Introduction

What is a pseudorandom sequence?

Boolean

Functions

GF(2) Boolean

Functions Discrete Fouri

> ransiorms Sent Functions

2 adic intere

Sequences

Shift Register

Breaking a Stream Cipher

Pseudorandom Sequences of

Analyzing

Conclusion

Analysis of Pseudorandom Sequences

Charles Celerier

March 29, 2012

Introduction
What is a
pseudorandom
sequence?
Stream Cipher

Boolean Function

Boolean Functions Discrete Fourie Transforms

2 adic interes

Boolean

Shift Register
Breaking a

Pseudorandom Sequences of 0s and 1s

Analyzing Constructing

Conclusion

1 Introduction

What is a pseudorandom sequence? Stream Ciphers

2 Boolean Functions

GF(2)

Boolean Functions

Discrete Fourier Transforms

Bent Functions

3 2-adic integers

4 Boolean Sequences

5 Shift Registers
Breaking a Stream Cipher

6 Pseudorandom Sequences of 0s and 1s

Analyzing Constructing

Conclusion

What is a pseudorandom sequence?

Stream Ciph

Boolean

Function

GF(2)

Functions
Discrete Four

Discrete Fourie Transforms

Bent Functions

2-adic intege

Boolean

Shift Register

Breaking a Stream Cipher

Pseudorandom Sequences of

Analyzing

Conclusion

What is a pseudorandom sequence?

- uniform distribution
- low auto-correlation

Introduction

What is a pseudorandom

Stream Ciphers

_ .

Doolean

Function

CE(2)

Boolean

Functions

Discrete Fo

Transforms

Dent Function

2-adic intege

_ .

Sequence

Shift Registe

Breaking a Stream Cipher

Pseudorandom Sequences of

Analyzing

Constructin

Conclusion

Stream Ciphers

0100111001000011010101010101010 = NCUR

Introduction

What is a pseudorandom

Stream Ciphers

.

Eunction

Function

CE(O)

Boolean

Functions Discrete Four \oplus

Transforms

Bent Function

2-adic intege

Б. 1

Sequence

Shift Registe

Breaking a

Pseudorandon Sequences of

Sequences of 0s and 1s

Analyzing Constructin

Conclusion

Stream Ciphers

0100111001000011010101010101010 = NCUR 00000101000010010001100100000010



Introduction

What is a pseudorandom

Stream Ciphers

Boolean

Function

GF(2)

Boolean Function

Discrete Fouri Transforms

Bent Function

2-adic integer

Daalaan

Sequence

Shift Registe

Breaking a Stream Cipher

Pseudorandon Sequences of

Analyzing

Conclusion

Stream Ciphers

01001110010000110101010101010 = NCUR ⊕ 00000101000010010001100100000010 01001011010010100100110001010000 = KJLP



Stream Ciphers

Boolean

Functio

Boolean Functions

Discrete Fourier Transforms Bent Functions

Dent Function

Boolean

Sequence

Shift Register

Breaking a Stream Cipher

Pseudorandon Sequences of

Analyzing Constructin

Conclusion

Why use stream ciphers?

- fast
- easy to implement with hardware
- plaintext length is not always known
- near one-time-pad security

What is a

Stream Ciphers

Breaking a

- Boolean functions
- 2-adic integers
- pseudorandom sequences
- shift registers

Introduction

What is a pseudorandom sequence?

Boolean

Function

GF(2)

Boolean

Functions Discrete Fo

Bent Functions

Sequence

Shift Registe

Breaking a

Pseudorandon

Os and 1s

Analyzing Constructin

Conclusion

\mathbb{F}_2 or "GF two"

| XOR | AND |
|-------------------|------------------|
| $0 \oplus 0 := 0$ | $0 \cdot 0 := 0$ |
| $0\oplus1:=1$ | $0 \cdot 1 := 0$ |
| $1\oplus0:=1$ | $1 \cdot 0 := 0$ |
| $1\oplus1:=0$ | $1 \cdot 1 := 1$ |

Table: Binary Operations for \mathbb{F}_2

Pseudorando

Sequences of 0s and 1s

Analyzing Constructin

Conclusion

\mathbb{F}_2^n or "GF two to the n"

Example

Let $a,b\in\mathbb{F}_2^3$ such that a=(1,0,1) and b=(0,1,1) then

$$a + b = (1 \oplus 0, 0 \oplus 1, 1 \oplus 1) = (1, 1, 0)$$

 $a \cdot b = 1 \cdot 0 \oplus 0 \cdot 1 \oplus 1 \cdot 1 = 1$

Fact

 \mathbb{F}_2^n is a vector space.

Properties of $x \in \mathbb{F}_2^n$

Definition

Let $x, y \in \mathbb{F}_2^n$. Then $wt : \mathbb{F}_2^n \to \mathbb{N} \cup \{0\}$ is defined by

$$wt(x) := \sum_{i=0}^{n-1} x_i$$

and $d: \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{N} \cup \{0\}$ is defined by

$$d(x,y) := w(x+y).$$

Then wt(x) is the Hamming weight of x and d(x, y) is the Hamming distance between x and y.

Some examples

Example

Let $a, b, c \in \mathbb{F}_2^5$ such that

$$a = (0, 1, 1, 0, 1), b = (1, 1, 1, 0, 0), and c = (0, 0, 1, 1, 0).$$

Then.

$$wt(a) = 3$$
 $d(a, b) = 2$

$$wt(b) = 3$$
 $d(a, c) = 3$

$$wt(c) = 2$$
 $d(b, c) = 3$.

Pseudorandor Sequences of

Analyzing Constructin

Conclusion

Boolean functions in \mathcal{BF}^n

Definition

Any function f defined such that

$$f: \mathbb{F}_2^n \to \mathbb{F}_2$$

is a *Boolean function*. The set of all Boolean functions on n variables will be denoted by \mathcal{BF}_n .

What is a pseudorandom

Boolean

Functions

Breaking a

Example

Let $f = x_0 + x_1$.

| <i>x</i> ₀ | <i>x</i> ₁ | $f(x_0,x_1)$ |
|-----------------------|-----------------------|--------------|
| 0 | 0 | 0 |
| 1 | 0 | 1 1 |
| 0 | 1 | 1 1 |
| 1 | 1 | 0 |

Table: Truth Table of f

What is a pseudorandor sequence? Stream Ciphe

Boolear Functio

GF(2)

Functions
Discrete Fourier

Transforms
Bent Functions

Bent Function

Boolean

Sequence

Shift Registers
Breaking a

Pseudorando Sequences o

Analyzing Constructin

Conclusion

Definition

A character χ of a finite abelian group G is a group homomorphism from G into a multiplicative group of complex numbers.

Fact

 $\chi_{\lambda}(x) := (-1)^{\lambda \cdot x}$ where $\lambda, x \in \mathbb{F}_2^n$ is a group character of \mathbb{F}_2^n .

Boolea

FUNCTIO

Boolea

Punctions
Discrete Fourier

Transforms
Bent Functions

2-adic integ

Boolean Sequence

Shift Register

Pseudorandom Sequences of

Analyzing Constructing

Conclusion

Discrete Fourier Transform

Definition

The discrete Fourier transform or DFT of a Boolean function is defined by

$$\mathcal{F}f(\lambda) = \sum_{x \in \mathbb{F}_2^n} f(x) \chi_{\lambda}(x) \tag{1}$$

Shift Registers

Pseudorando Seguences o

Analyzing Construction

Conclusion

Pseudo Boolean Functions

Definition

$$\hat{f}(x) := (-1)^{f(x)}$$
 and $\hat{\mathcal{BF}} = \{\hat{f} : f \in \mathcal{BF}\}.$

Lemma

The characters of \mathbb{F}_2^n are functions in $\hat{\mathcal{BF}}_n = \{\hat{f} : f \in \mathcal{BF}_n\}$ and form an orthonormal basis of that set.

Introduction

What is a pseudorandom sequence?
Stream Cipher

Functions Functions

GF(2)

Boolean

Discrete Fourier Transforms

Bent Functions

2-adic intege

Daalaaa

Sequence

Shift Register

Stream Ciphe

Pseudorandon Sequences of

0s and 1s

Analyzing Constructing

Conclusion

Lemma

$$\hat{f}(x) = \frac{1}{2^{n/2}} \sum_{\lambda \in \mathbb{F}_2^n} c(\lambda) \chi_{\lambda}(x)$$
 (2)

where $c(\lambda)$, the Fourier coefficients of $\hat{f}(x)$ are given by

$$c(\lambda) = \frac{1}{2^{n/2}} \mathcal{F}\hat{f}(\lambda). \tag{3}$$

Introduction

What is a pseudorandon sequence?

Boolean

Funct

GF(2) Boole

Functions
Discrete Fouri

Bent Functions

Boolean

Sequence

Shift Register

Pseudorando Sequences o

Analyzing Construction

Conclusion

Rothaus' Definition and First Theorem

Definition

If all of the Fourier coefficients of \hat{f} are ± 1 then f is a *bent function*.

Theorem

If f is a bent function on \mathbb{F}_2^n , then n is even, n=2k; the degree of f is at most k, except in the case k=1.

Rent Functions

Breaking a

Properties of Bent Functions

- 1. perfectly non-linear
- 2. nearly balanced
- derivative is balanced.

What is a

pseudorandom

2-adic integers

Breaking a

What happens when we write positive integers with infinitely many digits?

Introduction
What is a

pseudorandon sequence? Stream Ciphe

Boolean

Function

GF(2)

Functions
Discrete Four

Transforms

Bent Functions

2-adic integers

Boolean Sequences

Shift Registers Breaking a

Pseudorandom Sequences of

Analyzing Construction

Conclusion

What happens when we write positive integers with infinitely many digits?

You get elements of N-adic integer rings!

2-adic integers

$$1=1000\cdots$$

$$2=0100\cdots$$

$$3=1100\cdots$$

$$-1 = 1111 \cdots$$

$$1/3 = 1101010101 \cdots$$

$$-1/3 = 1010101010 \cdots$$

I am intentionally skipping the details of how to construct rational numbers such as 1/3. It is only important to know that as long as the denominator is not divisble by 2, it can be done.

Introduction

What is a pseudorandon sequence?
Stream Ciphe

Boolea

Functi

Boolean Functions Discrete Fourie

Transforms Bent Functions

2-adic integers

Boolean

Shift Registe

Breaking a Stream Cipher

Pseudorandor Sequences of

Sequences of 0s and 1s

Analyzing Construction

Conclusion

Definition

Let $\alpha=(a_n)\in\mathbb{Z}_2\setminus(0)$. If m is the smallest number in $\mathbb{N}\cup\{0\}$ such that $a_m\not\equiv 0\pmod 2^{m+1}$, then the 2-adic valuation of α is m, or $\log_2(\alpha)=m$. If $\alpha=0$, thensess $\log_2(\alpha)=\infty$.

Example

Let $\alpha = 00010111011111\cdots$. Then $\log_2(\alpha) = 3$.

Boolean

GF(2)

Boolean Functions Discrete Four

Discrete Fourie Transforms Bent Function

0 - 41 - 1 - 4 - - -

Boolean Sequences

Shift Registers
Breaking a

Pseudorandor Sequences of

Analyzing Constructing

Conclusion

Boolean Sequences

Definition

Let (a_n) be a sequence. If T is the smallest integer such that $a_i = a_{i+T}$, then the *minimal period* of (a_n) is T.

Definition

Let $f \in \mathcal{BF}_n$ and $v_i \in \mathbb{F}_2^n$ such that $v_i = B^{-1}(i)$ for $0 \le i < 2^n$. Then,

$$seq(f) = (f(v_0), f(v_1), \dots, f(v_{2^n-1}), f(v_0), \dots)$$
 (4)

is a lexicographical Boolean sequence.

Analyzing Constructing

Conclusion

2-adic Expansion

Definition

Let $f \in \mathcal{BF}_n$ and $v_i \in \mathbb{F}_2^n$ such that $v_i = B^{-1}(i)$ for $0 \le i < 2^n$. Then,

$$\alpha_f = (f(v_0), f(v_0) + f(v_1) \cdot 2, \cdots, f(v_0) + \cdots + f(v_i) \cdot 2^i, \cdots)$$
 (5)

where $\alpha_f \in \mathbb{Z}_2$ is called the 2-adic expansion of f.

Lemma

The digit representation of α_f is seq(f).

Boolean

Functions

Functions

Boolean

Discrete For

Bent Function

2-adic integer

Daalaaa

Sequence

Shift Registers
Breaking a

Stream Cipher

Pseudorando Sequences of

Analyzing

C..........

LFSR

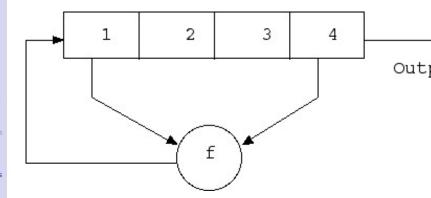


Figure: Linear Feedback Shift Register from Google Images

Boolean

Funct

GF(2) Boolea

Discrete Fourier Transforms

Bent Functions

Boolean

Sequence

Shift Registers

Pseudorando

Sequences of 0s and 1s

Analyzing Constructin

Conclusion

Eventually periodic shift registers

Solomon W. Golomb wrote the famous book *Shift Register Sequences* in 1967 which contain numerous elementary facts about finite state machines.

Theorem

If the input sequence to a finite state machine is eventually periodic, then the output sequence is eventually periodic.

Introduction

pseudorandor sequence? Stream Ciphe

Boolea

Funct

GF(2

Functions
Discrete Fourie
Transforms

Transforms Bent Functions

2-adic intege

Boolean Sequences

Shift Registers

Breaking a Stream Cipher

Pseudorando Seguences o

Analyzing

Conclusion

Breaking a Stream Cipher

Kerckhoffs' principle: "In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used."

Typically, breaking a stream cipher will mean recovering the state of the shift register at a given time.

Analysis of Pseudorandom Sequences

> Charles Celerier

Introduction

What is a pseudorandom sequence?

Boolean

Functions

Function

Boolean

Functions Discrete Fou

Bent Function

z daic integer

Sequence

Sequence

Breaking a Stream Cipher

Pseudorando Sequences of

Analyzing

Conclusion

State of the register

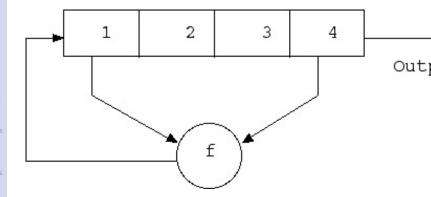


Figure: Linear Feedback Shift Register from Google Images

Two Methods

Charles Celerier

What is a

pseudorandom

Boolean

Breaking a

Analyzing

1. 2-adic integers

2. Boolean sequences

What is a pseudorandom sequence?

Boolean Functions

GF(2) Boolean

Discrete Fourie

Bent Functions

_ aaic iiicg

Boolean Sequences

Shift Registers
Breaking a
Stream Cipher

Pseudorandom Sequences of 0s and 1s

Analyzing Constructing

Conclusion

Maiorana-McFarland Class Boolean Functions

A simple bent function construction is accomplished by the Boolean functions in the *Maiorana-McFarland class*. This is the the set \mathcal{M} which contains all Boolean functions on $\mathbb{F}_2^n = \{(x,y) : x,y \in \mathbb{F}_2^{n/2}\}$, of the form:

$$f(x,y) = x \cdot \pi(y) \oplus g(y)$$

where π is any permutation on $\mathbb{F}_2^{n/2}$ and g any Boolean function on $\mathbb{F}_2^{n/2}$.

All functions in the Maiorana-McFarland class of Boolean functions are bent.

Analysis of Pseudorandom Sequences

> Charles Celerier

Introduction

pseudorandom sequence? Stream Cipher

Boolean

Function

GF(2)

Functions
Discrete Fourie
Transforms

Bent Functions

2-adic in

Boolean

Shift Registe

Breaking a Stream Cipher

Pseudorandon Sequences of Os and 1s

Analyzing Constructing

Conclusion

Using Bent functions for Boolean Sequences

Theorem

The lexicographical Boolean sequence of a Bent function has a period exactly 2^n .

Introduction

What is a pseudorandon sequence? Stream Ciphe

Boolea

GE(2)

GF(2) Boolea

Functions
Discrete Fourie
Transforms

Transforms Bent Function

2 adic intere

Boolean Sequence

Shift Registers

Pseudorando Sequences of

Analyzing Constructing

Conclusion

Consider the subset of Maiorana-McFarland class Boolean functions where g(y)=0. $\bar{\pi}$ will be the function which specifies where each index moves to under the permutation π .

Theorem

$$\log_2(\alpha_{x \cdot \pi(y)}) = 2^{n/2} + 2^{\bar{\pi}(y_0)}$$

The 2-adic valuation of the Boolean sequence of the functions in this subset is entirely dependent on the permutation π .

Conclusion

Conclusion

- Pseudorandom sequences
- Stream Ciphers
- Analysis using Boolean functions and 2-adic integers
- Connections between Bent function and 2-adic valuation

What is a pseudorandom

Boolean

Breaking a Stream Cipher

Analyzing

Conclusion

Questions?

