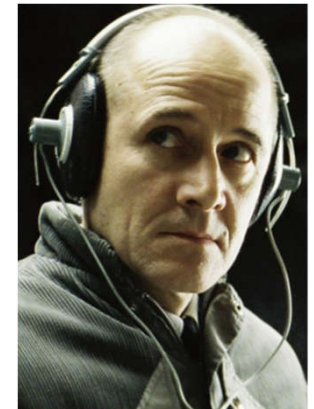


Block Ciphers: Lessons from the Cold War



Nicolas T. Courtois
University College London, UK

Topics:

Part 1: **Lessons** from Cold War

Part 2: **NonLinear** Cryptanalysis

- Attacks with polynomial **invariants**
 - Product attack [**P*Q*R*...**] = very powerful

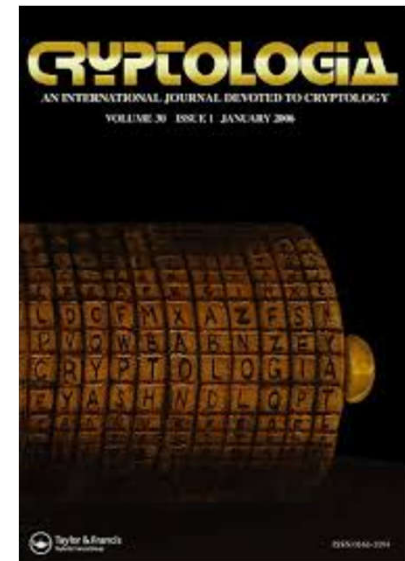
Topics:

Part 1: Lessons from Cold War: see

- Nicolas Courtois, Jörg Drobick and Klaus Schmeih:
"Feistel ciphers in East Germany in the communist era,"
In Cryptologia, vol. 42, Iss. 6, 2018, pp. 427-444.

Part 2: NonLinear Cryptanalysis:

- Attacks with polynomial invariants
 - Product attack [$P*Q*R*...$] = very powerful
- References:
 - Courtois @Crypto 2004
 - (NEW) [eprint/2018/1242](https://eprint.iacr.org/2018/1242)
 - few more...



Dr. Nicolas T. Courtois

People,
Problems,
and Proofs



blog.bettercrypto.com



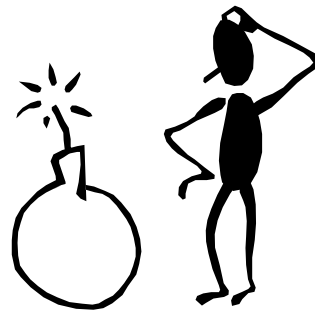
UNIVERSITY CIPHER CHAMPION

March 2013



Question 1:

Why **0%** of symmetric encryption
used in practice are
provably secure?



Provably Secure Encryption!

Based on MQ Problem.

Dense MQ is VERY hard.

- top of the top hard problem.
- for both standard and PQ crypto

Best attack $\approx 2^{0.8765n}$

mqchallenge.org FXL/Joux 2017/372

=> Allows to build a provably secure stream cipher based on MQ directly!

C. Berbain, H. Gilbert, and J. Patarin:

[QUAD: A Practical Stream Cipher with Provable Security](#), Eurocrypt 2005

Question 2:

Why researchers have found
so few attacks on block ciphers?

Question 2:

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? two very large
polynomials are simply **equal**



LinkedIn


LinkedIn  Account Type: Basic

[Home](#) [Profile](#) [Contacts](#) [Groups](#) [Jobs](#) [Inbox](#) **2** [Companies](#) [News](#) [More](#)

Your Groups (51) [Reorder »](#)

[+ Create a](#)



 Code Breakers

Members (712)



 IACR Cryptographers



Russian Translation:

code breakers ==

ВЗЛОМЩИКИ КОДОВ

History: Cold War Russia vs. USA

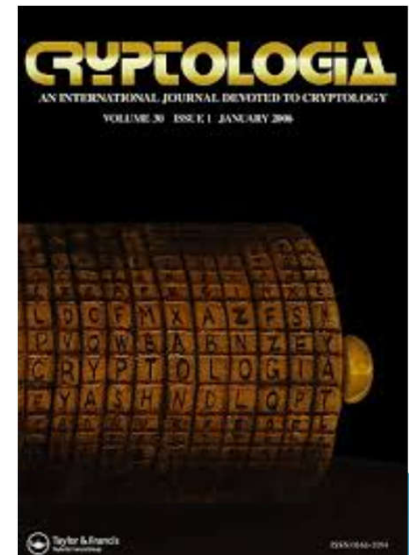


Cold War

Cold War: Soviet Union was breaking codes and employed at least **100 cryptologists**...

[Source: Cryptologia, interviews by David Kahn
with gen. Andreev=first head of FAPSI=Russian NSA]

Example: In 1967 GRU (Soviet Intelligence)
was intercepting cryptograms from 115 countries,
using 152 cryptosystems,
and among these they broke 11 codes
and “obtained” 7 other codes.



Compromise of Old Crypto

- USS Pueblo / North Korea
Jan 1968



US/NATO crypto broken

Russia broke the NATO KW-7 cipher machine:
Walker spy ring, rotors+keys,

- paid more than 1M USD (source: NSA)
- “greatest exploit in KGB history”
- allowed Soviets to “read millions” of US messages [1989, Washington Post]



1970s


Modern **block ciphers** are born.

In which country??

Who knows...

Our Sources

Referat 11

Gehelme- und Verschlusssache
ZCO Nr.: 402/80
10. .Ausf. 123 Blatt
10.12.90 

BStU
000001

Kryptologie Analyse
des Chiffriertes T 310/50

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

Gehelme- und Verschlusssache
ZCO Nr.: 402/80
Entlassungsgutachten/entlassen/entlassen

Our Sources

Gehelme- und Verschlusssache
ZCO Nr.: 402/80
10. Ausf. 123 Blatt
10.12.90

BStU
000001

BStU = Stasi
Records Agency

Kryptologie Analyse
des Chiffriertes T 310/50

Boolean Functions Expertise: Imported

[3]

Краткий конспект лекций для специалистов
ЦШО МГБ ГАР

сов.секретно К-1 Инв.2243



Kapitel II / Boolesche Funktionen

Algebraic Cryptanalysis – 1927

The real inventor of the

ANF = Algebraic Normal Form, see

en.wikipedia.org/wiki/Zhegalkin_polynomial

Russian mathematician and logician

Ива́н Ива́нович Жега́лкин [Moscow State University]

“best known for his formulation of
Boolean algebra
as the theory
of the **ring** of integers mod 2”

$B_n, +, *$

Cipher Class Alpha –1970s

Who invented Alpha?

[full document not avail.]

- 3 -

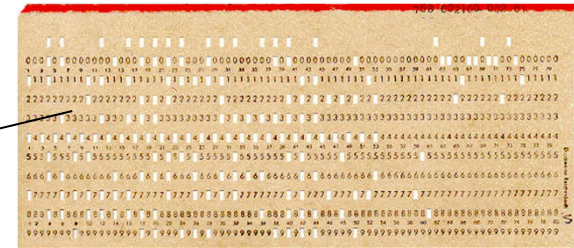
GVS-ZCO-198/77

8STU
0166

Введение

Класс АЛЬФА определён в /I/. Там же имеется ряд определений и обозначений, которые в настоящем документе не объясняются.

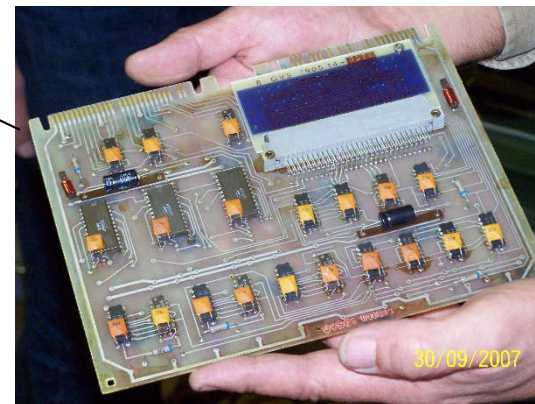
East German T-310



240 bits

“quasi-absolute security”
[1973-1990]

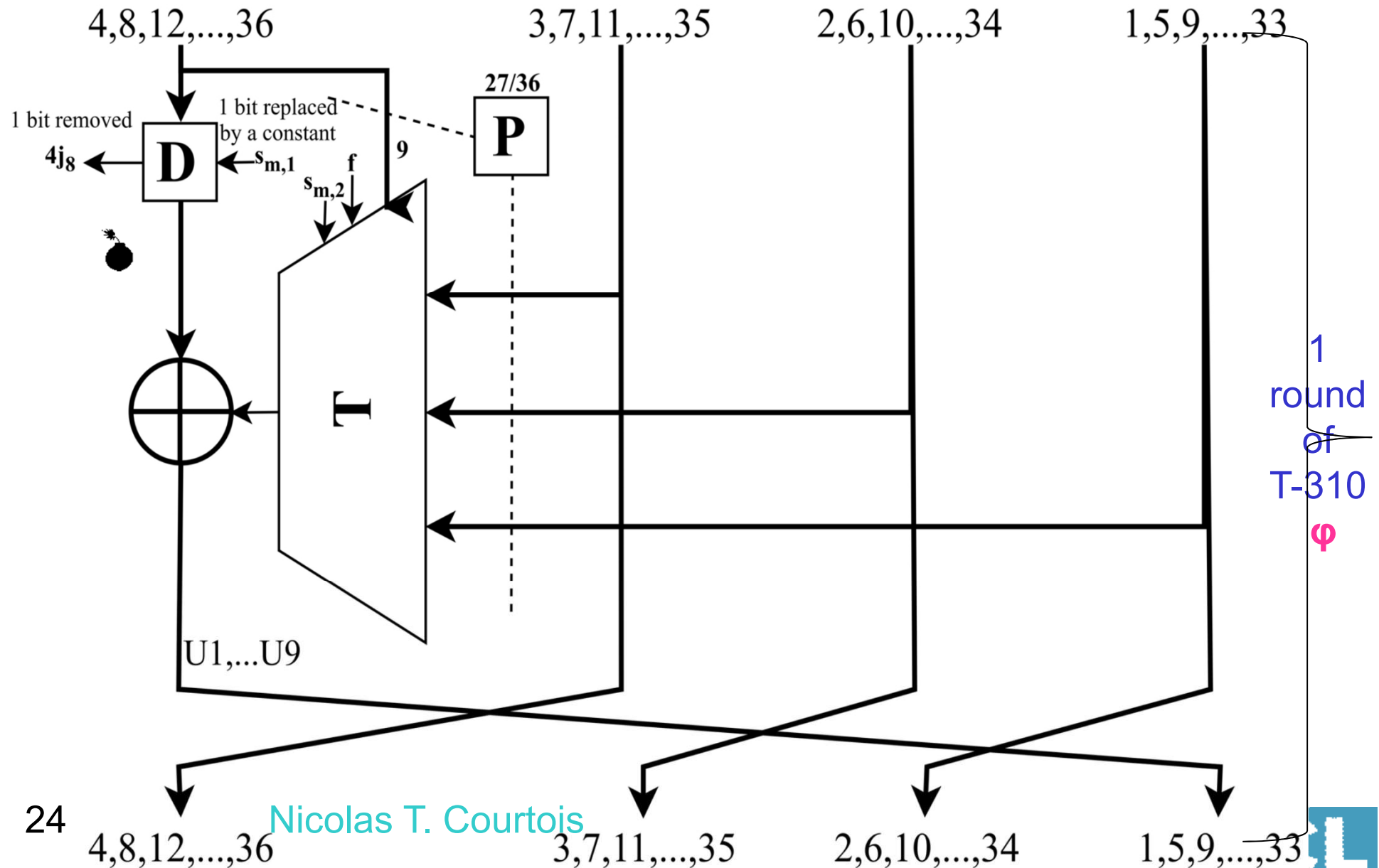
has a
physical
RNG=>IV



long-term secret
90 bits only!



Contracting Feistel [1970s Eastern Germany!]



Differential Cryptanalysis (DC)

“Official” History

- Differential Cryptanalysis :
Biham-Shamir [1991]

IBM USA 1970s

Wikipedia DC entry says:

[...] IBM had discovered differential cryptanalysis on its own

[...] 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

MIS -323-Nr: 747 / 73/BL 45

BSTU
000053

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

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

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

($r = 0, 1, \dots, 6$)

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

($i = 1, 2, \dots, 6$)

Open Problem

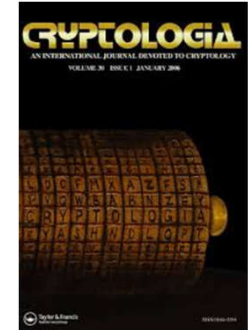
- Backdoor symmetric encryption?

How to Backdoor T-310 [1st method]

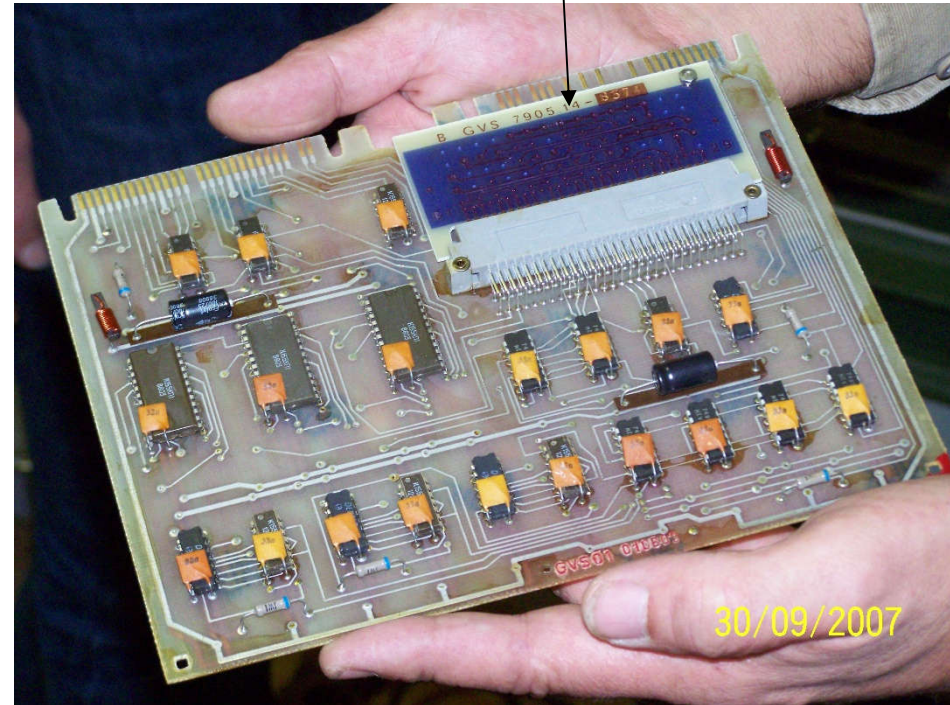
omit just 1 out of 40 conditions:

ciphertext-only

bad
long-term
key



D and P are injective
 $P(3) = 33, P(7) = 5, P(9) = 9, P(15) = 21, P(18) = 25, P(24) = 29$
 Let $W = \{5, 9, 21, 25, 29, 33\}$
 $\forall i \geq 9, D(i) \notin W$
 $\alpha \notin W$
 Let $T = (\{0, 1, \dots, 12\} \setminus W) \cap (\{P(1), P(2), \dots, P(24)\} \cup \{D(4), D(5), \dots, D(9)\} \cup \{\alpha\})$
 Let $U = (\{13, \dots, 36\} \setminus W) \cap (\{P(26), P(27)\} \cup \{D(1), D(2), D(3)\})$
 $|T \setminus \{P(25)\}| + |U \setminus \{P(25)\}| \leq 12$
 $A = \{D(1), D(2), D(3), D(4), D(5), D(6), D(7), D(8), D(9)\} \cup \{P(6), P(13), P(20), P(27)\}$
 $A_1 = \{D(1), D(2)\} \cup \{P(27)\}$
 $A_2 = \{D(3), D(4)\} \cup \{P(20)\}$
 $A_3 = \{D(5), D(6)\} \cup \{P(13)\}$
 $A_4 = \{D(7), D(8)\} \cup \{P(6)\}$
 $\forall (i, j) \in \{1, \dots, 27\} \times \{1, \dots, 9\} : P_i \neq D_j$
 $\exists j_1 \in \{1, \dots, 7\} : D_{j_1} = 0$
 $\{D(8), D(9)\} \subset \{4, 8, \dots, 36\} \subset A$
 $\forall (i, j) \in \overline{1, 27} \times \overline{1, 9} : P_i \neq D_j$
 $\exists j_1 \in \overline{1, 7} : D_{j_1} = 0$
 $\{D_8, D_9\} \subset \{4, 8, \dots, 36\} \subset A$
 $\exists (j_1, j_2) \in (\{j \in \overline{1, 4} : D_j \neq 0\})^2 \wedge$
 $\exists (j_4, j_5) \in (\overline{1, 4} \setminus \{j_1, 2j_2 - 1, 2j_2\}) \times (\overline{5, 8} \setminus \{j_1, 2j_2 - 1, 2j_2\}) \wedge$
 $\exists j_6 \in \overline{1, 9} \setminus \{j_1, 2j_2 - 1, 2j_2, j_4, j_5\} :$
 $j_2 \neq j_6 \wedge \{4j_1, 4j_6\} \subset A_{j_2} \wedge$
 $A_{j_2} \cap (\overline{4j_1 - 3, 4j_1} \cup \overline{4j_6 - 3, 4j_6}) \neq \emptyset \wedge$
 $\{8j_2 - 5, 8j_2\} \subset A_{j_2} \wedge A_{j_2} \cap (\overline{4j_1 - 3, 4j_1} \cup \overline{4j_6 - 3, 4j_6}) \neq \emptyset ;$
 $\{D(9)\} \setminus \{33, 36 \cup \{0\}\} \neq \emptyset$
 $\{D(8), D(9), P(1), P(2), \dots, P(5)\} \setminus \{29, 32 \cup \{0\}\} \neq \emptyset$
 $\{D(7), D(8), P(1), P(2), \dots, P(6)\} \setminus \{25, 32 \cup \{0\}\} \neq \emptyset$
 $\{D(7), D(9), P(1), P(2), \dots, P(6)\} \setminus \{25, 28 \cup 33, 36 \cup \{0\}\} \neq \emptyset$
 $\{D(6), D(7), D(8), D(9), P(1), P(2), \dots, P(12)\} \setminus \{21, 36 \cup \{0\}\} \neq \emptyset$
 $\{D(5), D(7), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus (\overline{17, 20} \cup 25, 36 \cup \{0\}) \neq \emptyset$
 $\{D(7), D(8), D(9), P(1), P(2), \dots, P(6)\} \setminus \{25, 36 \cup \{0\}\} \neq \emptyset$
 $\{D(5), D(6), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus (\overline{17, 24} \cup 29, 36 \cup \{0\}) \neq \emptyset$
 $\{D(5), D(6), D(7), D(9), P(1), P(2), \dots, P(13)\} \setminus (\overline{17, 28} \cup 33, 36 \cup \{0\}) \neq \emptyset$
 $\{D(5), D(6), D(7), D(8), P(1), P(2), \dots, P(13)\} \setminus (\overline{17, 32} \cup \{0\}) \neq \emptyset$
 $\{D(5), D(6), D(7), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus (\overline{17, 36} \cup \{0\}) \neq \emptyset$
 $\{D(4), D(5), \dots, D(9), P(1), P(2), \dots, P(19)\} \setminus \{13, 36 \cup \{0\}\} \neq \emptyset$
 $\{D(3), D(4), \dots, D(9), P(1), P(2), \dots, P(20)\} \setminus \{9, 36 \cup \{0\}\} \neq \emptyset$
 plus the "Matrix rank = 9 condition" M_9 defined in Section D.4 below.



Linear Cryptanalysis (LC)

LC “Official” History

- **Davies-Murphy attack** [1982=classified, published in 1995] = early LC
- Shamir Paper [1985]..... early LC
- **Linear Cryptanalysis:** Gilbert and Matsui [1992-93]

LC at ZCO - 1976!

Definition 3.1-1

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

$$\|g\| \stackrel{\text{def}}{=} \sum_x g(x)$$

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

Geheime Verschlusssache

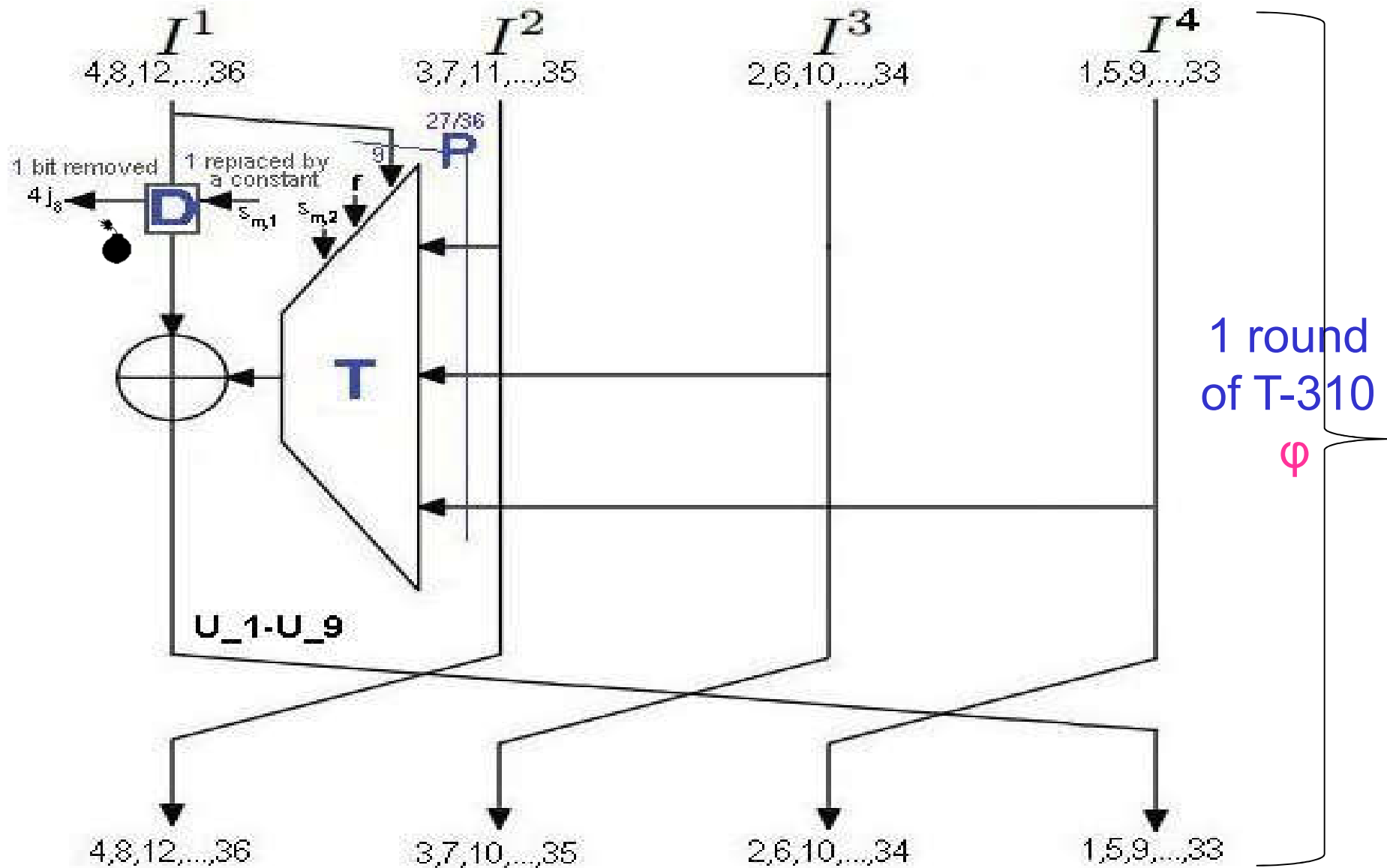
MfS -020-Nr.: XI/493/76 BL 18Ergebnisse:BSTU
0251

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!]



LC Method to Backdoor T-310

1,3,5 => 1,3,5

P=1

703

P=7,14,33,23,18,36,5,2,9,

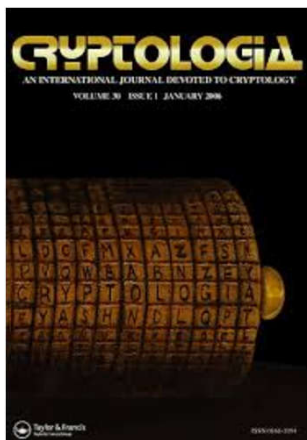
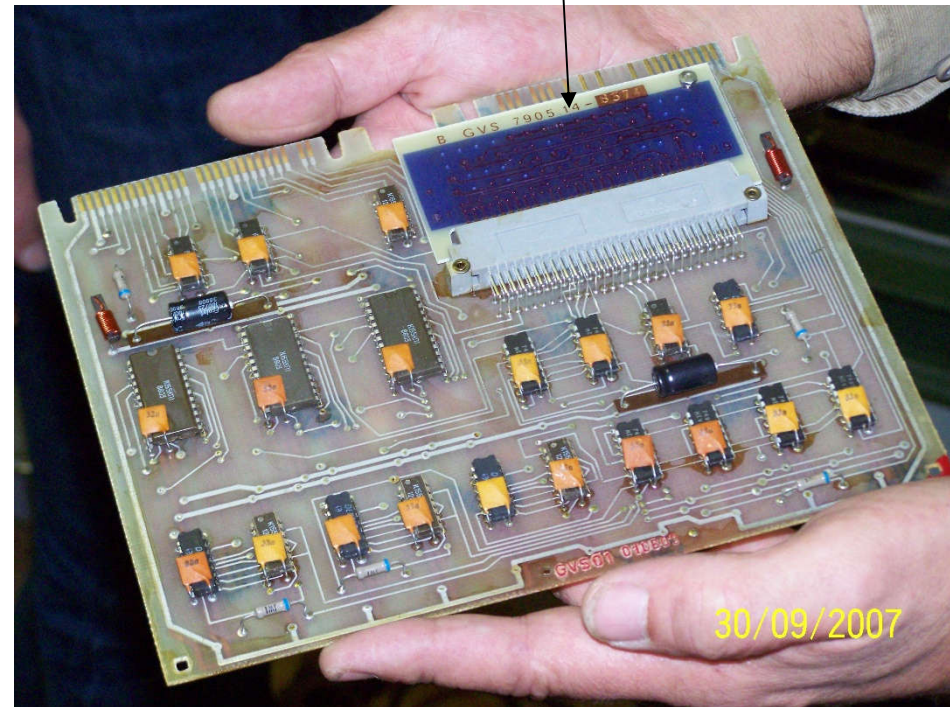
16,30,12,32,26,21,1,13,25,

20,8,24,15,22,29,10,28,6

D=0,4,24,12,16,32,28,36,20



bad long-term key



Shamir 1985

On the Security of DES

Adi Shamir
Applied Mathematics
The Weizmann Institute
Rehovot, Israel
(abstract)

$x_2 \approx y_1 \oplus y_2 \oplus y_3 \oplus y_4 .$



Common to all S-boxes !!!!

Super strong pty,

See our paper:

Courtois, Goubin, Castagnos [eprint/2003/184](https://eprint.iacr.org/2003/184)

revisiting crypto history

Advanced Differential Cryptanalysis

Higher Order Differentials – 1976 !

Definition 2.1-1

$$\frac{dZ(e_1, \dots, e_6)}{de_i} = Z(e_1, \dots, e_{i-1}, 0, e_{i+1}, \dots, e_6) + Z(e_1, \dots, e_{i-1}, 1, e_{i+1}, \dots, e_6)$$

ist die einfache Ableitung der Booleschen Funktion Z .

Higher Order:

Definition 2.1-2

$$\frac{d^k Z(e_1, \dots, e_6)}{de_{i_1} \dots de_{i_k}} = \left(\frac{d}{de_{i_1}} \left(\dots \frac{dZ(e_1, \dots, e_6)}{de_{i_k}} \right) \dots \right)$$

mit $1 \leq i_1, \dots, i_k \leq 6$ $k \in \overline{1, 6}$,

$i_j \neq i_l$ für $j \neq l$,

Same as Today's Cube Attack

Geheime Verschlusssache

MfS -020-Nr.: XI/493/76/BL 5

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

BSTU
0238

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

·
·
·

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

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

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

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

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

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

Part 2

Generalized Linear Cryptanalysis (GLC)

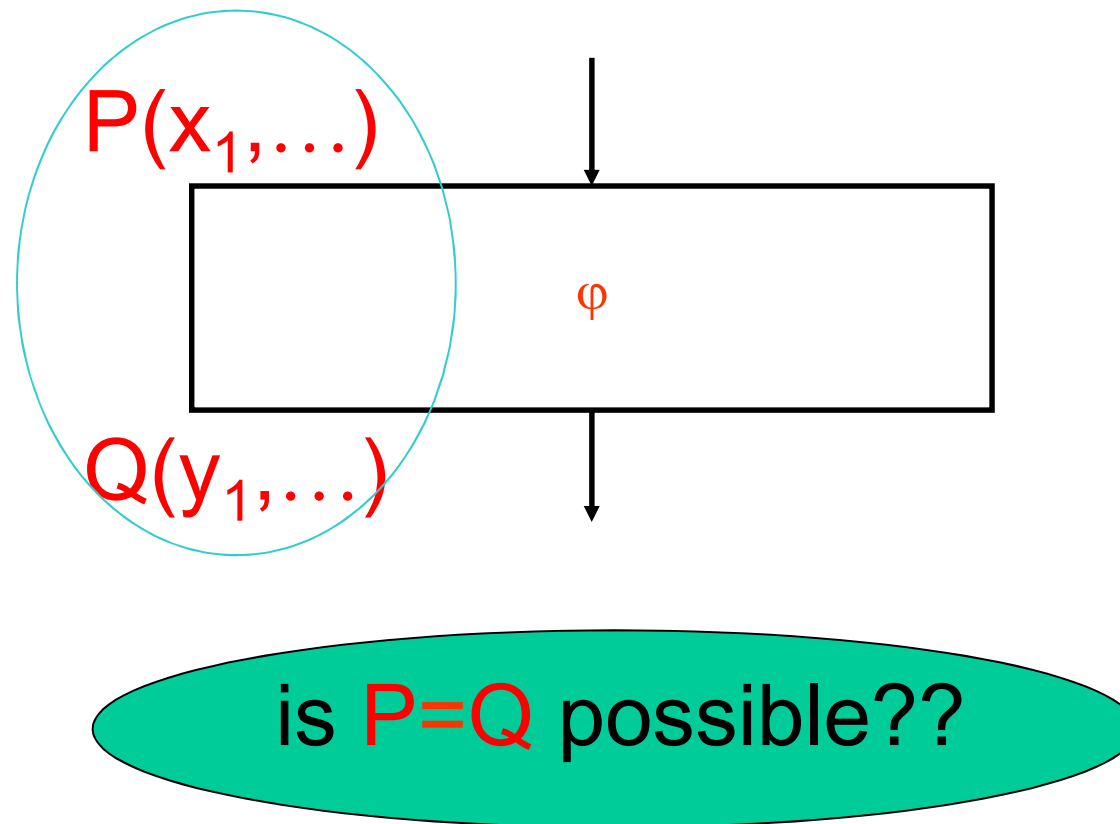
Scope

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

Stop, this is extremely complicated???

Main Problem:

Two polynomials $P \Rightarrow Q$.



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

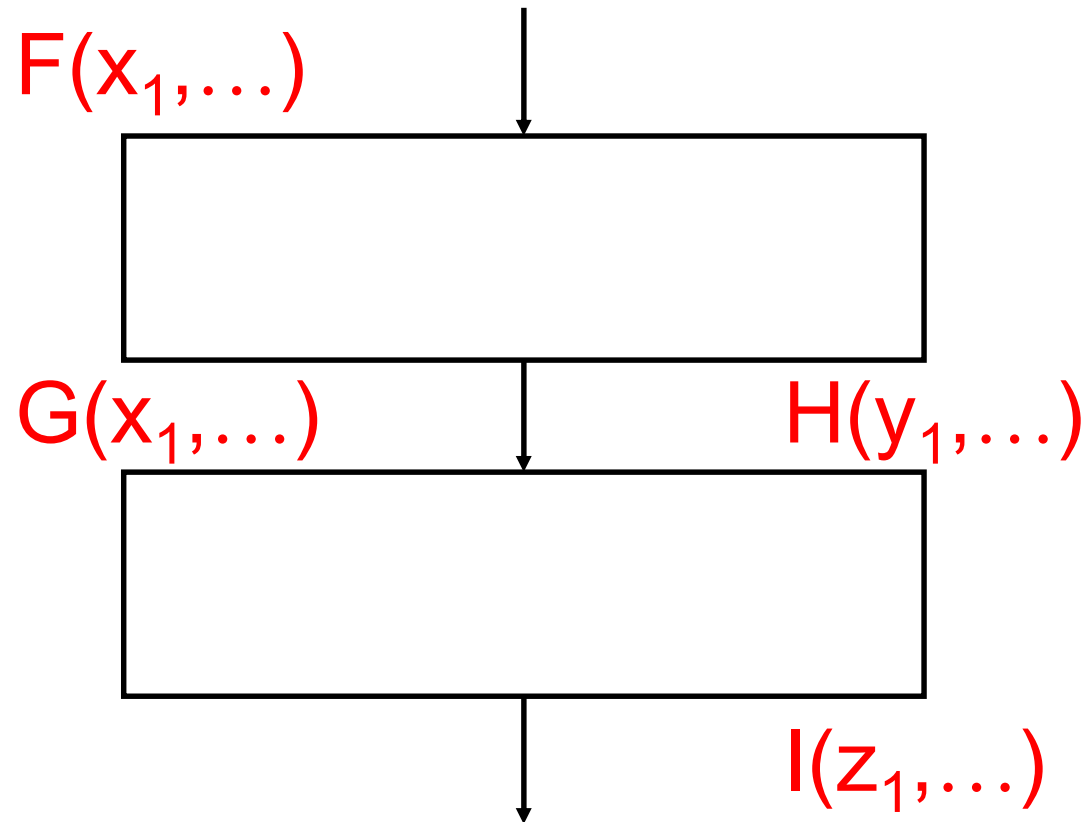
Generalised Linear Cryptanalysis = GLC =

[Harpes, Kramer and Massey, Eurocrypt'95]

Connecting Non-Linear Approxs.

Black-Box Approach [Popular]

Non-linear functions.



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

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

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



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

[Courtois 2018]

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

Formal equality of 2 polynomials.

shocking discovery

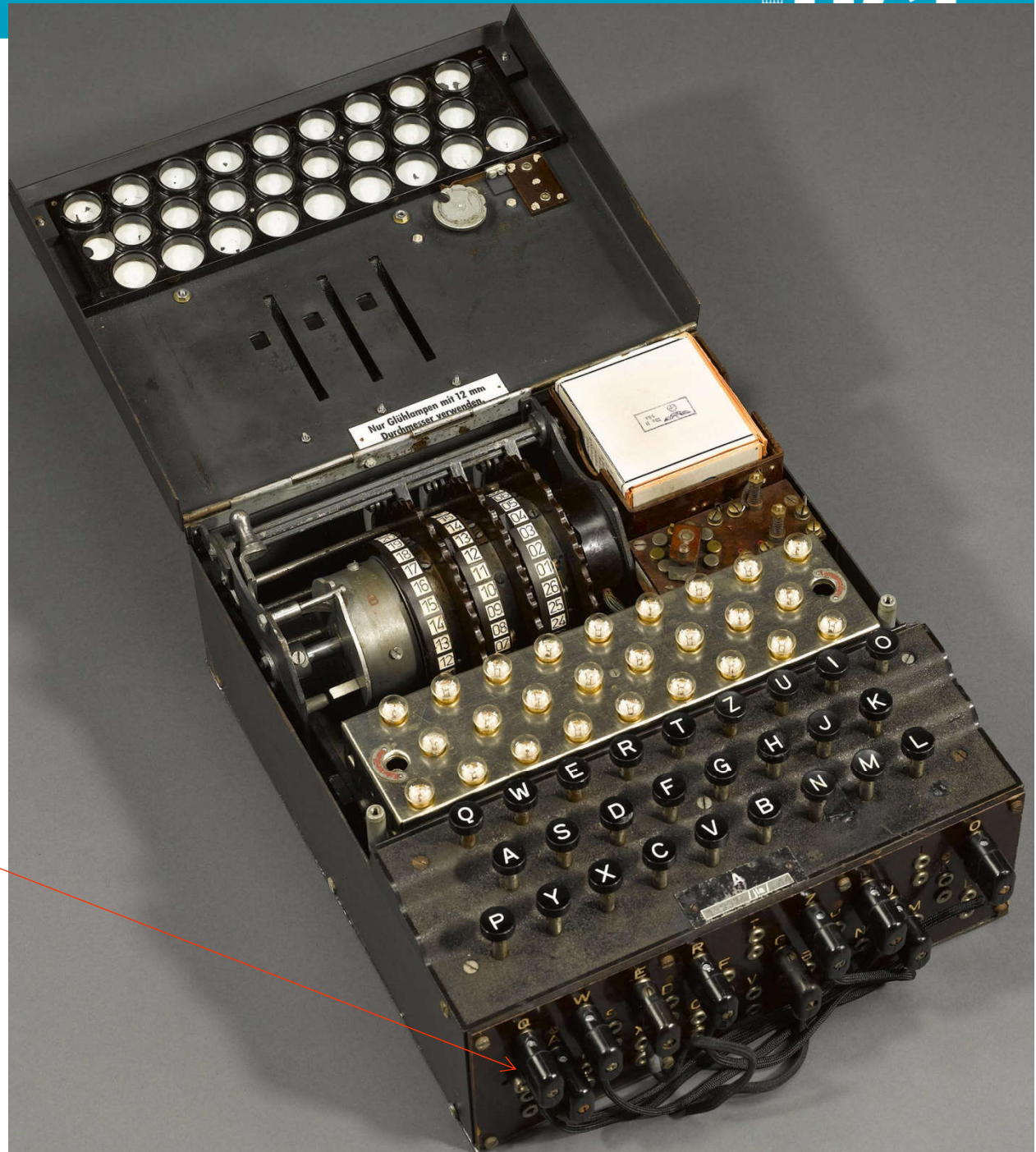
Eastern Bloc Ciphers
are **WEAK** w.r.t.
our Attack

1. Closed Loops
2. Key Entropy per Round

Military Enigma [1930s]

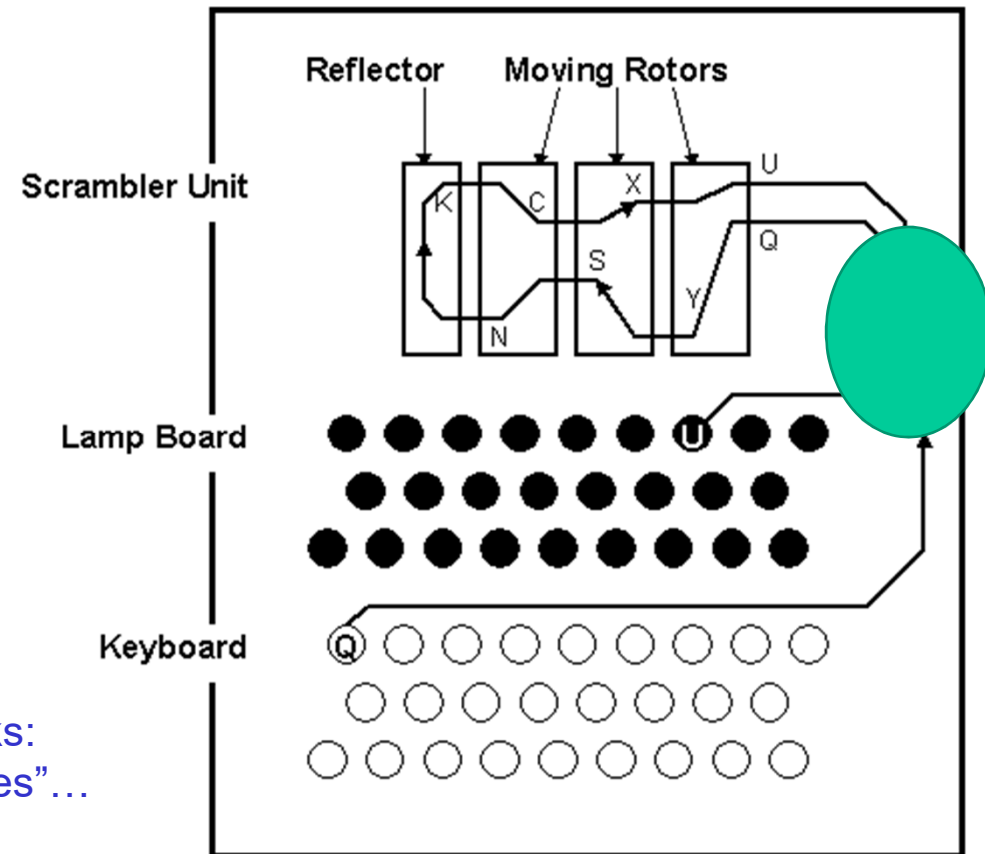
stecker=
plugboard

[after 1929]



Enigma Stecker

Huge challenge for
code breakers

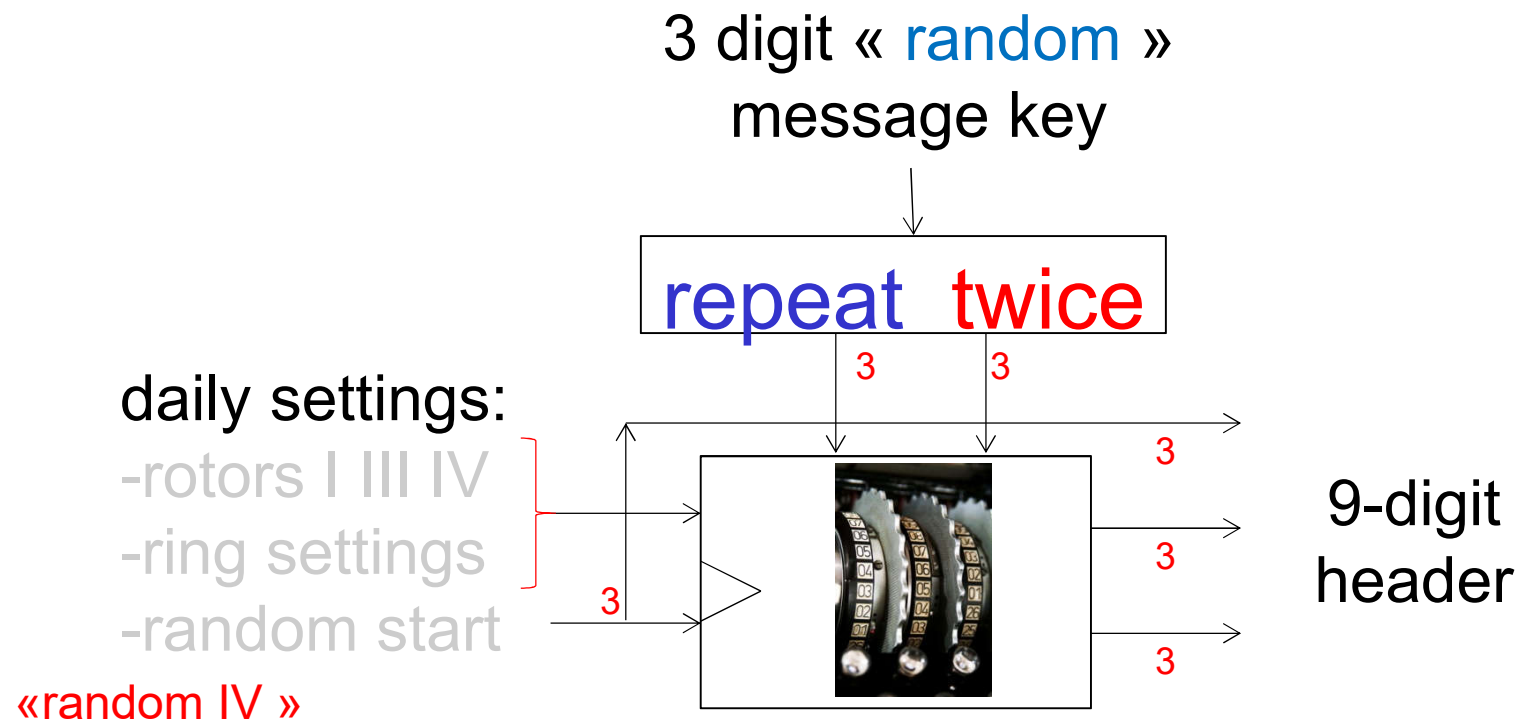


*common point in all good Enigma attacks:
eliminate the stecker, “chaining techniques”...

also for Abwehr

Double Encryption Method – Big Mistake

15 Sept 1938 - 1 May 1940





Bugs or Backdoors?

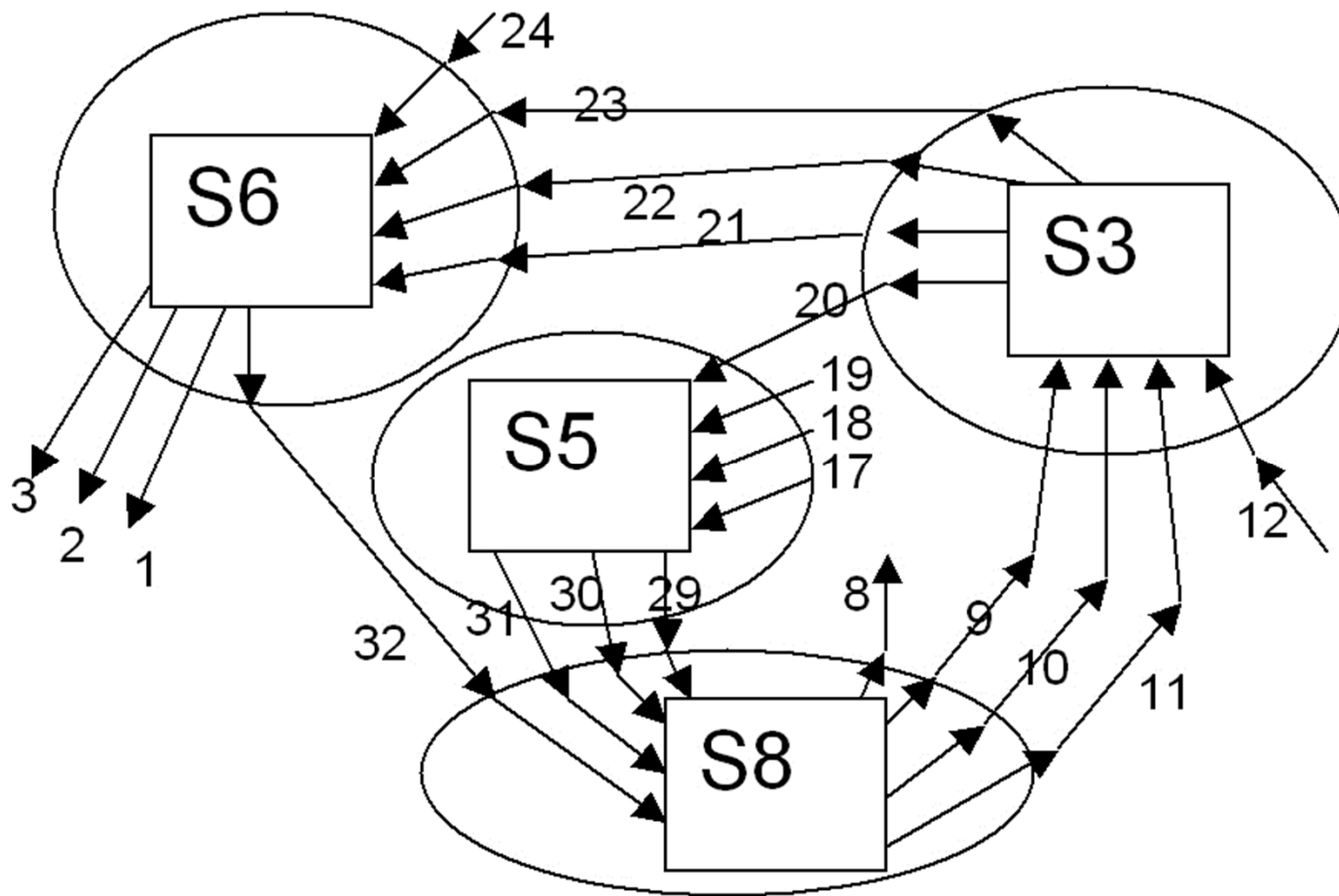
GOST 28148-89

Developed in 1970s...

- First "Top Secret" / Type 1 algorithm.
- Declassified in 1994.

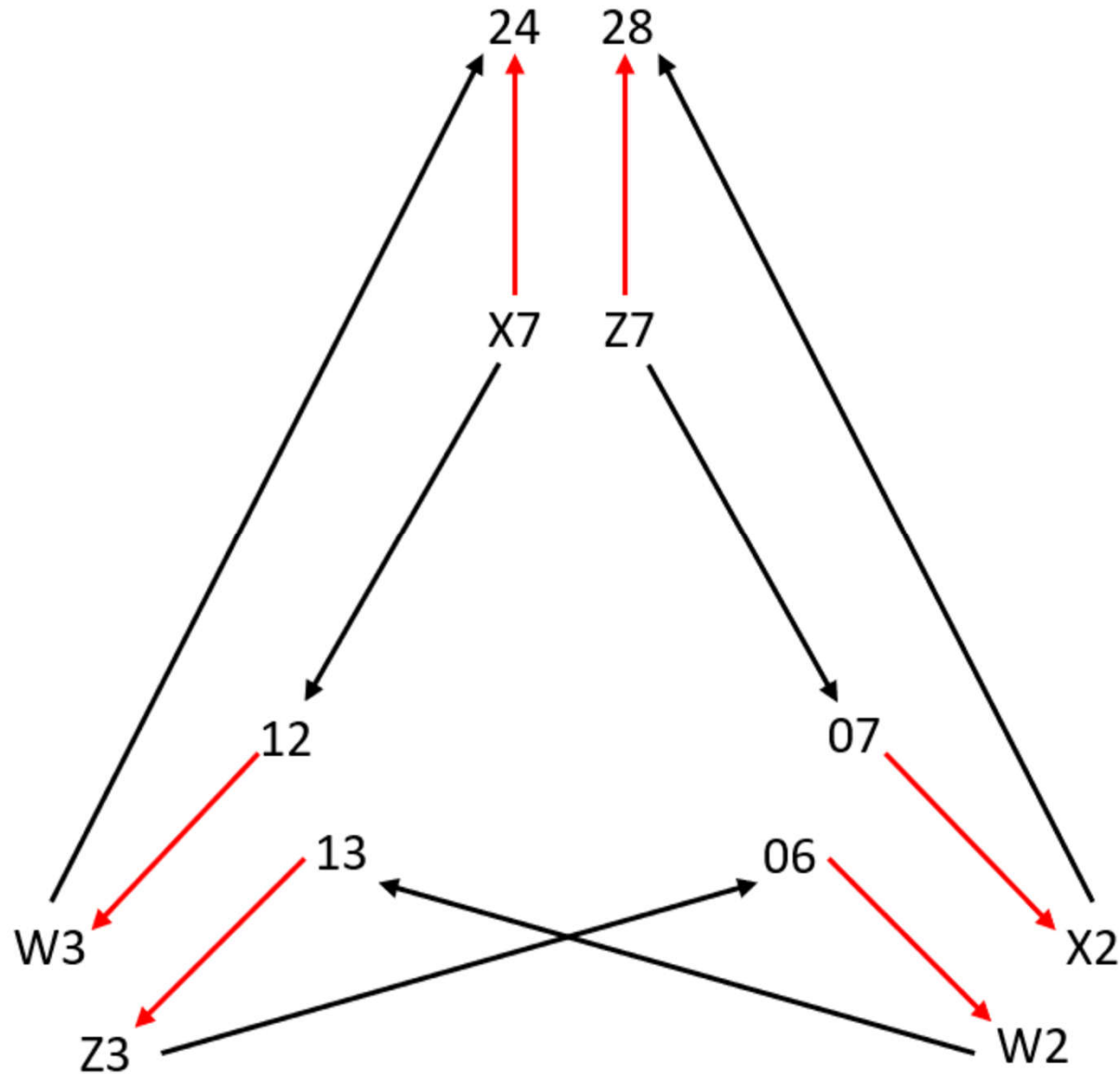
Closed Loops

In GOST block cipher:



highly
vulnerable!

Closed Loops - DES



[@eprint/](https://eprint.iacr.org/2018/1242)

[2018/1242](https://eprint.iacr.org/2018/1242)

Big Winner

“product attack”

a product of Boolean polynomials.

Claimed extremely powerful.

Why?

Key Remark:

To insure that

$$P * R \Rightarrow P * R$$

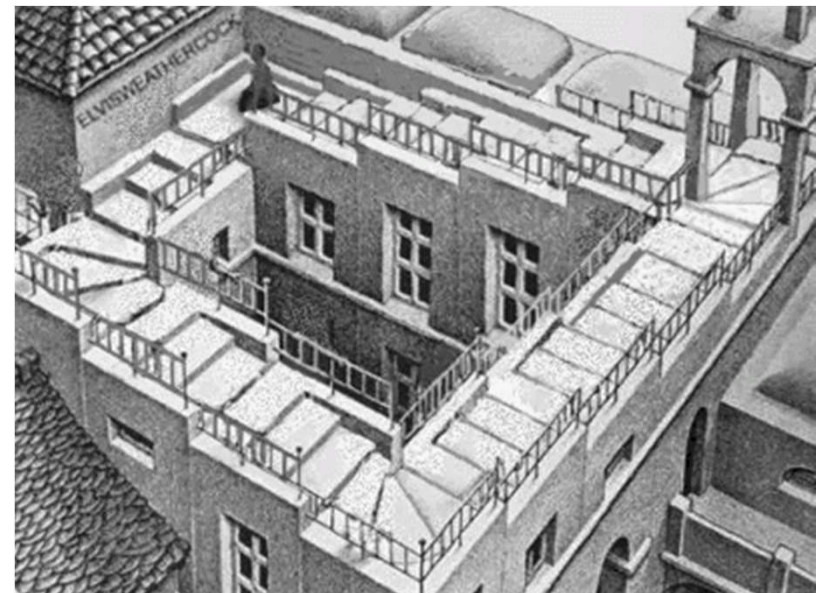
we only need to make sure
that $P \Rightarrow P$ but **ONLY** for a subspace
where $R(\text{inp})=1$ and $R(\text{out})=1$

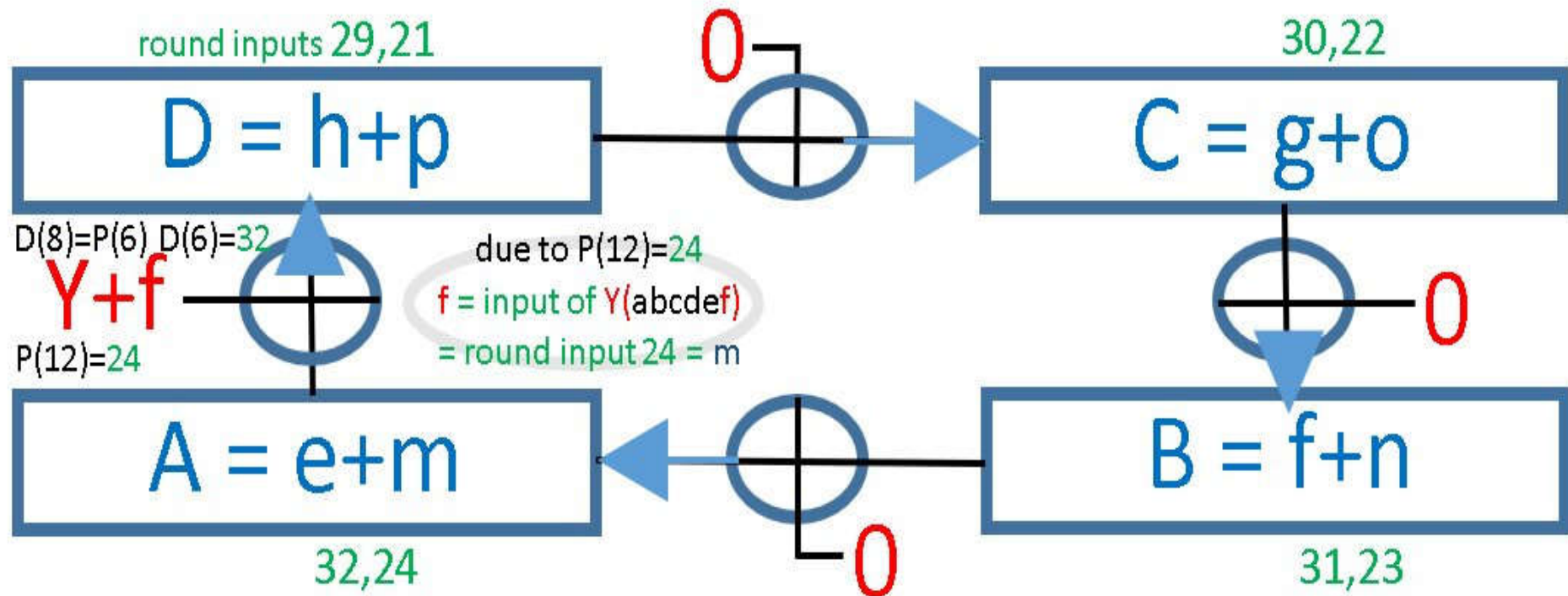
Impossible?

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

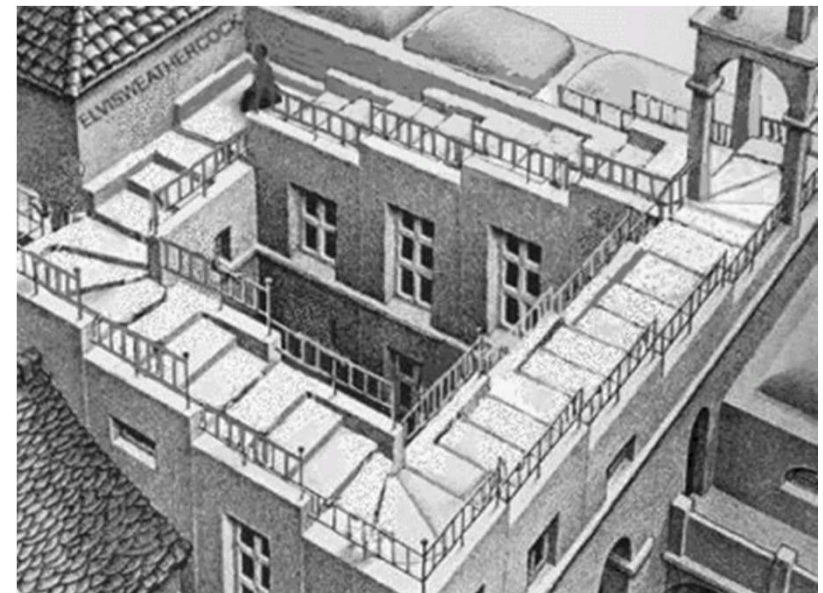
-- M. C. Escher

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





Cycles



Thm 5.5.

In [eprint/2018/1242](https://eprint.iacr.org/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?

Hard Becomes Easy

Phase transition: [eprint/2018/1242](https://eprint.iacr.org/2018/1242).

- 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 $\mathcal{P} = \text{ABCDEFGH}$.

attacks on DES

*work for a
fraction of keys

Degree 5 Attack on DES

Theorem: Let $\mathcal{P} =$

$$(1 + L_{06} + L_{07}) * L_{12} * R_{13} * R_{24} * R_{28}$$

IF

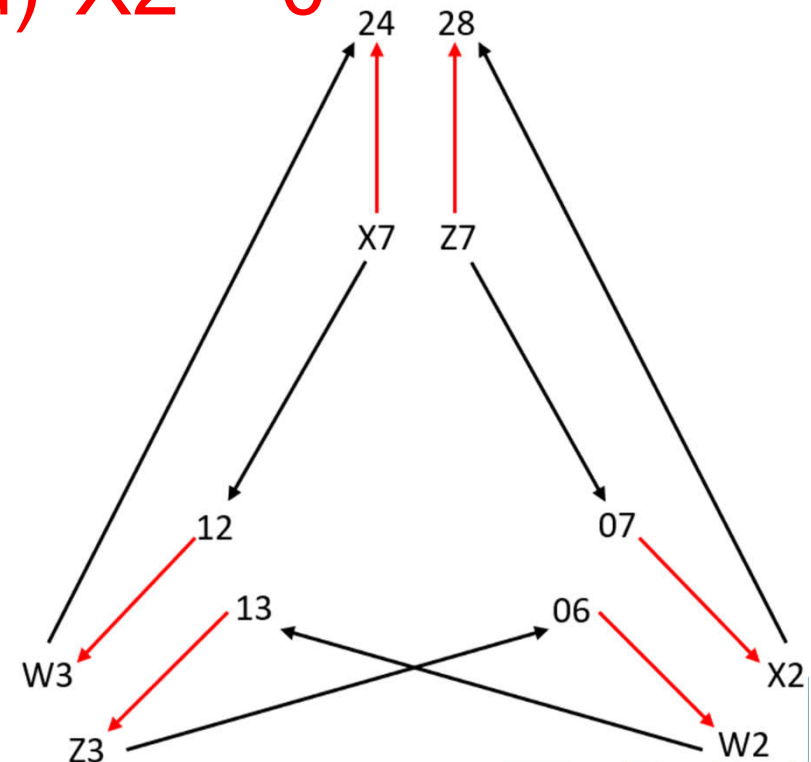
$$(1 + c + d) * W_2 == 0 \text{ and } (1 + c + d) * X_2 == 0$$

$$e * W_3 == 0 \text{ and } f * Z_3 == 0$$

$$ae * X_7 == 0 \text{ and } ae * Z_7 == 0$$

THEN

\mathcal{P} is an invariant for
2 rounds of DES.



East vs. West Block Ciphers

Cipher	Year	Country	Block Size	Key size (underlined number is used in the following columns)	Round number (in key schedule)	Rounds / bit encrypted	Proportion of key used per round		
SKS V/1	1973	Eastern Germany	27	208	104	119	1 %		
T-310	1976	Eastern Germany	36	240	120	165	0.8 %		
DES	1974	USA	64	56	16	0.25	75 %	2300^2	10,400
GOST (aka MAGMA)	1989	Russia	64	256	32	0.5	12.5 %	800^3	1600
TEA	1994	UK	64	128	64	1	50 %	2100^2	2100
AES	1996	Belgium	128	<u>128</u> /192/256	10	0.08	100 %	2400^1	30,000
PRESENT	2007	Germany/ France	64	80/ <u>128</u>	31	2.1	100 %	1100^2	533
Simon/ Speck	2013	USA	64	64/72/96/ <u>128</u> /144/ 192/256	27	0.42	100 %	1250^1	2963

