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?

RNG

Practical Security Solutions

Block and Stream Ciphers

easy methods

Backdoors

much harder
Bad Randoms – 1930s – Enigma Message Keys

(should be 3 random letters)

AAA

XYZ

Operators always found a way to «degrade » their security
Crypto History
HistoCrypt / Euro-HCC

European Historical Ciphers Colloquium 2017
The European colloquium for the research on historical ciphers and encryption devices.

18-19 May 2017, Slovakia
18-19 May Program

Day 1 – 18th May 2017
Opening Conference and Welcome
K. Nemoga
09:00 - 09:15

The ‘Gustave Bertrand’ Tales — 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

Lunch
12:15 - 13:30

Session 2 – Session Chair: D. Turing
Slot 5: 13:30 - 14:00: K. Schmeh - 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. Guillerot - The priceless gift - The Polish cryptanalysis of Enigma
Slot 8: 15:30 - 16:00: M-J. Durand-Richard - Cryptology at Bletchley Park (1939-1945)

Day 2 – 19th May 2017
History of public key cryptography and RSA — Session Chair: B. Esslinger
J.-J. Quisquater
09:00-10:00

Session 3 – Session Chair: K. Schmeh
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 - Wolfenbüttel, 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

Closing Remarks
12:30 - 12:45

Lunch and/or departure
12:45 - 14:00
LinkedIn

Your Groups (51) Reorder »

Code Breakers Members (712)

IACR Cryptographers
Post-WW2 Crypto History
1960s

NATO Cipher competition

• UK
• US
• France
• Germany

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

French Submission

Actes du septième Colloque sur l'Histoire de l'Informatique et des Transmissions

Histoire de la machine Myosotis [2004]

Xavier Ameil, Jean-Pierre Vasseur et Gilles Ruggiu

Association des Réservistes du Chiffre et de la Sécurité des Informations

- large period, non-linearity / removing the correlations (p.108)
  “…certainement la meilleure machine cryptographique de son époque…”

Nicolas T. Courtois
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
MfS Abteilung 11 = ZCO =
Zentrales Chiffrierorgan
der DDR

MfS = Ministerium für Staatssicherheit
= Ministry of State Security of GDR = Stasi
BStU = Bundesbeauftragter
= Stasi Records
Agency =
a.k.a. Birthler authority
Backdoors

Nicolas T. Courtois

Our Sources

BStU = Stasi Records Agency
ZCO = Zentrales Chiffrierorgan der DDR
How do you say “ZCO” in Russian?
How do you say “ZCO” in Russian?
East German SKS V/1 and T-310

240 bits long-term secret

“quasi-absolute security” [1973-1990]

90 bits only!

has a physical RNG=>IV

long-term secret
Bugs or Backdoors?

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

- 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!
**Definition 3.1-1**

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

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

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

**Ergebnisse:**

**Tabelle 3.1-2**

<table>
<thead>
<tr>
<th>(\alpha)</th>
<th>(\Delta_\alpha^2)</th>
<th>(t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0 0 0 0</td>
<td>32 0</td>
<td>32</td>
</tr>
<tr>
<td>0 0 0 0 0 L</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>0 0 0 0 L 0</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>0 0 0 L L 0</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>0 0 L 0 0 0</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>0 0 L 0 L 0</td>
<td>-2</td>
<td>30</td>
</tr>
<tr>
<td>0 0 L L L 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>0 0 L L L L</td>
<td>2</td>
<td>34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(\alpha)</th>
<th>(\Delta_\alpha^2)</th>
<th>(t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L 0 0 0 0 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>L 0 0 0 0 L</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>L 0 0 0 L 0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>L 0 0 0 L L</td>
<td>6</td>
<td>38</td>
</tr>
<tr>
<td>L 0 0 L 0 0</td>
<td>-4</td>
<td>28</td>
</tr>
<tr>
<td>L 0 0 L 0 L</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>L 0 0 L L 0</td>
<td>4</td>
<td>36</td>
</tr>
<tr>
<td>L 0 0 L L L</td>
<td>2</td>
<td>34</td>
</tr>
</tbody>
</table>
**Discrete Differentials and HO DC – 1976**

**Definition 2.1-1**

\[
\frac{d^2 z(e_1, \ldots, e_6)}{de_i} = 2(e_1, \ldots, e_{i-1}, 0, e_{i+1}, \ldots, e_6) + 2(e_1, \ldots, e_{i-1}, L, e_{i+1}, \ldots, e_6)
\]

ist die einfache Ableitung der Booleanen Funktion z.

**Higher Order:**

**Definition 2.1-2**

\[
\frac{d^k z(e_1, \ldots, e_6)}{de_{i_1} \ldots de_{i_k}} = \left( \frac{d}{de_{i_1}} \left( \ldots \frac{d^2 z(e_1, \ldots, e_6)}{de_{i_k}} \right) \right)
\]

mit \(i_1, \ldots, i_k \leq 6\), \(k \in \{1, 6\}, i_j \neq i_k\) für \(j \neq k\).
Bugs or Backdoors?

Computation of Differentials for All Orders
1970s, not 1990s…

- **Differential Cryptanalysis**
  Biham-Shamir 1991

- **Linear Cryptanalysis:**
  Gilbert and Matsui 1992-93
Contracting Feistel [1970s Eastern Germany!]

1 round of T-310

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

omit just 1 out of 40 conditions:

$ciphertext-only$

bad long-term key
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 ½ 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

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 $\phi$ – 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:

New Backdoors [to appear in 2017]

Level 2: Bijective $\varphi$ – secure???

• New attack to be published in 2017.
New Backdoors [to appear in 2017]

Level 2: Bijective $\varphi$ 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.
• Declassified in 1994.
Seki-Kaneko Split

0x70707070, 0x07070707
Type 3+3: S836 + S836

0x80700700, 0x80700700 [Courtois-Misztal 2011]
0x80700700,0x80700700

Type 3+3: S836 + S836

Bugs or Backdoors?

© Nicolas T. Courtois, 2006-2013