UNIKASSEL VERSITÄT

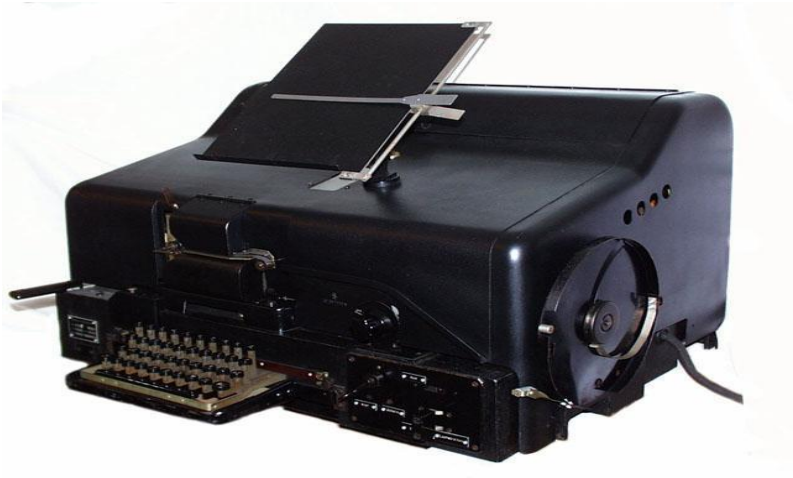
Angewandte Informations Sicherheit

Modern Codebreaking of T52

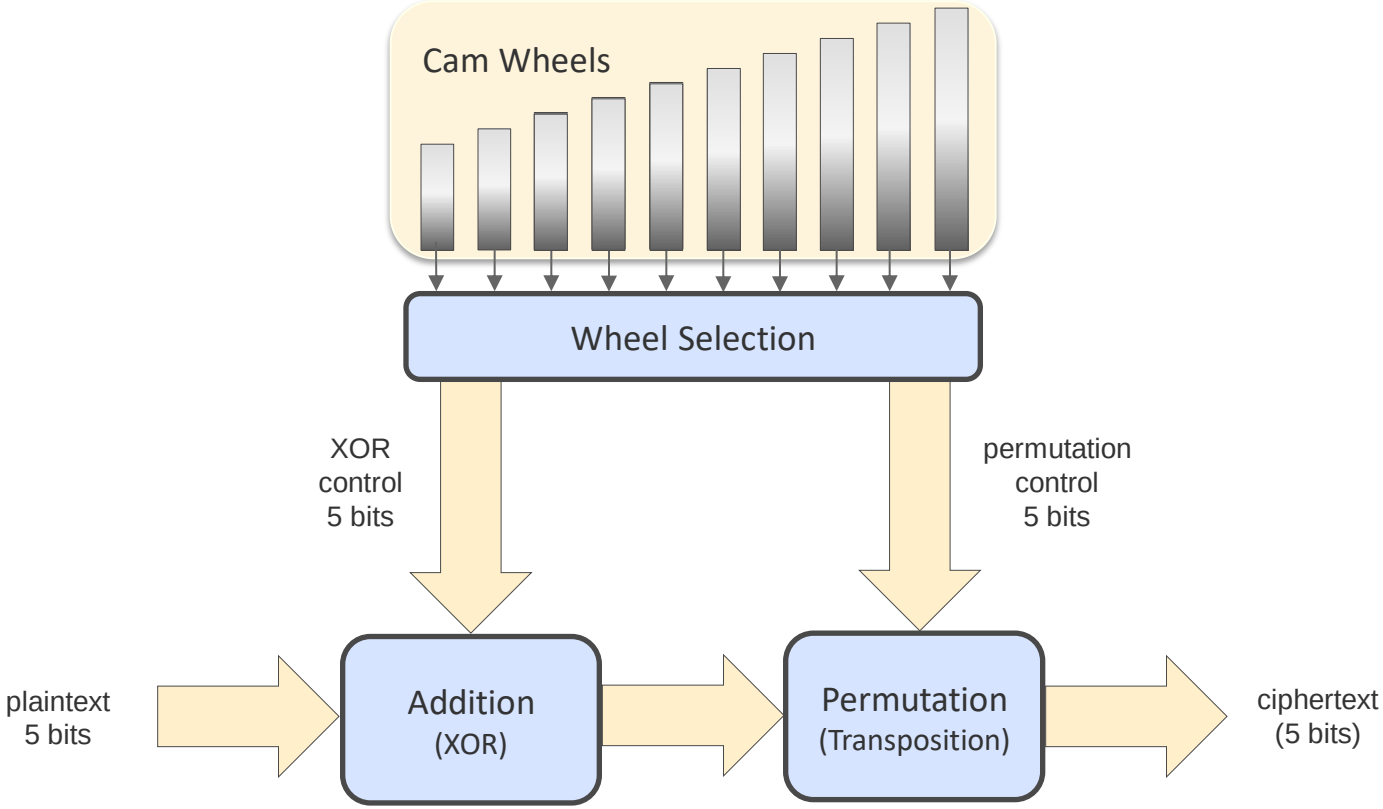
June 19, 2018
George Lasry
george.lasry@gmail.com

Agenda

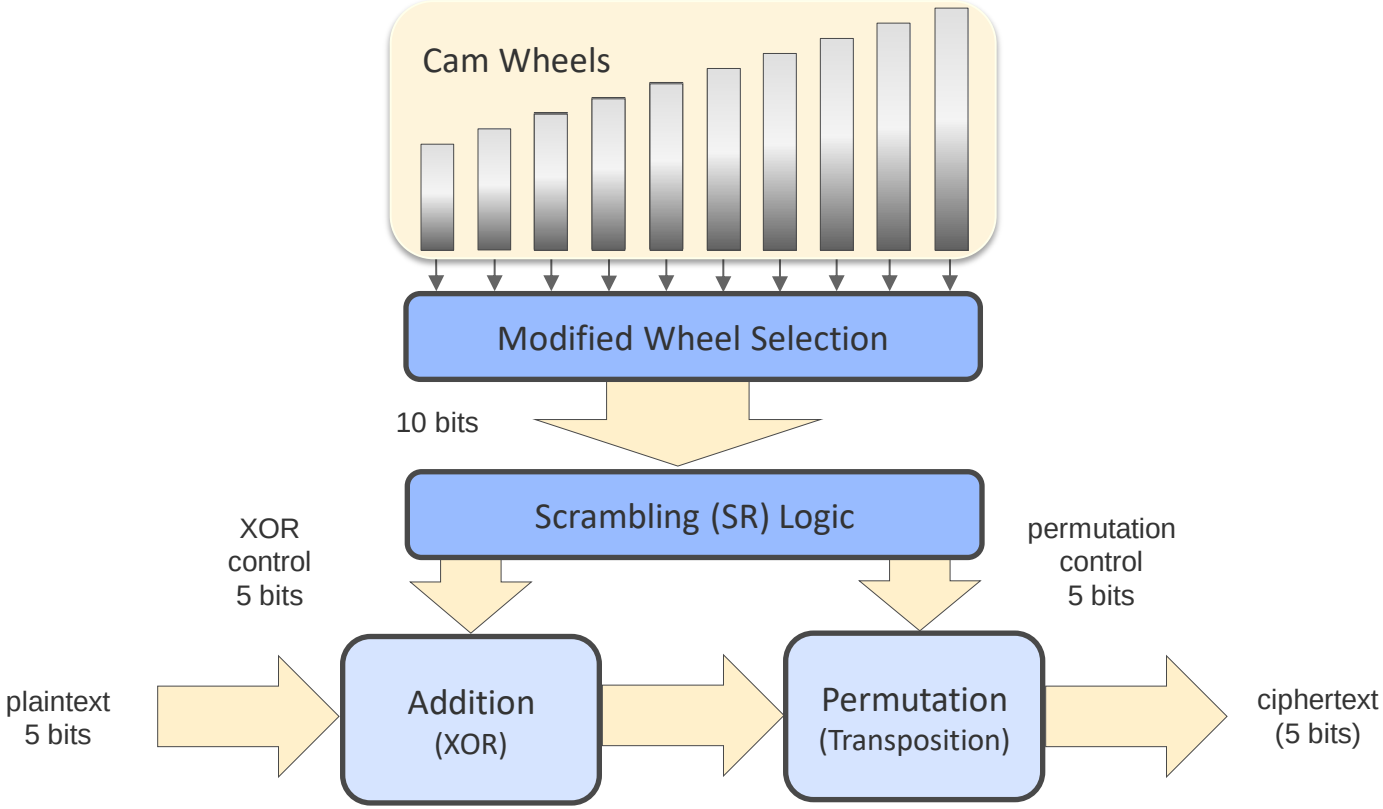
- T52 – description and evolution
- Historical codebreaking of T52
- New statistical attacks on early models
- Deciphering original messages
- A practical attack on late models



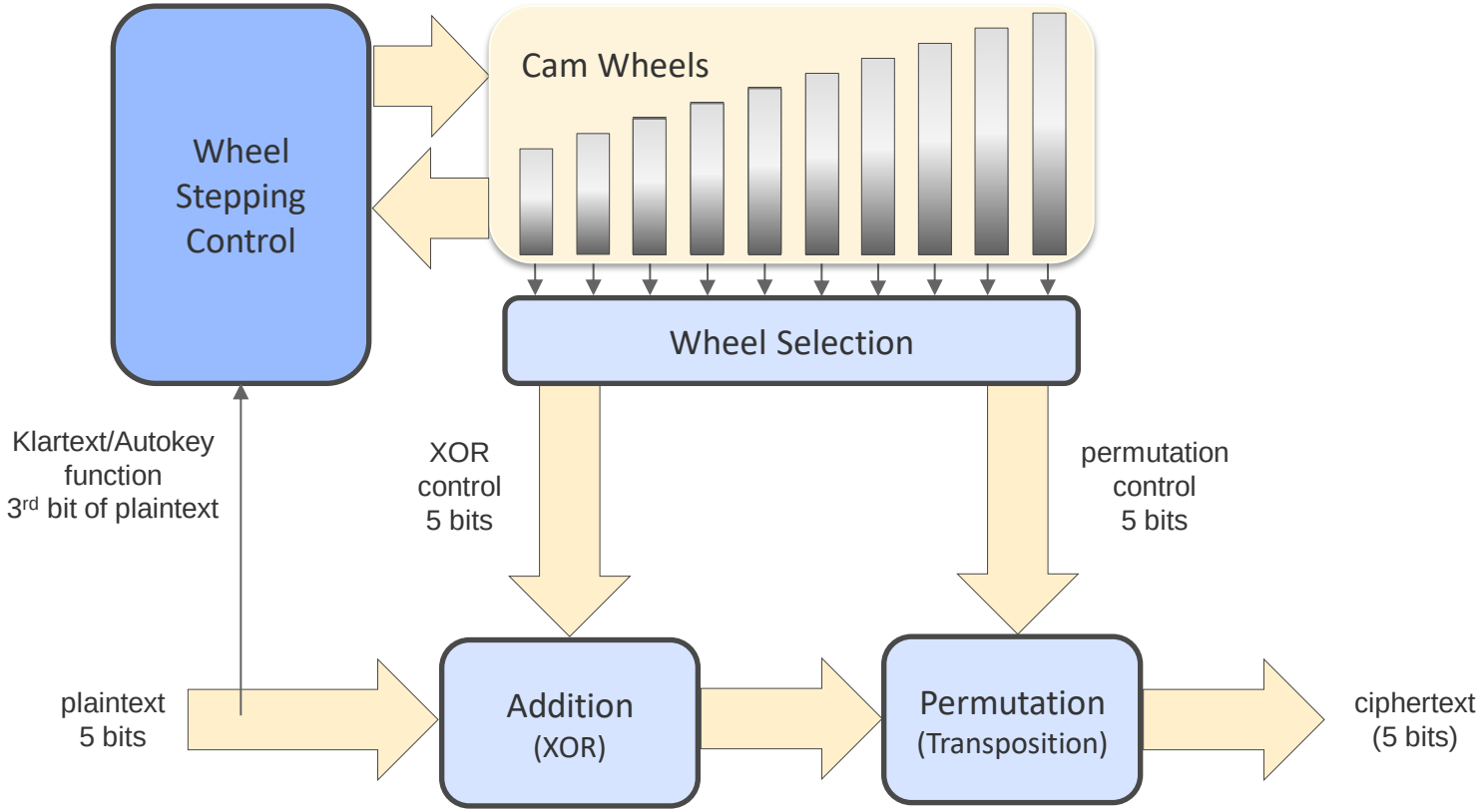
System Description – T52a/b



New Models – T52c and T52ca – Mid-End 1942

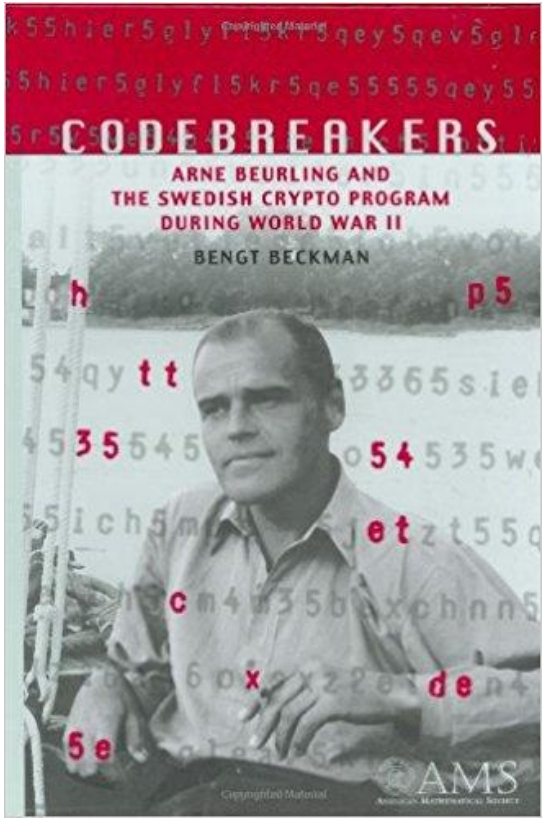


T52d – Irregular Stepping – Beginning of 1943

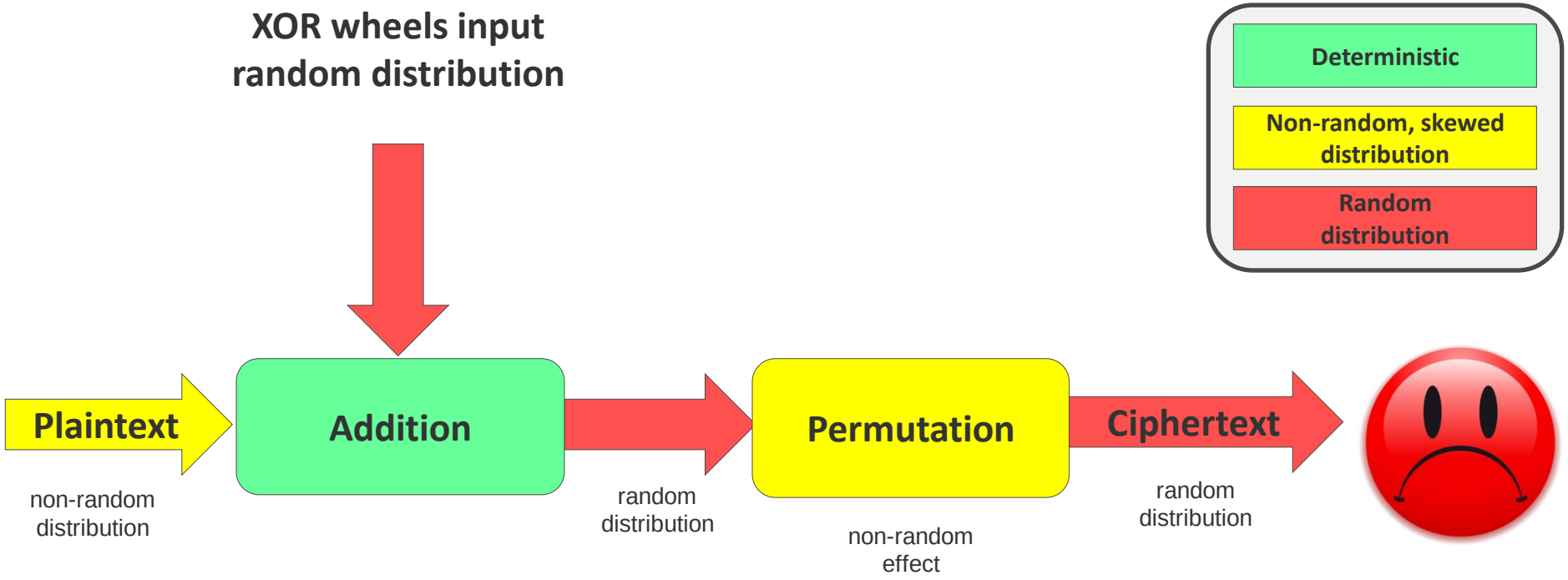


Historical Codebreaking

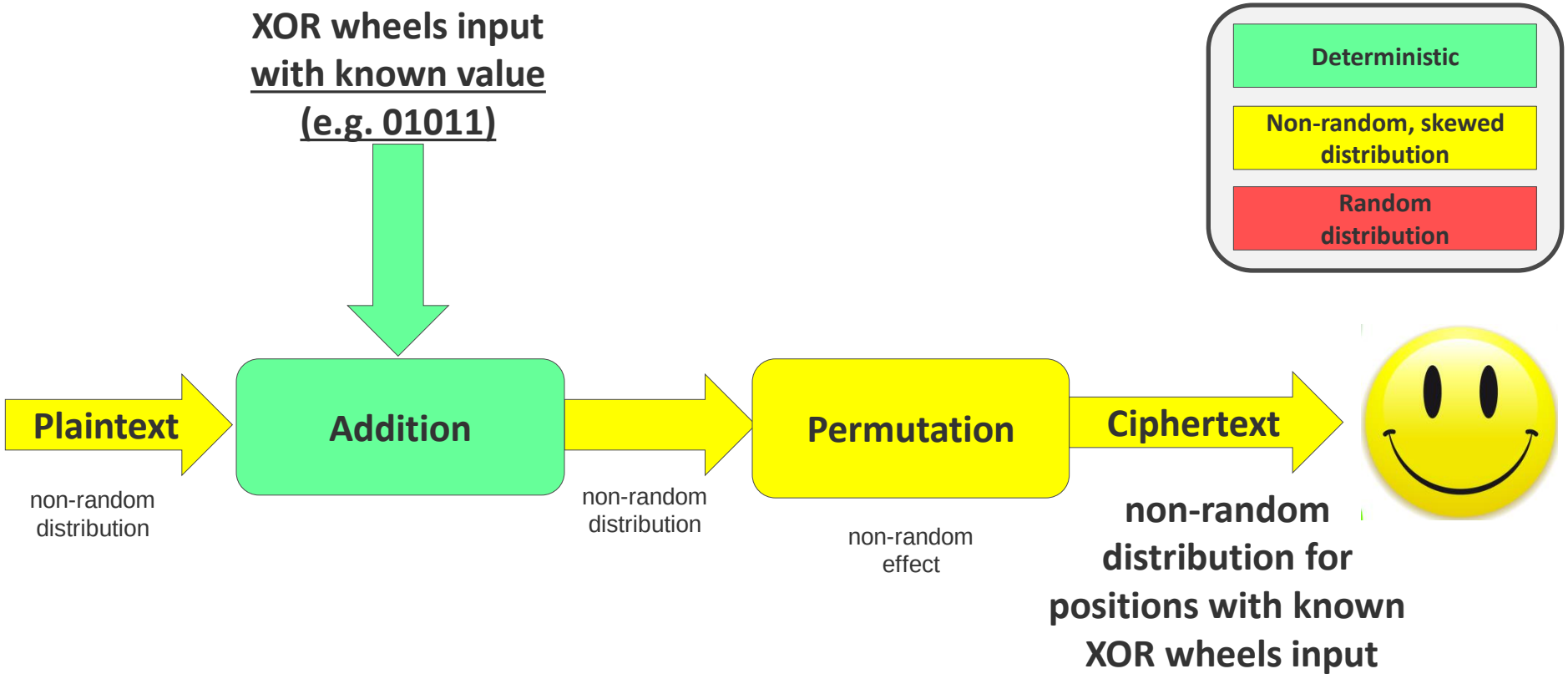
- **T52 reconstruction**
  - Arne Beurling
  - Bletchley Park
- **Attack on depths**
  - Messages encrypted with same key settings
- **Attack with crib**
- **Statistical attacks on T52a/b, T52c**
  - Developed by Sweden, Bletchley Park, German cryptographers
  - Require very long messages
- **No solution for T52d**



Statistical Analysis – T52a/b



Statistical Analysis – Deviation from Randomness

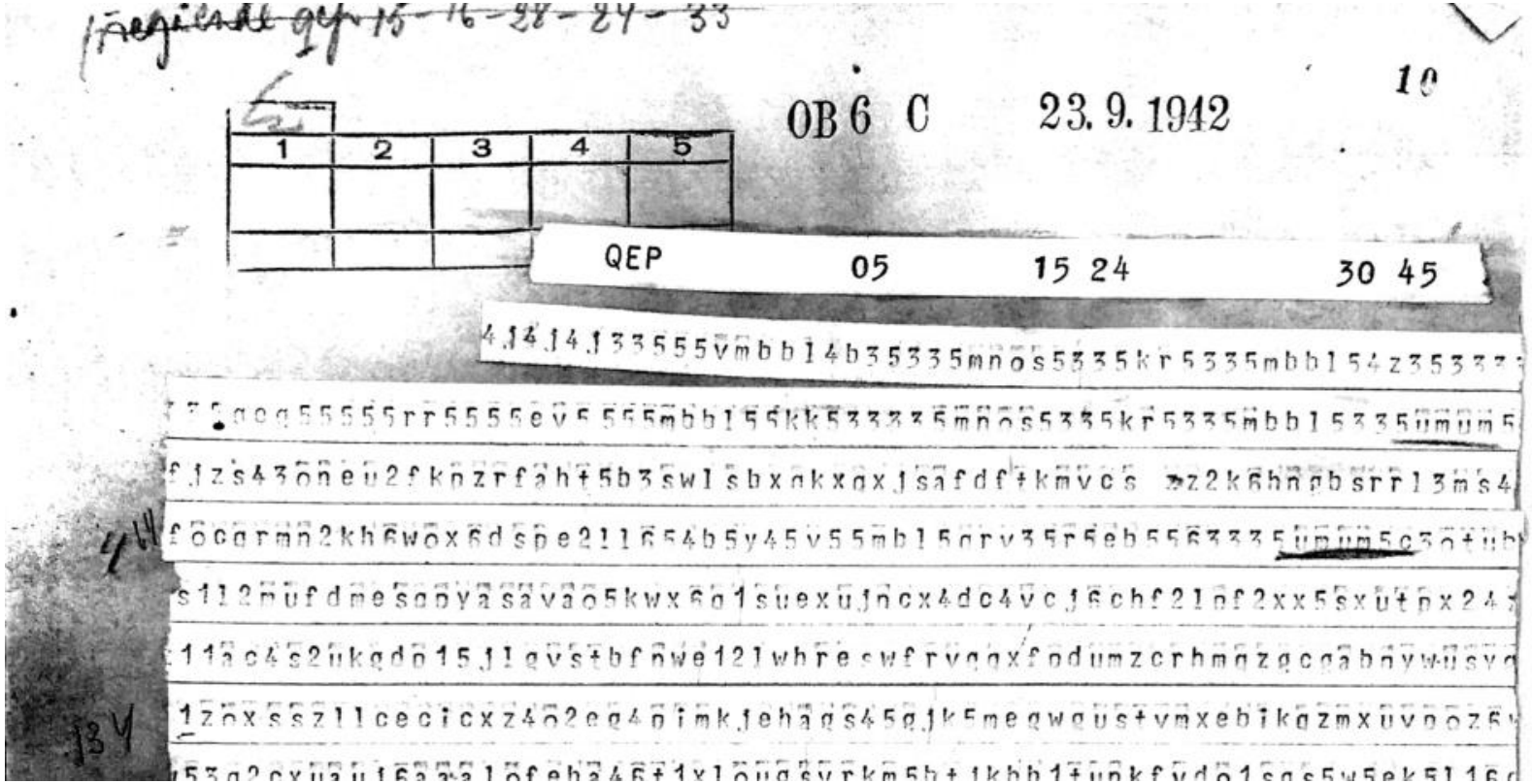


A New Ciphertext-only Statistical Attack

- **Find settings of XOR wheels**
  - Ignoring the rest
  - Maximize deviation from randomness
- **Reduces search from 10^{27} to 10^{18} options**
  - Still a lot, but **probabilistic search works** (“hillclimbing”)
  - Solution in minutes for T52a/b
  - Also for T52c and T52ca with adaptations

```
 2017][   4498295-         0][C:    1444] [ 3/ 6] -   0.058663 (0
4EDKYC3GMF33Y33KV54V34EXQB3Y3333333AN2QZF34MA3B53A3F3FQQC554DEE55
<3w(6:>GMF>>Y>>KV <=><3/1?>Y>>>>>>>AN QZF><.->B >A>F>FQQC  <w33
 2017][   4498301-         0][C:    1450] [ 3/12] -   0.059359 (0
4EDKYCBGMF33Y3BDN54X3OEXQB3Y3333333AN2QQF34MA3B53A3F3FQQC554KEE55
<3w(6:?Ö.Ü>>Y>BDN </>OEXQB>Y>>>>>>>AN QQF><.->B >A>F>FQQC  <(33
 2017][   4498306-         0][C:    1455] [ 3/17] -   0.066055 (0
XEKK3C3GGU33333DN54V3OE4Q33Y3333333AN5QQF34MA3353A333FQQCC54KEEU5I
XEKK>C>GGU>>>>>DN <=>OE<1>>Y>>>>>>>AN QQF><.->> >A>>>FQQCC <(337
 2017][   4498456-         0][C:    1605] [ 6/19] -   0.070561 (0
OYKX3333G33F333DN54K3RE4L33533333334N5QQFC4MAF353A3333QQCC54KEBUUI
OYKX>>>>G>>F>>>DN <(>RE<)>> >>>>>>><, 11Ü:<.-Ü> >A>>>>QQCC <(3?77
 2017][   4498488-         0][C:    1637] [ 6/51] -   0.070816 (0
XEKK333G33C3M33DK54V3OEVL3353333333AN5QSCC4MAF353A333FQQCC54KEBU5I
XEKK>>>G>>C>M>>DK <=>OEVL>> >>>>>>>AN QSCC<.-Ü> >A>>>FQQCC <(3?7
 2017][   4498496-         0][C:    1645] [ 6/59] -   0.081581 (0
OE4K33333333333DK54K3OE4L3353333333AN5QQCC4MA3353I3333QQCC54KEEUUI
```

Deciphering Original Cryptograms – FRA Archives



Order of Battle of German Navy in Norway – Sept. 23, 1942

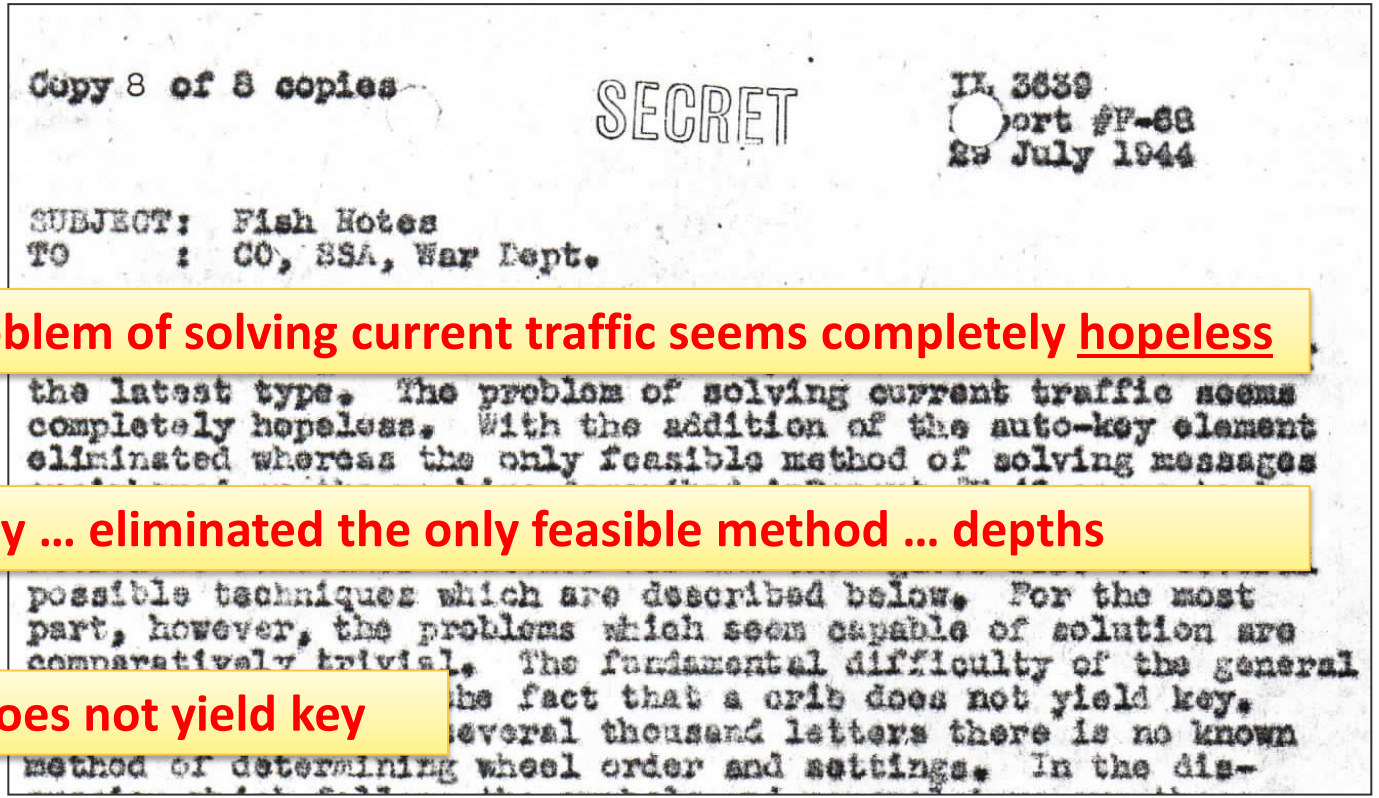
GEHEIM - STANDORTUEBERSICHT DER SEESTREITKRAEFTE IM NORWEGENBEREICH V 23/9 42 1000 UHR
IN SEE: R BEITZEN , E STEINBRINCK , CHEF 8 ZFL M Z 2,23,30,5 ZFL M FR
ECKHOLDT , M 302, 381, 382, M 1106,1107,1108, R 151,153,154,155,157, 173, 160,161,
GRFBT JORDAN , LAZSCH STUTTGART , UJ 1101, 1103, 1104, 1106, 1108, 1112,
NETZTD 10, MS ROLAND, MS SKAGERRAK, MRS PARIS
OSLO : SPERRBR 22.-
STAVANGER: UJ 1708.-
BERGEN: LAZSCH GLUECKAUF, UJ 1709 , 1711.-
DRONTHEIM: PLBT RUDEN, NETZSPERRGR NORD, M 31, R 58, 59, 64, R 156,
NARVIK : Z 29, T 9, 12, M 205, 253, TROSZSCH NORDMARK, KAERNTEN
HARSTAD : M 36, 81, 101, 132, 255, SCHIFF 31.-
TROMSOE : M 301, 321, 322, UJ 1109.- ALTA : Z 28, DITHMARSCHEN , MS IRBEN .-
KIRKENES : LUEDERITZ , R - BGLSCH WESER, BEATRIX, RENATE, LAZSCH METEOR, ...

MS - Minenschiff (Mine layer), M - Minensuchboote (Minesweeper), MRS - Minenräumschiff Minesweeper), UJ - U-bootsjäger (Submarine hunter)
Sperrbrecker (Mine barrage breaker), Lazarettschiff (Hospital ship), PLBT - Peilboot (Direction finding boat), T - Torpedoboot (Torpedo boat),
Z - Zerstörer (Destroyer), Trossschiff (Supply ship), R - BGLSCH - Räumbootbegleitschiff (Minesweeper supply ship), Lazarettschiff (Hospital ship):

Other Telegrams – Sept. 22-23, 1942

From/To	Topics
Kirkenes listening station to OKM Funkaufklärung (B-Dienst)	**Retransmission in full of Russian Navy codes**, e.g. from Konin Peninsula. Includes frequencies (e.g. on 480 m - 625 kHz, and 2200 m - 136 kHz), and Russian call signs (from P1M1 to K7R7, W7R1 and W7W1). Report about broadcast message from the Chief of the Russian Nordmeerflotte. Reporting keyword (Stickwort) MARWA and location (as 3935 North, 3308 East). Reports on Russian submarines (5934) and **British Navy activity ("very busy in the Arkhangelsk area").**
OKM weather service (WEWA OKM) and weather stations in Bergen, Trondheim, Tromsø	Vacation of Dr. Collmann via Berlin. Weather signals. Weather data from balloons and radiosonde. Reports on interference from other transmissions
(missing)	Shipping report from 22 September about ships entering the harbours of Narvik and Harstad.

T52d – A Hopeless Problem? (Bletchley Park, July 29, 1944)



Copy 8 of 8 copies

SECRET

IL 3639
ort #F-68
29 July 1944

SUBJECT: Fish Notes
TO : CO, SSA, War Dept.

the latest type. The problem of solving current traffic seems completely hopeless. With the addition of the auto-key element eliminated whereas the only feasible method of solving messages

possible techniques which are described below. For the most part, however, the problems which seem capable of solution are comparatively trivial. The fundamental difficulty of the general he fact that a crib does not yield key. several thousand letters there is no known method of determining wheel order and settings. In the dis-

The problem of solving current traffic seems completely hopeless

auto-key … eliminated the only feasible method … depths

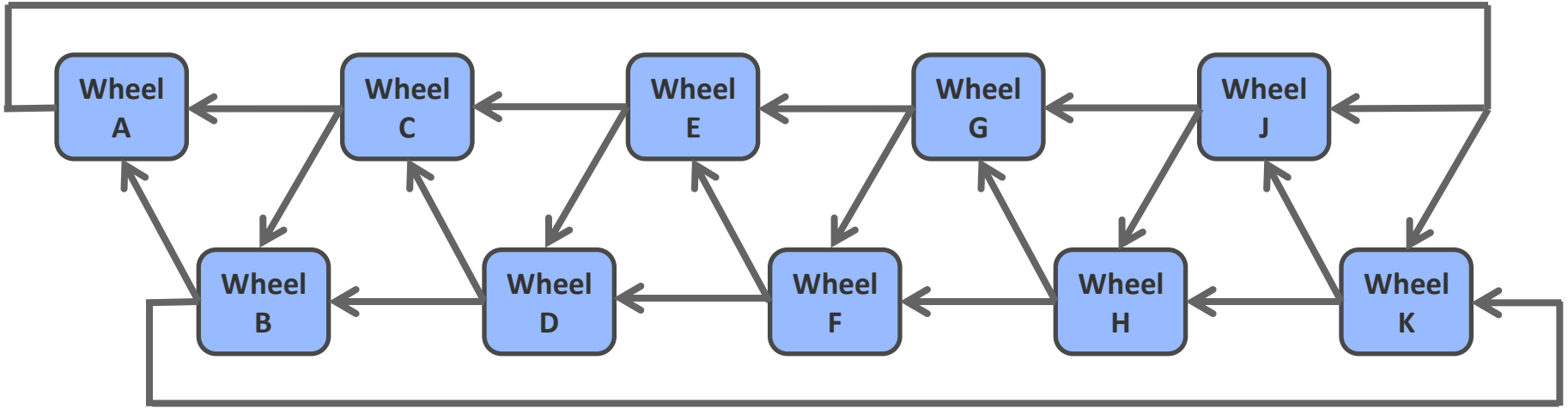
a crib does not yield key

Modern Known-plaintext ("Crib") Attack

- **10 letter crib**
- **Recursive, incremental search**
  - One wheel after the other
  - Test all starting positions
  - Backtrack if contradiction is found
- **Solution in minutes for T52a/b**
  - Instead of testing 10^{27} options
  - In days for T52c/ca, using longer crib
- **Does not apply to T52d**
  - Stepping depends on other wheels

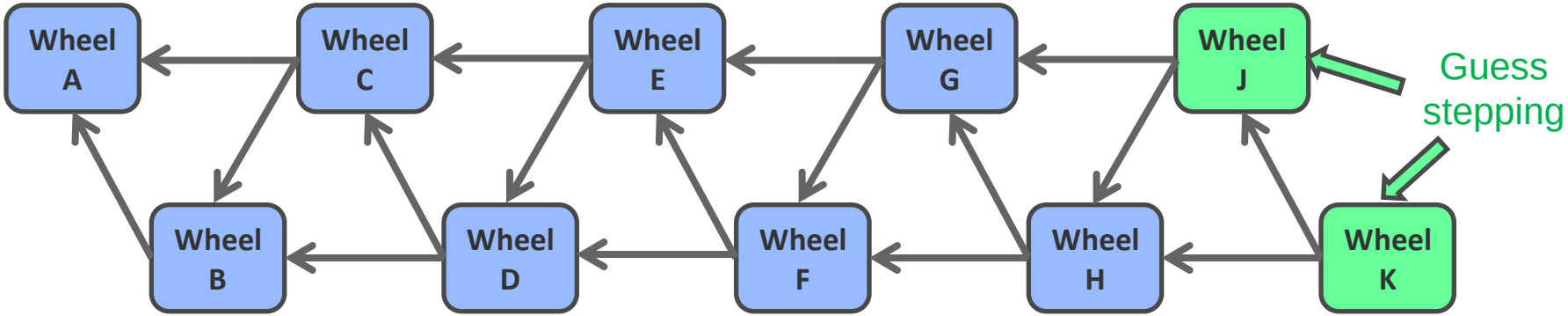
```
Searching for crib match:
Ciphertext:
GW4AKUNA614QYLEUWHD1DFFSKKGOE…
Plaintext:
5QRV4B35RR5
Without special characters:
 QRV ?  RR
....... Searching ........
Solution found with Key:
05:69:18:07:28:63:08:03:52:06
I:V:III:1-2:7-8:II:9-10:3-4:IV:5-6
Elapsed - 122 seconds
```

T52d – Stepping Control Dependencies (KTF Mode)



Problem: Can't know how a certain wheel steps unless/until we know the positions and stepping of its two predecessors. But the graph is circular!

Known-plaintext Attack – T52d and T52e



Solution: **Guess the stepping of the first 2 wheels** (J and K). Then process H, G, F, … until A. Then verify assumption.

In practice, for a crib of 10 letters, this means testing $2^{(10-1)}*2^{(10-1)}$ = about 250,000 options.

Known-plaintext Attack – T52d and T52e

- **For the first time, crib does yield key**
  - Not hopeless anymore, but 75 years too late ☺
- **T52d**
  - Thousands of computers x days
    - Instead of 1 computer x minutes as for T52a/b
  - Costly, but feasible!
  - Also works in Klartext (autokey) mode
- **T52e**
  - Attack requires longer cribs
  - 100 times more processing time
  - Not practical, unless parts of the key are known

UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

Special thanks to Anders Vik for discovering some unique original cryptograms, and to Frode Weierud and Geoff Sullivan for their landmark research and their constant support for this project. Additional thanks to Toby Anderson and Sandy Zabell for providing access to key documents.

Thank You

June 19, 2018
George Lasry, Ph.D.
University of Kassel, Germany
george.lasry@gmail.com

Further reading:

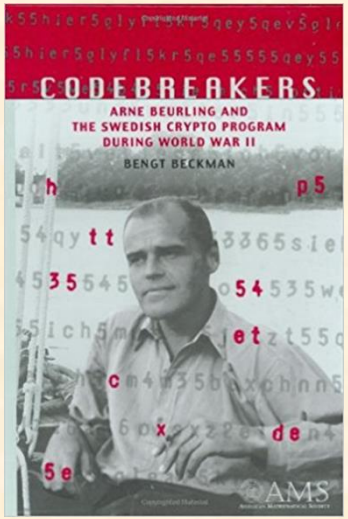

The Rutherford Journal
rutherfordjournal.org

Bletchley Park's Sturgeon, the Fish that Laid No Eggs

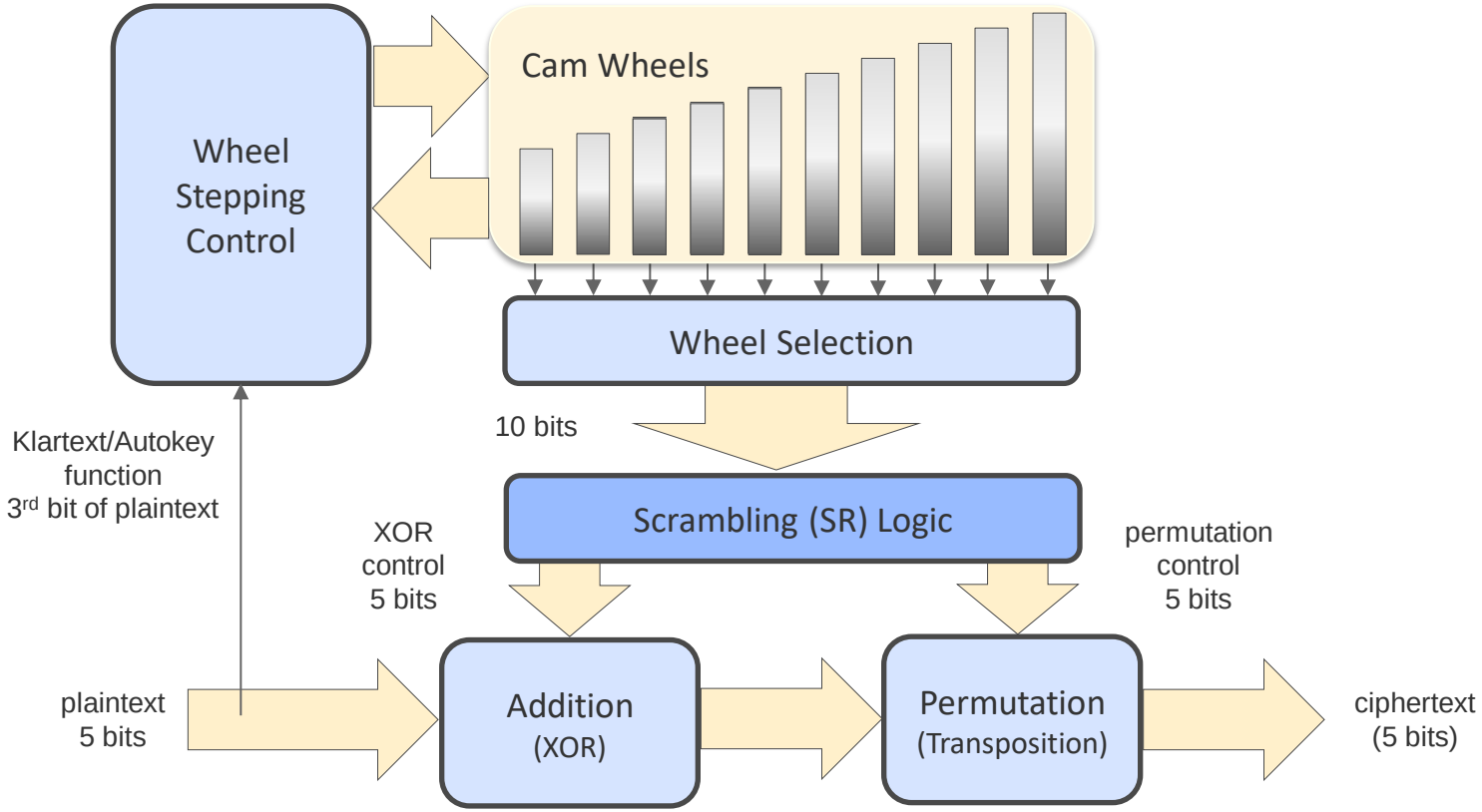
Frode Weierud

Introduction

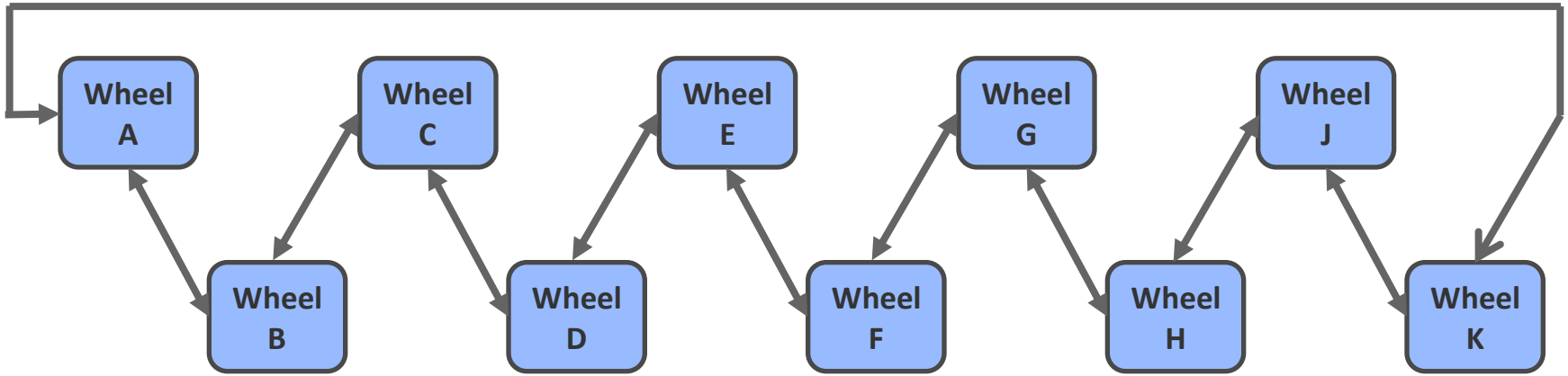
The German armed forces employed three different types of teleprinter cipher machines during the Second World War, the Lorenz machines SZ40 and SZ42 also called Tunny by Bletchley Park (BP), the Siemens & Halske *Schlüsselfernschreibmaschine* (SFM) T52, and the one-time-tape machine T43, also manufactured by Siemens.[1] The Lorenz machines, which existed in three different models, SZ40, SZ42a, and SZ42b, are well known as the machines that were broken at BP with the aid of Colossus. The Siemens T52 existed in four functionally distinct models, T52a/b, T52c and T52ca - which was a modified



T52e - 1944-1945



T52d – Protecting Against New Attack



Full, bi-directional circle. Cannot break circular dependencies by guessing the stepping of any 2 wheels.