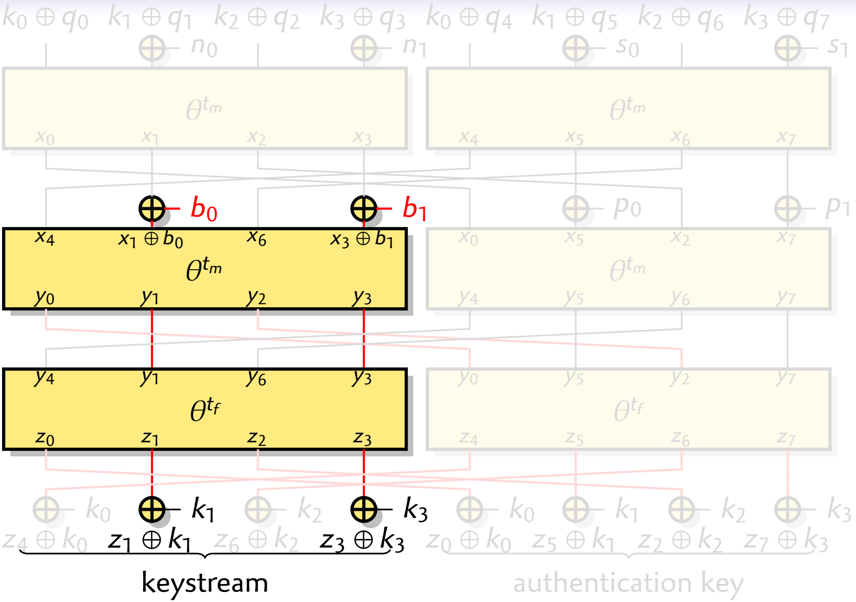
Our results

1. Generic keystream distinguisher
   - Using 2^{71} data & time
2. Generic key recovery
   - Using 2^{197} data, 2^{192} time
3. Key recovery for Wheesht-3-1-256
   - Using 2^{10} data, 2^{200} time

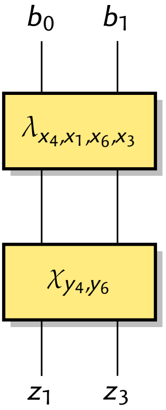
Incrementing the counter



Incrementing the counter



A Simple Distinguisher



$$(y_1, y_3) = \lambda_{x_4,x_1,x_6,x_3}(b_0, b_1)$$
$$(z_1, z_3) = \chi_{y_4,y_6}(y_1, y_3)$$

- $\lambda_{x_4,x_1,x_6,x_3}$ and χ_{y_4,y_6} fixed for a given message
  - Behave like random functions

The composition of two random functions is not a random function!

- Output space $0.46N$ rather than $0.63N$
- Distinguisher with $O(\sqrt{N})$ samples: time to first collision

Attack Algorithm

Capture 16 known plaintext messages of length 2^{67} blocks.

Denote the keystream as $\left(\sigma_j^{(i)}\right), 0 \leq i < 16, 0 \leq j < 2^{69}$

for $0 \leq i < 16$ **do**
  for $0 \leq k < 2$ **do**
    $\mathcal{S} \leftarrow \varnothing$
    for $0 \leq j < 2^{67}$ **do**
      if $(\sigma_{4j+k}, \sigma_{4j+2+k}) \in \mathcal{S}$ **then**
        $B[2i+k] \leftarrow j$
        break loop
      else
        $\mathcal{S} \leftarrow \mathcal{S} \cup \left\{(\sigma_{4j}, \sigma_{4g+2})\right\}$

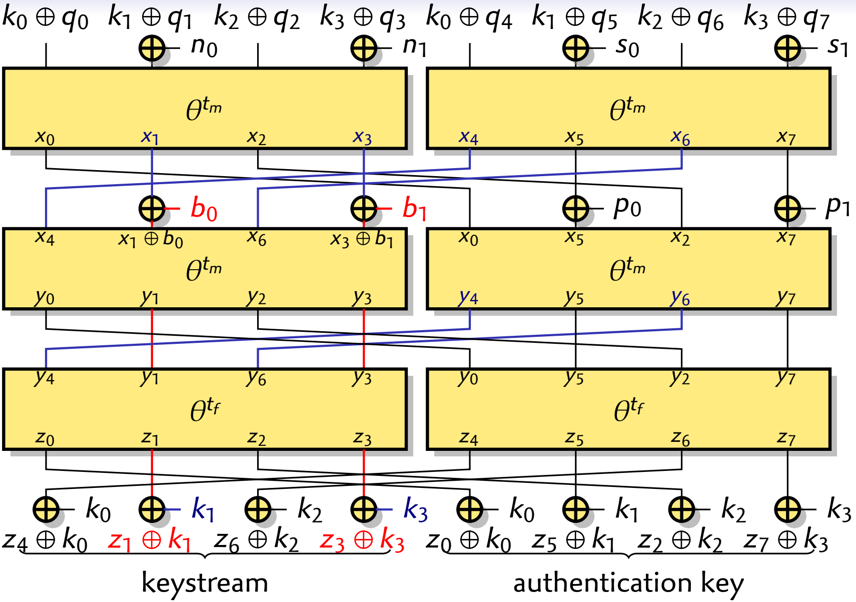
if Average$(B) < 1.038 \cdot 2^{64}$ **then**
  return 1: *keystream is from Wheesht*
else
  return 0: *keystream is random*

Wheesht Analysis

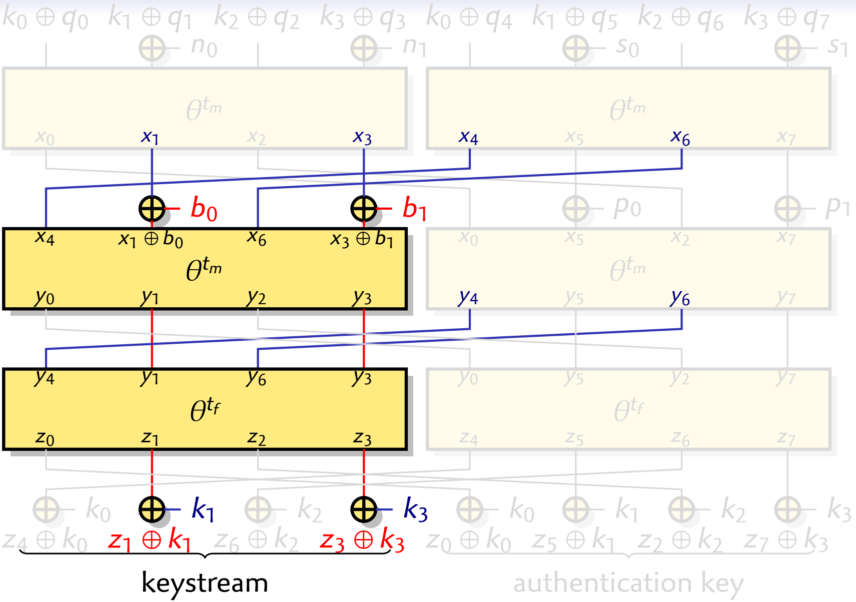
Our results

1. Generic keystream distinguisher
   - Using 2^{71} data & time
2. Generic key recovery
   - Using 2^{197} data, 2^{192} time
3. Key recovery for Wheesht-3-1-256
   - Using 2^{10} data, 2^{200} time

Generating output



Generating output



Key recovery attack

Simplified representation

$$(z_1^{(b)}, z_3^{(b)}) = f(x_4, x_1, x_6, x_3, y_4, y_6, b)$$
$$(\sigma_1^{(b)}, \sigma_3^{(b)}) = (z_1^{(b)}, z_3^{(b)}) \oplus (k_1, k_3)$$

- $x_4, x_1, x_6, x_3, y_4, y_6$ fixed for a given message

- Remove k_1, k_3:
  $g(x_4, x_1, x_6, x_3, y_4, y_6)$
  $= f(x_4, x_1, x_6, x_3, y_4, y_6, 0) \oplus f(x_4, x_1, x_6, x_3, y_4, y_6, 1)$
  $= (\sigma_1^{(0)}, \sigma_3^{(0)}) \oplus (\sigma_1^{(1)}, \sigma_3^{(1)})$
- Birthday match to recover $x_4, x_1, x_6, x_3, y_4, y_6$
  - Evaluate g with 2^{192} random states offline
  - Evaluate online with 2^{192} different messages

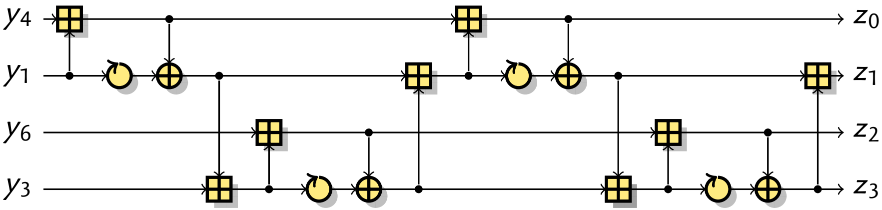
Wheesht Analysis

Our results

1. Generic keystream distinguisher
   - Using 2^{71} data & time
2. Generic key recovery
   - Using 2^{197} data, 2^{192} time
3. Key recovery for Wheesht-3-1-256
   - Using 2^{10} data, 2^{200} time

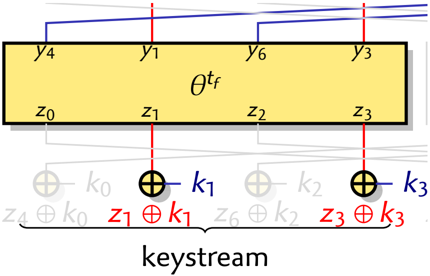
Low data complexity attack

- We target Wheesht-3-1-256, and the final θ layer
- y_6 can be computed from z_1, z_2, z_3



Low data complexity attack

- We target Wheesht-3-1-256, and the final θ layer
- y_6 can be computed from z_1, z_2, z_3



- y_6 fixed inside a message
- Keystream: $k_1 \oplus z_1$, $k_3 \oplus z_3$

1. Guess k_1, k_3
2. For each message block, compute the set of possible y_6 (iterate over z_2)
3. Verify whether the intersection is non-empty
   - Expect single k_1, k_3 candidate with 256 blocks, time 2^{200}