Boolean Functions and Resistance against NL Polynomial Invariant Attacks
[on Some Block Ciphers]

Nicolas T. Courtois
University College London, UK
Roadmap

• Non-Linear Cryptanalysis
  – Polynomial Invariants and Backdoors

• Can “strong” Boolean functions help to secure block ciphers against polynomial invariant attacks?
  – “product attack”
  – attacks based annihilators =>
    • potentially some attacks are HARD to avoid
Carlet Meta-Theorem:

“Almost all Boolean functions do not have any property we would wish them to have”

Partial Opposite [today]

Up to 15% of Boolean functions **DO** have the properties we need to make our NL attack work.

- Well, at least for **some** block ciphers…
- Proof of concept for T-310 for DES.
Question:
Why researchers have found so few attacks on block ciphers?

LC = small HW words on 64 bits.
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??
Scope

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

Stop, this is extremely complicated???
Claim: Finding new attacks on block ciphers is EASY and FUN
Block Cipher Invariants

Code Breakers - LinkedIn

LinkedIn Account Type: Basic

Your Groups (51) Reorder »

- Code Breakers Members (712)

- IACR Cryptographers
Cryptanalysis

=def= Making the impossible possible.

How? two very large polynomials with 16+ vars are simply equal
inspired by the master of impossible:

-- M. C. Escher
Algebraic Attacks on Block Ciphers

Nicolas T. Courtois

@eprint/2018/1242

Big Winner

“product attack”

a product of Boolean polynomials.

Claimed extremely powerful.

Why?
Definition

We say that $P \Rightarrow Q$ for $1R$ if

$P(\text{inputs}) = Q(\text{outputs})$

with proba $=1$, i.e. for every input
Another notation:

\[ P = Q^\varphi \]

\[ \Leftrightarrow \quad P \Rightarrow Q \text{ for } 1R \]

\[ \Leftrightarrow \quad P(\text{inputs}) = Q(\text{outputs}) \]

for any input with \( Pr=1 \)

\( \varphi \) is 1 round of encryption
Main Problem:
Two polynomials $P \Rightarrow Q$.

Is $P = Q$ possible??

“Invariant Theory” [Hilbert]: set of all invariants for any block cipher forms a [graded] finitely generated [polynomial] ring. $A+B; A*B$
Key Remark:

To insure that

\[ P \times R \Rightarrow P \times R \]

we only need to make sure that \( P \Rightarrow P \) but ONLY for a subspace where \( R(inp)=1 \) and \( R(out)=1 \)
East German T-310 Block Cipher

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

- Long-term secret is only 90 bits!
How to Backdoor a Block Cipher

I have written an elementary tutorial and a first proof of concept about how to backdoor a block cipher in a quite general setting. Potentially it applies to any block cipher. Success is not guaranteed though, see the paper.

ADDED 2 JAN 2019:
a new paper shows that invariants of higher degree are substantially more powerful. Instead of a progression, we have a qualitative leap in what can be now achieved: see new paper.

ADDED 4 April 2019: here are slides presented at WCC 2019.
“Official” History of Cryptanalysis

- **DC** was known @IBM in 1970s

- **Linear Cryptanalysis**: Gilbert and Matsui [1992-93]
Block Cipher Invariants

LC in 1976 [Eastern Germany]

Definition 3.1-1

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

\[ \| g \| \sum_{x} g(x) \]

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

Geheime Verschlüsselung

Mfs -020-Nr.: X1/493/3761 BL 18

Ergebnisse:

Tabelle 3.1-2

<table>
<thead>
<tr>
<th>( \alpha )</th>
<th>( \Delta^2_{\alpha} )</th>
<th>( t )</th>
<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</td>
<td>32</td>
<td>L 0 0 0 0 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>0 0 0 0 0 L</td>
<td>2</td>
<td>34</td>
<td>L 0 0 0 0 0</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>0 0 0 0 L O</td>
<td>-4</td>
<td>28</td>
<td>L 0 0 0 0 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>0 0 0 L O L</td>
<td>6</td>
<td>38</td>
<td>L 0 0 0 0 0</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>0 0 L O O L</td>
<td>-4</td>
<td>28</td>
<td>L 0 0 0 0 0</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>0 0 L O L L</td>
<td>-2</td>
<td>30</td>
<td>L 0 0 0 0 0</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>0 0 L L L L</td>
<td>0</td>
<td>32</td>
<td>L 0 0 0 0 0</td>
<td>4</td>
<td>36</td>
</tr>
<tr>
<td>0 0 L L L L</td>
<td>2</td>
<td>34</td>
<td>L 0 0 0 0 0</td>
<td>2</td>
<td>34</td>
</tr>
</tbody>
</table>

Seit der Anzahl der Übereinstimmungen der Funktionenvektoren von 2.
Generalised Linear Cryptanalysis
\[= \text{GLC} =\]

[Harpes, Kramer and Massey, Eurocrypt’95]

Concept of [invariant] non-linear I/O sums.

\[P(\text{inputs}) = P(\text{outputs})\]
with some probability…
Connecting Non-Linear Approxs.

Black-Box Approach

Non-linear functions $F$, $G$, $H$.

$F(x_1, \ldots)$

$G(y_1, \ldots)$

$\varphi$

$G(y_1, \ldots)$

$\varphi$

$H(z_1, \ldots)$
GLC and Feistel Ciphers?

[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

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

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: \( \frac{1}{2} \pm 1.2 \cdot 2^{-15} \)
Better Is Enemy of Good!

DES = Courtois @ Crypto 2004:

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

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

\[
\text{proba}=1.0 \quad \text{deg 10}
\]
New White Box Approach

non-linear I/O sums.

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

Formal equality of 2 polynomials.
Variable Boolean Function

We denote by $Z$ our Boolean function.
We consider a space of ciphers where $Z$ is variable.

Question: given a fixed polynomial $P$
what is the probability over random choice of $Z$ that $P(\text{inputs}) = P(\text{outputs})$ is an invariant (for any number of rounds).
How Do You Find An Attack?

\[ 2^{2^n} \text{ possible attacks} \]
Invariant Hopping

- Attack 1: 2x linear
- Attack 2: 1x linear
- Attack 3: Strong Bool + high degree invariant + high success proba
- Attack 4: Strong Bool + high success proba
Group Theory – Is DES A Group?

Study of group generated by \( \phi_K \) for any key \( K \).
Typically AGL not GL. Any smaller sub-groups?
Related Research

A NOTE ON SOME ALGEBRAIC TRAPDOORS FOR BLOCK CIPHERS

MARCO CALDERINI
Department of Informatics, University of Bergen, Norway

ABSTRACT. We provide sufficient conditions to guarantee that a translation based cipher is not vulnerable with respect to the partition-based trapdoor. This trapdoor has been introduced, recently, by Bannier et al. (2016) and it generalizes that introduced by Paterson in 1999. Moreover, we discuss the fact that studying the group generated by the round functions of a block cipher may not be sufficient to guarantee security against these trapdoors for the cipher.
Hopping in Group Lattices

attack 1
three invariants
linear Boolean function

AGL
Hopping in Group Lattices

- **Attack 1**: Three invariants, linear Boolean function
- **Attack 2**: Two invariants, bad Boolean function

Diagram showing the group lattice with labeled sets and arrows indicating hopping between sets.
Hopping in Group Lattices

- **Attack 1**: Three invariants
  - Linear Boolean function

- **Attack 2**: Two invariants
  - Bad Boolean function

- **Attack 36**: One high degree invariant
  - Strong Boolean function
Hopping in Group Lattices

- **Attack 1**: Three invariants, linear Boolean function
- **Attack 2**: Two invariants, bad Boolean function
- **Attack 36**: One complex high degree invariant, strong Boolean function
“Hopping” Discovery

• Learn from examples.

• Find a path from a trivial attack on a weak cipher to a non-trivial attack on a strong cipher.
T-310 [Contracting Feistel, 1970s, Eastern Germany!]

1 round of T-310
Impossible => Possible?

• We literally use “impossible” linear properties, which cannot happen and do not happen, and construct a non-linear attack which works.
Hopping Step 1 [WCC’19]

First we look at an attack where the Boolean function is linear and we have trivial LINEAR invariants (same as Matsui’s LC)

Example:

\[ Z(a, b, c, d, e, f) = f \]

4R linear invariant

\[ D \rightarrow C \rightarrow B \rightarrow A \rightarrow D \]

\[ A \overset{\text{def}}{=} (e + m) \]
\[ B \overset{\text{def}}{=} (f + n) \]
\[ C \overset{\text{def}}{=} (g + o) \]
\[ D \overset{\text{def}}{=} (h + p) \]
Impossible?

3 trivial, 1 impossible transitions

\[ D \rightarrow C \rightarrow B \rightarrow A \rightarrow ? \rightarrow D \]
A Vulnerable Setup

551: \( P = 17, 4, 33, 12, 10, 8, 5, 11, 9, 30, 22, 24, 20, 2, 21, 34, 1, 25, 13, 28, 14, 16, 36, 29, 32, 23, 27 \)
\( D = 0, 12, 4, 36, 16, 32, 20, 8, 24 \)
Now could you please tell us if $P = eg + fh + eo + fp + gm + hn + mo + np$ is an invariant? $= AC + BD$

$$\begin{align*}
A & \overset{\text{def}}{=} (e + m) \\
B & \overset{\text{def}}{=} (f + n) \\
C & \overset{\text{def}}{=} (g + o) \\
D & \overset{\text{def}}{=} (h + p)
\end{align*}$$
Hopping Step 2

Now could you please tell us if
\[ P = eg + fh + eo + fp + gm + hn + mo + np \]

is an invariant?

The answer is remarkably simple.
Hopping Step2

Theorem:

\[ P = eg + fh + eo + fp + gm + hn + mo + np \]

is an invariant

IF AND ONLY IF

a certain polynomial = FE =
Hopping Step 2

Theorem:

\[ \mathcal{P} = eg + fh + eo + fp + gm + hn + mo + np \]

is an invariant IF AND ONLY IF a certain polynomial = FE = is zero (as a polynomial, multiple cancellations)
Compute FE?

Theorem:

\[ \mathcal{P} = eg + fh + eo + fp + gm + hn + mo + np \]

is an **invariant**

IF AND ONLY IF

the Fundamental Equation \( FE \)

\[ \mathcal{P}(a, b, c, d, e, f, g, h, \ldots, V) = \mathcal{P}(b, c, d, F + m, f, g, h, F + Z + O, \]

\[ \ldots, F + Z + O + Y + q + L + X + i + W + j + K) \]

is zero
Theorem:

\[ P = eg + fh + eo + fp + gm + hn + mo + np \]

is an invariant

IF AND ONLY IF

is zero (as a polynomial, multiple cancellations)
Notation

We have

\[ P = eg + fh + eo + fp + gm + hn + mo + np \]

is an invariant

IF AND ONLY IF

\[ P = P(\text{inputs}) \equiv P(\text{output ANF}) = P^\varphi \]

IF AND ONLY IF

is zero (as a polynomial, multiple cancellations)

\[ P + P^\varphi = \text{FE} \]
Block Cipher Invariants

Compact Notation

\( P \) is an invariant

IF AND ONLY IF

\[ P \equiv P\varphi \]

= FE is zero
White Box Cryptanalysis = New

[Courtois 2018]
Same concept of a non-linear I/O sums.
Focus on perfect invariants mostly.

\[ P(\text{inputs}) = P(\text{outputs}) \text{ with probability 1.} \]
Formal equality of 2 polynomials.
Exploits the structure of the ring \( B_n \).
• annihilation events \( \Leftrightarrow \) absorption events, nb. of vars collapses
• would be unthinkable if we had unique factorisation
\[ ABCD = A'B'C'D' \]
New Paradigm [1905.04684]

Lack of Unique Factorization as a Tool in Block Cipher Cryptanalysis

Nicolas T. Courtois, Aidan Patrick

(Submitted on 12 May 2019)

Linear (or differential) cryptanalysis may seem dull topics for a mathematician: they are about super simple invariants characterized by say a word on n=64 bits with very few bits at 1, the space of possible attacks is small, and basic principles are trivial. In contract mathematics offers an infinitely rich world of possibilities. If so, why is that cryptographers have ever found so few attacks on block ciphers? In this paper we argue that black-box methods used so far to find attacks in symmetric cryptography are inadequate and we work with a more recent white-box algebraic methodology. Invariant attacks can be constructed explicitly through the study of roots of the so-called Fundamental Equation (FE). We also argue that certain properties of the ring of Boolean polynomials such as lack of unique factorization allow for a certain type of product construction attacks to flourish. As a proof of concept we show how to construct a complex and non-trivial attack where a polynomial of degree 7 is an invariant for any number of rounds for a complex block cipher.

Subjects: Cryptography and Security (cs.CR)
MSC classes: 13A50, 94A60, 68P25, 11T71, 14G50
ACM classes: K.3; I.1; K.2
Cite as: arXiv:1905.04684 [cs.CR]
Conclusion Step2

Theorem:

\[ P = eg + fh + eo + fp + gm + hn + mo + np \]

is an invariant

IF AND ONLY IF

the Fundamental Equation \( FE \)

\[ Y(g + o) = m(g + o) \]

is zero (as a polynomial, multiple cancellations)
What is Special About $P$

2-factoring decomposition

$P = eg + fh + eo + fp + gm + hn + mo + np$

= AC+BD.

is invariant IF AND ONLY IF

$Y(g+o) = m(g+o)$

some solutions are:

$Z(a, b, c, d, e, f) = f$

$Z = 1 + d + e + f + de + cde + def.$
Attack of Degree 4

Q : Can we now have $ABCD$ to be an invariant of degree 4

Answer: easy: Y must be a root of

$$m_{BCD} = Y_{BCD} = FE$$
Product Attack

Construct NL invariants based on LC cycles:

A $\rightarrow$ B $\rightarrow$ C $\rightarrow$ D $\rightarrow$ A

Then ABCD is a round invariant of degree 4.
Phase Transition

When $\mathcal{P}$ is of degree 4, the Boolean function is still “inevitably” degenerated [WCC’18].

Q: Can we backdoor or break a cipher with a random Boolean function?

Solution:
The degree of $\mathcal{P}$ must increase to 8.
Phase Transition

When $\mathcal{P}$ is of degree 4, the Boolean function is still “inevitably” degenerated [this paper].

Q: Can we backdoor or break a cipher with a “strong” (e.g. random) Boolean function?

YES, see [eprint/2018/1242]
Degree 8 attack, $\mathcal{P}=ABCDEFGH$. 
Thm 5.5.
In eprint/2018/1242 page 18.

\[ P = ABCDEFGH \]

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?
Hard Becomes Easy


- When $\mathcal{P}$ degree grows, attacks become a LOT easier.

- Degree 8: extremely strong:
  15% success rate over the choice of a random Boolean function and with $\mathcal{P}=$ABCDEFGH.

(3 variants)

WHAT?????????????
Let $Y = \text{Random Bool}$. Can we HOPE that for we have for example:

$$mBCD = YBCD \text{ i.e. } 0 = (Y + m)BCD = FE$$


For any $Z$ with 6 variables, $Z$ or $Z+1$ always has some cubic annihilators.

Thm 6.4: [eprint/2018/1242]

For $Z(a+b)(c+d)(e+f) = 0$, any Boolean function works with probability of 5%.
Less Trivial Attacks

an irregular sporadic attack with $\mathcal{P}$ of degree 7

Theorem 6.1 (A Degree 7 Invariant Attack). Let


then $\mathcal{P}$ is a non-zero polynomial of degree 7. We also assume that

$$\begin{cases}
  \{D(2), D(3)\} = \{6 \cdot 4, 7 \cdot 4\} \\
  \{D(6), D(7)\} = \{2 \cdot 4, 3 \cdot 4\}
\end{cases}$$

and that inputs of $Y$ are in order bits 27, 6, 10, 23, 21, 25 and inputs of $W$ are in order bits 26, 9, 5, 22, 7, 11. We assume that the Boolean function used inside the cipher has after adding 1 TWO degree 3 annihilators as follows:

$$(Z+1)*(f+e)(d+a)(b+c)=0$$

$$(Z+1)*(f+e+1)(d+a+1)(b+c+1)=0$$

Then $\mathcal{P}$ is a round invariant for any key any IV and any number of rounds.
problem:
a LOT more key bits

48 instead of 2 in each round
What about the actual DES wiring?

realism is more interesting than fiction!
Theorem: Let $P = (1+L06+L07)\cdot L12 \cdot R13\cdot R24\cdot R28$

IF

$(1+c+d)\cdot W2 == 0$ and $(1+c+d)\cdot X2 == 0$
$e\cdot W3 == 0$ and $f\cdot Z3 == 0$
$ae\cdot X7 == 0$ and $ae\cdot Z7 == 0$

THEN

$P$ is an invariant for 1 round of DES.