Bent Sequences and Feedback with Carry Shift Registers

Charles Celerier

SASMC 2012

What is a pseudorandom sequence?

What is a pseudorandom sequence?

R1. uniform distribution

$$|\sum_{n=1}^{p}(-1)^{a_n}| \le 1$$

What is a pseudorandom sequence?

R1. uniform distribution

$$\left|\sum_{n=1}^{p}(-1)^{a_n}\right| \leq 1$$

R2.

$$\frac{1}{2^i} \text{ of the runs have length } i$$

What is a pseudorandom sequence?

R1. uniform distribution

$$|\sum_{n=1}^{p}(-1)^{a_n}| \leq 1$$

R2.

$$\frac{1}{2^i} \text{ of the runs have length } i$$

R3. low auto-correlation,

$$C(\tau) = \frac{\sum_{n=1}^{p}(-1)^{a_n + a_{n+\tau}}}{p}$$

Examples

Example

$$a = [0, 0, 0, 1, 0, 1, 1]$$

Examples

Example

$$a = [0, 0, 0, 1, 0, 1, 1]$$

R1. true.

$$\sum_{n=1}^{7} (-1)^{a_n} = 1$$

Examples

Example

$$a = [0, 0, 0, 1, 0, 1, 1]$$

R1. true.

$$\sum_{n=1}^{7} (-1)^{a_n} = 1$$

R2. true.

Examples

Example

$$a = [0, 0, 0, 1, 0, 1, 1]$$

R1. true.

$$\sum_{n=1}^{7} (-1)^{a_n} = 1$$

R2. true.

R3. true.

$$C(\tau) = \frac{\sum_{n=1}^{7} (-1)^{a_n + a_{n+\tau}}}{7} = \frac{-1}{7}$$

Stream Ciphers

Stream Ciphers

$$0101001101000001010100110100110101000011 \quad = \quad \text{SASMC}$$

Stream Ciphers

$$
\begin{array}{rlcl}
 & 0101001101000001010100110100110101000011 & = & \text{SASMC} \\
\oplus & 0001100000001011000111110001110100010010 & & \\
\hline
\end{array}
$$

Stream Ciphers

$$
\begin{array}{rlcc}
 & 0101001101000001010100110100110101000011 & = & \mathsf{SASMC} \\
\oplus & 0001100000001011000111110001110100010010 & & \\
\hline
 & 0100101101001010010011000101000001010001 & = & \mathsf{KJLPQ}
\end{array}
$$

Why use stream ciphers?

Why use stream ciphers?

- plaintext length is not always known

Why use stream ciphers?

- plaintext length is not always known
- fast

Why use stream ciphers?

- plaintext length is not always known
- fast
- easy to implement with hardware

Why use stream ciphers?

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

Topics

- Boolean functions
- Feedback with Carry Shift Registers
- 2-adic integers
- Bent Sequences

$\mathbb{F}_2$ or "GF two"

XOR	AND
$0 \oplus 0 := 0$	$0 \cdot 0 := 0$
$0 \oplus 1 := 1$	$0 \cdot 1 := 0$
$1 \oplus 0 := 1$	$1 \cdot 0 := 0$
$1 \oplus 1 := 0$	$1 \cdot 1 := 1$

Table: Binary Operations for $\mathbb{F}_2$

$\mathbb{F}_2^n$ 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 $wt : \mathbb{F}_2^n \to \{0, \cdots, n\}$ is defined by

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

and $d : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{N} \cup \{0, \cdots, n\}$ 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

$$a = (0,1,1,0,1), \; b = (1,1,1,0,0), \text{ and } c = (0,0,1,1,0).$$

Then,

$$\begin{array}{ll} wt(a) = 3 & d(a,b) = 2 \\ wt(b) = 3 & d(a,c) = 3 \\ wt(c) = 2 & d(b,c) = 3. \end{array}$$

Boolean functions in $\mathcal{BF}_n$

Definition

Any function f defined such that

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

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

An example

Example

Let $f = x_0 + x_1$.

x_0	x_1	$f(x_0, x_1)$
0	0	0
1	0	1
0	1	1
1	1	0

Table: Truth Table of f

Characters of $\mathbb{F}_2^n$

Definition

A **character** χ of a finite abelian group G is a group homomorphism from G into the 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* $\mathbb{F}_2^n$.

Walsh Transform

Let the **dual group** $\hat{\mathbb{F}_2^n}$ be the group of all characters of $\mathbb{F}_2^n$.

Walsh Transform

Let the **dual group** $\hat{\mathbb{F}_2^n}$ be the group of all characters of $\mathbb{F}_2^n$.

$$(\chi \cdot \psi)(x) = \chi(x)\psi(x), \; x \in \mathbb{F}_2^n$$

Walsh Transform

Let the **dual group** $\hat{\mathbb{F}}_2^n$ be the group of all characters of $\mathbb{F}_2^n$.

$$(\chi \cdot \psi)(x) = \chi(x)\psi(x), \ x \in \mathbb{F}_2^n$$

$$\mathbb{F}_2^n \cong \hat{\mathbb{F}}_2^n$$

Walsh Transform

Definition

Let $f \in \mathcal{BF}_n$. Then $\hat{f} : \mathbb{F}_2^n \to \{1, -1\}$ such that $\hat{f}(x) = (-1)^{f(x)}$ is a *pseudo-Boolean function*

Example

Let $f = x_0 + x_1$.

x_0	x_1	$f(x_0, x_1)$	$\hat{f}(x_0, x_1)$
0	0	0	1
1	0	1	-1
0	1	1	-1
1	1	0	1

Table: Truth Table of $\hat{f}$

Walsh Transform

Definition

Let $f \in \mathcal{BF}_n$ and $\lambda \in \mathbb{F}_2^n$. Then the *Walsh transform* of f is defined by:

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

Walsh Transform

Lemma

The characters of $\mathbb{F}_2^n$ belong to $\hat{\mathcal{BF}}_n = \{\hat{f} : f \in \mathcal{BF}_n\}$ and form an orthonormal basis of $\hat{\mathcal{BF}}_n \otimes \mathbb{R}$.

Lemma

For $\hat{f} \in \hat{\mathcal{BF}}_n$,

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

where $c(\lambda)$ are given by

$$c(\lambda) = \frac{1}{2^{n/2}} \mathcal{W}_f(\lambda) \tag{3}$$

Call the $c(\lambda)$'s **Fourier coefficients**.

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, $n = 2k$. Moreover, the degree of f is at most k, except in the case $k = 1$.

Properties of Bent Functions

Properties of Bent Functions

(R1) 1. $wt(f) = 2^{n-1} \pm 2^{n/2-1}$

Properties of Bent Functions

(R1) 1. $wt(f) = 2^{n-1} \pm 2^{n/2-1}$

(R2) 2. perfectly non-linear

Properties of Bent Functions

(R1) 1. $wt(f) = 2^{n-1} \pm 2^{n/2-1}$

(R2) 2. perfectly non-linear

(R3) 3. $\sum_{x \in \mathbb{F}_2^n} f(x) + f(x+a) = 0 \quad \forall a \in \mathbb{F}_2^n$

Finite State Machines

Definition

A **finite state machine** consists of a finite collection of **states** K, which sequentially accepts a sequence of **inputs** from a finite set A, and produces a sequence of **outputs** from a finite set B. Moreover, there is an **output function** μ which computes the present output as a fixed function of present input and present state, and a **next state function** δ which computes the next states as a fixed function of present input and present state. In a more mathematical manner, μ and δ are defined such that

$$\mu : K \times A \to B \qquad \mu(k_n, a_n) = b_n \tag{4}$$

$$\delta : K \times A \to K \qquad \delta(k_n, a_n) = k_{n+1} \tag{5}$$

FCSR

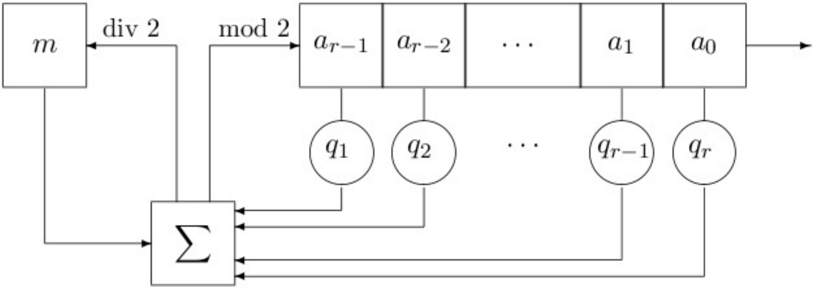
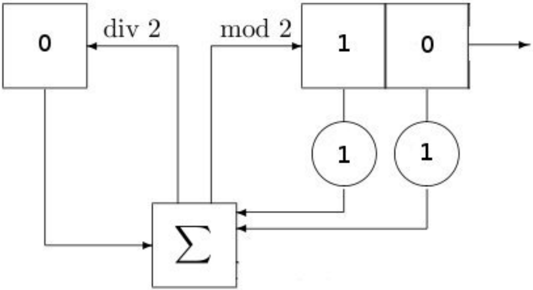
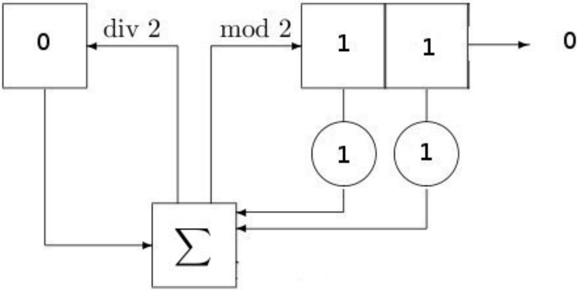


Figure: Feedback with Carry Shift Register

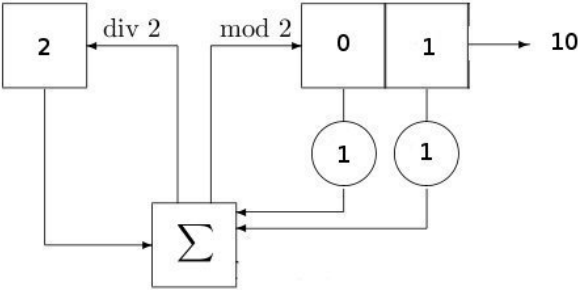
FCSR



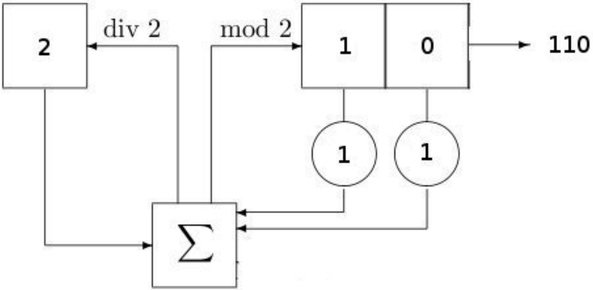
FCSR



FCSR



FCSR



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.

Two Methods

Two Methods

1. 2-adic integers

Two Methods

1. 2-adic integers
2. Boolean sequences

2-adic integers

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

2-adic integers

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

Definition

The infinite integer sequence (x_n) determines a **2-adic integer** α, or $(x_n) \to \alpha$, if

$$x_{i+1} \equiv x_i \pmod{2^{i+1}} \quad \forall i \geq 0. \tag{6}$$

Two sequences (x_n) and (x_n') determine the same 2-adic integer if

$$x_i \equiv x_i' \pmod{2^{i+1}} \quad \forall i \geq 0. \tag{7}$$

The **set of all 2-adic integers** will be denoted by $\mathbb{Z}_2$.

2-adic integers

Example

Let $(x_n) \to \alpha \in \mathbb{Z}_2$. Then the first 5 terms of (x_n) may look something like:

$$\begin{aligned}(x_n) &= (\ 1\ ,\ 1+1\cdot 2\ ,\ 1+1\cdot 2+0\cdot 2^2\ ,\\ &\qquad 1+1\cdot 2+0\cdot 2^2+0\cdot 2^3\ ,\ 1+1\cdot 2+0\cdot 2^2+1\cdot 2^4\ ,\ \dots)\\ &= (1,3,3,3,19,\dots)\end{aligned}$$

Then an equivalent sequence to (x_n) could look entirely different:

$$(y_n) = (19,3,3,19,19,\dots)$$

2-adic integers

$$\begin{aligned}
\alpha &= 11001\cdots \\
1 &= 1000\cdots \\
2 &= 0100\cdots \\
3 &= 1100\cdots \\
-1 &= 1111\cdots \\
1/3 &= 1101010101\cdots \\
-1/3 &= 1010101010\cdots
\end{aligned}$$

2-adic integers

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 $\alpha = 0$, then $\log_2(\alpha) = \infty$.

Example

Let $\alpha = 0001011101111 \cdots$. Then $\log_2(\alpha) = 3$.

Boolean Sequence

Boolean Sequence

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 $0 \leq i < 2^n$. Then,

$$seq(f) = (f(v_0), f(v_1), \cdots, f(v_{2^n-1}), f(v_0), \cdots) \tag{8}$$

is a **lexicographical Boolean sequence**.

Theorem

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

Boolean Sequence

Definition

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

$$\alpha_f = (f(v_0), f(v_0) + f(v_1) \cdot 2, \cdots, f(v_0) + \cdots + f(v_i) \cdot 2^i, \cdots) \quad (9)$$

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

Lemma

The digit representation of α_f is $seq(f)$.

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.

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

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