

# ABSTRACT

## ALGEBRAIC PROPERTIES OF THE OPERATIONS USED IN BLOCK CIPHER IDEA

Yıldırım, Hamdi Murat

Ph.D., Department of Mathematics

Supervisor: Prof. Dr. Ersan Akyıldız

March 2007, 68 pages

In this thesis we obtain several interesting algebraic properties of the operations used in the block cipher IDEA which are important for cryptographic analyzes. We view each of these operations as a function from  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ . By fixing one of variables  $v(z) = \mathbf{Z}$  in  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ , we define functions  $\mathbf{f}_z$  and  $\mathbf{g}_z$  from  $\mathbb{Z}_2^n$  to  $\mathbb{Z}_2^n$  for the addition  $\boxplus$  and the multiplication  $\odot$  operations, respectively. We first show that the nonlinearity of  $\mathbf{g}_z$  remains the same under some transformations of  $z$ . We give an upper bound for the nonlinearity of  $\mathbf{g}_{2^k}$ , where  $2 \leq k < n - 1$ . We list all linear relations which make the nonlinearity of  $\mathbf{f}_z$  and  $\mathbf{g}_z$  zero and furthermore, we present all linear relations for  $\mathbf{g}_z$  having a high probability. We use these linear relations to derive many more linear relations for 1-round IDEA. We also devise also a new algorithm to find a set of new linear relations for 1-round IDEA based on known linear relations. Moreover, we extend the largest known linear class of weak keys with cardinality  $2^{23}$  to two classes with cardinality  $2^{24}$  and  $2^{27}$ .

Finally, we obtain several interesting properties of the set  $\{(\mathbf{X}, \mathbf{X} \oplus \mathbf{A}) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n \mid (\mathbf{X} \bowtie \mathbf{Z}) \oplus ((\mathbf{X} \oplus \mathbf{A}) \bowtie \mathbf{Z}) = \mathbf{B}\}$  for varying  $\mathbf{A}, \mathbf{B}$  and  $\mathbf{Z}$  in  $\mathbb{Z}_2^n$ , where  $\bowtie \in \{\odot, \boxplus\}$ . By using some of these properties, we present impossible differentials for 1-round IDEA and Pseudo-Hadamard Transform.

Keywords: Boolean Functions, Nonlinearity, Modular Arithmetic, Block Ciphers, Cryptanalysis.

# ÖZ

## IDEA BLOK ŞİFRELEME SİSTEMİNDE KULLANILAN İŞLEMLERİN CEBİRSEL ÖZELLİKLERİ

Yıldırım, Hamdi Murat

Doktora, Matematik Bölümü

Tez Danışmanı: Prof. Dr. Ersan Akyıldız

Mart 2007, 68 sayfa

Bu tezde blok şifreleme sistemi IDEA da kullanılan işlemlerinin kriptografik analizler açısından önemli birçok ilginç cebirsel özelliklerini elde ediyoruz. Bu işlemlerden her birini  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  ye bir fonksiyon olarak bakıyoruz.  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$  daki değişkenlerden birisi olan  $z$  yi sabitleyip,  $\mathbb{Z}_2^n$  den  $\mathbb{Z}_2^n$  ye  $\mathbf{f}_z$  and  $\mathbf{g}_z$  fonksiyonlarını toplama  $\boxplus$  and çarpma  $\odot$  işlemleri için tanımlıyoruz. İlk  $\mathbf{g}_z$  nin doğrusalsızlığının,  $z$  nin bazı dönüşümleri altında aynı kaldığını gösteriyoruz.  $2 \leq k < n - 1$  olduğunda,  $\mathbf{g}_{2^k}$  nin doğrusalsızlığı için bir üst sınır veriyoruz.  $\mathbf{f}_z$  ve  $\mathbf{g}_z$  nin doğrusalsızlığını sıfır yapan tüm doğrusal bağıntılarını listeliyoruz ve ek olarak  $\mathbf{g}_z$  nin yüksek bir olasılığa sahip tüm doğrusal bağıntılarını sunuyoruz. Bu doğrusal bağıntıları IDEA nın birçok 1-tur IDEA doğrusal bağıntılarını bulmak için kullanıyoruz. Ayrıca bilinen doğrusal bağıntılara dayalı, yeni doğrusal bağıntılar kümesi bulmak için yeni bir algoritma tasarlıyoruz. Üstelik  $2^{23}$  elemanlı en büyük, bilinen doğrusal zayıf anahtar sınıfını  $2^{24}$  ve  $2^{27}$  elemanlı iki yeni bir sınıfa

geniřletiyoruz.

Son olarak,  $\mathbb{Z}_2^n$  elemanı, deęiřen  $\mathbf{A}, \mathbf{B}$  and  $\mathbf{Z}$  ve  $\bowtie \in \{\odot, \boxplus\}$  için  $\{(\mathbf{X}, \mathbf{X} \oplus \mathbf{A}) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n \mid (\mathbf{X} \bowtie \mathbf{Z}) \oplus ((\mathbf{X} \oplus \mathbf{A}) \bowtie \mathbf{Z}) = \mathbf{B}\}$  kümesinin bir kaç ilginç özelliklerini elde ediyoruz. Bu özelliklerden bazısını kullanarak 1-tur IDEA ve Pseudo-Hadamard Dönüřüm'leri için imkansız farkları sunuyoruz.

Anahtar Kelimeler: Boole Fonksiyonları, Doğrusalsızlık, Modüler Aritmetik, Blok Şifreleme, Kripto analiz.