Solomon W. Golomb—Mathematician, Engineer, and Pioneer

Guang Gong, Tor Helleseth, and P. Vijay Kumar, *Fellow, IEEE*

(Invited Paper)

Dedicated to the memory of Solomon W. Golomb (1932–2016)

***Abstract*— In this paper, we present some fundamental concepts and theoretical advances attributable to Solomon Golomb, together with the history and applications of this paper to communications, coding, and cryptography, along with some long-standing conjectures. Examples include the first engineering problem relating to feedback shift-register sequences that Sol Golomb was asked to solve in the mid-1950s. This paper covers *m*-sequences and Golomb's three randomness postulates, the cross-correlation of *m*-sequences, the exp-Golomb code, the Golomb ruler, Costas arrays, Golomb invariants, polyominoes, the distribution of prime numbers, and irreducible polynomials.**

***Index Terms*— Golomb, linear/nonlinear feedback shift-register sequence, code, cryptography, radar, communication, polyominoes, computer games.**

I. Golomb's Scientific Life

WE ARE honored to serve as guest editors for this special issue on shift-register sequences, codes and cryptography in memory of Solomon W. Golomb.

A large number of researchers know of Sol Golomb from his pioneering work on linear and nonlinear shift-register sequences (LFSRs, NLFSRs), work that has found, and continues to find, numerous applications ranging from deep-space, satellite and cellular communication to coding, compression, secure communications and cryptography. Many others know him from *Scientific American*, *The American Scholar* or his book *Polyominoes* as the polyominoes expert. We suspect that quite a few will be surprised to learn that all are the work of a single person.

In his book entitled *Idea Makers: Personal Perspectives on the Lives and Ideas of Some Notable People*, and in relation to Sol's pioneering contributions to the theory of LFSRs, Stephen Wolfram makes the following statement:

> *The Most Used Mathematical Algorithm Idea in History. An octillion. A billion billion billion. That's a fairly conservative estimate of the number of times a cellphone or other device somewhere in the world has generated a bit using a maximum-length linear-feedback shift-register sequence. It's probably the single most-used mathematical algorithm idea in history.*

Just ten days prior to his peaceful but sudden passing away, Sol was awarded the prestigious Franklin Medal in Electrical Engineering. The accompanying citation reads:

> *For pioneering work in space communications and the design of digital spread spectrum signals, transmissions that provide security, interference suppression, and precise location for cryptography; missile guidance; defence, space, and cellular communications; radar; sonar; and GPS.*

Over the years, Sol has received numerous other awards and honors as well including:

- Election to the US National Academy of Engineering (1976),
- Fellow of the IEEE (1982),
- Fellow of the American Association for the Advancement of Science (1988),
- Shannon Lecturer at the 1985 International Symposium on Information Theory, Brighton, England,
- Medal of the U.S. National Security Agency (1992),
- 2000 IEEE Richard W. Hamming Medal,
- Elected to National Academy of Sciences (2003),
- Fellow of the American Academy of Arts and Sciences (2003),
- The William Procter Prize of Sigma Xi (2012),
- 2011 National Medal of Science (in a White House ceremony),
- Fellow of the American Mathematical Society (2012),
- Fellow of the Society for Industrial and Applied Mathematics (2013),
- 2016 Franklin Medal in Electrical Engineering,
- Election to the Board of Governors and its Academic Advisory Committee, of the Technion Israel Institute of Technology (2003),
- Foreign Member: Russian Academy of Natural Sciences (1994); Lomonosov Medal, Russian Academy of Sciences (1994); Kapitsa Medal, Russian Academy of Natural Sciences (1995),
- Honorary Doctorate Degrees: Dubna International University (1995), Hebrew Union College (1996), The Technion Israel Institute of Technology (2011), and the University of Waterloo (2016).

A complete survey of Golomb's work would make for a very voluminous article indeed. Dean Yannis C. Yortsos of the USC Viterbi School of Engineering had this to say of

Manuscript received January 31, 2018; accepted February 23, 2018. Date of publication February 27, 2018; date of current version March 15, 2018.

G. Gong is with the University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@uwaterloo.ca).

T. Helleseth is with the University of Bergen, 5007 Bergen, Norway.

P. V. Kumar is with the Indian Institute of Science, Bengaluru 560012, India, and also with the University of Southern California, Los Angeles, CA 90007 USA.

Communicated by F. Kschischang, Editor-in-Chief.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2018.2809497

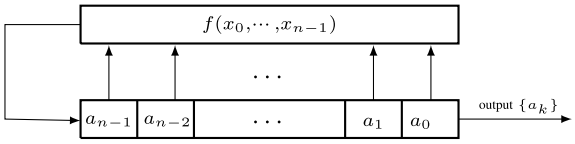


Fig. 1. A block diagram of an FSR.

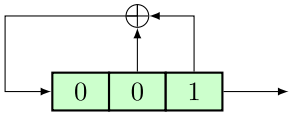


Fig. 2. A 3-stage LFSR having feedback function $f(x_0, x_1, x_2) = x_0 + x_1$.

Sol Golomb: "With unparalleled scholarly contributions and distinction to the field of engineering and mathematics, Sol's impact has been extraordinary, transformative and impossible to measure. His academic and scholarly work on the theory of communications built the pillars upon which our modern technological life rests."

In what follows, we attempt to describe how engineering problems were dealt with by the great mind of a multi-faceted Solomon Golomb as a mathematician as well as an engineer. We were guided in our selection of topics by an inspirational quote by Sol himself, in a 1998 article "Mathematics Forty Years After Sputnik" appearing in *The American Scholar*:

> *If nature were not beautiful, it would not be worth knowing, and if nature were not worth knowing, life would not be worth living.*

II. Feedback Shift-Register Sequences

A. Linear-Feedback Shift-Register Sequences (LFSRs)

During an internship with the Glenn L. Martin Company (now Lockheed Martin) in Baltimore, in June 1954, the leader of the Communications Group, Thomas Wedge presented Sol Golomb with a problem that was described as involving a tapped delay line with feedback. Sol labelled the structure as a binary, linear-feedback shift register (LFSR) and immediately set about using his background in pure mathematics to develop a theory for the output generated by this device. The feedback function f may be viewed as a boolean function in n variables: if $(a_0, \cdots, a_{n-1}), a_i \in \mathbb{F}_2$ ($\mathbb{F}_2 = \{0, 1\}$) is the initial state, then at each clock pulse, f causes a transition from one state to the next according to: $(a_0, \cdots, a_{n-1}) \longrightarrow (a_1, \cdots, a_{n-1}, a_n)$ with $a_n = f(a_0, \cdots, a_{n-1})$. When f is linear, i.e.,

$$f(x_0, \cdots, x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i, \quad c_i \in \mathbb{F}_2,$$

the FSR is referred to as a *linear-feedback shift register (LFSR)*, else, as a nonlinear-feedback shift register (NLFSR).

Example 1: An LFSR with 3 stages is shown in Figure 2. The associated recursive relation takes on the form:

$$a_{k+3} = a_k + a_{k+1}, \quad k = 0, 1, 2, \ldots$$

and the output of the LFSR, assuming the initial state of Figure 2, can be verified to be the periodic sequence

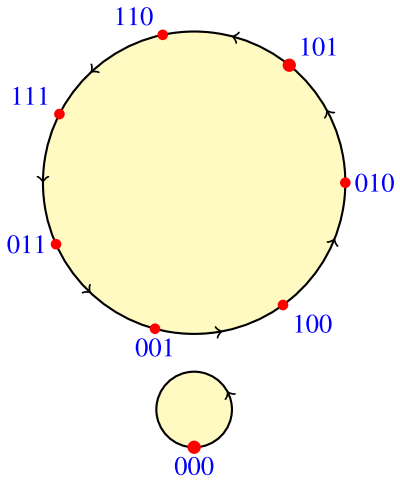


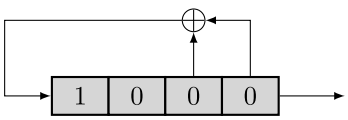
Fig. 3. State diagram of the 3-stage LFSR with feedback function $f(x_0, x_1, x_2) = x_0 + x_1$.

$10010111001011\cdots$ having period 7. The associated state diagram is shown in Fig. 3 with the state of the LFSR defined as the binary 3-tuple (x_2, x_1, x_0).

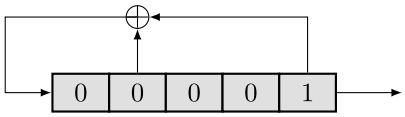
Experiments conducted during this period of Sol's research indicated that while some combinations of taps resulted in binary sequences having a very long period, others resulted in much shorter period. Sol adopted a generating-function approach which yielded a correspondence between LFSR sequences and polynomials. In the example above, the polynomial $f(x)$ associated to boolean function f and termed the characteristic polynomial of the m-sequence is given by $f(x) = x^3 + x + 1$. In general, we associate with boolean function $f(x_0, \cdots, x_{n-1}) = c_0x_0 + \cdots + c_{n-1}x_{n-1}, c_i \in \{0, 1\}$, the characteristic polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$.

The period of a polynomial $f(x)$ over the finite field $\mathbb{F}_q$ is defined as the smallest positive integer r such that $f(x)$ divides $x^r - 1$, i.e., $f(x) \,|\, x^r - 1$, but $f(x)$ does not divide $x^t - 1$ for $0 < t < r$. For the case when the characteristic polynomial is irreducible, the period of the output sequence of the LFSR is equal to the period of the characteristic polynomial. The maximal period of an LFSR sequence is $2^n - 1$. A maximal-period LFSR is generated whenever the associated characteristic polynomial $f(x)$ is *primitive* i.e., $f(x)$ has maximal period $2^n - 1$. In this case, the sequences are called *maximal length* LSFR sequences, *m-sequences* for short. An m-sequence is called a *pseudonoise sequence* in communication applications on account of its randomness properties, which include a thumbtack-shaped autocorrelation function, i.e., an autocorrelation function having a single large spike.

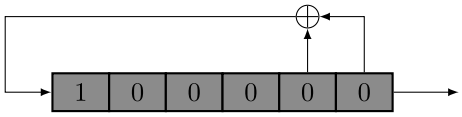
Example 2: Additional examples of LFSRs that generate m-sequences are presented here.



(a) Generates an m-sequence having period 15: 000100110101111



(b) Generates an m-sequence having period 31:
1000010101110110001111100110100



(c) Generates an m-sequence having period 63:
000001000011000101001111010000111
001001011011101100110101011111 1

Observation (Golomb, 1954): The LFSR associated to a characteristic polynomial that is a primitive polynomial, generates an m-sequence. This and other results may be found in the book [1]–[3] by Sol Golomb, first published in 1967.

B. Nonlinear Feedback Shift-Register Sequences

Here, the feedback function is nonlinear of the form

$$f(x_0, x_1, \cdots, x_{n-1}) = \sum c_{i_1 i_2 \cdots i_t} x_{i_1} x_{i_2} \cdots x_{i_t}, c_{i_1 i_2 \cdots i_t} \in \mathbb{F}_2$$

where the sum runs through all subsets $\{i_1, \cdots, i_t\}$ of $\{0, 1, \cdots, n-1\}$. The function f is thus, a general boolean function in n variables. The function is declared to be nonlinear when there is at least one $t > 1$ such that $c_{i_1 i_2 \cdots i_t} \neq 0$. The associated state diagram S_f depicts all transitions in state of the shift register, when transitions are governed by the feedback function f.

For example, setting $n = 3$ and feedback function f to be the nonlinear boolean function $f(x_0, x_1, x_2) = x_0 + x_1 x_2$ generates an NLFSR (nonlinear-feedback shift-register) sequence. The associated state diagram S_f turns out to have three cycles, corresponding to the output sequences: {0} of period 1, {100} of period 3, and {1011} of period 4.

The total number of nonlinear boolean functions in n variables equals 2^{2^n}. This is a very large number for large n. When $n = 9$, this number exceeds the total number of atoms in the universe. Sol discovered that the state diagram has no branches and only cycles, if and only if

$$f(x_0, x_1, \cdots, x_{n-1}) = x_0 + g(x_1, \cdots, x_{n-1}) \tag{1}$$

where g is a boolean function in $n-1$ variables. If f satisfies (1), then f is said to be *nonsingular*. It turns out that nonsingularity is equivalent to the requirement that the mapping

$$(a_0, \cdots, a_{n-1}) \longrightarrow (a_1, \cdots, a_{n-1}, f(a_0, \cdots, a_{n-1}))$$

be a permutation. A natural question that one may ask here is: How many cycles does the nonsingular feedback function f decompose the state diagram into? Sol made the following conjecture:

Conjecture (Golomb (1967)): The maximum number of cycles in S_f is upper bounded by the number $Z(n)$, defined as the number of cycles of the feedback function $f(x_0, x_1, \cdots, x_{n-1}) = x_0$, (i.e., a feedback function where $g = 0$) called a *pure-cycling register (PCR)*.

This conjecture was subsequently proven by Mykkeltveit in 1972 [4].

C. Golomb's Open Problems on NLFSRs

Open Problem 1 (Analysis of NLFSRs): Given a nonlinear feedback function $f(x_0, x_1, \cdots, x_{n-1})$, how many cycles are there in S_f and what are the lengths of the corresponding cycles, or equivalently, how many shift-distinct sequences can the NLFSR generate and what are the periods of these sequences?

Open Problem 2 (Synthesis of NLFSRs): For a given r, $0 < r \leq 2^n$, how does one go about identifying a nonlinear feedback function that will generate a sequence with period r?

Despite more than six decades of investigation, little progress has been made on these two problems. Even today, Sol's book on *Shift Register Sequences* [1]–[3] contains most of the known results on NLFSRs.

III. Randomness Properties of m-Sequences and Applications to Communication

In Sol's 1954 report to the Glenn Martin Company, the property on 2-level autocorrelation of m-sequences was identified by Sol as the key property applicable to space communications. Sol worked at NASA's Jet Propulsion Laboratory (JPL), as the Leader of the Information Processing Group and his group provided a solution to early orbit determination of Explorer I launched in 1958 following the launch of Sputnik in 1957 by the Soviet Union. The signal sent back from Explorer I, was a binary phase-shift-keying (BPSK) pulse modulated by an m-sequence. A second amazing application of the autocorrelation property of an m-sequence took place in 1958 shortly after the launch of Explorer I. At the time, preparations were being made to launch a space probe that would arrive in the vicinity of Venus. Sol was the leader on the Venus Radar detection project. He had designed an interplanetary ranging system at JPL, based on BPSK of an RF carrier using m-sequences, that basically counted RF-cycles, and thus potentially provided extreme range accuracy. Venus was successfully detected by the JPL team in 1961, in a manner that was more accurate than ever before. In their Venus radar experiment, Sol and his team showed that the distance between Earth and Venus reported earlier to be significantly off the mark.

The concept of correlation in the context of an m-sequence, is the same as that employed in statistics. For a binary sequence $\mathbf{a}$ of period N, we define the *autocorrelation* function of $\mathbf{a}$ to be given by

$$C_{\mathbf{a}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_{i+\tau} - a_i}.$$

Given two distinct binary sequences $\mathbf{a}$ and $\mathbf{b}$ of period N, we define

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} (-1)^{b_{i+\tau} - a_i},$$

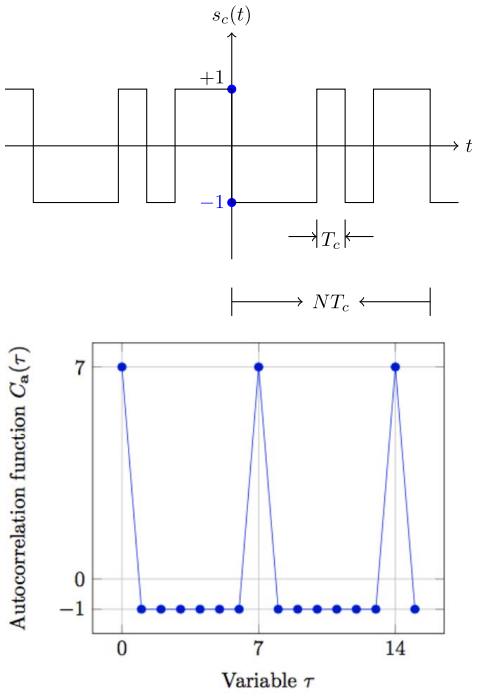


Fig. 4. Above: The continuous-time signal $s_a(t)$ associated to m-sequence $\{a_i\} = \{1110100\}$ of period 7. Below: The autocorrelation $C_{\mathbf{a}}(\tau)$ of the m-sequence, showing all out-of-phase autocorrelation values to equal -1.

to be the *cross-correlation* function of $\mathbf{a}$ and $\mathbf{b}$. If $\mathbf{a} = \mathbf{b}$, then $C_{\mathbf{a},\mathbf{b}}(\tau)$ reduces to $C_{\mathbf{a}}(\tau)$ and when $\mathbf{a}$ is clear from the context, we will simply write $C(\tau)$ in place of $C_{\mathbf{a}}(\tau)$.

A. Golomb's Three Randomness Postulates

Sol's randomness postulates given below, place requirements on a deterministically generated, periodic sequence to qualify as being pseudorandom.

- *R-1*. In every period, the number of zeroes is nearly equal to the number of ones, i.e., the disparity is not to exceed 1.
- *R-2*. In every period, *half the runs* have length one, one-fourth have length two, one-eighth have length three, etc., as long as the number of runs so indicated exceeds 1. Moreover, for each of these lengths, there are equally many runs of 0's and of 1's.
- *R-3*. The autocorrelation function $C(\tau)$ is two-valued, given by

$$C(\tau) = \begin{cases} N & \text{if } \tau \equiv 0 \pmod N \\ K & \text{if } \tau \not\equiv 0 \pmod N \end{cases} \tag{2}$$

where K is a constant. If $K = -1$ for N odd and $K = 0$ for N even, then we say that the sequence has the *(ideal) 2-level autocorrelation function*.

Sol showed that every m-sequence satisfies the three randomness postulates.

Example 3: The example in Figure 4 shows: (a) the $\{\pm 1\}$ continuous-time signal, $s_a(t)$, associated to the m-sequence $\{a_i\} = \{1110100\}$ of period 7, (b) the autocorrelation function $C_{\mathbf{a}}(\tau)$ of the sequence $\{a_i\}$ using dots and the autocorrelation of the signal waveform $s_a(t)$ using solid lines. An exhaustive list of all currently-known sequences having a two-level autocorrelation function, (including m-sequences), can be found in the more recent book by Golomb and Gong [5].

B. Applications of Two-Level Autocorrelation to Radar Distance-Ranging

After the successful detection using radar of Venus by JPL in 1961, Sol wrote a paper, entitled "Radar Measurements of the Planet Venus" [6]. The paper opens with the following paragraph:

> *At intervals of about 584 days, the planet Venus passes through inferior conjunction and approaches within 25 million miles of the earth. A maximum separation of 162 million miles occurs at superior conjunction. The inverse fourth-power law expressed by the radar range equation and the present state of the art make it most practicable to attempt radar contact with Venus during the few weeks just before and after each inferior conjunction. For the year 1961 this period is defined between 10th March and 10th May.*

The method employed to detect Venus has since been extended to all radar distance ranging systems including current GPS systems. The method measures *range* as being the distance from the radar site to the target measured along the line of sight. Since the propagation of radio waves takes place at the speed c of light, and the waves travel to the target and back, the round trip time is divided by two in order to obtain the time taken by the wave to reach the target. The formula for computing range is thus given by

$$c = \frac{S}{T/2} \Longrightarrow S = \frac{cT}{2}$$

where

$c = 3 \cdot 10^8$ m/s (meters per second, the speed of light)

$T =$ measured round-trip time in seconds

$S =$ range in meters.

Sol showed how the round-trip time T could be determined using the two-level autocorrelation property of an m-sequence. This works as follows. The transmitter sends out the direct sequence, binary, phase-shift-keying (DS-BPSK) signal

$$s(t) = As_a(t)\cos(2\pi f_c t), \quad 0 \le t \le T_b, \tag{3}$$

where T_b is the time duration of a single transmitted bit,

$$s_a(t) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (-1)^{a_k} g(t - kT_c),$$

$\{a_k\}$ is an m-sequence of period N that serves as the spreading sequence having *chip duration* T_c and where $g(t)$ is a rectangular pulse of width T_c centered around $t = 0$, i.e.,

$$g(t) = \begin{cases} 1 & t \le |T_c/2|, \\ 0 & \text{else.} \end{cases}$$

The received signal is the sum

$$y(t) = r(t) + n(t) + I(t),$$

of signal $r(t)$, noise $n(t)$ and interference $I(t)$, with signal given by

$$r(t) = A' s_a(t - \tau T_c)\cos(2\pi f_c t + \phi), \tag{4}$$

in which the ratio $\frac{A'}{A}$ represents signal attenuation, ϕ the random phase shift and τT_c the time delay, all introduced by the channel. The receiver, called a correlation receiver, correlates the received signal with different time-shifted versions $\{s_c(t + iT_c), i = 0, 1, 2, \cdots\}$ of the transmitted signal $s_c(t)$. The resulting correlation takes on the form:

$$\begin{aligned} z(t) &= \int r(t) s_a(t - iT_c) dt \\ &= \int A' s_a(t - \tau T_c) s_a(t - iT_c)\cos(2\pi f_c t + \phi) dt \\ &\quad + \text{a noise-related term} \\ &\quad + \text{an inference-related term} \\ &\approx K\rho(\tau - i) + \text{other terms}, \end{aligned}$$

where K is a constant and ρ is the normalized autocorrelation of the m-sequence $\mathbf{a}$:

$$\rho(\tau - i) = \int s_c(t + \tau T_c) s_c(t - iT_c) dt = \frac{1}{N} C(\tau - i).$$

The computation is carried out for each i until the value of i for which $\rho(\tau - i)$ assumes the large (and hence hopefully easily detectable) value $\rho(\tau - i) = 1$, corresponding to synchronization i.e., $\tau = i$ of the transmitted signal and the replica employed by the correlation receiver. This allows the round-trip time to be estimated as $T = iT_c$ seconds. From this the distance S to the target can be determined.

C. Other Applications

The use of m-sequences in DS-BPSK modulation for the purpose of spreading the spectrum of a signal in communication is referred to as *spread-spectrum communication*. The m-sequences used here are referred to as *spreading codes or signature sequences*. This is different from a cryptographic digital signature, although the functionality is essentially the same. Spread-spectrum signals constructed in this manner from an m-sequence find numerous applications starting from earlier applications in anti-jamming in military communication systems to popular applications such as energy-density reduction, high-resolution ranging, low-probability-of-intercept and multiple access using to advantage their ability to discriminate against narrowband interference, multipath interference, multiple-access interference, and other types of structured interference that arise in radio-frequency (RF) communication channels. These signals also offer a certain degree of privacy.

Sol's revolutionary book, *Shift Register Sequences* [1]–[3], has long been required reading for new recruits in many organizations, including the National Security Agency and a variety of companies that design spread-spectrum communication systems to provide an anti-jamming and/or a low-probability-of-intercept capability. The same technology applied in a commercial, cellular-communication context, goes by the name CDMA (code-division multiple access) in general, as IS-95 in 2G cellular systems, and as CDMA 2000 or WCDMA in 3G systems.

Feedback shift-register sequences also find application in cryptography, ranging from their use as a stream ciphers in a one-time pad to applications in modern cryptography. They also find application in hardware testing.

D. Combining the Outputs of Several LFSRs

In 1958, while at JPL, Sol investigated the problem of generating a sequence having a long period, starting from several LFSRs, each having a bounded number of stages. His investigations included the use of a nonlinear function to combine the outputs of multiple m-sequences. One such sequence of long period was employed in the radiation detector on board Explorer I, the spacecraft that discovered what today are known as the van Allen radiation belts. James van Allen was at the time, a graduate student who worked on this problem with Sol. Even today, in the field of cryptography, there is keen interest in output sequences generated at the output of a nonlinear function whose inputs are m-sequences. Such sequence generators are today called *filtering or combinatorial generators* and will be introduced in Section VIII-A.

E. Classification of Sequences

In order to measure the randomness of a sequence with the same period as an m-sequence, Sol defined the concept of span n sequences, i.e., any nonzero n-bit string occurs exactly once in a binary sequence with period $2^n - 1$. Then he made the following conjecture.

Conjecture 1 (Golomb (1980) [7], open): Any sequence with 2-level autocorrelation and span n property must be an m-sequence.

The significance of this conjecture in cryptography is that a random sequence with large linear span (or linear complexity, i.e., the shortest length of the LFSR which generates the sequence) has to comprise one of those two properties.

IV. Cross Correlation of m-Sequences

Sol Golomb visited the University of Bergen, Norway in January 1970 at the invitation of Norwegian mathematician Ernst Selmer and in this period, he delivered two lectures: (a) "Tiling a 3D Cartesian box with bricks of different dimensions" and (b) "Cross correlation of m-sequences". This was the first time the second author of the present article met Sol and found the second talk so interesting that he went on to make this topic the main subject of both his Master's and PhD thesis.

There are two key properties satisfied by an m-sequence. Let $\mathbf{a} = \{a_i\}$ be an m-sequence of period $N = 2^n - 1$.

(a) The *d-decimation* $\mathbf{a}^d = \{b_i\}$ of $\mathbf{a}$ where $b_i = a_{di}$ and $\gcd(d, 2^n - 1) = 1$ is also an m-sequence. There are a total of $\frac{\phi(2^n-1)}{n}$ shift distinct m-sequences, where ϕ is Euler's totient function.

(b) *Shift-and-add property*: Given an integer τ, there exists for any m-sequence $\mathbf{a} = \{a_i\}$, an integer v such that $a_{i+\tau} + a_i = a_{i+v}$, for any $i = 0, 1$.

In Sol's second talk, he presented the following problems without proof and taken from his paper (1968) [8]:

1) *The Welch Conjecture:* for $d = 2^{(n-1)/2} + 3$, n odd, the cross-correlation of $\mathbf{a}$ and $\mathbf{b} = \mathbf{a}^d$ is 3-valued, specifically

$$C_{\mathbf{a},\mathbf{b}}(\tau) \in P = \{-1, -1 \pm 2^{\frac{n+1}{2}}\}, \quad \forall \tau. \tag{5}$$

2) For a pair of cyclically-distinct m-sequences having the same period, there are at least 3 values in the cross-correlation function.

The second problem was solved by Helleseth (1971) in his Master's Thesis [9] and later published in [10]. The Welch conjecture was proven by Canteaut *et al.* in 2000 [11].

In the 1960s only three pairs of m-sequences, i.e., sequences pairs

$$\{\{a_i\}, \{b_i = a_{di}\}\}, \quad \text{with } \gcd(d, 2^n - 1) = 1,$$

having the 3-valued cross-correlation appearing in (5), were either known or conjectured. The first pair was identified and proven by Gold in 1968 [12]. The second pair was conjectured by Sol and first proven by Welch in an unpublished result. The first published proof of Sol's conjecture was by Kasami in 1971 [13]. The third pair corresponds to the Welch conjecture discussed above. The values of d corresponding to the three pairs are listed below:

- $d = 2^k + 1$ (Gold 1968),
- $d = 2^{2k} - 2^k + 1$ (Welch, Kasami 1971),
- $d = 2^{(n-1)/2} + 3$ (Welch's conjecture),

where for the first two decimations, k and n are selected such that $\gcd(d, 2^n - 1) = 1$. Over the course of the last 5 decades, the cross-correlation of m-sequences has been extensively examined by many researchers. Several new instances of d corresponding to 3-valued cross-correlation have been found. The problem of determining all decimations d corresponding to a 3-valued cross-correlation, however, remains open.

A convenient representation of an m-sequence is in terms of the trace function over a finite field $\mathbb{F}_{2^n}$. Let $\mathbb{F}_{2^n}$ be defined by the primitive polynomial $t(x)$ and α be a root of $t(x)$ lying in $\mathbb{F}_{2^n}$. Let $\mathbf{a} = \{a_i\}$ be the m-sequence generated by a LFSR having characteristic polynomial $t(x)$. Then it can be shown that

$$a_i = Tr(\beta \alpha^i), \quad i = 0, 1, \ldots,$$

for some nonzero element $\beta \in \mathbb{F}_{2^n}$ and where

$$Tr(x) = x + x^2 + \cdots + x^{2^{n-1}}$$

is the trace function, mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In this situation, we will identify the sequence $\mathbf{a} = \{a_i\}$ using the somewhat loose notation:

$$\mathbf{a} \leftrightarrow f(x) = Tr(\beta x), \quad \beta \in \mathbb{F}_{2^n}.$$

In terms of this notation, the decimation of $\mathbf{a}$ by the integer d can be represented by the monomial trace term, i.e., $\mathbf{b} \leftrightarrow g(x) = Tr(\beta x^d)$.

Example 4: For $n = 3$, let the finite field $\mathbb{F}_{2^3}$ be defined by primitive polynomial $f(x) = x^3 + x + 1$, and α be a root of $f(x)$. Then the m-sequence $\mathbf{a} = \{1001011\}$, generated by an LFSR of order 3 having characteristic polynomial $x^3 + x + 1$ is given by $a_i = Tr(\alpha^i)$. Let $d = 3$ and $\mathbf{b} = \{a_{3i}\}$. Then $\mathbf{b}$ is the m-sequence $\{1110100\}$. Then $b_i = Tr(\alpha^{3i}) \leftrightarrow Tr(x^3)$. It turns out that $\mathbf{b}$ has characteristic polynomial $x^3 + x^2 + 1$.

There is a close relationship between m-sequences having the 3-valued cross-correlation given in (5) and the cryptographic concept of an *almost-perfect nonlinear (APN) function*. Let $f(x)$ be a function over $\mathbb{F}_{2^n}$. Then f is termed an APN function if the equation $f(x) + f(x+a) = b$ has at most two solutions in $\mathbb{F}_{2^n}$ for all $(a, b) \in \mathbb{F}_{2^n}^2$ with $a \neq 0$. To date, there are only six known classes of monomial APN functions, i.e., APN functions $f(x)$ of the form $f(x) = x^d$. Of the 6 known values of d for which the function $f(x) = x^d$ is an APN function, three values of d happen to correspond to the values listed above of d for which the cross-correlation of the sequences $\{a_i\}$, $\{a_{di}\}$ is 3-valued.

V. Exp-Golomb Code for Lossless Data Compression

"Run-Length encodings", the title of a paper that Golomb published in 1966 [14], became a widely used lossless data compression technique, adopted and under the terminology *Golomb run-length codes* and a variation, termed as the *Exponential-Golomb (Exp-Golomb) code*. This data-compression technique was used to send back scientific data from the Mars Rover in the 1960s. Currently, the Exp-Golomb code has been selected in the standards of multimedia communications such as MPEG-4 (or H.264). Sol was not aware of this application. When the first author of the present survey mentioned this incredible influence on image and video compression, Sol's response was simply that he had given up tracking the various applications of his work since the mid-90s. Golomb's 1966 paper begins with the following sentence:

> Secret Agent 00111 is back at the Casino again, playing a game of chance, while the fate of mankind hangs in the balance. Each game consists of a sequence of favorable events (probability p), terminated by the first occurrence of an unfavorable event (probability $q = 1 - p$).

This game can be modeled as a binary bit stream where 0 represents an unfavorable event and 1, a favorable event. Thus the outcome of each game can be modeled by a sequence of consecutive 1's followed by a single 0. The number of consecutive 1's is called the *run-length* of the game or equivalently, of the sequence. For example, the sequence $A = 1111110$ is said to have a run-length of 6 meaning that the player encountered for the first time, an unfavorable event at the 7th roll. In general, the probability of having a run-length of n is given by $p^n q$. This sequence of probabilities for $n = 0, 1, \ldots$ is termed the *geometric distribution*. For example, if $p = \sqrt{1/2} = 0.7071 \Longrightarrow q = 1 - p = 0.2929$, then the probability that the the sequence A associated with run-length 6 occurs, is given by

$$P\{A \text{ occurs}\} = p^6 q = 0.0366.$$

TABLE I

GOLOMB RUN-LENGTH CODE FOR ENCODING AN INTEGER n GIVEN m AND k

Encoder	Write $n = m\ell + r, 0 \le r < m$. A codeword is a $(\underbrace{11\cdots1}_{\ell} \|$binary representation of $r')$ where $r' = \begin{cases} r, & r < 2^{k-1} - m, \text{using } k-1 \text{ bits for } r \\ t = r + 2^{k-1} - m, & r \ge 2^{k-1} - m, \text{using } k \text{ bits for } t \end{cases}$
Decoder	From the left end, counting the number of 1's, decoded as ℓ. Let the rest of the bits after the run of 1's be called A. If A is a $(k-1)$-bit vector, then decode r as the binary represention of A. Otherwise decode r as the binary representation of $A - (2^{k-1} - m)$. Set $n = qm + r$.

TABLE II

CODEWORDS FOR n WHEN $m = 12$ AND $k = 5$

n	Codeword	n	Codeword	n	Codeword
0	0000	12	10000	48	11110000
1	0001	13	10001	49	11110001
2	0010	14	10010	50	11110010
3	0011	15	10011	51	11110011
4	01000	16	101000	52	111101000
5	01001	17	101001	53	111101001
6	01010	18	101010	54	111101010
7	01011	19	101011	55	111101011
8	01100	10	101100	56	111101100
9	01101	21	101101	57	111101101
10	01110	22	101110	58	111101110
11	01111	23	101111	⋮	

If each event in the game corresponds to a sub-game of roulette, then the game terminates with a win (let us say) which occurs with probability

$$q = 1/37 = 0.027 \Longrightarrow p = 1 - q = 0.973 \text{ and}$$
$$P\{A \text{ occurs}\} = p^6 q = 0.0229.$$

The data-compression problem in this context asks for lossless representation of all possible sequences using the least number of bits. Equivalently, how can one compress in an efficient and practical manner, an integer-valued random variable obeying the geometric distribution $p^n q$ on the probability of occurrence of the integer n? The algorithm that Sol came up with here is called the *Golomb run-length code*. In the following, we explain Sol's explicit encoder and decoder for his run-length code. Sol begins by introducing a parameter, $m = -\log 2/\log p$, i.e., $p^m = 1/2$ where m is preferably, an integer. Next, Sol sets k to be the smallest integer such that $2^k \ge 2m$. The encoder and decoder rules are presented in Table I.

Example 5: Let $m = 12$. So $k = 5$, and the codebook or the dictionary has 4 codewords with length 4, and 8 codewords with length 5 for encoding any positive integer n, as shown in Table II for $0 \le n \le 58$.

When m is a power of 2, i.e., $m = 2^{k+1}$, the codebook consists of all binary codewords of length k and there is no codeword with length $k - 1$.

The idea of applying this algorithm to compress a bit string starting with a run of 1's is to use two integers to represent the bit string where the first integer is the length ℓ of the run and the second integer is the binary number of the rest of the bits. As long as the data has long runs, it is extremely efficient, since it only needs $\log_2 \ell$ bits to transmit the first integer instead of ℓ bits in the original bit stream. Golomb run-length code for compression replaces a run of 1's by its length, Lempel-Ziv compression algorithm, published in the late of 1970s, has a similar fashion, but it replaces an arbitrary bit string by two integers where one is its position locating where it occurs previously, and the second is the length of the pattern. This path is not surprising, since Abraham Lempel was Sol's first post-doc.

VI. GOLOMB RULER

A pattern that Sol observed, originally in the context of coded pulse radar, was that of a ruler of length L having n marks placed in such a way that any distance $1 \le d \le L$ can be measured in one and only one way as the distance between two of the n marks. A ruler having this pattern was popularized in Martin Gardner's column in the *Scientific American* as a Golomb Ruler. Since then, Golomb rulers have been applied in fields as far ranging as X-ray diffraction, crystallography, radio antenna placement, and error correction.

Symbolically, a ruler of length L has exactly n marks on it, at integer positions $a_1, a_2, \ldots, a_n$, where $a_1 = 0$ and $a_n = L$ are the two endpoints of the ruler. If every integer distance $d, 1 \le d \le L$, can be measured in one and only one way as a distance between two of the n marks, i.e., if the differences $(a_j - a_i)$ for $\{1 \le i < j \le L\}$ are all distinct and $\{a_j - a_i \mid 1 \le i < j \le L\} = \{1, 2, \cdots, L\}$, then the ruler is called a *perfect ruler*. It is known that there do not exist perfect rulers for $n > 4$ [5].

To get around the problem of non-existence, there are two obvious ways to relax the requirement on a perfect ruler, so as to obtain rulers that exist for all possible values of n. A *covering ruler* with n marks and length L measures every distance from 1 to L, as a distance between two marks on the ruler, in *at least one way*. A *spanning ruler* with n marks and length L measures every distance from 1 to L, as a distance between two marks on the ruler, in *at most one way*. The interesting combinatorial problems are to determine the

longest covering ruler with n marks, and the *shortest spanning ruler* with n marks, for each positive integer n. However, the application to radar communication involves only finding the *shortest spanning ruler*, i.e., finding the shortest length $L(n)$, for each n.

For example, for $L = 6$ and $n = 4$, the four marks of a perfect ruler are given by

a_0	a_1	a_2	a_3		Differences
0	1	4	6		$a_j - a_i,\ i < j$
1	4	6		$\Longrightarrow$	1 3 2
4	6				4 5
6					6

For $L = 11$ and $n = 5$, the five marks of a shortest spanning ruler are given as follows.

a_0	a_1	a_2	a_3	a_4		Differences
0	1	4	9	11		$a_j - a_i, i < j$
1	4	9	11		$\Longrightarrow$	1 3 5 2
4	9	11				4 8 7
9	11					9 10
11						11

The above ruler cannot measure distance 6. It is still an open problem as to whether or not there exist infinitely many shortest Golomb spanning rulers. The latest exhaustive search results have been extended to length $L = 27$.

VII. Costas Arrays for Radar Detection

John Costas (1984) presented the following problem to Sol: At each of n consecutive time intervals, $t_1, t_2, \cdots, t_n$, a different frequency is transmitted from a set of n adjacent frequencies $f_1, f_2, \cdots, f_n$, in such a way that the *ambiguity function* (the two-dimensional autocorrelation function in both time and frequency), while having the value n at $(\Delta t, \Delta f) = (0, 0)$, has only the values 0 or 1 at any shift $(\Delta t, \Delta f) \neq (0, 0)$. This *ideal* (or *thumb-tack*) *ambiguity function* is best possible for determining the *range* (proportional to the time shift) and *Doppler* (the velocity to or from the observer, proportional to the frequency shift) of a target.

A Costas array of order n, also called an $n \times n$ Costas array, is a subset C of size n of the n^2 lattice points (i, j) with $1 \leq i, j \leq n$, such that no two of the n lattice points in C are in the same row or column, and such that no two of the $\binom{n}{2}$ line segments between pairs of points in C agree in both magnitude and slope.

Sol discussed this problem with Lloyd Welch and Abraham Lempel and shortly they came up with three systematic constructions to this problem, known as the Welch, Lempel and Golomb constructions, respectively [15]. These constructions remain the only known general constructions until now apart from some special techniques that expand or reduce the order of these three general constructions [16] and some unsolved problems are presented in [17]. Recently, Golomb and Hess tackled this problem from a slightly different angle [18]. The latest exhaustive search has been extended to $n = 29$. Table III shows a Costas array of order 4.

The Welch Construction. For every prime $p > 2$, let g be a primitive element of the prime field $\mathbb{F}_p$. Then the pairs (j, g^j) for $1 \leq j \leq p-1$ are the coordinates of the points in an order $(p-1)$ Costas array.

TABLE III
A Costas Array of Order 4

4			•	
3	•			
2		•		
1				•
	1	2	3	4

The Lempel and Golomb Constructions. For every finite field $\mathbb{F}_q$ of $q > 2$ elements (where $q = p^k$), let α and β be two distinct primitive elements. Then the pairs $\left(i, \log_\beta(1 - \alpha^i)\right)$ with $1 \leq i \leq q-2$ are the coordinates of the points in an order $(q-2)$ Costas array. Setting $\beta = \alpha$, one obtains the Lempel construction, else the Golomb construction in the general case.

Example 6: For $\mathbb{F}_7$, $C = \{(i, 3^i) \mid 1 \leq i \leq 6\}$ is a Costas array of order 6, which gives the permutation that maps $(1, 2, 3, 4, 5, 6)$ onto $(3, 2, 6, 4, 5, 1)$.

For $\mathbb{F}_{2^3}$ defined by a primitive polynomial $t(x) = x^3 + x + 1$ and α, a root of $t(x)$, let $\beta = \alpha^3$. We have the following two Costas arrays of order 6.

Lempel Construction:

$$(\log_\alpha(1 + \alpha^i),\ 1 \leq i \leq 6) = (3, 6, 1, 5, 4, 2)$$

Golomb Construction:

$$(\log_\beta(1 + \alpha^i),\ 1 \leq i \leq 6) = (1, 2, 5, 4, 6, 3)$$

The Costas array of order 4 in Table III results from removing two points, $(1, 1)$ and $(2, 2)$, of the above Costas array of order 6 from the Golomb construction. Methods of obtaining Costas arrays with reduced orders from known arrays are presented in [16].

An equivalent condition for Costas arrays, realized by Sol is that every $n \times n$ Costas array is a permutation, say $\pi(x)$ on $\{1, 2, \ldots, n\}$ with the Costas property, i.e., *difference triangle*: $(\pi(i + \tau) - \pi(i) : i = 0, \cdots, n - \tau - 1)$ as a τth row for $\tau = 1, \cdots, n-1$, and satisfying that no row contains a repeated entry [15]. For example, the above Costas array $(i, 3^i)$ has the following difference triangle:

3	2	6	4	5	1
−1	4	−2	1	−4	
3	2	−1	−3		
1	3	−5			
2	−1				
−2					

with no repeated entry in any row.

VIII. Golomb's Invariants and Modern Cryptography

A. Golomb's Invariants and Nonlinearity in Cryptography

There are only a few general known results relating to nonlinear-feedback shift-register sequences. Most of these can

TABLE IV
INVARIANTS OF f

$\mathbf{u}=(u_2,u_1,u_0)$	000	001	010	100	011	101	110	111
	0th order	1st order			2nd order			3rd order
$c_{\mathbf{u}}$	4	2	4	2	2	4	6	4
$T_{\mathbf{u}}$	4	6	4	6	6	4	6	4

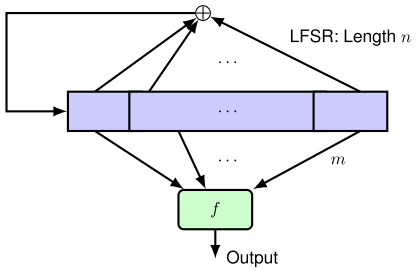


Fig. 5. A diagram of a filtering generator.

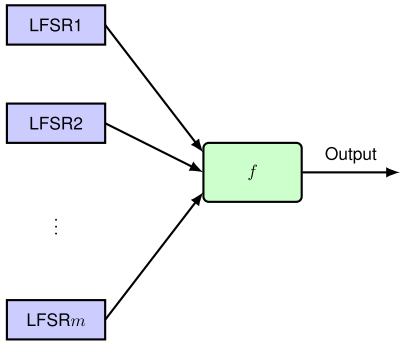


Fig. 6. A diagram of a combinatorial generator.

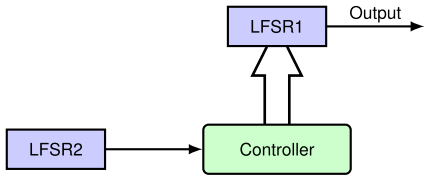


Fig. 7. A diagram of clock-control generator.

be found collected in Sol's book, *Shift Register Sequences* [1]–[3]. In cryptographic applications, in order to realize Shannon's concept of a one-time-pad, i.e., stream cipher encryption, m-sequences were used taking advantage of their long periods in the 1950s and 1960s. However, m-sequences are linear, so they cannot be directly used in cryptographic systems as this makes them vulnerable to various attacks. For this reason, researchers turned their attention towards nonlinear sequences, generated by filtering (i.e., combining in nonlinear fashion) a single LFSR or multiple LFSRs or else by using an LFSR to control a second LFSR, as shown in Figures 5-7. (In this section of the survey, by LFSR we will mean an LFSR that generates an m-sequence.)

A question in relation to a sequence obtained through filtering is how to measure the cryptographic strength of these filtering functions. Sol (1959 [19]) investigated the invariants of a boolean function $f(x_0,\cdots,x_{n-1})$ for classification of boolean functions. These invariants measure the distance between the boolean function and functions obtained by taking different linear combinations of its inputs.

Let $\mathbb{F}_2^n=\{(x_0,x_1,\cdots,x_{n-1})\,|\,x_i\in\mathbb{F}_2\}$ be a vector space over $\mathbb{F}_2$ with dimension n, and G consist of the following operations on the variables $(x_0,\cdots,x_{n-1})$ or on f: (a) all permutations on $\mathbf{x}=(x_0,x_1,\cdots,x_{n-1})$; (b) complementation on any subset of the components of $\mathbf{x}$; and (c) complementation on functions. So $|G|=2^{n+1}n!$. For $u_{n-1}\in\mathbb{F}_2^n$, let

$$c_{\mathbf{u}}=\sum_{\mathbf{x}\in\mathbb{F}_2^n}(f(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}), \tag{6}$$

where $\mathbf{u}\cdot\mathbf{x}=\sum_{i=0}^{n-1}u_ix_i$, the inner product on $\mathbb{F}_2^n$, the addition in $f(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}$ is the addition in $\mathbb{F}_2$, i.e., the sum is reduced modulo 2, while the $\sum$ is ordinary integer summation. Thus, $c_{\mathbf{u}}$ is equal to the (Hamming) weight of the function $f(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}$ (Hamming weight $H(\mathbf{z})$ of $\mathbf{z}\in\mathbb{F}_2^n$ is the number of 1's in $\mathbf{z}$). Sol defined

$$T_{\mathbf{u}}=\max\{c_{\mathbf{u}},2^n-c_{\mathbf{u}}\}$$

and showed that the multiset $I_i=\{T_{\mathbf{u}}\,|\,H(\mathbf{u})=i,\mathbf{u}\in\mathbb{F}_2^n\}$ is invariant under G for each $i=0,1,\cdots,n$, and I_i is called *the ith-order invariant*.

Example 7: Let $n=3$ and $f(x_0,x_1,x_2)=x_1+x_0x_1+x_1x_2$. The invariants of f appear in Table IV.

The concept of an invariant has tremendously important applications in modern cryptography. Given a boolean function $f(x_0,\cdots,x_{n-1})$, the nonlinearity of f, denoted as N_f is defined as

$$N_f=\min\{T_u\,|\,\mathbf{u}\in\mathbb{F}_2^n\}. \tag{7}$$

We say that f has *kth-order correlation immunity* if f is statistically independent of any t-subset of variables $\{x_0,\cdots,x_{n-1}\}$ for $1\le t\le k$ when the variables are treated as random variables. Furthermore, we say that f is kth-order if it has kth order correlation immunity and f is balanced, i.e., $T_0=2^{n-1}$.

Sol made the observations relating to invariants appearing in Figure 8. These observation leads to the fact recorded below.

Fact (Golomb, 1959): The condition that f is independent of $\{x_{i_1},x_{i_2},\cdots,x_{i_t}\}$ where $\{i_1,\cdots,i_t\}\subset\{0,1,\cdots,n-1\}$ is equivalent to f being independent of $x_{i_1}+x_{i_2},+\cdots+x_{i_t}$.

From this, it follows that f has kth-order correlation immunity if and only if

$$T_{\mathbf{u}}=2^{n-1},\quad\forall 1\le H(\mathbf{u})\le k. \tag{8}$$

Sol also introduced the technique of using the Walsh transform for computing $c_{\mathbf{u}}$ as shown in Figure 9. The Walsh

7. Application to Finding Assymetrical Logical Functions

If all the first-order invariants of a Boolean function $f(x_1,\ldots,x_k)$ are distinct, no permutation of variables leaves the function unaltered. If there is a variable whose complementation leaves the function unchanged, the corresponding first-order invariant must be 2^{k-1} (to satisfy $T_1^x = 2^k - T_1^x$). If all the first-order invariants are distinct, there is at most one such invariant (say T_1^x) such that $T_1^x = 2^{k-1}$. If there is no such invariant, the function f is changed by all $2^{k+1}\,k!$ operators in G. If there is an invariant $T_1^x = 2^{k-1}$, the only possible symmetries for f are $f(x', y,\ldots,z) = f(x, y,\ldots,z)$ or $f'(x', y,\ldots,z) = f(x, y,\ldots,z)$. In either case it is easy to determine by inspection whether or not f is altered by the entire transformation group. (A necessary condition for either of the symmetries mentioned to occur is that all the first order invariants be multiples of four, which already requires a large number of variables.)

Fig. 8. The text for discussing the condition when f is independent of variable x_i from [19].

5. The Rademacher-Walsh Expansion Coefficients

Rademacher defined a set of functions $\{r_i(x)\}$ on the half-open interval $[0, 1)$, $i = 0, 1, 2,\ldots$, according to the rule:

$$r_i(x) = \begin{cases} 1 & \text{if } \dfrac{m}{2^i} \leqq x < \dfrac{m+1}{2^i}, \quad m \text{ even} \\ -1 & \text{if } \dfrac{m}{2^i} \leqq x < \dfrac{m+1}{2^i}, \quad m \text{ odd}. \end{cases}$$

Walsh proved that the collection of finite products of Rademacher functions form a complete orthonormal system of functions for the interval [0, 1).

Some typical Rademacher-Walsh functions are shown in Figure 4. The completeness theorem implies that every real-valued function on [0,1) with only finitely many discontinuities is a linear combination of these Rademacher-Walsh functions, and the linear combination is unique.

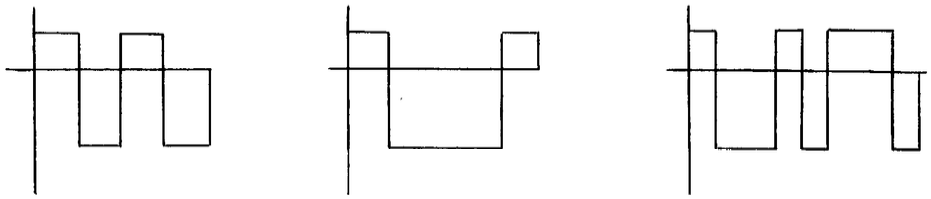


Figure 4. Some typical Rademacher-Walsh Functions.

The component of f relative to $r_o(x) \equiv 1$ gives c_o, from which the zero-order invariant is computed. The components of f relative to $r_1(x), r_2(x),\ldots,r_k(x)$ give $c_1^1, c_1^2,\ldots,c_1^k$, from which the first-order invariants of f are computed. The higher order invariants of f correspond to the coefficients of f relative to the Walsh functions.

Fig. 9. The text is from the original printing of his paper [19], c_1^j corresponds to $c_{\mathbf{u}}$ where $\mathbf{u}$ has Hamming weight 1.

transform or equivalently, the Hadamard transform, of the function $f(\cdot)$ is defined by

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+\mathbf{u}\dot{\mathbf{x}}}.$$

The relationship between $c_{\mathbf{u}}$ and $\hat{f}(\mathbf{u})$ is given by

$$\hat{f}(\mathbf{u}) = 2^n - 2c_{\mathbf{u}} \text{ or equivalently, } c_{\mathbf{u}} = 2^{n-1} - \frac{1}{2}\hat{f}(\mathbf{u}).$$

Thus, f has kth-order correlation immunity if and only if

$$\hat{f}(\mathbf{u}) = 0, \quad \forall H(\mathbf{u}) \text{ such that } 1 \leq H(\mathbf{u}) \leq k, \mathbf{u} \in \mathbb{F}_2^n.$$

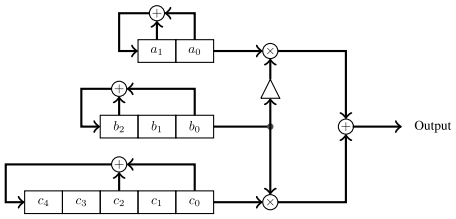
Sol's results, presented in 1959, were overlooked by the cryptographic community. The results on invariants were rediscovered in the late 1980s. The nonlinearity of a boolean function is currently regarded as one of the most important criteria to consider in designing cryptographically-strong boolean functions.

B. Golomb's Invariants for Correlation Related Attacks

The immediate applications of Sol's invariants of boolean functions in cryptography are the so-called *correlation attacks*. As long as a boolean function is correlated with some of the input variables, the initial states, loaded as keys, those correlated LFSRs can be recovered individually by computing the correlation between the output of the boolean function and that input. This converts the overall time complexity from the

product of the number of states in each LFSR to the sum of the number of states of those correlated LFSRs plus the remaining part from exhaustive search. This is a significant reduction to the size of the exhaustive search. Although Sol did not explicitly mention this application in his 1959's paper, he was awarded a Medal for his contribution to cryptography by the National Security Agency in 1992. In the following, we present an example for demonstrating the principle behind a correlation attack.

Example 8 (Correlation Attack): Let a combinatorial generator be given as follows.



Suppose it is used as a key stream generator and a 10-bit key is loaded in the form of initial states of all three LFSRs. An attacker obtains 40 consecutive bits of the outputs of this generator:

$$\mathbf{s}^{40} = (1001110111110100101001001001111100001101).$$

Now the attacker's goal is to recover the 10-bit key, i.e., the initial state of each LFSR.

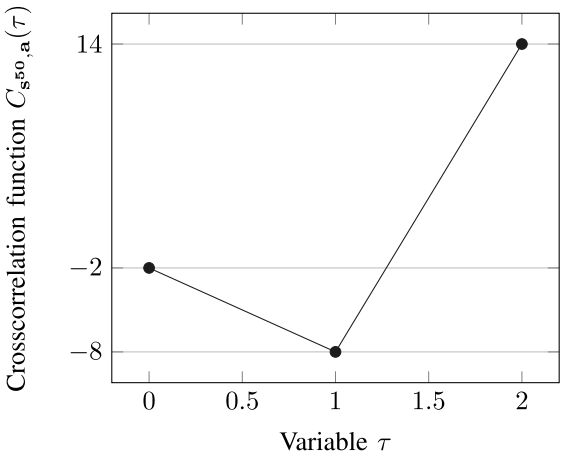
From Example 7 above, we know that the combining function $f(x_0, x_1, x_2) = x_0\overline{x}_1 + x_1x_2$ is correlated with x_0 and x_2 because the values of invariants $T_{\mathbf{u}} = 6$ for $\mathbf{u} = 001$ and $\mathbf{u} = 100$. So, we can compute the cross-correlation between LFSR 0 and **s**, and the cross-correlation between LFSR 2 and **s** to find their respective initial states, then do an exhaustive search to find the initial state of LFSR 1.

Now we assume reference initial states for each LFSR and the corresponding m-sequences:

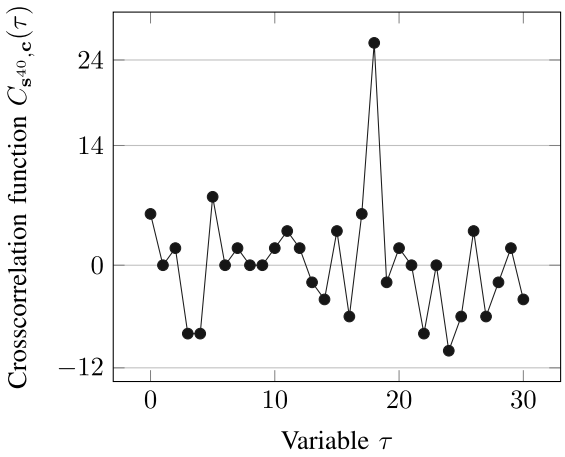
$$\mathbf{a} = 101\cdots$$
$$\mathbf{b} = 1001110\cdots$$
$$\mathbf{c} = 10000100101100111110000110111010\cdots$$

The cross-correlation between **s** and **a** and the cross-correlation between **s** and **c** are given as follows.

$$\{C_{(\mathbf{s}^{40},\mathbf{a})}(\tau) \mid \tau = 0, 1, 2\} = \{-2, -8, 14\}.$$



$$\{C_{(\mathbf{s}^{40},\mathbf{c})}(\tau) \mid \tau = 0, 1, \cdots, 30\}$$
$$= \{6\ \ 0\ \ 2\ \ -8\ \ -8\ \ 8\ \ 0\ \ 2\ \ 0\ \ 0$$
$$2\ \ 4\ \ 2\ \ -2\ \ -4\ \ 4\ \ -6\ \ 6\ \ 26\ \ -2$$
$$2\ \ 0\ \ -8\ \ 0\ \ -10\ \ -6\ \ 4\ \ -6\ \ -2\ \ 2$$
$$-4\}$$



So, we can decode it according to the peak values of the cross-correlations for LFSR 0 and LFSR 2. The cross-correlation between **s** and **a** has the peak value at $\tau = 2$, so the initial state in LFSR 0 for generating **s** is the 2nd state of the reference LFSR 0; and the cross-correlation between **s** and **c** has the peak value at $\tau = 18$, so the initial state in LFSR 2 is the 18th state of the reference LFSR 2. That is:

Initial state of LFSR 0: 11

Initial state of LFSR 2: 10001

Exhaustive search for a 3-bit initial state of LFSR 1: 010

So this complexity is much smaller than exhaustive search for 10 bit keys. The key is: 11 010 10001.

C. Two Faces of Invariants and Correlation Attacks

The first application of Golomb's work in 1959, i.e., investigating the correlation between the output and a linear combination of the input variables, as depicted in Figure 10, was to design f for the distance ranging problem using LFSRs with short periods to get a sequence with large period for the Venus ranging project and reduce the computational complexity by computing the cross-correlation between the incoming signal and locally generated PN sequence for each LFSR in order to recover the timing, which is equivalent to recovering the initial states which generates the incoming signal, as explained Section II-B. In this case, f should be correlated with input variables!

The second application is in cryptography, which means that it should be uncorrelated, otherwise the attacker can recover a key, loaded as initial states of those LFSRs, as shown in Example 7.

Golomb's invariants or correlation immunity of boolean functions can be computed by the Hadamard transform. Thus it is equivalent to measuring the correlation between a sequence and an m-sequence. However, there are a number of distinct LFSRs, corresponding to the number of primitive polynomials,

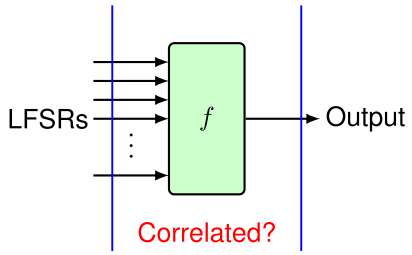


Fig. 10. When is it needed that the output should be correlated with inputs?

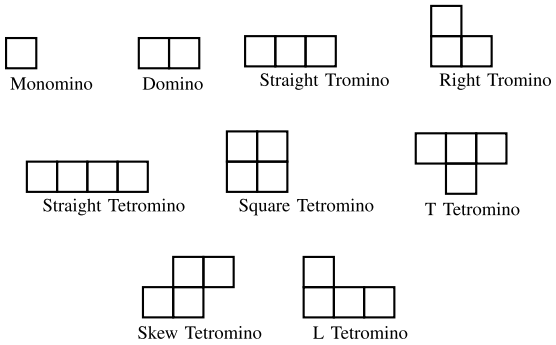


Fig. 11. The simple polyominoes.

which generate distinct m-sequences with the same period. It makes sense that the cryptographic strength should be measured from all distinct LFSRs instead of a single LFSR. This method is called *extended Hadamard transform* [20], which leads to the topic of hyperbent functions, which is another fascinating topic in symmetric key cryptography.

IX. Polyominoes

The other branch that Sol investigated is recreational mathematics. Sol generalized a puzzle problem about putting dominoes on a checkerboard from which a pair of opposite corners had been removed, and created the subject of Polyominoes (1954). His book, *Polyominoes - Puzzles, Patterns, Problems, and Packings* (1965, revised 1994) has a world-wide audience, and has lead to the invention of the computer game Tetris. In the following, we present three examples of those interesting tiling problems.

A *domino* is made of 2 connected squares and has only one shape, a rectangle, a tromino is a polyomino with 3 squares (2 different shapes), a tetromino, four connected squares, there are a total 5 different shapes, see Figure 11 for all the possible shapes composed by less than or equal to 4 connected squares [21].

A first interesting problem related to dominoes that Sol asked is that given a check-board with a pair of diagonally opposite corner squares deleted (see Figure 12), and a box of dominoes, each of which covers exactly 2 squares, is it possible to cover this board completely with dominoes (allowing no vacant squares and no overlaps)? The answer is no. (How does one prove that? See the remarkable proof given by Golomb in [21]). The second example is about pentominoes. The shapes that cover five connected squares

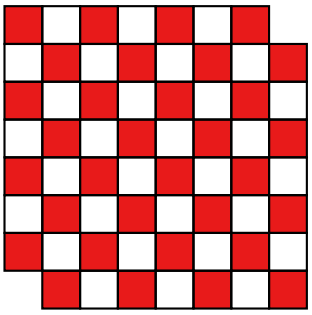


Fig. 12. Checkerboard with opposite corners deleted.

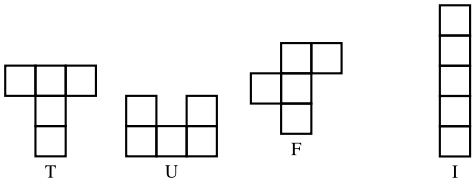


Fig. 13. Some shapes of pentominoes.

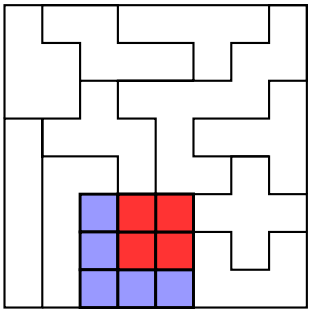


Fig. 14. The construction in this figure identifies a (8×8) board from which a (2×2) square (red squares) can be removed and the remaining region, tiled by 12 distinct pentominoes.

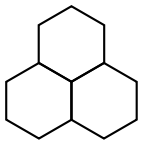


Fig. 15. A hexagonal triangle of side 2.

are called *pentominoes*. There are twelve of these, of which four are shown in Figure 13.

Since there are twelve distinct pentominoes, each covering five squares, their total area is sixty squares. So, it is obvious that one cannot place all twelve distinct pentominoes on an 8×8 board, since we will always have four squares left. A question that can be asked is whether they can be placed in such manner that the four surplus squares form a 2×2 area (a square tetromino) in some specified position on the board. Sol provides three solutions to this problem, of which one is shown in Figure 14.

The third example is to use hexagonals (referred to as *hexagonal animals*) for tiling. Sol proposed the following interesting question: can a larger hexagonal triangle be entirely tiled with copies of the triangles of side 2, as shown in Figure 15? The answer is positive and a solution is shown in Figure 16.

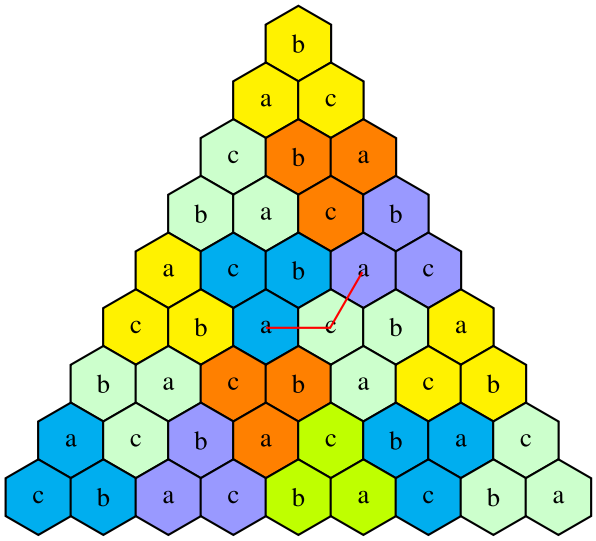


Fig. 16. A hexagonal triangle of side 9 is tiled with triangles of side 2.

The remarkable phenomenon about hexagonal tilings is their current application to cellular systems. A service area (a given spatial area, such as a city) is divided into non-overlapping cells, *hexagonals*, each cluster contains a set of hexagonals which use different frequencies for transmission (i.e., they all have different channels for transmission) for avoiding interference from other users. Channel reuse is a key element in cellular system design, as it determines how much interference is experienced by different users. For example, code-division multiple access (CDMA) can reuse every channel, since it differentiates users by their spreading codes (i.e., m-sequences in IS-95 and CDMA 2000). However, in other multiple access methods (e.g., time division multiple access (TDMA) and frequency division multiple access (FDMA)), the channel reuse is determined by the reuse distance, which is determined by their titling configuration.

The hexagonal triangle of side 9 in Figure 16 is an example which gives a solution to the channel reuse problem. In other words, it can be considered as a service area in a cellular system, for which a number of hexagonal triangles of side 2 are used to cover this service area where the channels can be reused in different hexagonal triangles of side 2, marked as a, b, c for different channels within one cluster. It has reuse distance 2. The channel assignment for reuse is determined by moving a center of a hexagonal (a cell) by one cell horizontally, then turning 60° counterclockwise and moving one cell, as shown in Figure 16.

X. Sol's "First Love" — Number Theory

Sol Golomb's "first love" was number theory, more specifically the aspect of analytic number theory dealing with the distribution of prime numbers. His Harvard thesis, and four or five subsequent papers, dealt with this topic, and even while in high school he contributed a problem in this area to the *American Mathematical Monthly*. His work played a role in the very recent breakthroughs (Zhang [22]) on the twin-prime conjecture [23]. Overall he wrote 20-25 papers on a wide variety of interesting topics in number theory. The deep and fascinating analogy between number theory and algebra over finite fields (especially between primes and irreducible polynomials) led to many of his important results in coding and communication theory.

The number of such primitive polynomials of degree n over $\mathbb{F}_2$ is known to be $\phi(2^n-1)/n$. This is the number of cyclically distinct m-sequences of degree n. Many unsolved problems concern the existence of such primitive polynomials with a restricted number of terms. Sol listed the two strongest conjectures as follows.

Conjecture 2 (Golomb, 1967): For infinitely many values of n there are primitive trinomials, $x^n + x^a + 1, 0 < a < n$.

Conjecture 3 (Golomb, 1967): For all degrees $n \geq 5$, there are primitive pentanomials, $x^n + x^a + x^b + x^c + 1,\ 0 < c < b < a < n$.

Those problems are still open. The corresponding advantages of those primitive polynomials with 3 or 5 taps provide less implementation cost, and are widely used in communications and hardware testing tools. However, they have some weakness for cryptographic applications as they admit some attacks.

XI. A Walk Through Time

This survey has taken a walk through time and drawn attention to some historical events of an academic nature that were part of Sol's academic career, as well as the practical problems he encountered and provided solutions to. The impact of Sol's work on linear and nonlinear feedback shift-register sequences has been immense, ranging from orbit determination of the Explorer 1 satellite launched in 1958, a more precise determination of the location of the planet Venus, spread-spectrum military communication, location determination using GPS, modern-day CDMA cellular communication and cryptography. The run-length Exp-Golomb code is part of the current standards of multimedia communication including MPEG-4 (or H.264). The popular Tetris computer game was inspired by Sol's work on Polyominoes. There are many new technologies on the horizon such as big data, cloud computing, the Internet-of-Things (IoT), blockchain networks to list just a few. The authors would not be in the least bit surprised to learn of new applications within these emerging technologies for the foundational theory and concepts laid down by Sol over the course of a remarkable career spanning over six decades.

References

[1] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA, USA: Holden-Day, Inc., 1967.
[2] S. W. Golomb, *Shift Register Sequences*, 2nd ed. Laguna Hills, CA, USA: Aegean Park, 1981.
[3] S. W. Golomb, *Shift Register Sequences*, 3rd ed. Singapore: World Scientific, 2017.
[4] J. Mykkeltveit, "A proof of Golomb's conjecture for the de Bruijn graph," *J. Combinat. Theory B*, vol. 13, no. 1, pp. 40–45, 1972.
[5] S. W. Golomb and G. Gong, *Signal Design for Good Correlation—For Wireless Communication, Cryptography, Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[6] L. R. Malling and S. W. Golomb, "Radar measurements of the planet Venus," *J. Brit. Inst. Radio Eng.*, vol. 22, no. 4, pp. 297–300, Oct. 1961.
[7] S. W. Golomb, "On the classification of balanced binary sequences of period 2^{n-1}," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 6, pp. 730–732, Nov. 1980.

[8] S. W. Golomb, "Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences," *Inf. Sci.*, vol. 1, no. 1, pp. 87–109, Dec. 1968.
[9] T. Helleseth, "The cross-correlation function between maximum-length sequences over GF(q)," M.S. thesis, Dept. Math., Univ. Bergen, Bergen, Norway, 1971.
[10] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, no. 3, pp. 209–232, Nov. 1976.
[11] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4–8, Jan. 2000.
[12] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.
[13] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed–Muller codes," *Inf. Control*, vol. 18, no. 4, pp. 369–394, 1971.
[14] S. W. Golomb, "Run-length encodings," *IEEE Trans. Inf. Theory*, vol. 12, no. 3, pp. 399–401, Sep. 1966.
[15] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combinat. Theory A*, vol. 37, no. 1, pp. 13–21, 1983.
[16] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proc. IEEE*, vol. 72, no. 9, pp. 1143–1163, Sep. 1984.
[17] S. W. Golomb, "Costas arrays—Solved and unsolved problems," presented at the Symp. Costas Arrays, CISS Conf., Princeton, NJ, USA, Mar. 2006.
[18] S. W. Golomb and R. Hess, "Optimum seating arrangements and Tuscan squares," *Ars Combinat.*, vol. 129, pp. 397–402, Oct. 2016.
[19] S. Golomb, "On the classification of Boolean functions," *IRE Trans. Circuit Theory*, vol. 6, no. 5, pp. 176–186, May 1959.
[20] G. Gong and S. W. Golomb, "Transform domain analysis of DES," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2065–2073, Sep. 1999.
[21] S. W. Golomb, *Polyominoes: Puzzles, Patterns, Problems, and Packings*. Princeton, NJ, USA: Princeton Univ. Press, 1996.
[22] Y. Zhang, "Bounded gaps between primes," *Ann. Math.*, vol. 179, no. 3, pp. 1121–1174, 2014.
[23] A. Hales, private communication, 2017.

Guang Gong received a B.S. degree in Mathematics in 1981 from Xichang Normal College, an M.S. degree in Applied Mathematics in 1985 from Xidian University, and a Ph.D. degree in Electrical Engineering in 1990 from University of Electronic Science and Technology of China (UESTC), a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, in Rome, Italy, and spent the following year there. She was promoted to an Associate Professor at UESTC in 1993. Dr. Gong worked with Dr. Solomon W. Golomb at the University of Southern California from 1996-1998. She joined the University of Waterloo, Canada in 1998, as an Associate Professor in the Dept. of Electrical and Computer Engineering (2000), and a full Professor (2004). Dr. Gong's research interests are in the areas of signal design, cryptography, and communication security. She has authored or co-authored more than 340 technical papers, two books, and two patents. Dr. Gong serves/served as Associate Editors for several journals including Associate Editor of the journal of *Cryptography and Communications* (2007 -) and Associate Editor of IEEE TRANSACTIONS ON INFORMATION THEOREM (2005-2008), and served on numerous technical program committees and conferences as co-chairs/organizers or committee members. Dr. Gong has received several awards including the Best Paper Award from the Chinese Institute of Electronics in 1984, the Premiers Research Excellence Award, Ontario, Canada, in 2001, Best Paper Award of IEEE ICC 2012, IEEE Fellow 2014, and the University Research Professor (2018).

Tor Helleseth (M'89–SM'96–F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973-1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981-1984, he was at the Chief Head quarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics, University of Bergen. During the academic years 1977-1978 and 1992-1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, the Netherlands. His research interests include coding theory and cryptology. Prof. Helleseth served as an Associate Editor for *Coding Theory* for the IEEE TRANSATIONS ON INFORMATION THEORY during the period 1991-1993 and 2012-2014. He was Program Chairman for Eurocrypt 1993 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co-Chairman for **SE**quences and **T**heir **A**pplications (SETA) in 1998, 2001, 2004, 2006 and 2012. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Solstrand, Norway in 2007. During 2007-2009 he served on the Board of Governors for the IEEE Information Theory Society. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography. In 2004 he was elected as a member of Det Norske Videnskaps-Akademi.

P. Vijay Kumar (S'80–M'82–SM'01–F'02) received the B.Tech. and M.Tech. degrees from IIT Kharagpur and IIT Kanpur respectively, and the Ph.D. degree from USC in 1983, all in Electrical Engineering. From 1983 to 2003 he was on the faculty of the EE-Systems Department at USC. Since 2003, he has been on the faculty of IISc Bengaluru. He currently also holds the position of Visiting Professor at USC.

His research interests include codes for distributed storage and wireless communication. He is a recipient of the 1995 IEEE Information Theory Society Prize Paper Award and the IEEE Data Storage Best Paper Award of 2011/2012. A pseudorandom sequence family designed in a 1996 paper co-authored by him now forms the short scrambling code of the 3G WCDMA cellular standard. He received the USC School of Engineerings Senior Research Award in 1994, the Rustum Choksi Award for Excellence in Research in Engineering in 2013 at IISc and the 2017-22 J. C. Bose National Fellowship awarded by the Indian Department of Science and Technology. He was on the Board of Governors of the IEEE Information Theory Society in 2013-15, was a plenary speaker at ISIT 2014 and a TPC Co-Chair of ISIT 2015. He is a Fellow of the INAE, IAS and INSA Indian academies.