

Cold War Crypto, Correlation Attacks, DC, LC, T-310, Weak Keys and Backdoors

Nicolas T. Courtois
University College London, UK

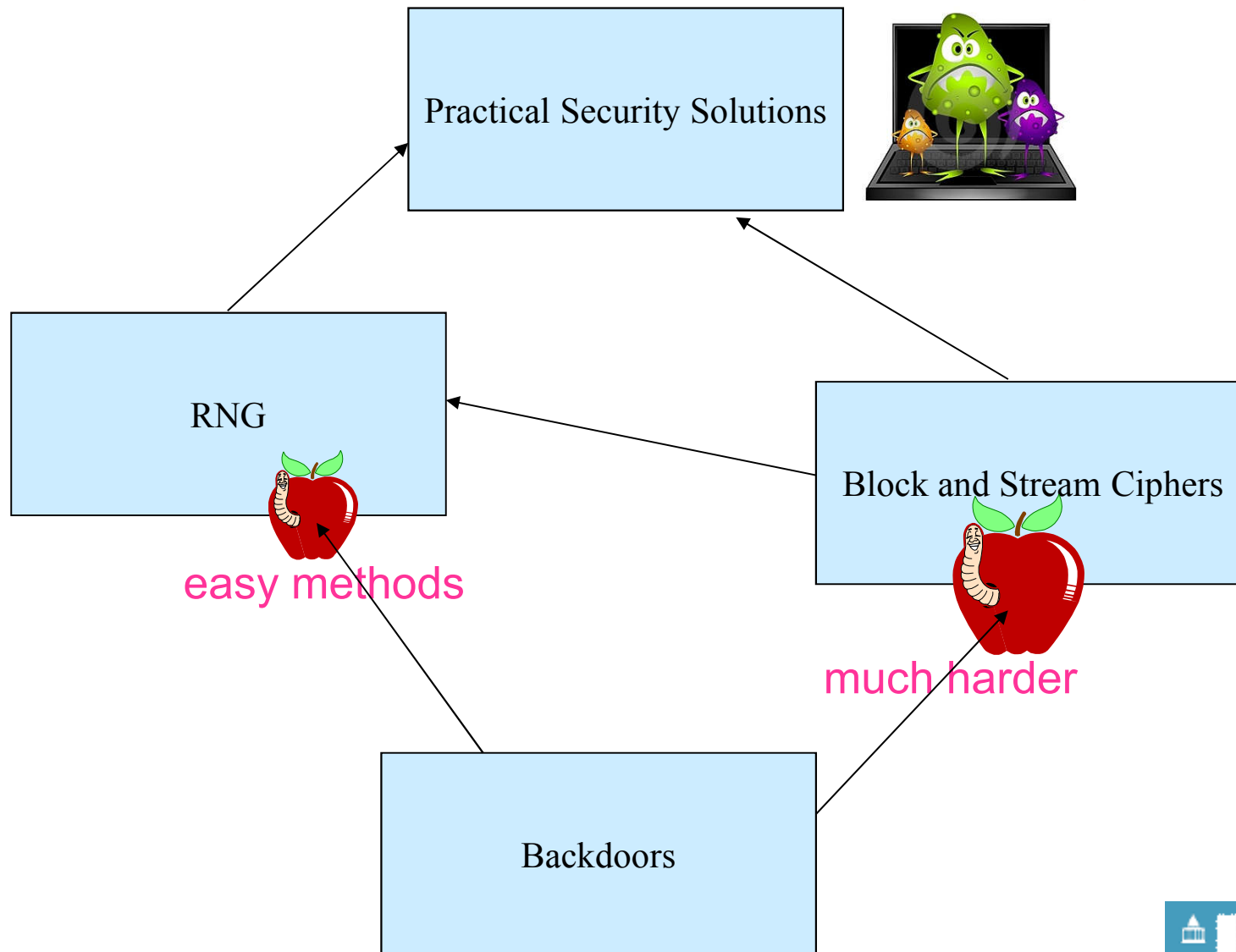
bugs or backdoors?



False Backdoors = def =

strong properties of ciphers/systems/RNGs
which are **maybe** dangerous...

Any Backdoors?



Bad Randoms – 1930s – Enigma Message Keys

(should be 3
random letters)

~~AAA~~
~~XYZ~~



Operators always found a way to «degrade » their security

Crypto History

CRYPTOLOGIA

EDITOR-IN-CHIEF

Craig Bauer
York, PA, USA
cryptoauthor@gmail.com

REVIEW EDITOR

Chris Christensen
Department of Mathematics
Northern Kentucky University
Highland Heights, KY, USA
christensen@nku.edu

FOUNDING EDITORS

Cipher A. Deavours
Department of Mathematics
Kean University of New Jersey
Union, NJ, USA
cdeavours@kean.edu

Brian J. Winkel
Editor Emeritus
Dept. of Mathematical Sciences
United States Military Academy
West Point, NY, USA
brianwinkel@hvc.rz.com

Editorial Assistant

Dante Molle
Roseto, PA, USA
dante42.13@gmail.com

David Kahn
New York, NY, USA
DavidKahn1@aol.com

Greg Mellen
Editor Emeritus
In Memoriam

Louis Kruh
Editor Emeritus
In Memoriam

EDITORIAL BOARD

Kent D. Boklan
Queens College,
The City University of
New York, NY, USA
boklan@boole.cs.qc.cuny.edu

Stephen Budiansky
Leesburg, VA, USA
sb@budiansky.com

Augusto Buonafalce
San Terenzo, Italy
augusto@cdh.it

Colin Burke
Columbia, MD, USA
burke@umbc.edu

Jan Bury
Cardinal Stefan
Wyszynski University,
Warsaw, Poland
j.bury@uksw.edu.pl

Nicolas T. Courtois
Computer Science,
University College London,

Whitfield Diffie
Center for International Security
and Cooperation,
Stanford University,
Stanford, CA, USA
diffie@stanford.edu

Ralph Erskine
Parliament Buildings, Stormont,
Belfast, Northern Ireland, UK
erskineralph@yahoo.co.uk

Wes Freeman
Mt. View, CA, USA
wesf@worldnet.att.net

David W. Gaddy
Tappahannock, VA, USA
dwgaddy@verizon.net

James J. Gillogly
Los Angeles, CA, USA
screyer@gmail.com

Lee A. Groisman

Bob Hanyok
6500 Walker Branch Dr.
Laurel, MD, USA
rjhanyok@verizon.net

David Hatch
Center for Cryptologic History,
National Security Agency,
Fort Meade, MD, USA
dahatch@nsa.gov

Joshua Brandon Holden
Department of Mathematics,
Rose-Hulman Institute
of Technology,
Terre Haute, IN, USA
holden@rose-hulman.edu

David Joyner
Mathematics Department,
United States Naval Academy
Annapolis, MD, USA
wdj@usna.edu

David Kahn
Great Neck, NY, USA

David Naccache
Ecole normale supérieure,
Département d'informatique,
Paris, France
david.naccache@ens.fr

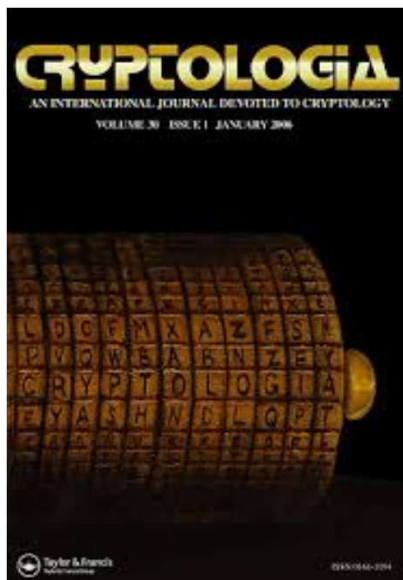
Raphael C.-W. Phan
Multimedia University,
Malaysia
raphaelphan.crypt@gmail.com

Klaus Schmeh
Gelsenkirchen, Germany
klaus@schmeh.org

Alan T. Sherman
Department of Computer
Science & Electrical Engineering,
University of Maryland,
Baltimore County
Baltimore, MD, USA
sherman@umbc.edu

William Stallings
USA, ws@shore.net or
http://williamstallings.com/

Frøde Weierud



HistoCrypt / Euro-HCC



18-19 May 2017, Slovakia

18-19 May Program

Day 1 – 18th May 2017	Day 2 – 19th May 2017
Opening Conference and Welcome K. Nemoga 09:00 - 09:15	History of public key cryptography and RSA – Session Chair: B. Esslinger L.-J. Quisquater 09:00-10:00
The 'Gustave Bertrand' files – Session Chair: N. Courtois D. Turing 09:15 - 9:45	
Session 1 – Session Chair: G.F. Strasser Slot 1: 09:45 - 10:15: G. Lasry - The Hagelin Cryptosystems - Historical and Modern Cryptanalysis Coffee Break 10:15 - 10:45 Slot 2: 10:45 - 11:15: N. Kopal - A General Solution for the M-94 Slot 3: 11:15 - 11:45: J. Kollár - Determining the text reading direction of an unknown text Slot 4: 11:45 - 12:15: B. Esslinger - Automated Cryptanalysis of Classical Ciphers	Session 3 – Session Chair: K. Schmeb Slot 9: 10:00 - 10:30: P. Bonavoglia - How I decrypted Pietro Giannone's last poem Coffee Break 10:30 - 11:00 Slot 10: 11:00 - 11:30: G.F. Strasser - Wollenbüttel, a Minor German Duchy but a Major Center of Cryptology in the Early Modern Period Slot 11: 11:30 - 12:00: S. Porubsky - STP cipher of the Czechoslovak Ministry of Defence in London during WWII Slot 12: 12:00 - 12:30: M. Grajek - Interrogation at Eisenberg Castle - How two Polish officers saved the Ultra secret just before Overlord
Lunch 12:15 - 13:30	
Session 2 – Session Chair: D. Turing Slot 5: 13:30 - 14:00: K. Schmeb - German Spy Ciphers of World War II Slot 6: 14:00 - 14:30: C. Taaks - The Early Times of the Enigma – Political, Economic and Military Coffee Break 14:30 - 15:00 Slot 7: 15:00 - 15:30: P. Guillot - The priceless gift - The Polish cryptanalysis of Enigma Slot 8: 15:30 - 16:00: M.-J. Durand-Richard - Cryptology at Bletchley Park (1939-1945)	Closing Remarks 12:30 - 12:45
	Lunch and/or departure 12:45 - 14:00

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)



5



 IACR Cryptographers



1



Post-WW2 Crypto History

1960s

NATO Cipher competition

- UK
- US
- France
- Germany

Requirements:

- “tapeless and rotorless”
=> semi-conductor electronic,
- high EM/SCA security!



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??

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

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

Referat 11

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

Gehelme- und Verschlusssache
ZCO Nr.: 402/80

MfS = Ministerium für Staatssicherheit
=
Ministry of State Security of GDR = Stasi

BStU

Referat 11

Gehelme- und Verschlusssache

ZCO Nr.: 402/80

10. Ausf. 123 Blatt

10.12.90

BStU

000001

BStU =

Bundesbeauftragter
= Stasi Records
Agency =
a.k.a. Birthler authority

Kryptologie Analyse
des Chiffriertes T 310/50

Our Sources

Referat 11

ZCO =
Zentrales Chiffrierorgan
der DDR

Gehelme... aufheben/aufgehoben
ZCO Nr.: 402/80

10. Ausf. 123 Blatt

10.12.90

BStU
000001

BStU = Stasi
Records Agency

Kryptologie Analyse
des Chiffrie... ätes T 310/50

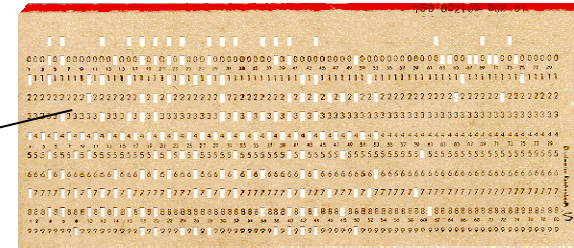
How do you say “ZCO” in Russian?

How do you say “ZCO” in Russian?

[3] Краткий конспект лекций для специалистов
ЦШО МГБ ГАР
сов.секретно К-1 Инв.2243

Kapitel II / Boolesche Funktionen

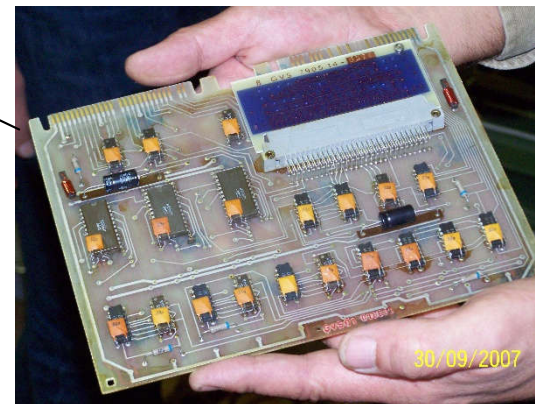
East German SKS V/1 and T-310



240 bits

“quasi-absolute security”
[1973-1990]

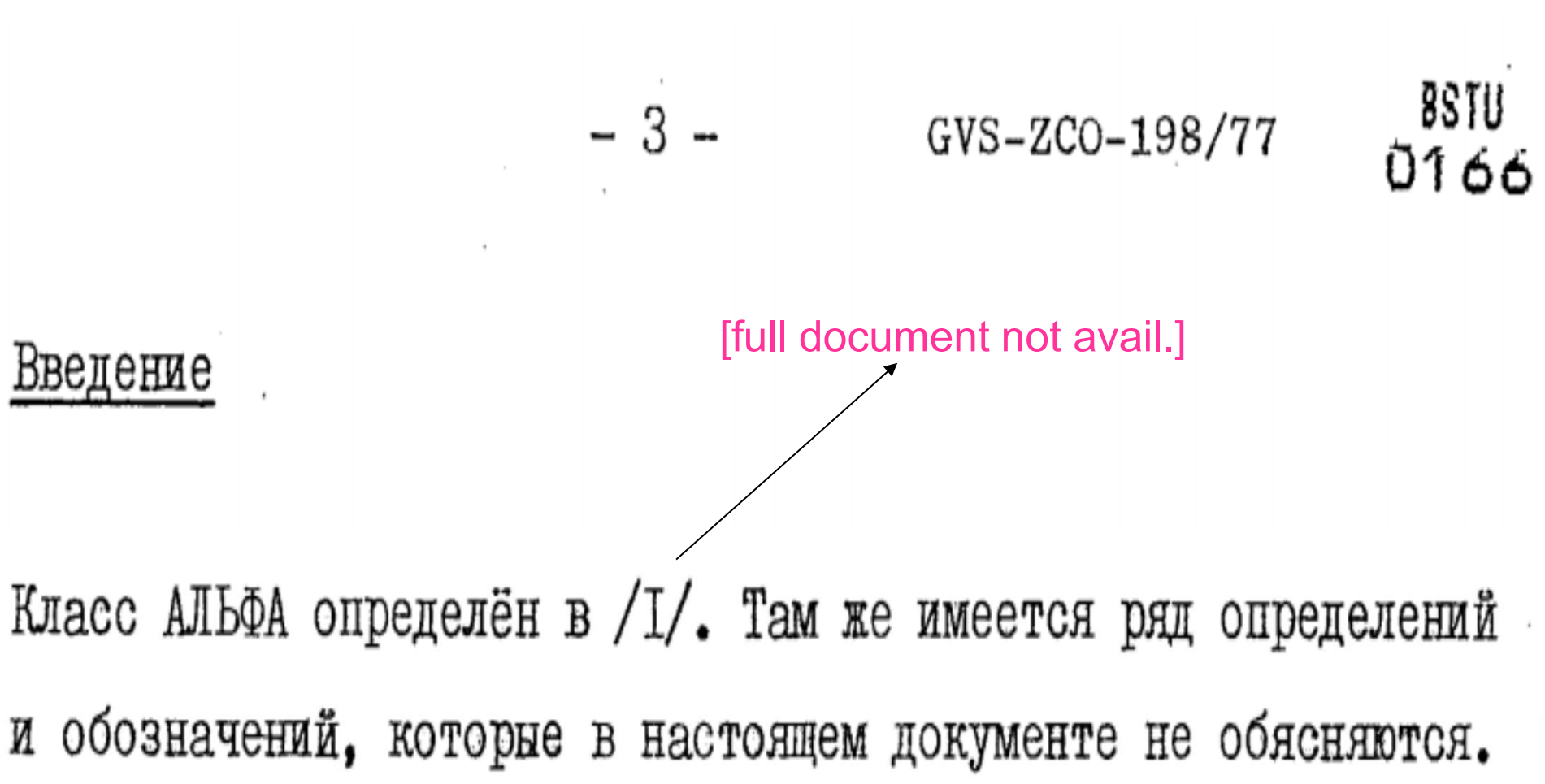
has a
physical
RNG=>IV



long-term secret
90 bits only!

Block Cipher Class Alpha = c.1970

obscure origins...



Differential Cryptanalysis = DC

Wikipedia DC entry says:

In 1994 [...] IBM [...] Coppersmith published a paper stating that DC was known to IBM as early as 1974.

[...] IBM had discovered differential cryptanalysis on its own
[...] NSA was apparently well aware of the technique.

Coppersmith explains: "After discussions with NSA, it was decided that **disclosure** of the design considerations would reveal the technique of DC, a **powerful technique** that could be used against many ciphers. This in turn would weaken the **competitive advantage the United States enjoyed over other countries in the field of cryptography**."

“Official” History

- **Davies-Murphy attack** [1982=classified, published in 1995] = early LC
- Shamir Paper [1985]..... early LC
- **Differential Cryptanalysis** :
Biham-Shamir [1991]
- **Linear Cryptanalysis**: Gilbert and Matsui [1992-93]

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:

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

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

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

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

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

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 18

Ergebnisse:

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

Discrete Differentials and HO DC – 1976 !

Definition 2.1-1

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

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 $j \neq l$,

Computation of Differentials for All Orders

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

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

.

.

.

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

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

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

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

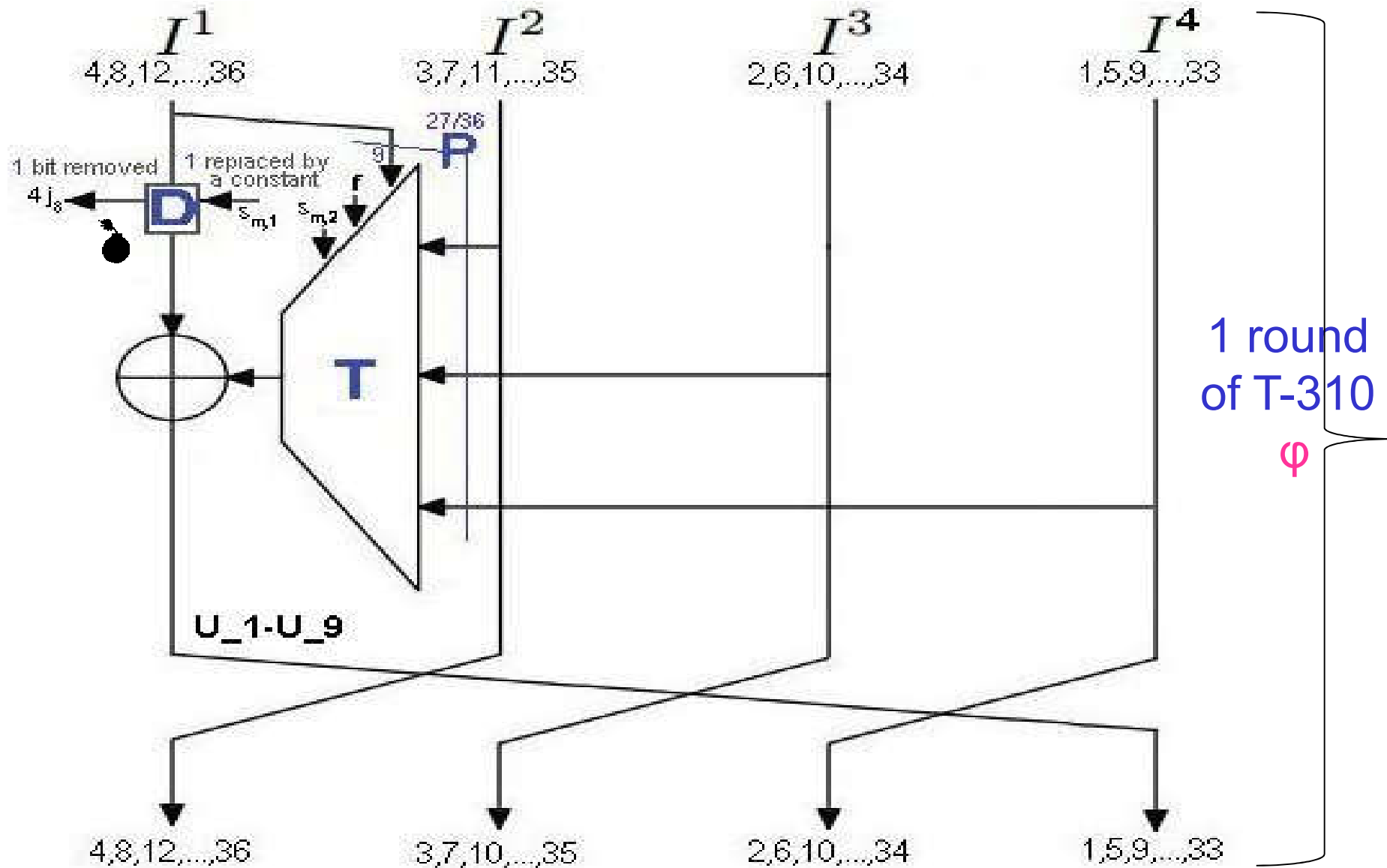
$$Z^{(1256)} = L$$

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

1970s, not 1990s...

- **Differential Cryptanalysis**
Biham-Shamir 1991
- **Linear Cryptanalysis:**
Gilbert and Matsui 1992-93

Contracting Feistel [1970s Eastern Germany!]



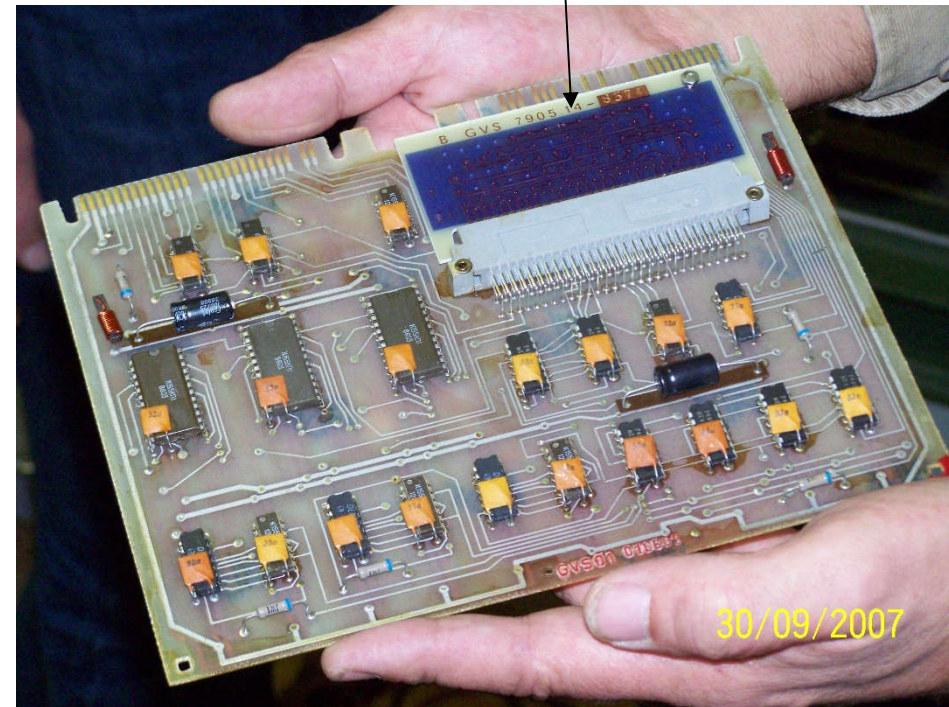
How to Backdoor T-310 [to appear in 2017]

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



bugs or backdoors?



False Backdoors = longer def =
strong properties of ciphers/systems/RNGs
which exist for NO apparent reason and which
are clearly counter-productive or harmful.

- in some cases a really good attack was never found!
- or maybe we just discovered $\frac{1}{2}$ of what we need to uncover?

Mystery Paper - Shamir 1985

On the Security of DES

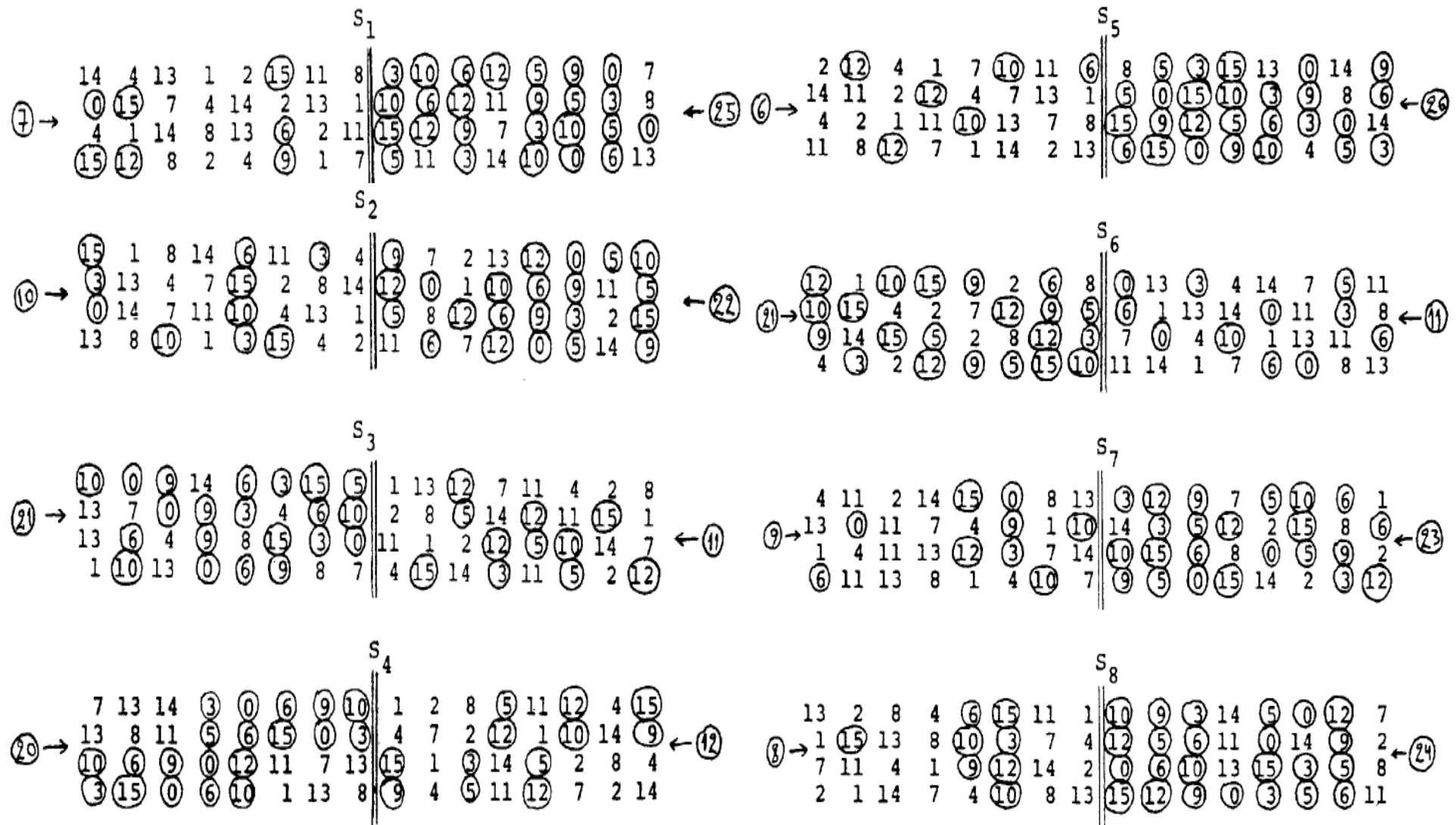
Adi Shamir
Applied Mathematics
The Weizmann Institute
Rehovot, Israel
(abstract)

The purpose of this note is to describe some anomalies found in the structure of the S-boxes in the Data Encryption Standard. These anomalies are potentially dangerous, but so far they have not led to any successful cryptanalytic attack.

Mystery thing.

Related to LC published 8 years later.

** Shamir 1985



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 !!!!

Mystery never explained, super strong pty,

We found more such properties [Courtois, Goubin, Castagnos [2003/184](#)]

Another Method to Backdoor T-310

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

P=1

703

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

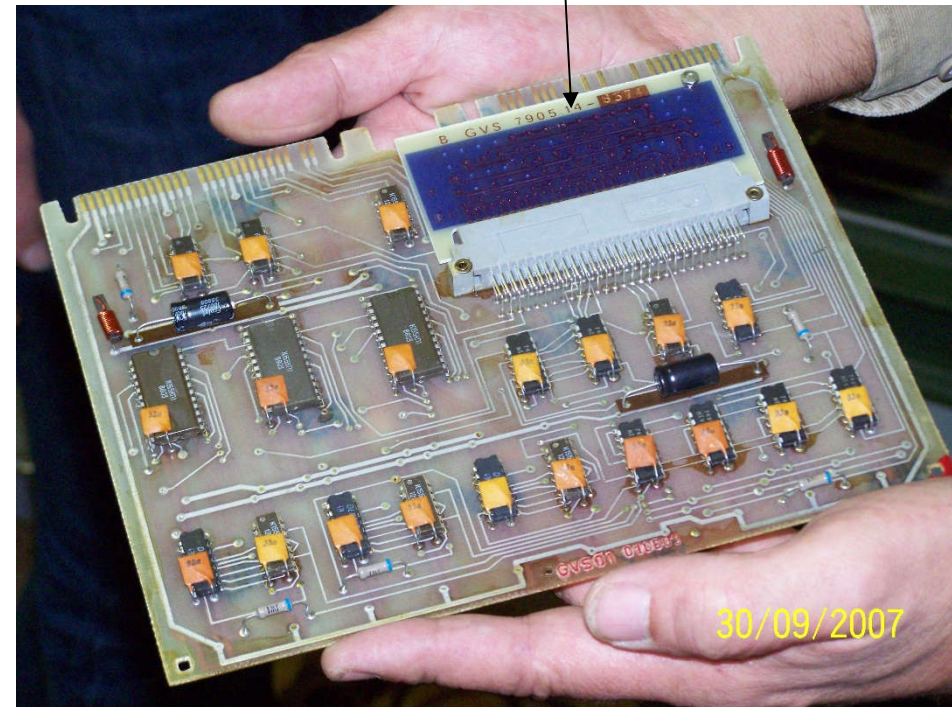
16,30,12,32,26,21,1,13,25,

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

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



bad long-term key



Another 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,

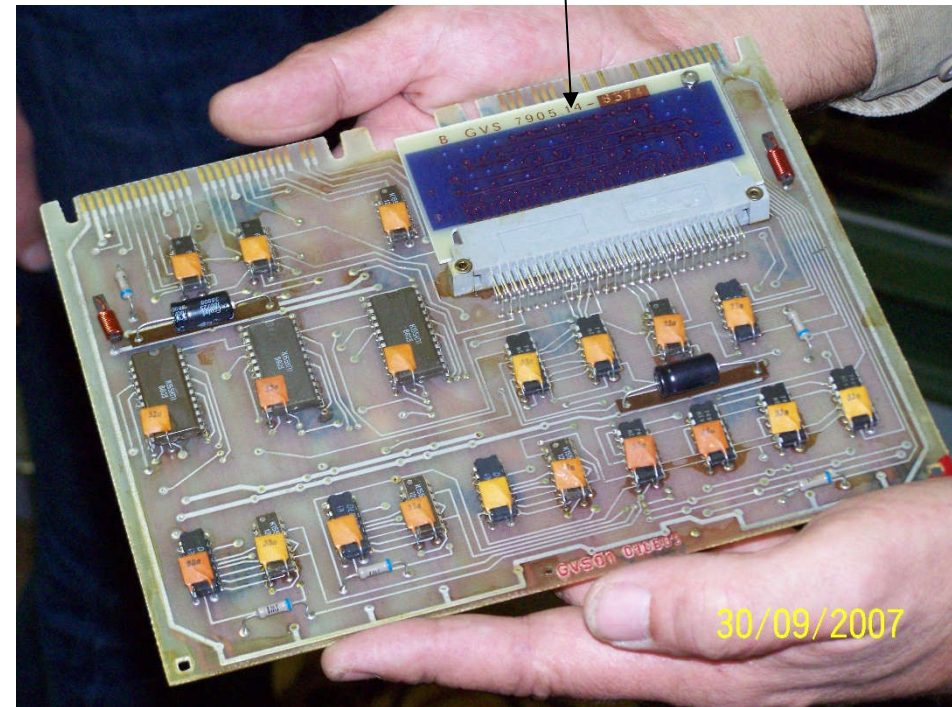
20,8,24,15,22,29,10,28,6

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



Backdoor NOT
KT1 compliant ☹

bad long-term key



New Backdoors [to appear in 2017]

Level 1: Non-bijective φ – **ALL broken!** See:

1. Nicolas T. Courtois, Maria-Bristena Oprisanu: “Ciphertext-Only Attacks and Weak Long-Term Keys in T-310”

and our long extended master paper:

2. Courtois et al, “Cryptographic Security Analysis of T-310”, eprint.iacr.org/2017/440.

New Backdoors [to appear in 2017]

Level 2: Bijective φ – secure???

- New attack to be published in 2017.

New Backdoors [to appear in 2017]

Level 2: Bijective φ and KT1 compliant –
secure???

- Fact: some KT1 keys have 10 Linear approximations true with $P=1$. Cf. [2017/440](#).
- Not exploitable due to super-paranoid low-rate cipher mode.

=> A percentage of keys is also broken,
another NEW attack to be published soon.

Open Problems

- Backdoor symmetric encryption?

GOST Cipher



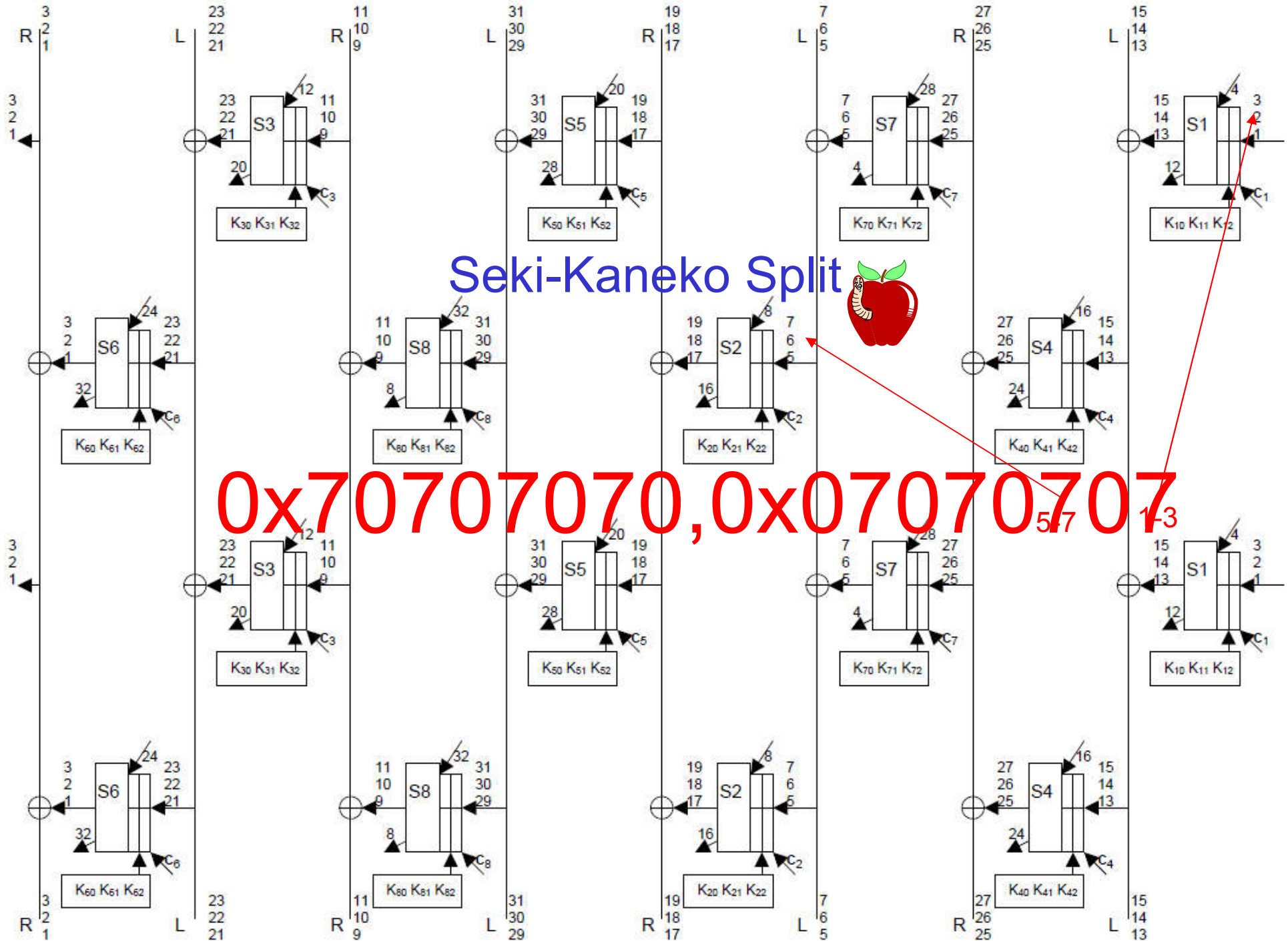
GOST 28148-89

- Developed in the 1970s, or the 1980s,
 - First "Top Secret" / Type 1/Type A algorithm.
 - Downgraded to "Secret" in 1990.
- Declassified in 1994.

Seki-Kaneko Split



0x70707070, 0x07070707



0x80700700, 0x80700700 [Courtois-Miszta 2011]

Type 3+3: S836 + S836

