From Concept to Production in Secure Voice Communications

Earl E. Swartzlander, Jr.
Electrical and Computer Engineering Department
University of Texas at Austin
Austin, TX 78712

Abstract
In the 1970s secure voice communications systems were developed initially for military applications. This paper reviews the basic process that led from the initial concept to the limited production of secure voice communications systems based on the linear predictive coding (LPC) algorithm. The LPC algorithm enabled voice signals to be digitized at rates comparable to analog voice signals. This algorithm also achieved adequate fidelity so that listeners could confirm the identity of speakers which is extremely important for many applications.

This paper describes three systems which were developed over a several years period in the mid 1970s to confirm the viability of the algorithms and to develop a cost effective production implementation. The evolution of these systems from breadboard model to prototype and finally to production units demonstrates the process of developing application specific processors for volume applications.

Introduction
Prior to the mid-1960s nearly all voice communications systems were based on analog implementations [1] .In basic analog systems processing at the transmitter consists of relatively simple signal conditioning involving isolation, level setting and low pass filtering. Because the bandwidth is limited (typically to 3.3 KHz) transmission can be done over wire lines or narrow bandwidth radio links. Processing at the receiver involves level adjustment and filtering. Analog systems are generally unable to implement secure encryption and decryption functions.

A direct digital approach is shown in Figure 1. The conditioned speech signal (from the conventional analog system) is sampled at a rate of at least 8,000 samples per second (i.e., 8 KSPS) and quantized (i.e., digitized) with a precision of at least 8 bits per sample. This produces a digital bit stream with a rate of 64,000 bits per second (i.e., 64 KBPS). At the receiving end the bits are converted to an analog signal with a digital to analog converter and the analog signal is filtered.

The advantage of the digital system is that the digital bit stream can be encrypted yielding an apparently random bit stream of 64 KBPS. which is transmitted. It has the disadvantage that it requires a bandwidth of at least 64 KBPS which is a factor of 15 to 20 times the bandwidth of the original analog speech signal. Thus while the digital implementation can be made secure, it has the strong disadvantage that it requires much more bandwidth than the conventional analog implementation which prohibited its use for all but a very few important applications for which the cost of operation was not a significant concern.

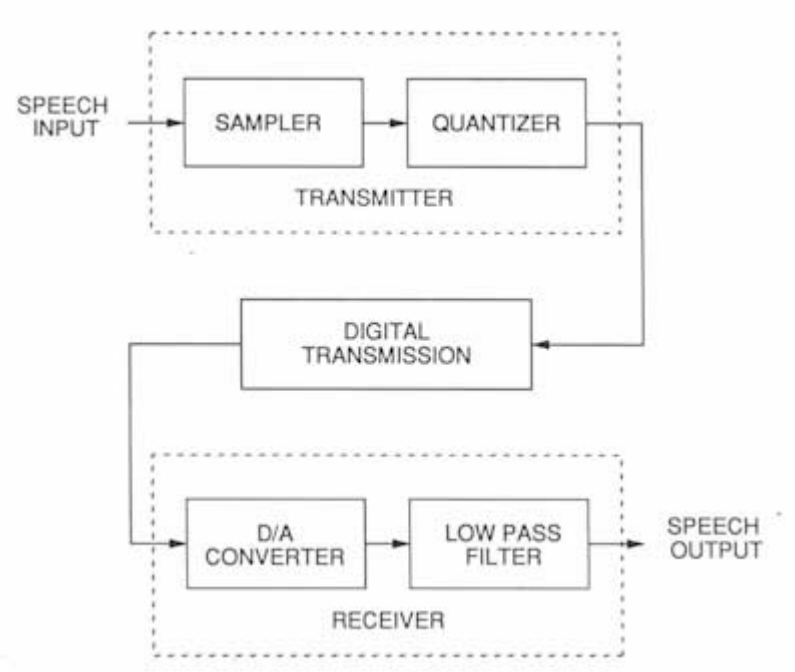

Figure I. Digital Voice Transmission System.

The LPC Algorithm

In the late-1960s the concepts of Adaptive Predictive Coding and slightly later Linear Predictive Coding were developed by Atal, Itakura and others [2] .LPC enabled the development of digital systems that required a bandwidth of only 2,400 bits per second (2.4 KBPS) while conveying audio fidelity such that a listener can recognize speech patterns that allow the identification of a specific person that the listener knows. This is frequently referred to as speaker identification.

A voice transmission system based on LPC is shown on Figure 2. The LPC algorithm is used to analyze the signal producing a set of LPC parameters which are encrypted and transmitted to the receiver where the parameters are used to synthesize the audio waveform. The details of the LPC analysis and synthesis processes are shown on Figure 3. On the left side of the figure the speech input is digitized and the LPC parameters (the voiced/unvoiced indicator, the pitch frequency, the RMS level of the speech and the LPC filter coefficients) are computed. These are encrypted, transmitted and decrypted. In the receiver the voiced/unvoiced indicator and (if voiced) the pitch frequency are used to create a stimulus for the vocal tract. The RMS level and the LPC filter coefficients are used to complete the vocal tract filter model. The output of the filter is converted into an analog speech signal. On the transmitter side this algorithm requires significant computing horsepower . The LPC filter coefficient extraction is especially computationally intensive with a requirement for large numbers of fixed point multiplications and additions.

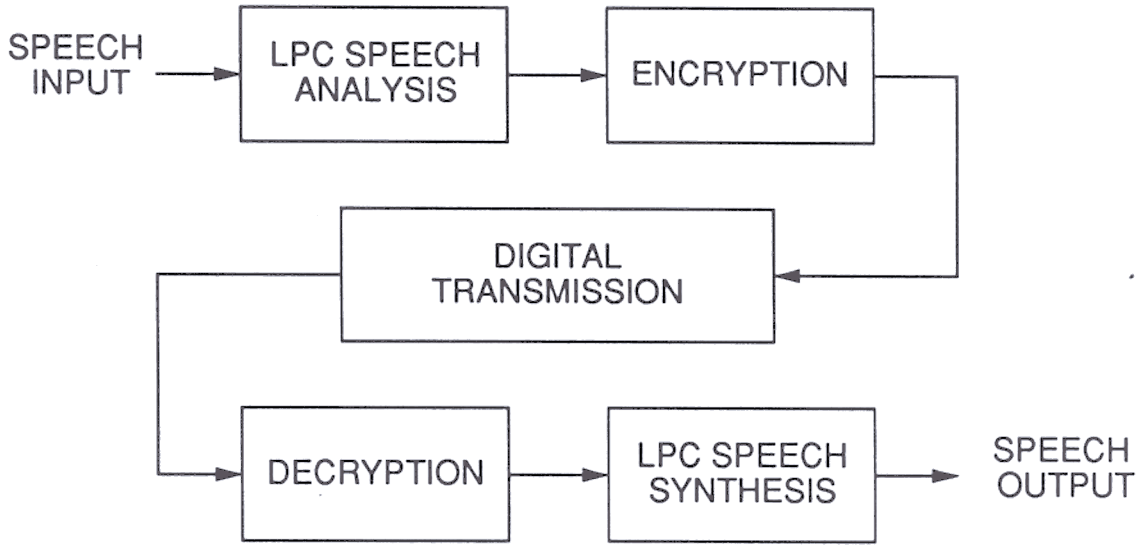

Figure 2. LPC Voice Transmission System.

Experiments with LPC were conducted with mainframe computers which suggested that it would be possible to achieve reasonable fidelity at data rates of 2.4 KBPS. Such an achievement would enable secure digital voice communication at bandwidths of less than traditional analog communications. LPC was not immediately usable due to the computational demands of the algorithm. The next section documents the progression of implementations at TR W Electronic Systems Group in the mid-1970s. .

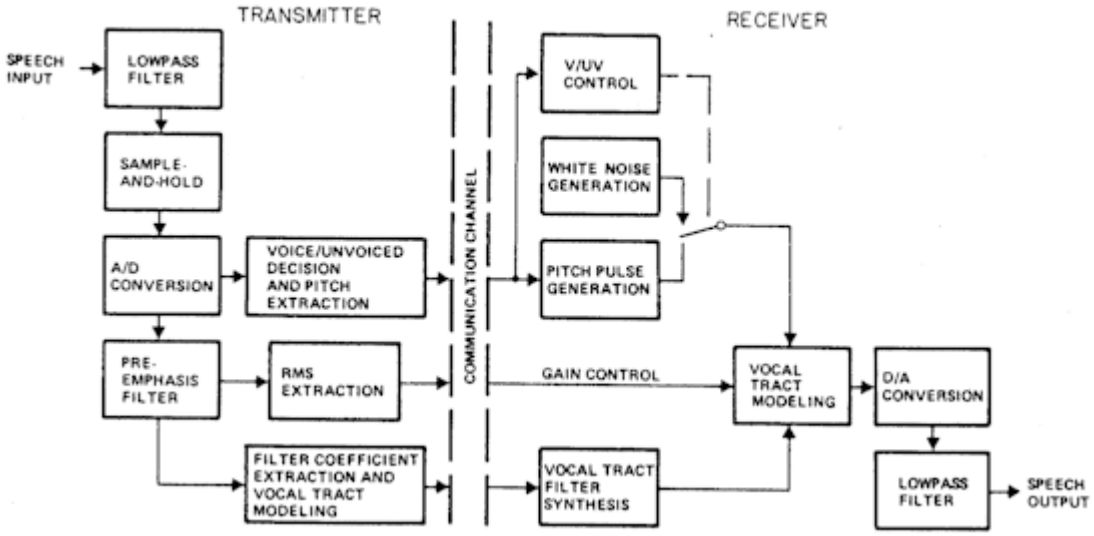

Figure 3. Linear Predictive Coding.

Implementation

With the existence of the LPC algorithm and limited experiments suggesting its utility, interest in applying it began to grow especially in the U.S. military community. A number of defense contractors began efforts to create production worthy systems. At TRW Electronic Systems

Group a succession of systems were developed including the 2A U Breadboard, the MVP Prototype, and finally the Micro Voice Processor. The Micro Voice Processor was a production unit that was suitable for military field use.

The 2AU Breadboard Processor
In the early 1970s TRW developed the 2AU breadboard processor. It used what is now called a Very Large Instruction Word (VLIW) architecture with two independent arithmetic units (hence the name 2AU). The photograph of the processor shown in Figure 4 shows that there are roughly 100 switches (on the unit on the right side of the photograph) used to set or reset the bits in each instruction word. The bits control the operations performed by the two arithmetic units as well as the sequencing of the instructions. Since the algorithm was not well understood the large instruction word was necessary to allow the many minute details of the implementation to be controlled.

As Figure 4 shows, the 2AU breadboard is very large, it consists of two units. When stacked the two units are 30 inches high by 19 inches wide (roughly the size of a washing machine). Approximately 1200 small and medium scale integrated circuits were required to implement the 2AU. This is due in part to the limited technology available when it was designed. For example a 16 bit array multiplier required 32 medium scale integrated circuits while later designs used a single array multiplier circuit.

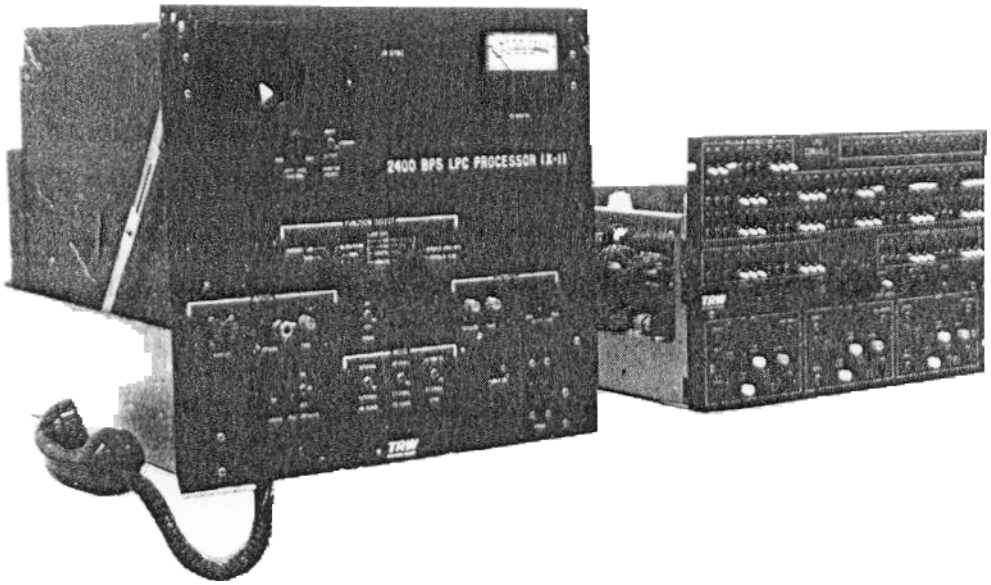

Figure 4. The 2AU Breadboard Processor.

The MVP Prototype Processor
The MVP prototype processor was developed after the 2A U was completed. Based on the experience with the 2AU and as a result of technology developments, it was much simpler than the 2A U as is evident from the photograph of the MVP Prototype on Figure 5. The technology developments included the availability of larger semiconductor random access memory , the 4-bit wide TTL bit slice microprocessors and single chip array multipliers. It is 12 inches high by 19 inches wide (roughly the size of a small microwave oven). The MVP prototype processor

contains approximately 350 integrated circuits. Like the 2AU it has a large number of switches on the front panel so that individual bits of any program word can be easily set or reset.

A block diagram of the MVP Prototype processor is shown on Figure 6. There are two processors (an addresses processor and a data processor) and two memories (a control memory which holds the program and a data memory which holds the operands).

The Micro Voice Processor Production Unit
The Micro Voice Processor production unit was developed after the LPC algorithm was successfully implemented on the MVP prototype processor. It has essentially the same block diagram as that of the MVP prototype shown in Figure 6. The main change is that the control memory is realized with Read Only Memory (ROM) which was much denser than RAM in the 1970s. Use of ROM also simplifies the system design as it is unnecessary to load the

Figure 5. **The MVP Prototype Processor** .

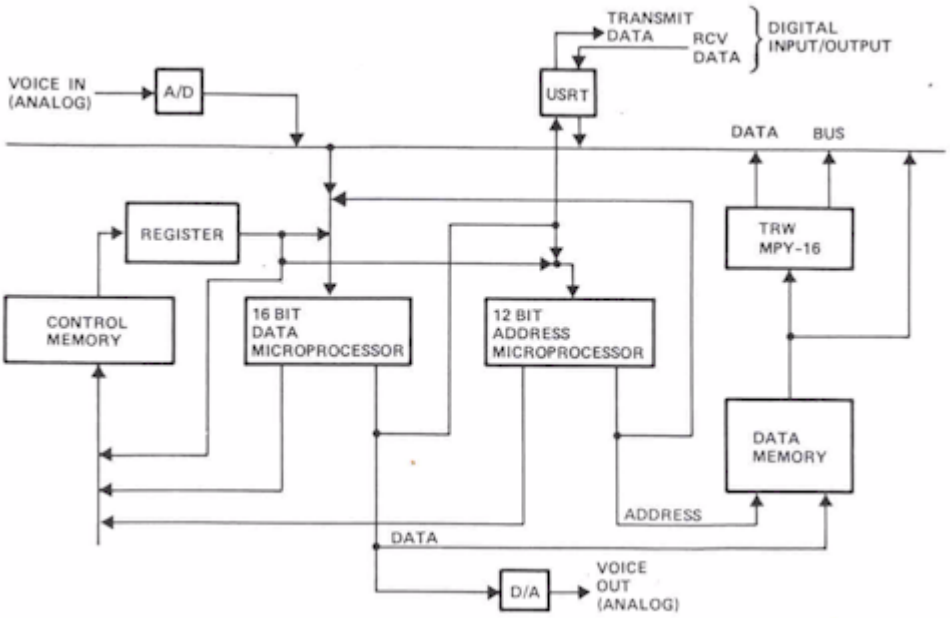

Figure 6. The MVP Processor Architecture.

Figure 7. The Micro Voice Processor Production Unit.

control memory on start-up. Also the switches on the front panel are eliminated since the control memory contents are fixed. The MVP production processor is shown in Figure 7. It is 8 inches high by 3 inches wide. The MVP production processor contains approximately 150 integrated circuits.

Conclusions

The physical characteristics of the three secure voice processors are compared on Table 1. The Micro Voice Processor production unit is 1/40 of the volume of the 2AU Breadboard and requires 1/8 of the chip count.

Table I. Processor Characteristics.

Processor	2AU	MVP Prototype	Micro Voice Proc.	Units
Height	30	12	8	In.
Width	19	19	3	In.
Depth	24	24	14	In.
Panel Area	4	1.6	.17	Sq. Ft.
Volume	8	3	.2	Cu. Ft.
Chip Count	1200	350	150	

The great reduction in size and parts count is a result of two independent factors: first, the advance in technology in the 1970s and second, the improved understanding of the algorithm. The technology advances are typified by the rapid increases in memory density and the development of bit slice microprocessors, single chip AID converters and array multipliers. These technology advances made it possible to reduce the size and component count of a given system by half every couple of years. The improved understanding of the LPC algorithm also helped to reduce the size and component count by allowing the designers to tailor the machine to the specific characteristics of the algorithm. It is said that flexibility is bought at a high price. We can see that as the characteristics and behavior of the LPC algorithm became better understood, the designs became leaner and more focused on the exact operations with the exact precision that is required as opposed to a general purpose system where overkill is the noon.

References

1, A. V. Oppenheim, "Digital Processing of Speech," in A. V. Oppenheim, ed., *Applications of Digital Signal Processing*, Englewood Cliffs, NJ : Prentice-Hall, 1978, Ch. 3, pp. 117-168.

2, F. Nebeker, *Signal Processing The Emergence of a Discipline* 1948 *to* 1998, New Brunswick, NJ: IEEE History Center, 1998, pp. 61,63.