German Mathematicians and Cryptology in WWII

Frode Weierud (Crypto Cellar Research)
and
Sandy Zabell (Northwestern University)

March 14, 2019

Abstract

By now, a great deal is known about the contributions of Alan Turing, I. J. Good, Max Newman, and other mathematicians who worked at Bletchley Park during World War II. But what about the other side? Until recently, very little was known about the German mathematicians who aided the Nazi war effort: who were they, where did they work, and what did they do? But now, thanks to the release of a large number of TICOM documents in recent years, an initial picture is beginning to emerge. In this paper we identify the most important mathematicians who worked in the different German cryptologic organizations during the war: who they were, how they were recruited, which organizations they were in, and what they did (when this is known). Although their successes never rivaled those of Bletchley Park, they did have successes, and these were sometimes due to the efforts of mathematicians who went on to have distinguished careers after the war.

One question that motivated this study was to understand the reasons for the German communications security meltdown during the war: how they got the Enigma and Tunny security assessments partly right but mostly wrong. As will be seen, this was not due to a lack of talent: some of the very best German mathematicians contributed to their war effort. The answer lies instead in how these potentially very useful assets were actually used (in striking contrast to what happened at Bletchley Park).

1 The motivating question for this paper

Many mathematicians worked at Bletchley Park during WWII and made major contributions to the war effort. These included outstanding research mathematicians such as Alan Turing, I. J. Good, Max Newman, Shaun Wylie, Peter Hilton, and William Tutte. But who were their German counterparts? After all, before the second world war (or at least before the rise to power of the Nazis) Germany was the world center for mathematics. It is hard to believe that German mathematicians, unlike their Allied counterparts, played no significant part in the 1939–1945 cryptologic war. And yet virtually nothing has been written on this intriguing subject.

1.1 Challenges

This paper is an initial attempt to answer this question. Cryptology is perhaps unique among the sciences as being the only one in which – for obvious reasons – its practitioners (at the state level) are usually reluctant to advertise their successes. But quite apart from this standard difficulty, several distinctive challenges present themselves to the historian attempting to answer our question. These challenges include:

a. The Germans lost. Under this head there are really two separate issues. First, there is the inevitable destruction of equipment, intercepts, documents, and so on that one would expect (and which indeed did take place) when a country suffers a defeat of the magnitude that Germany did. Second, there is the phenomenon that "Victory has a thousand fathers; defeat is an orphan". Unlike their Allied counterparts, who would have been more than willing to detail their wartime cryptologic exploits (and immediately began doing so when this was first permitted several decades later), very few German mathematicians (with one significant exception discussed later) displayed any eagerness to discuss their contributions to the fatherland in the aftermath of total defeat and the revelations of the extensive crimes of the Nazi regime.

b. German organization. There were no fewer than six major German cryptologic organizations at the outbreak of war, serving the Armed Forces (*Wehrmacht*), Army (*Heer*), Navy (*Kriegsmarine*), Air Force (*Luftwaffe*),

Foreign Office (*Auswärtiges Amt*), and Nazi party leadership.[1] Quite apart from the question of the impact such redundancy had on the efficient use of resources and operational security, this necessarily complicates systematic historical discussion of German cryptology during the war: there are really six separate such histories, because there was little cooperation between the six (the one major exception being contacts between OKW/Chi, the Wehrmacht organization, and its cryptanalytic counterparts in the Army and Foreign Office).[2]

c. Successive reorganization. Reorganization seems to be a constant in bureaucracies, and German signals intelligence was no exception. Simplifying a complex subject, one can identify three major periods in the evolution of German cryptologic efforts during the period in question: the transition from the Weimar Republic to the Third Reich; a dramatic expansion in German efforts after the outbreak of war; and finally the period after July 20, 1944. Organizations are renamed, responsibilities reassigned, personnel shifted from one group to another.

What is the relevance of the date July 20, 1944? This was the date of the unsuccessful plot to assassinate Adolf Hitler; several members of the Signal Corps, including its head, Lieutenant General Erich Fellgiebel, Colonel Kurt Hahn (his Chief of Staff), and Lieutenant General Fritz Thiele (the Chief of Wehrmacht Communications) were heavily implicated in the plot (indeed all three were executed for treason less than two months later), and this led to a major restructuring of the Wehrmacht and Army signals intelligence organizations.[3]

[1]These six organizations had a variety of customers and – especially in the case of the military ones – supplied information to intelligence services having a much broader scope (e. g. , human and technical intelligence), and which they served in various ways. For an excellent overview of the different German intelligence services during WWII together with some discussion of the role signals intelligence played, see David Kahn's classic *Hitler's Spies* (1978).

[2]The Wehrmacht (previously the *Reichswehr* until 1935), was the collective term for the armed forces of Germany, consisting of the Army, Navy, and Air Force. Because each of the three separate services had their own High Command and General Staffs, separate from those of the Wehrmacht, the latter had relatively limited control over the day-to-day operations of the three services. For this reason the limited coordination between OKW/Chi and the three service cryptologic organizations is hardly surprising.

[3]For further information about the July 20, 1944 plot to kill Hitler, see Fest (1997), Moorhouse (2006), Jones (2008), and Schradar (2009).

There seems to be no way to deal with the second of these challenges (the multiplicity of organizations) except to discuss each organization separately (although, as will be seen, there were relatively few mathematicians in the Navy, Air Force, and *Forschungsamt*, the latter of which served the Nazi leadership). And we will deal with the third challenge (reorganization) by focussing to a considerable extent on individuals (who might be reassigned from one organization to the other during the war). As for the first challenge (documentation), there is an important resource that has only recently begun to be mined.

1.2 Resources

This important resource is TICOM, an acronym for the **T**arget **I**ntelligence **Com**mittee. This was a joint UK-US operation set up at the end of the war, tasked with acquiring German signals intelligence assets: personnel, equipment, intercepts, and so forth. It can be thought of as analogous to Operation Paperclip, the much better known operation at the end of the war to round up German rocket scientists such as Werner von Braun (or the ALSOS Mission to discover German nuclear secrets).

The extent of the TICOM operation was remarkable: it continued its work for several years after the end of the war, issuing hundreds of reports in the process. Many of these have now been declassified, falling into different series (designated as D, DF, E, I, IF, M). Much of what TICOM found is summarized in the nine-volume report *European Axis Signal Intelligence in World War II as Revealed by "TICOM" Investigations and by Other Prisoner of War Interrogations and Captured Material, Principally German*, issued in 1946 by the US Army Security Agency (Army Security Agency, 1946, cited as EASI below).[4] Five of the nine volumes summarized the information gathered up to that point (1946) on five of the six organizations.[5] All referenced TICOM documents are listed in Section 12.3.

[4]EASI provides a convenient synthesis of the information contained in a large number of TICOM reports, some of which have not yet been declassified. It necessarily covers, however, only those reports issued prior to its release in May 1946. One should also "trust but verify" when using it: some statements in it differ from the cited TICOM source.

[5]Although a number of the TICOM reports dealt with German Naval cryptology, no volume of EASI is devoted to the German Navy's signals intelligence efforts. The reasons for this are unclear; perhaps the Army Security Agency thought it more appropriate to leave this to the US Naval Security Group.)

There are two other major sources of information worth noting here. One is the *Mathematics Genealogy Project* at `http://genealogy.math.ndsu.nodak.edu/index.php` (accessed December 8, 2018). This is an online reference database listing people who received a Ph.D. in mathematics, giving the date, institution, advisor, title of the thesis, and subsequent students, if any, of the person receiving the degree. It is genuinely international in scope, relatively complete and accurate in its content, and is an invaluable tool in tracing mathematical lineages. We will have frequent occasion to refer to it (cited below as the MGP). For German mathematicians in particular there is also Renate Tobies's *Kurzbiographien* (Tobies, 2006; "Short Biographies"), available at `https://www.mathematik.de/kurzbiographien` (accessed December 8, 2018).

Finally, there is the German version of the Wikipedia, which can be accessed at `https://de.wikipedia.org/`. Far more complete information (say about individual mathematicians) is sometimes given in the German version of the Wikipedia than its English counterpart (and indeed sometimes there is no English entry at all).

2 The history of OKW/Chi

The *Oberkommado der Wehrmacht*, the High Command of the German Armed Forces, had its own cryptologic organization. The history of this Cipher Bureau during the two decades prior to the outbreak of the Second World War illustrates some of the challenges in discussing this organization: essentially the same unit persisted under successive parent reorganizations.

After Germany's defeat in the First World War, the German Army's signals intelligence organization was reborn as a new *Chiffrierstelle* (Cipher Bureau), housed in the *Abwehr* (Military Intelligence). On April 1, 1928, the Abwehr was transferred to the *Reichswehrministerium* (Ministry of Defense), and with it, its Cipher Bureau.[6] When the Oberkommando der Wehrmacht (OKW) was established on February 4, 1938, this Cipher Bureau was detached from the Abwehr and transferred to the OKW, becoming its *Chiffrierabteilung* (Cipher Department). Organizationally, it was part of the *AmtsgruppeWehrmachtnachrichtenverbindungen* (Armed Forces

[6]In 1935 the *Reichswehrministerium* was ominously renamed the *Reichskriegsministerium*, or Ministry of War.

Group Wehrmacht Communications, Ag. WNV), which in turn was part of the *Wehrmachtführungsstab* (Armed Forces Operations Staff, WFSt).

So the official designation of the Cipher Department was OKW/WFSt/Ag. WNV/Chi . . . , but for both TICOM and us, OKW/Chi. (We will use this even for the period prior to 1938.)

In this type of situation, it is often easier to focus on the individuals in an organization, rather than the organization itself, whose home, title, and responsibilities can change – sometimes radically – over time.

2.1 Wilhelm Fenner (1891–1961)

In 1922 an ex-Army officer, Wilhelm Siegwart Fenner (April 14, 1891–July 25, 1961), was placed in charge of the Reichswehr's cryptanalytic unit. Fenner wrote later that at this point "I still understood very little about cryptanalysis" (TICOM DF-187, p. 4). Although apparently of good—but not outstanding—cryptanalytic ability, Fenner was however clearly a gifted organizer, and under him the cryptanalytic section grew substantially. He continued in this role until the surrender of Germany on May 7, 1945. Originally released June 20, 1945 without being questioned about OKW/Chi, he was later put on a list of "most wanted" individuals for interrogation, and eventually detained on the evening of July 2, 1946. TICOM I-200 summarizes his interrogation. TICOM then asked Fenner to write a detailed history of his career in OKW/Chi; they could scarcely have found a more cooperative individual. Fenner proceeded to write a 244 page report in German, translated by TICOM into English (as DF-187 and DF-187A to 187G).[7] Much of Alvarez (2007) is based on this material, but Fenner's meticulous account could easily be expanded to an entire book.[8]

In 1936 there were no professional mathematicians working for OKW/Chi. (Or indeed anywhere else in German signals intelligence, with the arguable

[7]EASI, Volumes 3 and 4 (both dated May 1, 1946) were written before Fenner was (re)detained. As I-206 notes, "[t]he information available from this source [Fenner] considerably expands and to some extent modifies the history of [OKW/Chi and OKH/Chi] given in [EASI, Volumes 3 and 4]".

[8]Fenner's whereabouts after 1946 are not a matter of public record, although he was in correspondence with Dr. Hüttenhain (see below) as late as 1958, and may have played some role in West German signals intelligence. He died July 25, 1961, in Bad Godesberg, of heart and lung disease. (Source for date, place, and cause of death of Fenner: unpublished letter from his daughter Ilse Fenner to David Kahn, June 8, 1970, National Cryptologic Museum, Kahn papers, DK 63-37; Bonn city archives.)

exception of the Foreign Office, discussed later.) This all changed in 1937 when Fenner made the unusual decision to hire a Dr. Erich Hüttenhain.

2.2 Enter Dr. Hüttenhain (1905–1990)

Dr. Erich Hüttenhain (January 26, 1905–December 1, 1990) came to what was to be a lifetime in cryptology by a rather curious path. Receiving his doctorate at Münster in astronomy in 1933 (supervisor Martin Ludlow), he came in contact with Professor Friedrich Wilhelm Hans Ludendorff (1873–1941), the Director of the Potsdam Observatory. Ludendorff (a brother of the famous General Erich Ludendorff) was interested in dating astronomical events reported in Mayan records in order to reconstruct Mayan history. Mayan scripts at that time were largely undeciphered, and Hüttenhain's interest in them led him in turn to cryptography. In 1937 he submitted a proposed cryptographic system to the German military. Although neither novel nor secure, it seems to have been far more sophisticated than what the amateur puzzle enthusiast might come up with, for on the strength of it Hüttenhain was interviewed by Fenner and then offered a job in OKW/Chi (I-31, p. 2; DF-187E, pp. 16–18). He was the first mathematician to join that organization.

Dr. Hüttenhain's rise in OKW/Chi was rapid, as he soon proved valuable to it. In 1937 Hüttenhain and Fritz Menzer visited Dr. Werner Liebknecht in Wa Pruef 7;[9] "[t]hey discovered that a message on the old SZ40 [an online teleprinter encryption device then under development] could be solved within two days" (I-31, p. 17). In 1939 Hüttenhain was asked for his opinion of the Siemens T52 A/B (another online teleprinter encryption device also under development); although the Army thought it secure, "he found that it could be solved on a hundred letters without a crib [that is, conjectured or known plaintext]" (I-31, p. 14). After about a year in OKW/Chi Hüttenhain became an independent member of it, concentrating on mathematical cryptanalysis and "instructed to expand the mathematical side as he thought fit" (I-31, p. 2). By the outbreak of the war he headed OKW/Chi's mathematical cryptanalysis section. Here too he was quite successful: when on September 2, 1939, a French Army Code (called F110 by the Germans) was replaced by a new code, Hüttenhain was dispatched the next day to Frankfurt to lead a

[9]The HWA, *Heeres Waffenamt*, was Army Ordinance; Wa Pruef, *Waffenpruefung*, the division of the HWA devoted to developing and testing weapons and other devices; Wa Pruef 7 the signals section of Wa Pruef.

group tasked with breaking the new code. This was successfully accomplished by the start of October (TICOM D-60, pp. 4–5).[10]

Dr. Hüttenhain was detained by TICOM in Flensburg in May 1945. His interrogators very quickly recognized the value of their prize: his initial interview on May 21, 1945 (I-2) was cut short (noting that "Regierungsrat Dr. Erich Hüttenhain was the best cryptographer at OKW/Chi"); more detailed interrogations then took place on June 15 and 18–21 (I-21 and 31), and arrangements were made to send him to the UK for further questioning. He was subsequently returned to the British zone in 1946 (I-202, p. 1) and then released.

At this point Dr. Hüttenhain's career took a second surprising turn. General Reinhard Gehlen had been the head of the FHO (*Fremde Heere Ost*), the German Army's military intelligence organization for the Eastern Front (see generally Pahl, 2016). After surrendering to US forces at the end of the war, in June 1946 Gehlen was put in charge of an intelligence operation, the OG (*Organisation Gehlen*, sponsored first by the US Army and then the CIA), to collect information and intelligence about the Soviet Union. The OG rapidly expanded, soon becoming the main West German spy organization. In 1947 a cryptologic unit was set up within it, under the cover name of the *Studiengesellschaft für Wissenschaftliche Arbeiten* (Study Group for Scientific Work), with Dr. Hüttenhain as its head.

After the *Bundeswehr*, the Armed Forces of the new Federal Republic of Germany, was established on November 12, 1955, the OG became the BND (*Bundesnachrichtendienst*, Federal Intelligence Service), with General Gehlen remaining as its head until retiring in 1968. Soon after (1956), the Studiengesellschaft became the *Zentralstelle für das Chiffrierwesen* (ZfCh, the Central Office for Cryptology, the West German equivalent of the UK GCHQ), Hüttenhain heading it until his retirement in 1970.

Thus Dr. Hüttenhain, who started out as a mathematical astronomer, interested in orbits and Mayan astronomical texts, ended up having a 33-year career in German signals intelligence, beginning before the war and—except for a brief period when he was detained by TICOM—apparently seamlessly continuing on in it for another quarter of a century thereafter. Comparatively little is known about this important figure; some of the most impor-

[10]The Germans identified French systems, codes and ciphers, with the country letter F and a running number. The F110 was a four-digit re-enciphered army field code with an eleven digit repeating additive and indicator 55555; see I-176, p. 2.

tant sources are his detailed TICOM interrogation I-31, a paper by Bauer (2008, based on an unpublished manuscript by Hüttenhain), many references throughout TICOM documents (including a glowing evaluation by Fenner in DF-187E), and the occasional mention in historical papers (such as van der Meulen, 1996).

TICOM tells us "Hüttenhain evidently used his acquaintance with German mathematical circles to advantage. He introduced into the organization"

- Ernst Witt
- Werner Weber
- Wolfgang Franz
- Georg Aumann
- Johann Friedrich Schultze
- Alexander Aigner

"These men remained with the organization until the end, and formed the backbone of its cryptanalytic work, both in attacks on enemy systems and in security scrutiny."

Several of these individuals are of considerable interest, in particular Franz and Witt.

2.2.1 Professor Wolfgang Franz (1905–1996)

Dr. Wolfgang Franz (October 4, 1905–April 26, 1996) received his Ph.D. in 1930 from the University of Halle-Wittenberg, under the direction of the famous algebraic number theorist Helmut Hasse. He joined OKW/Chi on July 17, 1940 and worked there throughout the war. He had no trouble returning to academia after the war ended, and in fact had a very distinguished career: he taught at the University of Frankfurt from 1946 to 1974, serving as its Rector 1964–1965 and Vice-Rector 1965–1967. The MGP (Mathematical Genealogy Project) lists him as having no fewer than 24 doctoral students and 246 "descendants" (that is, students, students of students, and so on). His best known student was Wolfang Haken, one of those responsible for the proof of the celebrated "four-color theorem" (the statement that, subject to certain conditions, only four colors are needed to color a map).

The capstone of Dr. Franz's career was his election as President of the DMV (the *Deutsche Mathematiker-Vereinigung*, or German Mathematical Society). *Reidemeister-Franz torsion* in algebraic topology is named after him. He thus had a long and successful career after the war and an important impact on post-war German mathematics; see generally Burde and Schwarz (1998).

What of his time in OKW/Chi? His main cryptologic success was the breaking of the US State Department M138A Strip Cipher. It is not our purpose here to discuss in detail specific technical achievements (and indeed in many cases even when we know of an exploit, all too often little or nothing is known of the specifics); but Dr. Franz was sufficiently good at what he did that by the end of the war he headed OKW/Chi's section devoted to the initial break into difficult systems.[11] Dr. Franz was interviewed by TICOM in 1946 and prepared a detailed memoir of his time in OKW/Chi (DF-176). His was a not entirely unfamiliar recruitment story:

> [A] friend and colleague who was working at the observatory at Babelsberg wrote me that a college friend of his, a certain Mr. Hüttenhain, who was working for an important office of the Armed Forces, needed mathematicians. Presumably the work would be half-way interesting, at least in comparison with other possibilities. Was I ready to accept the invitation from this source?
>
> [After I reported to the office Dr. Hüttenhain] revealed to me in a general way what the work was. Up to this moment I had never had anything to do with cryptographic affairs, and never even heard of such except in novels or newspaper articles and had no ideas on the subject.

Why did Dr. Hüttenhain recruit someone with no prior experience in or knowledge of cryptology? Presumably innate ability and promise played the major role here although—as discussed below—Hüttenhain appears to have had other motives as well.

[11] He also seems to have maintained an interest in cryptology. In 1988 he published an article in the *Sitzungsberichte* (Minutes), Volume XXIV, of the *Wissenschaftliche Gesellschaft an Der Johann Wolfgang Goethe Universität, Frankfurt am Main*, with the title: "Kryptologie, Konstruktion und Entzifferung von Geheimschrifte". This was later published as a small pamphlet. It was originally given as a talk on January 10, 1987 to the Gesellschaft.

2.2.2 Professor Ernst Witt (1911–1991)

Dr. Ernst Witt (June 26, 1911–July 3, 1991) received his Ph.D. in 1934 at Göttingen, studying under Emmy Noether, an important figure in the development of modern algebra in the twentieth century. He spent virtually his entire professional life at the University of Hamburg, teaching there from 1937 to 1979 (succeeding in 1939 to the chair of the great Emil Artin). The MGP lists him as having had 15 doctoral students and 179 descendants. *Witt vectors* in algebra are named after him. For further information about Witt, see the memoirs by his student Ina Kersten (1993 and 2000), and his *Collected Papers* (Kersten, 1998).

Our knowledge of Witt's work during the war is very limited, although it was certainly highly regarded: in his narrative for TICOM Dr. Franz reported

> The most successful work [in OKW/Chi] along with that on the Am10 [the M138A strip cipher] was that of Professor Witt, who very skillfully solved a cipher of the Polish Government-in-Exile in London. This was a large complicated grille which was laid over a large number sheet. Several such grilles were constructed and messages were read currently. Photographic aids were used in the process. [DF-176, p. 11]

This cipher was a Polish stencil subtractor system.[12] The attack used the *Wittskiste* ("Witt's box"), a device constructed by Witt for the purpose.[13] (Thus Witt appears, like Turing, to have combined great mathematical power with a practical bent for implementation.)

[12]For details of the German attack on this system and their successes against it, see EASI 2, p. 81, and EASI 3, pp. 57–58, citing TICOM I-31, pp. 20–21, I-118, pp. 8–9, and I-124, p. 3. For details of the related British stencil subtractor system, see Erskine and Freeman (2003, pp. 310–313).

[13]The formal name of the Wittskiste was the *Zahlenwurm-Reduzier-Gerät* (I-31, p. 4). Detailed technical information about the Wittskiste is given in the 1955 dissertation of Dipl. Ing. Willi Jensen, *Hilfsgeräte der Kryptographie* (Flensburg, Germany, 1955). For reasons that are unclear the thesis was never published. It was initially submitted to Professor Friedrich L. Bauer but he declined to review it because he did not feel competent to do so. Bauer however kept his copy of the manuscript and later donated it to the *Bayerische Staatsbibliothek*.

Jensen worked in OKW/Chi IVb, devoted to cryptanalytic machinery, and is mentioned several times in the TICOM documents.

Note: The Wittskiste is referred to in the TICOM documents as the "Witzkiste" (literally "Joke box"); see TICOM I-31. It is unclear whether this was merely an error in transcription or in fact the actual termed used, reflecting a taste for puns similar to that at Bletchley Park. The "Wittskiste" was the term a German mathematician remembered hearing many years later.

2.2.3 Dr. Werner Weber (1906–1975)

Not all of the mathematicians in OKW/Chi enjoyed a successful academic career after the war. This was notably the case for Dr. Werner Weber (January 3, 1906–February 2, 1975), who received his Ph.D. in 1930 at Göttingen, under Noether and Edmund Landau. After the Nazis came to power in 1933 Weber joined the NSDAP (the *Nationalsozialistische Deutsche Arbeiterpartei*, or National Socialist German Workers Party); that is, the Nazi Party. He played an active role in German university politics during the next several years, ensuring the dismissal of Jewish faculty and others deemed politically unreliable (despite the fact that both his advisors were Jewish and world-class mathematicians of the very first rank). Segal (2003) discusses Weber's activities at length. Weber taught at Göttingen, Heidelberg, and Berlin before the war, but due to his close affiliation with the Nazis was unable to teach at a German university after.

TICOM I-124 is a record of Weber's TICOM interrogation after the war. Weber states there that he was the second mathematician hired by Hüttenhain (after Franz). He is credited with some cryptologic successes, including reading Japanese and Polish diplomatic traffic.

2.2.4 Professor Georg Aumann (1906–1980)

Dr. Georg Aumann (November 11, 1906–August 4, 1980) received his Ph.D. in 1931 from the University of Munich; his two advisors were Heinrich Franz Friedrich Tietze and Constantin Carathéodory, both mathematicians of great distinction. In 1934–5 Aumann was a Fellow at the Institute for Advanced Studies in Princeton and then taught at the University of Frankfurt. He joined OKW/Chi on October 1, 1942 and was a member of Section IVc (initial breaking of more difficult systems; cryptanalytic theory).

Although a member of the NSDAP (Nazi Party), Aumann had a "non-Aryan" wife; this, together with a negative Party evaluation of "mangelnden Aktivismus" (insufficient activity), as well as "politischer Unzuverlässigkeit"

(political unreliability) by the Ministry of Education, created substantial problems for Aumann during the war. Despite this, he was dismissed from his position at the University of Frankfurt after the war due to his Party membership. Eventually, however, he was cleared and became successively Professor at the University of Wurzberg (1949), the University of Munich (1950–1960), and the Technical University of Munich (1961–1972). The MGP lists him as having 12 students and 1,217 descendants. His best known doctoral student (for us) was Friedrich L. Bauer (the author of *Decrypted Secrets*). In 1958 he was elected a Member of the Bavarian Academy of Sciences. For further information, see Haupt (1981) and Schwarz (2005, pp. 89–90).

Of the two remaining individuals on the list of Hüttenhain's initial hires there is less to be said. Professor Alexander Aigner (1909–1988) received his Ph.D. in 1936 from the University of Graz (advisor Karl Brauner). After the war he returned to Graz, teaching at the University of Graz from 1947 to 1979, and working in number theory (for example, he was the author of *Zahlentheorie*, Walter de Gruyter, 1974). For further information, see Halter-Koch (1999).

Almost nothing seems to be known about Dr. Johann Friedrich Schultze (October 3, 1911–?; Ph.D. Berlin, 1939; advisors Ludwig Bieberbach and Alfred Klose), other than that he "worked under Prof. Franz in OKW as an expert on the Hagelin" (GCCS, 1945b, Appendix 1). There are entries on him in the MGP and *Kurzbiographien*; the latter gives a few details about his prewar career.

2.3 Eventual subdivisions of OKW/Chi

Throughout the war OKW/Chi continued to grow. Here is its organization as of April, 1945 (partial breakdown, names in parentheses are heads of section):

- Chi I: Interception (Captain Grotz)
- Chi II: Development and allocation of German systems
  - Section IIb: Development of cryptographic systems (Fricke)
  - Section IIc: Agent codes and ciphers (Menzer)

- Chi III: Production and distribution of keys (Metzger)
- Chi IV: Analytical cryptanalysis (Hüttenhain)
  - Section IVa: Security testing (Stein)
  - Section IVb: Cryptanalytic machinery (Rotscheidt)
  - Section IVc: Initial breaking into difficult systems (Franz)
  - Section IVd: Training (Hüttenhain)

(There were three additional sections of less interest to us: Chi V, routine breaking and translation, headed by Viktor Wendland; Chi VI, monitoring of press, broadcasts, and commercial traffic, headed by Kaehler; and Chi VII, evaluation, headed by von Kalckstein. For further information regarding the organization of OKW/Chi, see DF-8, I-39, and I-150.)

OKW/Chi had thus evolved into an organization of considerable size, and mathematicians beyond the initial six were eventually hired.

2.4 Later mathematicians in OKW/Chi

OKW/Chi continued to acquire mathematicians after the core group of six. The best known of these later hires was Oswald Teichmüller (1913-1943, Ph.D. Göttingen, 1935, advisor Helmut Hasse). Of all the mathematicians whose name will come up in our study, Teichmüller's is the most famous, the one name every research mathematician would immediately recognize. (Which others they might recognize would depend on their research specialization.) But Teichmüller spent only a short time in OKW/Chi, and it is unclear whether he ever achieved anything while there.[14] He had previously joined the army and insisted on rejoining his unit when conditions deteriorated in Russia. He was killed in fighting on the front shortly afterwards.

Security studies, as we have seen, were housed in *Referat* (Section) IVa. Notable members of this section included:

- Karl Stein (1913–2000); Ph.D. Münster, 1937 (advisor Heinrich Behnke; 28 students, 214 descendants)
- Gisbert Hasenjaeger (1919–2006); Ph.D. Münster, 1950 (advisor Heinrich Scholz; 11 students, 275 descendants)

[14] Weber (I-124, p. 3) says that in June-July 1941 the two had worked on "U. S. Diplomatic 5-letter traffic" but were unable to read it.

2.4.1 Professor Karl Stein (1913–2000)

Dr. Stein received his doctorate in 1937 from the University of Münster. He was responsible for investigating the security of the Lorenz *Schlüsselzusatz* SZ40 and SZ42, the online teleprinter systems codenamed "Tunny" by the British. His coming to OKW/Chi was a stroke of good luck:

> At a certain point he was sent to the eastern front. Luckily, however, the authorities were informed of his mathematical abilities, and he was called back to Berlin to work until the end of the war in some form of cryptology. Stein told me he was not very good at this. [Huckleberry, 2008, p.1]

Stein had a very distinguished career after the war. First Lecturer and later Associate Professor at Münster from 1946 to 1955, he then moved to Munich where he was Professor from 1955 to 1981. In 1966 he became President of the DMV (the year before Franz). He left a large footprint in the field of complex analysis, and is known today for *Stein manifolds* and the *Remmert-Stein theorem*. For further information, see Forster (2000), Huckleberry (2010).

2.4.2 Professor Gisbert Hasenjaeger (1919–2006)

Hasenjaeger joined OKW/Chi not only before receiving his doctorate, but even before attending university. After graduating from high school (the *Reformgymnasium* in Mülheim an der Ruhr) in 1937, he was immediately drafted into the military, and later seriously injured during fighting on the Eastern Front in January 1942. During his recovery the mathematical logician Heinrich Scholz (with whom he had been in contact since his last year in high school) arranged for him to join OKW/Chi, where he served in Referat IVa, assigned to review the security of the (Army) Enigma. By his own admission, he missed one of the major insecurities in the device (Schmeh, 2009).

Hasenjaeger enjoyed a very successful career in mathematical logic after the war, closely linked to that of his mentor (and wartime savior) Scholz. Managing to evade TICOM, he studied at Münster, receiving his doctorate in 1950 under the supervision of Scholz and later (1961) published a textbook on logic with Scholz as co-author. He left Münster for Bonn in 1962 as a Professor (until his retirement in 1984), and visited the Institute for

Advanced Study in Princeton in 1964–65. References include Diller (2000), Schmeh (2009).

2.5 Motivations, cryptologic and otherwise

What were Hüttenhain's motivations in recruitment? Friedrich L. Bauer (2008, p. 251) quotes Otto Leiberich as saying:

> Hüttenhain hatte sich zum Ziel gesetzt, wichtige Mathematiker vor dem Einsatz an der Front zu bewahren, darunter Franz, Witt, Hasenjäger. Stein wurde 1942 von der Front weg berufen.

("Hüttenhain had set himself the goal of saving important mathematicians before they had been sent off to the front, including Franz, Witt, and Hasenjaeger. Stein was brought back from the front in 1942.") Inasmuch as Leiberich was Hüttenhain's successor as head of the *Zentralstelle für Chiffrierwesen*, his testimony must be regarded as having considerable weight; see also his comments in Leiberich (1999).

So Hüttenhain had a motive other than just cryptologic ability. Viewed in this light, his hiring of Franz in 1940 makes much more sense – although Franz had zero knowledge of cryptology he was a mathematician of very considerable talent. (It might be suggested that Hüttenhain's actions here were no more different than policies that the British and Americans implemented during the war as well. But those were national policies, as opposed to the personal agenda of an individual.)

3 Signals Intelligence in the German Army

As we have seen, the Army lost control of its Cipher Bureau when the Abwehr was transferred to the Ministry of Defence in 1928. As a result, in 1933 the Army set up the *Horchleitstelle* (HLS), or Intercept Control Center, as its own independent cryptologic organization, housed in *Inspektion 7*, some of its personnel taken from the Cipher Bureau. The HLS had only a small staff, overseeing a number of intercept stations tasked with monitoring the military traffic of adjoining states (I-78, p. 2). It became part of OKH, the *Oberkommando des Heeres* (Army High Command), when the OKH was created in 1935. But it remained small: by 1939 the HLS still had only five men available for analyzing British traffic, the fixed intercept stations were

assigned only six cryptanalysts, the mobile intercept companies none (Praun, 1950, p. 220).[15]

After the outbreak of war – and especially in 1941 when it became clear the war would not be a short one – several expansions and reorganizations of basic functions in overall German Army signals capabilities took place; these changes included both cryptanalysis and communications security. In particular, the Army established two important units:

- 1939: *Inspektion 7 Gruppe IV* (In 7/IV), for signals security (composed of "mathematicians and former actuaries")
- 1941: *Inspektion 7 Gruppe VI* (In 7/VI), a central cryptanalytic agency located in Berlin.

3.1 In 7/IV and In 7/VI

In the Fall of 1939 the German Army set up In 7/IV, an organization responsible for the security of the German Army's communication systems. It eventually "had about a dozen mathematicians ... Most of these were drawn from the statistical offices of insurance companies" (I-92, p. 6). Its initial members included Dr. Carl Boehm, Dr. Hans Pietsch, and Friedrich (Fritz) Steinberg.[16]

Boehm, Pietsch, and Steinberg immediately demonstrated their value. After the defeat of Poland, the Germans found evidence the Poles might have been reading Enigma messages. An investigation into this was then launched, termed "Der Fall Wicher"; see generally Meyer (1975). As a result the new In 7/IV was asked to investigate the security of the Enigma. Although Boehm,

[15]This had consequences. In November 1939, when Hüttenhain returned to Berlin from Frankfurt after leading the successful effort by OKW/Chi to break a French Army code (mentioned earlier), the head of the project on the Army side told him that "in his opinion such a large decyphering task could not be done [by] OKH either now or in the future" (D-60, p. 5).

[16]Both Boehm and Steinberg joined In 7/IV on October 21, 1939; Pietsch a month later on November 22. Boehm received his Ph.D. from Berlin in 1936 on a topic in economics, advisor unknown. He is listed in the MGP but not the *Kurzbiographien*. A personnel list for In 7/VI (which he later moved to) lists him as having been an *Abteilungsleiter* (Section Leader) of the *Viktoria Versicherungsgesellschaft* (a life insurance company). Dr. Pietsch will be discussed below. Steinberg apparently did not have a doctoral degree. He was an insurance mathematician who worked for the *Allianz Versicherungsgesellschaft* before the war.

Pietsch, and Steinberg had apparently no prior experience in cryptology, they soon detected what the Polish mathematician Marian Rejewski had also noticed eight years earlier: the double-encryption of the message setting was a serious (and exploitable) insecurity in the use of the machine. As a result of their investigation and based on "the theoretical work alone, In 7/IV was able to force a change in the indicator system" (I-92, p. 5). From now on the message setting was encrypted just once; see Erskine and Bloch (1986).[17]

Pietsch and Steinberg were both assigned to Referat 4 of In 7/IV, with Steinberg serving as its leader and Pietsch as his deputy. This section, radio communications, dealt with production and distribution of German army codes and ciphers, as well as having a small cryptanalytical group tasked with investigating the security of of those codes and ciphers. It was also responsible for the monitoring and control of the German Army's radio and cipher communications.

In contrast, the cryptanalysis of military traffic was initially handled by five mobile Signal Intelligence Regiments (the *Kommandeur der Nachrichten Aufklärung*, or "KONA"), as well as the Horchleitstelle in Berlin. But by 1941 the limited resources of the Horchleitstelle were found to be inadequate to handle the ever-increasing volume of traffic, and so it was replaced by two new agencies: In 7/VI, a central cryptanalytic agency located in Berlin, and the LNA (the *Leitstelle der Nachrichten Aufklärung*, or Central Control Station for Signal Intelligence), a central evaluation agency housed in Zossen (about twenty miles south of Berlin). In 7/VI became operational in January 1941. The new cryptanalytical group took over the work of Referat 4 of In 7/IV, as well as the codebreaking work done by the Horchleitstelle. Initially Group VI had nine sections, its staff drawn from those of the Horchleitstelle (95 persons), and In 7/IV (22 persons). Referat 1 was the general cryptanalytical mathematics section, led by Steinberg with Dr. Pietsch as his deputy; Referat 7 dealt with the security of German ciphers, and was initially led by Dr. Boehm, with Dr. Pietsch again as deputy. (For reasons that are unclear, Dr. Boehm left In 7/VI soon after, in April 1941, and was replaced by Pietsch.) Referats 2-6 dealt respectively with English, French, Italian, Russian, and Balkan traffic.

[17]It is a measure of the disfunctional nature of German cipher security that in other branches of the German military the double encipherment of the message setting was still sometimes employed: the *Luftwaffe* used it for its "Yellow" cipher throughout the Norwegian campaign (which ended in June 1940), and the Navy used it in several cases until mid-1944. For the case of the Yellow cipher, see GCCS (1945a, pp. 58–59).

Reorganization(s) strike The subsequent organizational fortunes of In 7/VI were complex to say the least. Some its initial staff were drawn from In 7/IV. But in late 1941 staff from both In 7/VI and the LNA were transferred to a new organization, the *Horchleitstelle Ost* (HLS Ost), located in Lötzen, East Prussia, (today the Polish city of Giżycko), tasked with the cryptanalysis and evaluation of Russian traffic. The responsibilities of In 7/VI were subsequently increased, however, when in 1942 the task of testing the security of German methods of encryption was transferred to it from In 7/IV, with In 7/IV restricted to the development, production, and distribution of new systems. Further reorganization then followed: in the Fall of 1943, In 7/VI was transferred to the new Department of Signals (*Amtsgruppe Nachrichten*, AgN) housed in the General Army Office (*Allgemeines Heeres Amt*, AHA), and given the new name of Signals Intelligence (*Nachrichten Aufklärung*, NA). So now its designation was the impressive OKH/AHA/AgN/NA, but its mission statement and tasks remained essentially unchanged.[18] Finally, in October of 1944 (in the aftermath of the attempted assassination of Hitler) a much more substantial reorganization took place: the NA, LNA, and HLS Ost were merged into a single entity, the GdNA (*General der Nachrichten Aufklärung*), the Signal intelligence Agency of the Army High Command (thus OKH/GdNA). But at the same time all responsibility for development and testing was transferred to OKW/Chi, together with the appropriate personnel. Arguably the Wehrmacht had finally gotten it right—in October 1944.

Despite the above, as a cryptanalytic organization In 7/VI remained a relatively stable entity until at least late 1944. Perhaps for this reason it is sometimes referred to as OKH/Chi, capturing the essentially common entity denoted at various times as In 7/VI, NA, and the GdNA.

3.2 The mathematicians of OKH

The result of all this was that ultimately a substantial number of mathematicians were working for the Army. Here is a partial list of the most important:

- Dr. Willi Rinow, Ph.D. Berlin, 1932
- Dr. Max Wernick, Ph.D. Berlin, 1934

[18] Dr. Buggisch (I-58, p. 3) refers to this change as a "renaming" of In 7/VI.

- Dr. Herbert von Denffer, Ph.D. Berlin, 1935
- Dr. Rudolf Kochendörffer, Ph.D. Berlin, 1937
- Dr. Werner Schulz, Ph.D. Berlin, 1937
- Dr. Hans-Peter Luzius, Ph.D. Berlin, 1938
- Dr. Hans Pietsch, Ph.D. Berlin, 1938
- Dr. Walter Fricke, Ph.D. Berlin, 1940
- Dr. Wilhelm Vauck, Ph.D. Dresden, 1924
- Dr. Alfred Kneschke, Ph.D. Dresden, 1927
- Dr. Günther Wünsche, Ph.D. Dresden, 1933
- Dr. Heinrich Döring, Ph.D. Göttingen, 1939
- Dr. Otto Buggisch, Ph.D. Darmstadt, 1938
- Dr. Horst Schubert, Ph.D. Heidelberg, 1949

Note that in this list alone there are eight individuals with a Ph.D. from Berlin, three from Dresden, and one each from Göttingen and Darmstadt; there was no lack of talent. These individuals were housed in the Mathematical Research Section of In 7/VI, headed by Dr. Hans Pietsch, who, according to *Oberstleutnant* (Lieutenant colonel) Mettig, the head of In 7/VI from November 1941 to June 1943 (and therefore certainly in a position to know), "collected together in this section the best available mathematical brains" (I-78, p. 6). Dr. Pietsch is discussed further below.

At one point there were separate subsections in the Mathematical Referat devoted to:

- research (von Denffer; Hilburg, Rinow, Wünsche)
- security of hand systems (Lüders)
- security of machine systems (Döring; Buggisch)

The research subsection "appears to have done some excellent work in the solution of the more simple machine systems used by foreign countries" (EASI 4, p. 181). Its accomplishments included:

- Reading US Converter M-209 traffic given suitable messages in depth.
- Reading de Gaulle traffic enciphered by the Hagelin C-36.
- Theoretical solution of the French Hagelin B-211 (and old traffic).
- Theoretical solution of the Russian K-37 (a version of the B-211).
- An attack on the Swedish Hagelin SM-1 via depths.[19]

Among the mathematicians of OKH listed above, several deserve special mention.

3.2.1 Dr. Hans Pietsch (1907–1967)

Dr. Hans Karl Georg Heinrich Pietsch (November 22, 1907–October 14, 1967) received his doctorate from the University of Berlin in 1938, his thesis advisor the famous mathematician Ludwig Bieberbach. Beginning in 1930 Dr. Pietsch had worked for the *Jahrbuch über die Fortschritte der Mathematik*, a mathematical review journal.

The limited evidence available suggests Pietsch was quite good in his wartime cryptographic work: Dr. Buggisch (in I-64, p. 3) describes Pietsch as the "best man" on (at least some) Russian systems; Boezel (TICOM IF-5, p. 6) included him as being "[a]mong the German 'ace' cryptographers". As noted earlier, along with Boehm and Steinberg he recognized the insecurity in the double-encipherment of the Enigma message setting, resulting in its abandonment on May 1, 1940 (I-92, p. 5). He eventually became head of the Mathematical Research Section of In 7/VI. (Recall he was said to have collected "the best available mathematical brains" for this section. His decade-long work for the *Jahrbuch* before the war would have served him well here, giving him a broad sense of German mathematics and mathematicians.) Dr. Pietsch also played an important role in the later investigations into the "Fall Wicher" (recall this was the German investigation into the possibility that the Poles had been able to read Enigma messages); see I-176, pp. 11–12. Although he was held in custody at the Civilian Internment Camp No. 6 at

[19]The SM-1 was not a Hagelin machine model per se but a system name adopted by the Germans similar to their name AM-1 for the M-209. The Swedish SM-1 was based on the Hagelin C-38 but used 29 bars instead of the standard 27.

Moosburg until June 1946, Dr. Pietsch was unfortunately never interrogated about his wartime work (see I-204, pp. 2, 4).[20]

After the war Dr. Pietsch returned to editorial work, working for the (East) German Academy of Sciences and the *Zentralblatt für Mathematik*, another mathematical review journal, from 1946 until his death in 1967. (The *Jahrbuch, Zentralblatt*, and German Academy of Sciences are discussed further in Subsection 12.1 below.) Dr. Pietsch is listed in both the MGP and the *Kurzbiographien*, but there seems little other readily available information about him. He never married and had no children (or at least he did not report any on a post-war employment form). The end apparently came quite suddenly on October 14, 1967. He was last seen alive at around noon that day but was declared dead on arrival at the Berlin-Wilmersdorf city hospital at 15:25. (The source for the date of his death is the *Landesarchiv Berlin*, for the dates of his employ by the Academy, the Academy records.)

3.2.2 Professor Walter Fricke (1915–1988)

Dr. Walter Ernst Fricke (April 1, 1915–March 21, 1988) is a case-study of the apolitical scientist caught up in the winds of war. He came of humble beginnings: his father was a carpenter and miner, but this did not prevent Fricke's talent being recognized early on. After receiving his *Abitur* (high school diploma) in 1934 from the *Stephaneum*, a *Gymnasium* in Aschersleben, Fricke studied astronomy, mathematics, and physics at the University of Berlin, publishing his first paper in astronomy (about the distribution of spiral nebulae) at the age of 22, in 1937. Through the assistance of the noted British astronomer George Cunliffe McVittie he received a scholarship to study at the University of Edinburgh starting October 1, 1939. But the war of course intervened.[21]

Fricke received his Ph.D. in 1940 from the University of Berlin on the dynamics of stellar systems (under the direction in part of Professor Otto Heckmann, the Director of the Göttingen Observatory). Fricke then began work at the Hamburg Observatory on May 1, 1940, but was drafted

[20]Moosburg was previously the prisoner of war camp Stalag VII A. Another prisoner kept at Moosburg was Dr. Stein, who was also not interrogated about his work (at OKW/Chi).

[21] Ironically, Dr. McVittie himself became an important cryptanalyst at Bletchley Park. He was an Air Ministry civilian who worked at BP from November 1939 until 1945 in the Air Section of Hut 10. He was the Head of the Meteorological Subsection and BP's specialist on meteorological ciphers.

into the *Nachrichtentruppe* (Army Signal Corps) later that year and subsequently posted to In 7/VI on May 15, 1941. At that time, by his own statement, "he knew nothing of cryptography" (I-20, p. 2). Despite this, he soon became adept in this strange new world. During his first year he worked on solving German systems, then switched over to developing new ones: first a *Schlüsseltafel* (an enciphering table for a three-letter field code), then a *Rasterschlüssel* (transposition based grille); see I-20, p. 3 and, for the *Rasterschlüssel*, Cowan (2004). On November 1, 1944, Fricke was transferred to OKW/Chi (as part of the shakeup that occurred after the July 20th plot), where he was put in charge of Referat IIb, the desk responsible for the development of German code and cipher systems as well as giving advice on the production of keys and supervising their production.

In his TICOM interrogation Fricke demonstrated that despite his largely theoretical background he understood the practical aspects of cryptology: the drawbacks, for example, to not being provided real traffic to review for secure usage (I-20, p. 3); or in using weak weather ciphers (p. 7, "an enemy might think these messages unimportant, but in fact they were extremely valuable and could even be used by enemy bombers for calculating the trajectory of their bombs"). He also displayed an openness sometimes bordering on the naive: when discussing rasters, he asked his interrogators (apparently as a matter of scientific curiousity) if they had ever solved them (the interrogators of course declined to comment); and at the end of the first session he closed by saying

> he hoped he would be allowed to return to Hamburg observatory where he could on[c]e more engage in useful work. He has a job open to him there. [I-20, p. 6]

His wish was granted, but not immediately: he was flown to the UK together with Hüttenhain and questioned extensively about German cryptologic efforts during the war; the two were the subject of several TICOM reports: I-21, 36, 45, 77, 79, 118. But Fricke was eventually released, returning to astronomy and what was to be a very distinguished career: the Director of the *Astronomisches Rechen-Institut* (Astronomical Calculation Institute) in Heidelberg from 1955 to 1985, as well as Professor at the University of Heidelberg from 1958; see Westerhout (1985), Wielen and Lederle (1990), Treder (2008). His *Schriften und Vorträge zur Astronomie und Astrophysik : 1937–1985* (Fricke, 1985), published the year of his death, was

a 1,230-page long collection of papers and lectures written by him over a half-century of activity.

We will return to Dr. Fricke at the end of this paper; as will be seen, he was all too aware of the weaknesses in German encryption methods.

3.2.3 Professor Willi Rinow (1907–1979)

Dr. Willi Ludwig August Rinow (February 28, 1907–March 29, 1979) received his Ph.D. in 1932 from the University of Berlin; his advisor was Heinz Hopf. The MGP lists him as having had 16 students and 152 descendants. He is noted for the *Hopf-Rinow theorem* (an important result in differential geometry), and became President of the DMV in 1959. (Thus no fewer than three of the mathematicians involved in cryptologic work during the war ultimately went on to be Presidents of the German Mathematical Society.) During the war he worked on breaking the English Typex machine.[22]

But the arc of Rinow's career was not a simple one. In 1937 he had joined the NSDAP, and from 1937 to 1940 was a member of the editorial board of the notorious journal *Deutsche Mathematik*.[23] Thus he had clear ties to the Nazis, although certainly not as close as those of Werner Weber, for his academic career did not end with the war. The Wikipedia tells us:

> In 1937, he became a professor in Berlin and lectured there until 1950. His lecturing was interrupted because of his work as a mathematician at the *Oberspreewerk* in Berlin (a producer of radio and telecommunications technology) from 1946 to 1949. In 1950, he became a professor at the University of Greifswald. He retired in 1972.[24]

[22]This work was done in collaboration with Pietsch, Steinberg, and Dr. Werner Schulz, but was abandoned when it was concluded that no attack on the machine was possible without a knowledge of the wheel wirings. Nevertheless, Rinow made a valuable theoretical contribution to this effort: the entry in the In 7/VI *Kriegstagebuch* for September 1941 recorded that "Lance Corporal Dr. Rinow delivered a thorough theoretical probability analysis of a general problem that plays a big role in the deciphering work, which led to a satisfactory formula centric result and which computational evaluation led to remarkable numerical values about which the practical estimates had supplied no reliable indication".

[23]Founded in 1936, *Deutsche Mathematik* had a largely Nazi editorial board and, besides pure mathematics, initially published Nazi propaganda pieces on a purported relationship between mathematics and race, promoting what was termed "German mathematics" and seeking to eliminate supposedly alien Jewish influences from it.

[24]`https://en.wikipedia.org/wiki/Willi_Rinow` (accessed February 10, 2019).

What was a pure mathematician of Rinow's ability and distinction doing working for a technology company from 1946 to 1949? In 1946 he had been dismissed from his academic position because he had been a member of the NSDAP, but later on, both in the West and the East (where Rinow was), this ceased to matter. For further information on Rinow, see the contributions to his "Ehrenkolloquium" (University of Greifswald, 2007) and the entry on him in the *Kurzbiographien*.

3.2.4 Professor Horst Schubert (1919–2001)

Oberleutnant (later Dr.) Horst Schubert (June 11, 1919–2001) illustrates a very different way a German mathematician might become a cryptanalyst during the war. Schubert was an undergraduate student of mathematics at the University of Frankfurt when called up for military service in 1937. He went directly into signals intelligence as an intercept and direction finding operator, serving in this capacity until the end of the French campaign. At the beginning of 1941 he was assigned to a signals school, became an officer, and was posted to Frankfurt, where he served as an instructor and adjutant, but also given leave to study during the winter of 1941. After his studies he was posted to OKH to take a course in cryptanalysis, and from that point on worked as a cryptanalyst specializing in Soviet hand systems. He joined KONA 6, taking part in the campaign in the Caucasus (which began in July 1942), working first on Russian Army ciphers until March 1943, and after this Russian partisan traffic until September 1943, when KONA 6 was dissolved. He was then posted to the GdNA and put in charge of the NKVD and partisan branches of *Ostentzifferung* (Eastern Cryptanalysis) OKH. In what was perhaps a symptom of the strained resources of German military cryptanalysis at the end of the war, at the beginning of 1945 Schubert was also tasked with reviewing a number of British and American cryptosystems, as well as being posted to the Navy at the end of February to study Naval ciphers. At the very end of the war (sometime after March 16, 1945) he was supposed to be part of a small group of cryptanalysts sent to Japan by submarine to work with Japanese counterparts, but this never took place (see EASI 4, p. 314, I-48, p. 3, and IF-108, p. 12).

While in Frankfurt during the war, Schubert was able to study under the mathematician William Threlfall (1888–1949), and after the war ended followed Threlfall to Heidelberg, where he received a Ph.D. in 1949 under the direction of Threlfall's close collaborator Herbert Siefert (1907–1996);

see Epple (1999, p. 332).[25] Schubert then had a very successful career as a mathematician, carving out a niche for himself in the area of knot theory, at that time a neglected subject in Germany; see Epple (1999, pp. 332–335). Schubert remained at Heidelberg until he moved to Kiel in 1959, first as Associate (*außerordentlicher*) and later (1962) Full (*ordentlicher*) Professor. In 1969 he moved to Düsseldorf, where he remained until his retirement in 1984. He wrote well-regarded books on topology (1968) and category theory (1972), and had in all 18 doctoral students and 82 descendants.

Schubert was thus both an important German cryptologist during the war (I-15, I-26, and I-60 are all TICOM interviews of him, he is mentioned in I-21 and I-78, and is cited 19 times in EASI 4), and an accomplished mathematician after. And yet it would be difficult to link the cryptanalyst of the TICOM reports with the distinguished post-war mathematician, were it not for the chance remark at the beginning of I-15 that Schubert's pre-war employment was as a "Student of mathematics at Frankfurt am Main University" (I-15, p. 1).

3.3 Some non-academic mathematicians

Not all the mathematicians in In 7/VI went on to careers in academia, but that does not mean they were not highly successful during the war as cryptanalysts. Our next several examples illustrate this.

3.3.1 Dr. Heinrich Döring (1913–?)

One of the In 7/VI mathematicians, Heinrich Döring, is of particular interest.[26] One postwar report says of Döring: "All [prisoners of war] stress his excellent work. An inspired cryptographer" (GCCS, 1945b, Appendix 2). Dr. Otto Buggisch, who worked directly under Döring, was described by his interrogator, Major William Bundy (who later in life served as a foreign affairs advisor to Presidents Kennedy and Johnson), as having "a good memory for names and is familiar with a wide variety of sections and

[25] Siefert and Threlfall are well known in the topological literature in part because of their book *Lehrbuch der Topologie* (Seifert and Threlfall, 1934), still available in both the German original and an English translation.

[26] The TICOM documents (as is often the case) only report Döring's last name, but a promotion list in the war diary for In 7/VI gives his first name as "Heinrich".

the specialists in them" (I-58, p. 9). So Buggisch was in a good position to make comparisons. Bundy reported:

> The one name for which he adds conspicuous lustre is that of Wachtmeister Döring.[27] (Incidentally both Hentze and Karrenberg concur in B's estimate.) Döring did many original studies and solutions, and B. rates him .. frankly above himself.

Buggisch went on to describe some of Döring's successes. One of these was the solution of a Hungarian raster cipher, which Buggisch termed "brilliant" (p. 7) and "one of the achievements of this section" (p. 9). On the security side, Döring demonstrated in the summer of 1942 that the Siemens T52 A/B (an online enciphered teleprinter) "could be easily cracked" due to operators sending messages in depth; and the T52 C (a supposedly improved version) was not much better, being breakable on a text of 1000 letters (I-58, p. 6). This led to the development of the T52 D but, in a comedy of errors, in 1943 Döring was able to show that this too was insecure, leading to the development of the T52 E (see I-78, pp. 11-12, which briefly describes the nature of Döring's attack).[28] These concerns were not merely theoretical in nature: after the conquest of Norway in April 1940, the Germans used lines running from Norway to Sweden over which T52 A/B (and later T52 C) traffic was sent. The FRA (Swedish Signals Intelligence), proceeded to tap these lines and, thanks to the efforts of the brilliant Swedish mathematician Arne Beurling, were able to read T52 traffic for several years; see generally Beckman (2002), McKay and Beckman (2003).

Tobies's *Kurzbiographien* gives brief details of Döring's life before the war: the son of a roofer, he studied at Göttingen from 1934 to 1939, receiving his doctorate in 1939 under the supervision of Edwin Lauprecht and Hans Georg Münzner (the subject of his thesis a topic in animal husbandry,

[27] In WWII the German *Wachtmeister* was an NCO rank roughly equivalent to that of a Technical or Staff Sergeant in the current US Army, or NATO rank OR-5.

[28] The full name of the T52 was the Siemens & Halske *Schlüsselfernschreibmaschine* (SFM) T52. The machine was developed by Siemens in the early 1930s, the design based on several German patents issued to Siemens in July 1930. It is probably best described as a Wehrmacht teleprinter cipher machine, even though it was developed by the Army; the Army appears not to have been the main user of this machine, but rather preferred the one they developed themselves, the Lorenz SZ40/42. The primary customers for the Siemens T52 machines were the Air Force, Navy, and Wehrmacht command networks, the Foreign Office, and various Nazi authorities. See Weierud (2005).

"Theoretical and empirical investigations of the errors occurring in milk performance tests").[29] Presumably drafted into the Army, Döring first appears on a personnel list of In 7/VI as a *Gefreiter* (Lance Corporal) promoted to the rank of *Unteroffizier* (Corporal) on May 1, 1941; he was later promoted at some point to Wachtmeister. (The *Kurzbiographien* says of this period only "Kriegsdienst", that is, war service.) After the war Döring joined in 1947 the Max-Planck Institute for Animal Breeding and Animal Nutrition (then the *Max-Planck-Institut für Tierzucht und Tierernährung*, presently the *Institut für Nutztiergenetik des Friedrich-Löffler-Institut*) in Mariensee. Over the next decade he wrote at least ten papers with his former advisor Lauprecht that appeared in the animal husbandry literature. This series of papers appears to have ended in 1959 and Döring did not contribute to the 1962 *Festschrift* marking the 65th birthday of his mentor and collaborator Lauprecht, so he may have died around this time.

3.3.2 Dr. Hans-Peter Luzius (February 29, 1912–?)

Dr. Hans-Peter Luzius received his doctorate in 1938 from the University of Berlin, advisor Paul Riebesell, his dissertation on actuarial mathematics. Earlier, after a visit to England in 1933, he moved to the US and began to work for the Alliance Insurance Company, continuing there until the outbreak of war, when he returned to Germany. He "was called up into the Army in 1941 . . . [and] posted almost immediately to OKH" (I-211, p. 1); he became a member of Referat 7 (security of German hand systems) of In 7/VI on February 3, 1941. At the end of the war he moved to Flensburg, where he lived until at least 1949. He was later active in the German Actuarial Association, and between 1956 and 1964 wrote several papers that appeared in the actuarial literature. There are entries on him in the *Kurzbiographien* and the MGP.

TICOM managed to track him down in 1949, during a holiday visit to England. At the time he was employed as a translator ("he speaks almost perfect English, with a strong American accent") by the British element of the Control Commission for Germany (CCG/BE), and during his holiday in England was the guest of a CCG officer. He was interviewed in London at

[29] The identification of the cryptologist Heinrich Döring with the mathematician in the *Kurzbiographien* is based on the concordance between the information about Döring in a document in the UK National Archives, HW 80/49 (GCCS, 1945b), and that in the *Kurzbiographien*.

the War Office on May 11, 1949 (I-211).[30]

After Hitler declared war on the US on December 11, 1941, an American Referat was set up, its members drawn from the Mathematical Referat (I-78, p. 10). One device the US Army used was the Cylindrical Cipher Device M-94, a twenty-five disk device invented by Parker Hitt, which was first fielded in 1922. It was broken by Luzius and Steinberg in the summer of 1942 (EASI 4, p. 155); about 70-80% of the traffic could be read (I-113, p. 3).

The M-94 was superseded by the M-209 (a Hagelin device, the C38) in 1943, and was widely used by the US Army. Rinow, Luzius, and Steinberg were able to diagnose the structure of the machine prior to a copy of it being captured (IF-107, p. 7). In the summer of 1943 Luzius and Kochendörffer had the first recovery of key based on a crib (I-58, p. 3). The first break based on depths was achieved in Autumn 1943 by Luzius and Steinberg, and from that point on the machine was read regularly (10-20%) until the end of the war (EASI 4, p. 156). For details regarding the In 7/VI attack on the M-209, see DF-120, I-211, IF-107.

Thus Luzius was intimately involved in one of the most important operational achievements of In 7/VI. Döring and Luzius illustrate that a number of the "mathematicians" employed by the Army were mathematicians only in a sense much broader than that of the professional research mathematician.

3.3.3 The Referat Vauck

The *Funkwesen* (OKW/WNV/Fu) was the Department (*Abteilung*) of WNV having overall responsibility for the radio communications of OKW; the *Funküberwachung* (OKW/WNV/Fu III, the Radio Monitoring Service) was the section of the Funkwesen tasked with intercepting and locating via direction finding all illegal radio transmissions (e. g., that of enemy agents), both within the Reich proper and all territories occupied by it.[31] The liqui-

[30] Although willing to talk about his own work, Luzius clearly did not want to create problems for others. As his interrogator drily noted, "He remembered no details of the organization, nor could he recall the name of a single one of his colleagues!" (I-211, p. 1).

[31] There was another organization with similar responsibilities, the *Funkabwehrdienst*, a unit within the sinister *Ordnungspolizei* (Orpo), which was administratively part of the Ministry of the Interior but headed by SS officers. The situation might be viewed as analogous to that of the Abwehr and the *Sicherheitsdienst* (SD), the competing intelligence organizations of the Army and SS, respectively. The OKW's Funküberwachung and Orpo's Funkabwehrdienst did coordinate their efforts to a considerable extent, however, and were often collectively referred to as the *Funkabwehr*. The corresponding British organization

dation of enemy agent networks identified in this way could be carried out with deadly efficiency.[32]

German conquests in Europe after April 1940 put strains on the resources of Fu III, especially on the cryptanalytic side. Initially Fu III requested assistance from OKW/Chi, but after they were turned down on the grounds of insufficient manpower, they turned to In 7/VI. As a result a new Referat 12 was set up in the Summer of 1942, devoted to attacking enemy agent codes and ciphers.[33]

This coincided with the assignment of Dr. Wilhelm Vauck (June 8, 1896–December 8, 1958) to In 7/VI in 1942. Dr. Vauck (Ph.D. Technical University of Dresden, 1924; advisor Gerhard Kowalewski) may have worked in military intelligence during the First World War (the *Kurzbiographien* says only "Kriegsdienst, Nachrichtendienst" in 1916), and after receiving his Ph.D. taught at a secondary school (*Oberrealschule*) in Bautzen during the interwar period. He appears to have been drafted in 1942 and given the rank of Lieutenant.[34] He initially took a deciphering (Ez) course given by an Inspector Kühn from April 10 to June 6, 1942 in which "he proved to be a very able cryptographer" (I-115, p. 5).

Vauck's possible prior experience in military intelligence, officer status, seniority, and cryptographic ability all made him a natural choice to head the unit. He in fact proved to be an able leader and this, together with his personal cryptographic achievements led to good results on the part of the section (I-115, p. 4), which came to be known as the "Referat Vauck". Under Vauck the organization worked closely with Fu III, being located only three houses down from the evaluation center of Fu III in Berlin (1-115, p. 2). In early 1943 the anomaly of closely cooperating units housed separately in

---

was the RSS (Radio Security Service, eventually part of MI6).

[32]One of the best known of these operations was *Das Englandspiel* (The England Game) or *Unternehmen Nordpol* (Operation North Pole). The Abwehr had completely penetrated the SOE network in the Netherlands, and enemy agents were picked up as they parachuted into the country; see Giskes (1953), a first-hand account by Abwehr Major Hermann Giskes who led the operation. More than 50 agents were eventually arrested and most executed at Mauthausen September 6–7, 1944. Warnings by Leo Marx, an SOE cryptographer, that there were clear signs the operation had been compromised were ignored (Marx, 1998).

[33]Referat 12 became operational in August 1942, its first report covering the period August 1–31, 1942. From March 1, 1942 to July 31, 1942 agent systems (*Agentenverfahren*) were handled by Referats 1 and 7.

[34]Vauck is listed on a May 1, 1942 personnel list as Olt. (*Oberleutnant*, First Lieutenant). He was transferred to In 7/VI on June 15, 1942.

OKH and OKW was eliminated when the Referat Vauck was transferred to OKW/Chi. This was, however, essentially just a change in the organization chart, and when the Funkabwehr moved to Dorf Zinna (two miles northwest of Jüterbog) in the Fall of 1943, the Referat Vauck moved with it. Vauck developed good working relationships with both the Gestapo and Abwehr, and after a while members of the section were sometimes represented during the arrest and questioning of agents.

The TICOM report I-115 gives a broad overview of the activities of the Referat. The territories it covered included France, Spain, Belgium, the Netherlands, Poland, Czechoslovakia, Russia, the Balkans, and Germany itself. Not surprisingly it grew over time, from an initial staff of 26 in the Spring of 1942 to 40 in 1943. Dr. Vauck thus headed a unit of substantial size with a significant number of successes. For further information about the Funkabwehr and the Referat Vauck, see EASI (Volume 8, Chapter 7), IF-176, the post-war report of the UK Radio Security Service (RSS, 1946), and CSDIC/CMF/SD 80 (CSDIC, 1945).[35] Regarding Vauck's wartime work, the Technical University of Dresden online distinguished alumni page says

> Ab 1940 leistete er Kriegsdienst als Leiter einer Entschlüssel–ungsgruppe. Dass er damit auch zum Aufdecken einer antifaschistischen Widerstandsgruppe beigetragen hat, belastete ihn tief bis an sein Lebensende.[36]

Translated, this reads: "From 1940 he performed his military service as the head of a decryption group. That as a result he contributed to uncovering an anti-fascist resistance group, deeply troubled him until his death". This is to put the matter in very muted terms. Dr. Vauck played an important role in the liquidation of the Schulze-Boysen/Harnack portion of the "Red Orchestra" Soviet spy ring (the part, that is, located in Berlin); see Tarrant (1995, pp. 52-60). Not surprisingly, many books have been written on the Red Orchestra; pertinent references include Perrault (1967), Trepper (1983), Tarrant (1995), Brysac (2002), and Nelson (2009).

After the war Vauck eventually ended up as a Lecturer at an Engineering College (*Ingenieurschule*) in Bautzen. Despite efforts to locate him, he was never interrogated by TICOM.

[35] CSDIC was the "Combined Services Detailed Interrogation Centre", a set of facilities run by the British War Office (specifically MI19) between 1940 and 1948.

[36] `https://tu-dresden.de/ua/dokumentationen/alumni/das-alumni-projekt-des-universitaetsarchivs-der-tu` (accessed December 30, 2018).

3.4 Statisticians and actuaries

The mix of mathematicians in OKW and OKH was quite different, as was apparently often their mode of recruitment. In OKW/Chi, Dr. Hüttenhain was able to attract pure research mathematicians of outstanding ability, and these were sometimes invited to join the organization (as in the case of Franz), or pulled from the front (as in the case of Stein and Teichmüller), or had been convalescing in a hospital (as in the case of Hasenjaeger). OKH, on the other hand, appears to have relied primarily on the power of the draft, and many – if not most – of the mathematicians of In 7/IV and In 7/VI did not come from universities, but were drawn instead from the life insurance sector or were high school teachers. The statisticians and actuaries included Drs. Wolf-Günter Ackermann, Carl Boehm, Herbert von Denffer, Georg Heubeck, Hans-Peter Luzius, Hans Thunsdorff, Alfred Tröbliger, and Günther Wünsche; those without doctoral degrees included Fritz Hilburg, Johannes Anton Marquart, Edgar Panzer, and Friedrich Steinberg.

Many of these people went on to highly successful careers in the life insurance industry after the war and contributed extensively to its literature. Dr. Georg Heubeck, for example, developed a widely used set of of mortality tables (the *Heubeck'sche Richttafeln*), was chairman of the ABA (the *Arbeitsgemeinschaft für betriebliche Altersversorgung*, the German professional association for occupational pensions) from 1969 to 1984, taught at the University of Cologne from 1973 to 1983, and wrote several books and many papers on pensions. Dr. Carl Boehm, another example, was the editor of the *Blätter der DGVFM* (the *Deutschen Gesellschaft für Versicherungs- und Finanzmathematik*, that is, the German Association for Insurance and Financial Mathematics) for 15 years, from 1954 to 1969 (volumes 2-8, see Kracke, 1969). Many of the former members of In 7/VI contributed to the *Blätter*: aside from numerous conference reports and book reviews, these include papers by Boehm (10), von Denffer (2), Heubeck (9), Luzius (3), Tröbliger (4), and Wünsche (4). One amusing case in point is the April 1964 issue of the *Blätter*: it contains two papers by Luzius, one each by Heubeck and Wünsche, and reviews by Boehm and Heubeck (as well as an announcement by F. L. Bauer). Despite this, it is unclear to what extent these individuals maintained contact after the war, but at a minimum some co-authored papers: the *Blätter der DGVFM* contains two papers by Boehm, one with Heubeck and one with Luzius.[37]

[37]Boehm died sometime before November 1986; see the comment in the *Journal of the*

4 Pers Z, the Foreign Office Cipher Bureau

Pers Z was the oldest of the six major German cryptologic organizations, having its origins in the First World War.

4.1 The origins and organization of Pers Z

During World War I the German Foreign Office (the *Auswärtiges Amt*, AA) had a unit charged with the production of its codes and ciphers (the best known instance of these being the enciphered codebook used to encrypt the Zimmermann telegram). In 1919 Curt Richard Selchow (May 28, 1886–December 15, 1967), a former signal officer in the Army, was put in charge of this unit and remained its head until the defeat of Germany in May 1945.[38]

Under Selchow the charge of the organization was substantially expanded to include the cryptanalysis of foreign diplomatic traffic. It was eventually called Pers Z (an abbreviation for the Z branch of the Personnel Department of the Foreign Office), and had four sections: Pers Z Gen (Administration), Pers Z F (Communications), Pers Z Chi (Cryptography), and Pers Z S (Cryptanalysis) or—for TICOM and us—Pers ZS.[39]

When Selchow moved to the Foreign Office in 1918 he also recruited six soldiers he had known during the war: Werner Kunze, Rudolf Schauffler, Adolf Paschke, Karl Zastrow, Wilhelm Brandes, and Ernst Hoffmann (I-208, pp. 1–2). Apart from Hoffmann (who began as a cryptanalyst but later headed Pers Z F), all of these held important positions in Pers ZS during the

Institute of Actuaries (1886-1994), Vol. 114, No. 1 (June 1987), pp. 15-19 at p. 18.

[38]Selchow was a *Hauptmann* (Captain) in the German Army who was assigned to the staff of the Chief of Communications for the *Großen Hauptquartier* (GrHQu, the Supreme Headquarters of the German Armed Forces) on August 1, 1917, and appointed the *Referent* (Section Head) for Interpretation and Encryption. He joined the AA on December 1, 1918, transferred to its Cipher Bureau (*Chiffrierbüro*) on February 26, 1919, and became head of the unit on October 1, 1919; see also Footnote 36 below. For further information on Selchow, see I-208 and his entry in the AA's *Biographisches Handbuch* (Isphording, Keiper, and Kröger 2017); the latter is an invaluable source of information for many of the individuals in Pers Z discussed here. Most sources give Selchow's first name as "Kurt", but it appears as "Curt" both on his birth certificate and in his AA biography.

[39]The Cipher Bureau became part of the AA's Department (*Abteilung*) for Personnel and Administration (*Personal und Vertwaltung*) on October 1, 1919, and its duties enlarged to include *Chiffrier- und Nachrichtenwesen* ("Encryption and Communications"). This reconfigured Cipher Bureau was then renamed Referat Z in December 1926. The "S" in Pers ZS stood for *Sonderdienst*, or "Special Service", a cover for its sensitive function.

Second World War: Kunze, Schauffler, and Paschke were in overall charge, while Zastrow led the US desk and Brandes the desk for French, Belgian, and Swiss traffic.[40] Thus the Foreign Office, not subject to the same restrictions as the Reichswehr under the Treaty of Versailles, enjoyed a continuity in its cryptologic operations absent in the military organizations.

Pers ZS had two subsections, one for linguistic cryptanalysis, run jointly by Adolf Paschke and Rudolf Schauffler, and one for mathematical cryptanalysis, run by Dr. Werner Kunze.

4.2 The linguistic section of Pers ZS

Paschke and Schauffler, who ran the linguistic section, had very different personalities. Although Paschke was junior to Schauffler, who led the section prior to the war, Paschke had more of a taste for administration and later ran the section jointly with Schauffler: Paschke became responsible for its overall administration and for Western Europe, while Schauffler was responsible for Asian languages, in particular Japanese.

4.2.1 Adolf Paschke

Adolf Paschke (September 20, 1891–February 1, 1978) was born in St. Petersburg. After graduating from a *Gymnasium* in 1909, he studied law and economics in Berlin and St. Petersburg, completing his studies in 1914. Interned by the Russians at the start of the war, he was exchanged after ten months, returned to Germany, and was assigned to the Signal Corps, where he worked on the Eastern Front as a cryptanalyst (his fluency in Russian an obvious advantage here). After the war he moved to the Foreign Office (on January 20, 1919) where he worked on the cryptographic systems of a

[40] Pers Z Chi, design of cryptographic systems, was initially overseen by Erich Langlotz (February 14, 1893–May 22, 1943), and then Horst Hauthal (September 3, 1913–April 21, 2002). During the First World War Langlotz had worked in the Communications Division at Army Headquarters (*Chef des Nachrichtenwesens im Großen Hauptquartier*). He joined the Foreign Office at the end of 1918 and put in charge of deploying new ciphers on October 1, 1919. He committed suicide in 1943. Hauthal had studied mathematics, chemistry, and physics at Halle and Berlin before the war and joined the Foreign Office on May 28, 1939. He became the leader of Pers Z Chi in May 1943. After the war Hauthal, Paschke and Kunze played an important role in Foreign Office cryptology; see van der Meulen (1996 and 1999). Hauthal received a Ph.D. in Economics from the University of Bonn in 1954, and was later active as a career diplomat.

number of countries, including those of Russia, Austria, the Vatican, Italy, Greece, France, and Czechoslovakia. He advanced steadily, becoming the effective head of Pers ZS in 1942. A detailed statement prepared for TICOM in 1948 (DF-111) summarizes his life up to then and his career in Pers ZS. A member of the NSDAP since 1933, during denazification proceedings after the war Paschke was classified as a *Mitläufer* ("Follower"), and presumably for this reason was reduced to working as a violinist in Marburg. This fall from grace ended in January 1950 however, when Paschke was tasked by the Federal Chancellery of the FRG with creating a new cryptologic service for it, Referat 114. Paschke suggested setting up an advisory board, its members including such familiar names as Hüttenhain, Kunze, Schauffler, and Selchow. Referat 114 itself was initially headed by Paschke and then Dr. Hans Karstien (July 10, 1903–May 10, 1967), another old hand from Pers ZS, until 1956 (when responsibility for cryptology in the FRG passed to the BND, ZfCh, and Dr. Hüttenhain). For further information on Paschke, see EASI 6, I-22, DF-111, Kahn (1996, pp. 436-7 and 439), and van der Meulen (1996).

4.2.2 Dr. Rudolf Schauffler

Dr. Rudolf Schauffler (August 11, 1889–February 6, 1968), born in Ulm, had been a schoolmaster before the First World War, after studying mathematics, physics, and languages at Tübingen and Munich. Apparently gassed during the war (I-22, p. 1), he did some form of cryptanalytical work at Army Headquarters beginning in 1916 (Kahn, 1996, p. 437). But on returning to civilian life, Schauffler "found schoolmastering too much" (I-22, p. 1), and joined Pers Z shortly after (December 1, 1918). His career there had three distinct phases. The first was cryptographic: he was part of a team (along with Kunze and Langlotz) which developed a one-time pad system for the Foreign Office in the years 1921–1923 (Kahn, 1996, pp. 402–403, van der Meulen, 1996, pp. 151–162). For further information about this one-time pad system, see below, Section 4.4.1. The second phase was cryptanalytic: he became interested in Japanese and Chinese systems (working on the latter for 20 years). The third and final phase was cryptological: Schauffler became interested in the theoretical foundations of cryptology and edited an in-house journal containing papers on topics of cryptologic interest: the *Wissenschaftliche Schriften des Sonderdienstes Dahlem* ("Scientific Writings of the Dahlem Special Service", Dahlem being the district of Berlin where

Pers ZS was located). Several of these papers were translated as part of the TICOM DF series, for example DF-38 ("The Enigma", by Dr. Rudolph Kochendörffer).[41]

Schauffler's precise administrative role in Pers ZS is unclear. He was its (at least nominal) head in the years 1937–1941 (EASI 6, p. 11), but in later years deferred to the more energetic Paschke. (Kahn, 1996, p. 437, quotes an unnamed source as saying "Paschke said he was in charge and Schauffler was modest and didn't object".) In 1943 Paschke and Schauffler were joint leaders of the linguistic cryptanalysis section, but an April 1945 organization chart (I-22, pp. 24-25, EASI 6, last page) shows Schauffler as the leader (*Referent*) of a new section on fundamental research (*Systematik, Grundlagenforschung, Wissenschaftliches Archiv, Berichtwesen*). Although TICOM thought him an "unworldly academic type" (I-22, p. 22), no one in Pers ZS appears to have doubted his abilities: he was "[g]reatly respected by his colleagues" (I-22, p. 22), and Hüttenhain regarded him as a "true scientist" (I-31, p. 11).

Although he did not have a Ph.D. during his time in the Foreign Office, Schauffler must clearly be regarded as a mathematician. Early on he wrote two papers (Schauffler 1917 and 1921) that appeared in the *Mathematische Annalen*, one of the leading mathematical journals in Germany. After World War II Schauffler received a Ph.D. in Mathematics from the University of Marburg in 1948, his thesis on a topic in cryptanalysis (*Eine Anwendung zyklischer Permutationen und Ihre Theorie*).[42] He later wrote at least two more mathematics papers (Schauffler, 1956 and 1957), the first of these an early contribution to the theory of check digit systems. Schauffler also had a considerable knowledge of Asian languages: in the years 1922 to 1930 he shared an office in Pers Z with the well-known polyglot Emil Krebs (1867–1930, see Hoffmann, 2017); under Krebs's supervision he became a proficient translator of Japanese and also learned some Chinese.[43] This knowledge served him in good stead after the war when he taught at Marburg.

[41] Schauffler even solicited articles for the journal from Hüttenhain, but nothing came of this because Fenner disapproved, regarding it as a security risk (EASI 3, p. 100.)

[42] Schauffler was never a student at Marburg. The thesis (accepted September 14, 1948) had been written in 1941 but was not published at the time because of its cryptologic content.

[43] National Cryptologic Musuem, David Kahn Papers, DK 65-50.

4.3 The Mathematical Section of Pers ZS

The mathematical section of Pers ZS housed its mathematicians, tackled its hardest problems, and was run by its most talented cryptanalyst.

4.3.1 The head of the mathematical section: Dr. Werner Kunze

Dr. Werner Kunze (August 16, 1890–April 22, 1970) was born in Eisleben, the hometown of Martin Luther. After graduating from an *Oberrealschule* (preparatory secondary school) in Eisleben in 1909, and then spending two semesters at Heidelberg (1909–1910), he moved to Halle, where he studied mathematics and science at the Friedrichs (now Martin Luther) University Halle-Wittenberg for three years. He received a Ph.D. in physics there in 1913, his *Doktorvater* (thesis advisor) Ernst Dorn.[44,45]

Kunze was drafted by (or joined) the Army just before the start of the war (August 7, 1914), and remained in it until shortly before its end (September 30, 1918). Initially in the cavalry, he eventually became a *Leutnant d.R.* (Lieutenant of the Reserve), and in January 1918 was assigned to work as a cryptanalyst in the *Nachrichtenchef der OHL im Großen Hauptquartier*, that is, the staff of the Chief Signal Officer of the Supreme Command of the German Army.[46] Immediately after the war, Kunze joined the Foreign

[44]Friedrich Ernst Dorn (1848–1916) was a German physicist best known for his work on radium and the co-discovery of radon, one of the emission products of radium; see Wigand (1916). Kunze's thesis was on the decay products of "radium F", that is polonium, itself a decay product of radon.

[45]The Halle-Wittenberg University Archives (UAHW, Rep. 46, Nr. 27 and Rep. 21, Nr. 402) show that Kunze was registered at the University from May 7, 1910 to July 18, 1913, passed his oral exam (*Rigorosum*) on August 1, 1913, and that his thesis (Kunze, 1914) was approved for publication by Dorn on March 3, 1914. The thesis was titled *Über Zerfallsprodukte des Radium F* ("On the decay products of radium F"). Kunze remained at Halle for two additional semesters after passing his oral exam (Winter 1913/1914 and Summer 1914), presumably continuing to work in Dorn's laboratory.

Kahn's (1996, p. 436) statement "Kunze had his doctorate in mathematics from the University of Heidelberg" appears to stem from a later misreading of notes he took during his interview with Kunze on May 4–5, 1962 in Bonn (National Cryptologic Museum, Kahn papers, DK 65-49). His suggestion "Kunze may well have been the first mathematician employed in a modern cryptanalytic office" thus appears unwarranted. It is of course true that as a physicist Kunze would have had extensive training in mathematics and, given his study of radioactive decay, likely a considerable knowledge of probability and statistics.

[46]The OHL (*Oberste Heeresleitung*) was the Supreme Army Command, headed by the Chief of Staff of the German Army; the *Nachrichtenchef* was the Chief Signal Officer.

Office (AA) on December 1, 1918 (along with Selchow, Schauffler, Langlotz, and Brandes) and became a member of the AA's Cipher Bureau.[47] Kunze eventually headed the mathematical cryptanalysis section. He was, as noted earlier, part of a three man team that developed a one-time pad system for the Foreign Office in 1921–1923, but he had even then already begun to study and work on cryptanalysis. In his post-war interrogation Dr. Hüttenhain identified Kunze as being "the most able cryptanalyst" in Pers ZS.[48] Kunze's successes included an attack on a French enciphered codebook in the 1920s, and breaking the Japanese "Orange" and "Red" machines in the 1930s; this work is briefly mentioned by Kahn (1996, pp. 402 and 436–7), and more fully discussed in EASI 6 and I-22.

Like several other of his Pers Z colleagues, Kunze had a post-war career in the Foreign Office. He returned to it on August 1, 1951, subsequently retiring on August 16, 1955. (When David Kahn spoke to Kunze in May 1962, he wrote in his notes "Kunze remains remarkably sharp, good clear memory, alert, laughs a lot". He could have also added "discreet": when the subject of his post-war life came up, Kunze just told Kahn "Retired in 1945".)

4.3.2 The structure of the mathematical section of Pers ZS

The structure of Kunze's subsection was succinctly described by TICOM thus:

> The Mathematical-Cryptanalytic Subsection, usually operated apart from the main Pers ZS party (Stammabteilung). Primar-

In the German military parlance of the day, the rank of an officer could also be used to designated the officer's staff (as here) or organization (as in the GdNA).

[47] All five were initially assigned to the *Politische Nachrichtenstelle* (PNS, the Political Information Desk), a new cryptanalytic unit that had just been set up in the AA headed by Dr. Hans Riesser (1887–1969). Selchow initially served as Riesser's deputy, but after Riesser left for Versailles, the PNS and Cipher Bureau merged and Selchow became head of the combined unit on October 1, 1919; see Grupp (1988, p. 151) and van der Meulen (1996, pp. 150–151), whose account is largely based on Paschke (1957). Selchow knew the others because they had all worked at the Supreme Headquarters of the German Armed Forces (GrHQu) during the war. For Riesser's later diplomatic career, see his autobiography (Riesser, 1962).

[48] Horst Hauthal, the head of Pers Z Chi, shared this opinion: "Er war wohl unser bester Analytiker" (letter to David Kahn, September 28, 1983, National Cryptologic Museum, David Kahn papers, DK 65-64).

> ily a mathematician, Dr. Kunze's subsection consisted of linguist mathematicians and was also responsible for the Pers ZS I.B.M. machinery. They specialized in difficult systems, complex encipherments, and those problems which required a large expenditure of time and personnel, or the application of technical devices. In December 1939, the group included 20 persons and was housed apart from Schauffler's Linguistic-Cryptanalytic Subsection. [EASI 6, p. 15]

4.4 The mathematicians of Pers ZS

Although much smaller than the OKH operation, Pers ZS housed an impressive array of mathematical talent: a partial list includes

- Dr. Werner Kunze
- Hans Rohrbach: Ph.D. Berlin, 1932
- Helmut Grunsky: Ph.D. Berlin, 1932
- Erika Pannwitz: Ph.D. Berlin, 1933
- Ralf Lohan: Ph.D. Berlin, 1935
- Fritz Dueball: Ph.D. Berlin, 1937
- Anneliese Hünke: Ph.D. Berlin, 1940
- Gottfried Köthe: Ph.D. Graz, 1927
- Helmut Ulm: Ph.D. Bonn, 1933
- Karl Schröter: Ph.D. Münster, 1941

Once again there were a large number of mathematicians from Berlin, but one of these names stands out in particular.

4.4.1 Professor Hans Rohrbach (1903–1993)

Dr. Rohrbach, who received his Ph.D. from Berlin in 1932, resumed a distinguished career after the war: he had 11 students and 149 descendants, and was Professor at Mainz from 1951 until his retirement in 1969 (as well as being Rector at Mainz in 1966–7). He had an international reputation, being both an editor of *Crelle's Journal* (one of the first mathematical journals to appear not associated with a national society or academy) and the *Collected Works* of his thesis advisor, the mathematician Issai Schur. There are entries on him in both the MGP and *Kurzbiographien*; Schwartz and Volkmann (2003) is a short biography with many references. Particularly useful is his entry in the University of Mainz's *Directory of Professors*.[49]

TICOM concluded that "[b]y personality rather than seniority, [Rohrbach] was one of the Pers ZS leaders" (EASI 6, p. 15). This was evident in the TICOM interrogation of twenty-one of the Pers ZS cryptologists in May 1945. Rohrbach was the first to be questioned, without the others present. TICOM reported:

> Professor Rohrbach was at pains to explain his own position. He had a chair of mathematics of Prague, which he held currently with his appointment with the Foreign Office, traveling often back and forth. He had chanced to be at Burscheidungen when the place was overrun [at the end of the war]. The senior members of the organisation had panicked in the absence of Selchow [the head of the organization], and he was the only person who had had the presence of mind to take any common sense action. He had thus become the leader of the party. He was careful to point out that this was not due to any position he held within the organisation or to any superior competence he might have as a cryptographer, but purely to force of character. In discussion of question[s] of cryptographic detail he wished to be regarded merely as a member of Dr. Kunze's section. [TICOM 1-22, p. 2]

We know a fair amount about what Dr. Rohrbach and his colleagues in Pers ZS did thanks to two papers he wrote that later appeared in English

[49]Hans Rohrbach, in: *Verzeichnis der Professorinnen und Professoren der Universität Mainz*. URI: `http://gutenberg-biographics.ub.uni-mainz.de/id/e5a284c4-7cfa-4e5c-941d-63c55ea94999`. (Accessed August 25, 2018)

translation in *Cryptologia* (Rohrbach 1978 and 1979). The first of these is a translation of a paper Rohrbach wrote that first appeared in 1948 (Rohrbach, 1948), and which effectively details many of the methods Pers ZS employed in its attacks on enemy systems. One cannot but admire the academic mind at work here: it is 1948, publishing is important in the academic world, and what better to write about than your activities during a six year period?[50] The second paper, originally a report written for TICOM (I-89), describes in detail the successful attack by a Pers ZS team on the U.S. diplomatic strip cipher O-2 (a variant of the M138A), work which earned Rohrbach the War Merit Cross (*Kriegsverdienstkreuz*) Second Class, in September 1944.[51]

Another one of the distinguished mathematicians of Pers ZS illustrates some of the difficulties that can arise in a study such as the present one.

4.4.2 Professor Gottfried Köthe (1905–1989)

Dr. Gottfried Maria Hugo Köthe (December 25, 1905–April 30, 1989), who received his Ph.D. from Graz in 1927 (advisors Tonio Rella and Robert von Sterneck), had a long and highly successful career after the war. In 1946 he became Director of the Mathematics Institute of the University of Mainz, was the Dean of the University from 1948 to 1950, and its Rector from 1954

[50]In general, former intelligence officers have to submit such material for prepublication review and approval before publishing it, but in the aftermath of the defeat of the Nazi state, this was apparently no longer a concern for Dr. Rohrbach. Curiously, the paper was published by FIAT (the US Office of Military Government for Germany (United States): Field Information Agency, Technical). Presumably, had the US Army Security Agency (or its 1947 successor AFSA, the Armed Forces Security Agency) been consulted beforehand one assumes it would have objected to publication.

[51]EASI 6, p. 2, lamented the absence of other such reports from Pers ZS personnel, noting that immediately after the war the practice of asking the German cryptologists "to do extensive 'homework' that is, write papers, as detailed as possible and in their own words, was not fully developed". It describes I-89, the sole exception, as "a most significant document from the cryptographic point of view", adding that even it "was issued with an apology for its preparation".

This last comment was diplomatic. What it is alluding to is a note at the beginning of the report added by Major William P. Bundy: "This [Rohrbach's report] was probably of no value. It was assigned to appease vanity and keep people busy" (I-89, p. 2). Why a detailed description of a successful attack on an important US system would not be of interest to TICOM passes understanding. Perhaps Bundy (who had a habit of derisively grading the German cryptologists, see I-58, p. 1 and I-63, paragraph 1) for once felt intellectually challenged by the formidable Professor Rohrbach.

to 1956.[52] In 1957 he moved to Heidelberg and became the founding Director of the new Institute for Applied Mathematics there (as well as later serving as Rector of the University in 1960–1961). Despite these demands on his time, he had 35 students and 261 descendants.

Köthe did work of great importance in functional analysis (*Köthe spaces* are named after him) and was a mathematician of outstanding ability, yet virtually the only testimony as to what he did during the war is the laconic comment in passing in an obituary that "Während des Krieges wurde er für längere Zeit zu einer Tätigkeit im Auswärtigen Amt einberufen und dort mit Dechiffrierarbeiten beauftragt" (During the war, he was summoned to work for a long time in the Foreign Office, where he was charged with deciphering work; Tillman, 2007, p. 3); see also Weidman (1990, p. 4) who confirms this. For further details of his life, see both Tillman (2007) and Weidman (1990).

4.5 The women of Pers ZS

Unlike OKW and OKH, some of the cryptologists in Pers ZS were women: Drs. Pannwitz and Hünke, as well as Frauen Friedrichs, Hagen, and Schrader. This appears to have been a bit of a culture shock for what had hitherto been an essentially all-male organization. In her TICOM interview on May 10, 1945,

> [Frau Friedrichs] touched on the position of women in the organisation. She said it had been a long fight to obtain for women the same pay as men, but that that had finally been achieved, but, though they received the same pay they had not the same status. At the beginning of the war a great many women had been engaged somewhat to the chagrin of men who had not been used to working with large numbers of women. [I-22, p. 4]

A short biography of Dr. Pannwitz (as well as several other of the mathematicians in Pers ZS) is given in Subsection 12.1 below.

[52] Köthe was presumably responsible for Rohrbach's appointment at Mainz as a Visiting Professor (*Gastprofessor*) from 1946 to 1951. (Rohrbach had joined the NSDAP in 1937 and may have initially had difficulties finding permanent employment.)

4.6 The impact of Pers Z

During the war Pers Z employed hundreds of cryptologists and support staff. How did they do?

4.6.1 Cryptography

The development and use of the one-time pad by the AA illustrates both the strengths and weaknesses of its cryptographers. The AA used a codebook during the war (the *Deutsch Satzbuch*, DESAB) with five digit codewords (lying between 00000 to 99999): the third version, DESAB 3 (containing some 31,500 codewords), was used through December 1941; the fourth, DESAB 4 (containing some 57,500 codewords), was used from January 1942 until the end of the war. The AA employed two major methods of encryption during World War II: the *Grundverfahren* and *Blockverfahren*.[53] In both cases five digit additives were added modulo 10 (per digit) to each codeword. The *Grundverfahren* was a system in which a pair of five digit additives, taken from a fixed book (the *Tangenstafel*), were added to a five digit codeword. It was used for less important messages such as visa regulations (van der Meulen, 1998, p. 159). The AA's one-time pad system, the *Blockverfahren*, used numbers on a one-time basis taken from a book, each page of which had eight lines, each line containing six five-digit groups, for a total of 240 characters per page. Pers Z thought both systems were unbreakable, while it regarded the underlying codebook itself as providing no security at all and sometimes even sent messages using the codebook in the clear (Phillips, 2000, p. 326, Erskine, 2003, p. 113). The discussion in van der Meulen (1996), which explains the roles that Kunze, Langlotz, and Schauffler played in the development of the two systems, relies heavily on Paschke (1957) and Hauthal (1958), unpublished manuscripts in the archives of the AA.

Unfortunately for the AA, both systems were in fact broken by the Allies. The *Grundverfahren* (codenamed "Floradora" by the UK, "Keyword" or GEC by the US) fell victim to poor operator usage and a small amount of key being captured; eventually (certainly by 1944) virtually all Floradora messages were being read. The *Blockverfahren* (codenamed GEE by the US) fell victim to a much more basic problem: although Kunze had insisted on the absolute randomness of the frequency with which the different additives

[53] A third method, the *Spalierverfahren*, based on reciprocal bigram tables, was less secure and used for the lowest grade of encrypted traffic (Erskine, 2003, p. 113).

occurred, the *sequence* of additives was far from random: a machine with 240 wheels, the digits from 0 to 9 on each wheel appearing in a scrambled order, was used to print the pages, two at a time. After the pages were printed, the wheels would turn (or not) according to a complex formula. Once the structure of the machine was diagnosed (thanks in part to some messages being sent in both systems) and a method for locating where in the key stream one was, a message could be immediately read. The exploits are described in part in two now declassified NSA internal papers (Waggoner and Jache, 1961 and 1962); Filby (1995) discusses the breaking of Floradora from the UK perspective, Phillips (2000) the breaking of GEE from the US perspective, Budiansky (2001) the use of IBM machines in the US attack, and Erskine (2003, pp. 112-114) the cooperation between the UK and US in the attack on the two systems. Waggoner and Jache (1962, pp. 67–69) is of particular interest because it quotes at length from a 1928 analysis Schauffler prepared regarding the security of the GEE system. (Their harsh comment, however, that "with rather arrogant confidence, Herr Schauffler convinced himself and the Foreign Office of the security of the one-time pad system", seems somewhat unbalanced, given that a system introduced by the AA in 1923 only began to be exploited by the Allies at the beginning of 1945. Indeed, until the US attack on the system in 1944, the UK's GCCS had regarded the system as unbreakable.)

4.6.2 Cryptanalysis

Pers ZS was the oldest, arguably most professional, but at the same time least effective of the German cryptanalytic organizations. This was despite its technical successes, discussed in EASI 6 and summarized in Alvarez (1996). The reasons for this ineffectiveness were many: a lack of adequate resources (I-172, p. 6); inadequate infrastructure for the handling and processing of intelligence (EASI 6, p. 57); a perceived lack of appreciation (EASI 6, pp. 58–59); and a lack of direction, both from Curt Selchow, the head of Pers Z (I-22, p. 5), and from Foreign Minister Joachim von Ribbentrop (Paschke, I-172, p. 6, von Ribbentrop, I-143, p. 11). Compounding this was the over-arching problem that what intelligence was produced was often suppressed or ignored. Looking back, in 1962 Schauffler told David Kahn "Ribbentrop did not dare give Hitler bad news", "they preferred their own propaganda to

our information".[54] Kahn (1967, p. 11) later wrote:

> The interview with Rudolf Schauffler, one of the chiefs of the German Foreign Office cryptanalytic service, was the most depressing one I had [while doing the research for his classic 1967 book *The Codebreakers*]. Elderly, not old, but broken by sickness and the ersatz food of the war years, he shuffled around his chilly apartment, barely able to put a pot of water on for tea. As rain dripped slowly from the gray sky, he ended our talk by saving, "A bridge builder can see what he has done for his countrymen, but we (German codebreakers) cannot tell whether our life was worth anything."

5 Networks?

Personal ties appear to have played a significant role in placing mathematicians into positions in the three organizations we have discussed thus far. Consider the case of the mathematician Ludwig Bieberbach, who gained notoriety for his support of Nazi racial doctrines, and who presumably had close ties to the regime.[55] Six of his last eight doctoral students, and a total of nine overall, went into signals intelligence (in the following, the date given refers to date of the degree): Helmut Grunsky (1932, Pers ZS), Max Wernick (1934, OKH), Herbert von Denffer (1935, OKH), Fritz Dueball (1937, Pers ZS), Rudolf Kochendörffer (1937, Pers ZS, OKH), Werner Schulz (1937, OKH), Hans Pietsch (1938, OKH), Johann Friedrich Schultze (1939, OKW/Chi), and Annelise Hühnke (1940, Pers ZS).

Or maybe it was that many of the mathematicians who went into signals intelligence had served as long-term staff of the *Jahrbuch über die Fortschritte der Mathematik* (edited by Bieberbach): Erika Pannwitz (15 years), Hans Pietsch (9 years), Willi Rinow (4 years), Fritz Dueball (3 years) and Rudolph Kochendörffer (3 years). There is certainly much potential for research here.[56]

[54] National Cryptologic Musuem, David Kahn Papers, DK 65-50.

[55] Bieberbach was one of the leading German mathematicians of his time. For an extensive discussion of his role in German mathematics during the 1930s, including his editorship of the journal *Deutsche Mathematik*, see Mehrtens (1987), Segal (2003, especially pp. 263–288 and Chapter 7).

[56] Another interesting connection here is that of the University of Münster and two of its Professors, Heinrich Behnke and Heinrich Scholz. Behnke had connections to three of

We now turn to the last three major German cryptologic organizations. These had far fewer mathematicians, and our discussion of them will therefore be quite brief.

6 The *Chi Stelle*

The *Chi Stelle* was the signals intelligence organization of the Luftwaffe, the German Air Force. Established January 1, 1937 as the *Chiffrier Stelle, Oberbefehlshaber der Luftwaffe* (*Chi Stelle, OBdL*) it initially had one officer and twenty civilians. But it grew rapidly, so that by the end of the war it had a staff of nearly 13,000; see EASI 5, p. 1. Its chief cryptanalyst was Dr. Ferdinand Voegele, a linguist.

Mathematicians did not have a large footprint in the Chi Stelle, but it was still highly effective. To quote TICOM: "The outstanding achievement of the German Air Force Signal Intelligence Service was its development of "signal intelligence without cryptanalysis" (EASI 5, p. 1). This is less paradoxical than it might sound: what is meant here is the highly effective use of direction finding and traffic analysis by the Chi Stelle. The Chi Stelle did, however, have one mathematician of note.

6.1 Professor Guido Hoheisel (1894–1968)

Dr. Guido Kark Heinrich Hoheisel (July 14, 1894–October 11, 1968; Ph.D. University of Berlin, 1920; advisors Erhard Schmidt and Issai Schur) "entered the OKL only in 1944 but was already rated the brains in an otherwise weak section" (Dr. Buggisch, I-92, p. 4). He spent much of his professional life as a Professor at the University of Cologne (from 1939 to 1962), and had 12 doctoral students and 38 descendants. One of these students of his is of great interest: Dr. Otto Leiberich (Ph.D. 1953). Leiberich is of considerable interest because he did not go into academia, but immediately began work in the ZfCh (the *Zentralstelle für Chiffrierwesen*, recall this was the West German equivalent of the UK GCHQ), was later head of its mathematical cryptology

the individuals mentioned in our study: Hüttenhain had studied under him, Köthe had been his assistant, and he was the *Doktorvater* of Karl Stein. Further, both Hasenjaeger and Schröter received their doctorates under the supervision of Behnke's colleague Scholz. Helmut Ulm taught at Münster beginning in 1935; he was helped by Behnke after the war in finding employment.

section, and eventually became head of the ZfCh itself in 1972. Later on, in 1991, he became the first head of the BSI, the *Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for Security in Information Technology); see (Hange, 2015). Thus Leiberich, Hoheisel's student, was effectively Hüttenhain's successor as head of the ZfCh, yet another connection in a highly connected world.

6.2 Attitudes towards mathematicians and women

Part of the genius of Bletchley Park was that civilian (and sometimes eccentric) mathematicians could work alongside uniformed officers, and that the talents of women such as Joan Murray (née Clarke), Mavis Batey (née Lever), and Regene Lewis were recognized and put to good use.[57] This was not always the case with the German cryptologic organizations.

The Chi Stelle had few serious academic mathematicians. There was a simple reason for this: academic mathematicians were viewed with distain. At the end of the war Oberleutnant Waldemar Werther prepared a report (Werther, 1959), presumably for TICOM, in which this was made clear:

> The mathematical ability so often called for or presupposed does indeed belong among the essentials, but this talent is not to be confused with mathematical schooling. The best cryptanalysts with great analytic and constructive talents have, as a rule, no notion of the theory of combinations. The few mathematically trained workers on the other hand often use their knowledge merely to calculate, on the basis of well-known formulae, how many possibilities this or that system permits – the system being generally broken by others. [Werther, 1959, p. 86]

Mathematicians were not the only ones looked down on by Oberleutnant Werther; he had unfavorable views (perhaps similar to those of the men of Pers ZS) regarding women as well:

> While a man works for the job, a woman works for a person. Her productivity depends, therefore, much more than does the man's, on released sympathetic or antipathetic impulses. The

[57] For Regene Lewis, see `https://bletchleypark.org.uk/roll-of-honour/5503` (accessed December 9, 2018).

> performance of female workers was therefore dependent on the attitude of the chief cryptanalyst, the other military authorities, and the general living conditions.
>
> Though a goodly number of intelligent women and girls showed good average results, working together and particularly living together under war conditions created an atmosphere which could hardly be called serious and intellectual. Undoubtedly purely male organizations showed better and more substantial results. [Werther, 1959, p. 81]

Oberleuntant Werther's comments cannot be dismissed as those of some cranky underling: he was the Director for Cryptography for the northern sector of the Eastern Front (*Luftflotte I*) from August 1942 to August 1943, and Director of Cryptography for the central sector of the Eastern Front (*Luftflotte VI*) from September 1943 to May 8, 1945. For a brief summary of his life, see I-121, pp. 2–3. TICOM I-120 and I-121 are, respectively, translations of reports he wrote about Soviet systems, including Luftwaffe cryptanalytic efforts against them, and the different cryptosystems (both Soviet and non-Soviet) attacked by the Chi Stelle.

Volume 5 of EASI is devoted to the Chi Stelle; EASI 5, pp. 6–8 lists its sources of information. Particularly important, in addition to the many TICOM reports, is the Seabourne Report, "The Signal Intelligence Service of the German Luftwaffe", released by TICOM as reports IF-175 through IF-189.[58] Indeed, the "TICOM and the Seabourne reports taken together present a comprehensive picture of the German Air Force Signal Intelligence Service" (EASI 5, p. 8). More generally, David Kahn's 1978 *Hitler's Spies* gives throughout many interesting examples of Luftwaffe intelligence; see in particular Chapter 8 and Chapter 20, pp. 38–387.

7 The *B-Dienst* (OKM/4 SKL/III)

The *B-Dienst* (the *Beobachtungsdienst*, or Observation Service) was the Naval cryptologic organization; its full name was OKM/4 SKL/III: that is, the *Oberkommando der Marine/4 Seekriegsleitung/III*. (Breaking this down,

[58] National Archives and Records Administration, Record Group 457, Boxes 974–976. Colonel J. G. Seabourne was a colonel in the USAAF (United States Army Air Forces), and chief of its Air Technical Intelligence Team.

this was OKM, the Naval High Command; SKL, the Naval Warfare Staff; 4 SKL, the Communications Division; III, the Signals Intelligence Subdivision.)

The B-Dienst had little contact with other cryptanalytic organizations yet was highly successful. Its leading cryptanalyst was Wilhelm Tranow; see Kahn (1978, Chapter 14). His preliminary TICOM interrogation (I-12) summarizes its many offensive successes against the British. There is little evidence however that high-level mathematicians were brought into the B-Dienst. It is for that reason that we do not discuss it here, despite the considerable amount of information about it now available.[59]

8 The *Forschungsamt* ("Research Bureau")

Finally, there is the *Forschungsamt*. Founded in April 1933 by Hermann Göring, it was ostensibly part of the RLM (*Reichsluftfahrtministerium*, the State Ministry of Aviation). In reality, it was the Nazi leadership's signals intelligence organization and as such targeted domestic (and some foreign) communications. Divided into six *Hauptabteilungen* (Chief Departments) and fifteen *Abteilungen* (Departments), at its peak it was staffed by 2,000 (or more) people, 180 of whom were in the cryptanalytic section. But despite its size it was entirely unknown to the Allies until Spring 1945. (Presumably this was because its targets were primarily domestic.) Its principal mathematician was Dr. Martin Paetzel (*Hauptabteilung IV: Entzifferung*). Important sources of information about it include EASI (Volume 7), Kahn (1978, pp. 178–184 and 1978a) and Irving (1989).

TICOM had a high opinion of the organization: EASI, Volume 7 (p. 73) concluded:

[59]But despite this apparent lack of professional mathematical talent, the B-Dienst had many talented individuals. One of them, Lt. Hans-Joachim Frowein, deserves special mention. In 1944, concerned about mounting U-boat losses, Lt. Frowein was charged by the Navy with investigating the security of the Naval Enigma. He worked on the problem from July 1944 to January 1945, with an initial staff of two officers and ten men (although this was later cut down to two men of any ability). Despite Frowein's previous lack of experience with the device ("I started with no knowledge of the Enigma machine"), within six months he was able to find an attack based on a 25 letter crib. Although the German Navy did not undertake significant changes as a result of his theoretical findings (he thought the primary weakness of the Naval Enigma was that the right wheel had only one turnover, which was changed), his work was highly enough regarded for him to be awarded the War Merit Cross. For further details, see I-38, his TICOM interrogation on July 14, 1945.

> In the light of all the evidence available the FA must be recognized as a highly successful source of intelligence in the fullest sense of the word. So important was the intelligence produced that careful arrangements were made for furnishing it throughout the final stages of the war.

In sum, Germany had a very large investment in signals intelligence, involving tens of thousands of people, including a substantial number of research mathematicians, and throughout the course of the war they scored many successes on the offensive side of code breaking. But recognizing this fact raises an important and very natural question.

9 The paradox of German high-level cryptography

This is the title of Chapter 1 of the second volume of *European Axis Signal Intelligence*, which starts off:

> German high-level cryptographic systems were insecure although brilliantly conceived.

There were several reasons for this: organizational redundancy (six different major organizations), lack of coordination (the reason Rejewski was able to break the two new Enigma wheels in 1938), intra- and interservice obstruction (the Army refused to give cryptanalysts its own traffic to monitor), and a lack of understanding about the most basic principles of communications security.

One could document at great length the reasons for this meltdown in communications security, but the simplest approach to understanding the nature of the problem for the Germans is to let their own mathematicians testify. First and foremost, it is essential to understand the hierarchical and bureaucratic nature of the system within the German military. For example, after July 20, 1944 there was a major shakeup in the Signals Corps, with the executed General Fellgiebel replaced by General Willy Gimmler. Hüttenhain and Fricke relate:

> He (Gimmler) gave a sort of standard lecture to various groups at various times. His approach was that of the Officer-layman. He

> had no technical knowledge and no one could tell him anything. His speech began something like this: "I will make Chi an orderly organization. Before this, it has not been so. We must have three pillars in our work: Development, Security, Cryptanalysis." Then he would expound his views on the relation between these three. The head of the first branch must be an **Officer** who would know what the troops need. The second could be left to a civil servant. It is the most important of the three, and the other two exist primarily to fertilize it. He considered cryptanalysis very unimportant in itself. [EASI 3, pp. 23–24]

But of course one could argue that General Gimmler had it precisely right: securing one's own communications may well be more important than being able to read those of one's opponents. The problem was that for the previous five years of the war this attitude did not inform the German military. Dr. Fricke was very clear on this. In his TICOM interrogation

> [Dr. Fricke] said they always had wanted to work on their own traffic just as they would do on foreign material, but were never given the opportunity. They never knew how the Army actually used the systems which they put out and they never saw any real traffic. They often reflected that the work on Russian systems showed that those systems were secure if properly used, but if the cryptographers in Moscow could only see how they were used they would be very unhappy. [I-20, p. 3]

But things were in fact much worse: it was not just that the cryptanalysts of OKH were not permitted to monitor live traffic.

> Whenever the Army was asked to change a system, there was a storm of protest. It was not [the cryptanalysts] but the HNV [*Heeres Nachrichten Verbindungsabteilung*, Department of Army Communications] staff which made the decision on methods to be used. The results depended on whether the officer at HNV at the time happened to know anything about cryptography. He usually did not. *In 1942 all hand systems were solvable.* When the HNV was told this, the reply was that Germany had won all her battles so far, using these systems, and there was no need to overload the troops with new methods. [I-20, p. 3, emphasis added.]

Nor was Dr. Fricke alone in this conviction. Dr. Buggisch in OKH was of the same mind:

> [German security] is a pet subject with B. His story is that *up to 1942 the machines and systems introduced were not checked mathematically for security.* When Döring in that year pointed out the weakness of the early T52's to the higher-ups (Fellgiebel) it was decided to check all new devices. But the liaison on this was still bad ("tragisch-komisch") and even if In 7/VI detected an insecurity it was very hard to get action.
>
> Conversely it was very hard to get action on new devices. B. has the almost inevitable comments about the military non-technicians who blocked things. [I-58, p. 8, emphasis added.][60]

These were not just the carping theoretical objections of an ivory tower mathematician. When TICOM asked Dr. Buggisch what he thought the potential insecurities in the Army Enigma were, he went down a checklist (I-137, p. 5):

- Rotor I (the "fast" rotor) moved uniformly.
- Rotors II and III moved too infrequently.
- The machine should have used more than three rotors.
- There should have been more than five rotors to choose from.
- The reflector was not pluggable.

TICOM, impressed, agreed:

> Dr. Buggisch was so right! Improvement in any one of the foregoing particulars could easily have pushed the plugboard Enigma beyond the reach of already-straining Anglo-American cryptanalytic fingers, and possibly altered the course of the war. [EASI 2, p. 12]

[60] Note the "pet subject" and "almost inevitable comments". The first makes it clear that this was a subject Buggisch himself brought up on a number of occasions; the second that such complaints frequently came up in interrogations of other cryptologists as well.

Let us end with one final quotation, from Dr. Franz (the novice who entered OKW/Chi in 1940 with no knowledge of cryptology but ended up heading its section devoted to breaking into new and difficult systems). When asked to give an overarching assessment of OKW/Chi, he replied:

> In 1942 I had absolutely no overall picture of the cryptographic work at the Bureau. Hence, I cannot say anything positive in the regard. Naturally there was a general tendency to seek permanent improvement of our own cryptosystems, since *it was recognized that many systems regarded as unbreakable could nevertheless be solved if serious efforts were made.* [DF-176, p. 14, emphasis added]

If serious efforts were made ... . This perceptive comment really says it all. Unlikely Bletchley Park (which thanks to Prime Minister Winston Churchill had virtual carte blanche from late 1941 on), the German military apparently could not imagine an environment in which a government would invest the resources into signals intelligence that the British and US in fact did.

It is important to remember also in assessing Dr. Franz's statement that Dr. Franz (and Dr. Fricke and Dr. Buggisch), writing in 1946, had absolutely no knowledge whatsoever of Anglo-American cryptanalytic successes during the war. This fact was considered highly sensitive classified information and no mention of it was made during the TICOM interrogations.[61] Nevertheless, the insecurities in the German systems were obvious to Fricke, Buggisch, and Franz. But in wartime Nazi Germany, this was an unwelcome message that the higher-ups did not want to hear: that the systems that had been developed and deployed by them over the last decade were in fact insecure.

10 Conclusion

The interwar period from 1918 to 1939 saw a dramatic shift from hand-based methods of cryptography to those based on machine encryption. These new methods in turn required new kinds of cryptanalysts, mathematicians

[61] For example, when Dr. Fricke asked his interrogators if any German raster ciphers had been solved, because, although thought to be secure if properly used, he did not know if they had been compromised by operator usage, his interrogators told him "it would be impossible for us to give him an answer" (I-20, p. 3).

rather than linguists. Some countries, such as Poland and the US, realized this much sooner than others. Poland, which had already seen during the Polish-Soviet war of 1919–1921 just how useful mathematicians could be, hired three mathematicians in 1932 (Marian Rejewski, Jerzy Różycki, and Henryk Zygalski) to work on the new German Enigma machine; and thanks to their successful efforts were able to read Enigma traffic throughout much of the 1930s. After the dissolution of the American Black Chamber in 1929, the great American cryptologist William Frederick Friedman was tasked by the US Army in 1930 to set up the Signal Intelligence Service; and his first three hires (Frank Rowlett, Solomon Kullback and Abraham Sinkov) were all mathematicians.[62] This gave the US a valuable head start, among other things, in attacking Japanese diplomatic traffic.

The British and Germans only came to this game rather late in the day. True, the British had been recruiting and training "men of the Professor type" more than a year before the outbreak of war, but they had to have the mysteries of the Army Enigma explained to them by the Poles (in July 1939), and it was only after the outbreak of war that mathematically talented individuals such as the phenomenal Alan Turing reported to Bletchley Park (on September 4, 1939, the day after war was declared).[63] The Germans appear to have been even more near-sighted. True, Erich Hüttenhain was hired by (the predecessor of) OKW/Chi in 1937, but he is the exception that proves the rule: most of the Ph.D. mathematicians hired by the different branches of the German military and state institutions were hired in 1940 or later (after it became clear that the war would not be a short one). They paid for this: the gross insecurity of the double-encryption of the three-letter message indicator for the Army Enigma went undetected for nearly a decade (although Rejewski had spotted it within a few months), giving their opponents valuable knowledge such as the wiring of the wheels and the daily setting. Indeed, bizarre as it seems in retrospect, there was no agency

[62] All three had undergraduate degrees in mathematics and taught mathematics in high school. Kullback and Sinkov each went on to a Ph.D. in mathematics (Sinkov in 1933, Kullback in 1934) within a few years of joining the SIS in 1931.

[63] Turing had been recruited by GCCS no later than the summer of 1938, when he took a course in cryptanalysis they gave. Another mathematician, Peter Twinn, who worked with Turing and Dilly Knox on early Enigma problems, joined GCCS full time in early February 1939. Similarly, the Swedes also began to hire mathematicians for cryptological work shortly before the outbreak of war. Arne Beurling was contacted by the Swedish signals intelligence agency in early 1939 and asked to take a course in cryptology and help out with their cryptological problems; see Beckman (2002).

or unit in the German army tasked solely with communications security until the formation of In 7/IV in 1939. As a result, engineers would design prototype encryption devices which would only afterwards (if at all) be shown to cryptanalysts for vetting.

Early on Fritz Menzer noticed that too few stecker pairs were being used in the setting of the Enigma, resulting in the increase of October 1, 1936 (I-200, p. 12, I-202, p. 5). Other modifications followed over the next four years, increasing the security of the machine. The need for several of these would have been obvious to a mathematician much earlier. After Hüttenhain was hired in 1937, Menzer and he quickly identified serious weaknesses in the designs of both the SZ40 and T52-A/B teleprinter encryption devices, as did Heinrich Döring later on with the T52 A/B, C, and D. The usual German response in these cases was to take a pre-existing machine and modify it to make it more secure: the stecker board was added to the Enigma, irregular motion was introduced into the SZ40 by means of the μ wheels, and similar modifications were made to the early versions of the T52.[64] The problem was that often vulnerabilities in the devices remained: patterns in the Enigma permutations that could be detected even after the addition of the stecker board; a weakness in the "irregular motion" of the ψ wheels of the SZ40 that allowed one to strip off the χ wheel layer of encryption.[65] But change, as Fricke and Buggisch noted, was difficult: engineers resisted this, bureaucrats in an organization detest cost overruns, and – human nature being what it is – there would have been a natural resistance to admitting that devices that had already been developed and fielded were genuinely insecure. In wartime insecurities viewed as purely theoretical are orphans.

[64] In the original version of the SZ40 none of the wheels moved irregularly; see I-45, pp. 16–17. Hüttenhain and Fricke referred to this as the "SZ 40 (old type)", noting "the security of this type was not great". I-45, a report written by Hüttenhain and Fricke at the request of TICOM, is of great interest because it documents in considerable detail that German cryptologists were aware of the insecurities present in the earlier versions of the encryption devices used by the different branches of the German Armed Forces.

[65] For details of the attack on the SZ40, see Zabell (2015). It can be argued that the case of the Enigma was not so much a response to a perceived insecurity in the machine but intended rather as an improvement on the rotor machine principle. If *Chiffriermaschinen Aktiengesellschaft* (ChiMaAG – the Enigma manufacturer) had had their way it is possible a pluggable reflector might have been introduced as early as 1927. But although ChiMaAG had ideas about how to make the machine more secure, both the Reichswehr and the Army's Cipher Bureau had their own agenda and politics. For more information on the early history of the Army's adoption of the Enigma, see Ostwald and Weierud (2016).

Too little and too late: the Germans never invested the same level of resources that the Allies did, and they only brought in mathematicians in substantial numbers after the war broke out. (It is telling that In 7/VI, the cryptanalytic branch of the German Army, was only established in 1941.) But whatever missed opportunities this caused on the offensive, signals intelligence side, they were dwarfed by the impact on communications security. There were lessons here for the Allies to learn after the war.[66]

In the end, however, the failure of Germany to exploit its considerable national mathematical talent, is only one piece—albeit a very important one—in understanding the paradox of German high-level cryptography. Other elements we noted before in passing, such as organizational inefficiencies, lack of coordination between the different organizations, lack of adequate monitoring of its own traffic, and ultimately a complete lack of understanding of basic communications security, all played an important role. In a successor paper to this one we will consider this broader picture and the broader reasons for the breakdown in German communications security. Here too the TICOM documents, considered in their totality, paint a clear and compelling picture of the anatomy of failure.

11 Postscript

One of the curiosities to emerge from this study is that while so many German mathematicians worked in signals intelligence during the war, the extent of this participation is surprisingly little known, even in Germany today.

Consider the most productive (in terms of supervising doctorates) of the mathematicians noted in this paper: Franz, Witt, Aumann, Stein, Hasenjaeger, Rinow, Rohrbach, Köthe, Hoheisel, Kneschke, Grunsky, Ulm, and Schröter had between them 181 doctoral students and 3,068 descendants.

[66] New machines were in fact under development such as the Menzer machines SG 39 and SG 41, both designs that if implemented would have given the Allies major problems; see Mowry (1983). Both developments, however, were initiated after the war had started and this put all kinds of obstacles in their path. Increasing priority was put on war material needed at the front, and restrictions on these became increasingly severe as the war progressed. Another problem was the sheer challenge of introducing a new system in a secure way in an increasingly shifting and confused war situation. It is doubtful the Germans would have been able to achieve such changes on a large scale even if they had wanted to.

Thus it seems likely (even though of course some of these will have died in the interim) that perhaps as many as two thousand Ph.D. mathematicians alive today in Germany are descended from the mathematical cryptologists of the Second World War.

12 Appendix

12.1 Additional brief biographies

In addition to the individuals discussed in the body of this paper, who were of interest either because of cryptologic achievements during the war, or a highly successful post-war career, some of the other German mathematical cryptologists also had experiences that were not without interest. Several of these are briefly mentioned below.

12.1.1 Dr. Otto Buggisch

Dr. Otto Buggisch (June 28, 1910–September 15, 1991; Ph.D. Technical University of Darmstadt, 1938; advisor Ugo Wegner) is of interest as both a witness and a critic. As a witness because he had an excellent memory for names and organizations, and was a keen observer of developments in many areas outside those of his own immediate activities (I-58, pp. 1 and 9, see also I-64, p. 4). He is therefore an invaluable source of information in his interrogations and written reports. This is reflected in the large number of TICOM documents concerning him: I-46, I-58, I-64, I-66, I-67, I-92, I-137, and I-176, more than almost any other individual except key personnel such as Dr. Hüttenhain. And he is of interest as a critic, because of his perceptive comments about the weaknesses of the Enigma and more generally about the bureaucratic inertia that hamstrung efforts to improve communications security in the German Army. He joined the Army in May 1939, was transferred to In 7/VI when it was set up at the beginning of 1941, and became part of Referat 13 (security of machine ciphers) when it was established in August 1942. He was transferred to Wapruef 7 in June 1944 to work on speech encryption, but this transfer did not seem well thought out: his "first period in the Wapruef 7 was painful and useless as he found no mathematical application and did not know enough electricity" (I-58, p. 7). Eventually he "got to know his way around better", but by then of course the war was nearly over.

After the war he cooperated during a lengthy series of interrogations, but took great offense (I-176, p. 13) at his treatment afterwards (solitary confinement for four weeks, not permitted to contact his family even by mail, continued detention). He was eventually released in April 1946. By his own lights he then did very well. Before the war Dr. Buggisch had graduated from the *Ludwig-Georgs-Gymnasium* (LGG) in Darmstadt in 1928, and then studied at the Technical University (then *Hochschule*) in Darmstadt (THD); after receiving his doctorate from the THD in 1938 he taught at two local schools, a *Realgymnasium* in Darmstadt (1938) and then an *Oberschule für Jungen* in Bingen (1938–39, about an hour away). After the war he returned to high school teaching: for the most part at his alma mater the LGG (1948–1966), but for the last three years before his retirement (1969–1972) as an *Oberstudienrat im Hochschuldienst* (a senior civil service position) at the THD. He thus resumed his career after the war where it had left off before, and returned to the schools where he had been a student.

12.1.2 Professor Ludwig Föppl

Dr. *Ludwig Föppl* (February 27, 1887–May 13, 1976; Ph.D. Göttingen, 1912; advisor David Hilbert) illustrates the chaotic and haphazard way in which the German military dealt with the shortage of mathematical cryptologists at the outbreak of the Second World War. Föppl had served with distinction as a cryptanalyst during the First World War (see Brückner 2005), and afterwards became a Professor at the Technical University of Munich. At the time of the *Anschluss* in 1938 (when Germany occupied Austria) he was ordered to report for duty in Berlin and dispatched to Vienna, where he was almost immediately discharged and permitted to return home. A year later, with war imminent, on August 25, 1939 Föppl was again ordered to report to Berlin and this time assigned to OKW/Chi. Conditions were not what a distinguished 52-year old German Professor was used to, however, but he was able to secure a transfer to more amenable surroundings in Frankfurt, where "he secured a significant decryption success" (Samuels, 2016, p. 370). (This would have been the attack on the F110 French Army Code, mentioned earlier in connection with Dr. Hüttenhain.) But missing his family he was able to pull strings and was once again discharged on January 20, 1940. Samuels (2016) gives an excellent account of Föppl's experiences, based on a lengthy unpublished memoir.

12.1.3 Dr. Hermann Föppl

Ludwig Föppl's son *Dr. Hermann Föppl* (February 17, 1920–December 4, 1999) was for many years the chief chemist at the Max Planck Institute for Extraterrestrial Physics. But his interest for us is as a member of In 7/VI. He was a soldier in Russia in 1941/42 and suffered severe frostbite (for which he was awarded the *Ostmedaille*).[67] He was hospitalized near the Baltic sea and it was initially thought his leg would have to be amputated, but his Swedish stepmother traveled up from Munich to Northern Germany to prevent this. This was fortunate for Hermann, for he recovered and was then posted to In 7/VI in Berlin as a *Gefreiter*. (It is natural to speculate that Hermann's father Ludwig may have played some role behind the scenes in arranging this particular transfer.) He joined Referat 7, tasked with the security of hand ciphers. At this point there is no information available to us as to what he did in In 7/VI, but he presumably did have some success because he was promoted to *Unteroffizier* a year later. (Buggisch ranked him as a "very good cryptanalyst"; see I-176, p. 10.) He may have remained in OKH/Chi for the rest of the war. He returned to the family home at Ammerland on the evening of May 1, 1945, "completely exhausted": he had left his detachment a few days earlier only to then be captured by US forces, but managed to escape, and showed up at the family doorstep only "after great exertions and hardships" (Ludwig Föppl, *Lebenserinnerungen*, unpublished manuscript).

Although there is no record of Hermann Föppl having achieving notable cryptanalytic successes during the war, nor was he a mathematician (the primary focus of this paper), his subsequent life history does give a human face to one of the many thousands of youthful recruits to German signals intelligence in World War II, and how they picked up their interrupted lives afterwards. After the war Hermann studied chemistry at Göttingen, receiving his Diplom in 1951.[68] He then pursued further graduate studies in chemistry at Münster, working under the great Wilhelm Klemm (1896–1985)—an authority on magneto-, inorganic, and physical chemistry—and received his doctorate in 1956, his thesis on "Kristallstrukturen der Alkalioperoxide". Af-

[67]The "East Medal", *Medaille "Winterschlacht im Osten 1941/42"*, was awarded for service on the Eastern Front during the winter campaign of 1941/1942. There were a number of qualifications to receive the award, including severe frostbite of a limb.

[68]The Diplom was the standard undergraduate degree in the sciences in Germany at that time. Given a university's curriculum, it could take anywhere from four to six years. Although a first degree it is often viewed as more the equivalent of today's Master's.

ter initially serving as an *Assistant* to Klemm (1956–1959) and working in industry on semiconductor production (1959–1963, first at Wacker Chemie, Burghausen, later on in Aschau am Inn at a chemical plant), he moved to the Max Planck Institute for Extraterrestrial Physics in 1963, where he remained for more than three decades as chief chemist, until shortly before his death in 1999. He publishing many papers during this period, and as part of his work traveled extensively throughout the world (African Sahara, India, Argentina, Chile, Alaska, and northern Sweden). His research focussed primarily on the geomagnetosphere (including the Aurora Borealis, or Northern Lights); some of this work involved the dangerous element barium and he was burned twice during his experiments, once in a life-threatening way.[69]

12.1.4 Dr. Werner Schulz

Dr. Werner Hermann Wilhelm Schulz (May 30, 1909–August 22, 1984; Ph.D. Berlin, 1937; advisors Erhard Schmidt, Schur, and Bieberbach) joined In 7/IV in May 1940. After In 7/VI was established at the beginning of 1941, Dr. Schulz was transferred to it on March 31, initially placed in Referat 1 (General Cryptanalysis), and was part of a group that worked unsuccessfully on attacking the Typex. He made a significant theoretical contribution to its analysis, however, being "instrumental in solving, theoretically, the problem of how the internal settings had to be in the machine" (GCCS, 1945b). But by the Fall In 7/VI had effectively given up on the Typex (absent knowledge of the wiring of its wheels), and Schulz was transferred to Referat 2 (the English section, headed by Senior Inspector Zillman) on September 11, 1941. His work was presumably viewed favorably: he was promoted to Sonderführer (Z) on October 1, 1941 (along with Steinberg and Pietsch); and then Unteroffizier

[69]The Föppls were members of a remarkably accomplished family. Ludwig's father August Otto Föppl (1854–1924) was a Professor of Mechanics and Statics at the Technical University of Munich; he is known for the *Föppl-von Kármán equations*, and is thought to have had some influence on Einstein's early views on special relativity. He had only three graduate students, but one of them—the applied mathematician and engineer Ludwig Prandtl (1875–1953)—more than made up for this: the MGP lists Prandtl as having 87 students and 3721 descendants. Ludwig Föppl's brother Otto Föppl (1885–1963) was an engineer and Professor of Applied Mechanics at the Technical University of Braunschweig for 30 years. Both Otto and his sister Gertrud were closely connected with Prandtl: Otto was his assistant from 1909 to 1911, and Gertrud became his wife. Ludwig's grandson Martin Samuels received a Ph.D. in Military Studies from the University of Manchester, has had a career in the British public service, and is the author of (Samuels, 2016).

on April 1, 1942. He later headed the Middle Eastern desk of the English Referat during the period 1942–1944, and eventually succeeded Inspector Zillman as head of the Referat itself (this likely by the end of 1943). He may have been the best man in the English section. At the end of the war he headed the department of the GdNA devoted to English, US, and Swedish systems.[70]

The initial part of Dr. Schulz's postwar career was somewhat unusual. He had earlier married Erika Buth in 1938 and (according to the 1939 Berlin address book) lived at Zinsgutstrasse 56 in the Adlershof district of Berlin (the significance of the address will become apparent shortly). In the very last days of the war Schulz was likely relocated with his team to the southern part of Germany (and therefore separated from his wife). The *Kurzbiographien* tells us that after the war, he initially lived with family ("mit Familie") in Laubach and Frankfurt, both in the Western (Allied) zone of Germany, where presumably he or his wife had relatives. In July 1946 he received permission to return to Berlin and may have moved back to his Adlershof home, which was now in the Soviet sector. But his move back to Berlin, perhaps to rejoin his wife, proved to be a serious mistake. On July 15 he had begun to work for GEMA (the *Gesellschaft für elektroakustische und mechanische Apparate mbH*, the Corporation for Electro-Acoustical and Mechanical Equipment) as a member of its scientific staff. The Soviet Military Administration for Germany had taken over GEMA immediately after the war, and within just a few months of his arrival in Berlin Dr. Schulz moved, presumably on the orders of the Soviet authorities (one source refers to him as being in Soviet custody), to Ostaschkow (near Kalinin) in the USSR, working there for nearly six years as a specialist on ballistics research (October 1946–June 1952). He was released from these duties in June 1952, and returned to Germany and a position at the German Academy of Sciences in the GDR starting in September. But he had clearly had enough of life in the East, and almost immediately contrived to obtain a position at the *Deutsche Forschungsanstalt für Luftfahrt* (German Research Institute for Aviation) in Braunschweig in the West, at its new *Institut für Flugmechanik*. (He wisely decided to move to the West while this was still possible. Family reunification was one way to do this legally, but it was also possible in those days simply to walk from East to West Berlin.) After this happy move he went on to enjoy a highly

[70]The information in this paragraph about Dr. Schulz's time in In 7/VI is largely drawn from entries in the In 7/VI *Kriegstagebuch*.

successful career in aviation research, eventually becoming a section leader at the Institute and even serving at one point as acting director of the Institute itself, as well as becoming the editor of the *Zeitschrift für Flugwissenschaften* (the Journal of Aviation Sciences, a leading professional publication), and an honorary Professor at the Technical University of Braunschweig. He retired in 1974.

12.1.5 Dr. Hans Thunsdorff

As noted earlier, a number of the cryptologists in OKH/In 7/VI were drawn from the fields of statistics, economics, and the actuarial sciences. One particularly interesting example is that of *Dr. Hans Walter Thunsdorff* (August 5, 1907–December 14, 2000; Ph.D. Göttingen, 1932; advisors Felix Bernstein and Edmund Landau). Thunsdorff's thesis, *Konvexe Funktionen und Ungleichungen* (Convex functions and inequalities), although unpublished, contains a result which later became known as *Thunsdorff's inequality* and is still cited today. After receiving his doctorate he joined the *Verband Öffentlicher Lebensversicherer* (VOEL, Association of Public Life Insurance Companies), but never attained a senior management position in it because he was deemed to be "politisch unzuverlässig" (politically unreliable). In May 1940 In 7/IV attempted to recruit him (whether successfully or not is unclear), but he became a member of In 7/VI on April 8, 1942 and joined Referat 7 on April 28. He appears to have been permitted to continue to work at the same time for the VOEL. In early 1945 the VOEL instructed him to make a business trip to Dresden. Instead he chose to desert, going by train via Hamburg to Garding (in the Eiderstedt peninsula) where his wife and child (Peter, born 1943) had been evacuated. This had two immediate if unforeseen advantages: he both narrowly avoided the bombing of Dresden by one day, as well then being presumed dead by both the VOEL and OKH. After the war he continued on in life insurance, becoming Director-General of the *Provinzial-Lebensversicherung Hannover* in 1946; he moved to its Board of Directors when the company merged with another insurance company in 1957 to become the *Versicherungsgruppe Hannover*, currently the largest regional insurer in the German State of Niedersachsen, a position he held until his retirement in 1972. He also held important positions in professional life insurance organizations. In poor health for the last several decades of his life, he moved to Männdorf (in Switzerland) in 1963, and then lived in Weinheim an der Bergstrasse from 1976 until his death in 2000.

What Dr. Thunsdorff accomplished in In 7/VI during the war is unknown; an online family biography (Thunsdorff, 2011), however, states that

> Aus seinen späteren Erzählungen geht hervor, dass er—und wohl auch einzelne andere—wenn irgend möglich, die Entzifferungsvorgänge hintertrieben hat.

("From stories he later told it appears that he—and probably some others as well—had, when possible, thwarted the decipherment process.") This is not implausible: his wife Elfriede *née* Mollenhauer (October 29, 1902–July 8, 1994), whom he married in 1940, had been a member of a local KPD (German Communist Party) resistance cell until about 1937 (when she was questioned by the Gestapo but then released). She is one of the principal characters in the novel *The Package* (Dudley, 2011).

In contrast, a number of the wartime mathematical cryptologists were members of the NSDAP, but for a variety of reasons.

12.1.6 Professor Alfred Kneschke

Born of a relatively poor family, *Dr. Alfred Emil Richard Kneschke* (June 15, 1902–November, 24, 1979; Dr. Ing. Technical University of Dresden, 1927; advisors Georg Wiarda and Max Otto Lagally) seems to have advanced by virtue of hardwork. First *Privatdozent* in 1930 (that is, a lecturer paid directly by students) and then Professor at Dresden (1938), in 1939 Kneschke was drafted into the Army, and ended up working in OKH/Chi. He eventually headed Referat 2 (devoted to British, US, French, and Balkan systems), part of Group 4 (cryptanalysis) of the GdNA. Because of his membership in the NSDAP (he had also signed a letter of German professors supporting Hitler in 1933), he was dismissed from his state position in 1945, and so was initially unable to teach at a university. Nevertheless he eventually landed on his feet: in 1951 he became Professor at the *Technische Universität Bergakademie Freiberg* (the Freiberg University of Mining and Technology), heading its Institute of Applied Mathematics from 1953 to his retirement in 1967. During this time he supervised 7 students, and wrote several textbooks (including three-volume works on both differential equations and mechanics). He is mentioned on the websites of both the Technical University of Dresden and the *Bergakademie Freiberg*, the latter referring to him as a "wissenschaftlicher

Visionär und Vater des Freiberger Mathematik-Studiums" (scientific visionary and father of the Freiberg mathematics program). Neither mention the nature of his war work. Entries for him appear in both the *Kurzbiographien* and MGP.

12.1.7 Professor Helmut Grunsky

Dr. Helmut Grunsky (July 11, 1904–June 5, 1986; Ph.D. University of Berlin, 1932; advisors Bieberbach and Schur) became the editor of the *Jahrbuch über die Fortschritte der Mathematik* (a journal which published reviews of mathematical papers) in 1936, thanks to his advisor Bieberbach. But for several years he resisted pressure from Bieberbach to dismiss the *Jahrbuch's* Jewish reviewers (see Göbel, 2011, p. 6), and this led to his resignation from it on August 17, 1939; he then joined Pers ZS on September 3. Although he later applied for membership in the NSDAP (February 19, 1940), Siegmund-Schultze (2004) presents evidence that Grunsky tried to take the course of least possible accommodation with the regime. After the war, he was able (for the first time) to pursue an academic career, teaching initially at Tübingen in 1949, and later moving to Mainz and Wurzberg as Professor. He had seven Ph.D. students, all dating from his time at Wurzberg. In mathematics he is known for the *Grunsky inequalities* and *Grunsky's theorem.* For further information about Grunsky's life and career see Jenkins (1989) and Siegmund-Schultze (2004), as well as the entries in the *Kurzbiographien* and MGP. In Pers ZS he was part of the group that attacked the American strip cipher system.

12.1.8 Dr. Ralf Lohan

Dr. Herbert Ralf Lohan (October 5, 1902–August 10, 2000; Ph.D. University of Berlin 1935; advisors Klose and E. Schmidt) was born in Dresden, but his family later moved to Berlin where he grew up. Lohan's father was the author and editor Dr. Heinrich Max Lohan. In 1920 Heinrich committed suicide because of the extremely difficult economic conditions at that time ("Rumpelstilzchen", 1922). As a result, when Lohan graduated from the *Prinz-Heinrich-Gymnasium* in Berlin-Schöneberg in 1921, he did not immediately begin his university studies, but first worked instead at the *Deutsch-Südamerikanische Bank Aktiengesellschaft* in Hamburg and Berlin. In 1927 (one source says 1929) Lohan became a student at the University of Berlin,

and then went on to do graduate work there as well. He was apparently not a stellar student: he initially failed his oral examination in physics, but did go on to receive his doctorate in 1935.[71] He joined the SA in 1933 and the NSDAP in 1937. He never received his *habilitation* (permitting him to become a Privatdozent, and therefore teach); he began working at the Foreign Office (*Auswärtiges Amt*, AA) on September 8, 1939 and left it on December 31, 1941. Like some other members of Pers ZS such as Rohrbach and Ulm, he may have only worked part time while at the AA, but if so he appears not to have handled this appropriately: he was paid a salary by both the university and the AA, but the university discovered this and he was asked to reimburse his university pay. His biggest feat was to identify the cryptologic structure of the US B7 code (DF-15, p. 20); the work on this code is discussed in a declassified *NSA Technical Journal* article (Swift, 1960). After Lohan left the AA he started to work for the *Reichsgruppe Industrie*, probably in Berlin; in 1944 he was relocated to Munich. After the war Lohan was initially a POW of the British, but was released at the end of January 1946. During the decade from 1946 to 1955 he made a living as a journalist: first as head of the Munich office of the *Deutsche Pressedienstes* (the German Press Service), then as editor of the *Süddeutsche Zeitung* (a well known and respected newspaper, the first German newspaper to be published after the war) and later head of its Bonn office, and finally working as an independent publicist, including freelancing for the *Süddeutscher Rundfunk* (the South German Broadcasting Corporation). He eventually returned to the Foreign Office, however, serving at various points abroad in The Hague (Netherlands), Helsinki (Finland), Santiago (Chile), and Asunción (Paraguay), usually as a cultural attaché or legation councillor. He retired in 1967, and then settled in St. Augustin-Hangelar (near Bonn), where he became an active organizer in the Bonn chess scene. He died in 2000 at the age of 97.[72]

But perhaps the most surprising aspect of Lohan's life is something quite different. In 1936 he became the *Vorsitzender* (Chairman) of the *Ephraim Veitel Stiftung*, a foundation devoted to helping primarily Jewish students,

[71] Lohan's advisor was Hilda Pollaczek-Geiringer, the later wife of Richard von Mises. Both Geiringer and von Mises left Germany in 1933 when the Nazis came to power, and so it was necessary to replace Geiringer with the pro forma advisors Klose and Schmidt.

[72] We owe some of the information contained in this paragraph, including the reference to "Rumpelstilzchen", Hilda Geiringer's role as Lohan's advisor, and a CV originating with the German Foreign Office, as well as useful background, to the generosity of Professor Dr. Ingo Althöfer of the Friedrich-Schiller-Universität Jena.

established at the beginning of the nineteenth century thanks to a bequest by Frederick the Great. Under Lohan the name of the foundation was changed to the "1803 Foundation", and its beneficiaries had to be German (Aryan) youth. This was hardly surprising in 1936, but what is surprising is that after the war this state of affairs was permitted to persist until the death of Dr. Lohan *fifty-five years later* in 2000. After that the name of the foundation reverted to its original, as did its mission. The foundation is discussed, together with considerable information about the life of Dr. Lohan, in Grözinger and van der Linden (2009); see also the foundation webpage `http://www.ephraim-veitel-stiftung.de/` (accessed December 8, 2018).

Other members of Pers ZS were either actively hostile to the Nazis or (at least apparently) apolitical, and – like Rohrbach, Köthe, and Grunsky – went on to have relatively successful academic careers after the war. These include:

12.1.9 Dr. Helmut Ulm

Except for the war years, *Dr. Helmut Ulm* (June 21, 1908–June 13, 1975; Ph.D. University of Bonn, 1933; advisor Otto Toeplitz) spent virtually his entire career at the University of Münster (1935–1974). The initial part of his career suffered because of his opposition to the Nazis: he only received his habilitation in 1935, only began lecturing at Münster in 1938, and was only promoted to *Außerordentliche* (Associate) Professor in 1947. He began to work for Pers ZS in August of 1941, but even then not on a full time basis: beginning in December he worked in Berlin Thursday through Saturday, and then taught Monday through Wednesday at Münster. But working in Pers ZS was apparently not viewed as vital to the war effort, and Ulm was later drafted by the Army (November 1942) and sent to the Crimea. It was presumably there that he caught malaria; he was sent back a year later to work in the *Reichluftfahrtministerium* (Ministry of Aviation). Immediately after the war Behnke intervened on his behalf; at first Ulm gave mathematics lectures to English officers, and then resumed teaching at Münster in 1947. His health was never good from this point on and, although he taught a wide variety of courses over the years, he wrote almost nothing and had only six students. Before the war, however, he had written three papers about the theory of infinite abelian groups which are highly regarded today, and he is known in that field for *Ulm's theorem*. The definitive source for the facts

of his life is Elstrodt and Schmitz (2013, pp. 307–310); Ulm's mathematical work (and a brief summary in English of his life) is described in Göbel (1989).

12.1.10 Dr. Rudolf Kochendörffer

Another example of a mathematician who, like Ulm, started out working in Pers ZS but ended up in In 7/VI is *Dr. Rudolf Paul Joachim Kochendörffer* (November 21, 1911–August 23, 1980; Ph.D. University of Berlin, 1937; advisors Erhard Schmidt, Schur, and Bieberbach). After the outbreak of war, he joined Pers ZS, but was drafted into the Army in 1942, initially trained as a radio operator, and then transferred to OKH, where he again worked on deciphering in In 7/VI. An algebraist by training, in Pers ZS he wrote a paper on how the wiring and turnovers of the wheels of the commercial Enigma could be deduced given a sufficient number of depths (translated in DF-38); in In 7/VI he was part of the group that worked on the M-209. At the end of the war he lectured in Berlin (1946–7), moved to Greifswald in 1948, and then Rostock in 1950 (both of these were in the GDR). At Rostock his career was largely administrative (Dean, 1951–1954, Vice Rector for Research, 1956–1960); he had only four Ph.D. students. Somewhat surprisingly, he was permitted to leave the GDR: after visiting Adelaide from 1964 to 1966, he moved first to Mainz in 1968 and then Dortmund in 1970 (both in the FRG), where he remained until his retirement in 1977. The general impression is that he performed competently (but no more) in his cryptological work, consistent with the arc of his post-war career. For further information about his life and mathematical contributions, including confirmation of his wartime work in Pers ZS and OKH, see Wehefritz (1985, pp. 7–40).

12.1.11 Professor Karl Schröter

Immediately after receiving his degree, *Dr. Karl Walter Schröter* (September 7, 1905–August 22, 1977; Ph.D. University of Münster, 1941; advisor Heinrich Scholz) joined Pers ZS on April 1, 1941. EASI 6, p. 17 lists him as "working independently on Japanese additive and encipherment systems", and "head of a group under Dr. Kunze in the spring of 1945". (These Japanese systems would have been enciphered diplomatic codes such as J-19, called Fuji by Japan and J.B.57 by the Germans. Only a handful of important embassies had the Purple machine, all other diplomatic communications used a variety of enciphered codes.) Schröter was part of a group of

twenty-one Pers ZS cryptographers who were interrogated in London in seven meetings from May 9 to May 21, 1945; see I-22 (for specific information on what Schröter did, see I-22, p. 17). After the war Schröter had a very successful career: Associate Professor at the Humboldt University of Berlin (GDR) in 1948, member of the *Deutsche Akademie der Wissenschaften zu Berlin* (Germany Academy of Sciences) in 1962, and Director of the Academy's Institute for Pure Mathematics in 1967. He was also a founding editor in 1955 of the *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* (the *Journal of Mathematical Logic and Foundations of Mathematics*, later renamed the *Mathematical Logic Quarterly*). The MGP lists him as having 16 students and 224 descendants; he also appears in the *Kurzbiographien*. For further details of his life and work, see Elstrodt and Schmitz (2013, pp. 295–296).

The *Jahrbuch* and *Zentralblatt* Several of the In 7/VI and Pers ZS mathematicians were linked by being on the staff of the *Jahrbuch über die Fortschritte der Mathematik* prior to the outbreak of war (Grunsky, Pannwitz, Pietsch, Rinow, Kochendörffer, and Dueball). The *Jahrbuch* was the oldest of the mathematical review journals, founded in 1868; it was published annually under the sponsorship of the *Preußische Akademie der Wissenschaften* (Prussian Academy of Sciences); its editor Ludwig Bieberbach. A competing publication, the *Zentralblatt für Mathematik und ihre Grenzgebiete* was founded by Springer-Verlag in 1931; this was published more frequently than the *Jahrbuch* and, unlike it, accepted reviews in languages other than German. After the war the *Jahrbuch* ceased publication (its last issue came out in 1942), but the *Zentralblatt* resumed publication in 1947 under the management of the (East) German Academy of Sciences (the *Deutsche Academie der Wissenschaften*, the successor to the prewar Prussian or Berlin Academy). The *Zentralblatt* continues to be published up to the present, under the shortened title *Zentralblatt MATH*. For further information on the two publications, see Siegmund-Schultze (1993), Göbel (2009 and 2011).

After the war several members of the prewar *Jahrbuch* staff (Pannwitz, Pietsch, and Dueball) went on to work for the German Academy of Sciences ("Academy") and became members of the editorial staff of the *Zentralblatt*. The most important of these members was Dr. Erika Pannwitz.

12.1.12 Dr. Erika Pannwitz

Dr. Erika Pannwitz (May 26, 1904–November 25, 1975; Ph.D. University of Berlin, 1933; advisors Heinz Hopf and E. Schmidt) was on the staff of the *Jahrbuch* from 1930 to 1940; she left to become a member of Pers ZS in 1940, remaining there until the end of the war in 1945. After the war and with the demise of the *Jahrbuch* she moved to the *Zentralblatt*, eventually becoming its editor-in-chief from 1953 to 1964. Because she lived in West Berlin but the central office of the *Zentralblatt* was in the Eastern sector, this required special permission from the *Volkspolizei* in order for her to commute to work. The GDR had a mandatory retirement age of 60, however, and so in 1964 she relocated to the West Berlin office of the *Zentralblatt*, where she remained until her actual retirement in 1969. Despite the fact that she had written an outstanding thesis (graded "opus eximium", comparable to summa cum laude, and published in the prestigious *Mathematische Annalen*), Pannwitz never held a regular academic position; there may have been some element of discrimination here because of her gender or politics or both (see Vogt, 1999). Her *Zentralblatt* obituary was written by her Pers ZS colleague Gottfried Köthe (1976). There are entries for her in both the *Kurzbiographien* and MGP.

Of Pannwitz's two post-war colleagues at the Academy, we have already discussed Dr. Pietsch. About her other colleague at the Academy, Dr. Fritz Dueball, somewhat more can be said about his pre- and postwar life.

12.1.13 Dr. Fritz Dueball

Like his Pers ZS colleagues Grunsky and Ulm, *Dr. Fritz Emil Maximilian Dueball* (February 19, 1909–June 5, 1990; Ph.D. University of Berlin, 1937; advisors Bieberbach and E. Schmidt) also fell afoul of the Nazis, but in a much more serious way: in 1937 he was placed in pretrial detention (*Untersuchungshaft*) for high treason. He was imprisoned at Plötzensee, a rather grim place, from July 26, 1937 until November 19, 1937, after which he was released. The court records state the case for high treason was a case against a "Springer and others". The Springer in this case does not refer to Ferdinand Springer (the publisher, who had his own problems with the regime) but to an office employee named Robert Springer. The other people named in the case were a salesman, Werner Richard Franz Müller,

and an engine fitter, Walter Herz. Springer, Müller, and Herz were part of a small Trotskyite group in Berlin that Dueball came in contact with through a Jewish girl friend, Friedel Löwenstein. Ms. Löwenstein was a part of the group (she would unquestionably have been charged as well, but died earlier in a car accident in either 1935 or 1936); on one occasion she brought along Walter Herz to one of her meetings with Dueball; and later Dueball met via her both Robert Springer and two other people named Gustave Stern and Suse Chozen.[73] Even if, as appears likely, Dueball had some sympathy for the Left and their ideas, he was more or less apolitical and in fact did not like Ms. Löwenstein bringing these other people to meetings he wanted to have with her alone. His interest seems to have been in her as a person and woman, and not in her political ideas. In any case, because she was dead when the case came to trial, Dueball was able to play down both the relationship he had had with her and his connection to the other people in the Trotskyite group. He even claimed he was unaware Friedel Löwenstein was Jewish or that Löwenstein was a Jewish name. It is hard to imagine the judges bought this story, but apparently Dueball managed to present himself as a kind of unworldly professor type who had no interest in politics or other more worldly interests, and lived mainly for his scientific studies and research. It is clear that in the end the judges looked upon him as an unlucky fool who got mixed up in something he did not quite understand, and therefore were very lenient towards him and his dealings with the others. (They were not so lenient with Dueball's codefendants, however, all of whom received substantial prison sentences and two of whom died while in custody: Springer and Herz were murdered in 1942, but Werner Müller (1899-1990) was lucky and survived the war.[74])

In addition to working for the *Jahrbuch* for three years prior to the war, the records of the postwar Academy indicate that after the war Dueball was employed there until 1966, first at the Research Institute for Mathematics until 1958, and then from 1959 to 1966 at its successor, the Institute of Pure Mathematics. The only indication of what he did at Pers ZS during the

[73]Stern's first name appears as Gustav in the court records, but there is no question that this is in reality Gustave Stern (1914–1988), also known as Gérard Sandoz. He escaped via Denmark to France where after the war he became one of the leading French experts on Germany. Much later he wrote an autobiography, *Gérard Sandoz: Ein Leben für die Verständigung* (Sandoz, 1990). See also Sandvoß (1996, pp. 95–98).

[74]For further information on Walter Herz, see Humboldt-Universität zu Berlin (2010, pp. 23–26).

war is a paper he wrote for their in-house journal on "Anzahlbestimmungen spezieller Permutationen" (Determining the number of special permutations), in the issue of the journal for May 26, 1942. But perhaps the most interesting aspect of Dueball's life, however (apart from his prewar legal difficulties of course), is one that has nothing to do with either mathematics or cryptology. His father, Felix Dueball (March 20, 1880–October 8, 1970) helped introduce the Japanese game of Go to Germany and by the 1920s was the best player in Germany. Fritz Dueball was also a talented Go player: he won a major Go tournament in 1938, and the official European Championships in 1957, 1958, and 1959. Fritz's son Jürgen Dueball (April 17, 1943–October 15, 2002) was both a strong Go player (5-Dan) and a strong chess player (holding the title of International Master). There are entries for Fritz Dueball in both the *Kurzbiographien* and MGP. For a photograph of both Dueball and Pannwitz, see Göbel (2011, p. 11).[75]

12.2 Identification of individuals

We encountered a number of challenges in identifying some of the individuals in our study. One annoyance is that very often in TICOM documents only the last name of an individual is given.[76] In some cases this means that more than one candidate can be found, and even when there is only one, it remains to establish that the plausible candidate is indeed the person being referred to. In some cases this is easy to do: for example, an obituary notice might briefly allude to the person's wartime service.

Another challenge is that the use of the term "mathematician" by the German cryptologic organizations was often very broad and included people such as school mathematics teachers. This term is also often used to refer to actuaries and insurance mathematicians, some of whom were indeed top people, but who rarely appear in the Mathematical Genealogy Project or the *Kurzbiographien*. These professionals had their own societies such as the German Actuarial Association (*Deutsche Aktuarvereinigung*, the DAV); see, e. g. `https://aktuar.de/Seiten/default.aspx` (accessed December 8, 2018) and `https://de.wikipedia.org/wiki/Deutsche_Aktuarvereinigung` (accessed December 8, 2018). Unfortunately these groups do not appear to

[75]The information relating to the 1937 legal proceedings against Dueball is taken from contemporary court records, copies of which were kindly provided to us by Claus Taaks.

[76] It is interesting to note that even Dr. Buggisch did not know the first names of many of the top cryptanalysts in OKH and OKW; see I-176, pp. 6–10.

have compiled similar biographies of their members. True, a few books have been written about the history of German insurance mathematics such as Peter Koch's *Geschichte der Versicherungswissenschaft in Deutschland*; this last mentions many of the main actors but does not attempt to give any personal histories or biographies of these individuals.

There are also sometimes outright errors in the TICOM documents themselves. I-31, for example, refers to a "Dr. Aigner (mediziner)", but this cannot be right: Dr. Franz in DF-176 specifically identifies Dr. Aigner as Dr. Alexander Aigner of Graz. For a short biography of Aigner, see Franz Halter-Koch, "Alexander Aigner", *Nachrichten der Österreichischen Mathematischen Gesellschaft*, Nr. 181, August 1999, pp. 75-77. This memorial notice confirms (p. 75) Aigner's service in OKW/Chi: "war während des Krieges unter anderem bei der Dechriffrierabteilung der Wehrmacht in Berlin tätig" (was active during the war, among other things, in the Decipherment Department of the Wehrmacht in Berlin).

12.2.1 Werner Schulz

The identification of the mathematician Dr. Werner Schutz appearing in the TICOM documents with the mathematician in the *Kurzbiographien* provides a simple and straightforward example. It is based on the following considerations: there is only one mathematician with this name listed in the *Kurzbiographien*; one of his advisors was Ludwig Bieberbach, the majority of whose doctoral students in the late 1930s went into signals intelligence; he joined In 7/IV in May 1940 (as recorded in the In 7/IV *Kriegstagebuch* for May 1–31, 1940), consistent with the statement in the *Kurzbiographien* of war service beginning on May 1, 1940; and finally HW 40–89 (GCCS, 1945b) records he was an instructor in Berlin "of age about 30", again consistent with the information in the *Kurzbiographien*.

12.2.2 Hermann Föppl

An interesting but more complex example is the identification of Hermann Föppl. He is only listed in the *Kriegstagebuch* of In 7/VI, Section 7 for August 1942 as "Gefr. Föppl", and one might at first suppose that this was his father Ludwig, returned yet again to service. But on closer examination there are no fewer than four reasons why this cannot be the case: this Föppl is listed without the title of Dr. (unlike Fricke, Döring, and Buggisch); is listed as a

"Gefr." (that is, a *Gefreiter* or Lance Corporal) even though Samuels (2016, p. 368) tells us that Ludwig held the rank of Lieutenant; is listed as having received the *Ostmedaille* (an award for service on the Eastern Front during the Winter 1941–42 campaign), inconceivable for a distinguished Professor in his 50s; and is listed as taking an elementary course in cryptography when he came to In 7/VI. On the other hand, information from Hermann Föppl's family (frostbite severe enough to ensure he was awarded the Ostmedaille, hospitalization into 1942, and working in a code-breaking group in Berlin) all make it possible to identify "Gefr. Föppl" as the later Dr. Hermann Föppl of the Max Planck Institute for Extraterrestrial Physics.

12.2.3 Case Study: Harry Welsch

The case of *Funker* Harry Welsch provides a particularly good illustration of the challenges that can arise in attempting to identity some individuals. During the war Welsch worked as a cryptographer for In 7/VI. It is easy to establish from the available In 7/VI records that he was a codebreaker and cryptanalyst, and that he had considerable mathematical knowledge, but in what sense was he a "mathematician" (as the records indicate)? As noted earlier, the term mathematician had a very broad meaning for the personnel officers of In 7/VI. So when the records say Welsch was a mathematician, this in fact tells us very little about his formal mathematical education, his actual mathematical ability, or his past mathematical experience.

We do not know from the In 7/VI records (specifically, their war diary or *Kriegstagebuch*) when he was born, but as he undoubtedly had a higher education, possibly at the university level, it is reasonable to suppose he was at least twenty years old when he started working for In 7/VI. He joined Referat 1 (General cryptanalysis) on April 3, 1941 with the military grade of *Funker* ("Radioman", a rank at the level of private). This might mean he had earlier been drafted into the Army and already seen military service, but it could also mean he had been selected for signals intelligence right from the start.

Harry Welsch remained in Referat 1 less than a month: on April 24, 1941 he was transferred to Referat 3, the French section, which was located at Matthäikirchplatz 4 under the leadership of Senior Inspector Hans Wolfgang Kühn. What he specifically did in Referat 3 is unknown but the section was working on French diplomatic codes and Swiss commercial Enigma messages. But then Harry Welsch fell ill. We do not know what kind of illness he suffered

from, but it was apparently serious because he was repeatedly on sick leave: from May 29 to August 25 (hospitalized), September 25 to October 3, and November 5 to 16. After this he appears to have fully recovered, for there are no more reports of him being away from work due to illness for the rest of the year.

On January, 1942 then *Gefreiter* Welsch was promoted to the civilian grade *Sonderführer* (G), equivalent to a non-commissioned officer (NCO).[77] Given the considerable length of time he had been away due to illness, this promotion seems very rapid and likely indicates he must have been doing quite well in his cryptanalytical work. His new responsibilities appear to have included the security of the Enigma. On January 17 and 19, 1942 there was a conference in Referat 7 on the security of the Enigma, which Kühn, Buggisch, and Welsch from Referat 3 attended. Then there is no further word about Welsch before he went on vacation June 15-30. Once again we do not know what his duties were during this period, but he must have again performed well because on November 1, 1942 he was promoted to Unteroffizier.

On April 13, 1943 a special research section was created for In 7/VI, Referat F (*Forschung*, Research). By May 31, 1943 it consisted of nine people, including von Denffer (its leader), Rinow (his deputy), the insurance mathematicians Wünsche and Hilburg, and a Dr. Kühnel of whom we know very little. (In January 1942 Kühnel was a member of Referat 7 and it therefore seems likely that he was either a statistician or insurance mathematician.) And then we have Harry Welsch listed. The fact that he was included in this section of mathematically trained specialists is yet another indication that he had mathematical abilities well above the average. (There were also three other newly recruited members about whom we know nothing, not even their first names: Apel and Bringmann (both rank of *Gefreiter*) and Diehl (rank of *Funker*), who must also have been mathematicians or at least people with very good mathematical knowledge.)

[77]The Sonderführer, or "Special Leader" was a rank given to civilians with special skills (for example, in medicine or foreign languages) who were drafted into the Wehrmacht in order to capitalize on such expertise. Such individuals were usually not trained as soldiers and did not enjoy (until 1942) either the power of command or discipline that officers of standard military rank did. There were different ranks of Sonderführer; for example, a Sonderführer (Z) was equivalent to the standard military rank of either Leutnant or Oberleutnant (NATO rank OF-1); a Sonderführer (G), Welsch's rank, was equivalent to that of an Unteroffizier (OR-4).

But what about Harry Welsch, what is he doing? That is the problem: Welsch seems to fall below the radar almost everywhere. His name appears infrequently in the In 7/VI reports and he also appears to be completely absent from the post-war TICOM reports. It is almost as if he had never existed. Almost, because he did leave one significant trace, a report he wrote on January 12, 1944 entitled "Aktennotiz zum Tiefenproblem bei der Enigma" (Note on the problem of depth in the Enigma). The mathematics in this paper makes it apparent that he had a considerable knowledge of probability and statistics. (For example, he refers to and uses Poisson's formula, an important approximation in mathematical probability theory.)[78]

Thus, although we know a bit about Welsch during the war based on the information in the In 7/VI *Kriegstagebuch*, enough to conclude that he was a mathematician of some ability, we otherwise know absolutely nothing about him either before or after the war. And here the matter might have remained, save for a chance footnote in an obscure German government publication (Rademacher and Szenzenstein, 1984, p. 868), referring to a "Dipl–Math Harry Welsch" who had worked in Germany's *Statistichen Bundesamt*. This might still have been a dead end however (because this organization does not retain records of their employees after the age of 70), but an inquiry to the *Bundesarchiv* (German Federal Archive) led to a copy of Welsch's personnel file ("Personalakte"), containing a considerable amount of information about Welsch before, during, and after the war, including confirmation that he is indeed the In 7/VI cryptologist in question.

His life in brief: Harry Welsch (January 28, 1920–?), a life-long Berliner, received his *Arbitur* (a high school degree qualifying one to attend university) in March 1938, after studying eight years at the Prinz-Heinrichs-Gymnasium. After serving a mandated six months in the *Reichsarbeitsdienst* (RAD, State Labor Service), in November 1938 he became a student at the University of Berlin. But shortly before the war (July 13, 1939) Welsch joined the Foreign Office, becoming "part of a research group in which statistical and probabilistic methods were developed for their deciphering service" (that is, Pers ZS). But if he thought this would shield him from military service, he was wrong: On October 2, 1940 he entered the Army (presumably drafted, like Kochendörffer and Ulm) and after basic military training was posted to

[78]The sources for the above information in this section are documents from the TICOM files T2755–T2767 in the TICOM collection at the German Foreign Office, Bestand Rückgabe TICOM, Politisches Archiv des Auswärtigen Amts, Berlin.

OKH, where he worked on "problems similar to those in the Foreign Office" (that is, cryptanalysis). He remained there until Germany's capitulation in May 1945.

But after the war Welsch was unable to return to the University of Berlin and his mathematical studies. His parents were tailors with a large business, and when his father died in 1946 Welsch had to join it (the "Modesalon Welsch"), serving as a managing director and remaining there for sixteen years (1946–1962). But he was eventually able to resume his mathematical studies at the Free University of Berlin in 1957 (at first part time), held an assistantship there from 1963 to 1966, and was then able to concentrate on his studies, receiving his *Diplom* in mathematics from the University on December 2, 1969. With this degree he was able to begin working for the German government, first at the *Bundesaufsichtsamt für Versicherungs und Bausparwesen* (the Federal Supervisory Office for Insurance and Building Savings) from April 1, 1970 to April 30, 1971, and then at the *Statistischen Bundesamt* beginning on May 1, 1971. We do not know at this point when Welsch retired or died.

12.3 TICOM reports

The following is a list of the different TICOM reports referred to in this paper:

I-2: "Interrogation of Dr. Hüttenhain and Dr. Fricke at Flensburg 21 May 1945."

I-12: "A translation of the preliminary interrogation of Orr. Tranow of 4 SKL/II OKM, carried out at Flensburg on 24/25 May 1945 by TICOM Team 6."

I-15: "Interrogation report of Oblt. Schubert."

I-20: "Interrogation of Sonderführer Dr. Fricke of OKW/Chi (formerly of OKH/Chi)."

I-21: "Preliminary interrogation of Oberst Kettler, R.R. Dr. Hüttenhain, Sdf. Dr. Fricke (OKW/Chi) and Oblt. Schubert (OKH/Chi) 15th June 1945."

I-22: "Interrogation of German cryptographers of the 'Pers ZS' Department of the Auswärtiges Amt."

I-26: "Interrogation of Oblt. Schubert (OKH/Chef HNW/Gen. d. NA.) on Russian military and agents' systems."

I-31: "Detailed interrogations of Dr. Hüttenhain, formerly Head of Research Section of OKW/Chi, 18th - 21st June, 1945."

I-36: "Translation of paper written by Reg. Rat. Dr. Hüttenhain and Sonderführer Dr. Fricke on the development of OKW/Chi, Sections A.III and B.V."

I-38: "Report on interrogation of Lt. Frowein of OKM/4 SKL III, on his work on the security of the German Naval four-wheel Enigma."

I-39: "Organisation of OKW/Chi."

I-45: "OKW/Chi cryptanalytic research on Enigma, Hagelin and cipher teleprinter machines."

I-46: "Preliminary report on interrogation of Wachtmeister Dr. Otto Buggisch (of OKH/Gen. d. NA) and Dr. Werner Liebknecht (employed by OKH and OKW as tester of cryptographic equipment). 23 June 1945."

I-58: "Interrogation of Dr. Otto Buggisch of OKW/Chi."

I-60: "Further interrogation of Oblt. Schubert of OKH/Chef HNW/Gen.d.NA."

I-63: "Interrogation report on ORR Hermann Scherschmidt of Pers. Z. S., Auswaertiges Amt."

I-64: "Answers by Wm. Buggisch of OKH/Chi to questions sent by TICOM."

I-66: "Paper by Dr. Otto Buggisch of OKH/In. 7/VI and OKW/Chi on Typex."

I-67: "Paper by Dr. Otto Buggisch of OKH/In. 7/VI and OKW/Chi on cryptanalytic machines."

I-77: "Translations of joint report made by Drs. Hüttenhain and Fricke on the "Zaehlwerk" Enigma machine."

I-78: "Interrogation of Oberstlt. Mettig on the history and achievements of OKH/AHA/In 7/VI."

I-89: "Report by Prof. Dr. H. Rohrbach of Per ZS on American strip cipher.

I-92: "Final Interrogation of Wachtmeister Otto Buggisch (OKH/In 7/VI and OKW/Chi)."

I-79: "Supplementary paper by Drs. Hüttenhain and Fricke on the solution of the Hagelin machine."

I-113: "Interrogation of Major Dr. Rudolf Hentze Head of Gruppe IV (Cryptanalysis), General der Nachrichtenaufklärung."

I-115: "Further interrogation of Oberstlt. Mettig of OKH/Chi on the German wireless security service (Funküberwachung)."

I-118: "Joint reports by Reg. Rat. Dr. Hüttenhain and Sdf. Dr. Fricke, written at CSDIC on or about 28th August, 1945."

I-120: "Translation of homework by Obltn. W. Werther, Company Commander of 7/LN.Rgt. 353, written on 12 August 1945 at ADI(K)."

I-121: "Translation of homework by Obltn. W. Werther, Company Commander of 7/LN. Rgt. 353, written on 12th August, 1945 at A.D.I.(K)."

I-124: "Interrogation report on Dr. Werner Weber of OKW/Chi."

I-137: "Final report written by Wachmeister Otto Buggisch of OKH/Chi and OKW/Chi."

I-143: "Report on the interrogation of five leading Germans at Nuremberg on 27th September, 1945".

I-150: "Report by Uffz. Heinz Beyreuther on the organisation of OKW/Chi."

I-172: "Interrogations of Hagen and Paschke of Pers ZS."

I-176: "Homework by Wachtmeister Dr. Otto Buggisch of OKH/Chi and OKW/Chi."

I-200: "Interrogation of Min. Rat. Wilhelm Fenner of OKW/Chi."

I-202: "Interrogation of Min. Rat. Viktor Wendland of OKW/Chi."

I-204: "Preliminary interrogation report of former Regierungsbaurat Johannes Marquart of OKH/Gen d NA."

I-208: "Interrogation report of Kurt Selchow, former head of the Pers ZS Department of the German Ministry of Foreign Affairs."

I-206: "Extracts from homework written by Min. Rat. Wilhelm Fenner of OKW/Chi."

I-211: "Preliminary interrogation of Dr. Hans Peter Luzius of OKH/In 7."

IF-5: "Notes on field interrogation of various German Army and Air Force SIGINT personnel 18-20/5."

IF-107: "Report of interrogation of Werner K. H. Graupe."

IF-108: "The German Signals Service."

IF-175: "The Signal Intelligence Service of the German Luftwaffe ["The Seabourne Report"], Volume 13: Cryptanalysis within the Luftwaffe SIS."

IF-176: "The Signal Intelligence Service of the German Luftwaffe ["The Seabourne Report"], Volume 3: Operations and Techniques of the Radio Defense Corps, German Wehrmacht."

D-60: "Miscellaneous papers from a file of RR Dr. Huettenhain of OKW/Chi.

DF-8: "Captured Wehrmacht SIGINT document. Statement of Order of Battle of OKW/Chi based on document dated April 1945."

DF-15: "Reports of Group A. Folder of reports and studies by the American Group of the Cryptanalytic Section of the German Foreign Office, 1919–1942."

DF-38: "The Enigma by Dr. Rudolph Kochendörffer."

DF-111: "Comments on various cryptologic matters by Adolf Paschke."

DF-120: "Report on the solution of messages in depth of the American cipher device M-209."

DF-176: "Answers written by Professor Doctor Wolfgang Franz to questions of ASA Europe."

DF-187: "The career of Wilhelm Fenner with special regard to his activity in the field of cryptography and cryptanalysis."

DF-187A: "Organization of the Cryptologic Agency of the Armed Forces High Command, with names, activities, and number of employees together with a description of the devices used."

DF-187B: "The cryptanalytic successes of OKW/Chi after 1938."

DF-187C: "Relations of OKW/Chi with other German Cryptologic Bureaux."

DF-187D: "Relations of OKW/Chi with Foreign Cryptologic Bureaux."

DF-187E: "Comments by Fenner on the Austrian Cryptologic Bureau and former German colleagues."

DF-187F: "Remarks made by Ministerialrat Fenner in reply to certain questions of a general nature."

DF-187G: "Replies by Ministerialrat Fenner to questions regarding cryptologic matters."

Many of these were released by the NSA to the US National Archives and Records Administration in April 2011; these are in Record Group 457. In some cases the reports are in the National Archives of the United Kingdom. Many are available on internet websites, notably:

- chris-intel-corner.blogspot.com (accessed December 8, 2018)
- www.ticomarchive.com (accessed December 8, 2018)

Acknowledgements

The authors thank the families of Fritz Dueball and Hermann Föppl for information about these two cryptologists; Dr. Claus Taaks for providing copies of the court records of the 1937 Dueball trial; Dr. Ingo Althofer for sharing information about Ralf Lohan; René Stein and Robert Simpson of the National Cryptologic Museum in Maryland for providing us both with documents about Wilhelm Fenner and copies of papers in the David Kahn Collection; Dr. Gerhard Keiper of the *Politisches Archiv des Auswärtigen Amts* in Berlin for supplying information about several individuals who had worked in Pers Z; Dr. Carsten Lind of the University of Marburg Archive for information about Rudolf Schauffler; Mario Aschoff of the University of Halle-Wittenberg Archive for information about Werner Kunze's doctoral studies there, and the Heidelberg University Archives for information about Kunze and Horst Schubert. Thanks also to Klaus Schmeh for the assistance of his blog (and one of its readers, Thomas Bosbach) in tracking down the postwar careers of Heinrich Döring and Harry Welsch. Special thanks go to the Departmental Historian of GCHQ and indirectly the Director of GCHQ for agreeing to discretionary disclosure of the TICOM report I-31 prior to its public release. We are also grateful to James Reeds, Reinhard Siegmund-Schultze, and Ralph Erskine for many helpful comments on an initial draft of the manuscript. The first author would like to especially thank the staff of the *Politisches Archiv des Auswärtigen Amts* in Berlin whose arrangements and friendly help made his research there a great success.

About the authors

Frode Weierud is a retired electronics engineer formerly employed by the European Organization for Particle Physics (CERN) in Geneva. Cryptography has been his main interest for close to 50 years. His cryptological research is focused on cipher machines and cryptanalytical techniques combined with a deep interest in all historical aspects.

Sandy Zabell is a Professor of Mathematics and Statistics at Northwestern University. In the past his historical research on cryptology focused on the use of probability and statistics, and in particular their employment by Alan Turing during World War II, as well as currently on German cryptologic efforts during the war.

References

For all TICOM reports, see Section 12.3 in the Appendix above.

Alvarez, D. 1996. Diplomatic solutions: German Foreign Office cryptanalysis, 1919–1945, *International Journal of Intelligence and Counterintelligence*, 9(2): 169–185.

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

Army Security Agency. 1946. European Axis Signal Intelligence in World War II, Washington, DC. Nine volumes, cited throughout as "EASI". Available online at `https://www.nsa.gov/news-features/declassified-documents/european-axis-sigint/` (accessed June 20, 2018).

Bamford, J. 2001. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Doubleday.

Bauer, F. L. 1997. *Decrypted Secrets*. Berlin: Springer-Verlag. Fourth ed. 2007.

Bauer, F. L. 2008. Dr. Erich Hüttenhain: Entzifferung 1939–1945, *Informatik Spektrum* 31(3): 249–261.

Beckman, B. 2002. *Codebreakers: Arne Beurling and the Swedish Crypto Program During World War II* . American Mathematical Society.

Brysac, S. B. 2002. *Resisting Hitler: Mildred Harnack and the Red Orchestra*. Oxford University Press.

Brückner, H.-D. 2005. Germany's first cryptanalysis on the Western Front: Decrypting British and French naval ciphers in World War I, *Cryptologia* 29(1): 1-22.

Budiansky, S. 2001. Codebreaking with IBM machines in World War II. *Cryptologia*. 25(4): 241–255.

Burde, G. and Schwarz, W. 1998. Wolfgang Franz zum Gedächtnis, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 100(4): 284–292.

Cowan, M. J. 2004. Rasterschlüssel 44: The epitome of hand ciphers. *Cryptologia* 28(2): 115–148.

CSDIC. 1945. First detailed interrogation report on Lentz, Waldemar and Kurfess, Hans. Combined Services Detailed Interrogation Centre, CSDIC/CMF/SD 80.

Diller, J. 2000. Laudatio. University of Münster. Unpublished.

Döring, H. 1950. Über die Fehler, die bei Milchleistungsprüfungen auftreten. *Zeitschrift für Tierzüchtung und Züchtungsbiologie* 58(4): 389–408. [This contains the substance of Döring's 1939 doctoral dissertation.]

Dudley, E. 2011. *The Package: A Tale of the Holocaust*. North Charleston, South Carolina: Createspace Independent Publishing Platform [currently part of Amazon].

EASI. 1946. See American Security Agency, 1946.

Elstrodt, J. and Schmitz, N. 2013. Prof. Dr. Helmut Ulm (1908 – 1975). In *Geschichte der Mathematik an der Universität Münster*, Teil II: 1945–1969, pp. 307–310. [Unpublished, but available on the University of Münster website `http://www.uni-muenster.de/FB10/historie/kapitel7.pdf` (accessed on December 8, 2018).]

Epple, M. 1999. Geometric aspects in the development of knot theory. In *History of Topology*, I. M. James, ed. Amsterdam: Elsevier, pp. 301–357.

Erskine, R. 2003. From the archives: what the Sinkov mission brought to Bletchley Park. *Cryptologia*. 27(2):111–118.

Erskine, R. 2004. McVittie, George Cunliffe (1904–1988). *Oxford Dictionary of National Biography*, Volume 36, p. 46.

Erskine, R. and Bloch, G. 1986. The dropping of double encipherment. *Cryptologia* 10(3): 134–141.

Erskine, R. and Freeman, P. 2003. Brigadier John Tiltman: One of Britain's finest cryptologists. *Cryptologia* 27(4): 289–318.

Faulkner, M. 2010. The Kriegsmarine, signals intelligence and the development of the B-Dienst before the Second World War. *Intelligence and National Security* 25(4): 521–546.

Fest, J. 1996. *Plotting Hitler's Death: The Story of German Resistance*. New York: Metropolitan Books.

Filby, P. 1995. Floradora and a unique break into onetime pad ciphers. *Intelligence and National Security*. 10 (3):408–422.

Föppl, L. [No date] *Lebenserinnerungen: Ludwig Föppl*. Unpublished.

Forster, O. 2000. Karl Stein 1.1.1913–19.10.2000. In *Bayerische Akademie der Wissenschaften, Jahrbuch 2000*. Munich: Verlag der Bayerischen Akademie der Wissenschaften, 323–325.

Fricke, W. 1985. *Schriften und Vorträge zur Astronomie und Astrophysik 1937–1985*. Heidelberg: Astronomisches Rechen-Institut, Heidelberg. 1985.

GCCS. 1945a. *The History of Hut 6, Volume I*. Government Code and Cypher School, September 29, 1945. The National Archives, Kew, TNA HW 43/70.

GCCS. 1945b. Further Typex Interrogations. GCCS (SAC—Security of Allied Communications), ZIP/SAC/G.36, 20 Oct. 1945. Included in "Investigation into POW reports that German Sigint authorities exploited TYPEX (British cypher machine)", UK National Archives, TNA HW 40/89, pp.45–50.

Giskes, H. J. 1953. *London Calling North Pole*. London: William Kimber.

Göbel, R. 1989. Helmut Ulm: his work and its impact on recent mathematics. In *Abelian Group Theory* (L. Fuchs, R. Göbel, and P. Schultz, eds.), *Contemporary Mathematics* 87, Providence, RI: American Mathematical Society.

Göbel, S. 2009. *Jahrbuch über die Fortschritte der Mathematik* and *Zentralblatt MATH* – reporting on more than 140 years of mathematics. *Newsletter of the European Mathematical Society*, Issue 73, September 2009, 45–46.

Göbel, S. 2011. Glimpses into the history of Zentralblatt MATH. In *80 Years of Zentralblatt MATH: 80 Footprints of Distinguished Mathematicians in Zentralblatt*, Olaf Teschke, Bernd Wegner, Dirk Werner, eds., Berlin: Springer-Verlag, 1–16.

Grözinger, K. and H.van der Linden. 2009. *Die Stiftungen der Preussisch-Judischen Hofjuweliersfamilie Ephraim und ihre Spuren in der Gegenwar* (Judische Kultur. Studien Zur Geistesgeschichte, Religion Und Literatur). Wiesbaden: Otto Harrassowitz.

Grupp, P. 1988. *Deutsche Aussenpolitik im Schatten von Versailles 1918–1920. Zur Politik des Auswärtigen Amtes vom Ende des Ersten Weltkrieges und der Novemberrevolution bis zum Inkrafttreten des Versailler Vertrages.* Paderborn: Ferdinand Schöningh.

Halter-Koch, F. 1999. Alexander Aigner. *Nachrichten der Österreichischen Mathematischen Gesellschaft* 181(August): 75–77.

Hange, M. 2015. Obituary for Dr. Otto Leiberich, *Security in Focus - BSI Magazin*. `https://www.bsi.bund.de/EN/Publications/BSIMagazine/BSI-Magazine_node.html` (accessed May 26, 2017).

Haupt, O. 1981. Georg Aumann 11.11.1906–4.8.1980. In *Bayerische Akademie der Wissenschaften, Jahrbuch 1981.* Munich: Verlag der Bayerischen Akademie der Wissenschaften, 266–270.

Hauthal, H. 1985. Beitrag zur Geschichte des Chiffrierwesen im Auswärtigen Amt 1919 bis 1945 [A contribution to the history of the cryptologic service of the Foreign Office 1939 to 1945]. Berlin: Politische Archiv des Auswärtiges Amts (PAAA), VS-6025.

Hoffmann, E. 2017. *Emil Krebs: Ein Sprachgenie im Dienste der Diplomatie* (Fremdsprachen in Geschichte und Gegenwart, Band 18). Wiesbaden: Harrassowitz Verlag.

Huckleberry, A. 2008. Karl Stein, *Jahresbericht der Deutschen Mathematiker-Vereinigung* 110(4): 195–206.

Humboldt-Universität zu Berlin. 2010. *Versteinerte Spuren: Zur Erinnerung an ehemalige jüdische Studierende der Friedrich-Wilhelms-Universität.* Berlin: Berlin Stipendien der Stiftung EVZ.

Irving, D. 1989. *Das Reich Hört Mit*. Kiel: Arndt Verlag. [We are not unaware of the controversial status of much of Dr. Irving's work. This particular book however is quite good and a valuable contribution to the history of the Forschungsamt.]

Isphording, B., Keiper, G., and Kröger, M. (Editors). 2017. *Biographisches Handbuch des deutschen Auswärtigen Dienstes 1871–1945: Band 1–5*. Paderborn: Ferdinand Schöningh.

Jenkins, J. A. 1985. Helmut Grunsky, *Jahresbericht der Deutschen Mathematiker-Vereinigung* 91(4): 159–167.

Jensen, W. 1955. *Hilfsgeräte der Kryptographie*. Unpublished doctoral dissertation, Flensburg, Germany.

Jones, N. 2008. *Countdown to Valkyrie: The July Plot to Assassinate Hitler*. London: Frontline Books.

Kahn, D. 1967. How one Bucknellian wrote his book. *The Bucknell Alumnus*, November 1967: 10–14.

Kahn, D. 1978. *Hitler's Spies: Germany Military Intelligence during World War II*. New York: Macmillan.

Kahn, D. 1978a. The Forschungsamt: Nazi Germany's most secret communications intelligence agency, *Cryptologia* 2(1): 12–19.

Kahn, D. 1996. *The Codebreakers: The Story of Secret Writing*, 2nd ed. New York: Scribner. [First edition 1967]

Kersten, I. 1993. Ernst Witt 1911–1991 [in German]. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 95(4): 166–180.

Kersten, I. (ed.). 1998. *Ernst Witt: Collected Papers—Gesammelte Abhandlungen*. Springer Collected Works in Mathematics. Berlin: Springer-Verlag.

Kersten, I. 2000. Biography of Ernst Witt (1911-1991). In *Quadratic Forms and their Applications*, E. B. Fluckiger, D. Lewis, A. Ranicki, eds., *Contemporary Mathematics*, 272, Providence, RI: American Mathematical Society.

Koch, P. 1998. *Geschichte der Versicherungswissenschaft in Deutschland: Hrsg. vom Deutschen Verein für Versicherungswissenschaft e. V. aus Anlaß seines 100-jährigen Bestehens*. Karlsruhe: Verlag Versicherungswirtschaft.

Köthe, G. 1976. Erika Pannwitz. *Zentralblatt für Mathematik und ihre Grenzgebiete* 309: 3.

Kunze, W. 1914. *Über Zerfallsprodukte des Radium F*. Eisleben: Druck von Ernst Schneider.

Leiberich, O. 1999. Vom diplomatischen Code zur Falltürfunktion, *Spektrum der Wissenschaft* 6: 26–34.

Lüst, R. 2001. Barium cloud experiments in the upper atmosphere. In *The Century of Space Science*, J. A. M. Bleeker, J. Geiss, M. C. E Huber, eds., Dordrecht: Springer, pp. 179–187.

Marks, L. 1998. *Between Silk and Cyanide: A Codemaker's Story 1941–1945*. New York: The Free Press.

McKay, C. G. and Beckman, M. 2003. *Swedish Signal Intelligence 1900–1945*. New York: Frank Cass.

Mehrtens, H. 1987. Ludwig Bieberbach and "Deutsche Mathematik". In *Studies in the History of Mathematics*, Phillips, Esther R., ed., *MAA Studies in Mathematics*, 26, Washington, DC: Math. Assoc. America, pp. 195–241.

Meyer, J. A. 1975. Der Fall WICHER: German knowledge of Polish success on Enigma, *NSA Technical Journal* 20(2): 1–27. [Declassified and approved for release by NSA on October 31, 2007.]

Moorhouse, R. 2006. *Killing Hitler: The Plots, the Assassins, and the Dictator Who Cheated Death*. New York: Bantam Books.

Mowry, D. P. 1983–84. Regierungs-Oberinspektor Fritz Menzer: Cryptographic inventor extraordinaire. *Cryptologic Quarterly* 2(2–4): 21–36.

Nelson, A. 2009. *Red Orchestra: The Story of the Berlin Underground and the Circle of Friends Who Resisted Hitler*. New York: Random House.

Ostwald, O. and Weierud, F. 2016. History and modern cryptanalysis of Enigma's pluggable reflector. *Cryptologia* 40(1): 70–91.

Pahl, M. 2016. *Hitler's Fremde Heere Ost: German Military Intelligence on the Eastern Front 1942–45*. Solihull, UK: Helion and Company.

Paschke, A. 1957. Das Chiffrier- und Fernmeldewesen im Auswärtigen Amt, Seine Entwicklung und Organisation, Eine historische Studie [The cryptologic and signal service of the Foreign Office, development and organization, an historical study]. Berlin: Politische Archiv des Auswärtiges Amts (PAAA), VS-6025.

Perrault, G. 1967. *The Red Orchestra*. New York: Simon and Schuster.

Phillips, C. 2000. The American solution of a German one-time-pad cryptographic system (G-OTP). *Cryptologia* 24 (4):324–332.

Praun, A. 1950. *German Radio Intelligence*. Department of the Army, Office of the Chief of Military History.

RSS. 1946. R. S. S. (I). Note: The Funkabwehr. Radio Security Service, UK National Archives, TNA HW 34/2.

Rademacher, K. and Szenzenstein, J. 1984. Repräsentativstatistiken des Handels und des Gastgewerbes. *Wirtschaft und Statistik* 10: 868–881. Statistisches Bundesamt. Stuttgart und Mainz: W. Kohlmammer.

Rezabek, R. 2012. TICOM: The last great secret of World War II. *Intelligence and National Security* 27(4): 513–530.

Rezabek, R. 2013. TICOM and the search for OKW/ Chi. *Cryptologia* 37(2); 139–153.

Rezabek, R. 2017. *TICOM: the Hunt for Hitler's Codebreakers*. Independently published.

Riesser, H. 1962. *Von Versailles zur UNO: Aus den Erinnerungen eines Diplomaten*. Bonn: Bouvier.

Rohrbach, H. 1948. Mathematische und Maschinelle Methoden beim Chiffrieren und Dechiffrieren. *FIAT Review of German Science, 1939–1946: Applied Mathematics*, 3(1): 233–257. Wiesbaden: Government for Germany, Field Information Agencies.

Rohrbach, H. 1978. Mathematical and mechanical methods in cryptography. *Cryptologia*, 2(1):20–37, 2(2):101–121. [Translation of Rohrbach, 1948.]

Rohrbach, H. 1979. Report on the decipherment of the American strip cipher 0-2 by the German Foreign Office (Marburg 1945). *Cryptologia* 3(1):16–26. [Translation of a paper prepared for TICOM.]

Samuels, M. 2016. Ludwig Föppl: A Bavarian cryptanalyst on the Western front. *Cryptologia* 40(4): 355-373.

Sandoz, G. 1990. *Gérard Sandoz: Ein Leben für die Verständigung*. Marburg.

Sandvoß, H.-R. 1996. *Widerstand in Kreuzberg (Widerstand in Berlin 1933–1945, Band 10)*. Berlin: Gedenkstätte Deutscher Widerstand.

Schauffler, R. 1917. Über wiederholte Funktionen. *Mathematische Annalen* 78(1–4): 52–62.

Schauffler, R. 1921. Über wiederholbare Funktionen. *Mathematische Annalen* 84(1–2): 137–142.

Schauffler, R. 1956. Über die Bildung von Codewörten. *Arch. elektr. Übertragung* 10: 303–314.

Schauffler, R. 1957. Die Assoziativität im Ganzen, besonders bei Quasigruppen. *Math. Z.* 67: 428–435.

Schauffler, R. 1962. Erinnerungen eines Krypologen [Memories of a cryptologist]. Berlin: Politische Archiv des Auswärtiges Amts (PAAA), VS-6025.

Schmeh, K. 2009. Enigma's Contemporary witness: Gisbert Hasenjaeger. *Cryptologia* 33(4): 343–346.

Schradar, H. 2009. *Codename Valkyrie: General Friedrich Olbricht and the Plot Against Hitler*. Newbury Park, CA: Haynes North America.

Schubert, H. 1964. *Topologie: Eine Einführung*. Stuttgart: Teubner. Translated into English in 1968 as *Topology*, Siegried Moran, ed. Boston: Allyn and Bacon.

Schubert, H. 1970. *Kategorien I, II*. Heidelberger Taschenbcher, Bände 65, 66. Berlin: Springer-Verlag. Translated into English in 1972 as *Categories*, Eva Gray, ed. Berlin: Springer-Verlag.

Schwarz, W. 2005. Aus der Geschichte der Frankfurter Mathematik. Festschrift zu den 100. Geburtstagen von Ruth Moufang, Gottfried Köthe, Wolfgang Franz. Edited by Wolfgang Schwarz. Schriften des Universitätsarchivs Frankfurt am Main, 1. Frankfurt: University of Frankfurt.

Schwarz, W. and Volkmann, B. 2003. Hans Rohrbach zum Gedächtnis: 27.02.1903 –19.12.1993. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 105: 89–99.

Segal, S. 2003. *Mathematics Under the Nazis*. Princeton: Princeton University Press.

Seifert, H. and Threlfall, W. 1934. *Lehrbuch der Topologie*. Leipzig: B. G. Teubner. Translated into English in 1980 as *Seifert and Threlfall: A Textbook of Topology*, Michael A. Goldman and Joan Birman, eds. *Series in Pure and Applied Mathematics*, 89. London: Academic Press Inc.

Siegmund-Schultze, R. 1993. *Mathematische Berichterstattung in Hitlerdeutschland. Der Niedergang des Jahrbuchs über die Fortschritte der Mathematik (1869-1945)*. Göttingen: Vandenhoeck & Ruprecht.

Siegmund-Schultze, R. 2004. Helmut Grunsky (1904–1986) in the Third Reich: A Mathematician Torn between Conformity and Dissent, in Roth, O. and Ruscheweyh, S., *Helmut Grunsky: Collected Papers*. Lemgo: Heldermann Verlag, pp. XXXI–L.

Stein, A. ("Rumpelstilzchen"). 1922. Nachträgliches zu Lohans Tod. In *Berliner Allerlei* (Jahrgangsband 1920/21). Berlin: Verlag der Täglichen Rundschau, Gloss 24, März 1921. [Available online at `http://www.karlheinz-everts.de/rmp20-22.htm` (accessed December 8, 2018)]

Swift, K. L. 1960. How the Germans broke a U. S. code. *NSA Technical Journal*. 5(3 & 4): 1–7. [Declassified and approved for release by the NSA on August 16, 2012.]

Tarrant, V. E. 1995. *The Red Orchestra - the Soviet Spy Network Inside Nazi Europe*. London: Arms and Armour Press.

Tillmann, H. G. 2007. Gottfried Köthe, 1905–1989, *Heidelberger Texte zur Mathematikgeschichte*, Neu herausgegegeben von Gabriele Dörflinger, Universitätsbibliothek Heidelberg.

Tobies, R. 2006. *Biographisches Lexikon in Mathematik promovierter Personen : an deutschen Universitäten und Technischen Hochschulen ; WS 1907/08 bis WS 1944/45*. Augsburg: Rauner.

Treder, H.-J. 1988. Walter Fricke, 1. 4. 1915 – 21. 3. 1988. *Astronomische Nachrichten* 309(3): 226.

Trepper, L. 1983. *The Great Game: Memoirs of the Spy Hitler Couldn't Silence*. New York: McGraw-Hill.

University of Greifswald. 2007. *Ehrenkolloquium des Instituts für Mathematik und Informatik: 100 Jahre Willi Rinow*. `https://math-inf.uni-greifswald.de/fileadmin/uni-greifswald/fakultaet/mnf/mathinf/boldt/pdf-dateien/rinow-3.pdf` (accessed February 10, 2019).

van der Meulen, M. 1996. Cryptology in the early Bundesrepublik. *Cryptologia* 20(3): 202–222.

van der Meulen, M. 1998). The road to German diplomatic ciphers—1919 to 1945. *Cryptologia* 22(2): 141-166.

van der Meulen, M. 1999. Cryptologic Services of the Federal Republic after 1945. International Meeting of the Intelligence History Study Group, 18.–20. June 1999. Akademie für Politische Bildung Tutzing. Unpublished manuscript of talk.

Vogt, A. 1999. Von der Hilfskraft zur Leiterin: die Mathematikerin Erika Pannwitz. *Berlinische Monatsschrift* 5: 18–24.

Waggoner, T. and Jache, R. (1961). The GEE system–I. *NSA Technical Journal* 6(4): 1–38. [Declassified and approved for release by the NSA on September 29, 2008.]

Waggoner, T. and Jache, R. (1962). The GEE system–V. *NSA Technical Journal* 7(4): 67–76. [Declassified and approved for release by the NSA on June 5, 2009.]

Wehefritz, V. (ed.) 1985. *Prof. Dr. phil. Rudolf Kochendörffer (21.11.1911 - 23.8.1980), Bestandsverzeichnis aus dem Wissenschaftsarchiv der Universität Dortmund. Mit Beiträgen von Prof. Dr. Albert Schneider (Dortmund) und Prof. Dr. Hans Rohrbach (Mainz)*. Dortmund: Universitätsbibliothek Dortmund.

Weidman, J. 1990. Gottfried Köthe, 1905–1989. *Note di Mathematica* 10(Supplement 1): 1–7.

Weierud, F. 2005. Bletchley Park's Sturgeon, the fish that laid no eggs. *The Rutherford Journal*, Volume 1. `http://www.rutherfordjournal.org/article010106.html` (accessed December 8, 2018).

Werther, W. 1959. Cryptanalysis in the German Air Force. *NSA Technical Journal*,4(2): 73–89. [Declassified and approved for release by the NSA on September 29, 2008. This article is a translation of Chapter IV of Oblt. Waldemar Werther's "Study of Russian Cryptographic Systems" (*Die Geheimschriften Sowjetischen Fliegertruppe und Ihre Entzifferung*), the original German version of which appears in the second part of IF-175 (the"Seabourne Report", Vol. XIII). Chapter IV is entitled "Organisation und Arbeitsweise der Deutschen Entzifferung" and is on pp. 30–58.]

Westerhout, G. 1985. Fricke's influence on the world of astronomy, *Celestial Mechanics*, 37(3): 345–348.

Wielen, R. and Lederle, T. 1990. Obituary: Walter Ernst Fricke (1915–1988). *Quarterly Journal of the Royal Astronomical Society* 31(3): 515-517.

Wigand, A. 1916. Ernst Dorn. *Physikalische Zeitschrift* 17(14): 297–299.

Zabell, S. 2015. Statistics at Bletchley Park. In *Breaking Teleprinter Ciphers at Bletchley Park: An Edition of I.J. Good, D. Michie and G. Timms: General Report on Tunny with Emphasis on Statistical Methods (1945)*, W. Diffie, J. V. Field, J. A. Reeds, eds. New York: IEEE Press, lxxv-ci.