# *Differential Forgery Attack against LAC*

Gaëtan Leurent

Inria, France

SAC 2015

# Authenticated encryption

- Cryptography has two main objectives:

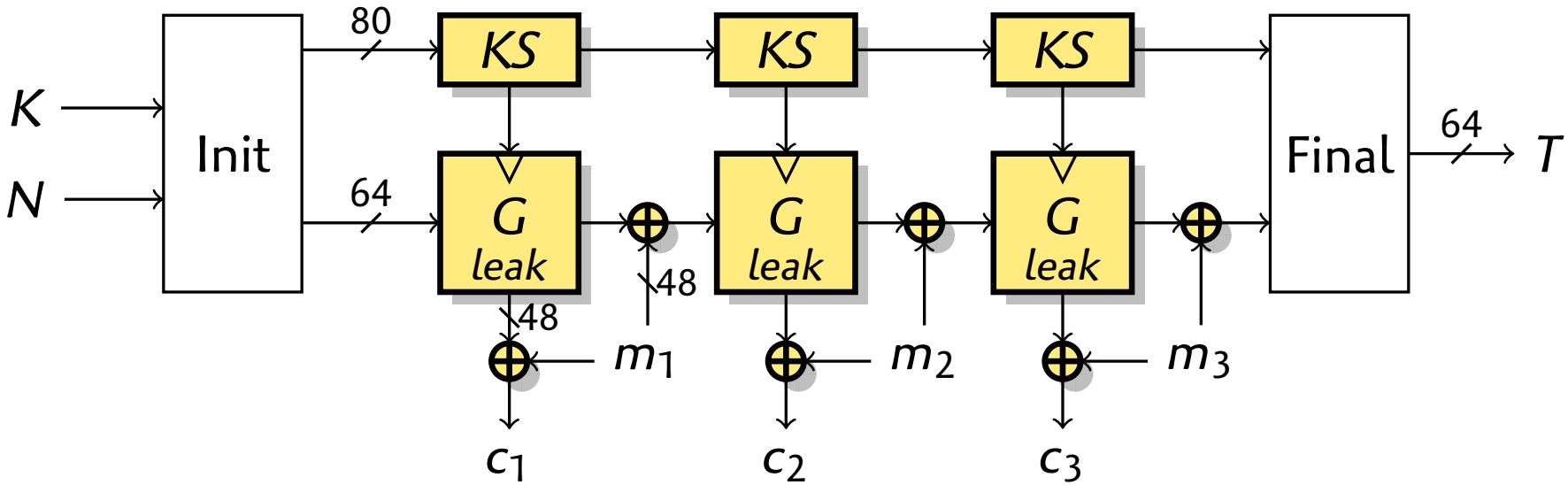
  *Confidentiality* keeping the message secret

  *Authenticity* making sure the message is authentic

- Authenticated encryption scheme provides both
  - Combines a cipher and a MAC

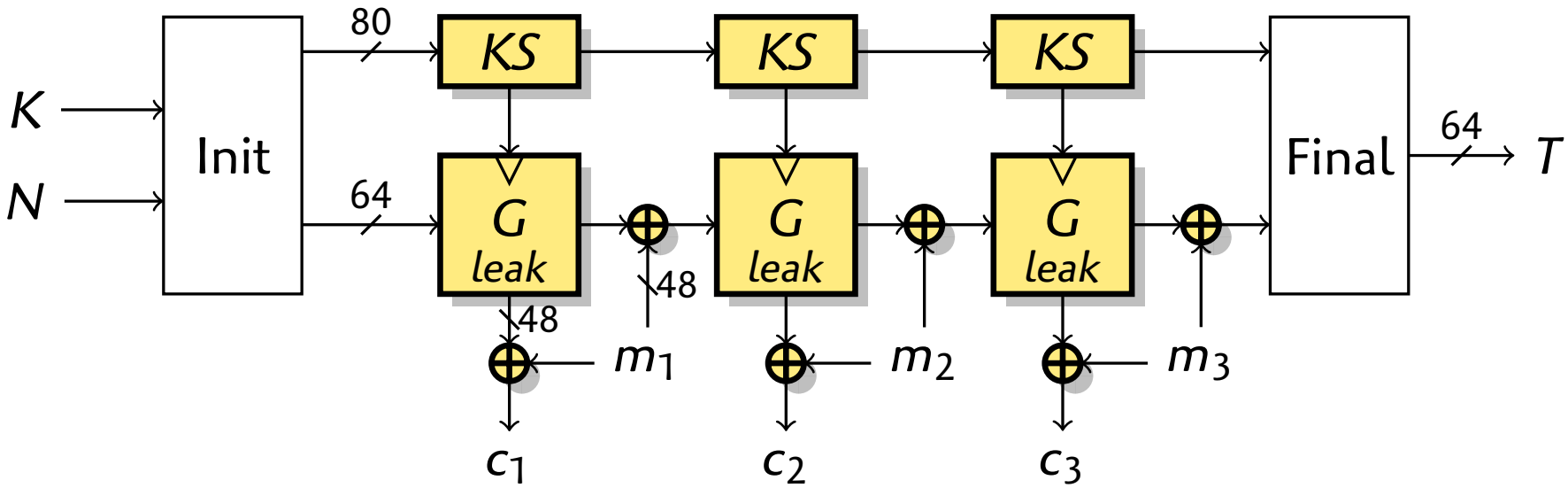
- CAESAR competition
  - Ongoing competition to design new AE schemes
  - 57 submissions in March 2014
  - 29 selected for second-round in July 2015
  - Important cryptanalysis effort

# Description of LAC




- CAESAR candidate, designed at Chinese Academy of Science
  - by Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, Jian Zhang
- Follows the structure of ALE [Bogdanov *& al.*, FSE '13]
  - $G$ based on modified LBlock (LBlock-s)
  - 80-bit key, 64-bit state, 48-bit leak

# Description of LAC

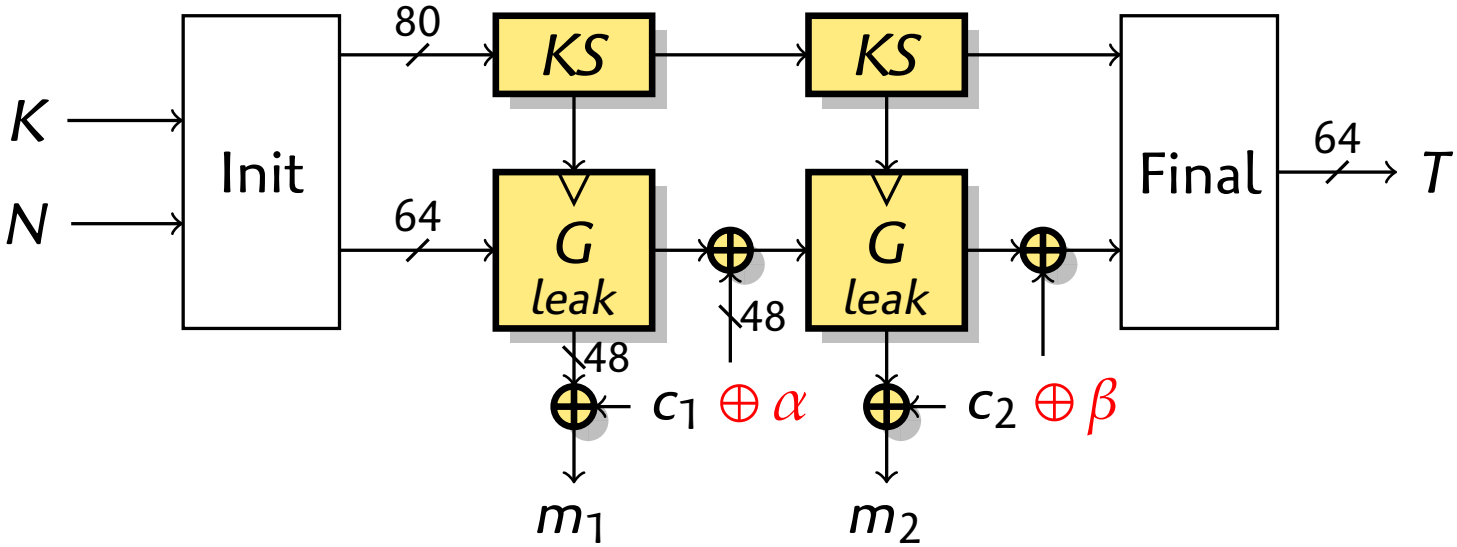



## Security claims

- Confidentiality: 80 bits
- Integrity: 64 bits

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

# Differential Forgery Attack




1. Find a differential $\alpha \rightsquigarrow \beta$ in $G$ with probability $p$
   - $p = \Pr_{k,x}\left[G_k(x \oplus \alpha) = G_k(x) \oplus \beta\right]$
2. Get a valid ciphertext $(N, c_1 \| c_2, \tau)$
3. $(N, c_1 \oplus \alpha \| c_2 \oplus \beta, \tau)$ is a forge with probability $p$

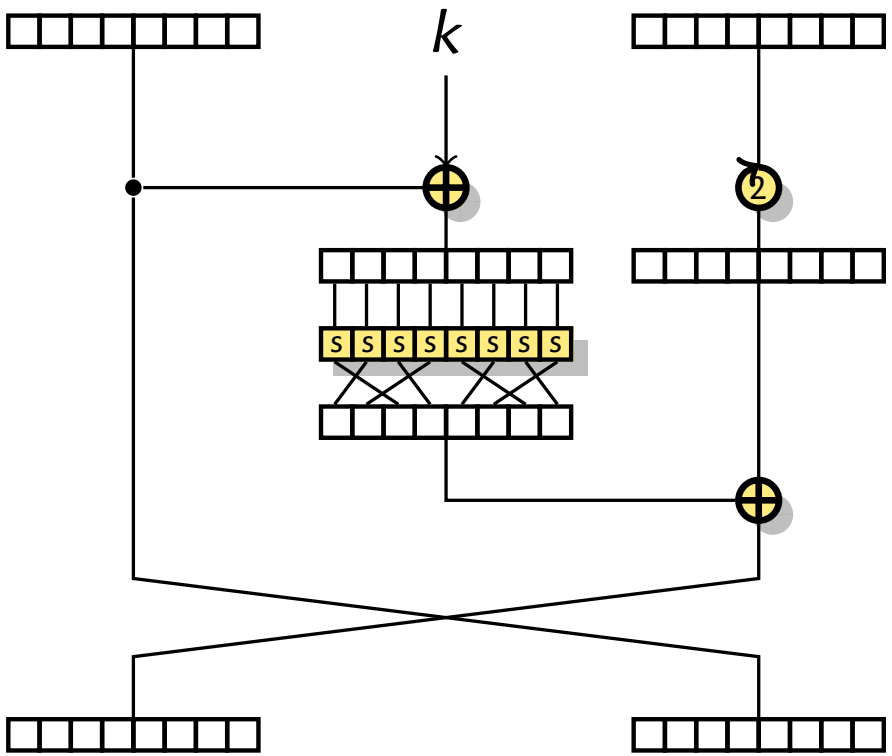
# Differentials and characteristics

*Differential* $\alpha \rightsquigarrow \beta$ $\quad p = \Pr_{k,x}[G_k(x \oplus \alpha) = G_k(x) \oplus \beta]$

*Characteristic* $\alpha_0 \rightarrow \alpha_1 \rightarrow \cdots \alpha_n = \beta$ $\quad p = \Pr_{k,x}[x'_i = x_i \oplus \alpha_i | x'_0 = x_0 \oplus \alpha]$

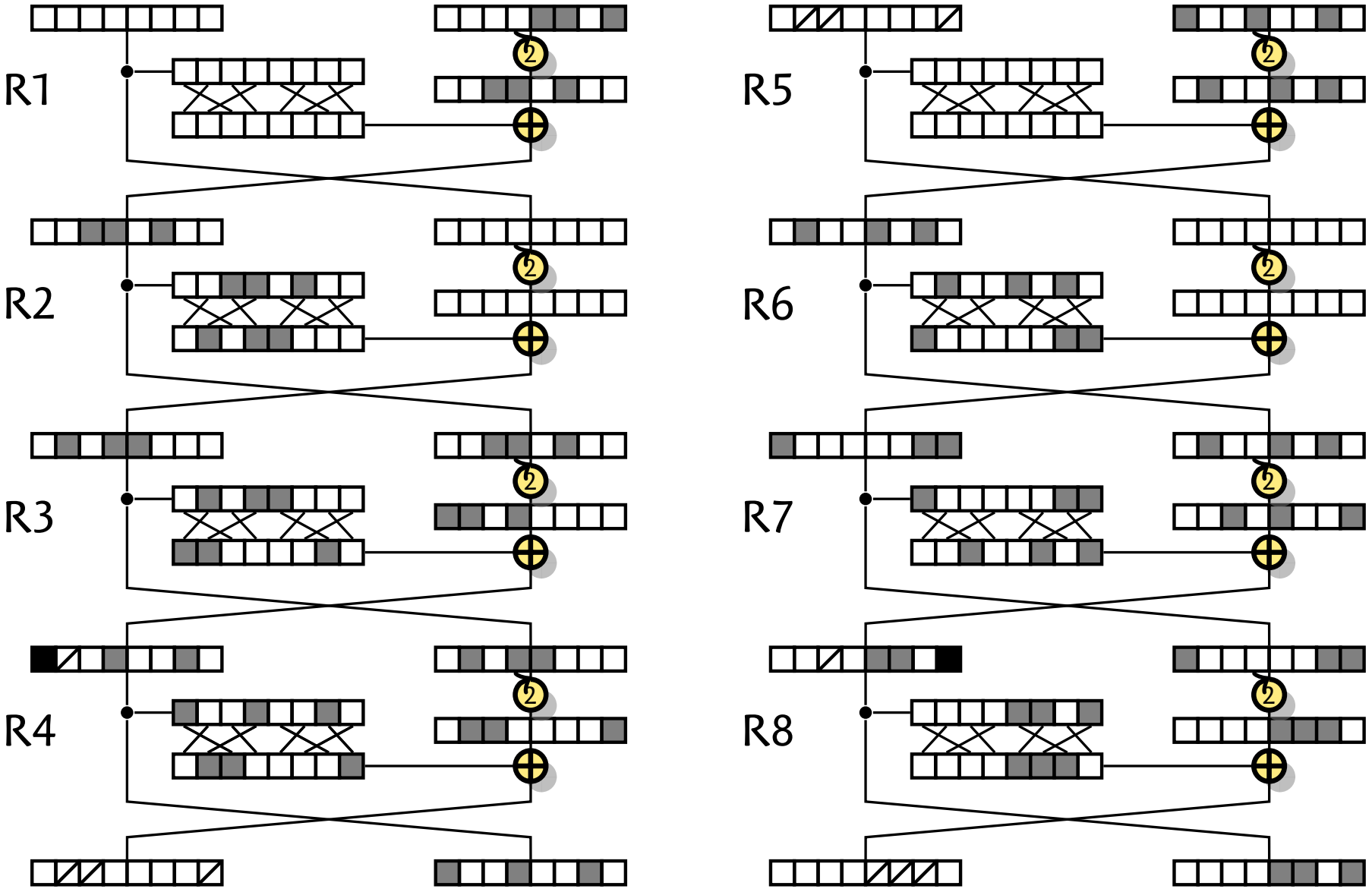
- The probability of a differential is hard to evaluate
- Common assumption:
  A single characteristic dominates the differential
  - Modifying one step leads to a significantly different characteristic
  - Security analysis bounds probability of characteristics
- Not always true for byte-wise SPN
  - Given a truncated characteristic, there are many instantiations with the same input/out differences
  - If S-Box differential table is flat, many of them are good

# Inside LBlock-s

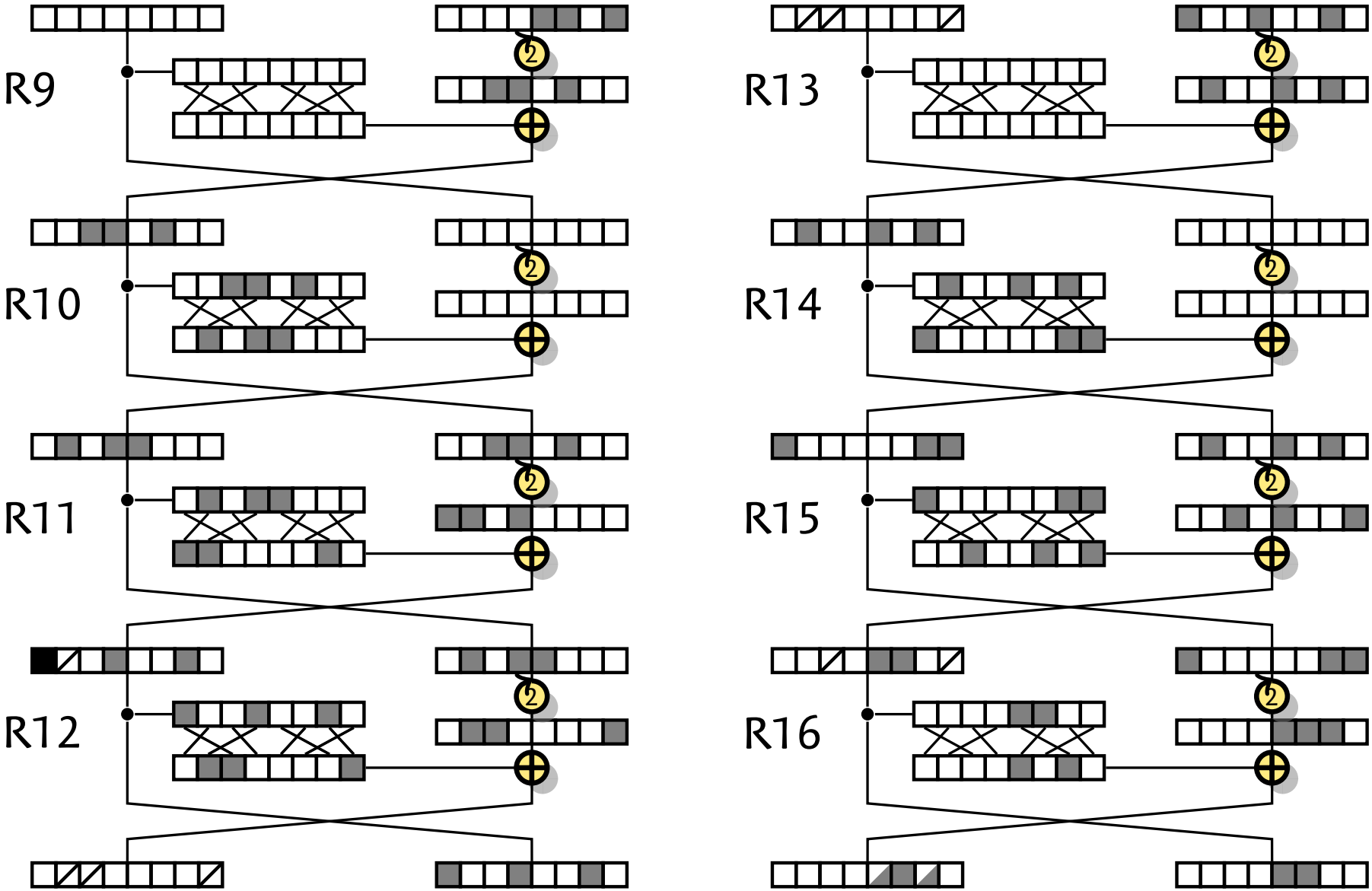



- Feistel structure
  - Nibble-oriented (4-bit words)
- 16 rounds
  - Key addition
  - Nibble S-box
  - Nibble permutation
- Best characteristics
  - 35 active S-boxes
  - $\delta(S) = 2^{-2}$
  - Proba $\leq 2^{-70}$

# Truncated differential characteristics



# Truncated differential characteristics



# Differentials and characteristics

*Differential* $\alpha \rightsquigarrow \beta$ $\quad p = \Pr_{k,x}[G_k(x \oplus \alpha) = G_k(x) \oplus \beta]$

*Characteristic* $\alpha_0 \rightarrow \alpha_1 \rightarrow \cdots \alpha_n = \beta$ $\quad p = \Pr_{k,x}[x'_i = x_i \oplus \alpha_i | x'_0 = x_0 \oplus \alpha]$

- The probability of a differential is hard to evaluate
- Common assumption:
  A single characteristic dominates the differential
  - Modifying one step leads to a significantly different characteristic
  - Security analysis bounds probability of characteristics
- Not always true for byte-wise SPN
  - Given a truncated characteristic, there are many instantiations with the same input/out differences
  - If S-Box differential table is flat, many of them are good

# Estimating of the probability of differentials

- For security proofs: upper bounds on the probability of differentials
  - Few results known...
  - Notable exception: AES [Keliher & Sui]
- For cryptanalysis: lower bound on the probability of differentials
  - Sum characteristics with the same input/output differences
  - Recent work: using MILP to find characteristics [Sun & al.]
- Our approach: use a truncated characteristic
  - Consider the set of all characteristics following the same truncated characteristic
  - Fix input/output differences, vary internal differences
  - Large number of characteristics, many with good probability

# Computing the 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 $D$
- Compute the probabilities of all 1-round transitions following $D$

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

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

# Computing the 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 $D$
- Compute the probabilities of all 1-round transitions following $D$

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

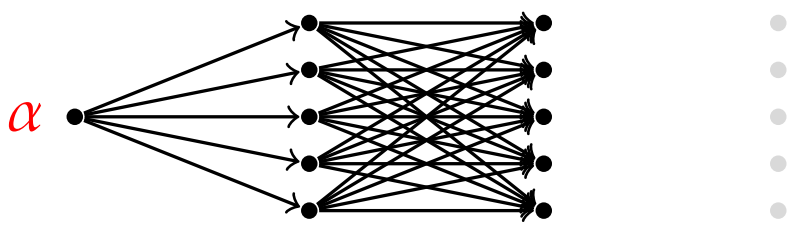
1. Compute $\Pr\left[D_1 : \alpha \rightsquigarrow x\right]$ for all valid $x$
2. Compute $\Pr\left[D_i : \alpha \rightsquigarrow x\right]$ for all valid $x$ iteratively:
   $\Pr\left[D_i : \alpha \rightsquigarrow x\right] = \sum_{x'} \Pr\left[D_{i-1} : \alpha \rightsquigarrow x'\right] \cdot \Pr[x'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

# Computing the 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 $D$
- Compute the probabilities of all 1-round transitions following $D$

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

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

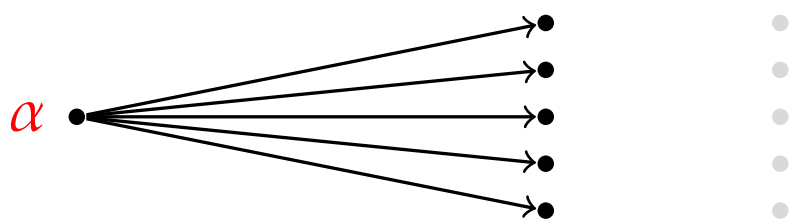


# Computing the aggregation

- 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 $D$
- Compute the probabilities of all 1-round transitions following $D$

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

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

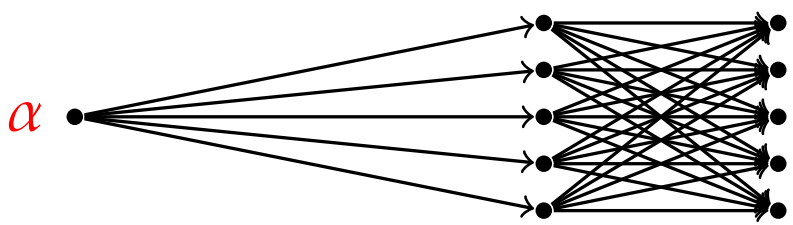


# Computing the aggregation

- 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 $D$
- Compute the probabilities of all 1-round transitions following $D$

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

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

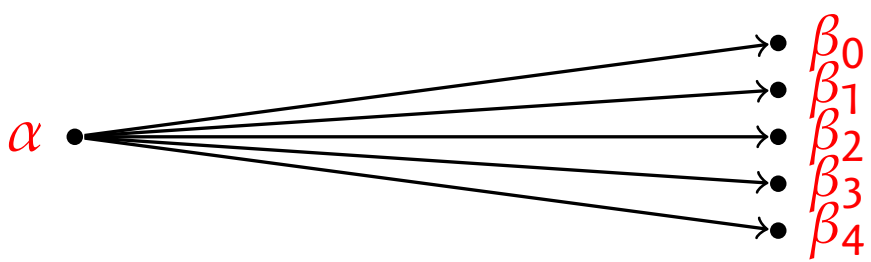


# Computing the aggregation

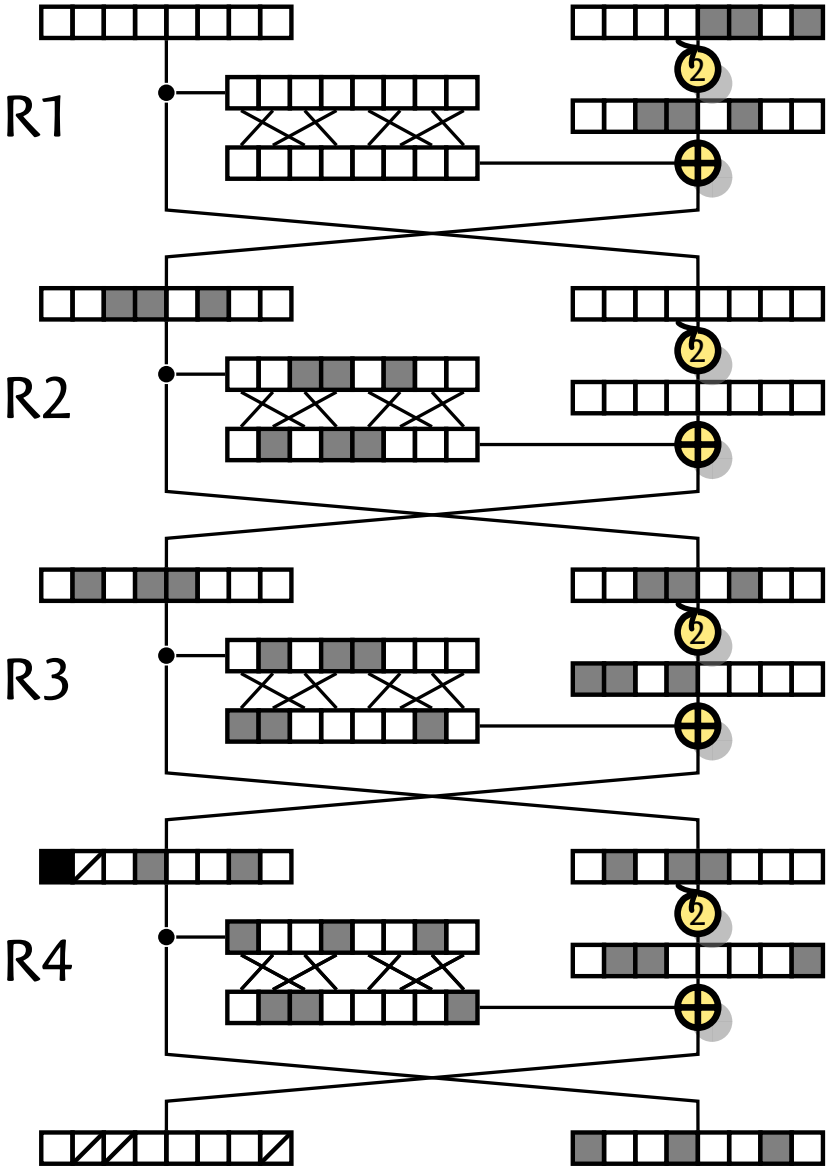
- Consider a fixed truncated characteristic D
  - $D_i$ is the first $i$ rounds of $D$
  - $\Pr\left[D : \alpha \rightsquigarrow \beta\right]$ probability that $\alpha \rightsquigarrow \beta$ following $D$
- Compute the probabilities of all 1-round transitions following $D$

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

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



# Application to LAC



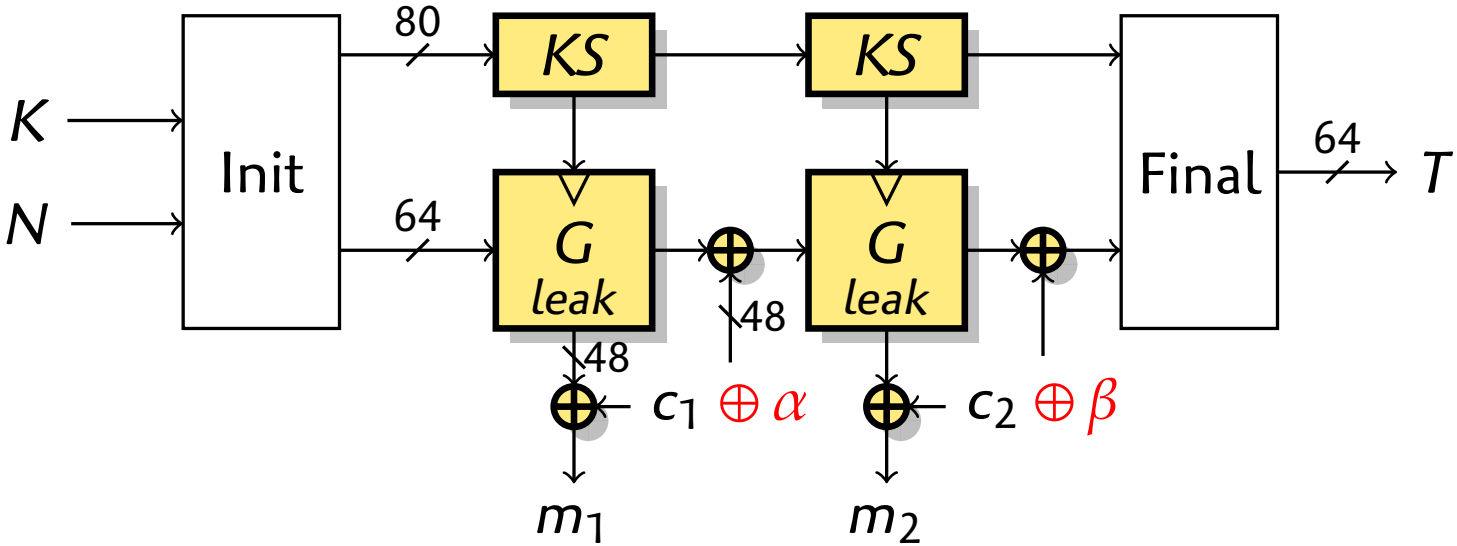

- At most 6 active nibbles
  - Storage $2^{24}$
- At most 3 active S-Boxes
  - At most $2^9$ transitions
  - Time $16 \cdot 2^{24} \cdot 2^9 = 2^{37}$

## *Results*

Best differential found: $p \geq 2^{-61.52}$

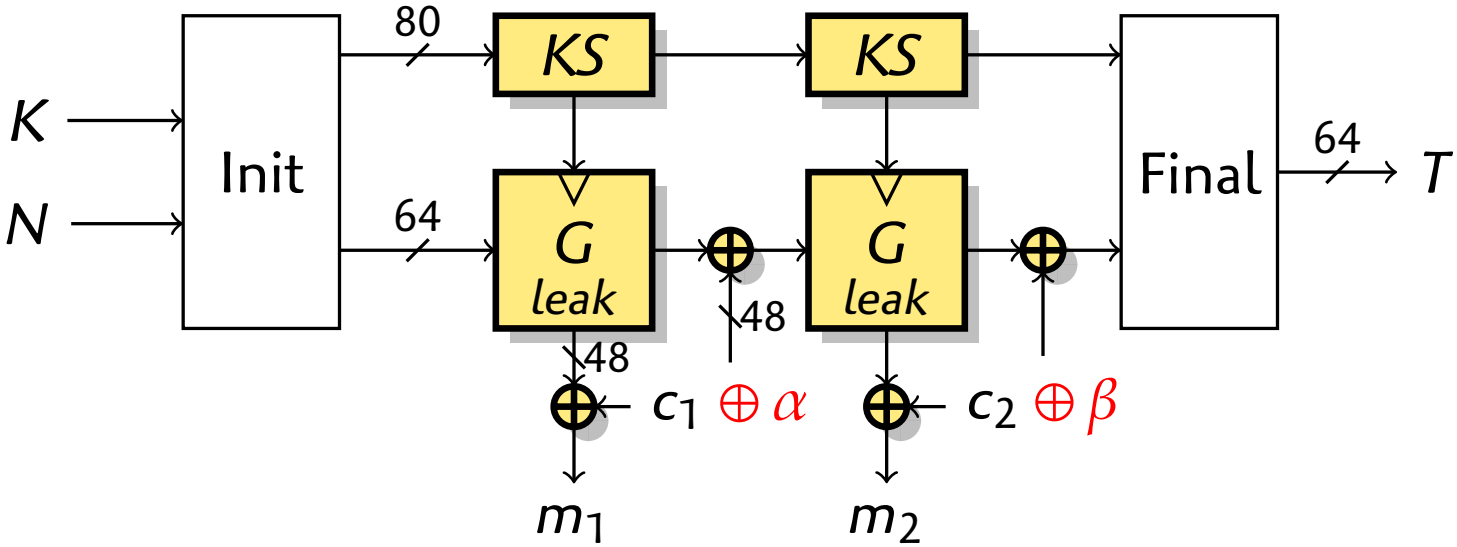
- Collection of 302116704 characteristics
- 17512 differentials with $p > 2^{-64}$

# Differential Forgery Attack




1. Get a valid ciphertext $(N, c_1 \| c_2, \tau)$
2. $(N, c_1 \oplus \alpha \| c_2 \oplus \beta, \tau)$ is a forge with probability $\geq 2^{-61.52}$
   - Corresponding plaintext: $m_1 \oplus \alpha \| m_2 \oplus \beta$, because the leak is not affected

# Differential Forgery Attack




## Limitations

- Probability slightly higher than security claims ($2^{-61.52}$ vs. $2^{-64}$)
- Need new data to repeat... (cannot increase success probability)
  - Or use several differentials
  - Limit to $2^{40}$ data per key

# Conclusion

- Lower bound on the probability of some differential
  - Collection of characteristics following a truncated characteristic
  - Good estimate of the probability of a differential
- Breaks the security claims of LAC
  - $\Pr[\text{characteristic}] \leq 2^{-70}$
  - $\Pr[\text{best differential}] \geq 2^{-61.52}$
- Designers should check if applicable

# Thanks

Questions?