The Zschweigert Cryptograph – A Remarkable Early Encryption Machine

Klaus Schmeh
Private Scholar
www.schmeh.org
klaus@schmeh.org

Abstract

The *Zschweigert Cryptograph* is one of the many cipher machine designs developed in the years following the First World War (1914-1918). It was invented by textile engineer Rudolf Zschweigert, who had designed programmable stitching machines before and apparently transfered his computing expertise to cryptology. Unlike the Enigma and as good as all other crypto devices of the time, the *Zschweigert Cryptograph* implements a transposition cipher, not a substitution cipher. To the author's knowledge, it was the first encryption machine that worked with keys provided on punched cards. The goal of this paper is to introduce the *Zschweigert Cryptograph* and its history, to provide a mathematical specification of its encryption algorithm, and to explore how it can be cryptanalyzed. It will be shown that the *Zschweigert Cryptograph*, which was probably never used in practice, was insecure even by the standards of the 1920s and not convenient enough to compete with other encryption machines of the time.

1 Introduction

It is a well-known fact that the failure of almost all important (manual) encryption systems used in the First World War led to the invention of numerous encryption machines in the years after. Among the best-known crypto devices of this era are the Enigma, the Hebern rotor designs, the Kryha encryption machines and Arvid Damm's cipher devices – just to name a few.

A lesser known encryption machine from the post-WW1 years is the *Maschine zum Herstellen chiffrierter Schriftstücke* ("Machine for producing enciphered documents") by German engineer Rudolf Zschweigert. We will refer to this machine as *Zschweigert Cryptograph*.

To the author's knowledge, the *Zschweigert Cryptograph* was never built (perhaps with the exception of prototypes that are now lost), let alone used in practice. The only known source describing this machine is a patent filed by Rudolf Zschweigert in 1919 and granted one year later (Zschweigert, 1920).

Though it was never used in practive, the *Zschweigert Cryptograph* is note-worthy for several reasons:

- Contrary to virtually all other mechanical and electric cipher machine designs, the *Zschweigert Cryptograph* implements a transposition cipher (not a substitution cipher). This property is the reason why this machine is mentioned in (LANAKI, 1996) and (Nichols, 1998). However, both sources give no description of the *Zschweigert Cryptograph*. As far as the author knows, nothing detailed has ever been published about this device, except the patent. The *Zschweigert Cryptograph* should not be confused with the transposition cipher tool (it's not really a machine) invented by Luigi Nicoletti in 1918, which is mentioned in (Kahn, 1996).

- The *Zschweigert Cryptograph* was invented by a textile entrepreneur. As is well known, the textile industry adapted computing hardware long before encryption technology did. As will be shown, the *Zschweigert Cryptograph* represents a design that transferred computing expertise from the textile industry to cryptology.

- The *Zschweigert Cryptograph* is the earliest cipher machine the author is aware of that applies a punched card as key.

2 Rudolf Zschweigert

Rudolf Zschweigert (1873-1947) was a German engineer, who lived in the cities of Chemnitz, Plauen, and Hof, Germany. In the 1930s, he was a member of the city council of Hof. He was married to Gertrud (1891-1982). Zschweigert is best remembered for having built up a major mineral and meteorite collection, which is today preserved in the *Museum Reich der Kristalle* in Munich, Germany (Wilson, 2019).

Rudolf Zschweigert's professional dedication was that of a textile manufacturer and factory owner. The *Weberei Zschweigert* ("Weaving Mill Zschweigert") existed from 1921 to the 1960s. Between 1909 and 1934, Zschweigert was granted at least 15 patents in Germany, Austria, Switzerland and the USA. 14 of these patents concerned textile technology, especially looms and stitching machines. Zschweigert's only patent not related to textiles is the one relating to the encryption machine discussed in this paper.

Rudolf Zschweigert was not the only cipher machine inventor with a background in the textile industry. A second and much more prominent person of this kind was Swedish engineer Arvid Damm (1869-1927), who cooperated with his country man Boris Hagelin in the 1920s and laid the foundation of what was to become Crypto AG, a company that still exists today (Hagelin, 1994).

3 Specification of the Encryption Algorithm

In the following, we provide a formal specification of the encryption algorithm implemented by the *Zschweigert Cryptograph*. It is based on the informal description in the patent.

The *Zschweigert Cryptograph* uses a $9 \times n$ binary matrix K as key, with n being a positive integer. Every row of K has a Hamming weight of one, which means that there is exactly one one per row, while the eight other values are set to zero. Here's an example (with $n = 5$) we denote as K_{exmpl}:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

In the following, we will denote the position of the one in row i as k_i. In other words:

$$k_i = j :\Leftrightarrow K_{i,j} = 1$$

The key space of the *Zschweigert Cryptograph* is, of course, dependent on n, the number of rows of the matrix. As there are nine possibilities for each row, the number of keys is 9^n. This means that with a 40-rows matrix, exhaustive key search is about as laborious as with a 128-bit key.

The alphabet used by the *Zschweigert Cryptograph* is not specified in the patent. Instead, it is assumed that every character provided by the typewriter in use can be encrypted. To keep things simple, we assume that only upper-case letters from A to Z are encrypted, which makes an alphabet of 26 characters. It seems likely that such an alphabet would also have been used in practice.

We denote the plaintext as $P = p_i$ with $i = 0, 1, ..., l-1$ and l being the number of letters in the plaintext. As an example, we take $P_{example} :=$ $"HISTOCRYPTTWENTY"$, which means that $p_0 = "H", p_1 = "I", p_2 = "S", ..., p_{15} = "Y"$ and $l = 16$.

The ciphertext is represented by another matrix, C. C has nine columns. The elements of C are from the set $\{A, ..., Z, -\}$ with $"-"$ representing a null character. At the beginning, all elements of C are set to $"-"$. When we write C, we omit all lines containing only the null character.

3.1 Encryption

To define the encryption algorithm, we need the following function:

```
Write-to-Matrix ($C, column \in \{1...9\}, p \in \{A, ..., Z\}$)
$i = 0$
while $C_{i,column} \neq "-"$ : $i = i + 1$
    $C_{i,column} := p$
return $C$
```

The encryption algorithm is specified as follows:

```
*Encrypt* $(P,K)$
$n :=$ number of rows of $K$
For $i = 0$ to $l-1$:
    $C :=$ Write-to-Matrix $(C, k_{i \bmod n}, p_i)$
return $C$
```

This means that the first letter of the plaintext takes the column of the one in the first line of the key matrix. The second character takes the column of the one in the second line and so on. Each letter is written into the highest line of the plaintext matrix that is still empty.

With P_{exmpl} and K_{exmpl}, we get the following ciphertext (denoted as C_{exmpl}, see also figure 1):

$$\begin{pmatrix} T & - & - & H & - & S & I & - & - \\ P & - & - & C & - & O & R & - & - \\ N & - & - & T & - & Y & W & - & - \\ - & - & - & Y & - & T & - & - & - \\ - & - & - & - & - & E & - & - & - \\ - & - & - & - & - & T & - & - & - \end{pmatrix}$$

Noting the ciphertext this way is unpractical if it is, for instance, sent by telegram. The patent therefore suggests the use of separators, but details are not given. A possible way to write down the ciphertext is: TPN - - HCTY - SOYTET IRW - -.

3.2 Decryption

To define the decryption algorithm, we need the following function:

```
*Read-from-Matrix* $(C, column \in \{1...9\})$
$i = 0$
while $C_{i,column} = " - " : i = i + 1$
    $p := C_{i,column}$
$C_{i,column} := " - "$
return $p$
```

The decryption algorithm now can be specified as follows:

```
*Decrypt* $(C,K)$
$n :=$ number of rows of $K$
For $i = 0$ to $l-1$:
    $p_i :=$ Read-from-Matrix $(C, k_{i \bmod n}, p_i)$
return $P$
```

4 Construction of the Machine

While the patent provides only short coverage of the encryption method (not to mention a theoretical foundation), the construction of the machine is described in great detail. This is probably because Rudolf Zschweigert was familiar with mechanical engineering, but not with cryptology.

As can be seen in figure 2, the *Zschweigert Cryptograph* is based on a mechanical typewriter. Instead of printing on a piece of paper, this typewriter prints on nine separate paper rolls. The roll used for a certain letter is controled by a unit that works with a punched card. This punched card corresponds with the matrix introduced in the previous chapter.

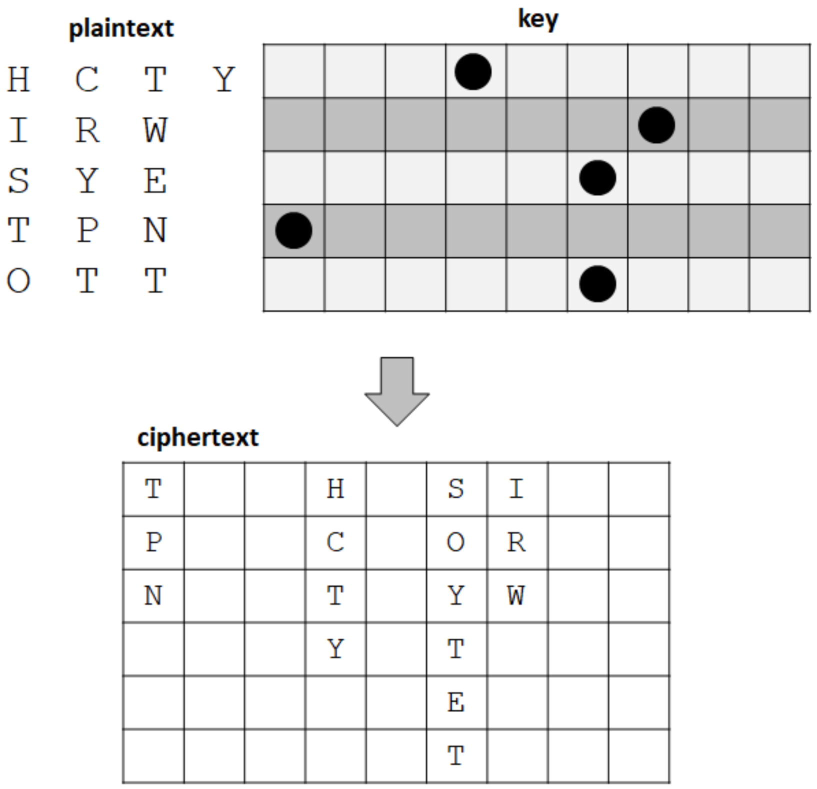
The punched card has nine columns and an arbitrary number of rows. In each row, there is exactly one hole. The mechanics of the machine always move the type used to the paper roll that corresponds with the column of the current punched card row and types a letter.

After a letter has been typed, the respective roll turns up by one unit and the next row of the punched card is read. When the end of the punched card is reached, the control unit starts with the first row again.

At the end, the user takes the nine paper rolls and reads the letter sequences on them. According to the patent, this can be done in a key-dependent order. However, from a cryptographic point of view, changing the order of the rolls doesn't make much sense, as this is equivalent with changing the order of the columns on the punched card, which can be done while the card is produced (unless, the card is reused and a different order of the rolls is applied each time – a case we don't cover in this paper).

If the encrypted message is transmitted by radio, the sender can read the ciphertext directly from the nine paper rolls and transmit them. If sent by letter, it is necessary to copy the ciphertext from the rolls (unless, of course, one doesn't mind sending nine paper strips by mail).

Decrypting works very similar as encrypting. Of course, an identical punched (key) card is necessary. No stylus is needed. The operator presses the space key repeatedly. The control unit will always move the paper roll to the center, where the next plaintext letter can be read. The receiver needs to copy each letter and thus receives the plaintext.



H	C	T	Y
I	R	W	
S	Y	E	
T	P	N	
O	T	T	

			●					
						●		
					●			
●								
					●			

T			H		S	I		
P			C		O	R		
N			T		Y	W		
			Y		T			
					E			
					T			

Figure 1: Using a matrix (represented by a punched card) as key, the plaintext HISTOCRYPT TWENTY is encrypted to a ciphertext that can be written as: TPN - - HCTY - SOYTET IRW - -.

It should be clear that encrypting a message with the *Zschweigert Cryptograph* is not especially convenient. The sender needs to copy the output in order to bring it to a format that can be sent by telegram or teletype. The receiver needs to copy every decrypted letter from the machine. This means that although the *Zschweigert Cryptograph* includes a typewriter, manual writing is necessary.

5 Historical Background

As is well-known, the textile industry played an important role in the history of information technology. In 1804, Joseph Marie Jacquard introduced the Jacquard machine, a loom controlled by punched cards (Jacquard, 2019). The Jacquard machine (figure 5) is generally regarded as the first programmable hardware in history. The concept of programming a machine with a punched card became widely accepted in the 20th century, first in Hollerith machines, later in computers.

It is an interesting question whether the crypto machine designs of aforementioned Swedish engineer Arvid Damm were influenced by computing technology he encountered in the textile industry. To our knowledge, this question has never been researched.

In the case of Rudolf Zschweigert, we have found a source that might link the computing technology of the textile industry with cryptology. In 1908, Zschweigert was awarded two patents for a stitching machine that is controlled by a punched card. The one patent concerns the machine itself (Zschweigert, 1908a), the other one a device for punching the holes into the card (Zschweigert, 1908b).

It seems likely that this stitching machine laid the foundation for the *Zschweigert Cryptograph* that was invented a decade later. While the punched card in the stiching machine controled the production of a pattern on a piece of cloth, the punched card in the cipher machine controled an encryption process on a typewriter.

To the author's knowledge, the *Zschweigert Cryptograph* is the earliest cipher machine that used punched-card keys. Many others were to follow, including the HC-9 (Reuvers, 2019), the Filka (Reuvers, 2019), the KW-7 (Reuvers, 2019), and the T-310 (Schmeh, 2006).

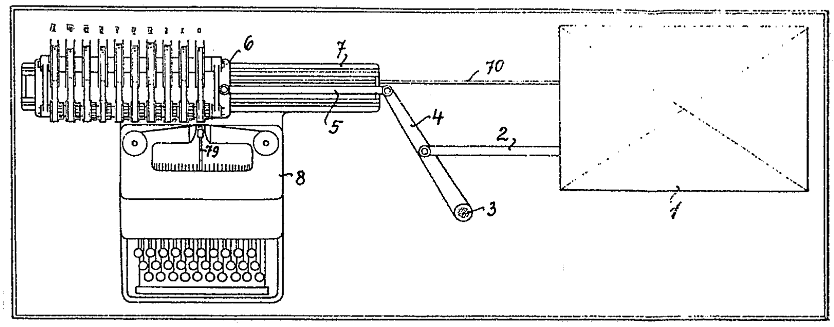


Figure 2: The *Zschweigert Cryptograph* is based on a mechanical typewriter. It uses nine movable co-axial paper roles (left) that are contoled by a unit (right), the details of which are not depicted in this diagram. *Source: Patent*

Fig. 3.

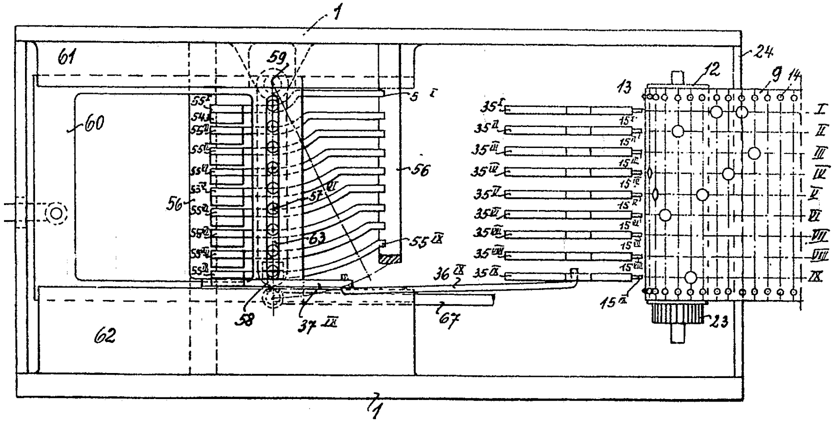


Figure 3: The key of the *Zschweigert Cryptograph* is provided on a punched card with nine columns (right). *Source: Patent*

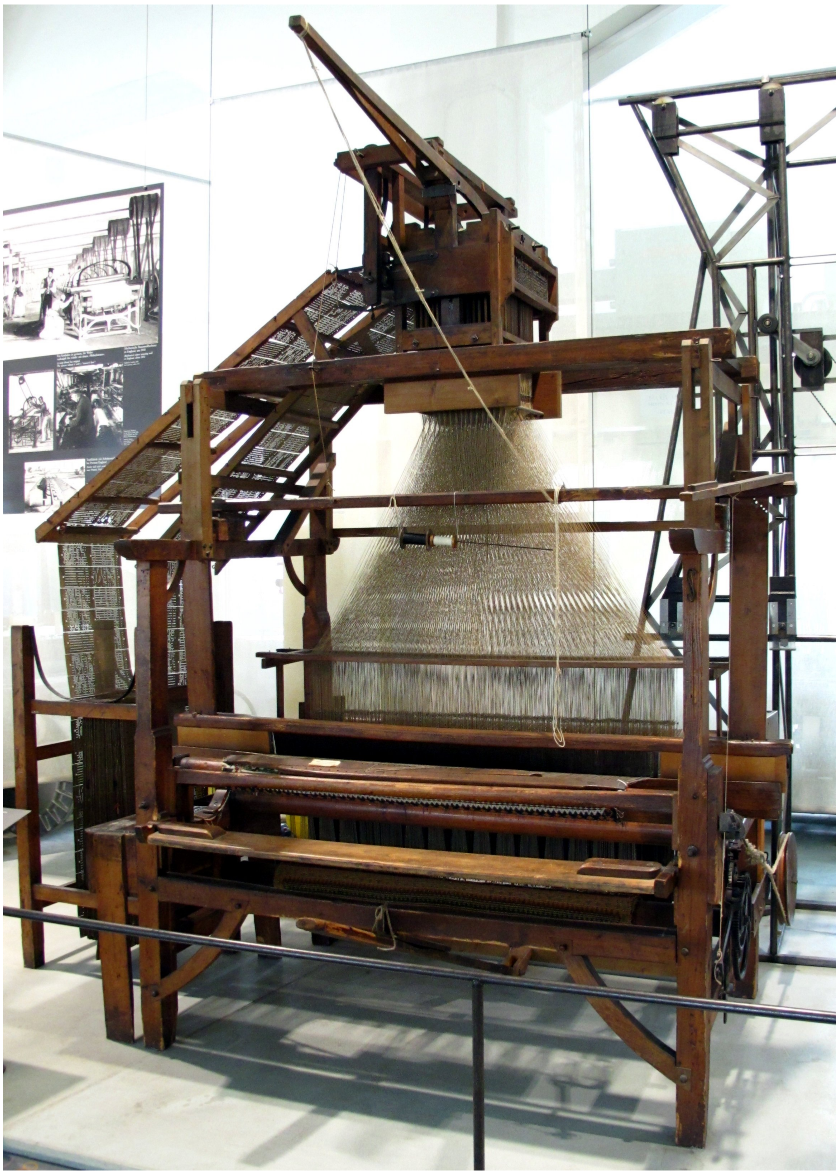


Figure 4: The Jacquard machine is a 19th century loom controled by a punched card. It is considered the first programmable device in history. Rudolf Zschweigert, a textile engineer, might have been influence by the Jacquard machine when he designed his punched-card controlled cryptograph. *Source: Wikimedia Commons / 29263a,b / Dmm2va7*

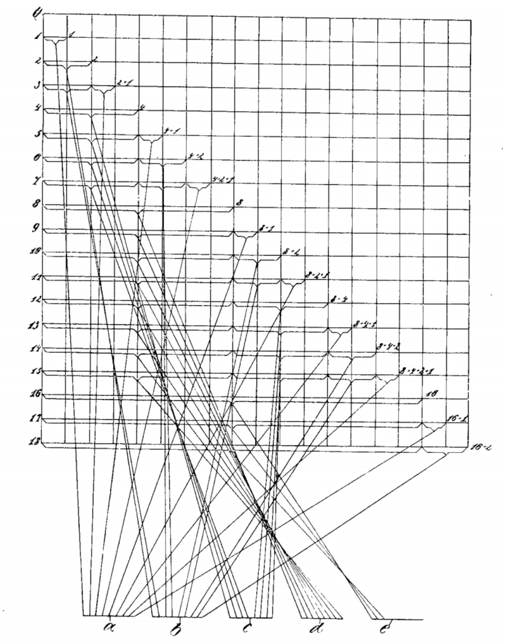


Figure 5: Rudolf Zschweigert invented a stitching machine that is controled by a punched card. It seems likely that this device machine laid the foundation for the *Zschweigert Cryptograph. Source: Patent*

6 Cryptanalysis Considerations

When it comes to cryptanalyzing the *Zschweigert Cryptograph*, two steps need to be distinguished. In the first one, the codebreaker tries to find out how many rows the key matrix has; in the second step, the position of the ones in the matrix is determined. When the matrix is completely reconstructed, the ciphertext can be easily decrypted.

6.1 Determining the Number of Matrix Rows

The most obvious method for determining the number of rows in the key matrix is brute force. If we look at the example ciphertext C_{exmpl}, we see that it consists of 16 letters. With a computer program it is not very difficult to check every matrix length between, say, 4 and 16. We need to apply the second step (locating the ones in the matrix) on each of these candidates.

While brute force (with a computer program) is certainly an appropriate approach today, the cryptanalysts of the 1920s needed an attack that could be carried out manually. In fact, such a method is available. If we look at our example ciphertext C_{exmpl}=TPN - - HCTY - SOYTET IRW - -, we see that the number of letters in the nine columns is 3, 0, 0, 4, 0, 6, 3, 0, and 0. With the exception of 4, each of these numbers is divisible by three. When 4 is divided by 3, the remainder is 1. Taking into account that we are dealing with a 16-letter message, this can best be explained with a five-row matrix, the first row of which is used four times, while rows 2-4 are used three times each. This means that the key matrix has five rows.

Of course, it is also possible that the number of rows is 16, which would mean that the matrix is as long as the plaintext. However, following Occam's Razor, which states that the simplest explanation should be taken first, a cryptanalyst will usually start with examining the five-rows hypothesis.

Things might not always be this easy, especially when the plaintext is longer than in our example and the matrix has more rows. However, we assume that guessing the number of rows in the key matrix will usually be possible. To find out more, further research is necessary.

6.2 Locating the Ones in the Matrix

We now assume that the number of matrix rows is known or that a guess has been made (for instance, in the course of a brute-force attack). In the next step, we need to detemine the location of the ones. The task of the cryptanalyst becomes easier if the number of rows is considerably smaller than the message length, i.e., if each row is used to encrypt several letters. The case where the number of matrix rows exceeds the plaintext length is not relevant, as we can always ignore the rows not used.

In the example shown in figure 1 five matrix rows encrypt a plaintext consisting of 16 letters.

One weakness of the *Zschweigert Cryptograph* is obvious: Just by looking at the ciphertext we can easily derive the number of ones of each column (i.e., the Hamming weight). If we look at the example ciphertext C_{exmpl}=TPN - - HCTY - SOYTET IRW - -, we immediately see that the second, the third, the fifth, the eigth, and the ninth column of the matrix must be empty, because there are no letters in the corresponding positions of the ciphertext.

Considering that there are three letters in both the first and in the seventh column of the ciphertext, we can conclude that each of the corresponding matrix columns contains exactly one one. The six letters in the sixth ciphertext column lead to the conclusion that the sixth matrix column contains two ones. The four letters in the fourth ciphertext column are especially helpful, as they not only tell us that there is one one in the fourth matrix column but also that this one is located in the top matrix row.

We have now reconstructed the first matrix row, and we know that columns 2, 3, 5, 8, and 9 are empty. This leaves us with 4!=24 possibilities for the positions of the ones in rows 2 to 5. We can even reduce this number to its half because we know that there are two equal rows, which are interchangeable. So, in the end, there are only 12 combinations to try. With a computer program, this can easily be achieved by brute force.

If no computer is available, as it was the case when the *Zschweigert Cryptograph* was invented, the technique of multiple anagramming, as described by Helen Fouché Gaines in her book *Elementary Cryptanalysis*, can be used (Fouché Gaines, 1939). The details are not within the scope of this paper.

Things become a little more complicated, of course, if we use a key matrix with more rows. This is especially the case if the matrix is as long as the plaintext. Multiple anagramming still seems possible, even if it is much more laborious than in the simple example we provided. We assume that the computer-based technique of hill climbing (Schmeh, 2017), which has proven extremely powerful in the breaking of historical ciphers, is the best means to attack a cryptogram of this kind and we believe that this approach would work well against the the *Zschweigert Cryptograph*. Again, the details are out of scope in this paper.

Overall, we can conclude that breaking a message encrypted with the *Zschweigert Cryptograph* is feasible, even with the means of a 1920 cryptanalyst. The machine can be made more secure by using matrices with more columns and by forbidding the use of matrices that are shorter than the plaintext. Nevertheless, the author's impression is that the concept of the *Zschweigert Cryptograph* is not suitable for a reasonably secure encryption machine. Future research might go into more detail about this question.

7 Future Work

As far as the author of this work knows, this paper is the first publication about the *Zschweigert Cryptograph*, except the patent. It is therefore obvious that additional research work is necessary in order to understand this machine and its background. Especially, the following items should be researched:

- The biography of Rudolf Zschweigert appears to be not especially well documented. While there is some information available online, the author of this paper is not aware of a comprehensive overview, let alone a detailed account of Zschweigert's life. The author assumes that one needs to research the archives in Zschweigert's home places Chemnitz, Plauen, and Hof in order to learn more.

- It is not known how Zschweigert came to the idea to construct an encryption machine and how much he was influenced by the textile technology of the time and his own inventions in this area. Perhaps, things become clearer when more about Zschweigert's biography is known.

- In this paper, the author provided a few approaches to cryptanalyze the *Zschweigert Cryptograph*. Further research might examine this topic in more detail. Especially, it will be interesting to explore additional methods for determining the number of rows of the key matrix. In addition, the use of hill climbing or a similar technique for locating the posisitions of the ones in the matrix deserves further investigation.

- As mentioned, the *Zschweigert Cryptograph* is one of the first (or even the first) encryption machines working with a key provided on a punched card. Many others were to follow. A comprehensive treatise of punched cards in cryptology would be an interesting research project.

- A software implementation of the algorithm of the *Zschweigert Cryptograph* or even a simulator of the machine could be created. Such a program could be integrated into CrypTool or a similar software.

8 Conclusion

The 1920s were a special time in the history of mechanical encryption technology. On the one hand, the necessity for automated encryption had become evident, which led to the first generation of encryption machines being developed. On the other hand, the topic was not especially well understood yet. This resulted in numerous cipher machine designs that were not suited for practical use. For instance, the first prototypes of the Enigma (with up to seven rotors and a typewriter functionality) proved too complex and too expensive. Alexander von Kryha's encryption machines had an impressing visual design and were marketed very well, but were completely insecure. The same is true for devices such as Cryptocode and the Beyrer Cryptograph. Arvid Damm's original designs were not very successful, either.

The *Zschweigert Cryptograph* fits perfectly well with the aforementioned crypto devices. Though it implements a few promising concepts – especially the punched card used as key –, it must be considered an experimental machine that was not suited to be used in practice.

The transposition cipher the *Zschweigert Cryptograph* realizes turned out to be an evolutionary dead end. No machine of this kind ever played a major role when machine encryption became popular in later years.

Acknowledgments

The author would like to thank Christiane Angermayr.

References

Fouché Gaines, Helen. 1939. *Cryptanalysis*. Dover Publications, New York, USA.

Boris Hagelin. 1994. *The Story of Hagelin Cryptos*. Cryptologia Volume 18, 1994 (3):204-242

David Kahn. 1996. *The Codebreakers*. Scribner, New York City, NY:764.

LANAKI. 1996. *Classical Cryptography Course*. www.ahazu.com/papers/lanaki:Lesson 21.

Randall K. Nichols. 1996. *ICSA Guide to Cryptography*. McGraw-Hill, New York City, NY:153.

Paul Reuvers, Marc Simons. 2019. *The HC-9*. www.cryptomuseum.com.

Paul Reuvers, Marc Simons. 2019. *The Fialka*. www.cryptomuseum.com.

Paul Reuvers, Marc Simons. 2019. *The KW-7*. www.cryptomuseum.com.

Klaus Schmeh. 2006. *The East German Encryption Machine T-310 and the Algorithm It Used*. Cryptologia Volume 30, 2006 (3):251-257

Klaus Schmeh. 2017. *A mird in the hand is worth two in the mush: Solving ciphers with Hill Climbing*. http://scienceblogs.de/klausis-krypto-kolumne/2017/03/26/a-mird-in-the-hand-is-worth-two-in-the-mush-solving-ciphers-with-hill-climbing/

Wikipedia entry "Jacquard machine". retrieved 2019-12-15.

Wendell E. Wilson. 2019. *Mineralogical Record*. Biographical Archive, at www.mineralogicalrecord.com.

Rudolf Zschweigert. 1908. *Einrichtung zum Verstellen des Stickrahmens für automatische Stickmaschinen*. Patentschrift 45620 des Eidgenössischen Amts für geistiges Eigentum vom 31. August 1908.

Rudolf Zschweigert. 1908. *Kartenschlagmaschine zum Lochen von Karten für Vorrichtungen zum automatischen Bewegen von Strickrahmen*. Patentschrift 46570 des Eidgenössischen Amts für geistiges Eigentum vom 31. August 1908.

Rudolf Zschweigert. 1920. *Maschine zum Herstellen chiffrierter Schriftstücke*. Patentschrift 329067 des Reichspatentamts ausgegeben am 12. November 1920.