TOBB Ekonomi ve Teknoloji Üniversitesi

MAT 421 - Şifreleme Bilimine Giriş

Ödev III

Teslim tarihi: 3 Nisan (final sınavına getiriniz), 2015

Problem 1

$f(x_1, x_2, x_3, x_4) = x_1 + x_2x_3 + x_1x_4$ Boole fonksiyonu olsun.

a) f nin doğruluk tablosunu bulunuz.

b) f nin nonlineerliğini bulunuz. (N_f).

c) f nin $x_1 + x_2$ fonksiyonuna olan uzaklığını bulunuz.

d) f SAC özelliğini sağlar mı?

Problem 2

f fonksiyonunun doğruluk tablosu $T_f = (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$ olarak verilmiştir.

a) f nin cebirsel normal formunu bulunuz (ANF).

b) f nin derecesini ve ağırlığını bulunuz.

c) f nin nonlineerliğini bulunuz (N_f).

d) f nin $x_1 + x_3 + x_4$ fonksiyonuna olan uzaklığını bulunuz.

e) f $PC(1)$ özelliğini sağlar mı?

Problem 3

f fonksiyonunun doğruluk tablosu $T_f = (0, 1, 0, 0, 0, 0, 1, 1)$ olarak verilmiştir.

a) f nin cebirsel normal formunu bulunuz (ANF).

b) f nin derecesini ve ağırlığını bulunuz.

c) f nin nonlineerliğini bulunuz (N_f).

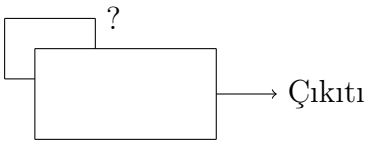
Problem 4

$f : \mathbb{F}_2^n$ den $\mathbb{F}_2$ ye dengeli bir fonksiyon ise nonlineerliği en fazla kaç olabilir?

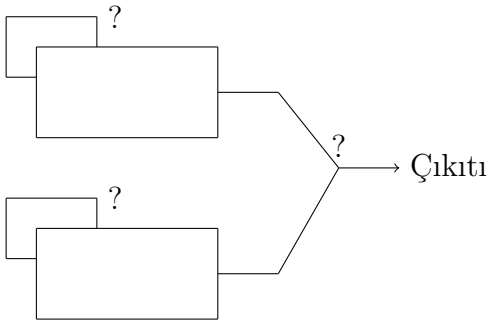
Problem 5

$f_1(x_1, x_2) = x_1 + x_2, f_2(x_1, x_2, x_3) = x_1 + x_3$ ve $f_3(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$ fonksiyonları kullanılarak aşağıdaki kısıtlara uygun bir akan şife sistemi tasarlanmak istenmektedir.

a) Sadece bir LFSR kullanılırsa sistemin periyodu en fazla kaç olur? Neden? (Sayısal Örnek Verilebilir).



b) İki LFSR kombine edilerek kullanılırsa sistemin periyodu kaç olur? Neden? (Sayısal Örnek Verilebilir).



Problem 6

Sıkıştırma fonksiyonlarının özelliklerini ve kullanım amaçlarını kısaca açıklayınız.

Problem 7

SHA-3 algoritmasının detaylarını araştırınız.