An Introduction to a Historic Computer Document: Betting on the Future – The 1946 Pendergrass Report Cryptanalysis and the Digital Computer

COLIN BURKE

The codebreakers of the American navy's OP-20-G had struggled since the early 1930s to obtain the funds needed to design and build high-speed electronic analytic machines. [11, 2] Unfortunately, their mid-1930's project, which was led by Vannevar Bush of MIT, did not produce a truly successful device. The developmental funds and the institutional supports provided by the navy were insufficient for the challenging move into digital electronics. The relatively special-purpose, optical-electronic Comparator that Bush constructed for the navy in 1938 was unreliable. OP-20-G began World War II with only a handful of IBM electromechanical tabulators and the hope that massive funding of electronics research would finally allow the creation of the more powerful Rapid Analytic machines Bush had suggested to the navy's S.C. Hooper and Joseph Wenger in 1936. [21] Hooper and Wenger hoped that such machines, distant cousins of the programmed digital electronic computer, would allow OP-20-G to create and apply advanced mathematical and statistical cryptanalytic techniques.

A stable, long-term program to develop the Rapid Machines might have led OP-20-G to be among the very first to conceive of and build a modern electronic computer, but the chance for such a program had been lost in the 1930s. It could not be reborn during the war. The demands created by Pearl Harbor and the Battle of the Atlantic turned OP-20-G away from speculative projects. Although the outbreak of World War II and a new faith in cryptanalysis led to the allocation of millions of dollars for machine development and the creation of a special group for machine design and construction, there were too many pressures to allow OP-20-G to do more than build a series of very limited and special-purpose electromechanical and electronic devices during the war. Most of them did not even attain the flexibility of Bush's original mid-1930's design, and few provided significant help to advanced statistical and mathematical cryptanalysis.

The need to immediately read the ever-changing codes and ciphers of the Axis powers caused the OP-20-G research group under Joseph Wenger and Howard Engstrom to take the cryptanalytical and technological paths of least resistance. In the early 1940s least resistance usually meant brute-force cryptanalytic methods and the creation of machines that were either physical representations of an enemy's encryption devices or fixed physical embodiments of decryption processes. The men in OP-20-G's research team knew that such a strategy could lead to expensive machines that suddenly became useless when enemy cryptographers made slight changes in their cipher systems. They realized,

however, that the creation of more general-purpose devices based on then blue-sky cryptanalytic and electronic techniques was impractical if not irresponsible. When the only sound cryptanalytic alternative was to attack systems through statistical methods, more general-purpose computing devices were constructed. But their architecture had to be sparse, and their components were based upon as much off-the-shelf technology as possible. [9]

The crises of World War II were too grave and too frequent to allow creative urges to have priority over practical solutions. Reliable electromechanics and analogue electronics thus triumphed over digital technology at OP-20-G. While easy to construct and relatively fast special-purpose devices were chosen over more general-purpose designs, the young engineers that OP-20-G plucked from the leading electronic computer projects in American industry and academia lobbied for the exploration of technological frontiers and for more general-purpose machines. But they never recommended the option of constructing one machine to perform all cryptanalytic functions. A "universal" cryptanalytic machine, let alone a high-speed device to perform all logical and mathematical routines, was something at the farthest edge of imagination in the early 1940s. Even Alan Turing, Bletchley Park's mathematical genius, left his philosophical defense of the possibility of a universal mathematical device as a set of formulas in an abstract article. [1, 13, 27]

Immediate problems, not long-term goals, shaped the accomplishments of the Rapid Machine group during the war. OP-20-G's teams at the National Cash Register Company, Eastman Kodak, and its Nebraska Avenue Annex in Washington, D.C., created a host of amazing machines that frequently used components that were far beyond the state-of-the-art in electronics and electromechanics. [12] But all were compromises between engineering visions and practical needs. The machines created between 1942 and 1945 were limited in technology as well as in their range of application. Although most used some electronics, many were based on analogue rather than digital logic and components. A few were unashamed reversions to much older electromechanical technology. Such choices were rational in the context of war. Analogue methods and electrical and electromechanical parts were reliable and inexpensive, ran faster than electronics in some applications, and demanded much less development time than the still experimental digital electronics. For example, in the attack against the Germans' Enigma systems, it proved quite efficient to use a special-purpose design and to base the American Bombe on electromechanics. The early 1942 dream of a fully electronic and perhaps relatively general-purpose digital Bombe, or even one centered on electronic versions of the wheels of the Enigma, devolved into a variation on England's combination of spinning shafts and electric commutators. [14, 15] Electronic digital counters played a very secondary role as the hard-rubber and brass wheels of the Bombe proved to be a combination of speed and reliability that surpassed the power of the tubes and circuits of the early 1940s. [16, 8, 26]

Even when OP-20-G's engineering wizards were told to create devices to speed the application of general cryptanalytic methods, such as the Index of Coincidence, or to go far beyond the power of tabulating machines to perform searches for repetitions and correlates

of code patterns, they had to follow that least resistant path. For example, digraph analysis machines were hurriedly constructed using the very primitive technologies of mechanical teletype readers and electromechanical industrial counters. [9, 10: 23] And while a new version of Bush's 1930s film Comparator was constructed, it barely achieved the power of its mid-1930's design. It merely tallied "coincidences" of varying lengths on electronic counters as offset messages punched on special paper tapes flew by an optical reading station. [9]

Other wartime applications of Bush's original ideas were even more limited. The hand-operated, table-top IC machine was based on analogue electronics. Its operators had to slide two photographic plates over each other until optical cells sensed enough light passing through the offset messages to indicate a desired level of coincidence. [9] The later and more sophisticated optical-electronic Copperheads were also essentially analogue devices. They did not even count or tally; they just stopped when the messages on the two high-speed tapes had enough coincident code spots. The operator of the machines had to rewind the films by hand to locate the position of the code overlap. [9]

Other machines built by OP-20-G's Naval Computing Machine Laboratory contained more advanced electronics and logic. But even the complex extensions of the Bombe remained special purpose as did the electronic digital machines built to model the encryption devices of the Japanese. [7, 5] OP-20-G was not alone in achieving less than its young engineers might have desired. The American army's cryptologic machine builders were also limited by the state of digital electronic technology and the need to respond to emergencies. For the same reasons, England's engineers did not build a universal machine. [22, 20]

In 1945, when there were fewer crises, the engineers and mathematicians at OP-20-G urged the higher-ups to allow them to go beyond what they had accomplished during the critical years of the war. The crew at OP-20-G knew of the similar and in some ways more advanced work in England, work which led to the famous electronic precomputer, the Colossus. [22] But they wanted to do more than catch up with their British counterparts. They had their own dreams of extending the power of digital electronics, optical memory devices, and magnetic data recording.

The new mathematical cryptanalysts at OP-20-G also wanted to continue and extend the World War II automation efforts, but they feared that peace would mean the end of the Rapid Machines project. Luckily, the sacrifices and accomplishments of the war were appreciated by the navy's leaders. The ongoing contributions of Ultra and Magic and the role of cryptanalysis at critical times, such as the battle of Midway, had finally won recognition for the codebreakers. Unlike the situation at the end of World War I, when funding was suddenly ended, OP-20-G was promised several million dollars for postwar technological development. Immediately, great plans were laid to produce the type of machines that would have been built during World War II if there had been time to develop digital electronics and to overcome the barrier that frustrated all computer builders of the period, the lack of high-speed memory. [19, 27]

By the end of 1945, OP-20-G had its Program Monogram computing wish list ready. No one envisioned a universal machine, but there were great hopes that the special devices of World War II could be replaced by much more general mathematical engines. A new, much faster, multipurpose digital Comparator was to be designed and built. It was to be one that would be able to perform the functions that had been assigned to separate machines during the war. Along with the search for the new Comparator was a quest for the best memory medium. Microfilm and the unproven magnetic recording were to be explored for use on the machine that later became known as Goldberg. There was even a great deal of thought given to the possibility of constructing an electronic Super-bombe. [19]

There was no thought given, however, to the creation of a general-purpose, electronic and program driven computer. Monogram was not a computer project; it was an effort to develop what we would now call powerful special-purpose machines. OP-20-G's team included some of the best electronics engineers, mathematicians, and logicians in the nation, but even in 1945 they did not think a general-purpose computer was a realistic option for 1940's codebreaking. Cryptanalytic functions, they thought, had to be hard-wired into a machine. Thus, Monogram's original list did not include a "programmed" computer.

Then, OP-20-G's technical leader, Howard Campaigne, decided to send one of his men to see what the University of Pennsylvania was offering at its Moore School's 1946 summer course on computers. The Moore School's computer group had just completed the ENIAC, the astounding yet special-purpose digital electronic version of the giant analogue differential analyzers. Unlike the engineers at the cryptanalytic agencies, the Moore School's team had been allowed enough time to experiment; Army Ordnance's computing crises were not of the same order as those of the cryptologic agencies. It could balance future usefulness against meeting production schedules. [24]

Although the huge ENIAC was a special-purpose machine, it was fully electronic, and its construction led to something more significant: the design of universal devices that later became know as the EDVAC and IAS computers. By 1945, the Moore School's men had sketched out a machine that would perform any mathematical routine through what we now call "software." When the young Philadelphia engineers, led by John Mauchly and Presper Eckert, were joined by the famous and powerful John von Neumann, their idea for a universal engine became more specific and gained recognition in the scientific community.

Although torn by policy and personal conflicts, the original ENIAC group was so famous that engineers and mathematicians from the most advanced computer projects flocked to Philadelphia in the summer of 1946 to gain insights into the latest computer developments. Von Neumann's design for a more sophisticated universal machine, which he planned to build at the Institute for Advanced Study, was revealed as were the ideas of Eckert and Mauchly, who were beginning to sketch the outlines of their own new computer, the UNIVAC. They were joined by a host of experts who described the advances

in digital electronic hardware and logic achieved at other American computer centers since the onset of the war. [4, 24]

Because of the continued security restrictions on OP-20-G's work, it could not reveal its computing secrets. But Campaigne accepted an invitation to send a representative to the summer meeting. He was to listen and learn. At the same time, Joseph Wenger began to establish a long-term relationship with John von Neumann. The contacts with von Neumann and the Philadelphia group were important to OP-20-G because although they were aware of the general nature of the work at all the American and British computer centers, OP-20-G's men had not yet realized the implications and potentials of the design of the proposed EDVAC and IAS computers. They, like most others, did not fully appreciate the critical importance of the idea of a general-purpose programmed computer.

James T. Pendergrass, a young academic physicist who had been drafted into naval cryptanalysis, was selected to represent OP-20-G at the summer conference and workshops. He was impressed by the size of the group and the credentials of the men who attended the nearly month-long meeting. He was even more impressed with what he heard. He very quickly became an advocate for the construction and use of a general-purpose digital computer for codebreaking, one based upon John von Neumann's scheme.

During his weeks in Philadelphia, Pendergrass convinced himself that most if not all cryptanalysis could be performed through digital methods. He came to believe that general-purpose digital computers would soon be fast enough to compete with the special-purpose and analogue devices being constructed under Monogram. His next step was to persuade the navy that OP-20-G should have its own version of the proposed IAS universal mathematical and information machine.

With the blessing of the operational head of OP-20-G, Joseph Wenger, Pendergrass devoted much time to preparing a long and detailed report. His two-part document was submitted to OP-20-G in late 1946. It remained Top Secret for decades. Only recently has one part been declassified, and the censors continue to black out and delete significant portions of it. [3]

There is a good reason for the continued caution about the Pendergrass Report, for it contains secret information. Pendergrass had to demonstrate to the navy that a programmed computer could perform all the critically important cryptanalytic tests that were embedded in the many special-purpose devices, both analogue and digital, that were in OP-20-G's operational center in Building Four in Washington, D.C. Those tests included the secrets of Ultra and Magic. His report had to go further, however. He had to show that cryptanalytic procedures of a more advanced nature, which were to be built into the planned special-purpose Project Monogram machines, could be done with a computer.

The nature of his audience shaped the content and style of Pendergrass' report. The men at OP-20-G did not need a tutorial on basic electronic technology. They were leaders in the field and thought they would be able to convince the navy's Bureau of Ships, the agency that supervised all of OP-20-G's materials acquisitions, of the viability of electronic machines. What OP-20-G's cryptanalysts did need from Pendergrass was a demonstration

that the yet-to-be-born "programming," digital methods and the nonexistent general-purpose computer were reasonable cryptanalytic options. It was critically important to build a convincing argument that a computer could attack the new automatic enciphering devices that had led to the first Rapid Machine of the 1930s. Pendergrass and his allies had to show that the general-purpose machine could attack the Purple, Enigma, and the more worrisome machines like those used in the German Fish system.

Thus, Pendergrass went into great detail about the logic of a general-purpose computer and the programming of cryptanalytic tests. His report outlined the architecture of the new computer, gave a version of John von Neumann's programming language, and hinted that a more practical computer language would soon emerge. More importantly, the report showed how the most difficult World War II cryptanalytic problems could be programmed. Because time was always critical to the codebreakers, his reports also contained estimates of how long it would take the programs to solve problems familiar to the crew at "G."

Because upgraded versions of Bush's old designs were central to the plans for Monogram, Pendergrass had to prove that his proposed machine could replace Bush's Comparator. Thus, one section of the report was devoted to the description of the steps necessary to compile the statistics needed for the ubiquitous Index of Coincidence analysis.

Then, Pendergrass went on to OP-20-G's truly secret techniques and to the problems that had been the focus of its attention during the war. Unfortunately, only one of the perhaps three World War II special cryptanalytic procedures Pendergrass explored in the first report have survived the censor's scissors and black pen. He demonstrated the solution to the now famous target of the American "Bombes," the four-wheel naval Engima machine. And, in Appendix II, Pendergrass programmed a solution to the Enigma "Grenade" problem. It was one of the less time-consuming tasks assigned to the Bombes. A Grenade demanded a shorter run than other anti-Enigma procedures but followed the general logic of the Turing-Welchman attack on the Enigma. [26] That critical method was crib-based and analogue and very fast. So Pendergrass had to prove that his all-purpose digital machine could at least match the Bombe's efficiency.

Pendergrass wanted to show that his device would be useful to everyone at OP-20-G. In Appendix III he demonstrated how the digital computer could be used as an ultra-high-speed version of the Hagelin ciphering machine. With a very different mechanism and logic than the Enigma, the Hagelin devices were used by several nations, including the United States, during and after World War II. [10] To aid the attack on the Hagelin systems used by an enemy, and perhaps to illustrate how to speed the decryption of friendly messages, OP-20-G had constructed an electrical analog of the Hagelin during the war. Pendergrass showed how his all-purpose electronic digital machine could take its place. [18]

The particular systems discussed in the missing appendices of the first report are unknown, but they perhaps included an example of how to program a computer for an attack against Japanese encryption machines and a demonstration of how to solve the

more sophisticated machine ciphers such as those produced by the American ECM. The other part of his report, which remains classified [3], perhaps contained proof of the ability of a universal digital computer to replace the dozens of tabulating machines and special-purpose Rapid Machine devices that were arrayed against code problems. Pendergrass perhaps demonstrated how to strip additives and, although he realized that there was no mass memory technology that could keep pace with the speed of electronics in 1945, showed how the computer could search for code groups. [10]

The Pendergrass report hit its mark, at least with the operational head of OP-20-G. As a result, Joseph Wenger began to lobby the very reluctant Bureau of Ships to allow yet another "computer" project. The job of convincing the Bureau was not easy. "G" already had the more special-purpose Goldberg and other machines with proven track records on the way to completion. The Bureau wondered if it wasn't wiser to let others, such as John von Neumann, carry the long and costly burden of the first stages of computer research.

The Bureau's men must also have wondered if the new computer would be cost effective. The electromechanical Bombes which worked so well against the Germans cost $45,000 each, and other World War II machines were built for similar amounts. The ENIAC, however, had cost hundreds of thousands of dollars, and the projections for the EDVAC and IAS computers were even higher. [12]

Even Pendergrass' optimistic estimates of the electronic computer's run times must have raised some concern. The machine he proposed would take seven minutes to run the regular Enigma problem. The inexpensive and reliable conglomeration of spinning wheels, the Bombe, took twenty minutes plus machine set-up time. A perhaps threefold advantage at a probable tenfold cost didn't seem a wise choice. An outside observer, even one who realized the other advantages of a general-purpose machine, might well have thought that OP-20-G was as much interested in "engineering" as in cryptanalysis.

Wenger won his battle, but it took some time to secure the go-ahead from the Bureau of Ships and to piece together the funds to study and then build OP-20-G's general-purpose Atlas computer. Its design went through several alterations as the engineering team learned more about computer logic. The army's cryptanalysts were also inspired by the Pendergrass report and soon began their quest which led to the Abner computer. [22, 23]

Neither service, however, found it easy to fund or build a machine. Using the private company established by the men who had been the core of OP-20-G's World War II computer program, Engineering Research Associates, the navy had a working computer at the end of 1950, some three and one-half years after letting the initial contracts. The army had an even more difficult time arranging for the construction of its device. It was finally delivered in the spring of 1952. [25, 23]

The price of the Atlas was much greater than expected, more than twenty times that of a Bombe. Just the assembled hardware cost some $950,000. That was much, much more than the navy paid for the many fast special-purpose machines ERA and other contractors continued to build throughout the 1940s and 1950s. [22 p.8]

The special-purpose machines continued to fill many cryptanalytic needs, but the great advances in computer technology in the 1950s vindicated Pendergrass and the others who had been willing to take a very great leap of faith in 1946. Although it was more than a decade before the general-purpose computer, even when augmented with special-purpose add-ons, could match the speed of dedicated devices for cryptanalytic problems, the codebreakers held to their commitment and continued to be major sponsors of the development of universal computers and their underlying technologies. [22]

(U) Colin Burke is a professor of history at the University of Maryland, Baltimore County. He is currently scholar-in-residence at the Center for Cryptologic History. He became interested in the history of computers after many years researching the course of American politics and education. He resides in Columbia, MD, and is now completing a history of computer development in the American cryptanalytic community from 1930 to 1965.

REFERENCES

[1] Bashe, Charles J. et al. *IBM's Early Computers*. Cambridge MA: MIT Press, 1986, 59.

[2] Bureau of Engineering. 18 November 1931. To CNO, "Automatic Machines of OP-20-G."

[3] Campaigne, H. and J.T. Pendergrass. 12 December 1946. Second Report on Cryptanalytic Use of High-Speed Digital Computing Machines. OP-20-G, Washington, D.C.

[4] Cambell-Kelly, Martin, and Michael R. Williams (eds). *The Moore School Lectures: Theory and Techniques for the Design of Electronic Digital Computers*. Cambridge MA: MIT Press, 1985

[5] Chief of Naval Operations, U.S. Naval Communications, 1945. Technical Paper TS-6, "Rattler."

[6] Chief of Naval Operations, U.S. Naval Communications, May 1945. Communications, Intelligence Technical Paper-41, "Copperhead I Punch and Scanner."

[7] Chief of Naval Operations, U.S. Naval Communications, March 1946. "Duenna Operations Manual." Washington, D.C.

[8] Chief of Naval Operations, U.S. Naval Communications, May 1946. Communications, Technical Paper TS-43, "The Bombe." Washington, D.C.

[9] Chief of Naval Operations, U.S. Naval Communications, June 1946. "Machine Comparisons." Washington, D.C.

[10] Deavours, Cipher A., and Louis Kruh. *Machine Cryptography and Modern Cryptanalysis*. Norwood MA: Artech House, 1985.

[11] Hooper, S.C. DNC, 26 September 1930. To OP-20-G, "Automatic Computing," NARA RG457, SRH355, "Naval Security Group History to World War II," 79.

[12] Meader, Ralph. USNR, 21 January 1940. To Capt. J.N. Wenger, USN, "Report of 14 Day Training Duty."

[13] OP-20-G, 3 November 1941. "Report of Meeting to Discuss New RAM Comparator."

[14] OP-20-G, May 1942. "Memo to Station X, Future E Policy."

[15] OP-20-G, 5 August 1942. Wenger to Ely, "Electronic Wheel."

[16] OP-20-G, 15 September 1942. To Joseph Desch, "Report on Proposed Bombe Design."

[17] OP-20-G, 21 February 1944. W. Wright to OP-20-G, "Report on Meeting with ASA."

[18] OP-20-G, 7 September 1944. OP-20-G to NCML, "Electrical Hagelin."

[19] OP-20-G, 20 December 1945. "Project Monogram."

[20] Randell, Brian. The Colossus. In N. Metropolis et al. (eds) *A History of Computing in the Twentieth Century*. New York: Academic Press, 1980, 47-92.

[21] Safford, L.R. to S.C. Hooper. 19 November 1940. "Comparator." NARA RG457, SRH355, 404, .

[22] Snyder, Samuel S. *History of NSA General-Purpose Electronic Digital Computers*. Washington: Department of Defense, 1964.

[23] Snyder, Samuel S. ABNER: The ASA Computer. Part I: Design. *NSA Technical Journal* 25 (2): 49–67, 1980.

[24] Stern, Nancy. *From ENIAC to UNIVAC: An Appraisal of the Eckert-Mauchly Computers*. Bedford MA: Digital Press, 1981.

[25] Tomash, Erwin. The Start of an ERA: Engineering Research Associates, Inc., 1946–1955. In, N. Metropolis et al. (eds) *A History of Computing in the Twentieth Century*. New York: Academic Press, 1989 485–95.

[26] Welchman, Gordan. *The Hut Six Story: Breaking the Enigma Codes*. New York: McGraw-Hill, 1982.

[27] Williams, Michael R. *A History of Computing Technology*. New York: Prentice-Hall, 1985.