Can a Differential Attack Work for an \textit{Arbitrarily Large} Number of Rounds?

\textbf{Nicolas T. Courtois}  
University College London, UK

\textbf{Jean-Jacques Quisquater}  
Université Catholique de Louvain, Belgium
Roadmap

1. Differential Cryptanalysis (DC)
   - aren’t all ciphers already protected?
   - can we beat the defenses against DC?

2. DC and Markov Cipher Requirement

3. T-310 block cipher

4. Linear Cryptanalysis (LC)

5. Generalized Linear Cryptanalysis (GLC) ==
   - Hidden polynomial invariants ==
   - Hidden invariant affine spaces

6. Combination of DC and GLC:
   Main Result – Non-Markovian Proof of Concept
Block Cipher Invariants

Dr. Nicolas T. Courtois

People, Problems, and Proofs

blog.bettercrypto.com

UNIVERSITY CIPHER CHAMPION
March 2013
Cryptanalysis
=def=Making the impossible possible.

How? the Unexpected and the Unlikely Happens
LinkedIn – Please Join!

Your Groups (51)

- Code Breakers: Members (712)
- IACR Cryptographers: Members (1)
Cryptanalysis
vs. ciphers with a
large number of rounds
[most block ciphers]

can this property be defeated?
Defences in Place:

Nyberg & Knudsen: Provable Security Against Differential Cryptanalysis @Crypto’92.

Fact:
ciphers are studied for avoiding high probability iterative differentials
• e.g. CHAM cipher@ ICISC 2019
• same for every cipher ever made!
Defences in Place:

Provable Security Against Differential Cryptanalysis @Crypto’92.

avoiding high probability iterative differentials

• same for every cipher ever made!
• Nash Postulate [1955 letter to NSA]:
  • the computation cost should increase exponentially...

this paper:
DC does not degrade exponentially!
One Method: Complexity Reduction

Goal: break XXX rounds for the price of X rounds [Courtois 2011]
Examples: slide attacks, reflection attacks, fixed point attacks, cycling attacks etc.

[Black Box] Complexity Reduction

GOST block cipher: 40 ways to reduce the effort, cf. eprint/2011/626.
- Given $2^X$ KP for the full 32-round GOST.
- Obtain $Y$ KP for 8 rounds of GOST.

KeeLoq block cipher: Courtois, Bard, Wagner @FSE2008:
- Given $2^{16}$ KP for the full 528-round KeeLoq
- Obtain 2 KP for 64 rounds of KeeLoq.

This paper: a new way of dealing with TOO many rounds…
Hiding Differentials?

Peyrin-Wang@Crypto 2020 summarizes old 1990s research on this topic: ``hiding differentials'' was claimed very difficult…

This paper:

• we do not “hide” high probability differentials
  – we hide low probability differentials!
    • the probability can be as low as we want

• provable security fails or does NOT scale:
  – nothing special is detected locally!
  – global long-term property for a large number of rounds
Differential Cryptanalysis (DC)
“Official” History

• Differential Cryptanalysis: Biham-Shamir [1991]
[...] IBM have agreed with the NSA that the design criteria of DES should not be made public.
One form of DC was known in 1973!

Durch die Festlegung von Z wird die kryptologische Qualität des Chiffriermethode beeinflußt. Es wurde davon ausgegangen, daß eine Funktion Z kryptologisch geeignet ist, wenn sie folgende Forderungen erfüllt:

1. \( \left\{ x = (x_1, x_2, \ldots, x_6) \in \{0, 1\}^6 \mid z(x) = 0 \right\} = 2^5 \)

2. \( \left\{ x = (x_1, x_2, \ldots, x_6) \in \{0, 1\}^6 \mid z(x) = 0, \sum_{i=1}^{6} x_i = +3 \right\} \approx \left( \frac{6}{-1} \right) \cdot \frac{1}{2} \)

3. \( \left\{ x = (x_1, \ldots, x_6) \in \{0, 1\}^6 \mid z(x_1, x_2, \ldots, x_5, x_6) = z(x_1, \ldots, x_5, 0, \ldots, x_6) \right\} \approx \frac{2^5}{2} \)
90% of Enigma Rotors 1938-1945

- 5x less invariant differentials than RP.
  - deliberate property intended by the manufacturer
  - also true in Russian Fialka cipher machines.

| rotor name    | Nb | code | dates | $|\text{ImS}(R)|$ | $|\text{Ent}(R)|$ | $|\text{Imk}|$ | possible differentials $k \rightarrow k$ |
|---------------|----|------|-------|----------------|----------------|---------|-----------------------------|
| Army I        | 1  | EKM  | 1930  | 17             | 3.95           | 10      | 2,3,6,7,9,11,12,13          |
| Army II       | 2  | AJD  | 1930  | 19             | 4.16           | 17      | 8,9,10,11                  |
| Army III      | 3  | BDF  | 1930  | 20             | 4.21           | 14      | 2,3,5,8,10,13              |
| Army IV       | 4  | ESO  | 1938  | 23             | 4.47           | 19      | 5,8,12                     |
| Army V        | 5  | VZB  | 1938  | 24             | 4.55           | 23      | 5                          |
| Army VI       | 6  | JPG  | 1938  | 24             | 4.55           | 22      | 6,13                       |
| Army VII      | 7  | NZJ  | 1938  | 23             | 4.47           | 19      | 3,5,8                      |
| Army VIII     | 8  | FKQ  | 1939  | 24             | 4.55           | 21      | 4,7                        |
| G-310 Abwehr/G 316.58 I | 28 | DMT  | 193X  | 21             | 4.32           | 17      | 5,6,7,8                    |
| G-310 Abwehr/G 316.58 II | 29 | HQZ  | 193X  | 24             | 4.55           | 22      | 8,13                       |
| G-310 Abwehr/G 316.58 III | 30 | UQN  | 193X  | 24             | 4.55           | 21      | 5,10                       |
T-310 – Slight Problem

- 1 bit subkey
- Permutation with 28 bits dropped
- 1 bit derived from subkey
- 1 bit from IV
- 27 bits

Diagram shows a process involving a T function and permutations, with key and input bits being processed through various transformations.
T-310: 27 bits used only

- 9 bits not used!

=> obvious vanishing differentials + further consequences

Table 2. Missing bits for some keys vulnerable to related-key differential attacks

<table>
<thead>
<tr>
<th>LZS nb</th>
<th>bits which are not used in $P(j)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>716</td>
<td>1, 2, 10, 14, 15, 18, 22, 27, 35</td>
</tr>
<tr>
<td>722</td>
<td>2, 3, 6, 10, 13, 19, 23, 26, 31</td>
</tr>
</tbody>
</table>
Higher Order
DC
Bugs or Backdoors?

Computing HO Differentials for All Orders

\[ 2^{(1)} = L + e_4 + e_3 e_4 + e_3 e_6 + e_4 e_5 + e_2 e_3 e_4 + e_2 e_3 e_5 + e_2 e_5 e_6 + e_2 e_3 e_4 e_5 + e_3 e_4 e_5 e_6 \]

\[ 2^{(2)} = e_3 + e_5 + e_3 e_6 + e_4 e_6 + e_1 e_3 e_4 + e_1 e_3 e_5 + e_1 e_5 e_6 + e_3 e_4 e_6 + e_1 e_3 e_4 e_5 \]

\[ 2^{(134)} = L + e_2 + e_2 e_5 + e_5 e_6 \]

\[ 2^{(135)} = e_2 + e_2 e_4 + e_4 e_6 \]

\[ 2^{(136)} = L + e_4 e_5 \]

\[ 2^{(1246)} = 0 \]

\[ 2^{(1256)} = L \]

\[ 2^{(1345)} = e_2 + e_6 \]

fast points!
Special/Peculiar DC
“Courtois Dark Side” Attack on MiFare Classic

Cf. eprint.iacr.org/2009/137. Basic Facts:
It is a multiple differential attack.

Simultaneous differences on 51 bits of the state of the cipher.
A VERY STRONG property(!).

In most ciphers this will NEVER happen.
Low probability. Probabilities multiply. Exponential decay.
Markov Ciphers

Lai, Massey, and Murphy @Eurocrypt 1991

page 24: in a Markov cipher
``every differential will be roughly equally likely”
after sufficiently many rounds

This paper:
• Non-Markovian, some differentials live forever.
• Claimed not detectable if we dispose of a limited computing power and a limited quantity of data:
Markov Property Violation

- Non-Markovian anomalous propagation
- the attack complexity is bounded by a constant
- it does NOT degrade exponentially as the number of rounds grows.
- claimed hard to detect [a small subspace, otherwise seems normal].

Deep violation of a big theory:
Kaisa Nyberg, Lars Ramkilde Knudsen:
Provable Security Against Differential Cryptanalysis@Crypto'92

A cipher is NOT secure just because it avoids high probability iterative differentials. Fails for non-Markov cipher.
Similar Result:

Leander, Abdelraheem, AlKhzaimi, Zenner:

Our attack is in many ways better:
• we work on a real-life historical cipher
• single differentials on full state, not truncated
• works for any key
• works in spite of the presence of round constants
Similar Result:

Leander, Abdelraheem, AlKhzaimi, Zenner:

Our attack is in many ways better:
• we work on a real-life historical cipher
• single differentials on full state, not truncated
• works for any key
• works in spite of the presence of round constants
Question:
Why researchers have found so few attacks on block ciphers?
Question:
Why researchers have found so few attacks on block ciphers?

“mystified by complexity”
lack of working examples: how a NL attack actually looks like??
**Cryptanalysis**

=def=Making the impossible possible.

How? The Unexpected and the Unlikely Happens
Invariants
and product attacks

How? two very large polynomials are simply equal
“Only those who attempt the absurd will achieve the impossible.”
-- M.C. Escher
Non-Markovian DC
- this paper –
becomes eventually possible…

How?

$P > 0$ !
Compromise of Rotor Machine Crypto

• USS Pueblo / North Korea
  Jan 1968
US/NATO crypto broken

Russia broke the NATO KW-7 cipher machine:

allowed Soviets to “read millions” of US messages [1989, Washington Post]
1970s

Modern block ciphers are born. In which country?? Who knows…
Our Sources

Communist Crypto Archives
MfS Abteilung 11 = ZCO = Zentrales Chiffrierorgan der DDR
Block Cipher Invariants

Nicolas T. Courtois

Our Sources

BStU = Stasi Records Agency
More details:


Eastern Bloc ciphers: a LOT more complex…
East German T-310

- 240 bits long-term secret
- Has a physical RNG => IV
- "quasi-absolute security" [1973-1990]
- 90 bits only!

T-310
Contracting Feistel [1970s Eastern Germany!]

Block Cipher Invariants
Linear Cryptanalysis (LC)
LC “Official” History

- Shamir Paper [1985]…….. early LC
LC “Official” History

- Linear Cryptanalysis: Gilbert and Matsui [1992-93]
### Definition 3.1-1

\[ \Delta^3_\alpha = 2^{n-1} - \| g(x) \| (\alpha, x) \| \forall \alpha \in 0,2^{n-1}. \]

\[ \| g \| = \sum g(x) \]

\[ (\alpha, x) = \sum_{i=1}^{n} \alpha_i \cdot x_i \]

### Ergebnisse:

#### Tabelle 3.1-2

<table>
<thead>
<tr>
<th>( \alpha )</th>
<th>( \Delta^2_\alpha )</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0 0 0 0</td>
<td>32 0</td>
<td>32</td>
</tr>
<tr>
<td>0 0 0 0 0 1</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>0 0 0 0 1 0</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>0 0 0 1 0 0</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>0 0 1 0 0 0</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>0 0 1 0 0 1</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>0 0 1 0 1 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>0 0 1 1 0 0</td>
<td>2</td>
<td>34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \alpha )</th>
<th>( \Delta^2_\alpha )</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>L 0 0 0 0 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>L 0 0 0 0 1</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>L 0 0 0 1 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>L 0 0 1 0 0</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>L 0 0 1 0 1</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>L 0 0 1 1 0</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>L 0 0 1 1 1</td>
<td>4</td>
<td>36</td>
</tr>
<tr>
<td>L 0 1 0 0 0</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>L 0 1 0 0 1</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>L 0 1 0 1 0</td>
<td>2</td>
<td>34</td>
</tr>
</tbody>
</table>
Inside T-310 Round

\( \Phi \)
Definition 3.1-1

\[ \Delta^3_\alpha = 2^{n-1} - \| g(x) + (\alpha, x) \| \quad \forall \alpha \in 0, 2^{n-1}, \]

\[ \| g \| = \sum \sum g(x) \]

\[ (\alpha, x) = \sum_{i=1}^m \alpha_i x_i \]

Geheime Verschlüsselsache
Mfs -020-Nr.: XI/433/76/BL 18

Beispiel:

Sei \( t \) die Anzahl der Übereinstimmungen der Funktionswerte von \( f \).

Tabelle 3.1-2

<table>
<thead>
<tr>
<th>( \alpha )</th>
<th>( \Delta^2_\alpha )</th>
<th>( t )</th>
<th></th>
<th>( \alpha )</th>
<th>( \Delta^2_\alpha )</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000000</td>
<td>320</td>
<td>32</td>
<td>L000000</td>
<td>0</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>000000L</td>
<td>2</td>
<td>34</td>
<td>L00000L</td>
<td>6</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>00000LL</td>
<td>-4</td>
<td>28</td>
<td>L0000LL</td>
<td>0</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>0000LLL</td>
<td>6</td>
<td>38</td>
<td>L000LLL</td>
<td>6</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>000L000</td>
<td>-4</td>
<td>28</td>
<td>L00L000</td>
<td>-4</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>000L00L</td>
<td>-2</td>
<td>30</td>
<td>L00L00L</td>
<td>2</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>000L0LL</td>
<td>0</td>
<td>32</td>
<td>L00L0LL</td>
<td>4</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>000LLLL</td>
<td>2</td>
<td>34</td>
<td>L00LLL</td>
<td>2</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>000LLLL</td>
<td>2</td>
<td>34</td>
<td>L00L</td>
<td>0</td>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>
Contracting Feistel [1970s Eastern Germany!]

1 round of $T-310$
How to Backdoor T-310 [Cryptologia 42@2018]

omit just 1 out of 40 conditions:

ciphertext-only attacks!

bad long-term key
Generalized Linear Cryptanalysis (GLC)

[Harpes, Kramer and Massey, Eurocrypt’95]
Scope

We study how an encryption function $\varphi$ of a block cipher acts on polynomials.

Stop, this is extremely complicated???
Main Problem:
Two polynomials $P \Rightarrow Q$.

$P(x_1, \ldots)$

$Q(y_1, \ldots)$

is $P = Q$ possible??

“Invariant Theory” [Hilbert]: set of all invariants for any block cipher forms a [graded] finitely generated [polynomial] ring. A+B; A*B
Connecting Non-Linear Approxs.

Black-Box Approach [Popular]

Non-linear functions.

\[ F(x_1,\ldots) \]
\[ G(x_1,\ldots) \quad H(y_1,\ldots) \]
\[ I(z_1,\ldots) \]
Fake News

[Knudsen and Robshaw, EuroCrypt’96

“one-round approximations that are non-linear [...] cannot be joined together”...]

At Crypto 2004 Courtois shows that GLC is in fact possible for Feistel schemes!
BLC better than LC for DES

\[ L_0[3, 8, 14, 25] \oplus L_0[3] R_0[16, 17, 20] \oplus R_0[17] \oplus \]
\[ L_{11}[3, 8, 14, 25] \oplus L_{11}[3] R_{11}[16, 17, 20] \oplus R_{11}[17] = \]

Better than the best existing linear attack of Matsui for 3, 7, 11, 15, … rounds.

Ex: LC 11 rounds: \( \frac{1}{2} \pm 1.91 \cdot 2^{-16} \)

BLC 11 rounds: \( \frac{1}{2} \pm 1.2 \cdot 2^{-15} \)
Phase Transition =def= Making the impossible possible.

How?
Use polynomials of higher degree
Strong Attacks on T-310


• When $P$ degree grows, attacks become a LOT easier.

• The more polynomials you multiply, the better.
Better Is Enemy of Good!

DES = Courtois @Crypto 2004:

\[
\frac{1}{2} \pm 1.91 \cdot 2^{-16} \quad P \text{ deg 1}
\]

\[
\frac{1}{2} \pm 1.2 \cdot 2^{-15} \quad P \text{ deg 2}
\]

\[
\text{proba}=1.0 \quad P \text{ deg 10}
\]
White Box Cryptanalysis

[Courtois 2018]

$P(\text{inputs}) = P(\text{outputs})$ with probability 1.

formal equality of 2 polynomials.
2. Closed Loops*

* informally, walks on cycles with simple polynomials, see our paper @ICISC 2019
Closed Loops - GOST

highly vulnerable!
ICISC 2019: we generalized the concept of closed loops
sets of bits \Rightarrow sets of cycles on polynomials
This Paper:

we generalize the concept of closed loops
sets of bits $= \Rightarrow$ sets of cycles on polynomials

Non-Markovian DC - ICISC 2020

constructing invariants

annihilation
$g2^*(M+Q) = 0$

4 terms are gone!
Imperfect Transitions:

we allow

addition of arbitrary non-linear functions

=> annihilated later

\[ Z_1() \times L_2() = 0 \]

for any input
Big Winner

“product attack”

=we multiply Boolean polynomials=
Impossible?

“Only those who attempt the absurd will achieve the impossible.”

-- M. C. Escher
Block Cipher Invariants

cycles - attack on T-310
(ICISC 2019 Thm. 6.2.)

\[(Y+f)\times B\times C\times D = 0\]
This Paper: Improve Thm. 5.5.  
In eprint/2018/1242 page 18.

\[
\mathcal{P} = ABCDEFGH
\]
is invariant if and only if this polynomial vanishes:

\[
FE = BCDFGH \cdot ((Y + E)W(\cdot) + AY(\cdot))
\]

Can a polynomial with 16 variables with 2 very complex Boolean functions just disappear?
Combined DC and GLC
– this paper

An invariant attack of order 2:
two encryptions.

Main idea:
there is an anomalous differential
which violates the Markov property.
• not in general, just in some cases
  [so hard to detect!]
Main Theorem

IF

\[
\begin{align*}
\{D(2), D(3)\} &= \{6 \cdot 4, 7 \cdot 4\} \\
\{D(6), D(7)\} &= \{2 \cdot 4, 3 \cdot 4\}
\end{align*}
\]

\[
\begin{align*}
A &\equiv (m+i) \quad \text{which is bits 24, 28} \\
B &\equiv (n+j) \quad \text{which is bits 23, 27} \\
C &\equiv (o+k) \quad \text{which is bits 22, 26} \\
D &\equiv (p+l) \quad \text{which is bits 21, 25} \\
E &\equiv (O+y) \quad \text{which is bits 8, 12} \\
F &\equiv (P+z) \quad \text{which is bits 7, 11} \\
G &\equiv (Q+M) \quad \text{which is bits 6, 10} \\
H &\equiv (R+N) \quad \text{which is bits 5, 9.}
\end{align*}
\]
Main Theorem

IF

AND

THEN

1..64 hard DC
Main Theorem

IF

AND

inputs $25, 10, 27, 21, 6, 23$ of $Y$

$Z(a + d)(b + e)(c + f) = 0$

inputs $5, 22, 7, 9, 26, 11$ of $W$

THEN

1..64 hard DC

64..$\infty$ easy!

+ product pty!
Experiments – 3 different Boolean Functions

Attack works with $P = 2^{-8}$ for any Boolean function.

- **typical**

<table>
<thead>
<tr>
<th>rounds</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>proba</td>
<td>$2^{-2.40}$</td>
<td>$2^{-4.82}$</td>
<td>$2^{-6.74}$</td>
<td>$2^{-7.71}$</td>
<td>$2^{-7.95}$</td>
<td>$2^{-7.99}$</td>
<td>$2^{-8.00}$</td>
<td>$2^{-8.00}$</td>
</tr>
</tbody>
</table>

- **very weak**

<table>
<thead>
<tr>
<th>rounds</th>
<th>8</th>
<th>32</th>
<th>128</th>
<th>2048</th>
</tr>
</thead>
<tbody>
<tr>
<td>proba</td>
<td>$2^{-1.1}$</td>
<td>$2^{-3.0}$</td>
<td>$2^{-5.5}$</td>
<td>$2^{-7.7}$</td>
</tr>
</tbody>
</table>

- **Stronger**

<table>
<thead>
<tr>
<th>rounds</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>proba</td>
<td>$2^{-4.53}$</td>
<td>$2^{-7.51}$</td>
<td>$2^{-7.98}$</td>
<td>$2^{-8.00}$</td>
<td>$2^{-8.00}$</td>
<td>$2^{-8.00}$</td>
<td>$2^{-8.00}$</td>
<td>$2^{-8.00}$</td>
</tr>
</tbody>
</table>
Experiments – 3 different Boolean Functions

Attack works with $P = 2^{-8}$ for any Boolean function.

- typical

<table>
<thead>
<tr>
<th>rounds</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>proba</td>
<td>2(^{-2.40})</td>
<td>2(^{-4.82})</td>
<td>2(^{-6.74})</td>
<td>2(^{-7.71})</td>
<td>2(^{-7.95})</td>
<td>2(^{-7.99})</td>
<td>2(^{-8.00})</td>
<td>2(^{-8.00})</td>
</tr>
</tbody>
</table>

- very weak

- Stronger

<table>
<thead>
<tr>
<th>rounds</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>proba</td>
<td>2(^{-4.53})</td>
<td>2(^{-7.51})</td>
<td>2(^{-7.98})</td>
<td>2(^{-8.00})</td>
<td>2(^{-8.00})</td>
<td>2(^{-8.00})</td>
<td>2(^{-8.00})</td>
<td>2(^{-8.00})</td>
</tr>
</tbody>
</table>

- the curve initially DOES decrease exponentially,
  HENCE expected HARD to detect [like a backdoor]
Conclusion

Nyberg-Knudsen @Crypto’92: Provable Security Against Differential Cryptanalysis.

=> ciphers are studied for avoiding high probability iterative differentials

Not sufficient.
=> all ciphers should be TESTED for long-term violations of Markov cipher property
  • e.g. CHAM cipher of ICISC 2019