RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 25 = 546 (2021): 51-77
DOI: https://doi.org/10.21857/y26kec4k89

ON WEAK ROTORS, LATIN SQUARES, LINEAR ALGEBRAIC REPRESENTATIONS, INVARIANT DIFFERENTIALS AND CRYPTANALYSIS OF ENIGMA

Nicolas T. Courtois, Marek Grajek and Michał Rams

Abstract. Since the 1920s until today it was assumed that rotors in Enigma cipher machines do not have a particular weakness or structure. A curious situation compared to hundreds of papers about S-boxes and weak setup in block ciphers. In this paper we reflect on what is normal and what is not normal for a cipher machine rotor, with a reference point being a truly random permutation. Our research shows that most original wartime Enigma rotors ever made are not at all random permutations and conceal strong differential properties invariant by rotor rotation. We also exhibit linear/algebraic properties pertaining to the ring of integers modulo 26. Some rotors are imitating a certain construction of a perfect quasigroup which however only works when N is odd. Most other rotors are simply trying to approximate the ideal situation. To the best of our knowledge these facts are new and were not studied before 2020.

1. Introduction

In modern cryptography we study block ciphers such as DES or AES, and we have almost forgotten about how cryptography has developed before, during and after the World War 2. There are essentially two major periods in encryption. We have rotor machines in 1920s-1960s and the development of code breaking machines and methods to cryptanalyse ciphers with ever increasing complexity. Then we have block ciphers in 1970s-now and the development of academic crypto research. In our work we emphasise the strong connections between these two worlds: rotor machines and block ciphers are not completely different worlds and they produce similar sorts of key dependent permutations with several layers of encryption. When the AES cipher was standardized in 2000, many researchers studied the AES S-box, which is a peculiar permutation with a very strong algebraic structure, and many

2020 *Mathematics Subject Classification.* 94A60, 68P25, 20N05, 05B15, 13A50.
Key words and phrases. Enigma, block ciphers, linear cryptanalysis, differential cryptanalysis, weak keys, Latin squares, algebraic representation, quasigroups, Turing-Welchman attack.

unusual properties, cf. [11,15]. Previously for DES, researchers studied linear differential and more general attacks carefully [16, 22, 23]. However for many other ciphers, in particular old ciphers, similar questions were never studied until now. Rotors are just considered to be some permutations, presumably random permutations. In fact as it seems no one suspected that these permutation building blocks would have any unusual properties whatsoever. Our research shows that they have very strong properties.

This paper is organised as follows. In Section 2 we review the history and main significant weak points of Enigma cipher machines. In Sections 2.5 and 2.7 we will briefly summarize the new properties which we study in this paper. In Section 3 we study the Enigma rotors and how the secret key acts on the rotors. In Section 4 we look at the question of how a table of permuted alphabets for one rotor can be weak or special in general, and we study one particularly weak rotor from 1930. In Section 5 we present our general possibility and impossibility result for any N. In Section 6 we study differential properties of Enigma rotors which are very special for almost all real-life rotors. In Section 7 we look at the probability that what we observe would happen for a random permutation. Then we have a conclusion.

2. Encryption with military Enigma machines

Military Enigma cipher machine was used primarily by Germany, in 1930-1960s. It is a complex cipher machine which generates a different permutation for each consecutive character of the plaintext. It should not be confused with the so called commercial Enigma which was sold on open market since approx. 1925 and was substantially less secure.

The main difference between the two machines is the presence of stecker, or a plugboard, which adds an excessively complex permutation which was an involution swapping some 6 to 10 letters, not all, and which was changed every day. The number of possible settings for the stecker varied in different historical periods but was always vastly superior than the number of distinct setting for the rotors. It was 2^{47} typically with 10 pairs being swapped. Military Enigma was essentially the most secure Enigma machine in wide deployment in 1930s and until 1945 and the stecker was the most complex component of it.

2.1. *On security of commercial Enigma.* The commercial Enigma was very weak and it was broken in 1920s by the so called "rodding" attack which consists of guessing the position of the fast rotor given some probable plaintext, it allows simply to "peel off" the external layer of encryption. Then the attacker can confirm if we obtain consistent pairs which belong to a permutation which is also going to be an involution. Examples of how this works can be found in [9, 18]. With high probability the slower rotors are not moving at all, otherwise the attack will not work correctly.

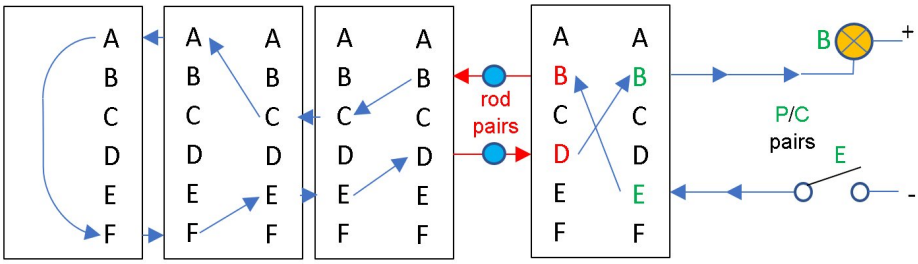

FIGURE 1. A commercial Enigma without a stecker and rodding attacks

Officially this attack is attributed to Dilly Knox, who has become the chief cryptographer at Bletchley Park when the WW2 started. In fact this attack is substantially older. According to Mavies Batey [4] who worked on this under direction of Dilly, "everybody who tried cryptanalysis of the commercial Enigma machine arrived at the rod solution". This was known in France and probably in the US by Friedman and Driscoll. It actually had a French name: Les Bâtons. Since 1935 French and British intelligence services had collaborated on monitoring and decryption of Italian Enigma traffic in the Spanish Civil War. Another name for this attack is the Method of Isomorphs and it was made public in 1946 by Rosario Candela, cf. page 281 in [5]. In contrast, the attack was not known to Rejewski in Poland in 1939, cf. [37,38]. We are also told that this attack was known in Germany. According to page 281 in [5] knowing this attack was the MAIN reason for the introduction as early as in the late 1920s, of the stecker in military Enigma machines.

2.2. *On weakness of Enigma machines.* In this paper when we talk about Enigma or a weakness of Enigma, we always mean the military Enigma WITH a stecker.

Enigma had several very important structural weak points which made cryptanalysis easier than expected. The most famous ones are:

1. Every permutation they produce is an involution.
2. A letter cannot be encrypted to itself.

These weak points are discussed every day if you visit a museum such as in Bletchley Park, Buckinghamshire, United Kingdom. However Enigma has other important points of tremendous weakness, which are less frequently mentioned. For example, we have:

3. The stecker (plugboard) is an involution.
4. The stecker (plugboard) is semi-transparent, and with probability at least 6/26 the output is equal to the input.

5. The stecker (plugboard) is situated in the last (outside) layer of encryption, it is connected directly to ciphertext and the plaintext letters.

The property 3. was essential in the design of the so called diagonal board, which was an enhancement invented by Gordon Welchman and added to the bombe code breaking machines initially developed by Turing [41]. The property 4. was sometimes exploited just before WW2 started and is somewhat essential in the working principle of the so called Polish bombe, which was developed in 1938-1939, [37,38]. However later it was not exploited a lot until... 1995 when modern ciphertext-only attacks on Enigma were first developed [29]. This was apparently never done before 1995, wartime code breaking relied initially on the initialisation procedures until May 1940, [37]. Then with Turing-Welchman bombes cf. [9] relied on cribs, i.e. highly probable plaintexts making it a Known Plaintext Attack.

In addition, there is another well-known weakness of wartime Enigma, which is rarely discussed as it is usually silently assumed and taken for granted:

6. Enigma rotors move in an odometer-like simple way (a.k.a. cyclometric method) where fast rotor moves all the time, and other rotors almost never move.

It turns out that this property is rather completely accidental, and we are very lucky it is this way, and we are wrong never to discuss it because it could have been otherwise. According to various sources combined at `cryptomuseum.com` and [5] German Reichsmarine started experimenting with Enigma C around 1925 and these machines did not have a stecker. Then it seems that Germany decided to make these machines more complex and more secure. In the Reichswehr another model, Enigma G, was introduced in July 1928 by Major Rudolf Schmidt. It had a relatively complex rotor movement for that time (with multiple rotor turn-overs) but it did not have a stecker. It is an incredible accident, that later in 1930 the German army introduced another different Enigma machine, with simpler odometer-like rotor movement (a.k.a. cyclometric method), and with a stecker.

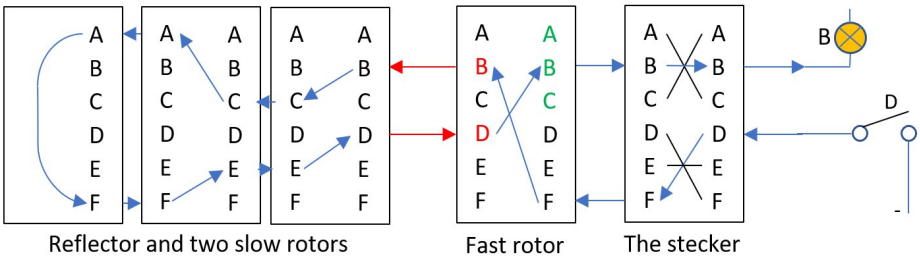

FIGURE 2. A military Enigma with a stecker.

The development of this exact version is attributed to a German crypto engineer and serial inventor Willi Korn from Berlin, cf. page 114 in [5]. This machine was later adopted by all German armed forces [5]. As a result, machines with complex rotor movements were far less popular until 1945, with exceptions such as with the Abwehr Enigma and Japanese Enigma T known as Tirpitz.

In addition there is a major asymmetry here:

7. The fast rotor is situated in outer layers of encryption, i.e. closer to ciphertext and closer to the plaintext (but deeper than the stecker).

This again could be otherwise, this property was probably inherited from commercial Enigmas from 1920s and never changed, except that the stecker now became the outer layer (see however weakness 3. and 4. above). For example, the British TypeX cipher machines do exactly the opposite.

2.3. *Comparison to block ciphers.* This property also makes that Enigma is very much like a block cipher with a small block size. For sure the permutation is different for each encrypted character. However, as the change occurs in outer layers of encryption, which are largely those **accessible** to the attacker through partial guesses, or his knowledge (or choice) of plaintext and ciphertext, this remains a mild complication. Potentially the attacker can tolerate this. As it turns out the majority of attacks on block ciphers such as linear and differential cryptanalysis and many other do already work by guessing some parts of the key embedded in these outer layers of encryptions while in both block ciphers and Enigma, the key inside the inner permutation which is the hard part for the attacker, does not change. If the attacker in a block cipher context is actually able to partially predict or what the outer layers is doing, it does not really matter if technically these outer layers are constant or not in every encryption.

In all cases, with Enigma and block ciphers alike, the attacker can be seen as seeking to gain some statistical advantage to distinguish one SINGLE fixed inner permutation which does not change, from a random permutation. Or he can directly try to determine or confirm the key inside.

2.4. *Cryptanalysis and long term key question.* This paper is not about cryptanalysis though everything we do is motivated by cryptanalysis. It is rather about reverse engineering, which would still be called code breaking or just cryptanalysis in 1930s. This is also sometimes known as the Long-Term Key question, *Langzeitschlüssel* in German, which means a long-term key [17]. In 1932-33 Rejewski has recovered the 3 rotors of Enigma by solving a system of simultaneous non-commutative equations involving 3 unknown permutations [38]. There are $26! \approx 2^{88}$ possible wirings for one rotor therefore this is **harder** than any other part of Enigma cryptanalysis. The daily key of Enigma is simply substantially shorter. Recovering these rotors was much

later called by David Kahn "the greatest breakthrough in cryptanalysis in a thousand years". In [32] he wrote: "only mathematics could make it possible". Later in Britain this was never done except incrementally, to recover one new rotor at a time.

Alan Turing has also studied the question of recovering the rotors of Enigma. It is covered in [40] starting from page 16. Alan Turing uses the so called "boxes" which are a method of encoding the cyclical structure when composing two involutions without cycles. On page 17, Turing says that both involutions can be recovered from this. In fact it is a well-known and earlier theorem of Rejewski, cf. Section 13.8 in [10], Section 3 in [37], and pages 9-10 in [35]. Turing also writes on page 18 that this does not work for a product of 3 involutions, which shows that Turing took these questions very seriously and tried to look beyond what was already known. He would be very surprised to hear that this type of questions can and need to be asked again from scratch, because most Enigma rotors are very special.

2.5. *A new type of weakness.* Another tremendous weakness of Enigma cipher machines have remained unknown to the public until 2020, cf. [8] and this paper.

8. The great majority of rotors and their wirings used in real-life Enigma applications are NOT chosen at random and have extremely strong properties in terms of differential properties, linear properties, and in general approximations mixing **both** group operations $+$ and $\times$ in the ring of integers modulo 26.

In this article we do take reverse engineering to a new level. Instead of just saying what the secret permutations are, which is sufficient for the purpose of routine code-breaking, like recovery the short term (daily) secret keys, we look at HOW these permutations were created in the first place. We are going to discover that these permutations have some, more or less hidden, quite unusual properties. These questions were not studied before 2020, because no one thought such things could actually happen. We naively assumed that rotors in Enigma cipher machines are random permutations.

2.6. *Historical background.* The story goes back to Hebern, a US inventor and businessman, who has in 1920s filed a series of patent on rotor machines with increasing complexity. Many initial designs of Hebern are quite simplistic and did not have large complexity or a large period. This changes in 1929: the ultimate design of Hebern was US Patent 1683072A of 1929 with five moving rotors. Compared to Enigma in Hebern cipher machines, the current was flowing just once and in one direction through the rotors (so it did not share the weakness 1. and 2. of Enigma!). Inside this patent, Hebern makes numerous claims about randomness and security of his machine. Then he explicitly proposes that "each code wheel is wired at random and differently". For an

unknown reason, this is not quite what actually happened later when cipher machines achieved wider adoption. It comes as a shock, but almost no Enigma rotors ever used in real-life wartime encryption were random permutations. On the contrary.

2.7. *Strong linear and differential properties.* Something unusual happens with most real-life Enigma components ever made.
Example of a Linear Property. We consider rotor R_{III} from 1930 and we assume that output letter is odd y =B,D,F,H,.., and rotor position i is even, then:

$$y = \rho^{-i}(R_{III}(\rho^i(x))) = i + 2x + 1 \text{ with } Pr = \frac{10}{13}.$$

Example of a Differential Property. We consider invariant differential properties of type $k \to k$. Can input difference be equal to the output difference for any $k \in 0 \dots 25$? With rotor V in Zagreb Enigma 16081 from 1943 it turns out that only $k = 9$ can happen. This contrasts very strongly with what we observe for a random permutation: most values of k will be possible.
Probability. For each of rotors we study, the probability of what we see happening by accident is as small as winning in a lottery cf. Section 7 and Table 2.
Prevalence. All this is true for each single rotor already. Moreover this happens more or less for all rotors ever made, or for almost all rotors, and rotors from the same source behave in the same way, cf. our later Table 3.

2.8. *A short explanation.* We can in fact provide a plausible explanation why we observe these extremely strong properties. The explanation is the same for both linear and differential properties. It turns out that cipher designers were influenced by hundreds of years where cryptography have developed slowly, but already noticed that some ciphers are weaker than other, cf. de Viaris Attack in Section 14 in [5] later studied and improved by Friedman. Here the ideal properties require something which was called latin squares since Euler, and in fact older, see Section 4.1. Therefore cryptologists should in principle design a rotor such that this table is a latin square. This property is in fact very hard to achieve, see an imperfect latin square by Mauborgne in Table 3 page 137 in [5]. This is actually the same as the notion of a quasigroup in modern abstract algebra.

In addition, there are some simple prescriptive ways of making sure that a rotor gives a latin square, using simple modular arithmetic see our later Thm. 5.1. Even though these do not work for $N = 26$ as we will see later, these methods have apparently been used to obtain an imperfect solution.

2.9. *Implications for security of encryption with Enigma.* In general the designers of Enigma machine did not do a good job. All these properties do NOT necessarily make ciphers stronger. Our properties are such that they

are invariant w.r.t. the rotor rotation. As such they partially work the same way for any key, thus potentially making attacks on Enigma easier, and also making reverse engineering attacks easier (we can hypothesise a lot about an unknown rotor). We do not claim that our observations do not necessarily lead to many new attacks or it is too early to make such claims.

Rather, they can be used to improve almost any already known attack on Enigma, at least slightly, this including reverse engineering attack by Rejewski mentioned above, the Turing-Welchman bombe attack, and many others. We need to revisit almost all cryptanalysis research since 1930s, knowing that in addition rotors have extra unexpected properties. If rotors are not random permutations, their combinations are potentially also distinguishable from random permutations. This leads to at least small improvements in some known attacks such as faster variants of Welchman-Turing attack.

What is even more surprising is that permutations inside ciphers have deep structural properties involving differences and both operations in the ring $\mathbb{Z}_{26}$. This is very much like in modern cryptanalysis of block ciphers where algebraic modelling is extremely common. In Enigma nobody have noticed these undeniable facts for more than 80 years.

Example of Attack 1. We can design many statistical attacks combining Friedman's Index of Coincidence with our biases.

Example of Attack 2. Another way is to speed up the best WW2 Turing-Welchman attack by simulating a 2 rotor Enigma combined with reflector CHEAPER with less entropy to guess. For example we get $15/26$ with either $i+2x+1$ or $-3i-2x+13-1$ which cases are disjoint. A further optimization would be to see that it can be profitable to discard some ciphertext letters where approximations don't work, and rather break another message with the same stecker. If we implement Rotor III rotated by i steps by $y = i + 2x + b$ with a variable b, then the entropy of b is only $2.9 \ll 4.7$, hence faster guessing step in known attacks.

3. On rotor permutations

Our conventions and notation are consistent with all major Enigma simulators such as `https://cryptii.com/pipes/enigma-machine` and with 100 % of modern works on Enigma, cf. `cryptomuseum.com`, various wikipedia pages, [28], etc. We recall the Enigma the fast rotor is on the right side and it rotates anti-clockwise when we look from the right side. When we press a key on a keyboard, it rotates by one position anti-clockwise, and only then the first ciphertext letter is produced. This means that if an Enigma simulator shows AAZ in the window, and if the hidden ringstellung setting is a neutral position which is AAA, then the actual position of rotors which will be used to encrypt the first character will be AAA. We recommend our set of student

exercises about Enigma which are fully compliant with Enigma simulator and also show how major attacks on Enigma [9] work.

We order the letters in alphabetic order. This is however very different than what we find in old work of Turing, cf. page 6 of [40] where letters are ordered starting from Q to Z etc following the ordering on a German keyboard. Here is how the Enigma rotor is typically described in modern sources. For example the third rotor R_{III} will be described by:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
BDFHJLCPRTXVZNYEIWGAKMUSQO
```

3.1. *Enigma vs. block ciphers.* We recall that we aim at developing a unified theory of block ciphers and Enigma alike, and that due to the weak points 6.) and 7.) above, the differences are not as large as it seems. In contrast, there are huge differences in how the (short term) secret key is applied. In block ciphers the algebraic structure on which cryptographers work is relative to the vector space structure of $\mathbb{F}_2^n$ and in most ciphers the key is XORed to some internal value. Thus the key will transform one affine space into another. This situation makes that differential cryptanalysis will essentially ignore the key and this is one of the root causes why differential cryptanalysis is so important and popular in crypto research. There are however cases where the propagation probability for one differential depend on the key, for example in DES, for some differentials the differential propagation probability is a constant such as $1/256$ for 2 rounds and for any key, and sometimes will take two different values such as say $1/146$ or $1/585$ depending on the key, see [23].

3.2. *Notation and permuted rotor alphabets.* We will use the symbol $\circ$, which we apply from right to left, to denote a composition of functions. Let ρ be the $+1$ translation modulo 26. Then ρ^i is the same as $+i$ modulo 26 and corresponds to rotating the rotor physically inside the cipher machine. In rotor machines the key is applied by rotation of the rotor, which corresponds to $+1$ mod 26 without a multi-dimensional vector space structure. Then the rotation is applied back at the exit.

Overall the permutation we obtain for a rotor permutation R at position i is defined as:

$$\rho^{-i} \circ R \circ \rho^i.$$

We can also write

$$\rho^{-i} \circ R \circ \rho^i(x)$$

where again the rightmost function ρ^i is the one which is applied first to x.

Remarks. Contrary to block ciphers, in Enigma machines the secret key is in fact applied twice from our point of view or with our notations. This

particular method of conjugation ρ^i implies that invariant differentials of type $k \to k$ will play an important role in Enigma, as we will see later in Section 6.

3.3. *On permutation cycle structure.* Our rotor which rotates operates a conjugated permutation transformation. A conjugation preserves the cycle structure of the initial permutation. This basic theorem formulated and used by Rejewski had played an important role in early WW2 cryptanalysis [30]. In particular it was used in the so called Netz attack with perforated sheets, invented by Zygalski and implemented at Bletchley Park in 1939-1940, which was the main and only method of decrypting Germany Army Enigma used until May 1940 [37,38]. This moment corresponds to the invasion of France, when Germany have upgraded their cipher initialisation methods.

For example we consider rotor R_{III} introduced in Germany around 1930. It is easy to see that R_{III} has the following cycle lengths with multiplicity:

```
{1: 1, 8: 1, 17: 1}
A=>B=>D=>H=>P=>E=>J=>T=>A
C=>F=>L=>V=>M=>Z=>O=>Y=>Q=>I=>R=>W=>U=>K=>X=>S=>G=>C
N=>N
```

Does it look normal? Various statistics on random permutations are studied in block cipher cryptanalysis using generating series cf. [3,27] and some specific statistics will be needed later in this paper. For example in [39] we learn a basic and well-known result that:

THEOREM 3.1 (Cycle Structure). *A random permutation of length at least m contains on average $1/m$ cycles of length m, then 0 for larger sizes. The expected number of cycles of length at most m is about* $\ln(m)$.

We see that having one fixed point seems perfectly normal, we expect 1 fixed point on average. Then, given that $ln(17) = 2.8$, and we have 3 cycles of length up to 17, we do not think that Rotor III has an abnormal cycle structure. We have not yet found any abnormalities when looking at cycle structure for this Enigma rotor. However what is interesting is that in this paper we study many other properties which are also invariant by the rotation of the rotor.

4. What is wrong with German Army Rotor III

A classical approach to encryption in the first half the 20th century, was to study multiple "permuted alphabets" jointly cf. Section 7.1. in [5] and [26]. We make a table 26×26 of how the same rotor III will encrypt the same letter of plaintext say A (first column) for different keys (in different lines). This is shown in Figure 3.

Interestingly, there are some collisions if you do so. For example K appears 3 times in the first column. The situation as it turns out is that we always get collisions and never obtain a perfect latin square. For all known rotors, this

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
0	BDFHJLCPRTXVZNYEIWGAKMUSQO
1	CEGIKBOQSWUYMXDHVFZJLTRPNA
2	DFHJANPRVTXLWCGUEYIKSQOMZB
3	EGIZMOQUSWKVBFTDXHJRPNLYAC
4	FHYLNPTRVJUAESCWGIQOMKXZBD
5	GXKMOSQUITZDRBVFHPNLJWYACE
6	WJLNRPTHSYCQAUEGOMKIVXZBDF
7	IKMQOSGRXBPZTDFNLJHUWYACEV
8	JLPNRFQWAOYSCEMKIGTVXZBDUH
9	KOMQEPVZNXRBDLJHFSUWYACTGI
10	NLPDOUYMWQACKIGERTVXZBSFHJ
11	KOCNTXLVPZBJHFDQSUWYAREGIM
12	NBMSWKUOYAIGECPRTVXZQDFHLJ
13	ALRVJTNXZHFDBOQSUWYPCEGKIM
14	KQUISMWYGECANPRTVXOBDFJHLZ
15	PTHRLVXFDBZMOQSUWNACEIGKYJ
16	SGQKUWECAYLNPRTVMZBDHFJXIO
17	FPJTVDBZXKMOQSULYACGEIWHNR
18	OISUCAYWJLNPRTKXZBFDHVGMQE
19	HRTBZXVIKMOQSJWYAECGUFLPDN
20	QSAYWUHJLNPRIVXZDBFTEKOCMG
21	RZXVTGIKMOQHUWYCAESDJNBLFP
22	YWUSFHJLNPGTVXBZDRCIMAKEOQ
23	VTREGIKMOFSUWAYCQBHLZJDNPX
24	SQDFHJLNERTVZXBPAGKYICMOWU
25	PCEGIKMDQSUYWAOZFJXHBLNVTR

FIGURE 3. Table of permuted Alphabets for German Army rotor III.

was already observed in pp. 138–139 in [5]. Here below we will show what happen in general for any rotor of any size.

4.1. *On Latin squares.* The ideal situation would be of course that letters do not repeat, a property known as a latin square, or a quasigroup in mathematics. In post-war French cryptography this was known as "alphabets réellement non-parallèles", cf. [26]. According to [5], latin squares were studied in cryptography since the 18th century. They play a certain role in optimizing the diffusion P-box in DES, cf. page 58 in [6]. Latin squares are fun and have been a popular recreational mathematics topic ever since Euler. Moreover, the study or latin squares predates Euler, in the form of recreational puzzles

with cards, for example a 4×4 pair of orthogonal latin squares was published by Jacques Ozanam in 1725. This is not yet the latest reference we found. In fact, a Korean mathematician Seok-Jeong Choi published in year 1700 a work known as Gusuryak where he studied magic squares and presents an orthogonal Latin square of order 9, see [36].

Returning to our Figure 3 we see that we study a special problem: alphabets in each line cannot be arbitrary like in the Mauborgne square page 137 in [5]. They must all be derived from one single rotor by changing the position of this rotor. In this article we show that it is NOT possible to find a permutation of 26 characters, such that we obtain a latin square (or in mathematical terms, a quasigroup). In other terms collisions are **guaranteed** to occur each time when the number of contacts is even. We will also show that the number of collisions will be the same in each column, cf. Thm. 4.2 below. In contrast, the problem is perfectly solvable when N is odd, where N is the number of contacts. This is shown in our key Thm. 5.1 in Section 5.2. Collisions are however inevitable for an even N and we never obtain a perfect latin square. In later Thm. 6.3 page 69 we will also see that this implies vulnerability to invariant differentials.

4.2. *The question of contact ordering and hidden permutations.* We recall our table of permuted alphabets and zoom at the left upper corner. We see a lot of consecutive letters. A strange order reigns in our table for old wartime Rotor III, in particular if we look at the first two lines and only at the first 13 inputs:

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

FIGURE 4. A highly regular pattern observed in various positions $i = 0, 1, 2, 3$ with old wartime Rotor III from 1930, cf. [8]

This brings a question of ordering contacts in different ways. When Turing studied Enigma rotors during WW2 and similar tables found inside his book [40], he would order columns in order QWERTZ etc.. If we do this, we would probably **not notice** at all that there is something wrong here. It is important to see that in pre-war Britain, the specification of Military Enigma was not known, and in particular the initial permutation, literally, in which order the keyboard was connected to the first rotor. The number of possibilities is of course enormous, again $26! \approx 2^{88}$. Following [4], Denniston and

Batey has recalled that a certain "Mrs. BB", presumably a lady code breaker working closely with Dilly Knox at Bletchley Park has actually suggested this possibility (alphabetic ordering). However apparently this possibility was discarded and not studied at the time, as everyone "thought the Germans were not stupid enough to make it that easy!", cf. [4], page 116.

Now, if we order the contacts alphabetically, in the same way as all modern sources [5,42], a strong pattern emerges. In addition, this faulty rotor was used since 1930 and never withdrawn from circulation and continuously used until 1945, and in some cases until 1956 (in post-war Eastern Germany).

Open Problem. If renaming letters conceals our property, could we have a hidden permutation such that a very weak rotor is disguised as a strong rotor, which does not have any apparent weakness?

Another Open Problem. Another interesting question is to see if a rotor could behave in a consistent way modulo 13. On the face value, this problem does not exist and we have $Pr_{R_{III}}(\Delta = 13 \to \Delta = 13) = 2/26$ which is very small. However there could be a backdoor property: a secret 2-to-1 mapping from 26 contacts to 13, and a hidden structure involving a complete quasigroup modulo 13, which as we see here exists, cf. Thm. 5.1. A related question is studied in Section 7.1.

On Backdoors. There exists countless academic works about backdoors in modern ciphers, cf. for example [1,7,13,24,33] and many researchers believe that there are no real backdoors, in the sense that if some properties weaken the cipher and lead to an attack, they will be "sooner or later" discovered, cf. for example Section 6.2 in [25] and Section 3.4. in [34]. In this article we show that the question of backdooring also occurs for relatively small permutations and that "sooner or later" could be 80 years, and possibly the space to research to uncover a hidden special subset of say 13 out of 26, could be quite large, at least 2^{23}. This is very large, knowing that the designers of Enigma did not have the ability to do experiments with today's powerful computers, and powerful computer algebra and maths software packages such as Sage Maths.

4.3. *A linear algebraic approximation.* We are looking here at an eminently algebraic law. It seems that the ONLY plausible way to get something which works for a substantial fraction of 26^2 cases is to use the full power of arithmetic of the ring of integers modulo 26 with both + and × where distributivity of multiplication over addition helps. It might appear very strange, but we can in fact mix both group operations modulo 26, and it turns out that we always have:

$$\rho^{-i} \circ R_{III} \circ \rho^i(j) \stackrel{?}{=} i + 2 \cdot j + 1 \text{ with A=0, B=1, etc. with } Pr = \frac{10}{26}$$

Nothing else than a strong **linear** approximation of an old Enigma rotor from 1930. Who says that Linear Cryptanalysis was invented only in 1990s?

Or maybe in 1970s, cf. [19]? Here we have a rotor from 1930 which has an extremely strong[1] algebraic linear approximation.

4.4. *On polynomial invariants and invariant theory.* In mathematics, and in applied mathematics such as cryptography, there are countless examples of invariants of different type. The classical end of 19-th century Hilbertian invariant theory deals with actions of groups on commutative rings. Invariants are the typically multivariate polynomials or/and use both operations in the ring, are the ones which are the most frequently studied. This is also exactly what we have here (!). In cryptography, invariant properties do not need to be exact, they can be true in approximation. Many known attacks on block ciphers such as linear and differential cryptanalysis amount to the study of periodic invariants which propagate with a certain probability.

A lot of work in mathematics deals with invariants w.r.t linear transformations, while in cryptography we always want our transformations to be highly non-linear and avoid any invariants whatsoever. However the space of possible invariants is typically so large, that invariants are typically nevertheless found. A well-known polynomial invariant with applications in symmetric cryptography is the cross-ratio, which is typically not perfect but degrades if we have many encryption steps, cf. Section 4 in [15]. This is related to the notion of the so called Carlitz rank which is a method of classifying all permutations on a finite set, and the so called "whitening paradox", cf. Appendix B in the extended version of [15].

In all cases in cryptography we study very complex groups, which are finite, yet so large and complex that they can hardly be understood fully. In contrast, we try to keep invariant properties as simple as possible for individual cipher components (they become more complex for several rounds of encryption). In block ciphers we work a lot with multivariate polynomial invariants over $GF(2)$, see Section 2.4 in [12] and Section 2.2. in [21]. Here we have invariants exploiting a small ring $\mathbb{Z}_{26}$ which is not a field, which is yet different than studied before.

Remark. It is easy to see with 1 variable, linearity w.r.t. multiplication modulo 26 is a substantially stronger property than a linear approximation modulo 2 exploited in great majority of cryptanalytic attacks. This is because a point satisfies such an approximation with smaller probability of $1/26$ instead of $1/2$. Binary linear approximations are simply more likely to work purely by accident which is far from being the case here, as we show more precisely in Section 7.

4.5. *Basic invariance results.* It is easy to see linear approximation for our table will behave in a way which is a bit counter-intuitive: Indeed it holds

[1] Strong in the sense of unlikely to occur accidentally, cf. Remark at the end of Section 4.4 and Section 7.

for a large proportion of 26^2 values not 26, for any i, j. How this is possible? Should not the probability be negligible for so many values? We have the following result:

THEOREM 4.1 (Conjugation Property). *Let a, b be two fixed integers. We fix i and we consider the probability (over all $x \in \mathbb{Z}_{26}$) that we have:*

$$\rho^{-i} \circ R_{III} \circ \rho^i(x) \stackrel{?}{=} (a-1)i + ax + b.$$

This probability is the same for every i, and for every j. Consequently, the number of coloured letters is the same in every line in our square, and also in every column, cf. Fig 3. This probability is also the same for every letter y where $y = \rho^{-i} \circ R_{III} \circ \rho^i(x)$ is the letter displayed. Consequently, the number of coloured letters is the same for every letter.

PROOF. We prove the first result by induction on i, modulo 26 we can start from any point. We assume that $\rho^{-i} \circ R_{III} \circ \rho^i(x) \stackrel{?}{=} (a-1)i + ax + b$ for some i. We apply ρ on both sides and we replace x by $z - 1 = \rho^{-1}(z)$ modulo 26, which is a bijective transformation:

$$\rho^{-i+1} \circ R_{III} \circ \rho^i(\rho^{-1}(z)) \stackrel{?}{=} (a-1)i + a(z-1) + b + 1 = (a-1)(i-1) + az + b$$

which gives us the same probability over $z \in Z_{26}$ for $i - 1$:

$$\rho^{-(i-1)} \circ R_{III} \circ \rho^{(i-1)}(z) \stackrel{?}{=} (a-1)(i-1) + az + b.$$

We see that if we have k solutions x for one i, we can produce also k solutions z for $i-1$. Moreover after 26 steps we can back to the same place so the number of solutions in this process cannot increase, it must stay constant for every i.

For the second column-wise invariance result we fix i and vary x. It is easy to see that $\rho^{-i} \circ R_{III} \circ \rho^i(x) = y$ is equivalent to $\rho^{-(i-1)} \circ R_{III} \circ \rho^{i-1}(x+1) = y + 1$. In each case where $y = (a-1)i + ax + b = \rho^{(a-1)i+b}(ax)$ we have also $y + 1 = (a-1)i + ax + b + 1 = (a-1)i + a(x+1) - a + b + 1 = (a-1)(i-1) + a(x+1) + b$ which is exactly what we expect. Finally the last result, is due y rotating though all possible values in 2nd result, letter y being in coloured in column x was transformed into $y + 1$ also in colour in column $x + 1$. ∎

4.6. *On invariance of collisions.*

THEOREM 4.2 (Rotor Collision Invariance). *We consider a rotor such that a collision occurs in one column in our table of rotated alphabets, i.e. there exist two integers (or two lines) $i \neq i'$ and one input letter (column) x such that*

$$\rho^{-i} \circ R_{III} \circ \rho^i(x) = \rho^{-i'} \circ R_{III} \circ \rho^{i'}(x).$$

Then for each column in our table x we obtain the same number of collisions.

PROOF. We can simply translate our property by c steps for every c, and these translations are one to one:

$$\rho^{-(i-c)} \circ R_{III} \circ \rho^{i-c}(x+c) = \rho^{-(i'-c)} \circ R_{III} \circ \rho^{i'-c}(x+c).$$

□

Example: For example in Fig 3, in each column we have four letters concerned by events of this type, with K repeated 3 times at $i = 9, 11, 14$, N repeated twice for $i = 10, 12$, P repeated twice with $i = 15, 25$ and S repeated twice for $i = 16, 24$. Then in fact in each column we also have four letters concerned by events of this type which are L,O,Q,T in the next column and so on.

5. A key theorem on permuted rotor alphabets

Until now, it was an open problem if we can get a latin square, cf. pp. 138–139 in [5].

5.1. *Can Enigma rotor give a Latin square?* We will first estimate the probability that we obtain a latin square for a rotor chosen at random to be approximately equal to the probability that there is no repeated characters in the first column, then we compute the first line, and again if we are lucky, there should be no repeated characters. This probability will be about:

$$(26!/26^{26})^2 \approx 2^{-67.6}.$$

This argument does not provide an efficient algorithm for generating a suitable rotor and we have little hope to find it by brute force - this probability is too small. We have used a smarter tool, a SAT solver, able to make deductions and capable of backtracking. With this tool this problem could be solved and impossibility was shown for $N = 26$. The good point about this tool is that it allows to generate solutions with arbitrary additional features, if they exist, and to formulate conjectures for many different N. Finally we found a direct mathematical theorem with a proof which solves this problem completely for any N.

5.2. *A key result on Latin squares generated by a single rotor.*

THEOREM 5.1 (On Existence of Quasi-groups Derived From a Single Permutation). *There exists no quasi group for even N such that our table is exactly the one obtained from a single actual bijective rotor rotated in all possible N positions. For any odd $N \geq 1$ a solution exists. For an even N the solution never exists.*

PROOF. For an odd N it is easy to check that the rotor $R(x) = 2 \times x + 1 \mod N$ always works for any odd $N \geq 1$. In line i we have then $x \mapsto i + 2 \times x + 1 \mod N$ which is always a permutation, and each column x we have $i \mapsto i + 2 \times x + 1 \mod N$ which is also always a permutation.

For even N the situation is more difficult and we will show that collisions always exist and they exist for any column x. Let R be a permutation on $\{0,\dots,N-1\}$ and $\rho(x) = x+1 \bmod N$. We need to show that:

LEMMA 5.2. *If N is even, then for every $x \in \{0,\dots,N-1\}$ there exist $i_1 \neq i_2$ modulo N such that $\rho^{-i_1} R \rho^{i_1}(x) = \rho^{-i_2} R \rho^{i_2}(x)$ modulo N.*

Proof of Lemma 5.2: The statement follows from two claims:

Claim 1: For every $x \in \{0,\dots,N-1\}$ we have

$$\sum_{i=0}^{N-1} \left(\rho^{-i} R \rho^{i}(x) - x\right) = 0 \bmod N.$$

Indeed,

$$\rho^{-i} R \rho^{i}(x) - x = \rho^{-i} R \rho^{i}(x) - \rho^{-i}\rho^{i}(x) = R(y_i(x)) - y_i(x)$$

for $y_i(x) = \rho^i(x)$. When we take all possible values of i, also y_i takes all possible values once. Thus,

$$\sum_{i=0}^{N-1} (\rho^{-i} R \rho^{i}(x) - x) = \sum_{y \in \{0,\dots,N-1\}} (R(y) - y)$$

and the last sum is obviously equal to 0 because R is a permutation.

Claim 2: If N is even, then for every $x \in \{0,\dots,N-1\}$ we have $\sum_{y\in\{0,\dots,N-1\}}(y-x) = N/2 \bmod N$. Indeed, our sum is:

$$\sum_{y \in \{0,\dots,N-1\}} (y - x) = (N-1)N/2 - Nx$$

and for even N we have $(N-1)N/2 = N/2 \bmod N$.

We now prove the assertion of Lemma 5.2 that collisions always exist and for any x. If for some special x it is true that $\rho^{-i_1} R \rho^{i_1}(x) \neq \rho^{-i_2} R \rho^{i_2}(x)$ for every i_1, i_2, then $\{\rho^{-i} R \rho^{i}(x)\}$ must be equal to $\{0,\dots,N-1\}$. Thus, by Claim 2,

$$\sum_{i=0}^{N-1} (\rho^{-i} R \rho^{i}(x) - x) = \sum_{y \in \{0,\dots,N-1\}} (y - x) = N/2 \bmod N.$$

However, this would contradict Claim 1 which says this sum must be 0 modulo N. ∎

5.3. *Discussion and examples.* Initially we have done a computer proof of this result with a SAT solver. If there is no solution the system outputs UNSAT which is a logical contradiction which guarantees there is no solution, and some SAT solvers can actually output a full rigorous mathematical proof. Such proofs are however not human readable, this is why finally we present a simpler proof above. Otherwise, if the solution exists, our software can actually generate such solutions on demand and on particular one which are non-linear and more complex than the simple linear solution proposed in our

proof. For example a valid solution for $N = 5$ is ACEBD and a valid solution for $N = 9$ is IHFBEGCAD. For $N = 13$ we have for example MLJBKGIHEAFDC. There is no solution for $N = 26$. We see that the ideal objective of the designers of Enigma rotors is not at all possible to achieve.

Connecting the Dots. In fact as we will see, with rotor R_{III} from 1930 we also have $x \mapsto i+2\times x+1$ with probability $\frac{10}{26}$. This strongly suggests that the Thm. 5.1 above or at least our method to construct a solution for an odd N was known to the designers of Enigma in 1930. The same closed formula was applied, even though it simply cannot work perfectly for when N is even. This sort of magic formula approximation, together with the associated feasibility result of Thm. 5.1, come together and tell us a story. The circumstantial evidence we observe is the cryptographic engineering equivalent of a message hidden in a bottle and thrown to the sea, cf. [8].

6. Differential properties of Enigma rotors

A major question is the study of differential properties of rotors. In theory, one rotor has 26^2 differential properties. For example for Rotor III the input difference 2 gives output difference 1 with very high probability 8/26, which is extremely high, which happens twice and is the highest ever seen differential probability for any known rotor. We write

$$Pr_{R_{III}}(\Delta^i = 2 \rightarrow \Delta^o = 1) = 8/26.$$

Here Δ^i is the input difference, and Δ^o is the output difference. If there is no ambiguity we will omit ^{i} and ^{o} and sometimes we will also omit Δ and just write $k \rightarrow l$. Now we recall that in Enigma, and unlike what we see in block ciphers, the key translation ρ^i is applied twice. This leads to focus on invariant differential properties of type $k \rightarrow k$.

It turns out that invariant properties $k \rightarrow k$ are extremely rare, not only with Zagreb Enigma, but almost always for most actual historical cipher machines, cf. later Table 3, and almost never for random permutations cf. Table 1 below.

We have the following definition.

Definition 6.1 (Imk). *We call Imk the number of horizontal offsets k which are impossible in any column of our table or rotated alphabets (such as in Fig. 3) when we have a collision in this column. In other terms we look at values of $k = k_1 - k_2$ such that for no value x we have:*

$$\rho^{-k_1} \circ R \circ \rho^{k_1}(x) = \rho^{-k_2} \circ R \circ \rho^{k_2}(x).$$

It also easy to see that the number Imk is equal to the number of impossible invariant differentials for this rotor R of type $k \rightarrow k$ where $k = k_1 - k_2$. It is also easy to see that this set of impossible offsets k is in fact the same in every column in Fig. 3 and in general.

The maximum value of Imk is 25 because $0 \to 0$ is always possible and we have 25 if and only if we have a latin square.

Example. For example we have:

$$Pr_{R_{III}}(\Delta = 2 \to \Delta = 2) = 2/26.$$

and when we look at one column of Fig. 3, when a collision happens, the difference in horizontal positions can be $2 = k_1 - k_2$.

Most values of k are however impossible, and extremely few are actually possible for real-life rotors. For example there are no collisions in consecutive lines which is equivalent to saying that for $k = 1$ we have:

$$Pr_{R_{III}}(\Delta = 1 \to \Delta = 1) = 0/26.$$

In contrast for a random permutation most values of k are actually possible, see Table 1 below which was obtained by a computer simulation.

TABLE 1. Probability distribution of Imk for random permutations

0	2	4	8	12	16	18	19	20	21	22	23	24	25
$2^{-7.8}$	$2^{-5.8}$	$2^{-4.5}$	$2^{-3.6}$	$2^{-4.2}$	$2^{-7.0}$	$2^{-9.5}$	$2^{-9.7}$	$2^{-13.2}$	$2^{-13.9}$	2^{-19}	2^{-20}	2^{-26}	0

6.1. *How Imk relates to Latin squares.* We have the following result:

THEOREM 6.2 (Imk Latin Equivalence). *For any rotor, the following three statements are equivalent:*

(1) $Imk = 25$.
(2) *All invariant differentials of type $k \to k$ are impossible for every $k \neq 0$.*
(3) *The Figure 3 of rotated alphabets is a latin square.*

PROOF. By definition of Imk it is about collisions in one column of our table, and (1) and (2) are the same. First we show that (2) $\Rightarrow$ (3) by contradiction. If for some $k \to k$ it is actually possible to have $R(x) = \rho^{-k} R \circ \rho^k(x)$, then the letters in line $i = 0$ and $i = k$ in our column would be the same and it would not be a latin square. Now we show that (3) $\Rightarrow$ (2), if all $\rho^{-k} R \circ \rho^k(x)$ are distinct in one column for a fixed x and variable k, then $R(x) = \rho^{-k} R \circ \rho^k(x)$ cannot happen and no differential $k \to k$ can occur. □

Now we recall that for even N we cannot have a latin square at all, and we also have the following theorem about differential cryptanalysis in general:

THEOREM 6.3 (Invariant differentials are inevitable for even N). *For any permutation R on $\{0, \ldots, N-1\}$ there exist an invariant differential $k \neq 0$ which works with a probability > 0.*

PROOF. This is due to our earlier Lemma 5.2. For every $x \in \{0, \ldots, N-1\}$ there exist $i_1 \neq i_2$ modulo N such that $\rho^{-i_1} R \rho^{i_1}(x) = \rho^{-i_2} R \rho^{i_2}(x)$ modulo N. We then just put $k = i_2 - i_1$ modulo N. □

7. Could this happen by accident?

We recall our linear approximation:

$$\rho^{-i} \circ R_{III} \circ \rho^{i}(x) = i + 2 \cdot x + 1 \text{ with } Pr = \frac{10}{26}.$$

What is the probability that this type of property happens by accident for a random permutation? We estimate that it is extremely low, less than winning a lottery.

We recall that $\rho^{-i} \circ R_{III} \circ \rho^{i}(x) = y$ is equivalent to $\rho^{-(i-1)} \circ R_{III} \circ \rho^{i-1}(x+1) = y + 1$. Therefore our property works if and only if it works inside the first column. We consider a union of disjoint events where we select 10 random lines out of 26, and for each of these lines the letter is determined by our linear formula, which also guarantees that these 10 letters are distinct, and then we have to select one letter from the remaining not 16 but 15 possibilities. We have basically 16! possibilities, but we need to exclude one choice for each remaining number, the one which is indicated by our linear formula. In approximation, there are 15! ways of doing it. We get about:

$$\binom{26}{10} \cdot 15!$$

possible ways of filling the first column in Fig. 3. Therefore for a fixed linear approximation, we get roughly

$$\binom{26}{10} \frac{15!}{26!} \approx 2^{-25}$$

probability for what we observe. Rotor III was certainly not chosen at random.

7.1. *Improving the success probability.* We are not quite happy with the probability 10/26. Can we do better? YES. We have $26 = 13 \cdot 2$ and a good way to do a partial key guess for an Engima rotor is for the attacker to guess i mod 2, this only 1 bit of information which will hold for one whole Enigma ciphertext (which could be 200 or 500 characters). It is easy to see that we have:

PROPOSITION 7.1 (Linear approximation parity result). *For any letter y =A,B,.. this letter occurs in our table exactly the same number of times in colour, i.e. when our linear approximation $y = i + 2x + 1$ holds. Moreover, if this letter is odd y =B,D,F,H,.., inside these 10 cases in colour, all of these or 100 %, are such that i is even, i.e. $i = 0, 2, 4, \ldots 24$. In other terms when y is odd, or equivalently when i even,*

$$y = \rho^{-i} \circ R_{III} \circ \rho^{i}(x) \stackrel{?}{=} i + 2x + 1 \text{ with } Pr = \frac{10}{13}.$$

where we check the equality $y \stackrel{?}{=} i + 2x + 1$ *in 13 cases when* i *is even, which is also exactly the same 13 cases where* y *is odd, and this equality holds in as many as 10 cases out of 13. Moreover, a sort of saturation or reciprocal property holds. For any even letter* y *=A,C,E,etc.., 100 % of 10 coloured occurrences of this letter in our table (i.e. those where* $y = i + 2x + 1$*) are such that* i *is odd.*

Proof. This result is quite obvious. We interpret our key property to the more general framework of Thm. 4.1, we have $a = 2$. The fact that each letter has the same frequency when coloured was already shown in Thm. 4.1. We are lucky because this a is even, and so if parity of i is known, the parity of the output letter y is determined, and all 10 cases for which our property holds are odd. □

7.2. *Application: Combined attacks with Enigma reflector UKW-A.* An important feature of all Enigma machines was the reflector, where 13 pairs of characters are connected, and the current returns back to flow in the opposite direction. The reflector was invented in 1926 by Willy Korn, known from numerous patents on Enigma cryptography, cf. page 114 in [5].

We recall that when output letter is odd y =B,D,F,H,.., and rotor position i is even, then:

$$y = \rho^{-i} \circ R_{III} \circ \rho^{i}(x) \stackrel{?}{=} i + 2x + 1 \text{ with } Pr = \frac{10}{13}.$$

Similarly, for any even letter y =A,C,E,.., 100 % and i odd, we have also 10/13. This opens many possibilities where attacker focuses on half of the letters and guesses the position of rotor i mod 2, just one bit of information and the attacker can infer a lot of things without knowing this part of the key.

This is remarkable knowing that in the oldest historical Enigma UKW-A reflector even letters are mapped to even letters with probability 11/13. For example A=0 is mapped to E=4 and both numbers are even.

Later in 1937 the reflector becomes stronger: the probability of mapping even to even letters becomes 8/13 for UKW-B. To the best of our knowledge we are the first to show, in 90 years of history of Enigma ciphers, that a reflector can sometimes be weak.

7.3. *Related facts: A study of Ims.* In our research on this topic we also studied a closely related definition is *Ims*:

Definition 7.2 (Ims). *We call Ims the number of distinct letters in one column of our table or rotated alphabets (cf. Fig. 3).*

We observe that for most Enigma rotors not only Ims is large but Imk is also typically quite large and both are closely related: if one is close to maximum, the other is also close to maximum. This does not hold for smaller values.

TABLE 2. Probability distribution of Ims for random permutations

7	8	10	12	14	16	18	20	22	23	24	25	26
$2^{-27.1}$	$2^{-22.4}$	$2^{-13.6}$	$2^{-7.4}$	$2^{-3.7}$	$2^{-2.1}$	$2^{-2.7}$	$2^{-5.6}$	$2^{-11.1}$	$2^{-14.8}$	$2^{-20.0}$	$2^{-26.4}$	0

Open problems. It would be interesting to propose a closed formula and a theorem which allows to derive these results by theory for any N, in the spirit of [3, 27].

8. Comparison of selected real-life rotors

A natural way to evaluate the quality of the probability distribution in one column in Figure 3 is to report the entropy of this probability distribution denoted by Ent. The result is the same in every column, due to Thm. 4.2. The entropy observed for different rotors is shown in Table 3.

In total we have examined 63 different rotors and we observed that these values are very consistent for rotors coming from the same origin. We also observe that rotors from the same source (e.g. the same country) and the same year (e.g. 1941) have very similar parameters.

On average, for all 63 rotors, the entropy Ent is 4.39 which is extremely high. The maximum possible would be $\log_2(26) = 4.7$ bits which however cannot happen due to Thm. 5.1. In contrast, Ent is 3.87 on average for random permutations.

We omitted Norwegian rotor IV, which was not rewired towards the end of the war like others, instead the original German rotor IV was kept.

In fact only Swiss and Norwegian rotors behave as rotors generated at random with $Ims = 15 - 17$ typically. All other rotors don't. For example, in all 3 Enigma KD Mil Apt, which was used by the successor of Abwehr, we have $Ims = 24$. This is 3 events the probability of which is 2^{-20} happening in a row, similar to wining in a lottery 3 times in a row.

9. Conclusion

Our research indicates that most historical Enigma rotors are weaker than expected. We have examined 63 known rotors in Enigma machines: German, Swiss, Italian, Hungarian, Spanish, Norwegian, Japanese etc. Rotors coming from the same origin behave consistently. We exhibit both linear and differential properties. Differential properties are more prevalent, they are present for almost all rotors, and invariant differentials are particularly relevant due to how the key is applied.

TABLE 3. Entropy *Ent* of one column with *Ims* and *Imk* for selected historical rotors used in Engima cipher machines

rotor name	Nb.	code	dates	*Ims*	*Ent*	*Imk*	possible 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
Railway I	12	JGD	1941	24	4.55	22	2,13
Railway II	13	NTZ	1941	24	4.55	21	6,7
Railway III	14	JVI	1941	23	4.47	21	1,12
G-312 Abwehr I	9	DMT	19YY	21	4.32	17	5,6,7,8
G-312 Abwehr II	9	HQZ	19YY	24	4.55	22	8,13
G-312 Abwehr III	9	UQN	19YY	24	4.55	21	5,10
KD Mil Amt I	34	VEZ	1944	24	4.55	21	9,10
KD Mil Amt II	35	HGR	1944	24	4.55	21	5,8
KD Mil Amt III	36	NWL	1944	24	4.55	21	6,9
Zagreb 16081 I	62	CVF	1943	24	4.55	21	4,12
Zagreb 16081 II	63	XJG	1943	22	4.36	17	5,6,9,11
Zagreb 16081 III	64	SYI	1943	24	4.55	21	4,8
Zagreb 16081 IV	65	HKT	1943	24	4.55	21	4,6
Zagreb 16081 V	66	WMG	1943	25	4.62	23	9
Hungary G-111 I	12	JGD	193X	24	4.55	22	2,13
Hungary G-111 II	13	NTZ	193X	24	4.55	21	6,7
Hungary G-111 III	14	JVI	193X	23	4.47	21	1,12
Norway I	20	WTO	1945	13	3.46	5	1,3,4,6,7,8,9,10,11,12
Norway II	21	GJL	1945	16	3.80	6	2,3,4,5,7,8,9,10,12,13
Norway III	22	JWF	1945	15	3.66	6	2,3,5,6,7,9,10,11,12,13
Norway V	24	HEJ	1945	15	3.80	8	2,4,5,6,7,9,10,12,13

In this article we look at how such results can be justified in theory by mathematical theorems. All the properties we observed can be explained by the fact that the table of permuted alphabets corresponding to all possible rotor positions can be a quasigroup for odd N and cannot be a perfect quasigroup for an even N. However it can behave as a quasigroup in approximation, imitating the latin square and minimizing the number of collisions in each column. We show that this requirement is equivalent to the fact that

extremely few invariant differentials $k \to k$ are allowed to happen. We also show that invariant differentials are inevitable for an even N, cf. Thm. 6.3.

For real-life rotors with $N = 26$, what we actually observe is quite unusual. We show that the probability of what we observe happening for a random permutation is of the order of 2^{-20} for just one rotor. This shows that these choices were deliberately made by the designers. They are the consequences of the state of the art of cryptographic science and the beginning of the 20-th century which focused on the study of polyalphabetic substitutions. The designers of Enigma have imitated an ideal latin square property the best they could. Our Thm. 5.1 implies that the ideal property the designers have tried to achieve in so many cases, is however not achievable perfectly for $N = 26$.

It is interesting that for more than 80 years rotors in cipher machines have been selected in a certain very special way, and nobody have noticed. This demonstrates the fallacy of the so called open source: even if we know the specification of a cipher, important facts can remain hidden for more than 80 years. The same applies to DES cf. [22] and other historical block ciphers [12,14,21]. We see that it is very difficult to assess what are the implications of just one particular component used inside any given cipher. Our observations can be used to improve brute force part in many major attacks on Enigma or/and in reverse engineering and statistical attacks. They are also here to show that the study of quality of cryptographic components and careful design and selection of quasi-optimal components (similar as with the AES S-box cf. [15, 20]) is a lot older than it is typically assumed.

References

[1] A. Albertini, J.-P. Aumasson, M. Eichlseder, F. Mendel and M. Schläffer, *Malicious hashing: Eve's variant of SHA-1*, in: Selected Areas in Cryptography – SAC 2014, Lecture Notes in Comput. Sci. **8781**, Springer, Cham, 2014. pp. 1–19.

[2] D. Alvarez, *Wilhelm Fenner and the development of the German Cipher Bureau, 1922–1939*, Cryptologia **31** (2007), 152–163.

[3] G. V. Bard, S. V. Ault and N. T. Courtois, *Statistics of random permutations and the cryptanalysis of periodic block ciphers*, Cryptologia **36** (2012), 240–262.

[4] M. Batey, *Dilly Knox - A reminiscence of this pioneer Enigma cryptanalyst*, Cryptologia **32** (2008), 104–130.

[5] F. L. Bauer, Decrypted Secrets: Methods and Maxims of Cryptology, Springer, Berlin, 2006.

[6] L. P. Brown, Analysis of the DES and the Design of the LOKI Encryption Scheme, PhD Thesis, Dept. Computer Science, UC UNSW, ADFA, Canberra, 1991.

[7] M. Calderini, *A note on some algebraic trapdoors for block ciphers*, Adv. Math. Commun. **12** (2018), 515–524.

[8] N. T. Courtois, *Si seulement Enigma tournait moins vite, ou cryptanalyse d'Enigma avec un rotor faible*, Bulletin de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information **46** (2020), 79–90.

[9] N. T. Courtois, Student exercises about breaking Enigma, updated March 2020, taught at University College London in 2020 as a part of COMP0058 Allied Cryptography and Cryptanalysis course, `http://www.nicolascourtois.com/teach/Exos_Engima_0058.pdf`.

[10] N. Courtois, Algebraic Complexity Reduction and Cryptanalysis of GOST, Monograph study on GOST cipher, 224 pages, available at `https://ia.cr/2011/626`.

[11] N. Courtois and J. Pieprzyk, *Cryptanalysis of block ciphers with overdefined systems of equations*, in: Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Comput. Sci. **2501**, Springer, Berlin, 2002. pp. 267–287.

[12] N. T. Courtois and A. Patrick, *Lack of unique factorization as a tool in block cipher cryptanalysis*, Preprint, `https://arxiv.org/abs/1905.04684` submitted 12 May 2019.

[13] N. T. Courtois, *On the existence of non-linear invariants and algebraic polynomial constructive approach to backdoors in block ciphers*, `https://ia.cr/2018/807`, last revised 27 Mar 2019.

[14] N. T. Courtois, *A nonlinear invariant attack on T-310 with the original Boolean function*, Cryptologia **45** (2021), 178–192.

[15] N. Courtois, *The inverse S-box, non-linear polynomial relations and cryptanalysis of block ciphers*, in: Advanced Encryption Standard – AES, Lecture Notes in Comput. Sci. **3373**, Springer, Berlin, 2005, pp. 170–188.

[16] N. Courtois, *Feistel schemes and bi-linear cryptanalysis*, in: Advances in Cryptology – CRYPTO 2004, Lecture Notes in Comput. Sci. **3152**, Springer, Berlin, 2004. pp. 23–40.

[17] N. T. Courtois, K. Schmeh, J. Drobick, J. Patarin, M.-B. Oprisanu, M. Scarlata and O. Bhallamudi, Cryptographic Security Analysis of T-310, Monography study on the T-310 block cipher, 132 pages, received 20 May 2017, last revised 29 June 2018, `https://ia.cr/2017/440.pdf`.

[18] N. Courtois, 100 years of Cryptanalysis: Compositions of Permutations, slides about cryptanalysis of Engima and block cipher cryptanalysis, used teaching GA18 Cryptanalysis course at University College London 2014–2016, `http://www.nicolascourtois.com/papers/code\_breakers\_enigma\_block\_teach.pdf`.

[19] N. Courtois, M.-B. Oprisanu and K. Schmeh, *Linear cryptanalysis and block cipher design in East Germany in the 1970s*, Cryptologia **43** (2019), 2–22.

[20] N. Courtois and J. Pieprzyk, *Cryptanalysis of block ciphers with overdefined systems of equations*, in: Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Comput. Sci. **2501**, Springer, Berlin, 2002. pp. 267–287.

[21] N. T. Courtois, *Invariant hopping attacks on block ciphers*, presented at WCC'2019, Abbaye de Saint-Jacut de la Mer, France, 31 March – 5 April 2019. Extended version available at `https://arxiv.org/pdf/2002.03212.pdf`, 8 February 2020.

[22] N. Courtois, G. Castagnos and L. Goubin, *What do DES S-boxes say to each other?*, Available on `https://ia.cr/2003/184/`.

[23] N. Courtois, *The best differential characteristics and subtleties of the Biham-Shamir attacks on DES*, Available on `https://ia.cr/2005/202`.

[24] N. T. Courtois, T. Mourouzis, M. Misztal, J.-J. Quisquater and G. Song, *Can GOST be made secure against differential cryptanalysis?*, Cryptologia **39** (2015), 145–156.

[25] N. T. Courtois and J.-J. Quisquater, *Can a differential attack work for an arbitrarily large number of rounds?*, in: Information Security and Cryptology – ICISC 2020, Lecture Notes in Comput. Sci. **12593**, Springer, Cham, 2021, pp. 157–181.

[26] C. Eyraud, Précis de Cryptographie Moderne, Editions Raoul Tari, Paris, 1st edition 1953, 2nd edition 1959.

[27] P. Flajolet and R. Sedgewick, Analytic Combinatorics, Cambridge University Press, Cambridge, 2009.

[28] J. R. S. Fuensanta, F. J. López-Brea Espiau, and F. Weierud, *Spanish Enigma: A history of the Enigma in Spain*, Cryptologia **34** (2010), 301–328.
[29] J. J. Gillogly, *Ciphertext-only cryptanalysis of Enigma*, Cryptologia **19** (1995), 405–413.
[30] I. J. Good and C. A. Deavours, *Afterword to: Marian Rejewski, "How Polish mathematicians deciphered the Enigma"*, Annals of the History of Computing **3 (3)** (1981), 229–232.
[31] C. Jennings, The Third Reich is Listening: Inside German codebreaking 1939–45, Osprey Publishing, Oxford, 2018.
[32] D. Kahn, *How I discovered World War II's greatest spy*, Cryptologia **34** (2009), 12–21.
[33] P. Morawiecki, *Malicious Keccak*, `https://ia.cr/2015/1085`.
[34] T. Peyrin and H. Wang, *The MALICIOUS framework: Embedding backdoors into tweakable block ciphers*, in: Advances in Cryptology – CRYPTO 2020, Lecture Notes in Comput. Sci. **12172**, Springer, Cham, pp. 249–278.
[35] K. Pommerening, *Permutations and Rejewski's Theorem*, `https://www.staff.uni-mainz.de/pommeren/MathMisc/Permut.pdf`.
[36] S. Ree, *Choi Seokjeong and traditional Asian mathematics, Confucian scholar's discovery predates the work of Euler*, In page 3 of Math & Presso, Daily News of the Congress, No 3, Friday 15 August 2014, printed and edited by Korea JoongAng Daily newspaper, publication commissioned by the International Congress of Mathematicians, ICM 2014, Seoul, Korea. Available on `http://www.icm2014.org/download/MP0815.pdf`.
[37] M. Rejewski, H. Zygalski and other undisclosed authors, Kurzgefasste Darstellung der Auflösungsmethoden, Bertrand archives, Service Historique de la Défense, Vincennes, France, DE 2016 ZB 25/6, Dossiers Nos. 281 and 282, ca. 1940.
[38] M. Rejewski, Memories of My Work at the Cipher Bureau of the General Staff Second Department 1930–45, second edition, Adam Mickiewicz University Press, Poznan, 2011.
[39] Random Permutation Statistics, Wikipedia article, consulted 14 March 2020, available at `http://en.wikipedia.org/wiki/Random_permutation_statistics`.
[40] A. Turing, Mathematical Theory of ENIGMA Machine, UK national archives, c. 1940.
[41] D. Turing with help of D. Kenyon, The Bombe Breakthrough, blue guide book, sold by Bletchley Park trust, 96 pages, 2018.
[42] H. Ulbricht, Die Chiffriermaschine ENIGMA, Trügerische Sicherheit, Ein Beitrag zur Geschichte der Nachrichtendienste, PhD thesis, Technische Universität Braunschweig, 14 April 2005.

O slabim rotorima, latinskim kvadratima, linearnim algebarskim prikazima, invarijantnim diferencijalima i kriptoanalizi Enigme

Nicolas T. Courtois, Marek Grajek i Michał Rams

Sažetak. Od 1920-ih do danas, pretpostavljalo se da rotori u stroju za šifriranje Enigma nemaju određenu slabost ili strukturu. To je zanimljiva situacija u usporedbi sa stotinama radova o S-kutijama i slabim postavljanjem blokovnih šifri. U ovom radu razmatramo što je normalno, a što nije normalno za rotor stroja za šifriranje, s referentnom točkom doista slučajnom permutacijom. Naše istraživanje pokazuje da većina originalnih Enigma rotora napravljenih u ratno vrijeme uopće nisu slučajne permutacije i skrivaju jaka diferencijalna svojstava nepromjenjiva pri rotaciji rotora. Također pokazujemo linearna / algebarska svojstva koja se odnose na prsten cijelih brojeva modulo 26. Neki rotori oponašaju određenu konstrukciju savršenih kvazigrupa, koja međutim funkcionira samo kad je N neparan. Većina ostalih rotora jednostavno pokušavaju aproksimirati idealnu situaciju. Prema našim saznanjima, ove činjenice su nove i nisu proučavane prije 2020. godine.

Nicolas T. Courtois
University College London, Gower Street, London, UK
E-mail: n.courtois@ucl.ac.uk

Marek Grajek
Independent expert on crypto history, Grodzisk Mazowiecki, Poland
E-mail: mjg@interia.eu

Michał Rams
Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland
E-mail: rams@impan.pl

Received: 11.12.2020.
Revised: 23.3.2021.
Accepted: 13.4.2021.