Correlation of Boolean Functions

Guang Gong
Department of Electrical & Computer Engineering
University of Waterloo, CANADA
Presentation Outline

- Sequences, Correlation, Cryptographic Properties, Cryptanalysis, and Their Relation to Transforms for Signals
- Indication Functions: A Bridge to Connect Resiliency (Cross Correlation) and Propagation (Additive Autocorrelation)
- Constructions of Boolean Functions with 2-Level (Multiplicative) AC and Three-valued Additive AC, and more
- Discussions
Applications of Pseudo-random Sequences

In communications:
- Orthogonal codes, cyclic codes
- CDMA (code division multiple access) applications
- Synchronization codes
- Radar, and deep water distance range
- Testing vectors of hardware design
- ....

In cryptography:
- Key Stream Generators in Stream Cipher Models
- Functions in Block Ciphers
- Session Key Generators
- Pseudo-random Number Generators in Digital Signature Standard (DSS), etc.
- Digital Water-mark
- ....
Design of Pseudo-random Sequence Generators

(a) Towards 2-Level Auto-Correlation and Low Correlation

(b) Towards Large Linear Span

LFSR as Basic Blocks
Stream Cipher Applications

A Combinatorial Function Generator

\[ f \] is a boolean function in \( n \) variables.

A Filtering Generator

LFSR: Length \( m \)

\( n \leq m \)

Output

G. Gong  Finse'04
1-1 Correspondences Between Sequences, Polynomial Functions and Boolean Functions

- Trace Representation (Inverse DFT)
- Evaluation
- Lagrange Interpolation
- Vector Space

- Periodic Sequences
- Polynomial Functions
- Boolean Functions
Notation

- \( F = \text{GF}(2^n) \), a finite field, \( \alpha \) is a primitive element of \( F \)
- \( F_2 = \text{GF}(2) \), binary field.

- \( a = \{a_i\} \), a binary sequence with period \( N | 2^n - 1; f(x) \)
  the trace representation of \( a \), i.e.,
  \[
  a_i = f(\alpha^i), \quad i = 0, 1, \ldots
  \]

Note. \( f(x) \) is a polynomial function from \( \text{GF}(2^n) \) to \( \text{GF}(2) \)
which can be represented by
\[
 f(x) = \sum_k Tr_{1}^{n_k} (A_k x^k), \quad A_k \in \text{GF}(2^{n_k})
\]
where the \( k \)'s are different coset leaders modulo \( 2^n - 1 \), and \( n_k \) is
the size of the coset containing \( k \).

- \( x = x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} = (x_1, \ldots, x_n) \), an element in finite field
\( \text{GF}(2^n) \) or an element in the vector space \( F_2^n \).
(Multiplicative) Autocorrelation

The (multiplicative) autocorrelation of function \( f(x) \) is defined as the autocorrelation of the sequence \( a \), which is given by

\[
C_f(\tau) = 1 + C(\tau) = 1 + \sum_{i=0}^{N-1} (-1)^{a_{i+\tau} + a_i}, \quad \tau = 0, 1, \ldots
\]

The sequence \( a \) has an (ideal) 2-level autocorrelation if

\[
C(\tau) = \begin{cases} 
N & \text{if } \tau \equiv 0 \pmod{N} \\
-1 & \text{otherwise}
\end{cases}
\]
The additive autocorrelation of $f$ (or the additive autocorrelation of the sequence is defined through its trace representation $f$) is defined as the convolution of $f(x)$:

$$A_f(w) = \sum_{x \in F} (-1)^{f(x) + f(x+w)}$$
Known Constructions of 2-Level Autocorrelation Sequences (or Orthogonal Codes, or Hadamard Difference Sets)

- Number theory approach ($N$ is a prime): quadratic residue sequences (with $N \equiv 3 \mod 4$), Hall sextic residue sequences, and the twin prime sequences.

$N = 2^n - 1$:
- PN-sequences = $m$-sequences (1931, Singer, 1958, Golomb)
- Hyper-oval Construction: (Maschietti, 1998)
- Kasami Power Function Construction (Dobbertin, Dillon, 1998)
**2-level Additive Autocorrelation**

\[ f(x) \text{ is a bent function if and only if } \hat{f}(\lambda) = \pm \sqrt{2^n}, \quad \forall \lambda \in F \]

Note. Bent functions only exists for \( n \) even.

\( f(x) \) has 2-level additive autocorrelation if and only if \( f(x) \) is bent. There are two general constructions for bent functions (compared with the constructions of the binary sequences with 2-level (multi.) autocorrelation, this is relatively easy).

**Question:** What is the best additive autocorrelation for \( n \) odd?
Convolution or Additive autocorrelation of $f$:

$$A_f(w) = \sum_{x \in F} (-1)^{f(x)+f(x+w)}$$

They are related by the Convolution Law.

In other words, the square of the Hadamard transform of $f$ is equal to the Hadamard transform of the convolution of $f$ with itself or additive autocorrelation of $f$. Conversely,

$$A_f(w) = \frac{1}{2^n} \sum_{\lambda \in F} (-1)^{Tr(w\lambda)} \hat{f}^2(\lambda)$$

which is a fundamental relation through this representation.
Desired Cryptographic Properties of Boolean Functions

Definition 1 (Siegenthaler, 1984)

A Boolean function \( f(x) \) in \( n \) variables is \textit{kth-order correlation immune} if for each \( k \)-subset \( K \) of \( \{0, \ldots, n-1\} \), \( Z = f(x) \), considered as a random variable over \( F_2 \), is independent of all \( x_i \) for \( i \in K \). Furthermore, if \( f(x) \) is balanced and \( k \)th-order correlation immune, then \( f(x) \) is said to be \textit{k-order resilient}.

Nonlinearity of \( f \) is defined as the minimum distance of \( f(x) \) with all affine functions, or equivalently,

\[
N_f = 2^{n-1} - \frac{1}{2} \max_\lambda |\hat{f}(\lambda)|
\]

Property (Xiao and Massey, 1988). \( f(x) \) is \textit{kth-order correlation immune} if and only if

\[
\hat{f}(\lambda) = 0, \ 1 \leq H(\lambda) \leq k
\]

where \( H(x) \) is the Hamming weight of \( x \).

A historical remark.
Golomb studied these concepts under the terminology of \textit{invariants} of boolean functions in 1959, and he is the first to compute them using Hadamard transform.
Definition 2.

A Boolean function $f(x)$ in $n$ variables is said to satisfy the avalanche criterion (SAC) if

$$A_f(w) = 0 \quad \text{for all } w \text{ with } H(w) = 1$$

to have the k-order propagation if

$$A_f(w) = 0 \quad \text{for all } w \text{ with } 1 \leq H(w) \leq k$$
Hadamard transform

Resiliency, nonlinearity

Linear cryptanalysis

Convolution or Additive autocorrelation

k-order propagation

Differential cryptanalysis

(cross correlation with m-sequences)
Differential cryptanalysis (or propagation) is to exploit the correlation of the signal $f(t)$ at time instances $t$ and $t + \tau$.

Correlation immunity (or resiliency, nonlinearity, linear cryptanalysis) is to exploit the correlation between the signal $f(t)$ and the reference linear signal $l(t)$ at time instances $t$ and $t + \tau$. 
**Indicator Function:** A Bridge for Connecting Resiliency and Additive Autocorrelation

**Definition.** A indicator function of \( f \), denoted by \( \sigma_f(x) \), is defined as

\[
\sigma_f(\lambda) = \begin{cases} 
0 & \text{if } \hat{f}(\lambda) = 0 \\
1 & \text{if } \hat{f}(\lambda) \neq 0
\end{cases}
\]

**Example.** For \( n = 5 \), GF\( (2^5) \) defined by \( \alpha^5 + \alpha^3 + 1 = 0 \), and

\[
f(x) = \text{Tr}(x^3)
\]

| \( i \) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| \( \hat{f}(\alpha^i) \) | -8 | 0 | 0 | 0 | 0 | -8 | 0 | 8 | 0 | -8 | -8 | 8 | 0 | 8 | 8 | 0 | 0 | 0 | -8 | 8 | -8 | 8 | 8 | 0 | 0 | 8 | 8 | 0 | 8 | 0 | 0 |

| \( \sigma_f(\alpha^i) \) | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
Preferred set: For \( n = 2m + 1 \), \( f \) is said to be preferred if the Hadamard transform of \( f \) has the following three values:

\[
P = \{0, \pm 2^{m+1}\}
\]

Optimal Additive autocorrelation (AC): For \( n = 2m + 1 \), let \( f \) be balanced, the additive AC of \( f \) is said to be optimal if the maximal magnitude of the additive AC at nonzero, denoted as \( \Delta_f \), is \( 2^{m+1} \) and \( A_f \) has \( 2^{n-1} \) zeros in \( \text{GF}(2^n) \).

Note.
1. According to the Parseval energy formula, \( 2^{m+1} \) is minimum among magnitudes of all 3-valued Hadamard spectra.
2. Zhang and Zheng (1995) conjectured that:

\[
\Delta_f \geq 2^{m+1}
\]
Observation 1: Indicator Function and Resiliency

Let $f$ be preferred. Then $f$ is 1-order resilient if and only if the dual of $f$ is nonlinear.

Observation 2: Indicator Function and Additive Autocorrelation

Let $f$ be preferred. Then the additive autocorrelation functions of $f$ at nonzero is equal to opposite of the Hadamard transform of $f$. In other words,

$$A_f(w) = -\hat{\sigma}_f(w), \quad \forall \ 0 \neq w \in GF(2^n)$$
Theorem. A Sufficient Condition for Preferred Additive Autocorrelation

If the Hadamard transforms of both \( f \) and its indicator functions are preferred, then the additive autocorrelation is preferred.

\[
\hat{f}(\lambda) \in P, \quad \sigma_f = g, \quad \hat{\sigma}_f(\lambda) \in P, \quad 1\text{-resiliency}, \quad \sigma_g, \quad 1\text{-propagation}, \quad A_f(w) \in P \quad P = \{0, \pm 2^{(n+1)/2}\}
\]
All functions, listed in Tables 1-3, are from binary sequences with 2-level (multiplicative) autocorrelation.

Cryptographic Properties:
a) 2-level AC
b) Nonlinearity: $2^{n-1} - 2^{(n-1)/2}$
c) Preferred $f$
d) 1-order resiliency
e) Preferred additive AC, so optimal additive AC
f) 1-order propagation.
### Table 1. Properties (a)-(d)

<table>
<thead>
<tr>
<th>Functions from the sequence sets</th>
<th>Indicator Functions</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kasami decimation: ( Tr(x^d), d = 2^{2^k} - 2^k + 1 )</td>
<td>( Tr(x^{2^k+1}), \text{ for } 3k \equiv 1 \mod n )</td>
<td>Kasami 1971, Dillon 1999</td>
</tr>
<tr>
<td>The other Kasami, Welch, Niho</td>
<td>Nonlinear</td>
<td></td>
</tr>
<tr>
<td>Subset of GMW sequences</td>
<td>Nonlinear</td>
<td>2-level AC (Goldon, Miller, Welch 1961) HT (Games (85), Klapper(96))</td>
</tr>
<tr>
<td>Welch-Gong sequences ( WG(x) )</td>
<td>( Tr(x^{d^{-1}}) )</td>
<td>2-level AC (No et. al 1998, Dillon et. al. 1999)</td>
</tr>
<tr>
<td>Glynn Type 1 hyperoval sequences</td>
<td>( Tr\left(x^{(k-1)/k}\right) )</td>
<td>2-level AC (Matchietti 1998), Hadamard transform (Xiang 1998, Dillon 1999)</td>
</tr>
<tr>
<td>Kasami power function sequences: ( C_k(x) )</td>
<td>( Tr\left(x^{(2^k+1)/3}\right) )</td>
<td>2-level AC (No et. al 1998, Dillon et. al. 1999)</td>
</tr>
</tbody>
</table>
### Table 2. Properties (a)-(e)

\[ 3k \equiv 1 \mod n \]

<table>
<thead>
<tr>
<th>(Boolean) Functions</th>
<th>Indicator Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kasami sequences:</td>
<td></td>
</tr>
<tr>
<td>( Tr(x^d), d = 2^{2k} - 2^k + 1 )</td>
<td>( Tr(x^{2^k + 1}) )</td>
</tr>
<tr>
<td>Welch-Gong sequences</td>
<td></td>
</tr>
<tr>
<td>( WG(x) = Tr(t(x + 1) + 1) )</td>
<td>( Tr(x^{d^{-1}}) )</td>
</tr>
<tr>
<td>Kasami power function sequences:</td>
<td></td>
</tr>
<tr>
<td>( C_3(x), k = 3 )</td>
<td>( Tr(x^3) )</td>
</tr>
<tr>
<td>( C_k(x) = Tr(t(x^{2^k + 1})) )</td>
<td>( Tr(x^{d^{-1}}) )</td>
</tr>
</tbody>
</table>

where

\[
t(x) = x + x^{2^k + 1} + x^{2^{2k} + 2^k + 1} + x^{2^{2k} - 2^k + 1} + x^{2^{2k} + 2^k - 1}
\]
### Table 3. Properties (a)-(f)

<table>
<thead>
<tr>
<th>(Boolean) Functions</th>
<th>Indicator Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welch-Gong sequences</td>
<td>$Tr(x^{d-1})$</td>
</tr>
<tr>
<td>$WG(x) = Tr(t(x+1)+1)$</td>
<td></td>
</tr>
<tr>
<td>Kasami power function sequences</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$(5\text{-term sequences})$:</td>
</tr>
<tr>
<td>$C_k(x) = Tr(t(x^{2^k+1}))$</td>
<td>$Tr(x^{d-1})$</td>
</tr>
</tbody>
</table>

where

$$t(x) = x + x^{2^k+1} + x^{2^k+2^k+1} + x^{2^{2k}-2^k+1} + x^{2^{2k}+2^k-1}, \quad 3k \equiv 1 \mod n$$
Example 11.7 Let $n = 7$. Then $k = 5 \Rightarrow n - k = 2 \Rightarrow 2^{n-k} + 1 = 5$, and $t(x) = x + x^5 + x^{21} + x^{13} + x^{29}$. Thus

$$C_5(x) = Tr(t(x^{2^2+1})) = Tr(x^5 + x^{19} + x^{29} + x^3 + x^9)$$
$$WG(x) = Tr(t(x+1)+1) = Tr(x + x^3 + x^7 + x^{19} + x^{29}).$$

Both $C_5(x)$ and $WG(x)$ have the following properties:

(a) Orthogonal or 2-level autocorrelation.

(b) Nonlinearity $N_f = 56$.

(c) Hadamard transform is preferred, i.e., belongs to $\{0, \pm 16\}$.

(d) 1-resiliency under some basis.

(e) The additive autocorrelation function is preferred, i.e., belongs to $\{0, \pm 16\}$.

(f) 1-order propagation under some basis.
What are the additive autocorrelations of the rest functions with 2-level autocorrelation?

The functions constructed from sequence design do not have linear structure for any fixed set of input variables (possible week leakage of Maiorana-McFarland like resilient functions).

Experimental results show that there are many functions having preferred Hadamard transform, and preferred additive AC, so optimal additive AC, but not 2-level AC.