Pseudorandom Sequences

Charles Celerier

March 28, 2012

Stream Ciphers

$$01001110010000110101010101010010 \quad = \quad \text{NCUR}$$

Stream Ciphers

$$
\begin{array}{cccc}
 & 01001110010000110101010101010010 & = & \text{NCUR} \\
\oplus & 00000101000010010001100100000010 & & \\
\hline
\end{array}
$$

Stream Ciphers

$$
\begin{array}{rccc}
 & 01001110010000110101010101010010 & = & \mathrm{NCUR} \\
\oplus & 00000101000010010001100100000010 & & \\
\hline
 & 01001011010010100100110001010000 & = & \mathrm{KJLP}
\end{array}
$$

Why use stream ciphers?

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

My research

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

$\mathbb{F}_2$ 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 $wt : \mathbb{F}_2^n \to \mathbb{N} \cup \{0\}$ 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

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

Then,

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

Boolean functions in $\mathcal{BF}^n$

Definition

Any function f defined such that

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

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

Discrete Fourier Transform

Definition

$\hat{f}(x) := (-1)^{f(x)}$

Lemma

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

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

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