Invariant Hopping Attacks on Block Ciphers

Nicolas T. Courtois

University College London, Gower Street, London, UK

Abstract. Block ciphers are in widespread use since the 1970s. Their iterated structure is prone to numerous round invariant attacks for example in Linear Cryptanalysis (LC). The next step is to look at non-linear polynomial invariants cf. Eurocrypt'95. Researchers have until 2018 found extremely few such attacks with some impossibility results [2, 3]. Eventually recent papers show how to construct polynomial invariant attacks for block ciphers, however almost all such results are of degree 2, cf. [6, 17, 4]. Can we find any higher degree attacks? In this paper we show a new incremental and highly practical methodology for constructing high degree polynomial invariant attacks on block ciphers. A trivial attack on one cipher setup will be transposed to show the existence of a more advanced attack on a stronger cipher in several steps. The key tool is the manipulation of the roots of the so called Fundamental Equation.

Key Words: block ciphers, Boolean functions, ANF, Feistel ciphers, weak keys, T-310, Linear Cryptanalysis, Generalized Linear Cryptanalysis, polynomial invariants, multivariate polynomials, algebraic cryptanalysis.

1 Introduction, Non-Linear Cryptanalysis

The concept of cryptanalysis with non-linear polynomials a.k.a. Generalized Linear Cryptanalysis (GLC) was introduced at Eurocrypt'95, cf. [12]. A key question is the existence of round-invariant I/O sums: when a value of a certain polynomial is preserved after 1 round. Such properties are notriously hard to find [17, 4]. There are 2^{2^n} possible invariants and systematic exploration is not feasible [2]. In this paper and unlike in [17] we focus on invariants which work for 100 % of the keys and we focus on stronger invariants which hold with probability 1 for one round. In addition we look at a an expensive government cipher where encryption is a lot more costly than 3DES, AES, cf. [10]. Here standard cryptanalytic attacks simply do not work. However all this complexity is not that useful if we can discover invariants attacks working for any number of rounds.

Invariants vs. Maths. There exists an extensive theory of multivariate polynomial algebraic invariants [11] which historically has studied mostly invariants w.r.t. linear transformations and has rarely studied invariants with more than 5 variables and in finite fields of small size. In our work we study invariants w.r.t **non-linear** transformations and 36 or more variables over $GF(2)$.

The Question of Weak Keys. There are numerous constructions of weak ciphers in cryptographic literature, cf. for example work related to the AES S-box [7, 8], and [1, 3]. In this paper, a weak key or rather a weak long-term key setup is primarily a tool to find some attack more easily, and the same attack may be transposed to hold also for another (stronger) cipher setup.

Partitioning Cryptanalysis. A more general approach considers arbitrary subsets of binary vector spaces and is called Partitioning Cryptanalysis (PC), cf. [1, 13]. Our work is then a special case: we study only partitions defined by the value (0/1) for a single Boolean polynomial, cf. [4]. This is less general but properties are more intelligible and follow clear rules of formal algebra. A serious theory is nowadays being developed around what is possible or not to achieve in partitioning and invariant attacks, cf. [2, 3]. There are two major types of invariants in recent research: linear sub-space invariants [2, 3] and proper non-linear polynomial invariants [17, 7, 4]. We focus on the latter.

Finding Advanced Invariant Attacks. The primary method proposed in 2018 is through solving the so called Fundamental Equation or FE cf. [4]. Solving such equation(s), or several such equations simultaneously, **guarantees** that we obtain a Boolean function and the polynomial invariant $\mathcal{P}$ which propagates for any number of rounds. However nothing guarantees that the FE equation has any solutions whatsoever. In this paper we construct polynomial invariants explicitly by modifying something which worked. A trivial attack on a weak cipher will be transformed into a better or higher degree invariant attack on a stronger cipher in several steps. We call this method "invariant hopping".

This paper is organized as follows. In Section 2 we show explain our objectives, notations and provide formulas which define one round of our block cipher. In Section 3 we explain that the problem of finding a one-round invariant can be formalized as the problem of solving the FE. A key tool is looking at different roots of the same equation. In Section 4 we show an example of our first non-linear attack which can be downgraded to a simple linear attack. Inversely a linear invariant $\mathcal{L}$ on one cipher may hide the existence of another non-linear invariant property $\mathcal{P}$ on the same cipher. We do not stop here: in Section 4.1 we show that an invariant of degree 4 also exists. Then in Section 4.2. the simpler invariants will be removed and we keep ONLY one invariant of degree 4. Finally in Section 4.3. we modify the wiring in order to accommodate a Boolean function of a higher degree. In few steps a pathological cipher becomes a substantially stronger cipher and the attack less obvious.

2 Polynomial Invariant Attacks on Block Ciphers

We call $\mathcal{P}$ a polynomial invariant if the value of $\mathcal{P}$ is preserved after one round of encryption, i.e. if $\mathcal{P}(\text{Inputs}) = \mathcal{P}(\text{Outputs})$. This works for any block cipher except that such attacks are notoriously hard to find [2] in the last 20 years since [12]. In this paper we are going to work with one specific block cipher with 36-bit[1] blocks. The main point is that any block cipher round translates into relatively simple Boolean polynomials, if we look at just one round. We follow the methodology of [4] in order to specify the exact mathematical constraint, known as the Fundamental Equation or FE, so that we could have a polynomial invariant attack on our cipher. Such an attack will propagate for any number of rounds (if independent of key and other bits). In addition it makes sense

[1] Block size could be increased and our attacks and methods would work all the same.

following [4] to consider that the Boolean function is an unknown. We denote this function by a special variable Z. We then see that our attack works if an only if Z is a solution to a certain algebraic equation [with additional variables]. The main interest of making Z a variable is to find some strong attacks in the cases where the Boolean function is extremely weak case, (e.g. Z is linear) and transpose them to stronger ciphers where Z will be increasingly complex.

We discard the attacks when the FE reduces to 0 which work for any Z yet such attacks are quite rare cf. [4] and our later specific trick or method for finding new attacks by manipulating the roots of FE would not work.

2.1 Notation and Methodology

In this paper the sign + denotes addition modulo 2, and frequently we omit the sign * in products. For the sake of compact notation we frequently use short or single letter variable names. For example let $x_1, \ldots, x_{36}$ be inputs of a block cipher each being $\in \{0, 1\}$. We will avoid this notation and name them with small letters $a - z$ and letters $M - V$ when we run out of lowercase letters. We follow the backwards numbering convention of [4] with $a = x_{36}$ till $z = x_{11}$ and then we use specific capital letters $M = x_{10}$ till $V = x_1$. This avoids some "special" capital letters following notations used since the 1970s [10, 16, 15]. We consider that each round of encryption is identical except that they can differ only in some "public" bits called F (and known to the attacker) and some "secret" bits called $S1$ or K and $S2 = L$. Even though these bits ARE different in different rounds we will omit to specify in which round we take them because our work is about constructing **one round** invariants (extending to any number of rounds). This framework covers most block ciphers ever made except that some ciphers would have more "secret" or "public" bits in one round. The capital letter Z is a placeholder for substitution of the following kind

$$Z(e_1, e_2, e_3, e_4, e_5, e_6)$$

where $e_1 \ldots e_6$ will be some 6 of the other variables. In practice, the e_i will represent a specific subset of variables of type *a-z*, or other such as L. Later Z (and maybe another letter like W) needs to be replaced by a formula like:

$$Z \leftarrow Z00 + Z01 * L + Z02 * c + Z03 * Lc + \ldots + Z62 * cklfh + Z63 * Lcklfh$$

where Zij are coefficients of the Algebraic Normal Form (ANF).

Polynomial Invariants We are looking for arbitrary polynomial invariants. For example say $\mathcal{P}(a, b, \ldots) = abc + abd + acd + bcd + \ldots$ In this space some solutions are considered as trivial and are easy to find, for example when $\mathcal{P}$ is a simple product of linear invariants cf. Appendix of [4]. Complex irreducible polynomials are considered as less trivial and are harder to find. One of the main points in discovery of innovative attacks on block ciphers is that attacks with irreducible polynomial invariants of degree higher than 2 are actually at all possible, and how to construct some (rather than just discover accidentally).

2.2 Constructive Approach Given the Cipher Wiring

Our attack methodology starts[2] from a given block cipher specified by its ANFs for one round. Specific examples are shown for T-310, and old Feistel cipher with 4 branches. This cipher offers great **flexibility** in the choice of the internal wiring and entirely compatible with original historical hardware. The block size is 36 bits and the key has 240 bits. We number the cipher state bits from 1 to 36 where bits $1, 5, 9 \ldots 33$ are those freshly created in one round, cf. Fig 1. One round of encryption is then described as 36 Boolean polynomials of degree 6.

$$
\begin{aligned}
y_{33} &= F + x_{D(9)} \\
Z1 &\overset{def}{=} Z(S2, x_{P(1)}, \ldots, x_{P(5))}) \\
y_{29} &= F + Z1 + x_{D(8)} \\
y_{25} &= F + Z1 + x_{P(6)} + x_{D(7)} \\
Z2 &\overset{def}{=} Z(x_{P(7)}, \ldots, x_{P(12)}) \\
y_{21} &= F + Z1 + x_{P(6)} + Z2 + \qquad x_{D(6)} \\
y_{17} &= F + Z1 + x_{P(6)} + Z2 + \qquad x_{P(13)} + x_{D(5)} \\
Z3 &\overset{def}{=} Z(x_{P(14)}, \ldots, x_{P(19)}) \\
y_{13} &= F + Z1 + x_{P(6)} + Z2 + \qquad x_{P(13)} + S2 + Z3 + x_{D(4)} \\
y_9 &= F + Z1 + x_{P(6)} + Z2 + \qquad x_{P(13)} + S2 + Z3 + x_{P(20)} + x_{D(3)} \\
Z4 &\overset{def}{=} Z(x_{P(21)}, \ldots, x_{P(26)}) \\
y_5 &= F + Z1 + x_{P(6)} + Z2 + \qquad x_{P(13)} + S2 + Z3 + x_{P(20)} + Z4 + x_{D(2)} \\
y_1 &= F + Z1 + x_{P(6)} + Z2 + \qquad x_{P(13)} + S2 + Z3 + x_{P(20)} + Z4 + x_{P(27)} + x_{D(1)} \\
x_0 &\overset{def}{=} S1 \\
y_{i+1} &= x_i \text{ for all other } i \neq 4k \qquad (\text{ with } 1 \leq i \leq 36)
\end{aligned}
$$

In order for our polynomials to be short and compact we further replace the 36 bits $x_1 - x_{36}$ by single letters (avoiding certain letters like F used elsewhere):

Numbers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Letters	V	U	T	S	R	Q	P	O	N	M	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Two things remain unspecified: the P and D boxes or the internal wiring. In T-310 this specification is called an LZS or *Langzeitschlüssel* which means a long-term key setup. We simply need to specify two functions $D : \{1 \ldots 9\} \rightarrow \{0 \ldots 36\}$, $P : \{1 \ldots 27\} \rightarrow \{1 \ldots 36\}$. For example $D(5) = 36$ will mean that input bit 36 is connected to the wire which becomes $U5 = y_{17}$ after XOR of Fig. 1. Then $P(1) = 25$ will mean that input 25 is connected as v1 or the 2nd input of $Z1$. We also apply a special convention where the bit S1 is used instead of one of the $D(i)$ by specifying that $D(i) = 0$. We study invariants for one round and therefore variables x_i and y_i are treated "alike" and can be called be the SAME letter, for example $x_{36} = a$ and then $y_{36} = a$ also.

[2] Our approach is to find invariant attack starting from arbitrary rounds ANFs is at the antipodes compared to [7, 8] where the ciphers are very special.

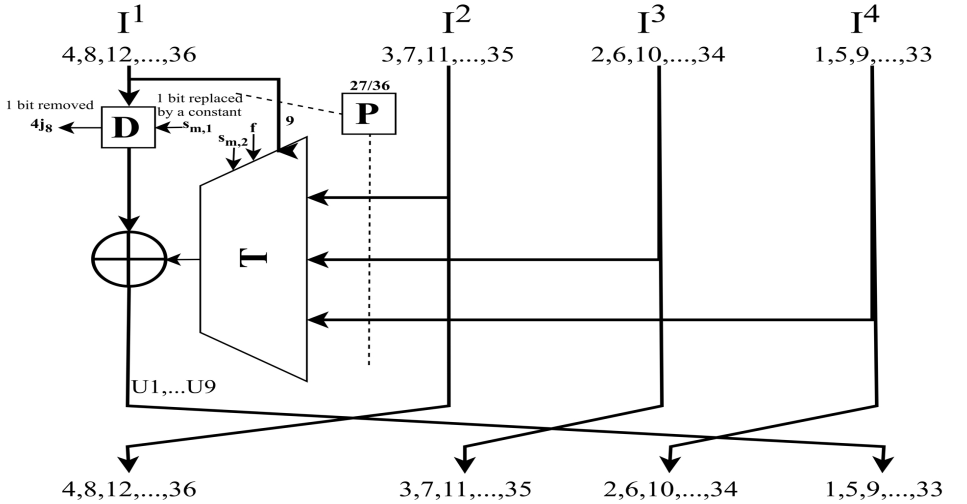

Fig. 1. T-310: a peculiar sort of Compressing Unbalanced Feistel scheme.

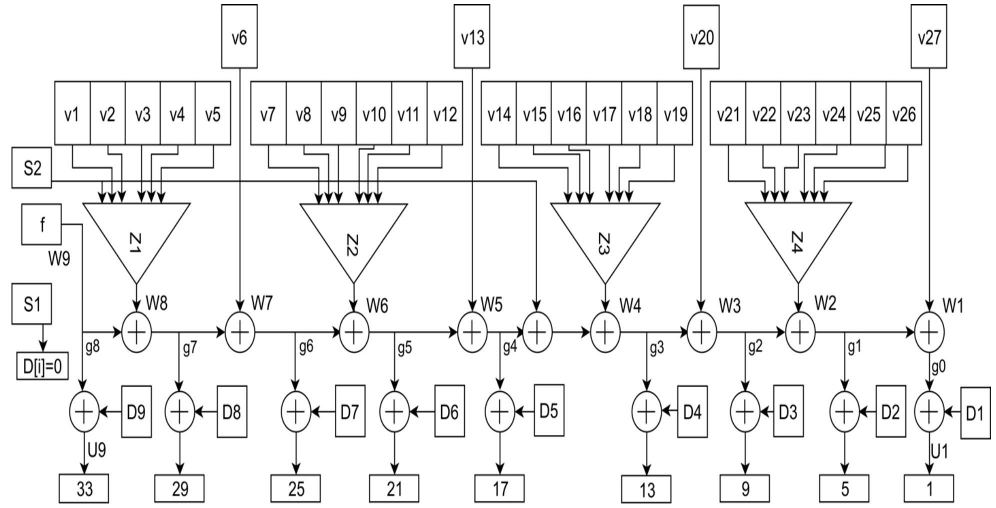

Fig. 2. The internal structure of one round of T-310 block cipher.

The Substitutions. In order to have shorter expressions to manipulate we need further to replace $Z1 - Z4$ by shorter abbreviations Z, Y, X, W respectively. We also replace S2 by a single letter L. When later in this paper we use some concrete LZS (for example LZS 551 specified later) this leads to replacing variables and to some simplifications, as shown in the example below. For example y_{25} is l and if $D(7) = 20$ then $x_{D(7)}$ becomes q, etc, and we get $l \leftarrow F + Z1 + O + q$. This can be interpreted as one round of encryption is equivalent to replacing l and all the other letters by our exact formulas, for example with LZS 551 we get:

$$
\begin{array}{l}
a \leftarrow b \\
b \leftarrow c \\
c \leftarrow d \\
\;[\ldots] \\
\;Z1 \leftarrow Z(L,t,S,d,y,m)) \\
l \leftarrow F + Z1 + O + q \\
\;[\ldots] \\
\;Z4 \leftarrow Z(w,u,a,h,e,n) \\
\;[\ldots] \\
V \leftarrow F + Z1 + O + Z2 + q + L + Z3 + i + Z4 + k + K
\end{array}
$$

3 The Fundamental Equation

In order to break our cipher we need to find a polynomial expression $\mathcal{P}$ say

$$\mathcal{P}(a,b,c,d,e,f,g,h,\ldots) = abcdijkl + efg + efh + egh + fgh$$

using any number between 1 and 36 variables such that if we substitute in $\mathcal{P}$ all the variables by the substitutions defined we would get exactly the same polynomial expression $\mathcal{P}$, i.e. $\mathcal{P}(Inputs) = \mathcal{P}(Outputs)$ are equal as multivariate polynomials. We obtain:

Definition 3.1 (Compact Uni/Quadri-variate FE). Our "Fundamental Equation (FE)" to solve is simply a substitution like:

$$\mathcal{P}(Inputs) = \mathcal{P}(Outputs)$$

or more precisely

$$\mathcal{P}(a,b,c,d,e,f,g,h,\ldots) = \mathcal{P}(b,c,d,F+i,f,g,h,F+Z1+e,\ldots)$$

where again $Z1 - Z4$ are replaced by Z, Y, X, W. In the next step, Z will be replaced by an Algebraic Normal Form (ANF) with 64 binary variables which are the coefficients of the ANF of Z, and there will be several equations, and four **instances** Z, Y, X, W of the same Boolean function Z:

Definition 3.2 (A Multivariate FE). At this step we will rewrite FE as follows. We will replace Z1 by:

$$Z \leftarrow Z00 + Z01 * L + Z02 * j + Z03 * Lj + \ldots + Z62 * jhfpd + Z63 * Ljhfpd$$

Likewise we will also replace $Z2$:

$$Y \leftarrow Z00 + Z01 * k + Z02 * l + Z03 * kl + \ldots + Z62 * loent + Z63 * kloent$$

and likewise for $X = Z3$ and $W = Z4$ and the coefficients $Z00 \ldots Z63$ will be the same inside $Z1 - Z4$, however the subsets of 6 variables chosen out of 36 will be different in $Z1 - Z4$. Moreover, some coefficients of $\mathcal{P}$ may also be variable.

In all cases, all we need to do is to solve the equation above for Z, plus a variable amount of extra variables e.g. $Z63$. This formal algebraic approach, if it has a solution, still called Z for simplicity, or $(\mathcal{P}, Z)$ will **guarantee** that our invariant $\mathcal{P}$ holds for 1 round. This is, and in this paper we are quite lucky, IF this equation does not depend on three bits F, K, L. This is the discovery process of [4].

In this paper we do NOT use this process. We will work by **attack hopping**. From one attack we will derive the existence of another attack on a different cipher (!). Thus we completely avoid all the most difficult questions in [4]: Do such equations have any solutions? If they have, can the solution be the same for several permutations simultaneously? We concentrate on transposing some working attacks to another cipher setup or where the Boolean function is modified.

4 KT1 Keys and Higher Degree Invariant Attacks

Most invariants on block ciphers published so far were of degree 2 [6, 4, 17] and finding any such invariants was quite difficult. The LZS examples were also not very good. The East German government cryptologist have mandated that for an LZS to be approved for "official" use, it must satisfy a certain very complex specification called KT1 which takes one full page to describe, cf. Appendix B in [9]. Our starting point will be a simple invariant from [4] which actually works for a genuine KT1 key, something considered hard to do until recently.

```
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
```

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

with this short $\mathcal{P}$ the Fundamental Equation FE will have very few terms:

$$\mathcal{P}(a, b, c, d, e, f, g, h, \ldots, V) = \mathcal{P}(b, c, d, F + m, f, g, h, F + Z + O,$$
$$\ldots, F + Z + O + Y + q + L + X + i + W + j + K)$$
$$Y(g + o) = m(g + o)$$

and one solution which makes our cipher weak is $Z = 1+d+e+f+de+cde+def$. The fact that our FE contains none of F, K, L implies that our polynomial $\mathcal{P}$ is an invariant which works for any key and any IV and for any number of rounds.

An Essential Insight It is easy to see that $\mathcal{P}$ is irreducible and no linear attack exists for this cipher setup. Interestingly we have $\mathcal{P} = AC + BD$ where:

$$\begin{cases} A \overset{def}{=} (e + m) \\ B \overset{def}{=} (f + n) \\ C \overset{def}{=} (g + o) \\ D \overset{def}{=} (h + p) \end{cases}$$

Now do A, B, C, D have any concrete significance for our cipher? To see this let us consider a yet simpler case when $Z(a, b, c, d, e, f) = f$. Then it is possible to check that our cipher would have 4R linear invariant $D \rightarrow C \rightarrow B \rightarrow A \rightarrow D$ which however is totally absent when $Z = 1 + d + e + f + de + cde + def$.

Downgrading Our Invariant: Now we show that our non-linear attack **hides the existence** of a yet simpler attack with a degenerated Boolean function. To shows this we observe that input f of Y is $P[12] = m$, i.e. last input of $Z2$ is precisely connected to m with LZS 551. What happens if $Y = m$ i.e. $Z = f$? We have another degenerated solution of our FE being $(Y - m)(g + o) = 0$ and we have in fact found a root for a **proper factor** $(Y - m) = 0$ of our general FE.
Next Step. An interesting question is can we do this in a reverse direction? Find a cipher setup where the FE is a multiple of $(Y - m)(g + o) = 0$? Yes!

4.1 Construction of Higher Degree Invariants.

Such invariants if they exist are NOT uniquely determined, they may depend on the choice of the Boolean function Z in the previous step (!). For the current pair LZS, Z as above we found that the following $\mathcal{P}$ of degree 4 also works:

$$\mathcal{P} = efgh + fghm + eghn + ghmn + efho + fhmo + ehno + hmno+$$

$$efgp + fgmp + egnp + gmnp + efop + fmop + enop + mnop$$

where in fact $\mathcal{P} = ABCD$. Interestingly, **no other** invariants being polynomials in A, B, C, D exist. We conjecture however that no invariants other than $AC+BD$ (irreducible) and $ABCD$ (not irreducible) exist for 1 round[3] and probably not in general[4]. For sure we have verified that no linear invariants exist here for LZS 551 and $Z = 1 + d + e + f + de + cde + def$.

Study of *FE*. If $\mathcal{P} = ABCD$ what is the FE? A quick computation gives

$$mBCD = YBCD$$

This decomposition implies that any solution Z which is a solution to the previous FE will also work here but **NOT vice versa**.

4.2 A More Autonomous Example of An Invariant of Degree 4

Until now we have seen that a weak cipher with linear invariants A, B, C, D shared the same non-linear invariants with a cipher where the only attacks are the non-linear ones $AC + BD$ and $ABCD$. Is it possible to **remove** the first attack and keep the second? Yes and it is requires minimal change. We recall that $AC + BD$ will be an invariant each time our Boolean function satisfies:

$$YC = mC$$

and in order for $ABCD$ to be an invariant, Z needed to satisfy:

$$mDCB = YDCB$$

[3] For 2 rounds we have closely related invariants $AC \to BD \to AC$ with AC and BD being invariants for 4 rounds. All these do not use F, K, L either.

[4] In fact it is hard to be sure, no method to explore all possible invariants with 36 variables at higher degrees is known and possibly such method does not exist

All we have to do now is to find a solution Y which satisfies one FE and not the other FE! For example we can find a solution to an alternative equation:

$$mB = YB$$

which is different than the most trivial solution $Y(......) = m$ and which then will satisfy only the first equation. For example $1 + n + nm + f + mf$ using the same variable names. An actual solution forces us to modify LZS 551 very slightly: we just need to make sure that letters f and n are actually inputs of Y. Only two modifications are needed. Here is a solution found by a SAT solver:

```
558: P=17,4,33,12,10,8,23,24,31,25,16,10,20,2,21,34,
1,25,13,28,14,16,36,29,32,23,27 D=0,12,4,36,16,32,20,8,24
Z(a,b,c,d,e,f)=1+a+ab+c+bc
```

We have checked that no other invariants at degree up to 3 exist with all the 36 state variables for $1, 2, 3, 4, 5, \ldots$ and various numbers of rounds. All simple invariants were removed with the new Boolean function and only $ABCD$ is left.

4.3 A Yet Stronger Example

One step further, we try to find a non-trivial (proper) solution to:

$$mBC = YBC$$

Here we will need to use as inputs of Z all the 5 variables which appear in this equation. A nice trick to quickly find a solution which is a "proper" root of $(m+Y)BC$ is to first create a new equation FE' which implies the previous one by multiplying both sides by B, yet at the same time FE' actually imposes the presence of the two variables f, n in B, and another $6-th$ variable, for example:

$$(Y + m)(f + n) = (Rnf + Rf)go$$

Again just one invariant $ABCD$ remains after changing the Boolean function but now our Boolean function must use 6 quite specific variables which must be connected to inputs of $Z2 = Y$. One possible solution is as follows:

```
550: P=17,4,33,12,10,8,22,23,24,31,30,20,20,2,21,34,
1,25,13,28,14,16,36,29,32,23,27 D=0,12,4,36,16,32,20,8,24
Z(a,b,c,d,e,f)=1+b+c+d+aef+abef
```

Quick Conclusion. This paper demonstrates a novel invariant hopping technique. An attack on a pathologically weak cipher setup is transposed to break another stronger cipher. In several steps we remove the trivial attacks and keep less trivial ones. The complexity and algebraic degree for the invariant and the Boolean function, and the number of variables needed increase progressively. Further more complex invariants of degree 8 can also now be constructed, cf. [5].

References

1. Arnaud Bannier, Nicolas Bodin, and Eric Filiol: *Partition-Based Trapdoor Ciphers,* eprint.iacr.org/2016/493.
2. C. Beierle, A. Canteaut, G. Leander, Y. Rotella: *Proving resistance against invariant attacks: how to choose the round constants,* in Crypto 2017, Part II. LNCS, 10402, pp. 647–678, Springer 2017.
3. Marco Calderini: *A note on some algebraic trapdoors for block ciphers,* last revised 17 May 2018, https://arxiv.org/abs/1705.08151
4. Nicolas T. Courtois: *On the Existence of Non-Linear Invariants and Algebraic Polynomial Constructive Approach to Backdoors in Block Ciphers,* https://eprint.iacr.org/2018/807.pdf, revised 3 Dec 2018.
5. Nicolas T. Courtois: *Structural Nonlinear Invariant Attacks on T-310: Attacking Arbitrary Boolean Functions,* https://eprint.iacr.org/2018/1242.pdf, received 28 Dec 2018.
6. Nicolas Courtois: *Feistel Schemes and Bi-Linear Cryptanalysis,* in Crypto 2004, LNCS 3152, pp. 23–40, Springer, 2004.
7. Nicolas Courtois: *The Inverse S-box, Non-linear Polynomial Relations and Cryptanalysis of Block Ciphers*, in AES 4 Conference, Bonn May 10-12 2004, LNCS 3373, pp. 170–188, Springer, 2005.
8. Nicolas Courtois: *The Inverse S-box and Two Paradoxes of Whitening,* Long extended version of the Crypto 2004 rump session presentation, *Whitening the AES S-box,* Available at http://www.minrank.org/invglc_rump_c04.zip. Main theorem appears in Appendix B of the extended version of [7].
9. Nicolas T. Courtois, Klaus Schmeh, Jörg Drobick, Jacques Patarin, Maria-Bristena Oprisanu, Matteo Scarlata, Om Bhallamudi: *Cryptographic Security Analysis of T-310,* Monography study on the T-310 block cipher, 132 pages, received 20 May 2017, last revised 29 June 2018, https://eprint.iacr.org/2017/440.pdf
10. Nicolas Courtois, Jörg Drobick and Klaus Schmeh: *Feistel ciphers in East Germany in the communist era,* In Cryptologia, vol. 42, Iss. 6, 2018, pp. 427–444.
11. Tony Crilly: *The rise of Cayley's invariant theory (18411862),* In Historia Mathematica, Vol. 13, Iss. 3, August 1986, pp. 241–254
12. C. Harpes, G. Kramer, and J. Massey: *A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma,* Eurocrypt'95, LNCS 921, Springer, pp. 24–38.
13. C. Harpes, J. L. Massey: *Partitioning cryptanalysis,* In FSE 97, LNCS 1267, pp. 13–27, 1997.
14. Lars R. Knudsen, Matthew J. B. Robshaw: *Non-Linear Characteristics in Linear Cryptoanalysis,* Eurocrypt'96, LNCS 1070, Springer, pp. 224–236, 1996.
15. Referat 11: *Kryptologische Analyse des Chiffriergerätes T-310/50. Central Cipher Organ, Ministry of State Security of the GDR, document referenced as 'ZCO 402/80', a.k.a. MfS-Abt-XI-594, 123 pages, Berlin, 1980.*
16. *Klaus Schmeh: The East German Encryption Machine T-310 and the Algorithm It Used,* In Cryptologia, vol. 30, iss. 3, pp. 251–257, 2006.
17. Yosuke Todo, Gregor Leander, and Yu Sasaki: *Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM and Midori64,* In Journal of Cryptology, pp. 1–40, April 2018.