DES'İN TMS320C6711 DSP CİHAZI ÜZERİNDEKİ UYGULAMASI, PERFORMANSI VE KARŞILAŞTIRILMASI

M. Tolga SAKALLI
Bilgisayar Mühendisliği Bölümü
Trakya Üniversitesi
tolga@trakya.edu.tr

Ercan BULUŞ
Bilgisayar Mühendisliği Bölümü
Trakya Üniversitesi
ercanb@trakya.edu.tr

Anahtar Kelimeler: DSP, DES, Triple-DES, Performans

ABSTRACT

Security is very important for information and data systems of all types. One means of providing security in communications is through encryption. Recently, encryption has become more important because of e--commerce. Nowadays encryption is performed by software more than hardware. But, if we compare software encryption with hardware encryption we see that we have three important criteria to select hardware: Speed, security and easy installation. Encryption made by software has disadvantages if speed, security and modification are concerned. In addition to that, if encryption is made on another CPU this will increase the performance of all the system. The aim is to see the performance on hardware of DES, Data Encryption Standard, using TI's TMS320C6711 DSP (Digital Signal Processing) device which is a hardware unit. Speech encryption and decryption was made on hardware after theit benchmarking was carried out. Cycle counts for DES and Triple-DES were measured for encryption and decryption of 1024 Bytes of data for each mode (CBC,ECB) and Data rates were calculated directly from these cycle counts.

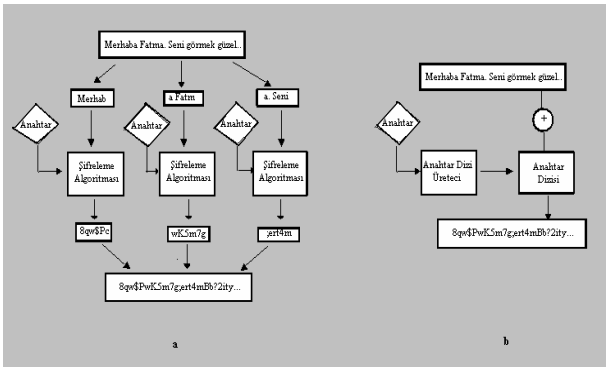
1. Giriş

Şifreleme, Sezar'dan başlayarak gelmekte ve verinin her türlü iletiminde verinin gizlenmesi ve güvenli bir şekilde iletilmesi için kullanılmaktadır. Bir şifreleme algoritması yazılım ile tanımlanabilir. Bunun bazı dezavantajları ve avantajları vardır. Yazılım kullanarak şifrelemenin dezavantajları hızda, maliyette ve modifikasyon kolay-lığındadır. Avantajları esneklik, yerleştirilebilirlik, kul-lanım kolaylığı ve güncelleme kolaylığıdır. Şifreleme yazılımlarında genellikle C dili kullanılır. C kodunda yazılan algoritmalar küçük değişikliklerle herhangi bir bilgisayarda uygulanabilir. Pahalı olmayacak şekilde kopyalanabilir, birçok makineye kolayca kurulabilir ve büyük uygulamalarla birleştirilebilir.. Yazılım şifreleme bugünlerde daha yaygın olmasına rağmen donanım hala askeri ve ciddi ticari uygulamalar için seçim durumundadır.

Bu çalışma yukarıda tanımlandığı üzere bir şifreleme standardı olan DES'in sinyal işleyen bir cihaz olan TI'ın C6711 DSP Başlangıç Kiti üzerinde ses uygulamasını yapmak ve bu donanım cihazı üzerinde etkin performansını bir yazılım ile ortaya koymaktır.

Donanım üzerinde şifreleme yapmanın üç önemli avantajı vardır. İlki hızdır. Özelleştirilmiş donanım üzerinde şifreleme yapmak ve şifrelemeyi diğer bir chip'e taşımak tüm sistemi daha hızlı yapar. İkincisi güvenliktir. Üçüncü ve son nedeni kurulum kolaylığıdır. İnsanlar kendi telefon konuşmalarının, faksimile iletişiminin veya veri hatlarının şifrelenmesini isterler. Telefonlara, faksimile cihazlara modemlere genel amaçlı şifreleme donanımı koymak daha ucuzdur.

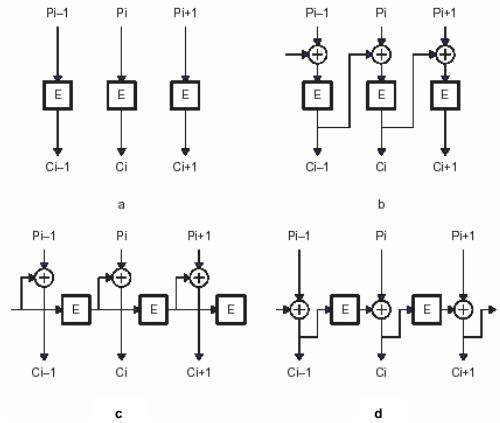
2. Şifreleme Algoritmaları İçin İşlem Metotları



Şekil 1: Şifreleme Çeşitleri : a) Blok Şifreleme
b) Dizi Şifreleme

2.1. Blok Şifreleme

Blok şifrelemenin en basit tanımı açık metni bitişik bloklara bölme, her bloğu şifreleyerek şifreli metin bloklarına döndürme, bu şifreli blokları şifreli metin çıkışı olarak gruplamaktır. Bu yapılan işlem moduna Electronic Code Mode (ECB) mod olarak adlandırılır. Bu modun ayırıcı özelliği şudur ki açık metnin özdeş blokları daima aynı şifreli metne şifrelenir. Bu bazı uygula-malarda sakıncalıdır. O anki bloğun girişine bir önceki şifreli bloğun sonuçlarını besleyerek bloklar arası geri besleme ortaya koymak mümkündür. Geri beslemenin ilk bloğu rastgele olarak üretilir. Ve başlatma vektör olarak adlandırılır. Bu yapıldığı zaman her şifreli metin sadece onu üreten açık metin bloğuna bağlı olmaz. Bunun yanında başlatma vektörünü içeren evvelki bloklara bağımlı olur. Eğer evvelki blokların herbiri özdeş ve başlatma vektörleri özdeşse özdeş açık metin blokları sadece aynı şifrelenmiş bloğu şifreleyecektir. Bu işlem moduna CBC mod denir.



Şekil 2: Blok Şifreleme İşlem Modları

a) Electronic Code Mode

b) Cipher Block Chaining

c) Output Feedback

d) Cipher Feedback

2.2. Dizi Şifreleme

Geçmişte kullanılan yer değiştirme algoritmalarının günümüzde kullanılan biçimidir. Dizi kriptolama yönte-minde, tek kullanımlı şerit yönteminde kullanıldığı gibi, uzun anahtar bilgisine ihtiyaç vardır. Bu sebepten, yarı rassal nitelikte bir anahtar üretmek amacıyla, geri beslemeli öteleme kütüklerinden yararlanılır. Üretilen anahtar ile açık metin dış veya'lanarak gizli metin elde edilir. Şifrenin çözülebilmesi için üretilen anahtarın alıcı tarafta da üretilmesi gerekir. Bunun sonucunda gizli metin ile dış veya'lanan anahtar bilgisi açık metni verecektir. Ancak anahtar üretecinde doğrusal olmayan bir yöntem kullanılmayacak olursa bu şifreleme yöntemi bilinen metin saldırısına açık olacaktır.

3. DES (Data Encryption Standard)

1974 de IBM'in NSA ile birlikte işbirliği ile geliştirilen DES 20 yıldan bu yana dünyada yaygın bir şifreleme standardı olmuştur. Bu 20 yıl içerisinde kendisini kriptanalize karşı dikkate değer bir şekilde korumuştur. Hala güvenli bir şekilde korumaktadır. Şifreleme piya-sasındaki yaygınlığından dolayı DES farklı şifreleme cihazları arasındaki mükemmel bir standarttır.

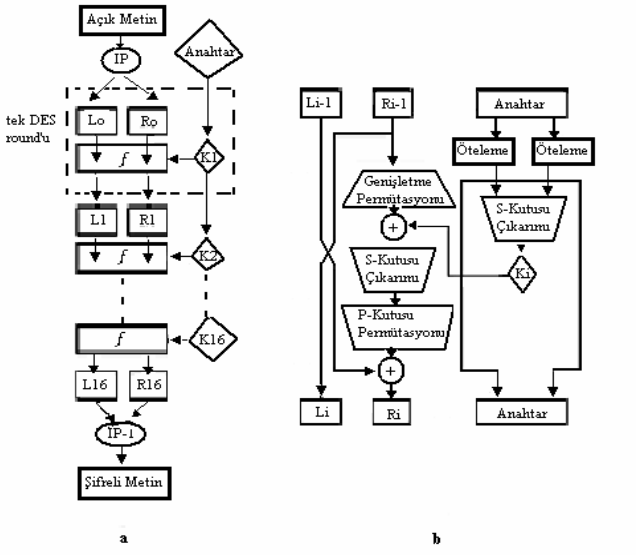
DES'in en büyük zaafı onun 56 bit anahtarıdır. Geliştirildiği zamanlarda çok iyi bir şifreleme algoritması olmasına rağmen modern bilgisayarlar tarafından yapılan anahtar saldırılarına karşı yetersiz kalmaya başladı. Daha büyük şifreleme ihtiyacının bir sonucu olarak DES Triple-DES şeklinde geliştirildi. Triple-Des, 3 adet 56 bitlik anahtarı kullanarak şifreleme yapar. Bu 168 bitlik anahtar gücüne eşit bir güç demektir. Bu uygulama bununla beraber şifreleme ve deşifreleme için 3 kat fazla çevrim gerektirir. Bu da DES'in ikinci bir zayıflığına dikkati çeker. O da hızdır. DES donanım üzerinde yürütülmek üzere geliştirildi. Ve yazılımda Des'in yürütülmesi yazılım performansının iyi olması niyetiyle geliştirilen diğer standartlardan sıkça daha az etkilidir.

4. DES'in Tanımı

DES karıştırma ve yayılma şifreleme tekniğine dayanır. Karıştırma yerdeğiştirme ile başarılır. Özellikle verinin seçilen bölgeleri orjinal veriden takip eden bölgeler ile yerdeğiştirilir. Yerdeğiştirilen verinin seçimi anahtara ve orjinal sade metne bağlıdır. Yayılma permütasyon ile başarılır. Farklı kısımların sırası yeniden düzenlenerek veri permute (değiş tokuş) edilir. Bu permutasyonlar, yerdeğiştirmeye benzer şekilde, anahtar ve orjinal yalın metne bağlıdır. Yerdeğiştirmeler ve permütasyonlar DES algoritması tarafından belirlenir. Veri ve anahtarın seçilen kısımları matematiksel olarak işlenir. Ve bir look-up tablosuna giriş olarak kullanır. DES'de bu tablolar sırasıyla yerdeğiştirme tabloları ve permütasyon tabloları S kutuları ve P kutuları olarak adlandırılır. Yazılımda bu look-up tabloları diziye index olarak kullanılan anahtar/veri girişi ve diziler olarak gerçekleştirilir. Genellikle S ve P kutuları yerdeğiştirme ve takip eden permütasyon bir tek look-up ile her roundun yapılabil-mesi için birleştirilir.

S ve P kutu dizilerine girişleri hesaplayabilmek için veri parçaları anahtar parçaları ile dar veya'lanır. 64 bitlik verinin 32 bitlik yarılarından biri ve anahtar kullanılır. Veri yarısından anahtar daha uzun olduğu için 32 bit veri yarısı bitlerini tekrar düzenleyen kesin

bitleri tekrar eden 48 bitlik ürünü oluşturmak üzere genişletilmiş bir permütasyona yollanır. Benzer şekilde 56 bitlik anahtar bitlerini tekrar düzenleyen sıkı bir permütasyon işlemine uğrar. Bazı bitler atılarak 48 bitlik ürüne dönüştürülür. Bu look-up tablolarına girişleri üreten anahtar, veri üzerin-deki hesaplamalar ve S ve P kutu look-upları DES'in bir tek çevrimini meydana getirir (şekil 3b).



Şekil 3: a) DES Core Algoritması

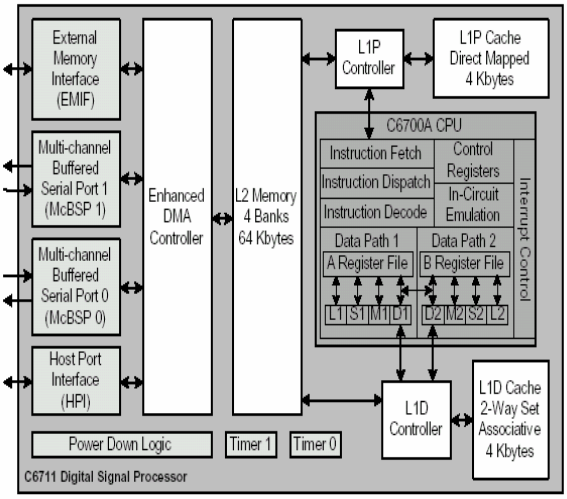
b) Genişletilmiş Tek Round

S ve P kutu yerdeğiştirme permütasyon prosesi 16 defa tekrar edilerek DES algoritmasının 16 roundu oluşur. Aynı zamanda başlatma ve sonuç permütasyonlarıda vardır. 16 rounddan önce ve sonra meydana gelirler. Bu başlatma ve final permütasyonları tarihsel nedenlerden dolayı donanım üzerinde uygulama ile uğraşmak için vardır. Algoritmanın güvenliğini geliştirmez. Bu neden-den dolayı onlar bazı zamanlar DES in uygulamasına ayrılır. Bununla beraber onlar bu analizde DES in teknik tanımının parçası olarak bulunur.

5. Kullanılan DSP Donanımı

Bilgisayar biliminde Digital Signal Processing ayrı bir data tipi olan 'sinyaller' ile diğer alanlardan ayrılır. Birçok durumda, bu sinyaller gerçek dünyadan alınmıştır; sismik titreşimler, görsel görüntüler, ses dalgaları vs. DSP bu sinyalleri sayısal sinyallere çevirdikten sonra işleyen bir matematiktir, algoritmadır, tekniktir. Bunun yanında donanımsal olarak sinyal işle-yen cihazlar da geliştirilmiştir.

Kullanılan cihaz Texas Instruments şirketinin geliştirdiği DSP cihazlarından biri olan TMS320C6711 cihazıdır. Geleneksel bir VLIW, çok uzun komut kelimesi, mimarisi tek bir saat çevrimi süresince birden fazla komutu üzerinde paralel olarak çalışabilen çoklu yürütme ünitelerine sahiptir. Paralellik yüksek performansın arkasındaki anahtardır. C6711 cihazı kayan noktalı bir cihaz olup kayan noktalı ve sabit noktalı komutları üzerinde işleyebilir. 150 MHz hızındaki bu cihaz paralel çalışan 8 üniteye sahiptir. Bir saat çevrimi süresince 6 kayan noktalı komut üzerinde çalışabilir. Bu da onun saniyede 900 milyon kayan noktalı komutu işleyebildiği anlamına gelmektedir. C6711, 72 Kb kendi üzerinde belleğe sahiptir. Bu bellek L1 ve L2 olarak ayrılmıştır. L1 de kendi içinde L1D ve L2D olarak 4KB' lık bölümlere ayrılmıştır. L2 belleği ise 8Kb'lık 4 bölüme bölünmüştür. C6711 cihazının Şekil 4' te blok diyagramı gösterilmiştir.



Şekil 4: TMS320C6711 DSP Blok Diyagramı

5.1 Performansı Verilen TMS320C6211 Ve TMS320C6711 Cihazı Arasındaki Farklılıklar

C6711 ve C6211 cihazları arasında sadece iki farklılık vardır.

- C6711 bir kayan noktalı bir CPU ya sahiptir. C6211 ise sabit noktalı.
- C6711'in 100 Mhzlik versiyonu C6000 platformuna en düşük maliyette giriş sağlamıştır.

Dolayısıyla C6211 için yazılan kod aynen C6711 cihazı içinde geçerli olacak ve düzgün bir şekilde çalışacaktır. Ancak C6711 cihazı için yazılan kod C6211 cihazında doğru bir şekilde çalışmayacaktır. C6211 cihazı ile C6711 cihazının cpu dışındaki tüm üniteleri aynıdır.

6. Kullanılan Yazılım

Şifreleme ve Deşifreleme işini yapan kod C kodunda yazılmıştır. Bununla beraber donanım üzerinde performansı arttırmak için bazı optimizasyonlar yapılmıştır. Bu optimizasyonlar algoritma, işlemsel mod ve bellek optimizasyonları olarak üç aşamada yapılmıştır.

7. Performans Analizi

Anahtar planlama, şifreleme ve deşifreleme için performans analizi bilgisayar ve cihaz arasındaki iletişimde arayüz görevi gören bir program olan kod birleştirici stüdyo ve cihazda bulunan DSP/BIOS kütüphanesi ile sağlanmıştır. İstatistik nesneler anahtar planlama, şifreleme, deşifreleme rutinleri için çevrim değerlerinin toplanmasında kullanılmıştır. Performans analizinin yapılabilmesi için kaynak kodlara ek olarak konfigürasyon dosyalarının yaratılması ve istatistik nesnelerinin bu dosya üzerinde tanımlarının yapılarak kullanacakları uygun özelliklerin belirtilmesi gerekmek-tedir. Performans analizi yapmak için yazılımın kullan-dığı donanım ve yazılım kesmeleri vardır. Yazılım kes-meleri performans analizi için kullanılır. Anahtar Plan-lama, Şifreleme, Deşifreleme işlemleri için yazılım kes-meleri konfigürasyon dosyasında tanımlanır. Bunlar bir fonksiyonu tetikleyeceklerdir. Ayrıca konfigürasyon dosyasında tanımlanan istatistik nesneler bu tetiklenen yazılımda bulunan API'ler ile performans bilgisini yani çevrim değerlerini toplamak için kullanılacaklardır.

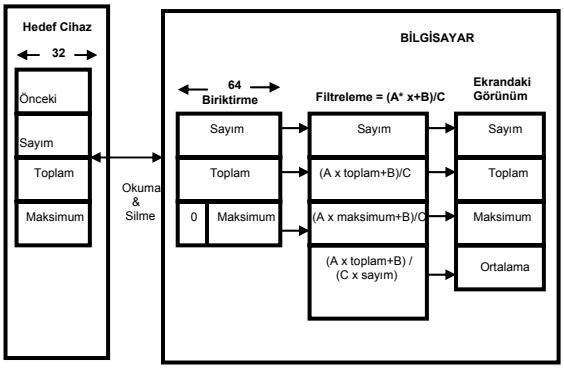
Örnek : Anahtar planlamanın performans analizi

KeySWI → key_isr → sts_set ve sts_delta → set_key
Yazılım kesmesi KeySWI key_isr fonksiyonunu tetikler. Bu fonksiyonda bulunan sts_set ve sts_delta fonksi-yonları set_key nesnesinin istatistik verileri toplamasını sağlar.
Key_isr fonksiyonun kodu :

```
void key_isr(void){
  /* set key schedule */
  STS_set(&set_key, CLK_gethtime());
  des_set_key((des_cblock *)enc_key1,sch[0]);
  STS_delta(&set_key, CLK_gethtime());
  des_set_key((des_cblock *)enc_key2,sch[1]);
  des_set_key((des_cblock *)enc_key3,sch[2]);

  des_set_key((des_cblock *)dec_key1,dec_sch[0]);
  des_set_key((des_cblock *)dec_key2,dec_sch[1]);
  des_set_key((des_cblock *)dec_key3,dec_sch[2]);

   SWI_post(&encryptSWI);
}
```



Şekil 5 : Bilgisayar ve cihaz arasındaki istatistik veri alışverişi

8. DES'in DSP Üzerindeki Performans Sonuçları

Cihaz üzerinde performans sonuçları elde edilirken **ses sinyali** cihaza gönderilmiştir. Bu ses sinyali cihaz üzerinde analog sayısal dönüşüme uğradıktan sonra cihaz üzerinde sayısal değerler üzerinde sırasıyla şifreleme, deşifreleme ve doğrulama işlemleri yapılmış ve daha sonra kod birleştirici stüdyo ve DSP/BIOS istatistik nesneleri ve gerekli ek kod ile performans değerlerinin çevrim olarak değerleri gözlenmiştir. DES ve Triple-DES gibi günümüzde önemli olan bu şifreleme algoritmaları için cihazın hızı, işlenen veri miktarı ve elde edilen çevrim değerleri göz önüne alınarak gerekli hesaplamalar yapılmıştır. Bu hesaplama sonucunda saniyede işlenen veri miktarı gösterilmiştir. Elde edilen değerler sesin şifrelenmesi ve deşifrelenmesi üzerine oldukça yüksek etkinlikte değerlerdir.

DES Modu	Anahtar Planlama (çevrim sayısı)	Şifreleme (çevrim sayısı)	Deşifreleme (çevrim sayısı)
Triple-Des, CBC	1140	122307	121603
Triple-DES, CBC 3 Kanallı	1167	186346	195624
Triple-DES, ECB	1148	61904	61293
DES, CBC	1159	48468	52459
DES, CBC 3 Kanallı	1169	82342	92882
DES, ECB	1169	25705	27075

Tablo 1-) C6711 üzerinde DES'in performansı için elde edilen çevrim değerleri

Yukarıdaki değerler C6711 de her mod için 1024 byte'lık verinin şifrelenmesi ve deşifrelenmesi ile ölçülen çevrim değerleridir (Üç kanallı her kanalda 1024 Byte'lık veriyi şifreler).

DES Modu	Şifreleme (veri / sn)	Deşifreleme (veri / sn)
Triple-Des, CBC	10,04 Mbps	10,10 Mbps
Triple-DES, CBC 3 Kanallı	19,77 Mbps	18,84 Mbps
Triple-DES, ECB	19,35 Mbps	20,05 Mbps
DES, CBC	25,38 Mbps	23,43 Mbps
DES, CBC 3 Kanallı	44,77 Mbps	39,71 Mbps
DES, ECB	47,92 Mbps	45,45 Mbps

Tablo 2-) DES' in C6711 üzerinde elde edilen performans hesabı sonucu

Yukarıdaki değerlerin hesaplanmasında

$$veri\ oranı = \frac{150\ Mhz\ (dsp\ cihazının\ hızı)}{(çevrim\ sayısı\ /\ 8192\ bits)}$$

Şeklindedir.

DES Modu	Anahtar Planlama	Şifreleme	Deşifreleme
Triple-DES, CBC	1448	133611	129680
Triple-DES,CBC 3 kanallı	1444	209544	220499
Triple-DES, ECB	1445	68884	68770
DES, CBC	1425	52540	51576
DES, CBC 3 kanallı	1440	96068	105836
DES, ECB	1447	31644	31722

Tablo 3-) C6211 üzerinde DES'in performansı için daha önce yapılan bir çalışmada elde edilen çevrim değerleri

DES Modu	Şifreleme	Deşifreleme
Triple-DES, CBC	9,2 Mbps	9,4 Mbps
Triple-DES, CBC 3 kanallı	17,6 Mbps	16,7 Mbps
Triple-DES, ECB	17,8 Mbps	17,8 Mbps
DES,CBC	23,4 Mbps	23,84 Mbps
DES,CBC 3 kanallı	38,4 Mbps	34,8 Mbps
DES, ECB	38,8 Mbps	38,7 Mbps

Tablo 4-) DES' in C6211 üzerinde daha önce yapılan bir çalışmada elde edilen performans hesabı sonucu

9. Sonuç

TMS320C6711 DSP cihazı kayan noktalı kod kullanırken TMS320C6211 cihazı sabit noktalı kod kullanır. Cihazlar arasında performans olarak az da olsa farklılık vardır. Ancak TMS320C6711 için yazılan kod TMS320C6211 için kullanılmaz.

C kodu kullanılarak TMS320C6711 DSP cihazı üzerinde DES şifreleme standardının uygulaması yapılarak DES için 47,92 Mbps Triple-DES için ise 19,35 Mbps veri oranları gözlenmiştir.

Bir çok şifreleme algoritması C kodunda herhangi bir lisans kısıtlaması olmadan Internetten elde edilebilmek-tedir. DES'in yerine geçebilecek bir standart için performans araştırmaları kolaylıkla sayısal sinyal işleyen cihaz üzerinde gerçekleştirilebilir.

Günümüzde artık Internet telefonculuğu yaygınlaşmaya başlamıştır. Dolayısıyla bu elde edilen performans sonuçları ağ için yeterli hatta yeterlilikten bile fazladır. Ağ üzerinde sesin şifrelenmesi ve deşifrelenmesi uygu-lamalarında eldeki değerler yadsınamayacak boyuttadır.

Daha önceden de bahsedildiği gibi şifrelemede sayısal sinyal işleyen cihaz kullanılmıştır. Donanım olarak bu cihazı kullanmanın avantajı cihazın gerçek zamanda çalışma avantajını kullanmaktır.

KAYNAKLAR

[1] **R. Stephen Preissig**, 2000. Data Encryption Standart (DES) Implementation on the TMS320C6000, Literature Number SPRA702, Texas İnstruments

[2] **Bruce Schneider**, 1996. Applied Cryptography, Second Edition, John Wiley & Sons, Inc. , New York, Ny

[3] **Dave Bell**, 2000. How to Begin Devolopment with the TMS320C6711 DSP, Literature Number SPRA522, Texas İnstruments

[4] TMS320C6000 Optimizing Compiler User's Guide, Literature Number SPRU187, Texas İnstruments, 2000

[5] TMS320C6000 DSP/BIOS User's Guide, Literature Number SPRU303, Texas İnstruments, 2000

[6] TMS320C6000 Code Composer Studio User's Guide, Literature Number SPRU328b Texas Instruments, 2000

[7] TMS320C62x/C67x CPU and Instruction Set Reference Guide, Literature Number SPRU189c, Texas Instruments, 1998

[8] How to Begin Devolopment Today with the TMS320C6211 DSP, Literature Number SPRA474, Texas Instruments, 1998

[9] TMS320C6000 Programmer's Guide, Literature Number SPRU198, Texas Instruments,2000

[10] TMS320C6000 Technical Brief, Literature Number SPRU197, Texas Instruments, 1999