4.3 Project X — A True Secrecy System for Speech

4.3.1 Introduction

One of the more closely guarded projects in World War II, and for years thereafter, was known simply as "Project X." It concerned the origination and development of a completely secret speech enciphering and transmission system, which by its nature could not possibly be deciphered by other than its intended receiver. To the people who worked on it, it was known as the "X System." To the people in the Signal Corps who handled the system, it was most generally known as "Sigsaly" or "Ciphony 1," and to the people in the telephone and radio transmission centers who handled its inviolate trunk circuits and were curious about its function, it was nicknamed the "Green Hornet" because the audible control tones were similar to the signature theme of a well-known radio program.

Table 5-5. Patents Related to Project X Research			
U.S. Patent No.	**Inventor**	**Filing Date**	**Issue Date**
3,024,321	K. H. Davis, A. C. Norwine	12/29/44	3/ 6/62
3,076,146	M. E. Mohr	12/27/45	1/29/63
3,188,390	M. E. Mohr	12/20/43	6/ 8/65
3,193,626	H. L. Barney	12/29/44	7/ 6/65
3,340,361	R. K. Potter	7/ 9/45	9/ 5/67
3,373,245	N. D. Newby, H. E. Vaughan	8/27/42	3/12/68
3,394,314	L. G. Schimpf	7/17/43	7/23/68
3,405,362	R. H. Badgley, L. G. Schimpf	12/20/43	10/ 8/68
3,470,323	H. W. Dudley	6/30/44	9/30/69
3,967,066	R. C. Mathes	9/24/41	6/29/76
3,967,067	R. K. Potter	9/24/41	6/29/76
3,985,958	H. W. Dudley	12/18/41	10/12/76
3,897,591	A. A. Lundstrom, L. G. Schimpf	8/27/42	7/29/75
3,912,868	R. H. Badgley, R. L. Miller	7/17/43	10/14/75
3,937,888	O. Myers	7/17/43	2/10/75
3,991,273	R. C. Mathes	10/ 4/43	11/ 9/76
3,979,558	E. Peterson	6/30/44	9/ 7/76
3,976,839	R. L. Miller	6/30/44	8/24/76
3,965,296	R. L. Miller	6/30/44	6/22/76
3,887,772	R. L. Miller	6/30/44	6/ 3/75
3,891,799	A. E. Melhose	9/27/44	6/24/75
3,893,326	D. K. Gannett	9/27/44	9/28/76
3,968,454	A. J. Busch	9/27/44	7/ 6/76
3,944,744	D. K. Gannett	5/10/45	3/16/76
3,944,745	D. K. Gannett	5/10/45	3/16/76
3,953,677	D. K. Gannett	5/10/45	4/27/76
3,953,678	D. K. Gannett	5/10/45	4/27/76
3,924,074	E. Peterson	5/19/45	12/ 2/75
3,983,327	D. K. Gannett, A. C. Norwine	7/ 9/45	9/28/76
3,934,078	D. K. Gannett	5/ 1/46	1/20/76
3,965,297	D. K. Gannett	5/ 1/46	6/22/76
3,924,075	D. K. Gannett	3/20/47	12/ 2/75

While the project was important as the initial development of a completely secret speech transmission system, historically it was also important as the pioneering digital speech transmission system employing a form of pulse code modulation. It was one of the starting points of the digital transmission age that followed. Although it remained for years as an unmentionable system, many knowledgeable people in Bell Laboratories became acquainted with its operating principles either through working on the project or being consulted about some aspect of it. In spite of this widespread knowledge, very effective security was maintained for many years. A list of patents related to this project is given in Table 5-5.[23]

[23] For reasons of secrecy the basic patents and all details were withheld until1975.

As noted previously, it was decided initially to assign two large groups to this project, one to carry on basic research and the other to handle the practical problems of design, instruction, and introduction to use. The Transmission Research group under R. C. Mathes was assigned the research task, one reason being that it included work on the vocoder under E. Peterson and H. W. Dudley,[24] inventor in the early 1930s of the vocoder. From the outset the vocoder was a logical candidate for consideration as a practical means of enabling the encipherment of speech signals, its virtues being that it offered a theoretical 10:1 frequency compression ratio for speech transmission and, secondly, that the control signals were in the telegraph range.[25] An important prior example of a perfect ciphering arrangement was the telegraph system invented by G. S. Vernam during World War I (discussed in Section 3.5.1 above). It seemed likely that the vocoder might lead to an equally effective scheme for encoding speech.

The systems, as finally used during World War II, were not small. A terminal occupied over 30 of the standard 7-foot relay rack mounting bays, required about 30 kW of power to operate, and needed complete air conditioning in the large room housing it. Members working on the job occasionally remarked about the terrible conversion ratio—30 kW of power for 1 milliwatt (m W) of poor-quality speech.

However, the system worked. One can look back on it with a certain amount of pride, since today's equivalent of about 1,500 bits per second was transmitted and maintained in complete synchronism over the fading of the transatlantic shortwave radio with only occasional errors. The system would become inoperative about the same time the normal commercial transatlantic radiotelephone would become unusable. Transpacific links were apparently somewhat better than the transatlantic. Operators of the system have stated that connections were actually tested successfully that went across the Atlantic and the continental United States and thence across the Pacific to Australia, although it is not known that any official conversations were ever carried over such a path.

The remainder of the war period was spent in developing a second system, which was called "Junior X," or AN/GSQ3. It occupied only six 5-foot bays and could be placed in a movable van but was not completed in time to see active service.

4.3.2 Invention

During the first two or three months following the inception of the project in October 1940, a large part of the thinking and experimentation reflected earlier thinking on speech privacy. There was no lack of ideas. A search by the Patent Department at the time uncovered about 80 patents.

[24] H. W. Dudley; U.S. Patent No. 2,151,091; filed October 30, 1935; issued March 21, 1939.

[25] A more complete description of the vocoder is given in Section 4.3.2.

But all of these methods invariably had one fault in common: they were just complex ways of transmitting speech that a person could undo with the necessary equipment and enough time. These were privacy, not secrecy, systems. In a secrecy system it is assumed that an eavesdropper having the same equipment as the intended receiver cannot determine the message unless he knows the coding sequence.

The vocoder, a frequency compression device for the transmission of speech, was a logical prospect for investigation and study, since the process of the vocoder resulted in a privacy system. The basic premise of a vocoder is that the information carried by a speech wave varies at relatively slow rates. These rates depend on how fast a person moves his lips and tongue (i.e., on vocal tract configuration). This motion modulates the sounds emanating from the person's mouth. The simplified functional schematic shown in Fig. 5-31 illustrates the operation of the vocoder. The frequency spectrum of a speech wave is first divided into ten nearly equal bands in the range of 150 Hz to 2,950 Hz. The amplitude of the speech signal in each band is obtained by means of a linear rectifier and smoothed by a low-pass filter, which limits the variations to less than 25 Hz. In an auxiliary process it is necessary to determine whether the sound is voiced (vowel or consonant sounds, such as *o, v,* or z) or unvoiced (such as the sibilant sounds of s or *sh).* If the sound is voiced, it is necessary to measure the pitch, or fundamental frequency. This information also varies at slow rates and can be limited by a 25-Hz low-pass filter.

After transmission of the 11 low-frequency channels to a receiving terminal, the speech can be reconstructed. This is done by first generating a source of harmonics of the fundamental frequency if the sound is voiced or by using a white noise source if the sound is unvoiced. These energy sources are appropriately switched into a set of bandpass filters similar to those used in the analysis. The output of each filter is then amplitude-modulated under control of the corresponding spectrum signal from the transmitting end. The modulated outputs of the 10 channels are then combined to give a reconstructed speech signal.

The spectrum control signals resulting from this spectrum analysis are at syllabic rates (below 25 Hz) or in the telegraph range (and unintelligible). Early proposals were pointed toward permuting the 11 control channels, but it was soon realized that this was closely analogous to the A-3 split-band privacy system.

In early January 1941, both R. C. Mathes and R. K. Potter discussed the adding of random noise signals in the syllabic range to the control signals of the vocoder, with the thought of using the same noise signals in opposite polarity to remove the masking at the receiving end. But it became clear that unless a large ratio of noise to signal were used the presence of speech signals would be apparent, and that if large amounts were used it would be at least difficult, and probably impossible, to balance out.

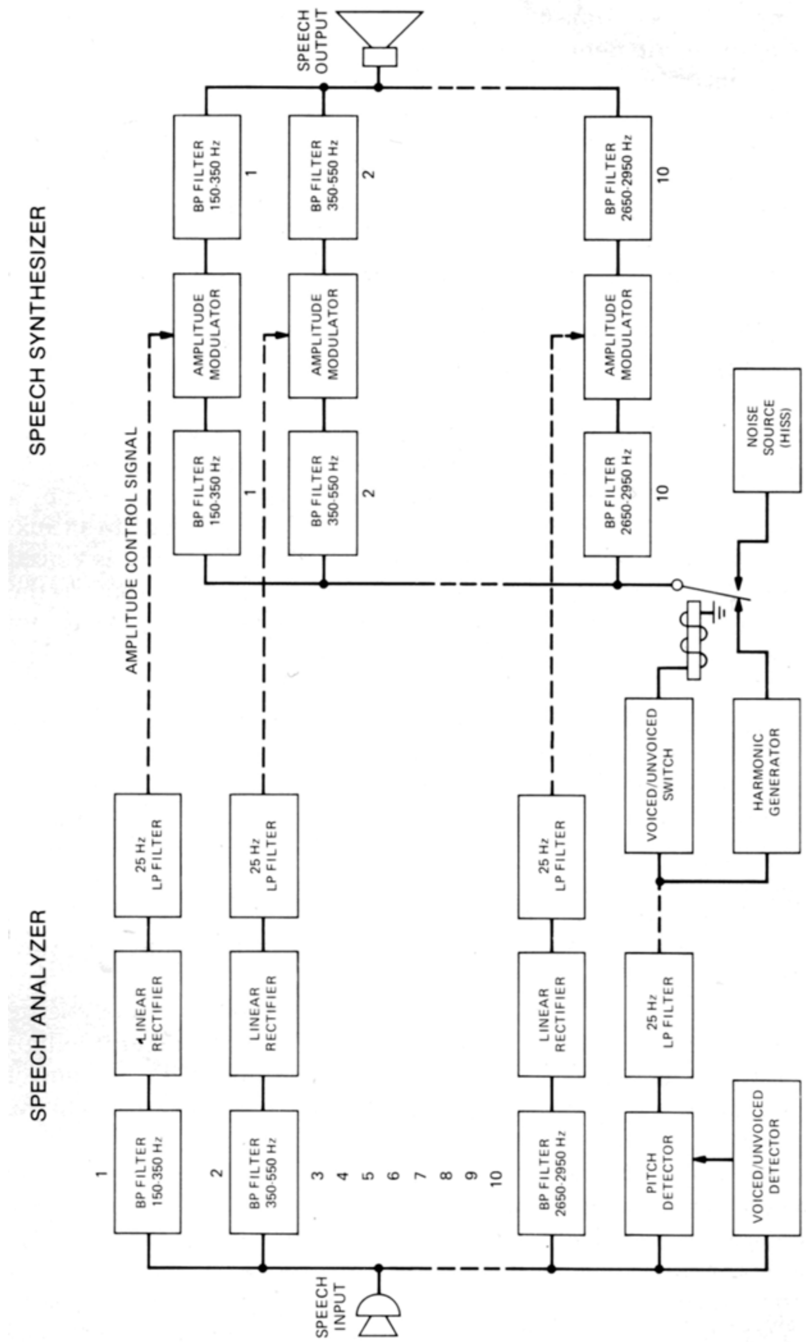

Fig. 5-31. Simplified schematic of a vocoder.

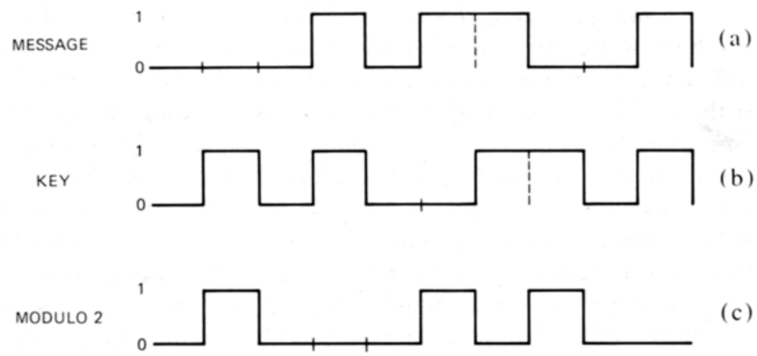

Fig. 5-32. Diagram of the addition of message and key signals by the Vernam method.

At this point, a letter was received from W. G. Radley, of the British Post Office, requesting design information26 on the vocoder and hinting that it was to be used in a secrecy system. This acted as a stimulus to the brainstorming that was going on at Bell Labs. Incidentally, the information that was sent to the British was sunk by submarine attack and had to be forwarded a second time.

As mentioned above, the outstanding example of a perfect ciphering system was the Vernam system[27] used on telegraph signals. It involved the addition of a random or nonrepeating set of on-off telegraph signals to the message signals by a process now called Modulo 2 addition, or, more commonly, "half-adding." The Vernam process as used with teletypewriters is illustrated in Fig. 5-4. To readers trained in logic, Fig. 5-32 may provide an explanation in more familiar terms. In this diagram the on-off (0, 1) values of a possible telegraph message and a key are shown in lines (a) and (b). The Modulo 2 addition of the two signals is shown in (c). It will be noted that if the sum of the message and the key do not exceed 1, the sum of the two values is obtained. If the sum is equal to 2 (M = 1 and K = 1), a 0 is substituted. This means that if the message value is 0, either 0 or 1 can result, depending on the key value; likewise, if the message is 1, then 1 or 0 can result. Hence, if the key has a random occurrence of values, it will result in a transmitted message that is also random and cannot be undone unless a copy of the key tape is available. With this tape at hand, the key signals can be added to the transmitted signal to provide the original message. The feeling that this same sort of process was necessary in communicating speech was a constant nagging thought with people who were working on the problem.

[26] O. O. Gruenz, "The Construction Information on the Rebuilt 10 Channel Vocoder," internal Bell Labs memorandum, February 24, 1941.

[27] G. S. Vernam; U.S. Patent No. 1,310,719; filed September 13, 1918; issued July 22, 1919.

Finally, in late February, the first real breakthrough resulted from a proposal by R. K. Potter[28] that the individual vocoder channels be treated as on-off channels by the use of a relay with a suitably adjusted bias. This solved the problem of adding the key, as in the Vernam approach, but experiments in the vocoder by O. O. Gruenz soon indicated that the quality and intelligibility of vocoder speech was badly mutilated. The next obvious step was to use two relays adjusted to different values in each channel to improve the quality; while there was some improvement with this move, it was becoming apparent that quite a number of step values were needed to get the quality that might be acceptable. This approach will be recognized as the process now known as quantization—i.e., representing a continuously variable signal by means of a series of steps which approximate the continuous function. It is interesting to note that up to the point of using two or more steps per channel, the rationale called for treating the on-off pattern of the 10 vocoder channels as a telegraph character. The addition of the *N*-level dimension in each channel shook the thinking loose from this mooring.

The need for multiple levels in the vocoder channels led directly to considering the use of a similar multilevel key signal. However, the problem of how to combine the stepped key and message signals to achieve a result similar to the Vernam process became a puzzle. A clue to how this should be accomplished came from a discussion on May 27, 1941, between R. K. Potter and H. Nyquist, who came to the conclusion that the sum of the key and message should "fall as points on a circle." In other words, if the sum became larger than the maximum level, the value should reenter as in following points around a circle; hence the term "reentry," which was to be used as a descriptive term for this critical process. In today's logic language it would be termed modulo N addition. Mathematically, it is relatively simple to describe the process, even though it was not easy to think of it in the first place. If we let M be an integer value of the message $(0,1,2, \ldots, n)$, K the value of the key, and C the maximum number of levels of either $(n + 1)$, then the reentered value R is

$$R = M + K \qquad (M + K \leqq C) \tag{1}$$

$$R = M + K - C \qquad (M + K > C) \tag{2}$$

Decoding at the far end is accomplished by subtracting a duplicate of the key from the reentered value. The message number is given directly if the result is positive, but with a negative result it is necessary to add $n + 1$ to give the message number. One possible way to visualize the process is in terms of a clock face with successive positions $0,1, \ldots, n$ with the speech levels (and the added code levels) stepping the hand by

[28] R. K. Potter; U.S. Patent No. 3,967,067; filed September 24, 1941; issued June 29, 1976.

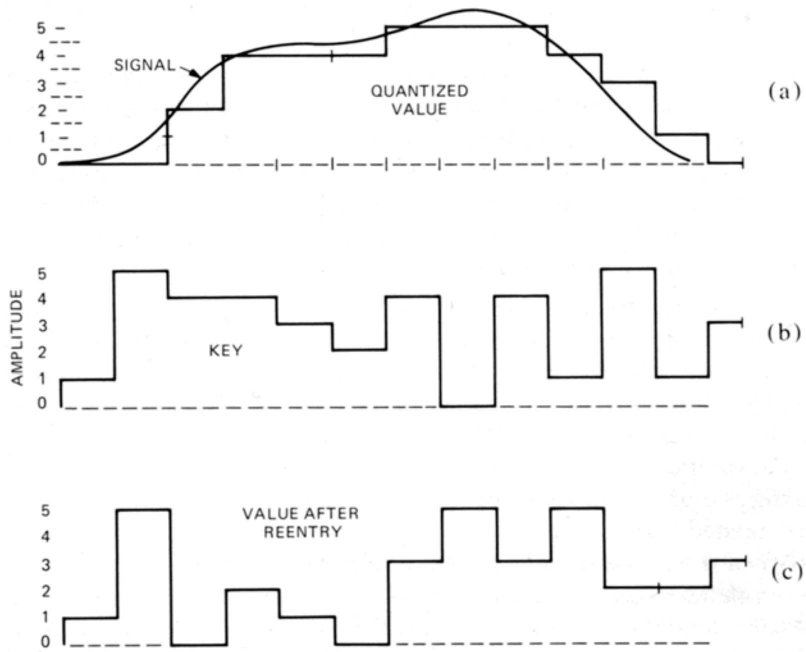

Fig. 5-33. Diagram of signal quantizing and the subsequent addition of key by the reentry process.

amounts corresponding to the quantized signal and key levels. Thus, when the signal and key are added, the sum is indicated directly if it is equal to or less than n. If it is greater than *n*, the hand continues on a second round and points to a reentered number equal to the sum less *n*+1.

An illustration of the reentry process is shown in Fig. 5-33. Here the original analog signal is quantized by the stepper to the closest of the six available levels, as shown by (a). The key (b) consists of a random series of the same possible quantized values. The reentered values, as given by equations (1) or (2), are shown in (c). It will be observed that if the sum exceeds 5, then the reentered value will always fall in the range of 0 to 5; likewise, any particular value of a signal, when reentered, can also result in any one of the six values, depending on the key value. Thus, just as in the Vernam approach, a random series in the key will result in an equally random series in the transmitted message, although not the same one. At a meeting in R. C. Mathes' office in the afternoon of the discussion between Potter and Nyquist, the thoughts on reentry jelled into a definite circuit proposal,[29] and the general building blocks of the overall system started

[29] R. C. Mathes; U.S. Patent No. 3,991,273; filed October 4, 1943; issued November 9, 1976.

to fall into place. A decision was made forthwith to proceed with the system's implementation.

While progress thus far represented a major breakthrough, the work and the inventing were far from over. In the end some 30 patent applications were filed. Thus, the final system represented the contributions of many minds. At this point, though, there were many aspects to be considered in addition to quantizing and reentry. Some of the main ones were the parameters of the vocoder, the mode of transmission to be used, synchronization, and production of the key.

About quantizing, one of the first problems to be solved was how many levels were needed for the vocoder. A quantizer, probably the first in existence, was constructed by M. E. Mohr; with it, any number of levels up to ten could be tried, and numerous tests could be carried out with the vocoder. Toward the end of the tests the use of nonlinear steps (instantaneous companding) was tried to obtain an improvement. Just who made this suggestion was never recorded. How many steps or quantized levels were needed turned out to be a compromise between an increase in the quality of the vocoder and a decrease in margins for the transmission of the stepped levels by FSK (frequency-shift keying) over such a circuit as transatlantic radio. The value that was finally settled on was six levels, which was somewhat over the knee of the curve in improving the quality of the vocoder and a reasonable possibility in transmission. In the end this turned out to be an excellent selection and was never changed. The basic design for the stepper and reentry circuits was carried out primarily by A. A. Lundstrom and L. G. Schimpf.[30] The design made use of a suggestion by H. W. Dudley[31] on how to simplify the originally proposed method of carrying out the reentry process.

A problem developed, however, in the transmission of the pitch signal of the vocoder, which turned out to be much more susceptible to the quantizing effect. Experiments soon indicated that it was going to need some 30 or more steps. The thought of using five channels to transmit this signal was not easy to accept. Shortly thereafter, a suggestion was made by R. H. Badgley and R. L. Miller[32] to use a technique which was likened to a vernier. The pitch signal would first be quantized to the nearest of the six levels, and then this value would be subtracted from the original signal. The remainder was then coded again to six levels.

An illustration of this process is given in Fig. 5-34. First a sample of the original pitch signal is taken. This acts to operate the main stepper.

30 A. A. Lundstrom and L. G. Schimpf; U.S. Patent No. 3,897,591; filed August 27, 1942; issued July 29,1975.

31 H. W. Dudley; U.S. Patent No. 3,985,958; filed December 18, 1941; issued October 12, 1976.

32 R. H. Badgley and R. L. Miller; U.S. Patent No. 3,912,868; filed July 7,1943; issued October 14, 1975.

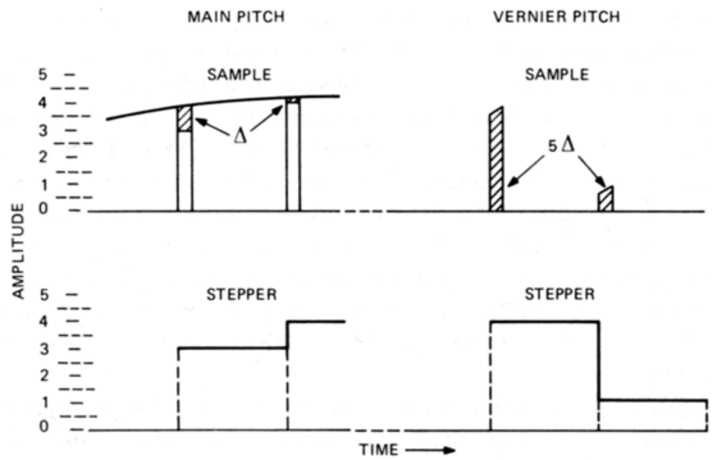

Fig. 5-34. Signal quantizing by means of the Vernier process.

The quantized value of the stepper, subtracted from the original pitch signal, will leave a small residual value Δ. The maximum possible value of Δ will be one-fifth of the total input range of the stepper; hence, after being multiplied by 5, this signal can be used to operate the same type of stepper as was used for the main operation. When the reverse process is carried out at the receiving terminal, the value of the vernier stepper must be divided by five before addition to the main value.

The vernier process in effect gave N^2 or 36 levels with two channels. It was soon realized that this was a very general process. Different numbers of channels and steps could be used to obtain many combinations (M^{ary} coding). Binary coding was one of the possible combinations to be considered, but at that time it was just another possible combination that did not lead in the right direction for the problem at hand.

A more important consideration was the fact that the desirable sampling rate of the vocoder channels was 50 Hz or a 20-millisecond (ms) sampling interval. Since it was known that the path delay differences causing selective fading on the transatlantic radio could be of the order of 2 to 3 ms, it was imperative that the sample interval be kept much longer; hence the six-level arrangement with a 20-ms sampling appeared to be about the best solution. Rather interestingly, this direct approach to multiple levels closely resembles the present practice in data sets, which convert to either four- or eight-level signals with longer sample intervals to obtain optimum transmission.

4.3.3 Transmission

The problem of transmitting a stepped or amplitude-quantized wave with multiple levels was a new situation. There was, of course, considerable experience with two-level telegraph signals. It soon became apparent that the use of amplitude modulation was not going to be possible on the transatlantic radio in the face of selective fades that could at times be as much as 20 dB. A six-level signal meant that amplitudes must be reproduced within about ±10 percent (1 dB). FSK (frequency-shift keying) had been used successfully with two-level telegraph signals and a similar scheme appeared to be the best solution for transmitting the X System signals. However, the job was much more complicated. For telegraph signals only two frequency positions were required to represent the two-state on-off signal. The X System used 6 frequency positions in each of 12 channels to represent all the information required for each speech sample.

Fortunately, sets of filters were available that could save much design time. Critical designs were required in both the frequency-shift oscillators and the limiter-detectors to obtain the required accuracy, stability, and freedom from transients at the pulse transition points. The oscillators were designed by M. E. Mohr around the use of a saturated-core inductor. L. G. Schimpf was mainly responsible for the limiter-detection circuit[33] for the receiving terminal.

For the first time the problem of the design of the filter system to give an optimum sampling of multilevel pulsed signals was encountered. This is the familiar "opening-of-the-eye" [34] problem in today's data systems. W. R. Bennett,[35] in an extension of H. Nyquist's telegraph theory, produced an excellent, as well as timely, solution to this difficult problem.

4.3.4 System Outline

A general outline of the system as it evolved is shown by Fig. 5-35. Actually, this is a functional schematic of the transmitting terminal; however, as will be explained later, the receiving terminal is surprisingly similar in structure. The slowly varying dc signals from the vocoder analyzer spectrum and pitch channels are applied to the message steppers, where they are periodically sampled as outlined in the processes of Figs. 5-33 and 5-34. The key steppers are quite similar but are operated directly by filtered signals from a phonograph record.

After the reentry process (Fig. 5-33), another stepper is used to regenerate the quantized signals. These signals are then used for controlling the FSK transmitting units (frequency modulation oscillators). The signals

[33] L. G. Schimpf, "A Regulated Limiter for Use in the X System," internal Bell Labs memorandum, September 30, 1942.
[34] This refers to the visual representation on a cathode ray tube display of the signal-to-noise margin of a data signal after modulation. A high quality signal has the appearance of an open eye. Distortion and other impairments tend to close the eye.
[35] W. R. Bennett, "Low Pass Filter Design for FM Detector Output of System," internal Bell Labs memorandum, March 3, 1942.

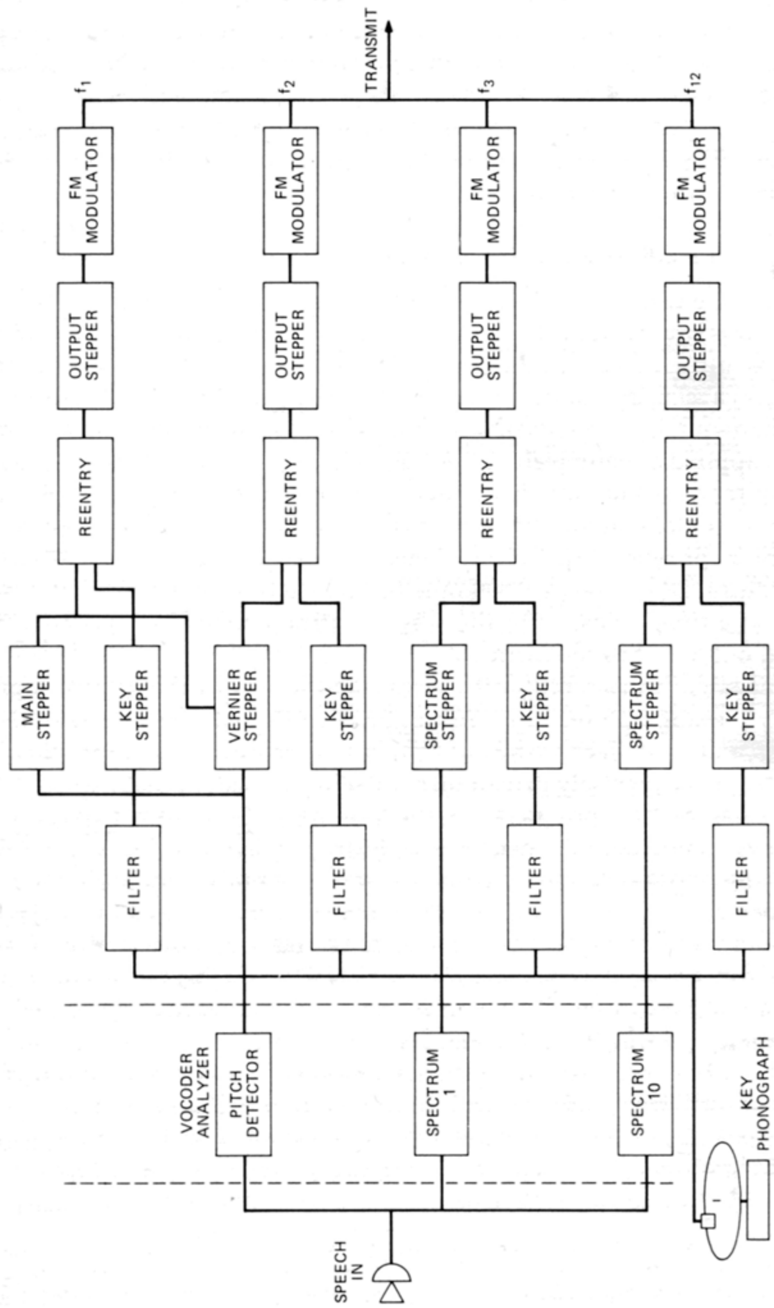

Fig. 5-35. Simplified diagram of the X System.

from these units are combined and transmitted to the receiving terminal. At the receiving terminal the quantized signals are reconstructed by frequency modulation detectors. From this point on the signals can be operated on in almost exactly the same manner as they are for the vocoder signals in the transmission terminal. By placing a simple inversion in the output signals of the fm detectors, the same reentry process will remove the key. The signals from the output steppers are then passed on to the vocoder synthesizer inputs.

4.3.5 Key Production and Synchronization

While the concept of having a key with six levels strictly random in nature was simple in itself, the actual implementation of this was one of the most difficult tasks in the development of the X System. Needless to say, from a security standpoint it was also the most sensitive. One of the well known requirements of a random step key for the Vernam system, which applied equally well to the X System, was not only that it be completely random but also that it never be repeated. Another problem, which might look prohibitive even to today's data transmission engineers, was the requirement that the systems be synchronized and maintained in synchronization over a 9,000-mile link, including shortwave radio, for hours at a time. Thanks to the way the parameters were chosen, this turned out not to be too difficult.

After much consideration it was decided to record the key on high-quality phonograph records. As might be imagined, the success of this approach hinged on carrying out a precision recording and reproducing process. Very precisely driven turntables were used for making the records as well as the reproduction at the terminals. Since only two records were ever made before a master was destroyed, even the very unlikely breaching of the elaborate distribution arrangement would probably not have been very useful. Early work on the key system was done by H. E. Vaughan[36] and N. D. Newby. Much of the responsibility for the final system rested with A. C. Norwine[37] and K. H. Davis. A great deal of credit for the mechanical design of the precision recording and reproducing equipment was due W. A. Marrison and I. E. Cole.

Although it occurred later, in the development phase, the design of a "mechanical" key source by A. J. Busch, O. Myers,[38] and A. E. Joel, Jr., rightly belongs under the heading of invention. This device, which made use of many relays, was affectionately called the "threshing machine" because of the noise it made in operation. Its theoretical security was not

[36] N. D. Newby and H. E. Vaughan; U.S. Patent No. 3,373,245; filed August 27,1942; issued March 12, 1968.

[37] A. C. Norwine, "Noise Sampling Means for Vocoder Key Producer," internal Bell Labs memorandum, June 4, 1942.

[38] O. Myers; U.S. Patent No. 3,937,888; filed July 17, 1943; issued February 10, 1970. A. J. Busch; U.S. Patent No. 3,968,454; filed September 27,1944; issued July 6,1976.

absolute like the records; so it was never used for high-priority calls. But it was very useful for lineup and testing procedures, which made it possible to avoid using the precious records.

Although the synchronization of the systems initially looked like a formidable job, it was finally solved by the use of very precise frequency standards at each terminal. Because of the long message sample intervals (20-ms), once the system had been started in synchronization it would run for several hours without drifting out appreciably, and long-term drifting could be easily corrected. Short-term variations on even the longest links were never large enough to give trouble. Although links might fail for considerable periods, the system would still operate when transmission was restored.

An automatic frequency corrector designed by H. L. Barney made it possible to correct for frequency shifts which might occur in carrier or radio systems. In particular, this capability made it feasible to operate over long land links without upsetting the FSK transmission system.

4.3.6 Vocoder

Research and development on the vocoder had been carried out since about 1936 under H. W. Dudley. Thus it was much better developed than other parts of the system, which, for the most part, were quite new. Nevertheless, considerable effort was continuously applied to improve the quality and reliability of the vocoder. One of the main problems involved the derivation of reliable pitch signals from a wide range of talkers. Much credit is due R. R. Riesz for his work in this area throughout the war.

4.3.7 Experimental Model

A group under A. B. Clark was given the task of implementing design and construction of the vocoder. In the early stages of the project only a few members of the group were active, notably R. K. Potter, D. K. Gannett, and H. Nyquist. After several months of investigating and inventing, it became apparent that a workable system using the vocoder was feasible. For the first time digital coding of speech signals was utilized to accomplish the kind of task they were working on.

By late 1941 tentative designs and breadboard testing had been carried out for nearly all the system components without encountering any insurmountable snags. At this point it was decided to build a prototype model. To do this, the remainder of the Circuit Research group under A. M. Curtis was assigned to the job. A few had already been working on individual parts—e.g., I. E. Cole on phonograph turntables and H. E. Vaughan on the key. Besides making a complete working system, it was also desirable to have a complete set of working drawings so that the manufacturing process could be started if this step was decided upon.

A. E. Melhose did much of the coordination work in building the model as well as in developing the drawings. As the parts were finished, the system was assembled on the twelfth floor of the Graybar-Varick building in New York City.

The X System was made up of 12 parallel channels (10 spectrum, 2 pitch), which were nearly duplicates of each other except for their frequency position in the FSK arrangement. In March 1942 one complete channel of the experimental model became available for making fairly successful tests on an artificial fader simulating the fading of the transatlantic shortwave radio. In April a complete set of drawings was sent to J. L. Dow of the Switching Development group to arrange for manufacture. E. W. Olcott was to be in charge of the follow-up of manufacture.

The experimental model was completed in the latter part of August and was quickly tested for operation and stability. By November it was being tested over the transatlantic radio[39] with a synthetic set of signals from a signal generator that had been previously sent to England. As refinements of the system became available, they were continuously being tested and substituted in the experimental model to keep it up to date. This process was continued until mid-1943 when the manufactured systems were being installed in the field. So long as the experimental model was being updated, it served as demonstration equipment for training Signal Corps personnel.

4.3.8 Development and Manufacture

By August 1942 the research prototype model was completed. Enough experience had been obtained with the individual parts of the system to have confidence that the complete system would be successful. Up to this point Bell Laboratories had carried out the work on its own initiative, although NDRC and the Signal Corps were aware of the work and interested in the program. As early as February 3, 1941, General Mauborgne, Chief Signal Officer, had called attention in a radio talk to the problem of maintaining secrecy on the telephone in military service. Shortly thereafter (April 23), Potter made a trip to Washington to brief him on the possibilities as Bell Labs saw them. At about the time of the completion of the experimental system, the Signal Corps decided to sponsor the building of several terminals.

To carry out this expanded project, the effort was considerably reorganized and expanded in September 1942. P. W. Blye was appointed project engineer and given overall responsibility for coordinating the engineering and manufacture of the final system. He brought with him a large group from Transmission Engineering to aid in the process. The

[39] W. R. Bennett, "Transmission Over Fading Medium," internal Bell Labs memorandum, November 1, 1943.

work of the research group on the experimental model, which had been going on in several groups of the Circuit Research Department, was pulled together under D. K. Gannett. E. W. Olcott and C. R. Gray would direct the actual manufacture at Western Electric.

The first main effort was to go over the drawings of the experimental model to convert them into manufacturing drawings suitable for use by Western Electric. Emphasis was placed on substituting readily available standard components wherever feasible. The use of standard Western Electric amplifiers for gain was one important substitution, since many of the operations were carried out in the audio range. While this change added to the size of the overall system, it aided considerably in reducing the time for manufacturing. One Transmission Engineering group under D. Mitchell carried out this conversion process for the message coding equipment as well as arranging for the manufacture of the key records. Another group, under J. M. Barstow, carried out the same process with the vocoder system.

By the end of September the flood of orders for component parts had started. Arrangements had been made for Western Electric to manufacture the system at the vacuum tube plant on Hudson Street, New York City, a convenient location with respect to West Street and the Graybar-Varick building. A substantial number of manufactured system items were being obtained from Western Electric by January 1943. As items were finished and preliminary testing was completed, the parts were taken to Room L30 at West Street, originally the sound movie laboratory, and assembled as a system. The first system was completed by April 1; shortly thereafter, a second system was also assembled in the same area, the first system serving as a test vehicle to aid in checking out the second. By the end of April 1943, some two months prior to the invasion of Italy, several terminals were completed and installed in Washington, London, and North Africa.

This process was to be repeated over and over again as additional systems were made ready. Each would be assembled as a complete system, checked, disassembled by bays, and sent out to where it was to be installed. The shipping and installation of the finished systems for the European theater were carried out during June and July 1943. A system was installed in Washington, D.C., almost simultaneously with the assembly of the first system in Room L30. Other terminals were later installed in Paris, Hawaii, Australia, and the Philippines. Thus in the short span of about seven months a large and complex communication system, much of whose circuitry was completely new, was engineered, manufactured, and installed. It was a good example of Bell Labs' ability to bring to bear its varied talents and skills on a complex problem—which was demonstrated a number of times during the war.

To have trained people capable of handling these complex systems, Bell

Labs started a school for Signal Corps personnel about the same time manufacturing of the system began at Western Electric. Though isolated, this was actually part of the Bell Labs School for War Training administered by R. K. Honaman.[40] R. N. Hunter originally headed up the school for the X System. The Signal Corps set up what became known as the 805th Signal Service Company to handle the system. This company was a rather unusual one in that it contained almost as many officers as it did enlisted men, and nearly all the enlisted men were technical sergeants. Practically all the personnel had previously worked in the Bell System. They were not informed of what they were to be working on until their first briefing at Bell Laboratories. Only enough specialists to handle a few systems were trained at first. After being indoctrinated in the principles and circuits of the system, they were trained first on the experimental system and finally on the actual system. In the end they were usually involved in the testing and dismantling of the particular system they were to work with in the field. In all, 186 Signal Corps personnel were trained.

To ensure that the systems would function in the field, a team of two or three Bell Labs engineers accompanied each system to help in putting it into operation. The teams were often composed of one engineer from the Research area who knew the circuit operation intimately and others from the transmission and switching engineering groups who had been closely associated with the system as it was being put together. The manufacture and installation of the systems continued until about the middle of 1944.

4.3.9 Junior X *System – AN/ GSQ3*

The size of the X System was not an accomplishment to be very happy about. Its use was feasible in a headquarters type of situation but not very practical in tactical situations. A number of possibilities for reducing its size had suggested themselves as the project progressed, but time was always the controlling factor. In the spring of 1943, as the assembly of the first manufactured X System was nearing completion, the pressures on the work of the Research group diminished considerably. At this point the Research people made a serious effort to see just how much the size could be reduced.

A step in this direction had already been made in a study[41] undertaken with the experimental system to reevaluate the effects of the number of quantized levels and of the number of vocoder channels on overall speech intelligibility. R. R. Riesz and O. O. Gruenz of the Research Department,

[40] See Section VI, Chapter 1.

[41] D. K. Gannett and R. L. Miller, "The Effect on Intelligibility of Reducing the Number of Channels and Steps and Increasing the Sampling Interval," internal Bell Labs memorandum, April 17, 1944.

working in cooperation with R. C. Edson and J. M. Barstow of the Transmission Engineering group, examined the basic vocoder system both with respect to an optimization of the number of channels to be used and with respect to the circuit design.

It was obvious from the start that a considerable saving in size could be obtained if specific circuit designs were optimized, rather than using existing amplifiers, power supplies, frequency standards, etc. Under pressure of the war, many vacuum tube types had also been reduced to miniature size. Basic redesigns of the FSK oscillators by M. E. Mohr[42] and the detectors by L. G. Schimpf[43] substantially reduced the size of these, especially with the miniature tubes. A proposal by R. L. Miller[44] to carry out the quantizing and coding operation in a single multiplexed arrangement, parallel to serial conversion, reduced the number of coders-decoders by a factor of 12. A more sophisticated form of the mechanical key was converted to an essentially all-electronic system, following suggestions of D. K. Gannett, A. E. Melhose, and M. E. Mohr.

The work on the basic design of the vocoder indicated that the number of spectrum channels could be reduced to eight without greatly affecting quality and intelligibility. This allowed a realignment and widening of the FSK channels and produced a corresponding improvement in transmission margins.

An outline of the much simplified system is shown in Fig. 5-36. With a serial sampling of the various vocoder channels, a common higher-speed quantizer and reentry system could carry out the necessary logic functions. By keeping the time between samples of a given channel to the 20 milliseconds used in the senior X System, an equivalent operation was obtained. With a holding, or clamp, arrangement at the output distributor, the signal operating the FSK transmitting oscillators was also kept at the 20-ms width necessary for overriding fading. This technique kept the synchronization problem the same, since the sampling of the transmitted signals was the critical process.

The design engineering and manufacturing procedures for the Junior X, or the AN /GSQ3 system (as it was later coded by the Signal Corps), followed a pattern similar to that of the Senior X System. In general, the same people followed up and worked on the same aspect of the system they had worked on before. The design and construction of the experimental prototype in the Research group occupied about a year.

In the fall of 1944, the Signal Corps contracted for a number of the systems. These were also built under the overall supervision of P. W. Blye,

[42] M. E. Mohr, "The Multivibrator as a Frequency Modulator," internal Bell Labs memorandum, April 17, 1944.

[43] L. G. Schimpf, "An Audio Frequency FM Demodulator," internal Bell Labs memorandum, April 17, 1944.

[44] R. L. Miller; U.S. Patent No. 3,965,296; filed June 30,1944; issued June 22,1976.

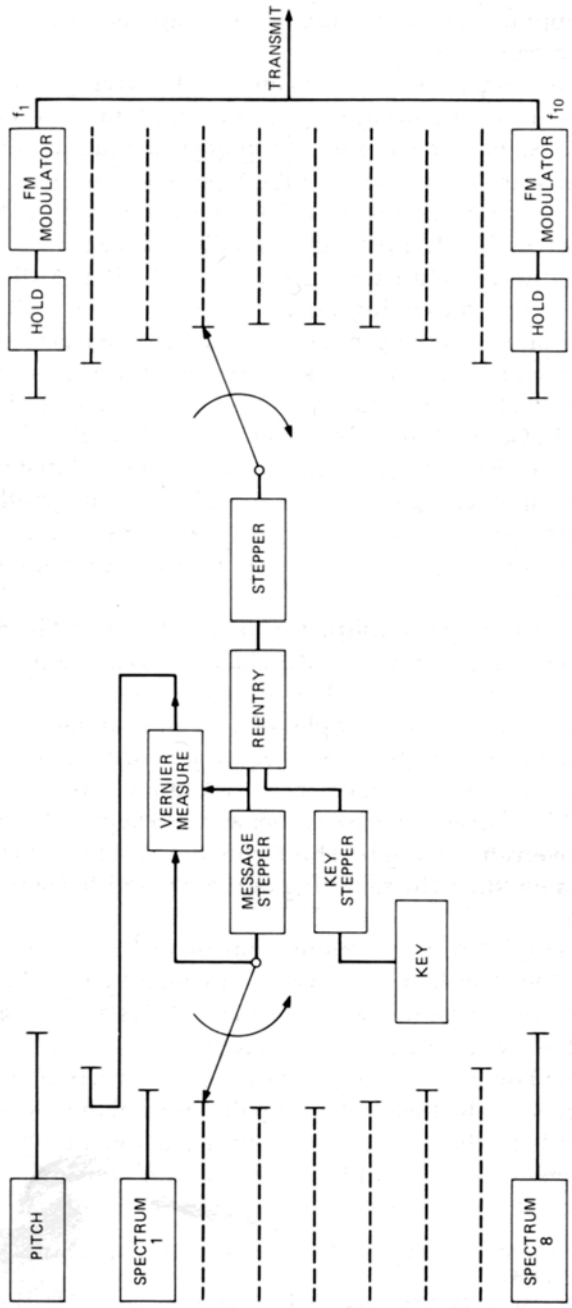

Fig. 5-36. Simplified diagram of the Junior X System (AN/GSQ3).

with J. M. Barstow having the major responsibility. The system as finally constructed occupied only six 5-foot bays and could be placed in a trailer van. The systems were delivered in March 1946, too late for use in the war.

4.3.10 Application

As might be expected from the nature of the X System, not much is known about experience with it in the field, although numerous stories drifted back with returning technicians. A general staff officer was reported to have said that it was very valuable during preparations for the invasion of the Philippines.

A terminal intended for use in the Philippine invasion was unloaded in the surf at Port Moresby in New Guinea. The salt water bath did not help some of its sensitive electronic circuits, designed for air-conditioned surroundings. However, the equipment was cleaned in record time and put into service on a barge. The detachment of the 805th Company in charge received a citation for its efforts from General MacArthur. Bell Labs also received a War Department Citation for the development of the X System.

Even though it was one of the most sophisticated pieces of cloak-and-dagger equipment developed during World War II, stories concerning the X System seem to have been either very dull or infrequent. An investigation team touring Germany after the war apparently uncovered an intercept station that had recorded reams of the signals but had come to the conclusion that they were the output of a complicated telegraph system. This lack of knowledge even of the system's objective probably accounts for the lack of stories.

One of the big thrills for workers on the X System came from a picture and article in Life magazine describing Winston Churchill's underground headquarters in London. Plainly visible was the telephone set especially designed for use with the X System vocoder. The handset had a distinctive ball-shaped transmitter which had been adapted from the Western Electric "8 Ball" high-quality microphone.

4.3.11 Coding

As we have seen, the early phases of brainstorming and inventing for the X System in 1941 were, because of its hush-hush nature, largely confined to people in the higher echelons of Bell Laboratories and to a few restricted groups, mainly in the Research Department. As the processes of keying, quantizing, and coding of the signal evolved, considerable interest and enthusiasm developed among these people. It was a new area to think about, creating considerable discussion and speculation about its many facets. The ability to regenerate the quantized signal in the face of noise, along with the different possible combinations of quantization, raised some intriguing questions. The relation of the signal-to-noise ratio to the probability of reproducing the signal was brought into sharp focus.

R. V. L. Hartley and H. Nyquist, major consultants at Bell Laboratories, were especially interested in the project. Hartley in particular found the possibilities interesting because they were related to some of his previous pronouncements on the transmission of information. He wrote a memorandum[45] philosophizing on the various processes in the system. M. E. Mohr, one of the more mathematically inclined researchers, had reached a tentative conclusion that a "tertiary," or three-level, system would probably be most efficient for general coding.

It was not until about the middle of 1943 that Bell Labs people became aware of the use of binary coding as already proposed by Alec H. Reeves, of The International Telephone and Telegraph Co. Reeves had filed for a French patent in 1938, but his U.S. patent[46] had not been issued until late 1942. In describing his invention, Reeves later wrote, "Having had it patented, for understandable reasons I then let the invention slip from my mind until the end of the war. It was in the United States during World War II that the next step in PCM's progress was made, by the Bell Telephone Laboratories." [47] Reeves was referring in particular to work carried out by H. S. Black and W. M. Goodall during and after 1943 (a part of the work being for the U.S. government) and described after the war by the first technical publications on PCM.[48,49] Others who contributed to this phase of work on PCM were F. B. Llewellyn, C. E. Shannon, and J. O. Edson.

This emphasis on binary PCM, which was mainly pointed toward wideband circuits, did make the personnel working on the X System take another serious look at the coding arrangement to be sure that something had not been overlooked. H. L. Barney[50] carried out a series of extensive tests with various possible combinations but came to the conclusion that for the situation it faced, the multilevel arrangement used was better. After the press of war work subsided, several people working on the X System or its fringes contributed to the further development of PCM, notably W. R. Bennett, E. Peterson, and L. A. Meacham.

It remained for C. E. Shannon to put together a complete theory of in-

[45] R. V. L. Hartley, "A Quantitative Measure of Amount and Quality of Information," internal Bell Labs memorandum, March 10, 1941.

[46] A. H. Reeves; U.S. Patent No. 2,272,070; February 3, 1942.

[47] A. H. Reeves, "The Past, Present, and Future of PCM," *IEEE Spectrum* 2 (May 1965), pp. 58-63.

[48] H. S. Black and J. O. Edson, "Pulse Code Modulation," *Trans. AIEE* 66 (1947), pp. 895-899.

[49] W. M. Goodall, "Telephony by Pulse Code Modulation," *Bell System Technical J.* 26 (July 1947), pp. 395-409.

[50] H. L. Barney, "Narrow Band Frequency Shift Transmission Using 2, 4, and 8 Valued Signals," internal Bell Labs memorandum, July 24, 1945.

formation. Shannon returned to Bell Labs in 1941 from M.I.T. and Princeton, where he had specialized in the application of Boolean algebra to switching. He had also become quite interested in cryptanalysis as a hobby. Although quite new in the company, his talents were well recognized and he served actively on some committees dealing with different aspects of cryptanalysis. He also became familiar with the X System, having been asked to take a close look at the reentry process to be sure that something had not been overlooked in the presumption that it was unbreakable. It is quite apparent that his work on cryptography and information theory was intimately tied up together, judging from his papers, "Communication Theory of Secrecy Systems" [51] and "A Mathematical Theory of Communication." [52] The former article was first issued as an internal memorandum in 1945, although it was not cleared for publication until 1949.

51 C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical J.* 28 (October 1949), pp. 656-715.

52 C. E. Shannon, "Mathematical Theory of Communication," *Bell System Technical J.*, 27 (July 1948), pp. 379-423 (October 1948), pp. 623-656.

A History of Engineering and Science in the Bell System

National Service in War and Peace (1925-1975)

Prepared by Members of the Technical Staff, Bell Telephone Laboratories.
M. D. Fagen, Editor.

Bell Telephone Laboratories, Incorporated

Credits for figures taken from other than Bell System sources appear on page 721.

First Printing, 1978

International Standard Book Number: 0-932764-00-2

Library of Congress Catalog Card Number: 75-31499

Printed in the United States of America

Part II. Post-World War 11-1945 to 1975

A note on this electronic version of

"Project X — A True Secrecy System for Speech," Section 4.3, RL Miller author,

pages 296 – 317 in:

"A History of Engineering and Science in the Bell System National Service in War and Peace (1925-1975)"

published 1978 by Bell Telephone Laboratories, Inc.
total 757 pages

This Acrobat version of Section 4.3 has been scanned and OCR'ed from the original book.

Though carefully read and corrected with the usual OCR ambiguities in mind, the detail neither of formal names nor of the numerous numbers, such as patent numbers and dates, has been proofread. Only a copy of the printed pages should be relied upon for such detail. That paper copy can be got, if needed to serve such a purpose, or indeed to proofread more exhaustively in general.

The font for the text has been changed, from the more graceful font used in the book (similar to Times New Roman) to a font more readable on a screen (Arial).

This leads to small infelicities at the end of pages, since the text is justified – but in this version not 'flowed' from one page to the next. The result may be a bottom line on a page that stops midway across the page; only a look at the next page can tell whether or not this actually indicates a new paragraph.

N.B.: Re reading on-screen, the document is set to open at 125 percent. Because of the smallish book font, some may find even higher magnification useful.

David Allen
October 2005