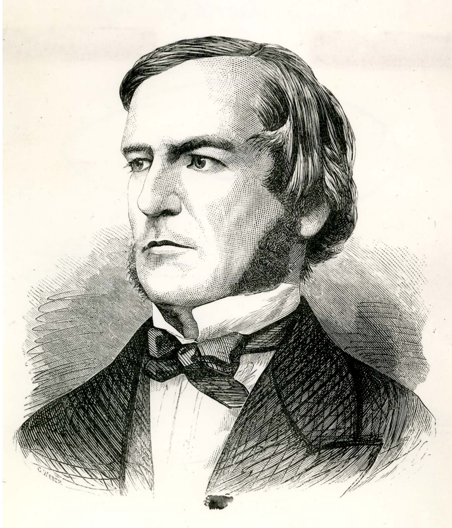
SCIENCE
PASSION
TECHNOLOGY

(Vectorial) Boolean Functions

Reinhard Lüftenegger

Mathematical Background of Cryptography – WT 2019/20

George Boole



Overview

Boolean Functions

- Preliminaries
- Representation of Boolean Functions
- Möbius Transform

Cryptanalysis of Boolean Functions

- Higher-Order Differential Cryptanalysis
- Mathematics of Higher-Order Differential Cryptanalysis

Motivation

Boolean functions are important because ...

- ... they natively allow to work with binary encoded information.
- ... they are used in many symmetric key primitives (AES, LowMC, MiMC, Prince, ...).

Our goals for today are:

- Discuss **different representations** of boolean functions.
- Outline a basic concept of **cryptanalysis** on boolean functions.

Boolean Functions

Boolean Functions

Our basic object of study in this lecture is outlined in the following

Definition

Let $n, m \in \mathbb{N}$. A function $\mathbb{F}_2^n \to \mathbb{F}_2$, with

$$(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n),$$

is called a boolean function. Similarly, a vectorial boolean function (or vector valued boolean function) is a function $\mathbb{F}_2^n \to \mathbb{F}_2^m$ with

$$(x_1, \ldots, x_n) \mapsto (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

The functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ are also called the coordinate functions of f.

Preliminaries I

Question: Which algebraic structure does the *n*-fold Cartesian product $\mathbb{F}_2^n$ admit?

Answer: First of all, it is an $\mathbb{F}_2$-vector space. Its elements are tuples of length *n* with coordinates in $\mathbb{F}_2$, i.e. we have

$$\mathbb{F}_2^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{F}_2 \text{ for all } i\}.$$

Vector addition is defined as

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

and scalar multiplication is given by

$$\lambda \cdot (x_1, \ldots, x_n) := (\lambda \cdot x_1, \ldots, \lambda \cdot x_n),$$

for all $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ and $\lambda \in \mathbb{F}_2$.

Preliminaries II

Question: Is there any connection between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$?

Answer: Yes, there is. We can endow $\mathbb{F}_2^n$ with the field structure of $\mathbb{F}_{2^n}$. Field addition is clear (how?). But what about field multiplication?

Structure of $\mathbb{F}_{2^n}$: Elements in $\mathbb{F}_{2^n}$ can be represented as polynomials of degree at most $n-1$, right? Multiplication in $\mathbb{F}_{2^n}$ is ordinary polynomial multiplication modulo some $\mathbb{F}_2$-irreducible polynomial f of degree n (see **L3 - Fields and Finite Fields**).

Relation between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$: To define multiplication in $\mathbb{F}_2^n$, we “encode” binary vectors as polynomials (and vice versa) via

$$x := (x_1, x_2, \ldots, x_{n-1}, x_n) \in \mathbb{F}_2^n \longleftrightarrow p_x := x_1 Y^{n-1} + x_2 Y^{n-2} + \cdots + x_{n-1} Y + x_n \in \mathbb{F}_{2^n}.$$

Then, in $\mathbb{F}_2^n$, we have $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (z_1, \ldots, z_n)$, where $p_z := z_1 Y^{n-1} + \cdots + z_n \in \mathbb{F}_{2^n}$ comes from the congruence

$$p_z = p_x \cdot p_y \pmod{f}.$$

Preliminaries III

Question: Considering the construction

$$\mathbb{F}_q[X_1, \dots, X_n] / \left(X_1^q - X_1, \dots, X_n^q - X \right),$$

how would you put into words the structure of its elements?

Preliminaries IV

Let's discuss some examples that may illuminate the aforementioned construction.

Example: Consider the quotient ring $\mathcal{Q} := \mathbb{F}_2[X, Y, Z]/(X^2 - X, Y^2 - Y, Z^2 - Z)$. What is the reduced representation of

$$X^2Y^5Z^4 \text{ and } X^2Y^3Z + XYZ + X + Z + Z^6$$

in above quotient ring?

Preliminaries V

Remark: For any field E, every polynomial $f \in E[X]$ induces a polynomial function $f : E \to E, a \mapsto f(a)$.

Theorem (Every Function over a Finite Field is a Polynomial Function)

Every map $f : \mathbb{F}_q \to \mathbb{F}_q$ on a finite field $\mathbb{F}_q$ can be uniquely described as a univariate polynomial over $\mathbb{F}_q$ with maximum degree $q - 1$.

Proof

For existence, consider the polynomial

$$F(X) := \sum_{a \in \mathbb{F}_q} f(a)(1 - (X - a)^{q-1}).$$

For uniqueness, observe, if there are two polynomials F, G of degree at most $q - 1$ with $F(x) = f(x) = G(x)$, for all $x \in \mathbb{F}_q$, then $F - G$ has q roots. Thus, $F = G$. □

Preliminaries VI

There is also a more general version of the preceding result

Theorem

Every map $f : \mathbb{F}_q^n \to \mathbb{F}_q$ can be uniquely described as a multivariate polynomial over $\mathbb{F}_q$ in n variables with maximum degree $q-1$ in each variable.

Proof

For existence, consider the polynomial

$$F(X_1, \ldots, X_n) := \sum_{(a_1,\ldots,a_n)\in\mathbb{F}_q^n} f(a_1, \ldots, a_n) \prod_{1\leq i\leq n} (1 - (X_i - a_i)^{q-1}).$$

Uniqueness follows from a cardinality argument: the two finite sets $\mathcal{S} := \mathbb{F}_q[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$ and $\mathcal{R} := \{f : \mathbb{F}_q^n \to \mathbb{F}_q\}$ have the same cardinality q^{q^n} and the map $\varphi : \mathcal{R} \to \mathcal{S}$ with $\varphi(f) := F(X_1, \ldots, X_n)$ is injective. $\square$

Truth Table I

If we arrange the inputs and outputs of a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)$, in form of a table

x_1	x_2	$\ldots$	x_{n-1}	x_n	$f(x_1, \ldots, x_n)$
0	0	$\ldots$	0	0	$f(0, 0, \ldots, 0, 0)$
0	0	$\ldots$	0	1	$f(0, 0, \ldots, 0, 1)$
0	0	$\ldots$	1	0	$f(0, 0, \ldots, 1, 0)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\ldots$	1	0	$f(1, 1, \ldots, 1, 0)$
1	1	$\ldots$	1	1	$f(1, 1, \ldots, 1, 1)$

we get the truth table representation of f.

Truth Table II

Nota Bene: Fixing an order of the input vectors (e.g. lexicographic) and denoting them (e.g. in ascending order) by $x^{(1)}, x^{(2)}, \ldots, x^{(q)}$ we can compress this representation into a single sequence, also called the value vector of f, given by

$$\left(\quad f\left(x^{(1)}\right) \quad , \quad f\left(x^{(2)}\right) \quad , \quad \ldots \quad , \quad f\left(x^{(n)}\right) \quad \right).$$

Example: Consider the function $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ with $f(x_1, x_2, x_3) := x_1^2 x_2 + (x_2 x_3)^2 + x_3$ (sic!). What is its truth table and value vector?

Algebraic Normal Form (ANF) I

Above theorem about the multivariate representation of functions $\mathbb{F}_q^n \to \mathbb{F}_q$ applies in particular to boolean functions $\mathbb{F}_2^n \to \mathbb{F}_2$. Therefore we can state the following

Theorem (Algebraic Normal Form of Boolean Functions)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function of n variables. Then there exists a unique polynomial $F(X_1, \ldots, X_n) \in \mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 - X, \ldots, X_n^2 - X_n)$ such that

$$F(x_1, \ldots, x_n) = f(x_1, \ldots, x_n), \text{ for all } (x_1, \ldots, x_n) \in \mathbb{F}_2^n.$$

In other words, we can write f as

$$f(X_1, \ldots, X_n) = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{F}_2^n} a_u \cdot X_1^{u_1} \cdots X_n^{u_n}.$$

with coefficients $a_u \in \mathbb{F}_2$.

Example

Problem: Consider the function $f : \mathbb{F}_2^2 \to \mathbb{F}_2$ given by the truth table:

y	0	1	0	1
x	0	0	1	1
$f(x, y)$	1	1	0	1

Compute the ANF.

Algebraic Normal Form (ANF) II

Theorem (Algebraic Normal Form of Boolean Functions)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $(x_1, \dots, x_n) \mapsto (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$, be a vectorial Boolean function in n variables and m coordinates. Then, for every $1 \le i \le m$, each coordinate function $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ can be written as

$$f_i(X_1, \dots, X_n) = \sum_{u=(u_1,\dots,u_n)\in\mathbb{F}_2^n} a_u^{(i)} \cdot X_1^{u_1} \cdots X_n^{u_n},$$

yielding

$$f(X_1, \dots, X_n) = \sum_{u=(u_1,\dots,u_n)\in\mathbb{F}_2^n} \begin{pmatrix} a_u^{(1)} \\ a_u^{(2)} \\ \vdots \\ a_u^{(m)} \end{pmatrix} \cdot X_1^{u_1} \cdots X_n^{u_n}.$$

with coefficients $a_u^{(i)} \in \mathbb{F}_2$.

Algebraic Degree

The next definition is important because it formalises a property of boolean functions that is used in cryptanalysis (more later).

Definition

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial boolean function and

$$f(X_1, \ldots, X_n) = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{F}_2^n} a_u \cdot X_1^{u_1} \cdots X_n^{u_n}.$$

the corresponding ANF with coefficients $a_u \mathbb{F}_2^m$. The multivariate degree (sometimes total degree or just degree) of f is also called the algebraic degree of f and denoted by $\delta(f)$; in other words

$$\delta := \delta(f) = \max\{u_1 + \cdots + u_n : u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n \text{ with } a_u \neq 0\}.$$

Möbius Transform

Question: Other ways to compute the ANF?

Answer: Indeed. Let's cast it into the following

Proposition (Binary Möbius Transform)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function and

$$f(X_1, \ldots, X_n) = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{F}_2^n} a_u \cdot X_1^{u_1} \cdots X_n^{u_n}.$$

be the ANF with coefficients $a_u \in \mathbb{F}_2$. Then we have the following relation between evaluations $f(x)$ of f and coefficients a_u of the ANF ($x, u \in \mathbb{F}_2^n$):

$$a_u = \sum_{x\in\mathbb{F}_2^n,\, x\preceq u} f(x) \quad \text{and} \quad f(x) = \sum_{u\in\mathbb{F}_2^n,\, u\preceq x} a_u,$$

where $u = (u_1, \ldots, u_n) \preceq (v_1, \ldots, v_n) = v$ if and only if $u_i \leq v_i$ for all $1 \leq i \leq n$.

Example

Problem: Consider the boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ given by the truth table:

x_3	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_1	0	0	0	0	1	1	1	1
$f(x_1, x_2, x_3)$	0	1	0	0	0	1	1	1

Compute the ANF using the Möbius transform.

Cryptanalysis of Boolean Functions

Boolean Functions and Block Ciphers

Nota Bene: An important criterion for boolean functions used in block ciphers is the algebraic degree.

Question: Why?

Answer: The algebraic degree is one measure of the "algebraic complexity" of a boolean function. Another measure is the number of non-vanishing monomials in its ANF (sometimes called weight).

Rule of Thumb: We can state

"Security against algebraic attacks $\Rightarrow$ High algebraic degree + High weight"

Disclaimer: High algebraic degree and high weight might not be sufficient for security against algebraic attacks (see e.g. an attack on the block cipher proposal JARVIS[1])

[1] https://eprint.iacr.org/2019/419

Primer on Higher-Order Differential Cryptanalysis

Starting point: A boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, e.g. describing (part of) a cryptographic primitive.

Assumptions

- We know the algebraic degree δ of f and it holds $\delta \ll n$.
- We know how to “differentiate” functions on $\mathbb{F}_2^n$.

Idea: Since f can be written as a polynomial, the $(\delta + 1)$-th order derivative of f is zero.

Consequences: By taking the $(\delta + 1)$ order derivative we can distinguish f from randomly sampled values. This allows us to build a zero-sum distinguisher, with which we potentially can set up a key-recovery attack for some of the key bits.

Spoiler: In practice, we don’t know the algebraic degree of a real-world cipher!

Mathematics of Higher-Order Differential Cryptanalysis I

We need: A notion of derivation on $\mathbb{F}_2^n$!

Remember: In calculus, the derivative of a function $f : \mathbb{R} \to \mathbb{R}$ at the point $x \in \mathbb{R}$ is defined as

$$\partial f(x) := \lim_{a \to 0} \frac{f(x+a) - f(x)}{a},$$

presuming the limit exists at all.

Transfer to finite fields: Discard the limit-part of the definition and just keep the difference-part!

Definition

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2, x = (x_1, \ldots, x_n) \mapsto f(x)$, be a boolean function. The (first-order) derivative of f in direction of $a \in \mathbb{F}_2^n$ at the point $x \in \mathbb{F}_2^n$ is defined as

$$\Delta_a f(x) := f(x+a) + f(x).$$

Mathematics of Higher-Order Differential Cryptanalysis II

The main reason for introducing above notion of derivation is made explicit in the following

Proposition (Derivation Strictly Reduces the Algebraic Degree)

Let $h : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function. Then, for any $a \in \mathbb{F}_2^n$ it holds

$$\delta(\Delta_a h) \leq \delta(h) - 1.$$

Lemma (Properties of Δ_a)

- $\Delta_a(f + g) = \Delta_a f + \Delta_a g$ ("homomorphic with respect to addition"),
- $\Delta_a(f \cdot g)(x) = f(x + a) \cdot \Delta_a g(x) + \Delta_a f(x) \cdot g(x)$, for $x \in \mathbb{F}_2^n$ ("Almost Leibniz").

Mathematics of Higher-Order Differential Cryptanalysis III

With these properties of Δ_a at hand, the proof of the aforementioned proposition becomes a lot more pleasant.

Proof sketch (for Propostion "Derivation Strictly Reduces the Algebraic Degree")

Because of Δ_a being homomorphic with respect to addition, it suffices to consider only one monomial $X_1, \ldots, X_k$ of the ANF of h. We proof this special case by induction. For $k = 1$, we get for any $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$

$$\Delta_a X_1 = (X_1 + a_1) + X_1 = a_1.$$

The induction step from $k - 1$ to k. "Almost Leibniz" yields

$$\Delta_a(\underbrace{X_1 X_2 \cdots X_{k-1}}_{=:f}\,\underbrace{X_k}_{=:g}) = \underbrace{(X_1 + a_1)\cdots(X_{k-1} + a_{k-1})}_{=f(x+a)}\;\underbrace{a_k}_{=\Delta_a g} + \underbrace{\Delta_a(X_1 \cdots X_{k-1})}_{=\Delta_a f}\,\underbrace{X_k}_{=g}.$$

Now we apply the induction hypothesis.

Recap

Let's reflect on the goals from the beginning of this lecture.

- Discuss **different representations** of boolean functions $\longrightarrow$ Multivariate, univariate polynomial representation
- Outline a basic concept of **cryptanalysis** on boolean functions $\longrightarrow$ Higher-order differential cryptanalysis

Many more aspects of boolean functions, especially in the context of stream ciphers and linear/differential cryptanalysis. **Standard readings** on boolean functions:

- Anne Canteaut, *Lecture Notes on Cryptographic Boolean Functions*,
- Claude Carlet, *Boolean Functions for Cryptography and Error Correcting Codes* and *Vectorial Boolean Functions for Cryptography*.

Questions?

Questions for Self-Control

1. What is a (vectorial) boolean function?
2. Discuss polynomial representations of boolean functions. Why is it possible to represent boolean functions as polynomials after all?
3. How is the Möbius transform connected to the ANF of a boolean function?
4. What is the algebraic degree and why is it important in cryptography?
5. Outline the basic idea of higher-order differential cryptanalysis and describe the involved notion of derivation.