Can a Differential Attack Work for an Arbitrarily Large Number of Rounds?

Nicolas T. Courtois

University College London, UK

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

Dr. Nicolas T. Courtois

People, Problems, and Proofs

blog.bettercrypto.com

Cyber Security Challenge UK

UNIVERSITY CIPHER CHAMPION

March 2013


IARIA

International Academy, Research, and Industry Association

BEST PAPER AWARD

Multiplicative Complexity and Solving Generalized Brent Equations With SAT Solvers

By

Nicolas Courtois, Daniel Hulme, Theodosis Mourouzis

Presented during COMPUTATION TOOLS 2012, The Third International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking, held in Nice, France - July 22-27, 2012

IARIA Board

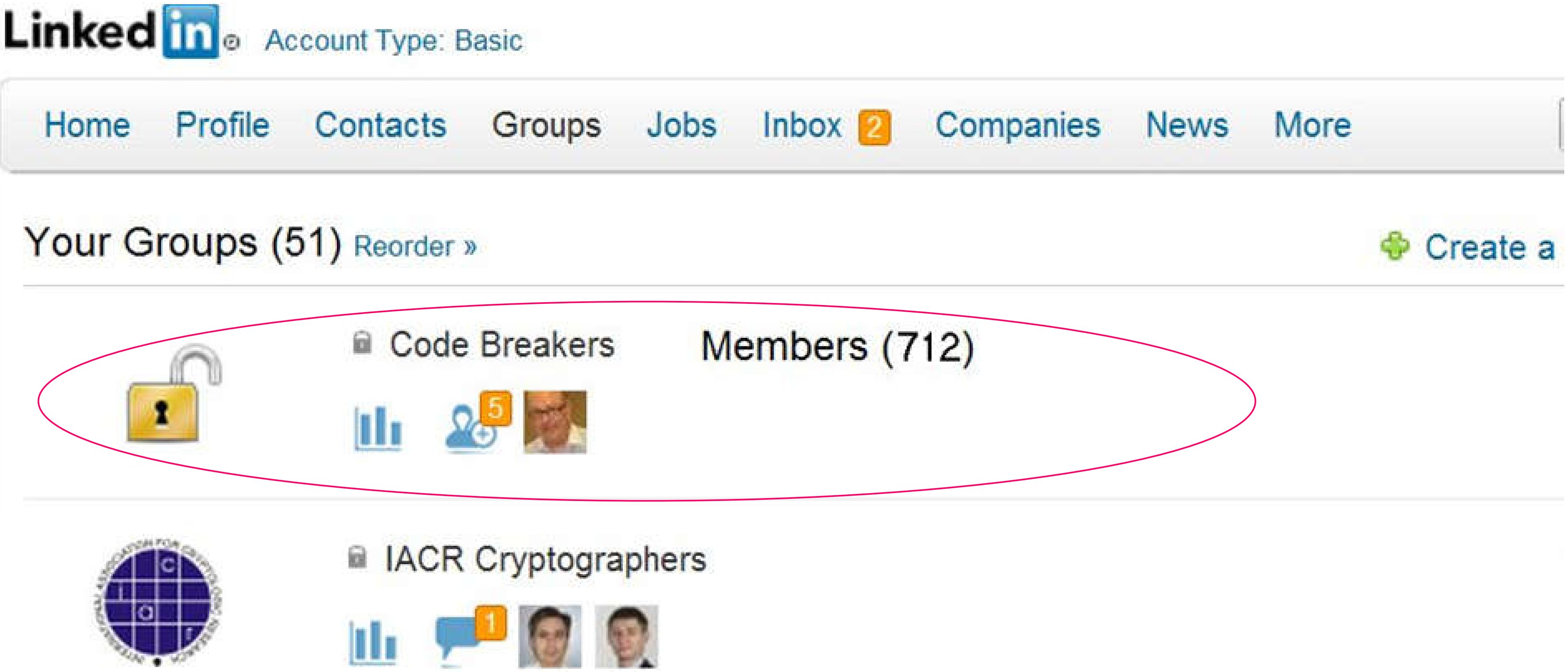
*not the official definition…

Cryptanalysis

=def=Making the impossible possible.

How? the Unexpected
and the Unlikely Happens

LinkedIn – Please Join!



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

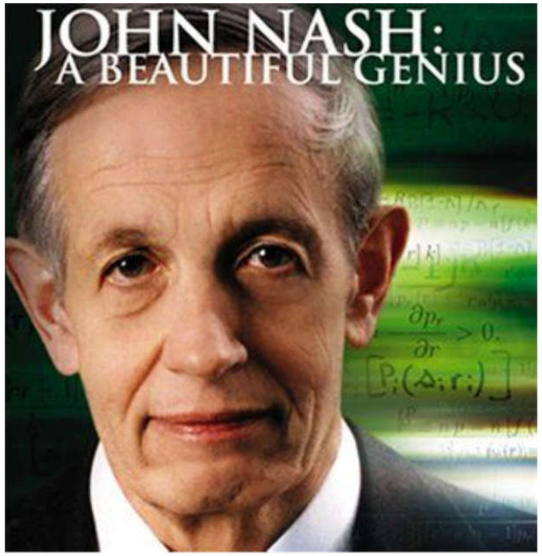
iterative differentials

- 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 of 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 USA 1970s

[…] 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!

Geheime Verschlußsache
MfS -020-Nr.: 747/73/Bl. 45

BSTU
000053

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

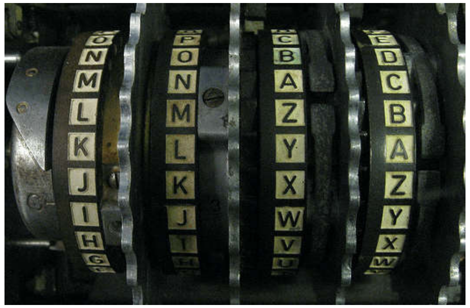
(1) $|\{x=(x_1,x_2,\cdots,x_6)\in\{0,1\}^6 \mid z(x)=0\}| = 2^5$

(2) $|\{x=(x_1,x_2,\cdots,x_6)\in\{0,1\}^6 \mid z(x)=0, \sum_{i=1}^{6} x_i = r\}| \approx \binom{6}{r}\cdot\frac{1}{2}$ $(r=0,1,\cdots,6)$

(3) $|\{x=(x_1,\cdots,x_6\}\in\{0,1\}^6 \mid z(x_1,x_2,\cdots,x_i,\cdots,x_6)=z(x_1,\cdots,x_i\oplus 1,\cdots,x_6)\}\approx 2^5$ $(i=1,2,\cdots,6)$

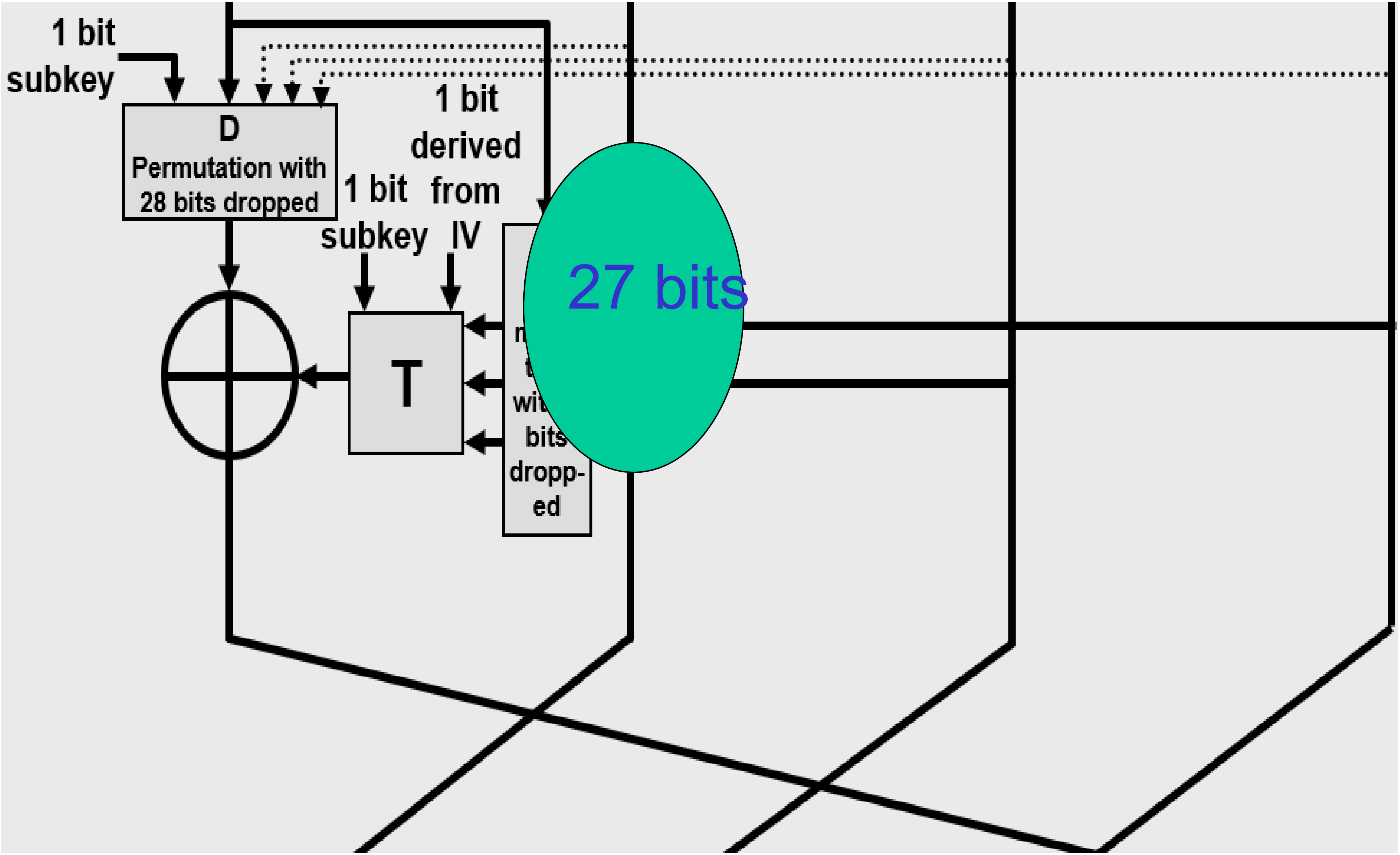
90% of Enigma Rotors 1938-1945

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



rotor name	Nb.	code	dates	$ImS(R)$	$Ent(R)$	Imk	possible differentials $k \to k$
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



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

LZS nb	bits which are not used in $P(j)$
716	1, 2, 10, 14, 15, 18, 22, 27, 35
722	2, 3, 6, 10, 13, 19, 23, 26, 31

Higher Order
DC

Computing HO Differentials for All Orders

Geheime Verschlußsache
MfS -020-Nr.: XI/493/76/Bl. 5

BSTU
0238

$$z^{(1)} = L + e_4 + e_3 e_4 + e_3 e_6 + e_4 e_5 + e_2 e_3 e_4 + e_2 e_3 e_5 + e_2 e_5 e_6 + e_2 e_3 e_4 e_5 + e_3 e_4 e_5 e_6$$

$$z^{(2)} = e_3 + e_5 + e_3 e_6 + e_4 e_6 + e_1 e_3 e_4 + e_1 e_3 e_5 + e_1 e_5 e_6 + e_3 e_4 e_6 + e_1 e_3 e_4 e_5$$

.
.
.

fast points!

$$z^{(134)} = L + e_2 + e_2 e_5 + e_5 e_6$$

$$z^{(135)} = e_2 + e_2 e_4 + e_4 e_6$$

$$z^{(136)} = L + e_4 e_5$$

$$z^{(1246)} = 0$$

$$z^{(1256)} = L$$

$$z^{(1345)} = e_2 + e_6$$

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:

"A cryptanalysis of PRINTcipher: The invariant subspace attack", Crypto 2011.

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:

"A cryptanalysis of PRINTcipher: The invariant subspace attack", Crypto 2011.

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.

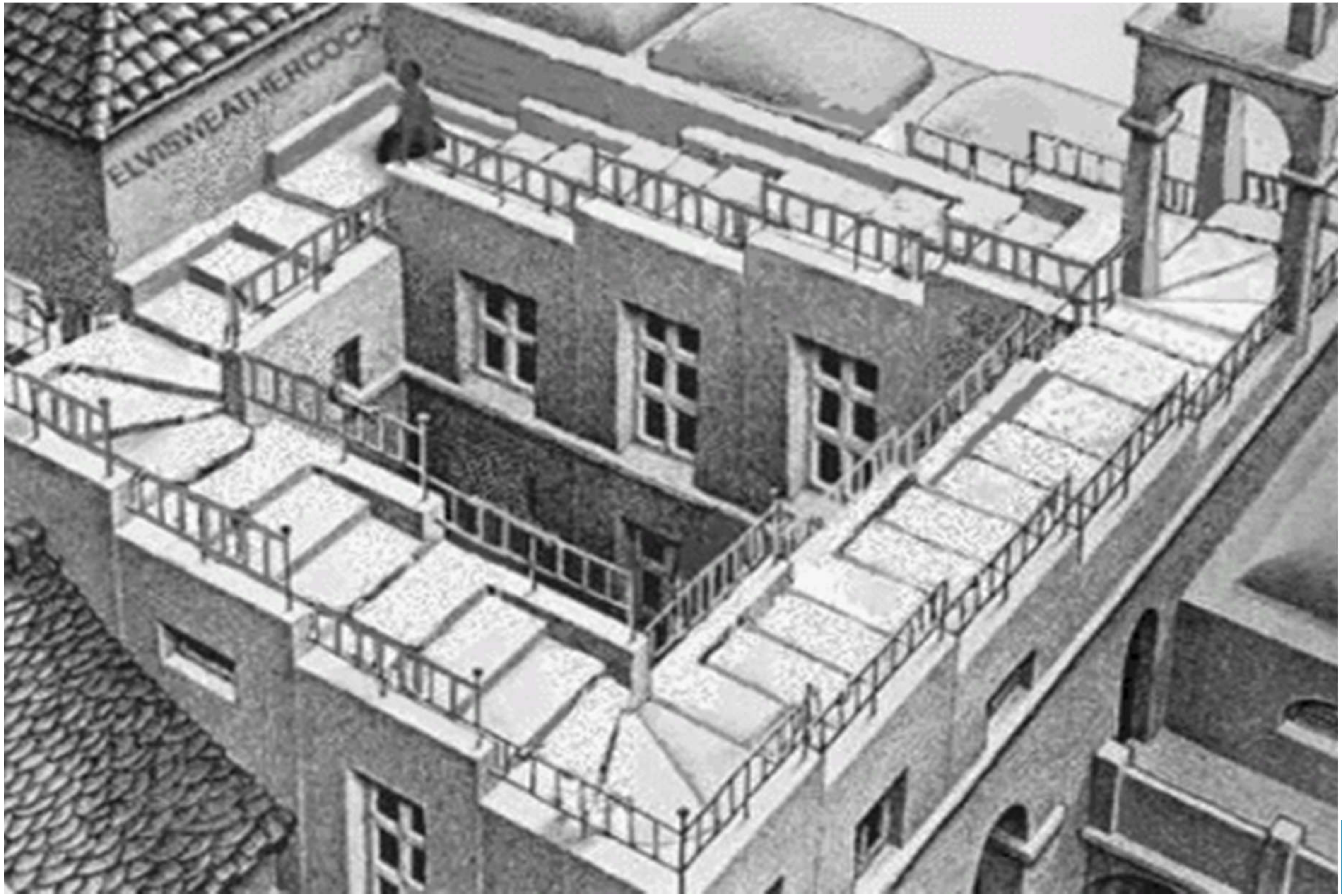
How? The Unexpected
and the Unlikely Happens

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



A
↧
B
↧
C
↧
D
~~↧~~ ?
A

Non-Markovian DC

- this paper –

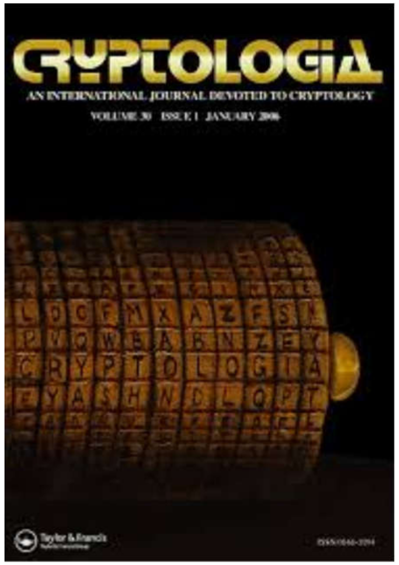
becomes eventually possible…

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:

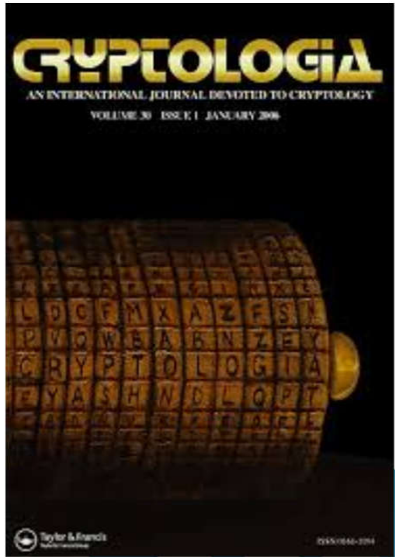
allowed Soviets to “read millions” of US messages [1989, Washington Post]

1970s

Modern block ciphers are born.

In which country??

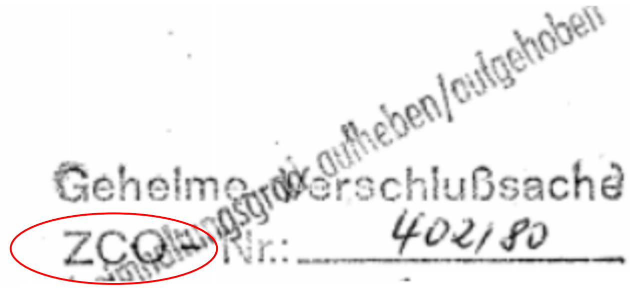
Who knows…



Our Sources

Communist Crypto Archives

MfS Abteilung 11 = **ZCO** =
Zentrales Chiffrierorgan
der DDR



Geheimhaltungsgrad aufheben/aufgehoben

Geheime Verschlußsache

ZCO Nr.: 402/80

10. Ausf. 123 Blatt

10.12.90

BStU

000001

BStU = Stasi Records Agency

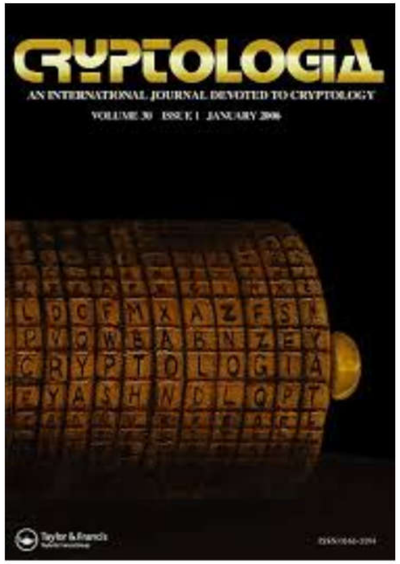
Kryptologi [redacted] Analyse

des Chiffrie [redacted] ätes T 310/50

More details:

- 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.

Eastern Bloc ciphers: a LOT more complex…

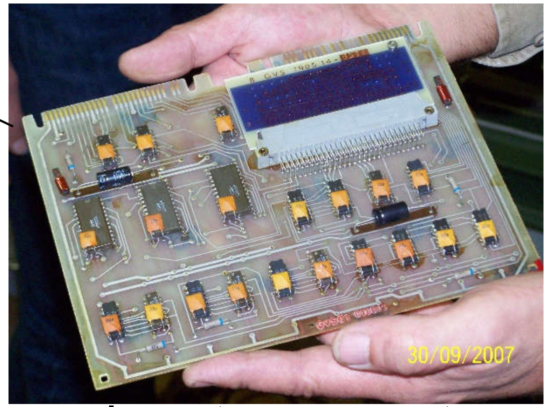


East German T-310

240 bits

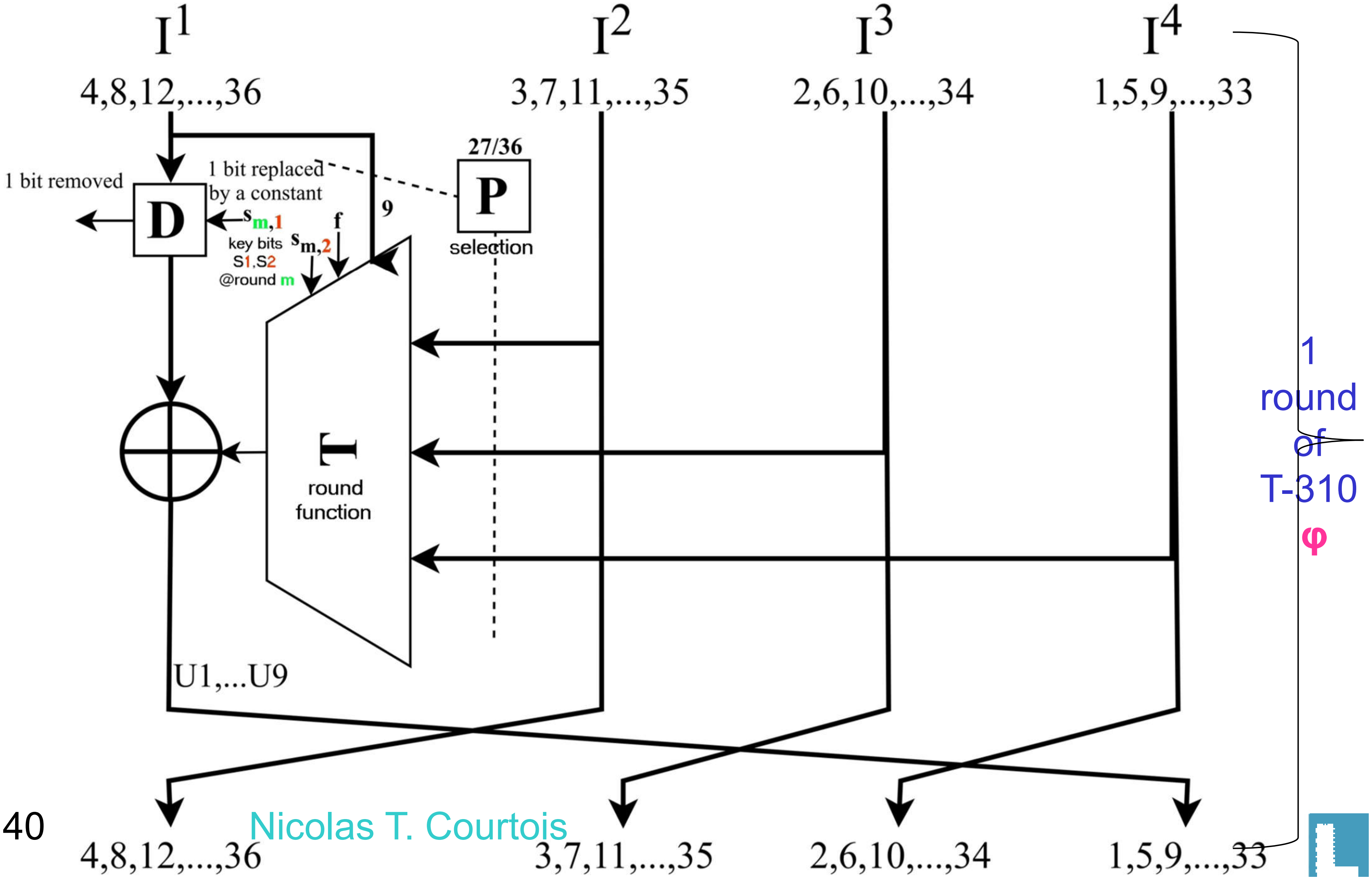
"quasi-absolute security"
[1973-1990]

has a
physical
RNG=>IV



long-term secret
90 bits only!

Contracting Feistel [1970s Eastern Germany!]



Linear Cryptanalysis (LC)

LC “Official” History

- Davies-Murphy attack [1982=classified, published in 1995] = early LC
- Shamir Paper [1985]……… early LC

LC “Official” History

- Linear Cryptanalysis: Gilbert and Matsui [1992-93]

LC at ZCO - 1976!

Definition 3.1-1

$$\Delta_\alpha^g = 2^{n-1} - \| g(x) + (\alpha, x) \| \quad \forall \alpha \in \overline{0, 2^n - 1} .$$

$\| g \| \underset{\text{Def.}}{=} \sum_x g(x)$ $\qquad (\alpha, x) = \sum_{i=1}^{n} \alpha_i x_i$

Geheime Verschlußsache
MfS -020-Nr.: XI/493/76/ Bl. 18

BSTU
0251

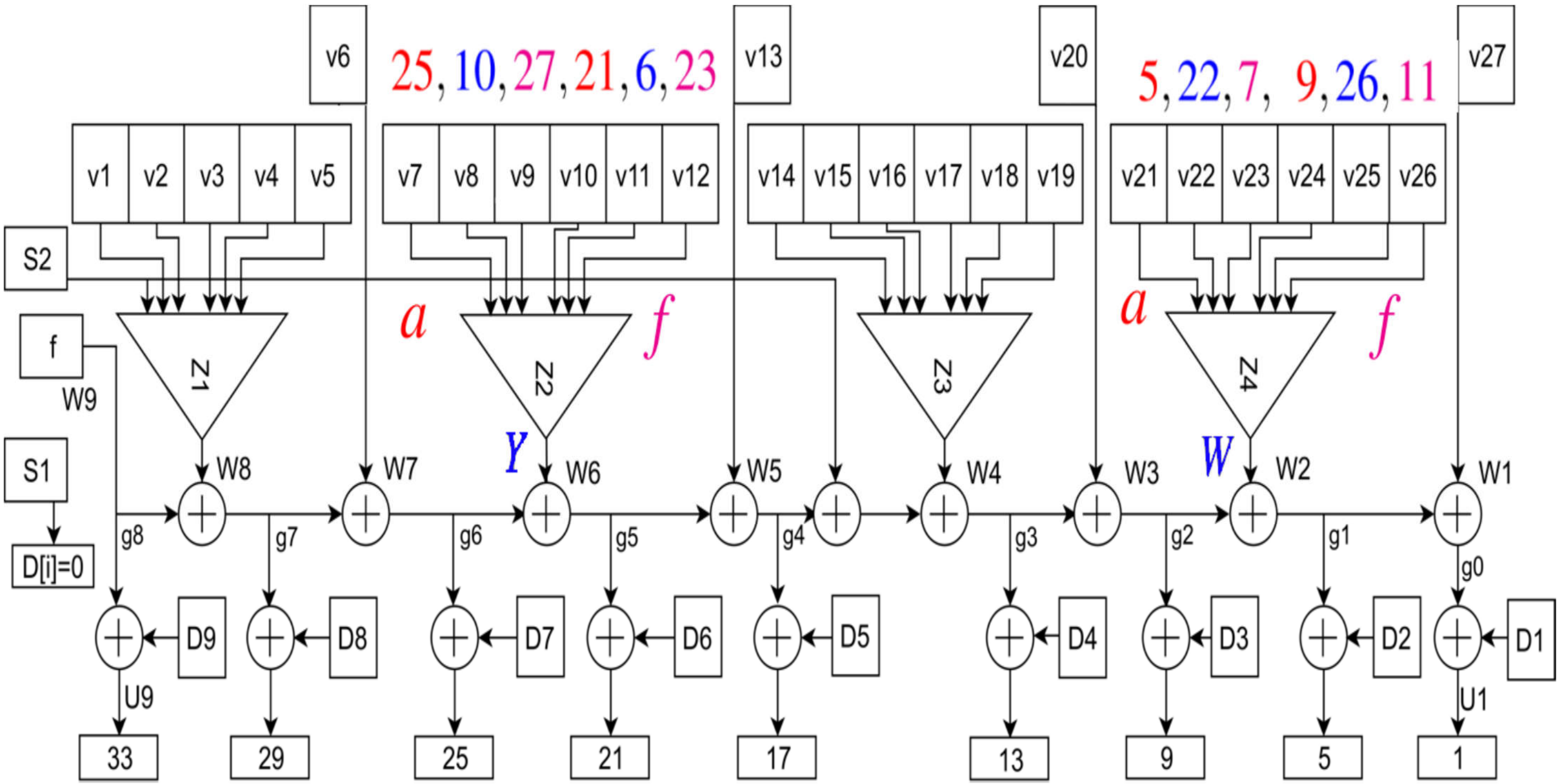
Ergebnisse:

Sei t die Anzahl der Übereinstimmungen der Funktionswerte von z.

Tabelle 3.1-2

α	Δ_α^z	t	α	Δ_α^z	t
0 0 0 0 0 0	~~32~~ 0	32	L 0 0 0 0 0	0	32
0 0 0 0 0 L	2	34	L 0 0 0 0 L	6	38
0 0 0 0 L 0	-4	28	L 0 0 0 L 0	0	32
0 0 0 0 L L	6	38	L 0 0 0 L L	6	38
0 0 0 L 0 0	-4	28	L 0 0 L 0 0	-4	28
0 0 0 L 0 L	-2	30	L 0 0 L 0 L	2	34
0 0 0 L L 0	0	32	L 0 0 L L 0	4	36
0 0 0 L L L	2	34	L 0 0 L L L	2	34

Inside T-310 Round φ



Nicolas T. Courtois

LC at ZCO - 1976!

Definition 3.1-1

$$\Delta_\alpha^g = 2^{n-1} - \| g(x) + (\alpha, x) \| \quad \forall \alpha \in \overline{0, 2^n - 1} .$$

$\|g\| \underset{\text{Def.}}{=} \sum_x g(x)$ $\qquad (\alpha, x) = \sum_{i=1}^{n} \alpha_i x_i$

Geheime Verschlußsache
MfS -020-Nr.: XI/493/76/ Bl. 18

BSTU
0251

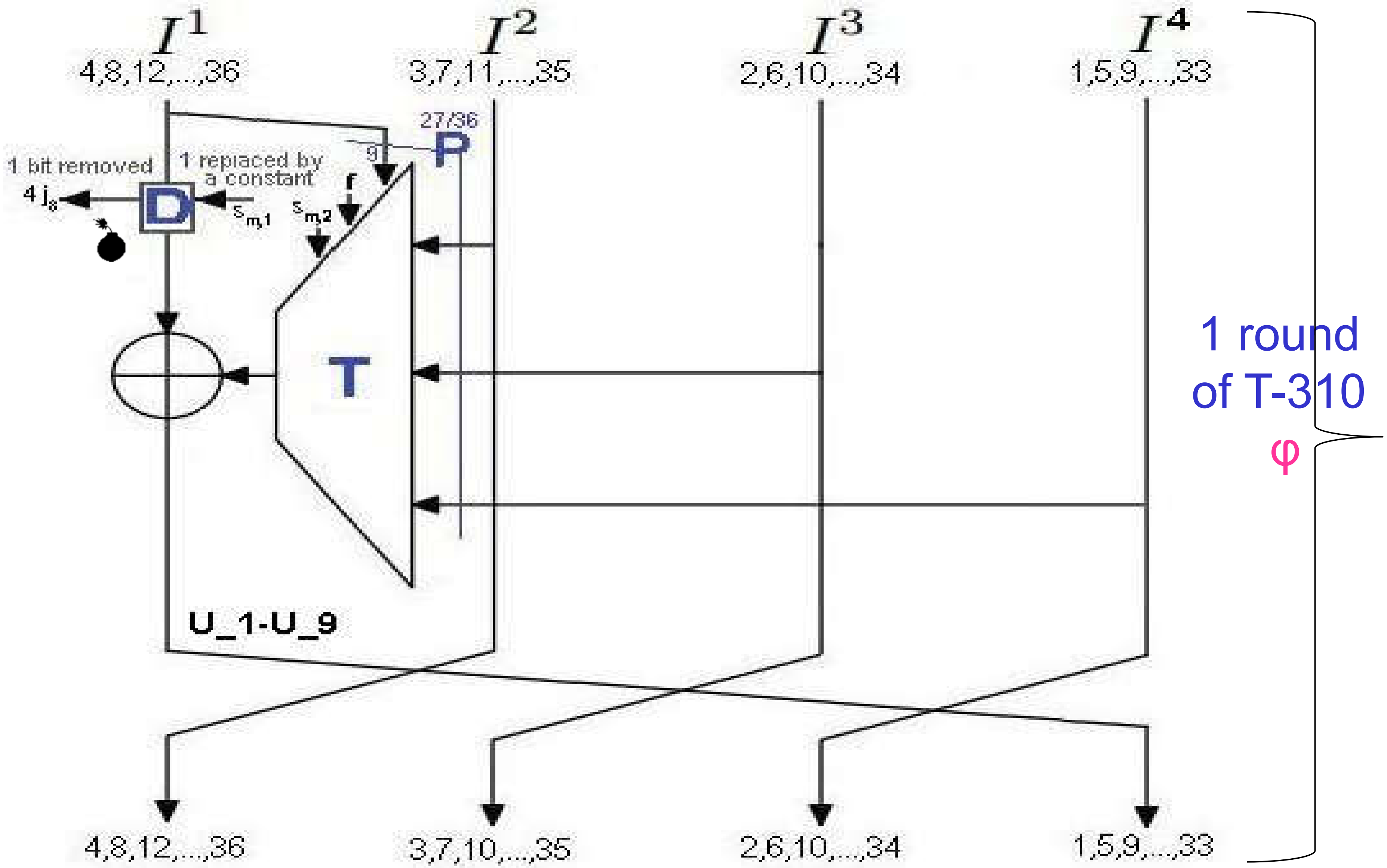
Ergebnisse:

Sei t die Anzahl der Übereinstimmungen der Funktionswerte von z.

Tabelle 3.1-2

α	Δ_α^z	t	α	Δ_α^z	t
0 0 0 0 0 0	~~32~~ 0	32	L 0 0 0 0 0	0	32
0 0 0 0 0 L	2	34	L 0 0 0 0 L	6	38
0 0 0 0 L 0	-4	28	L 0 0 0 L 0	0	32
0 0 0 0 L L	6	38	L 0 0 0 L L	6	38
0 0 0 L 0 0	-4	28	L 0 0 L 0 0	-4	28
0 0 0 L 0 L	-2	30	L 0 0 L 0 L	2	34
0 0 0 L L 0	0	32	L 0 0 L L 0	4	36
0 0 0 L L L	2	34	L 0 0 L L L	2	34

Contracting Feistel [1970s Eastern Germany!]



How to Backdoor T-310 [Cryptologia 42@2018]

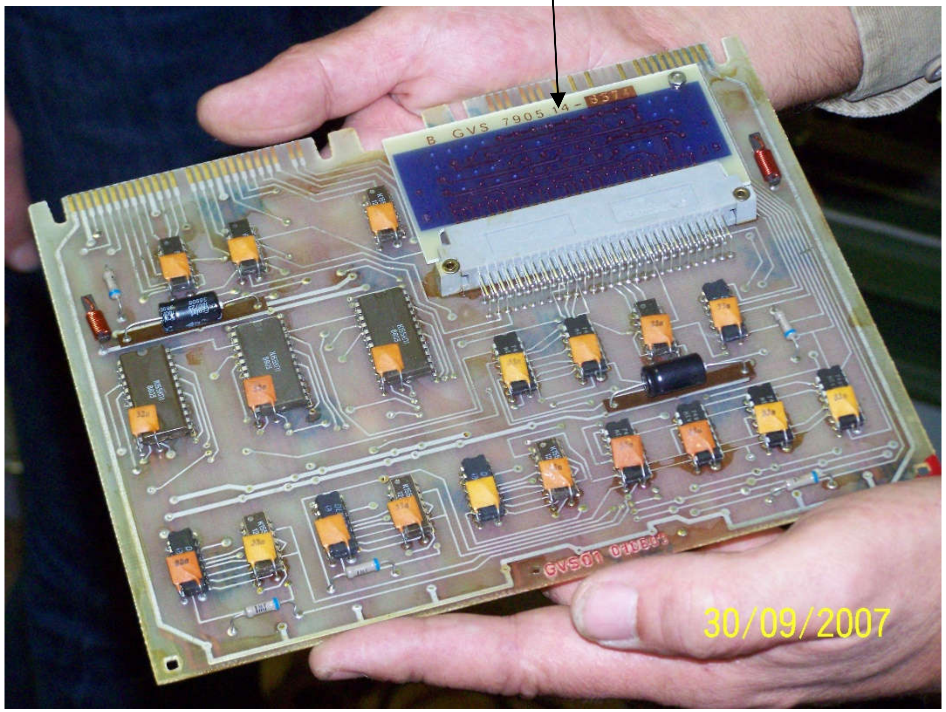
omit just 1 out of 40 conditions:

$$D \text{ and } P \text{ are injective}$$
$$P(3)=33, P(7)=5, P(9)=9, P(15)=21, P(18)=25, P(24)=29$$
$$\text{Let } W=\{5,9,21,25,29,33\}$$
$$\forall_{1\geq i\geq 9} D(i)\notin W$$
$$\alpha \notin W$$
$$\text{Let } T=(\{0,1,\ldots,12\}\backslash W)\cap(\{P(1),P(2),\ldots,P(24)\}\cup\{D(4),D(5),\ldots,D(9)\}\cup\{\alpha\})$$
$$\text{Let } U=(\{13,\ldots,36\}\backslash W)\cap(\{P(26),P(27)\}\cup\{D(1),D(2),D(3)\})$$
$$|T\backslash\{P(25)\}|+|U\backslash\{P(25)\}|\leq 12$$
$$A=\{D(1),D(2),D(3),D(4),D(5),D(6),D(7),D(8),D(9)\}\cup\{P(6),P(13),P(20),P(27)\}$$
$$A_1=\{D(1),D(2)\}\cup\{P(27)\}$$
$$A_2=\{D(3),D(4)\}\cup\{P(20)\}$$
$$A_3=\{D(5),D(6)\}\cup\{P(13)\}$$
$$A_4=\{D(7),D(8)\}\cup\{P(6)\}$$
$$\forall(i,j)\in\{1,\ldots,27\}\times\{1,\ldots,9\}: P_i\neq D_j$$
$$\exists j_1\in\{1,\ldots,7\}: D_{j_1}=0$$
$$\{D(8),D(9)\}\subset\{4,8,\ldots,36\}\subset A$$
$$\forall(i,j)\in\overline{1,27}\times\overline{1,9}: P_i\neq D_j$$
$$\exists j_1\in\overline{1,7}: D_{j_1}=0$$
$$\{D_8,D_9\}\subset\{4,8,\ldots,36\}\subset A$$
$$\exists(j_2,j_3)\in(\{j\in\overline{1,4}|D_j?\notin A_j\})^2\wedge$$
$$\exists(j_4,j_5)\in(\overline{1,4}\backslash\{j_1,2j_2-1,2j_2\})\times(\overline{5,8}\backslash\{j_1,2j_2-1,2j_2\})\wedge$$
$$\exists j_6\in\overline{1,9}\backslash\{j_1,2j_2-1,2j_2,j_4,j_5\}:$$
$$j_2\neq j_3\wedge\{4j_4,4j_5\}\subset A_{j_2}\wedge$$
$$A_{j_2}\cap(\overline{4j_1-3,4j_1}\cup\overline{4j_6-3,4j_6})\neq\emptyset\wedge$$
$$\{8j_2-5,8j_2\}\subset A_{j_3}\wedge A_{j_3}\cap(\overline{4j_1-3,4j_1}\cup\overline{4j_6-3,4j_6})\neq\emptyset;$$
$$\{D(9)\}\setminus(\overline{33,36}\cup\{0\})\neq\emptyset$$
$$\{D(8),D(9),P(1),P(2),\ldots,P(5)\}\setminus(\overline{29,32}\cup\{0\})\neq\emptyset$$
$$\{D(7),D(8),P(1),P(2),\ldots,P(6)\}\setminus(\overline{25,32}\cup\{0\})\neq\emptyset$$
$$\{D(7),D(9),P(1),P(2),\ldots,P(6)\}\setminus(\overline{25,28}\cup\overline{33,36}\cup\{0\})\neq\emptyset$$
$$\{D(6),D(7),D(8),D(9),P(1),P(2),\ldots,P(12)\}\setminus(\overline{21,36}\cup\{0\})\neq\emptyset$$
$$\{D(5),D(7),D(8),D(9),P(1),P(2),\ldots,P(13)\}\setminus(\overline{17,20}\cup\overline{25,36}\cup\{0\})\neq\emptyset$$
$$\{D(7),D(8),D(9),P(1),P(2),\ldots,P(6)\}\setminus(\overline{25,36}\cup\{0\})\neq\emptyset$$
$$\{D(5),D(6),D(8),D(9),P(1),P(2),\ldots,P(13)\}\setminus(\overline{17,24}\cup\overline{29,36}\cup\{0\})\neq\emptyset$$
$$\{D(5),D(6),D(7),D(9),P(1),P(2),\ldots,P(13)\}\setminus(\overline{17,28}\cup\overline{33,36}\cup\{0\})\neq\emptyset$$
$$\{D(5),D(6),D(7),D(8),P(1),P(2),\ldots,P(13)\}\setminus(\overline{17,32}\cup\{0\})\neq\emptyset$$
$$\{D(5),D(6),D(7),D(8),D(9),P(1),P(2),\ldots,P(13)\}\setminus(\overline{17,36}\cup\{0\})\neq\emptyset$$
$$\{D(4),D(5),\ldots,D(9),P(1),P(2),\ldots,P(19)\}\setminus(\overline{13,36}\cup\{0\})\neq\emptyset$$
$$\{D(3),D(4),\ldots,D(9),P(1),P(2),\ldots,P(20)\}\setminus(\overline{9,36}\cup\{0\})\neq\emptyset$$

plus the "Matrix $rank = 9$ condition" M_9 defined in Section D.4 below.

ciphertext-only attacks!

bad long-term key



Generalized Linear Cryptanalysis (GLC)

[Harpes, Kramer and Massey, Eurocrypt'95]

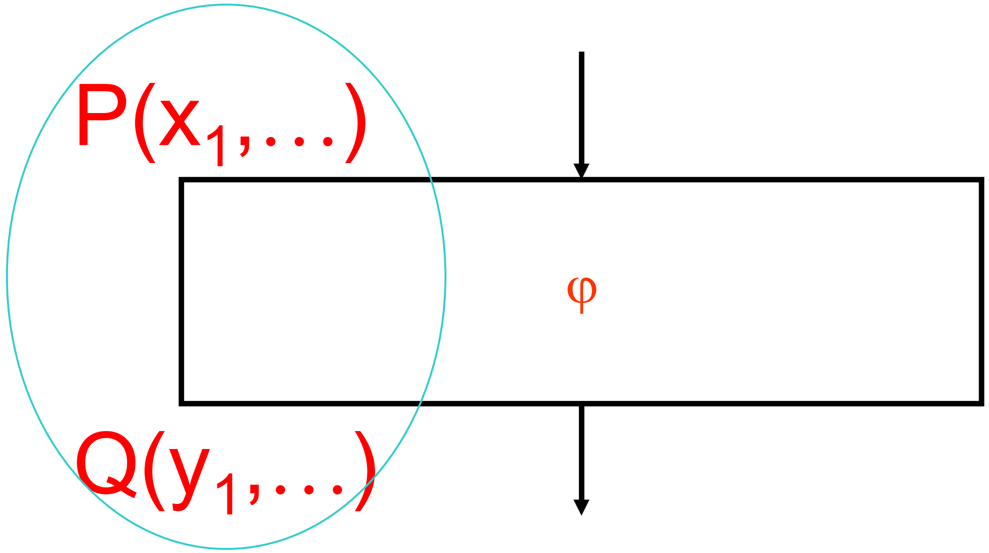
Scope

We study how an encryption function φ of a block cipher acts on polynomials.

Stop, this is extremely complicated???

Main Problem:

Two polynomials P => Q.



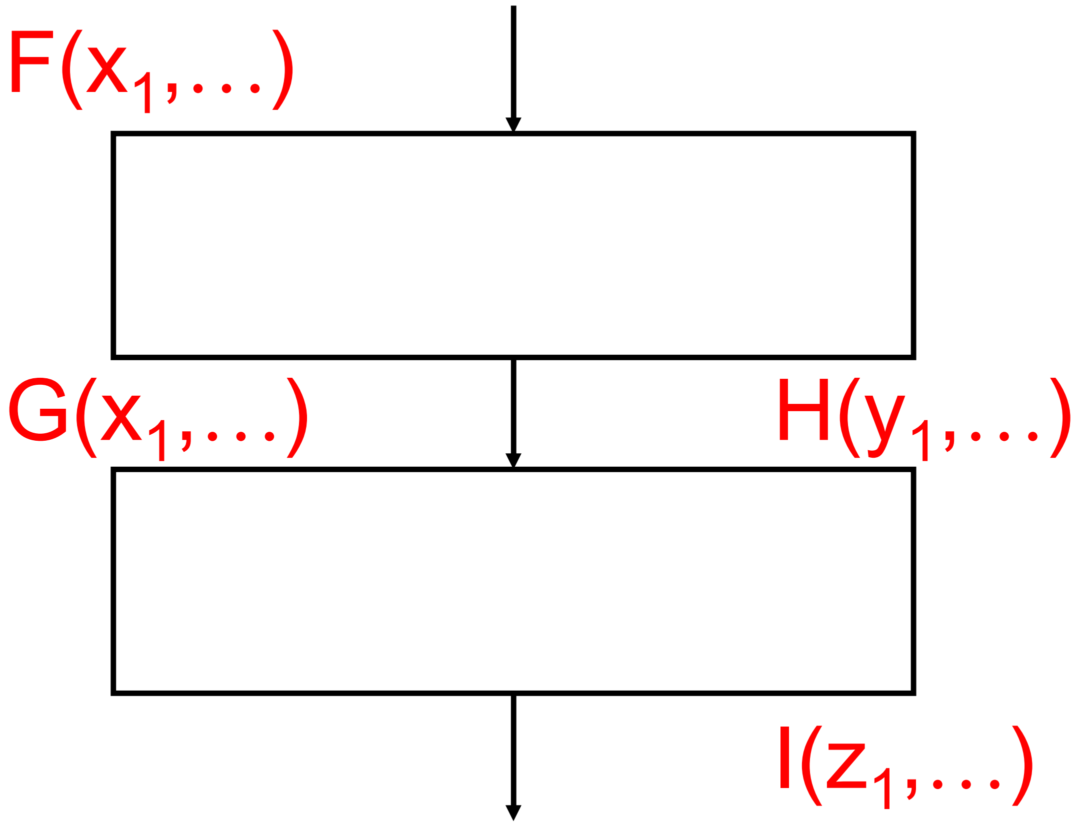
is P=Q possible??

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

Connecting Non-Linear Approxs.

Black-Box Approach [Popular]

Non-linear functions.



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

$$(*)\quad \begin{aligned} & L_0[3,8,14,25] \oplus L_0[3]R_0[16,17,20] \oplus R_0[17] \oplus \\ & L_{11}[3,8,14,25] \oplus L_{11}[3]R_{11}[16,17,20] \oplus R_{11}[17] = \\ & K[sth] + K[sth']L_0[3] + K[sth'']L_{11}[3] \end{aligned}$$

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

Phase transition: eprint/2018/1242.

- When $\mathcal{P}$ degree grows, attacks become a LOT easier.
- The more polynomials you multiply, the better.

Better Is Enemy of Good!

DES = Courtois @Crypto 2004 :

$$\frac{1}{2} \pm 1.91 \cdot 2^{-16}$$ $\mathscr{P}$ deg 1

$$\downarrow$$

$$\frac{1}{2} \pm 1.2 \cdot 2^{-15}$$ $\mathscr{P}$ deg 2

$$\downarrow$$

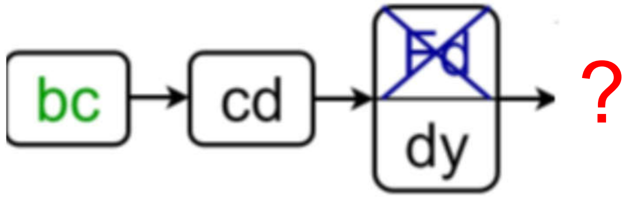
proba=1.0 $\mathscr{P}$ deg 10

White Box Cryptanalysis

[Courtois 2018]

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

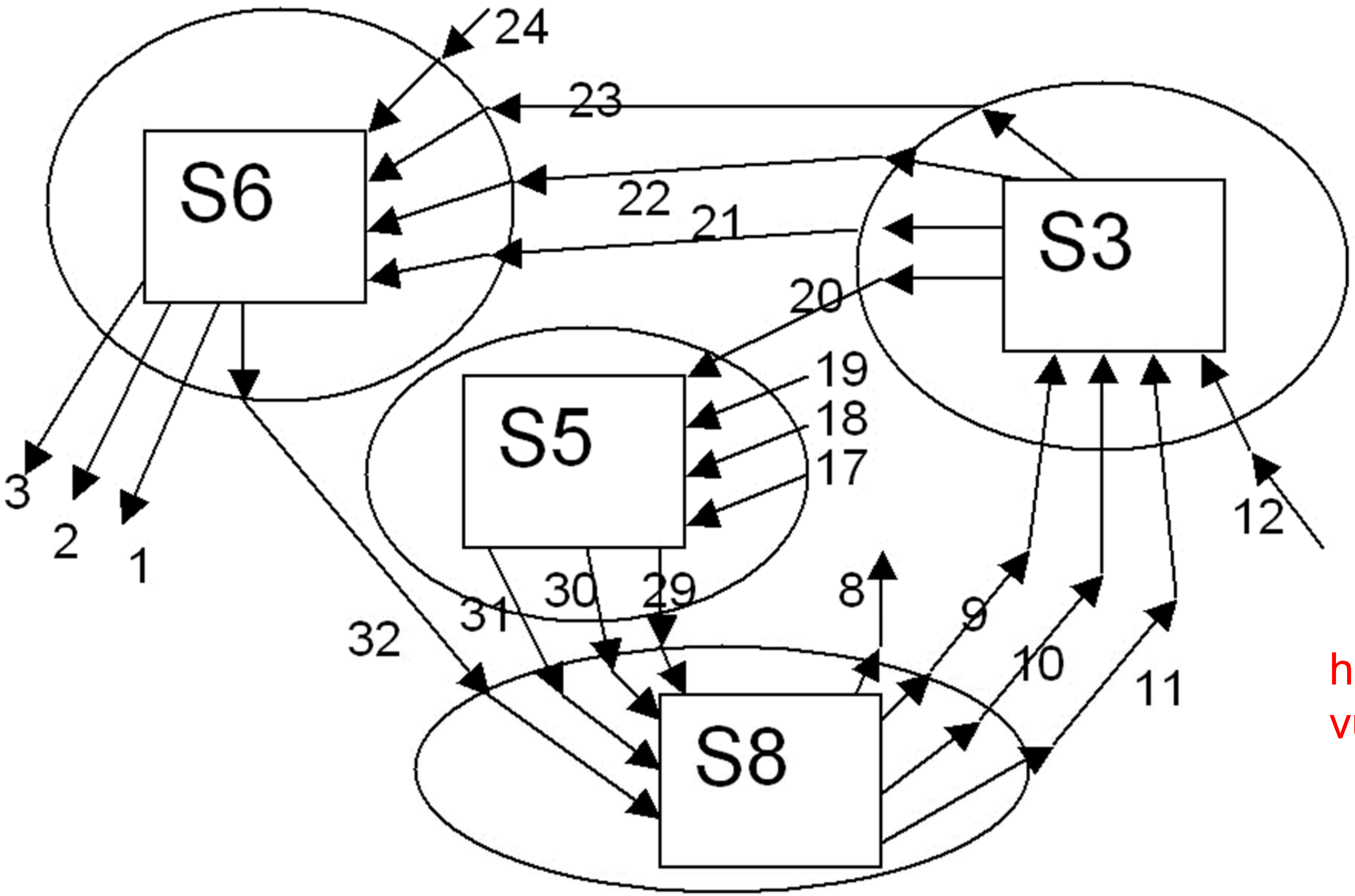
formal equality of 2 polynomials.



2. Closed Loops*

* informally, walks on cycles with simple polynomials, see our paper @ICISC 2019

Closed Loops - GOST



highly vulnerable!

ICISC 2019:

we generalized

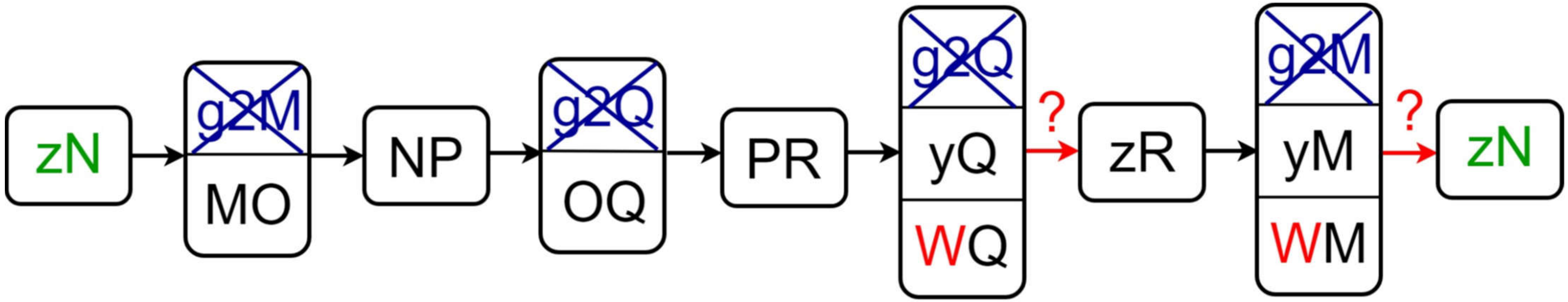
the concept of closed loops

sets of bits

=>

sets of cycles on polynomials

constructing invariants



annihilation

g2*(M+Q) = 0

4 terms are gone!

Imperfect Transitions:

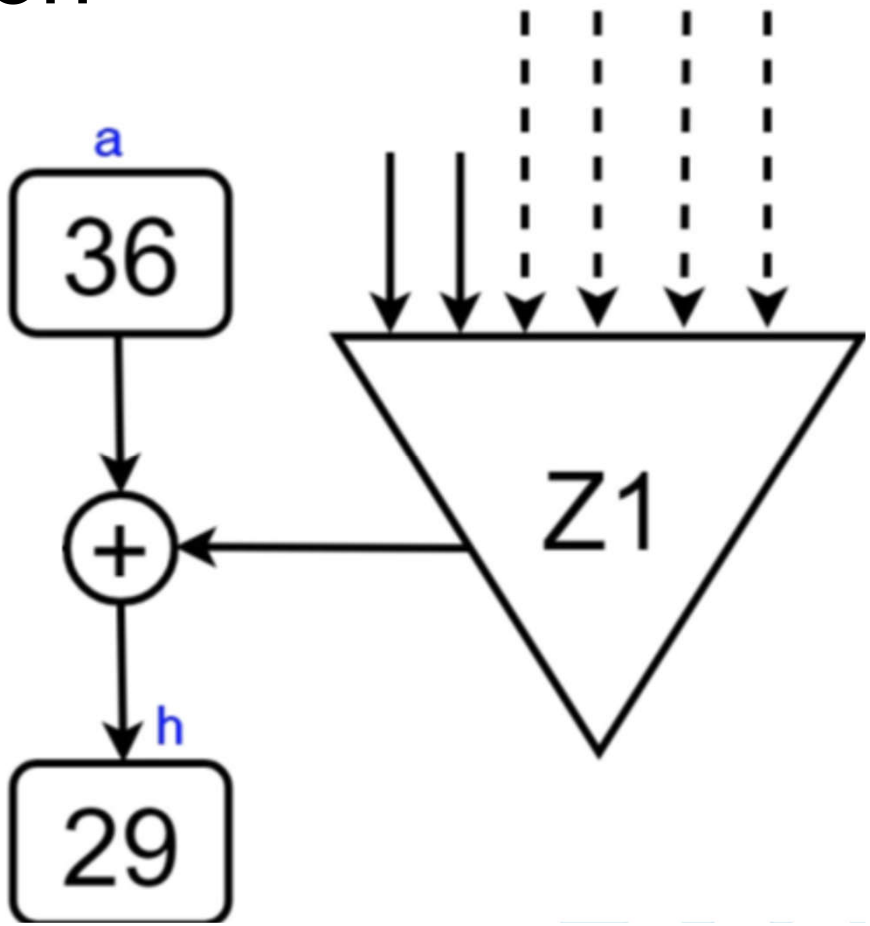
we allow

addition of arbitrary non-non-linear functions

=> annihilated later

Z1() * L2() = 0

for any input



@eprint/2018/1242

Big Winner

“product attack”

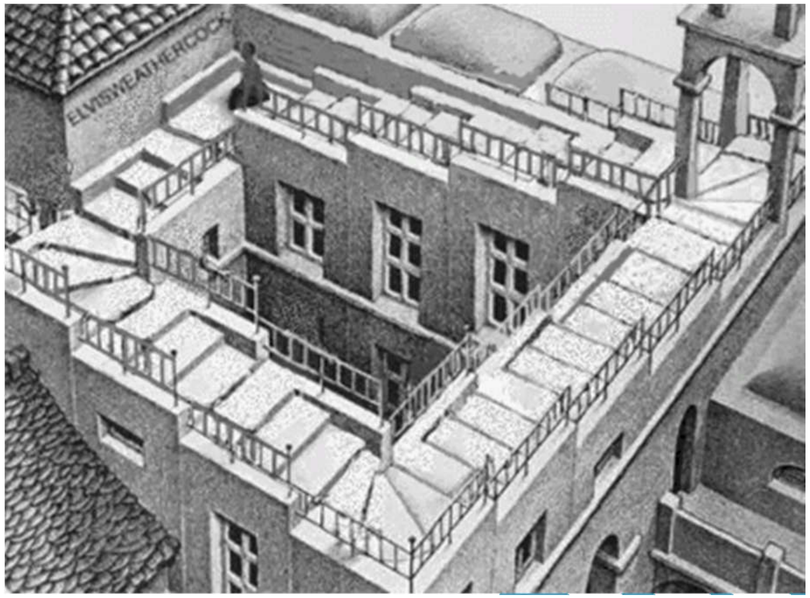
=we multiply Boolean polynomials=

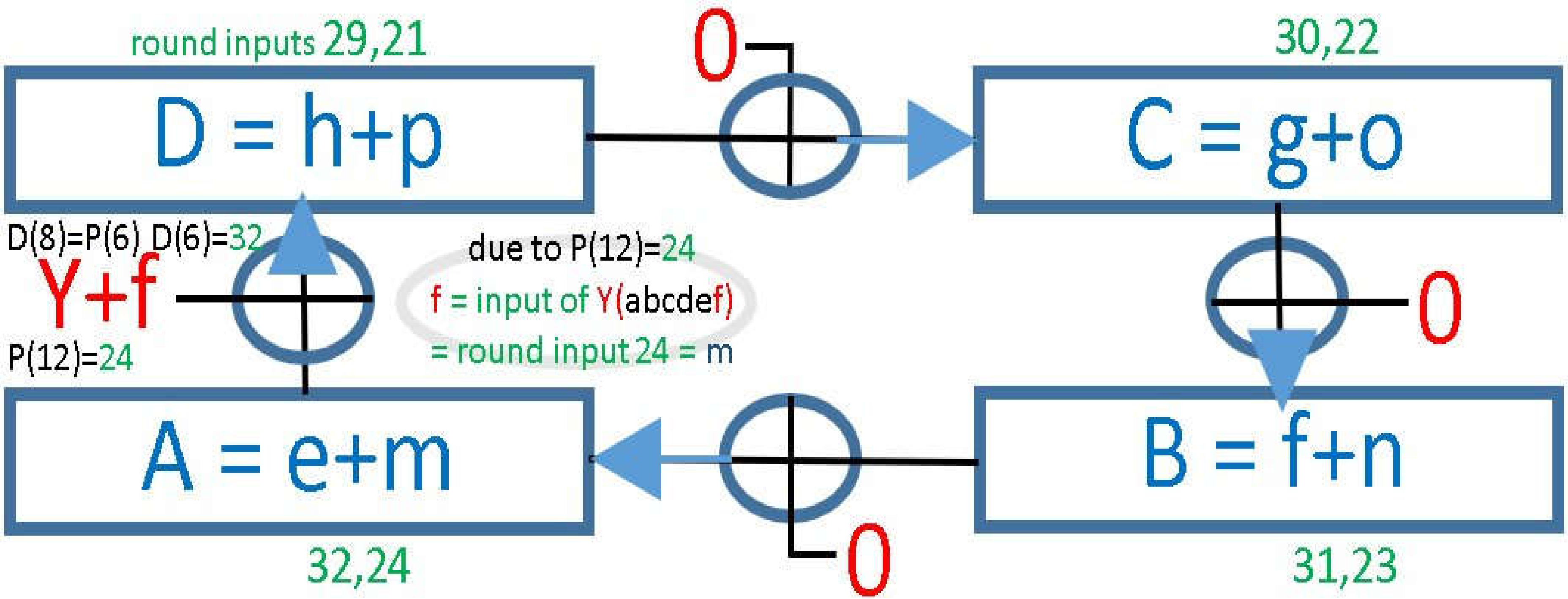
Impossible?

"Only those who attempt the absurd will achieve the impossible."

-- M. C. Escher

$$D \to C \to B \to A \overset{?}{\to} D$$



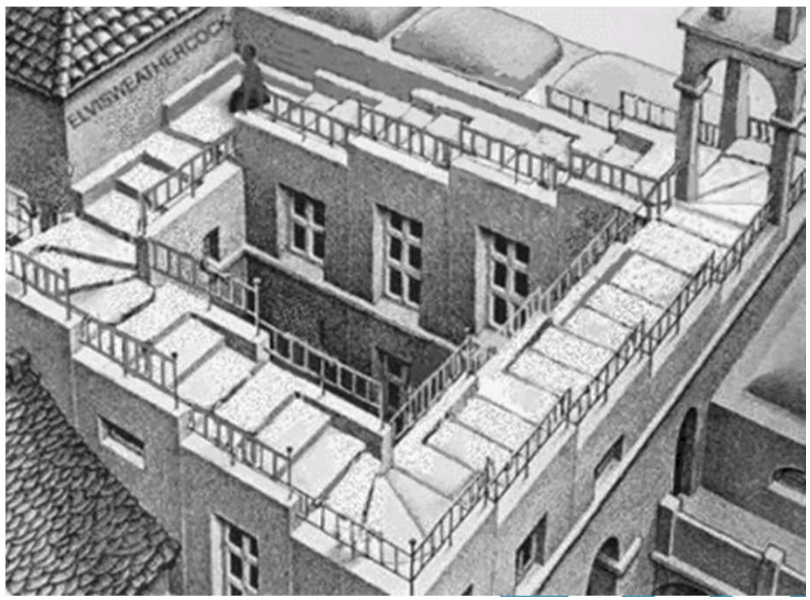


cycles -

attack on T-310

(ICISC 2019 Thm. 6.2.)

(Y+f)*B*C*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:

$$FE = BCDFGH \cdot ((Y + E)W(.) + AY(.))$$

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.

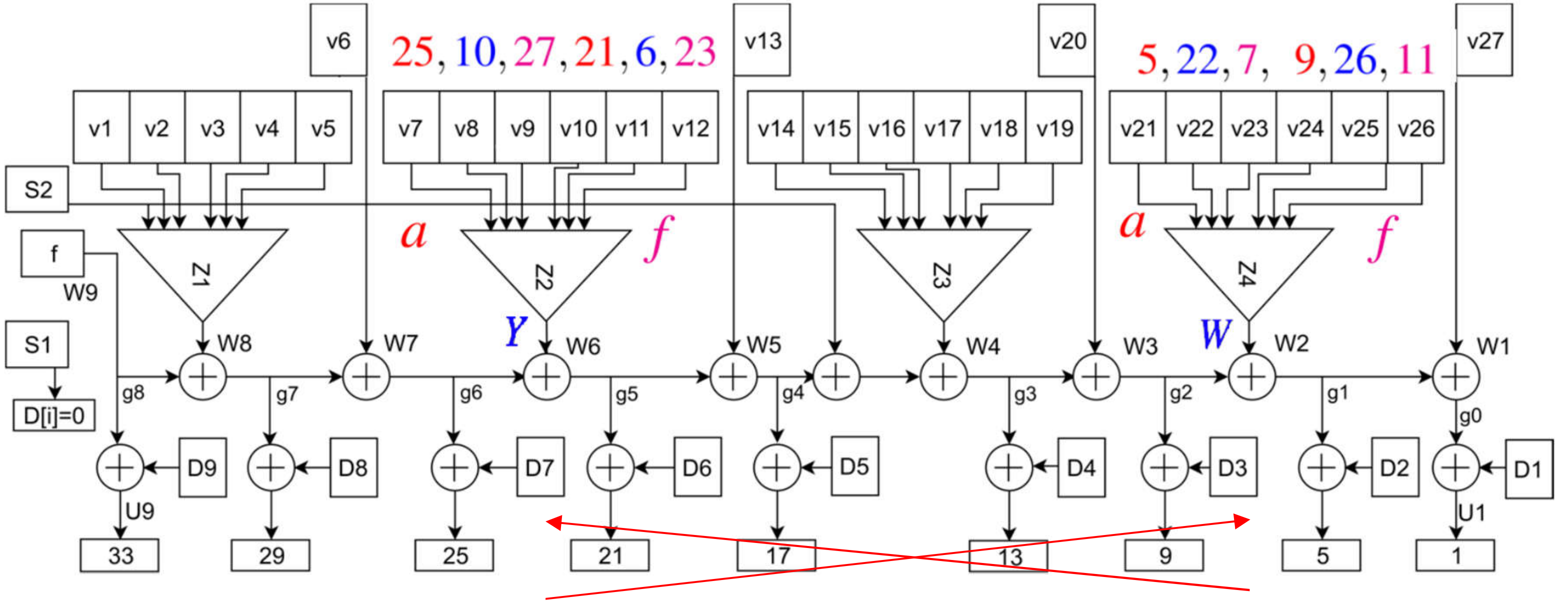
- not in general, just in some cases
  [so hard to detect!]

Main Theorem

IF

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

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



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

Main Theorem

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

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

AND

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

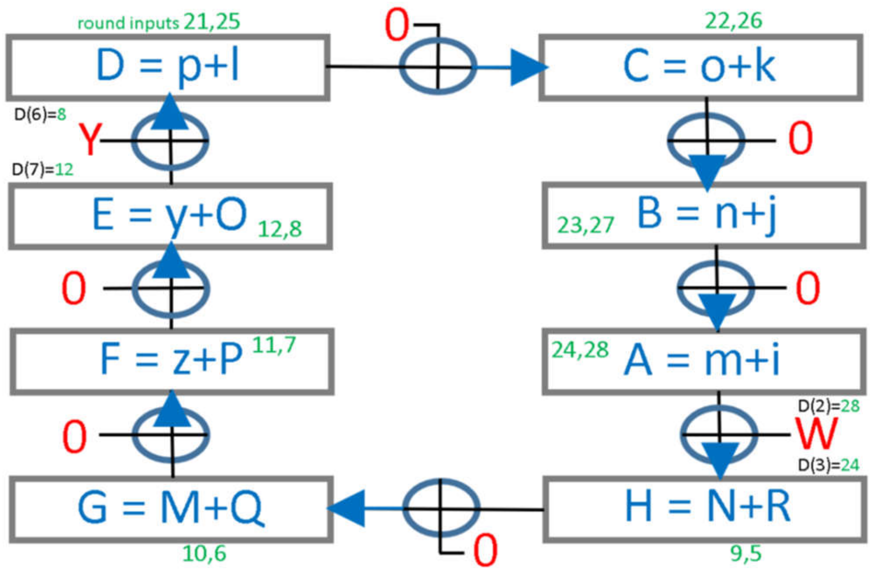
$P(7)$ $P(12)$

$$Z(a+d)(b+e)(c+f) = 0 \qquad = Y(D)(G)(B) \qquad = W(H)(C)(F)$$

$P(21)$ $P(26)$

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

THEN



1..64 hard DC

Main Theorem

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

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

AND

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

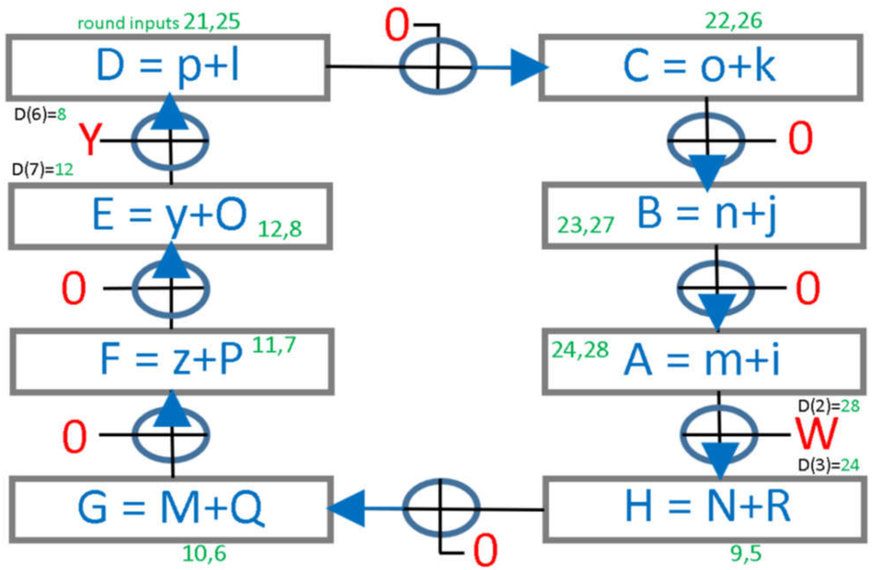
$P(7)$ $P(12)$

$$Z(a+d)(b+e)(c+f) = 0 \quad = Y(D)(G)(B) \quad = W(H)(C)(F)$$

$P(21)$ $P(26)$

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

THEN



1..64 hard DC

64..∞ easy!

+ product pty!

Experiments – 3 different Boolean Functions

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

- typical

rounds	8	16	24	32	40	48	56	64
proba	$2^{-2.40}$	$2^{-4.82}$	$2^{-6.74}$	$2^{-7.71}$	$2^{-7.95}$	$2^{-7.99}$	$2^{-8.00}$	$2^{-8.00}$

- very weak

rounds	8	32	128	2048
proba	$2^{-1.1}$	$2^{-3.0}$	$2^{-5.5}$	$2^{-7.7}$

- Stronger

rounds	8	16	24	32	40	48	56	64
proba	$2^{-4.53}$	$2^{-7.51}$	$2^{-7.98}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$

Experiments – 3 different Boolean Functions

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

- typical

rounds	8	16	24	32	40	48	56	64
proba	$2^{-2.40}$	$2^{-4.82}$	$2^{-6.74}$	$2^{-7.71}$	$2^{-7.95}$	$2^{-7.99}$	$2^{-8.00}$	$2^{-8.00}$

- very weak

- Stronger

rounds	8	16	24	32	40	48	56	64
proba	$2^{-4.53}$	$2^{-7.51}$	$2^{-7.98}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$

- 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 → nothing detected in short run

of Markov cipher property

- e.g. CHAM cipher of ICISC 2019