Kriptografi'de Boole Fonksiyonları

Zülfükar Saygı

Department of Mathematics,
TOBB University of Economics and Technology,
Ankara, Turkey.

1 Şubat 2015

İçerik

Outline

Motivasyon

Boole fonksiyonları birçok simetrik şifreleme sisteminin tasarımında ve güvenlik seviyelerinde kilit rol oynarlar.

Motivasyon

Boole fonksiyonları birçok simetrik şifreleme sisteminin tasarımında ve güvenlik seviyelerinde kilit rol oynarlar.

- Akan Şifreler (Stream Ciphers) (Kombinasyon üreteşleri, Filtre üreteçleri,...)
  - Birçok LFSR çıktısının kombinasyonu alınabilir veya tek bir LFSR nin içeriği filtrelenip tek bit çıktı verilir.
  - Sözde rastgele (pseudo-random) diziler üretilir ve Vernam benzeri şifreleme olarak kullanılır (Vernam: mesaj ile dizi mod 2 de toplanır).

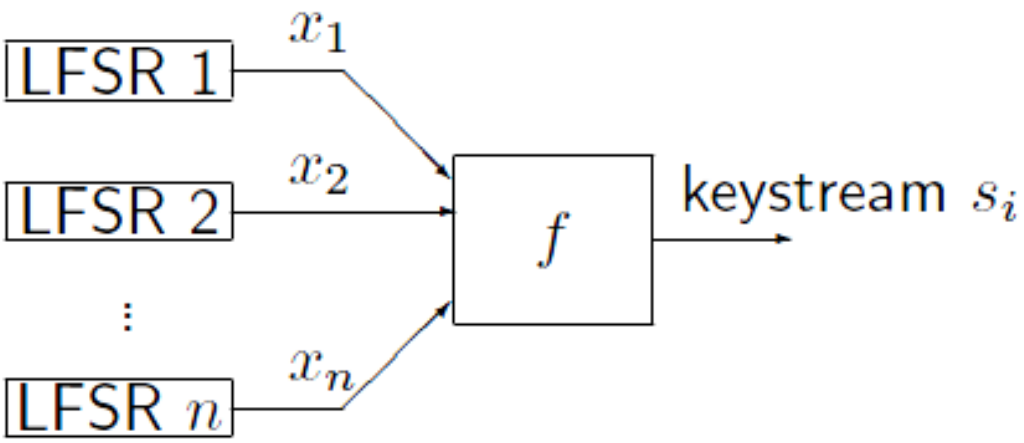
Motivasyon

Boole fonksiyonları birçok simetrik şifreleme sisteminin tasarımında ve güvenlik seviyelerinde kilit rol oynarlar.

- Akan Şifreler (Stream Ciphers) (Kombinasyon üreteşleri, Filtre üreteçleri,...)
  - Birçok LFSR çıktısının kombinasyonu alınabilir veya tek bir LFSR nin içeriği filtrelenip tek bit çıktı verilir.
  - Sözde rastgele (pseudo-random) diziler üretilir ve Vernam benzeri şifreleme olarak kullanılır (Vernam: mesaj ile dizi mod 2 de toplanır).
- Blok Şifreler
  - S-kutuları lineer olmayan Boole fonksiyonları birleştirilerek oluşturulurlar.

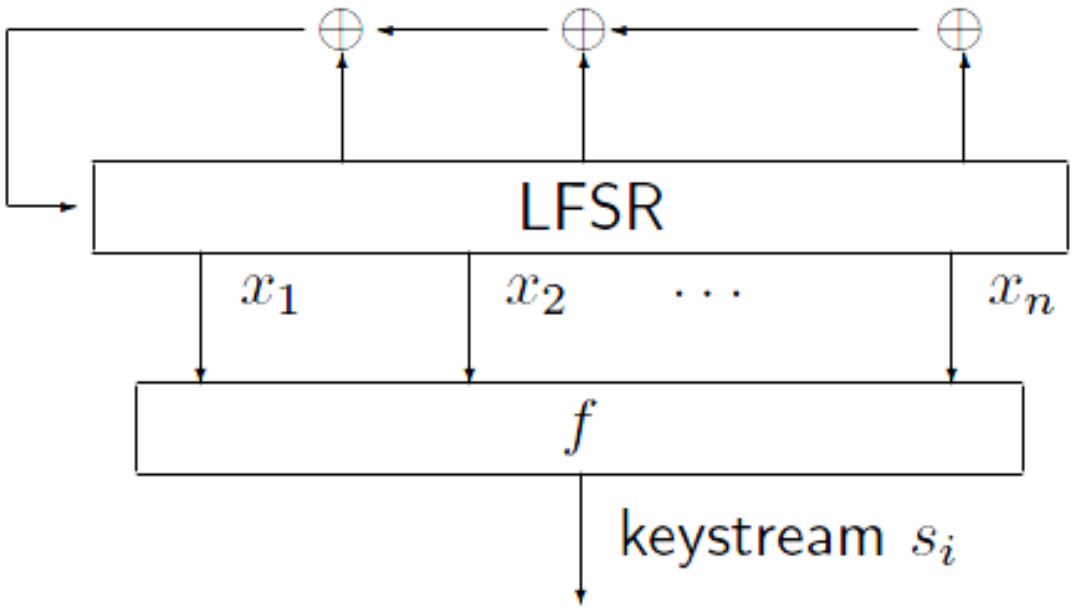
Motivasyon

Combiner model :

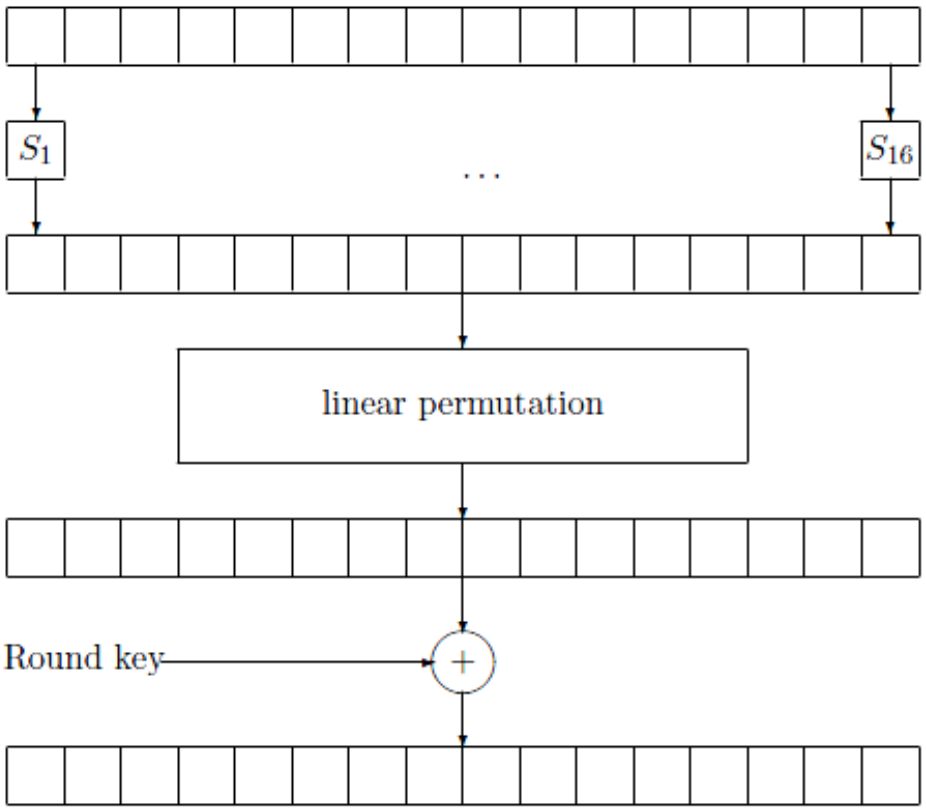


Motivasyon

Filter model



Motivasyon



An AES round

Bazı Gösterimler

- $\mathbb{F}_2 = \{0, 1\} \Rightarrow$ 2 elemanlı sonlu cisim.
- $\mathbb{F}_{2^n} \Rightarrow 2^n$ elemanlı sonlu cisim.
- $\mathbb{F}_2^n \Rightarrow \mathbb{F}_2$ üzerinde n-boyutlu vektör uzayı.
- $BF(n) \Rightarrow \mathbb{F}_2^n$ den $\mathbb{F}_2$ ye tüm Boole fonksiyonları kümesi.
- $w_H(f) = w(f) \Rightarrow f$ nin Hamming ağırlığı,
  - $w(f) = |\{x \in \mathbb{F}_2^n : f(x) \neq 0\}|$.
- $d(f, g) \Rightarrow f$ ile g arasındaki uzaklık,
  - $d(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| = w(f + g)$.

Bir NOT

- Kriptografide kullanılan Boole fonksiyonlarının değişken sayıları genellikle küçük sayılardır.
- İstenilen Kriptografik özelliklere sahip Boole fonksiyonları bütün fonksiyonları tarayarak bulmak çok kolay değildir!
  - $|BF(n)| = 2^{2^n}$ olduğundan $n \geq 6$ için sayılar çok büyür.
  -

n	4	5	6	7	8
$\|BF(n)\|$	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
$\approx$	$6 \cdot 10^4$	$4 \cdot 10^9$	10^{19}	10^{38}	10^{77}

Outline

Cebirsel Normal From (Algebraic Normal Form - ANF)

- $\mathbb{F}_2$ üzerinde n-değişkenli polinom gösterimi
  - $f(x) = \sum_{I \in P(N)} a_I \left(\prod_{i \in I} x_i \right)$
    - $P(N)$: $N = \{1, 2, \ldots, n\}$ nin kuvvet kümesi.
- $N = \{1, 2, 3\} \Rightarrow P(N) =$
  $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
- $f(x) =$
  $a_0 + a_1 x_1 + a_2 x_2 + a_3 x_3 + a_{12} x_1 x_2 + a_{13} x_1 x_3 + a_{23} x_2 x_3 + a_{123} x_1 x_2 x_3$

Cebirsel Normal From (Algebraic Normal Form - ANF)

- Bu gösterim $\mathbb{F}_2[x_1, \ldots, x_n] / \left(x_1^2 + x_1, \ldots, x_n^2 + x_n\right)$ üzerinde tanımlıdır.
- ANF tek türlüdür.
- Divide-and-conquer tipi "'Butterfly"' (Kelebek) algoritması ile hızlı biçimde ANF hesaplanabilir.
  - Doğruluk tablosundan ANF
  - ANF den Doğruluk Tablosu
- ANF nin **derecesi** $deg(f) = max\{|I| : a_I \neq 0\}$ olarak tanımlanır ($|I|$: I nın büyüklüğü).
- $deg(f) = 1$ olan f fonksiyonlarına afin fonksiyonlar denir ($a_0 = 0$ ise afin fonksiyona lineer fonksiyon denir).

ANF örneği

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

ANF örneği

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

$$\Rightarrow f = \underbrace{(1 + x_1)(1 + x_2)x_3} + \underbrace{x_1(1 + x_2)x_3} + \underbrace{x_1x_2x_3} = x_1x_2x_3 + x_2x_3 + x_3$$

ANF örneği

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

$$\Rightarrow f = \underbrace{(1+x_1)(1+x_2)x_3} + \underbrace{x_1(1+x_2)x_3} + \underbrace{x_1x_2x_3} = x_1x_2x_3 + x_2x_3 + x_3$$

- $deg(f) = 3$
- Not: f Boole fonksiyonunun cebirsel derecesi ancak ve ancak $w_H(f)$ tek ise n dir.

Butterfly Algoritması ile ANF

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	1.
0	0	0	0	0
0	0	1	1	$0 + 1 = 1$
0	1	0	0	0
0	1	1	0	$0 + 0 = 0$
1	0	0	0	0
1	0	1	1	$0 + 1 = 1$
1	1	0	0	0
1	1	1	1	$0 + 1 = 1$

Butterfly Algoritması ile ANF

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	1.	2.
0	0	0	0	0	0
0	0	1	1	$0+1=1$	1
0	1	0	0	0	$0+0=0$
0	1	1	0	$0+0=0$	$0+1=1$
1	0	0	0	0	0
1	0	1	1	$0+1=1$	1
1	1	0	0	0	$0+0=0$
1	1	1	1	$0+1=1$	$1+1=0$

Butterfly Algoritması ile ANF

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	1.	2.	3.
0	0	0	0	0	0	0
0	0	1	1	$0+1=1$	1	1
0	1	0	0	0	$0+0=0$	0
0	1	1	0	$0+0=0$	$0+1=1$	1
1	0	0	0	0	0	$0+0=0$
1	0	1	1	$0+1=1$	1	$1+1=0$
1	1	0	0	0	$0+0=0$	$0+0=0$
1	1	1	1	$0+1=1$	$1+1=0$	$1+0=1$

Butterfly Algoritması ile ANF

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	1.	2.	3.
0	0	0	0	0	0	0
0	0	1	1	$0+1=1$	1	1
0	1	0	0	0	$0+0=0$	0
0	1	1	0	$0+0=0$	$0+1=1$	1
1	0	0	0	0	0	$0+0=0$
1	0	1	1	$0+1=1$	1	$1+1=0$
1	1	0	0	0	$0+0=0$	$0+0=0$
1	1	1	1	$0+1=1$	$1+1=0$	$1+0=1$

$\Rightarrow f = x_1x_2x_3 + x_2x_3 + x_3$

- Karmaşıklık (Complexity) $n \cdot 2^n$ XOR operasyonu.

Outline

Tasarım Kriterleri

Seçilen kriptografik sisteme göre özellikler değişir...

- Dengeli (Balanced)
  - Çıktı ile girdi arasında istatistiksel bağımlılık olmamalı
  - Çıktı düzgün dağılmalı

Tasarım Kriterleri

Seçilen kriptografik sisteme göre özellikler değişir...

- Dengeli (Balanced)
  - Çıktı ile girdi arasında istatistiksel bağımlılık olmamalı
  - Çıktı düzgün dağılmalı
- Cebirsel derece yüksek olmalı
  - Akan şifrelerde Berlekamp-Massey atağı.
  - Blok şifrelerde diferansiyel atak.

Tasarım Kriterleri

Seçilen kriptografik sisteme göre özellikler değişir...

- Dengeli (Balanced)
  - Çıktı ile girdi arasında istatistiksel bağımlılık olmamalı
  - Çıktı düzgün dağılmalı
- Cebirsel derece yüksek olmalı
  - Akan şifrelerde Berlekamp-Massey atağı.
  - Blok şifrelerde diferansiyel atak.
- m. dereceden korelasyon-immune
  - girdinin m-biti sabit tutulduğunda çıktının istatistiği dağılımı değişmemeli.
  - m-resilient:= m. dereceden korelasyon-immune + dengeli
  - m yeterince küçük ise Siegenthaler atağı (Akan Şifreler için korelasyon atağı) ve gelişmiş versiyonları (Hızlı Korelasyon Atakları)
  - $m \leq n - 1 - deg(f)$

Tasarım Kriterleri

- f nin çıktısı ile lineer fonksiyonların korelasyonu düşük olmalı.
  - Nonlinearity (N(f)): f ile tüm afin fonksiyonlar arasındaki minimum Hamming uzaklık.
  - Walsh dönüşümü: $W_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}$.

    $\Rightarrow N(f) = 2^{n-1} - \frac{1}{2} max_{\omega \in \mathbb{F}_{2^n}} |W_f(\omega)|$.
  - $N(f) \leq 2^{n-1} - 2^{n/2-1}$. Eşitliğe ulaşan fonksiyonlara **bent** (bükük) fonksiyonlar denir.

Tasarım Kriterleri

- Yayılma (Propagation) Kriteri (PC)
  - Keskin çığ Kriterinin (Strict Avalanche Criterion - SAC) genellemesi.
  - Boole fonksiyonun şifre sistemine kattığı yayılma seviyesini ölçer.
  - Blok Şifre sistemleri ile alakalıdır.
  - f nin $PC(l)$ olması $w_H(a) \leq l$ olan $\forall a$ için $D_a f(x) = f(x) + f(x+a)$ nın dengeli olmasıdır.
    - SAC $\equiv PC(1)$
    - Bent fonksiyonlar $PC(n)$ dir.

Tasarım Kriterleri

- Cebirsel immunity ($AI(f)$)
  - $fg = 0$ yapan g fonksiyonuna f nin *annihilator*'ı denir.
  - $AI(f)$: f veya $f + 1$ fonksiyonlarının sıfırdan farklı annihilatorlarının minimum derecesidir.
  - $AI(f) \leq deg(f)$ ve $AI(f) \leq \lceil \frac{n}{2} \rceil$
  - Pratik uygulamalarda $AI(f) \geq 7$ olmalıdır. Dolayısıyla $n \geq 13$ ve $n \approx 20$ olmalı.
  - Aksi halde cebirsel atak yapmak mümkün olabilir!

Polinom gösterimi

- Not: $\mathbb{F}_2^n \cong \mathbb{F}_{2^n}$.
- $\mathbb{F}_{2^n}$ den $\mathbb{F}_{2^n}$ ye her fonksiyon (Vectörel Boole Fonksiyon)

$$f(x) = \sum_{i=0}^{2^n-1} c_i x^i \quad c_i, x \in \mathbb{F}_{2^n}$$

şeklinde tek türlü gösterime sahiptir.

- f Boole fonksiyondur $\Leftrightarrow (f(x))^2 = f(x) \bmod x^{2^n} + x$, yani, $c_0, c_{2^n-1} \in \mathbb{F}_2$ ve $c_{2j} = (c_j)^2$ (2j mod $2^n - 1$).

Trace gösterimi

- $\mathbb{F}_{2^n}$ den $\mathbb{F}_2$ ye Trace fonksiyonu: :
  $Tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$
- Tüm Boole fonksiyonlar aşağıdaki gibi gösterilebilir:

$$Tr\left(\sum_{i=0}^{2^n-1} c_i x^i\right) \quad c_i, x \in \mathbb{F}_{2^n},$$

fakat gösterim tek türlü değil!

Monomial Bent Fonksiyonlar

Definition

Monomial f fonlsiyon: $f(x) = Tr(ax^s)$, $\forall x \in \mathbb{F}_{2^n}$.

- f nin bent olması için aşağıdakiler sağlanmalı:
  - $gcd(s, 2^n - 1) \neq 1$.
  - either $gcd(s, 2^{n/2} + 1) = 1$ or $gcd(s, 2^{n/2} - 1) = 1$.

Definition

$s > 0$ için $Tr_1^n(ax^s)$ bent olacak şekilde bir $\exists a \in \mathbb{F}_{2^n}^*$ varsa s ye *bent kuvveti* denir.

Bent Kuvvetler

Table : Bilinen tüm bent kuvvetler, s

s	**Kısıt**
$2^i + 1$	$\frac{n}{gcd(n,i)}$ çift, $1 \leq i \leq \frac{n}{2}$
$r \cdot (2^{n/2} - 1)$	$gcd(r, 2^{n/2} + 1) = 1$
$2^{2i} - 2^i + 1$	$gcd(n, i) = 1$
$(2^{n/4} + 1)^2$	$n = 4r$, r tek
$2^{n/3} + 2^{n/6} + 1$	$n = 0 \ mod \ 6$

Referanslar

[1] C. Carlet "Boolean Functions for Cryptography and Error Correcting Codes", Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 257-397, 2010.

[2] C. Carlet, "Vectorial Boolean Functions for Cryptography". Idem, pp. 398-469, 2010.

[3] Henk C. A. Van Tilborg, Sushil Jajodia (editors) "Encyclopedia of Cryptography and Security", 2nd Edition - Springer 2011.