T.C.
SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

2018-2019 Güz Dönem Proje Ödevi

BSM465 - KRİPTOLOJİYE GİRİŞ

Lblock Algoritması

G151210023 – Ahmet Said BALASAR
G140910046 – Emin GÜNEY

Lightweight Block Şifreleme

Geleneksel blok şifrelere kıyasla, hafif sıklet şifreler aşağıdaki üç ana özelliğe sahiptir. İlk olarak, kısıtlı cihazlara yönelik uygulamaların, büyük miktarlardaki verilerin şifrelenmesini gerektirme olasılığı düşüktür ve dolayısıyla hafif sıklet şifreler için yüksek verim gerektirmez. İkincisi, bu kriptografi ortamında, saldırganların veri ve bilgi işlem yetenekleri eksiktir, bu da hafif sıklet şifrelere yalnızca orta düzeyde bir güvenlik sağlamak için ihtiyaç duyduğu anlamına gelir.

Son olarak, hafif sıklet şifreler genellikle donanım ortamında uygulanmaktadır ve bunların küçük bir kısmı da 8-bit mikrodenetleyici gibi yazılım platformlarında uygulanmaktadır. Bu nedenle, hafif şifreler için donanım performansı birincil etken olacaktır.

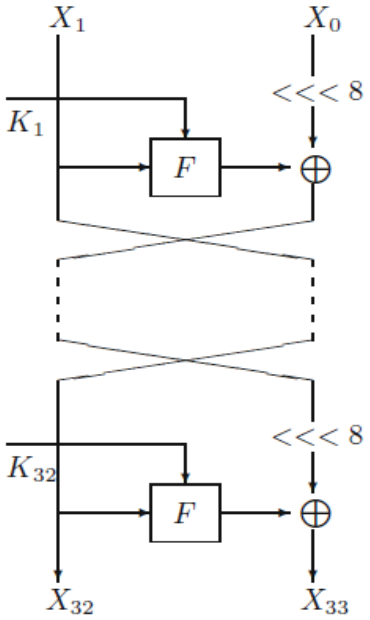
LBlock'un performans değerlendirmesi, sadece donanım verimliliğinin değil, 8 bit / 32 bit platformlarda yazılım uygulamalarının da çok hafif olduğunu göstermektedir.

Lblock Özellikleri

LBlock'un blok uzunluğu 64-bit ve anahtar uzunluğu 80-bittir. Değişken bir Feistel yapısı kullanır ve 32 turdan oluşur. LBlock'un özellikleri üç bölümden oluşur: şifreleme algoritması, şifre çözme algoritması ve anahtar programlama.

Lblock Şifrelenmesi

Lblock şifrelenmesi 32 turluk Feistel ağının bir değişkeni olan iteratif bir yapıdan oluşur.



Lblock'ta şifreleme işlemi

Şifreleme Adımları:

1. i için = 2, 3, . . . , 33
$Xi = F(Xi-1, Ki-1) \oplus (Xi-2 <<< 8)$

2. C = X32||X33 çıktısı 64 bitlik ciphertexttir.
Özellikle, her turda kullanılan bileşenler aşağıdaki gibi tanımlanmaktadır.

(1) Round fonksiyon F

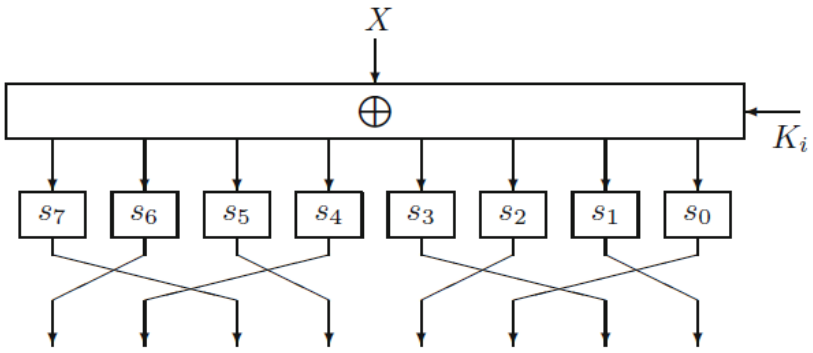
Round fonksiyon F, S ve P'nin confusion ve diffusion fonksiyonlarıyla aşağıda gösterildiği gibi tanımlanabilir.

$F : \{0, 1\}32 \times \{0, 1\}32 \dashrightarrow \{0, 1\}32$
$(X, Ki) \dashrightarrow U = P(S(X \oplus Ki))$

(2) Confusion Fonksiyonu S

Confusion fonksiyonu S, round fonksiyon F'nin doğrusal olmayan katmanını gösterir ve paralel olarak sekiz adet 4-bit S-kutu si içerir.

S: $\{0, 1\}32 \dashrightarrow \{0, 1\}32$
$Y = Y7||Y6||Y5||Y4||Y3||Y2||Y1||Y0 \dashrightarrow Z = Z7||Z6||Z5||Z4||Z3||Z2||Z1||Z0$
$Z7 = s7(Y7), Z6 = s6(Y6), Z5 = s5(Y5), Z4 = s4(Y4),$
$Z3 = s3(Y3), Z2 = s2(Y2), Z1 = s1(Y1), Z0 = s0(Y0).$



Round F fonksiyonu

(3) Diffusion fonksiyonu P

Diffusion fonksiyonu P, sekiz adet 4-bit kelimelik bir permütasyon olarak tanımlanır ve aşağıdaki denklemler olarak ifade edilebilir.

$P : \{0, 1\}32 \dashrightarrow \{0, 1\}32$
$Z = Z7||Z6||Z5||Z4||Z3||Z2||Z1||Z0 \dashrightarrow U = U7||U6||U5||U4||U3||U2||U1||U0$
$U7 = Z6,\ U6 = Z4,\ U5 = Z7,\ U4 = Z5,$
$U3 = Z2,\ U2 = Z0,\ U1 = Z3,\ U0 = Z1.$

2.3 Algoritmanın Çözümlenmesi

Lblock algoritmanın çözümlenme işlemi şifreleme işleminin tersi prosedürlerden oluşur. Çözümlenme işlemi aşağıdaki gibi ifade edilebilir.

1. j = 31, 30, . . . , 0 için
$Xj = (F(Xj+1, Kj+1) \oplus Xj+2) >>> 8$
2. M = X1||X0 çıktısı 64-bitlik bir plaintexttir.

2.4 Anahtar Oluşturma

80 bitlik ana anahtar K, anahtar kaydedicisinde saklanır.

1. i = 1, 2, . . . , 31, için anahtar kaydedicisi K'yı şu şekilde güncellemek gerekir:

(a) $K <<< 29$

(b) $[k79\ k78\ k77\ k76] = s9[k79\ k78\ k77\ k76]$
$[k75\ k74\ k73\ k72] = s8[k75\ k74\ k73\ k72]$

(c) $[k50k49k48k47k46] \oplus [i]2$

Tablo 1. Lblock'ta kullanılan S-Box'ın içeriği

s0 14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
s1 4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3
s2 1, 14, 7, 12, 15, 13, 0, 6, 11, 5, 9, 3, 2, 4, 8, 10
s3 7, 6, 8, 11, 0, 15, 3, 14, 9, 10, 12, 13, 5, 2, 4, 1
s4 14, 5, 15, 0, 7, 2, 12, 13, 1, 8, 4, 9, 11, 10, 6, 3
s5 2, 13, 11, 12, 15, 14, 0, 9, 7, 10, 6, 3, 1, 8, 4, 5
s6 11, 9, 4, 14, 0, 15, 10, 13, 6, 12, 5, 7, 3, 8, 1, 2
s7 13, 10, 15, 0, 14, 4, 9, 11, 2, 1, 8, 3, 7, 5, 12, 6
s8 14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
s9 4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3

Ekran Çıktıları :

```
run:
1. 16 Bitlik Karakter Şifreleme Yap
2. Text dökümanından şifreleme Yap
3. Cikis
Seçiminizi Yapınız=>1
16 bitlik şifrelenecek hexa-decimal veriyi giriniz..:1234aaaaddddffff
Girmiş olduğunuz verinin BİNARY karşılığı..:
0001001000110100101010101010101010110111011101110111011111111111111111
 Şimdi anahtarınızı üretiyorum ...
.............
İşte ürettiğim anahtar ..:
00000001000000000000000000000000100010001000000010001000100010001
Şifreleme Başlıyor
0001001000110100101010101010101010110111011101110111011111111111111111
xR[0]=11011101110111011111111111111111
++++++ENCRYPTION++++++


************
Round 0:
Round Key =  00000001000000000000000000000001


L[0]=00000000000000000000000000000000
R[0]=11111111111111111111111111111111

************
Round 1:
Round Key =  00010000000100010000000100010000


L[1]=00000000000000000000000000000000
R[1]=11111111111111111111111111111111

************
Round 2:
Round Key =  00000001000000010000000100010000


L[2]=00000000000000000000000000000000
R[2]=00000000000000000000000000000000

************
Round 3:
Round Key =  00000000000000000001000100010001


L[3]=00000000000000000000000000000000
R[3]=11111111111111111111111111111111
```

```
************
Round 27:
Round Key =  00000001000100000000000000000001


L[27]=00000000000000000000000000000000
R[27]=11111111111111111111111111111111

************
Round 28:
Round Key =  00010000000000010000000000000001


L[28]=00000000000000000000000000000000
R[28]=11111111111111111111111111111111

************
Round 29:
Round Key =  00000000000100010001000100000001


L[29]=00000000000000000000000000000000
R[29]=11111111111111111111111111111111

************
Round 30:
Round Key =  00010001000000000001000100010001


L[30]=00000000000000000000000000000000
R[30]=00000000000000000000000000000000

************
Round 31:
Round Key =  00010001000100010001000100010000
```

Kaynakça

Javier Lopez, Applied Cryptography & Network Security
(327, 328,329,330 ,331, 332)