On the Arithmetic Walsh Coefficients of Boolean Functions

Claude Carlet[1] Andrew Klapper[2]

[1]University of Paris 8, LAGA

[2]University of Kentucky

Workshop on Codes and Cryptography 2013

Outline

Without Carry

“Classical” symmetric key crypto:

- Boolean functions ($f : V_n = \mathbb{F}_2^n \to \mathbb{F}_2$), vectors, sequences
- eg: S-box $=$ Boolean vector valued function on $\mathbb{F}_2^n$
- Analysis of structures by polynomials, power series
- eg: Sequence $a_0, a_1, a_2, \cdots, a_n \in \mathbb{F}_2 \leftrightarrow \sum a_i x^i$
- Some analysis depends on finding “nearest" linear function function:

$$\ell_a(b) = \sum_{i=1}^{n} a_i b_i \pmod 2 = [a \cdot b]_2$$

“Near” = Hamming distance

With Carry

Research program since 1992: find & exploit with carry analogs of without carry structures:

Without carry	With carry
Boolean polynomial	Base 2 integer
Power series	2-adic number
LFSR	FCSR
Trace function	$a \pmod{q} \pmod{2}$
Polynomial over $\mathbb{F}_q$	Algebraic integer
Correlation function	Arithmetic correlation

SETA '10 (Goresky, K): With carry analog of Walsh-Hadamard transform of a Boolean function

Boolean Functions and Walsh-Hadamard Transforms

$B_n = \{$Boolean functions$\}$ is a ring with component-wise operations.

Definition

If f is a BF and $b \in V_n$, then $\widehat{f}(b) = \sum_{a \in V_n} (-1)^{f(a) - \ell_b(a)}$

Invertible: $\sum_{b \in V_n} \widehat{f}(b)(-1)^{\ell_a(b)} = 2^n f(a)$

Imbalance of f: $Z(f) = \sum_{a \in V_n} (-1)^{f(a)}$

Then $\widehat{f}(b) = Z(f - \ell_b)$

Poisson Summation Formula (PSF)

$f \in B_n$ a Boolean function on V_n: for any $d \in V_n$, subspace $S \subseteq V_n$:

$$\sum_{a \in S} (-1)^{d \cdot a} \widehat{f}(a) \quad = \quad |S| \sum_{b \in d + S^{\perp}} (-1)^{f(b)}$$

Useful for:

- bounding the algebraic degree of Boolean functions from divisibility properties of the WT
- studying normal functions
- relating bent functions and their duals

Further Application: Resilience

- Boolean function f is *m-resilient* if balanced and fixing any m coordinates gives a balanced function
- Measures resistance to Siegenthaler's attack on combiners
- m-resilient iff $(\mathrm{wt}_H(a) \leq m \Rightarrow \widehat{f}(a) = 0)$, thanks to PSF

Outline

2-Adic Algebra

Recall: 2-adic integer is a sum $f = \sum_{i=0}^{\infty} a_i 2^i$, $a_i \in \{0, 1\}$

Addition: to add $a = \sum a_i 2^i$ plus $b = \sum b_i 2^i$, add $a_i + b_i$, but there may be a carry to $i + 1$st coefficient

Formally: define c_i, carry $d_i \in \{0, 1\}$ by $d_0 = 0$ and

$$a_i + b_i + d_i = c_i + 2d_{i+1}$$

Then $a + b = \sum c_i 2^i$

Multiplication is similar

This makes $\mathbb{Z}_2 = \{\sum_{i=0}^{\infty} a_i 2^i : a_i \in \{0, 1\}\}$ an algebraic ring

Imbalance:
if a is eventually periodic, $z(a) = \sum_i (-1)^{a_i}$, sum over one period

Extended Boolean Functions

Addition with carry for Boolean functions: where do the carries go?

Extend the BF: given $f : V_n \to \mathbb{F}_2$, define $\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2$ by

$$\mathbf{f}(a_1, \cdots, a_n) = f(a_1 \pmod 2), \cdots, a_n \pmod 2))$$

Result is 2-periodic: $\mathbf{f}(a + 2b) = \mathbf{f}(a)$

More general: $R_n = \{\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2\}$

Addition: given $\mathbf{f}, \mathbf{g} \in R_n$, define $\mathbf{h}, \mathbf{k} \in R_n$ by $\mathbf{k}(a_1, \cdots, a_n) = 0$ if any $a_i = 0$ and for all $a \in \mathbb{N}^n$

$$\mathbf{f}(a) + \mathbf{g}(a) + \mathbf{k}(a) = \mathbf{h}(a) + 2\mathbf{k}(a + 1^n)$$

Then $\mathbf{f} + \mathbf{g} = \mathbf{h}$

Extended Boolean Functions (2)

Multiplication is similar

Theorem

R_n with these operations is a ring. The set of eventually 2-periodic elements of R_n is closed under $+$, $-$.

For $\mathbf{f} \in R_n$, let $$\phi_{\mathbf{f}} = \sum_{a=(a_1,\cdots,a_n)\in\mathbb{N}^n} \mathbf{f}(a) t_1^{a_1} \cdots t_n^{a_n} \in \mathbb{Z}[[t_1, \cdots, t_n]]$$

Theorem

The function $\mathbf{f} \mapsto \phi_{\mathbf{f}}$ is a ring isomorphism from R_n to $\mathbb{Z}[[t_1, \cdots, t_n]]/(t_1 t_2 \cdots t_n - 2)$.

So, $\mathbf{f} \in R_n$ corresponds to a choice of $\bar{f}(a) \in \mathbb{Z}_2$
for each $a \in$ coordinate hyperplane

Outline

Arithmetic Walsh Transform (AWT)

Let $\mathbf{f} \in R_n$ be eventually 2-periodic

Imbalance of $\mathbf{f}$ is $Z(\mathbf{f}) = \sum_a (-1)^{\mathbf{f}(a)}$ (sum over one period of $\mathbf{f}$)

$\ell_b(a) = [a \cdot b]_2 =$ inner product of a and b modulo 2

Definition

The *arithmetic Walsh Transform* of $\mathbf{f}$ is $W(\mathbf{f}) : V_n \to \mathbb{Z}$ defined by

$$W(\mathbf{f})(b) = Z(\mathbf{f} - \ell_b).$$

The *arithmetic Walsh Transform* of a Boolean function f is the arithmetic Walsh Transform of the extension $\mathbf{f}$ of f, $W(f)(b) = W(\mathbf{f})(b)$.

AWT Previous Results

Theorem

No two functions have the same arithmetic Walsh transforms.

So the AWT is invertble

Known:

- AWT of affine functions
- AWT of certain quadratic functions
- $E[W(f)(b)]$
- $E[W(f)(b)^2]$

Outline

Poisson Summation Formula for AWTs

Fix $d \in V_n$. Let S be a linear subspace of V_n. Goal: describe

$$\Gamma_S(f,d) = \sum_{a \in S} (-1)^{d \cdot a} W(f)(a) = \sum_{a \in S} (-1)^{d \cdot a} Z(\mathbf{f} - \ell_b)$$

in terms of attributes of f

Notation: For any set $T \subseteq V_n$, let

$$H_T(f) = H_T = \sum_{b \in T} f(b) \quad \text{and} \quad Q_T(f) = Q_T = \sum_{b \in T} f(b) f(b + 1^n)$$

If 1^n is not a parity check for S, then $S_0 = \{a \in S : a \cdot 1^n = 0\}$, and $S_1 = S \setminus S_0$

Theorem

Suppose that 1^n is a parity check for S. Then

$$\Gamma_S(f,d) = \begin{cases} |S|(2^n - 2H_{V_n} + Q_{V_n \setminus S^\perp}) & \text{if } d \in S^\perp \\ -|S|Q_{d+S^\perp} & \text{if } d \notin S^\perp. \end{cases}$$

Theorem

Suppose that 1^n is not a parity check for S. Then, with the notation above:

If $d \in S^\perp$: $\Gamma_S(f,d) = (|S|/4)(2^{n+1} - 2H_{V_n} - 2Q_{S_0^\perp} + H_{S_0^\perp} - 2H_{S^\perp} - H_{1^n+S_0^\perp} + 2H_{1^n+S^\perp})$.

If $d \in S_0^\perp \setminus S^\perp$: $\Gamma_S(f,d) = (|S|/2)(2^n - 3H_{V_n} + Q_{V_n} + H_{1^n+S_0^\perp} - H_{1^n+S^\perp} - H_{S_0^\perp} + H_{S^\perp})$.

If $d \notin S_0^\perp$: $\Gamma_S(f,d) = -(|S|/4)(2Q_{d+S_0^\perp} + 2H_{d+S^\perp} - 2H_{1^n+d+S^\perp} - H_{d+S_0^\perp} + H_{1^n+d+S_0^\perp})$.

Outline

- Fix $n-k$ coordinates to 0 = Coordinate subspace of dimension k $\Leftrightarrow$ pick $I \subseteq \{1,\cdots,n\}$, $|I|=k$ let $S=$ all a: support of $a \subseteq I$

- f is *m-resilient* if balanced and restriction to any translate of a dimension $n-m$ coordinate subspace is balanced $\Leftrightarrow \forall a, \mathrm{wt}_H(a) \leq m : \widehat{f}(a)=0$

- For $T \subseteq V_n$: $H_T(f)=\sum_{a\in T} f(a)$.
  f *unbiased* for H on T if $H_T(f)=E[H_T]=|T|/2$

- m-resilient: if S is a coordinate subspace of dimension $\geq n-m$, then $\forall d \in V_n$, f is unbiased for H on $d+S$

- What if we replace H_T by other statistical measures?

- Example: $Q_T(f)=\sum_{a\in T} f(a)f(a+1^n)$

Q-Resilience

- f is *unbiased* for Q on T if $Q_T(f) = E[Q_T] = |T|/4$
- $S \subseteq V_n$ a linear subspace. f is *Q-immune on S* if $\forall d \in V_n$, f is unbiased for Q on $d + S$. f is *Q-resilient on S* if balanced and Q-immune
- Even weight coordinate subspace of degree k: pick $I \subseteq \{1, \cdots, n\}$, $|I| = k$, let $S =$ all even weight a: support of $a \subseteq I$

Theorem

$f \in B_n$, S an even weight coordinate subspace of degree m.
f is Q-immune on $S^\perp$ iff $\forall a \neq 0^n \in S : W(f)(a) = W(f)(0^n) + 2^{n-2}$.
f is Q-resilient on $S^\perp$ iff $W(f)(0^n) = 0$ & $W(f)(a) = 2^{n-2}$, $a \neq 0^n \in S$.

Theorem

$f \in B_n$, S a coordinate subspace of dimension m.
If f is Q-resilient on $S^\perp$, then f is Q-resilient on $S_0^\perp$.

Suppose f is m-resilient. If f is Q-resilient on $S_0^\perp$, then

- $W(f)(0^n) = 0$,
- $W(f)(a) = 2^{n-2}$ *if* $a \neq 0^n$ *and* $a \in S_0$, *and*
- $W(f)(a) = 2^{n-1} - 2^{n-m-1}$ *if* $a \in S_1$.

Proof Sketch

S an even weight coordinate subspace

f balanced $\Rightarrow W(f)(0^n) = 2^n - 2H_{V_n} = 0$

f unbiased for Q on $d + S^\perp \Rightarrow Q_{d+S^\perp} = |S^\perp|/4$ if $d \notin S^\perp$

Gives $|S|$ linear equations (one per coset of $S^\perp$) in $|S|$ variables (the $W(f)(a), a \in S$)

Rank is $|S| - 1$, but $W(f)(0^n)$ determines a unique solution

Outline

1. Background
2. Arithmetic Walsh Transforms
   - Algebraic background
   - The Transform
   - Poisson Summation Formula
   - Application: Resilience
   - AWT and Cubic Boolean Functions
3. Further Thoughts

Old theorem (Carlet): $f \in B_n$, $c \in V_n$: $\exists p \geq 0 \in \mathbb{Z}$, $h \in B_{n+2p}$ so $\deg(h) \leq 3$ and $\widehat{h}(0^{n+p}) = Z(h) = 2^p \widehat{f}(c)$

Definition

$f \in B_n$ is *diagonal* if $\forall a \in V_n : f(a + 1^n) = f(a)$ (1^n is a linear structure).

Theorem

Let $f \in B_n$ be a diagonal Boolean function and let $c \in V_n$.

Then $\exists p \geq 0 \in \mathbb{Z}$, diagonal $h \in B_{n+2p}$ so $\deg(h) \leq 3$ and $W(h)(0^{n+p}) = Z(h) = 2^p W(f)(c)$.

Questions

Can we find a cryptanalytic attack based on Q-bias?

Is there a cryptanalytic attack whose effectiveness is measured by the arithmetic Walsh transform?

Other applications of Arithmetic Poisson Summation Formula?

Other transforms?