Ünite içeriği

- stream şifrelemeye giriş
- Rastgele sayı üreteci (Random number generators (RNGs))
- **Tek kullanımlık blok notlar(One-Time Pad (OTP))**
- Linear feedback shift registers (LFSRs)
- Trivium: a modern stream şifre

- **One-Time Pad (OTP)**

alışılmadık ölçüde güvenli şifreleme sistemleri:

- Eğer şifreleme sistemi sonsuz hesaplama kaynağıyla da kırılamıyorsa bu sistem şartlara bağlı olmayarak güvenlidir.

One-Time Pad

- Bu şifreleme sistemi Vernam's stream şifre yapısına dayanır:
- Özellikler:

  Düz metin, şifreli metin ve anahtar kendi bitlerinden oluşsun

  $x_i, y_i, k_i \in \{0,1\}$.

Encryption:	$e_{k_i}(x_i) = x_i \oplus k_i$.
Decryption:	$d_{k_i}(y_i) = y_i \oplus k_i$

OTP alışılmadık ölçüde güvenlidir eğer k_i Anahtar değeri sadece bir defa kullanılırsa!

- **One-Time Pad (OTP)**

Alışılmadık ölçüde güvenli şifreleme sistemi :

$$y_0 = x_0 \oplus k_0$$

$$y_1 = x_1 \oplus k_1$$

$$\vdots$$

Her denklem iki bilinmeyenli bir liner denklemdir

$\Rightarrow$ her y_i için $x_i = 0$ ve $x_i = 1$ dir!

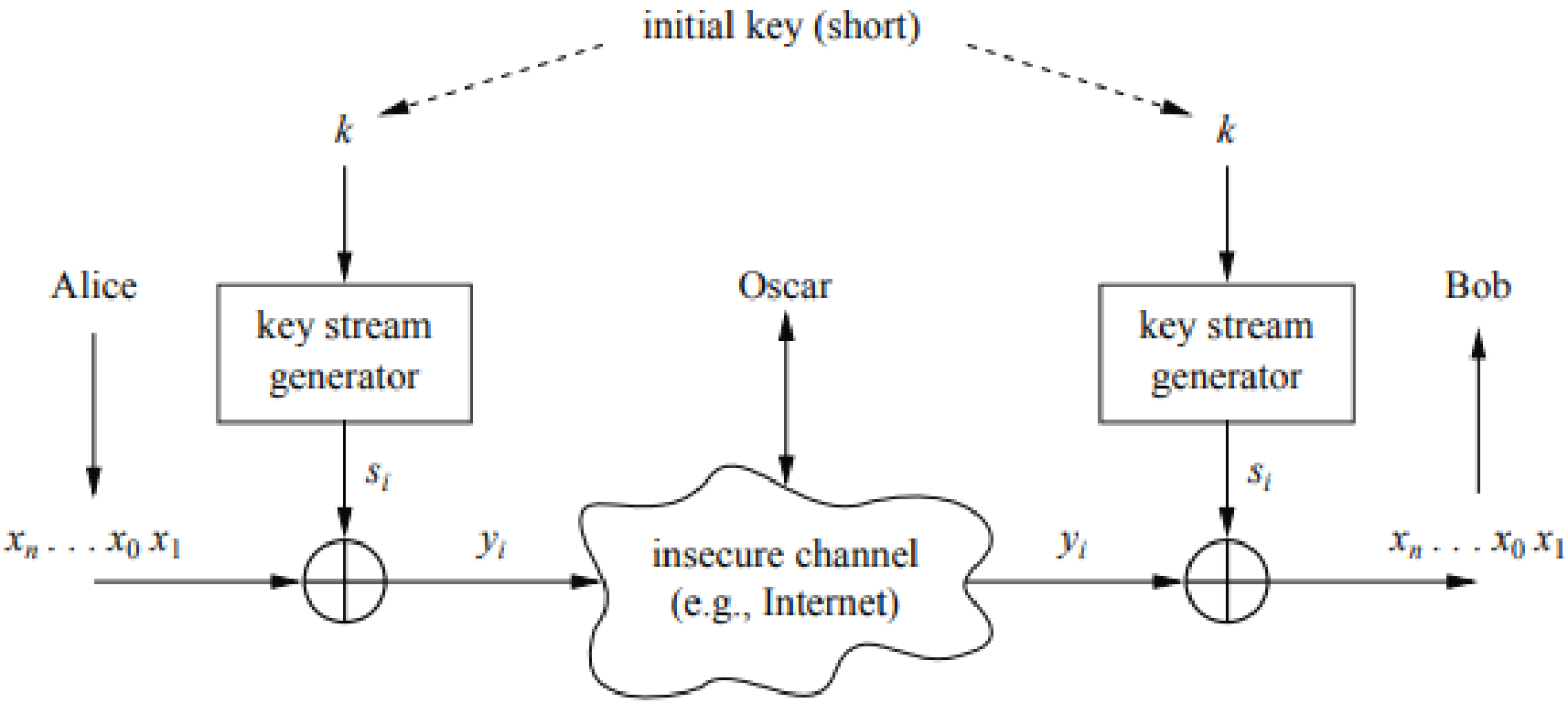
$\Rightarrow$Bu doğrudur eğer k_0, k_1, ... Değerleri bağımsızsa, örneğin k_i anahtar değerleri tamamen rastgele olursa

dezavantaj: Hemen hemen bütün OTP uygulamaları **pratik değildir** çünkü anahtar mesajla aynı boyutta olmalı! (Imagine you have to encrypt a 1GByte email attachment.)

Ünite içeriği

- stream şifrelemeye giriş
- Rastgele sayı üreteci (Random number generators (RNGs))
- Tek kullanımlık blok notlar(One-Time Pad (OTP))
- **Linear feedback shift registers (LFSRs)**
- Trivium: a modern stream şifre

Pratik Akış Şifrelerine Doğru

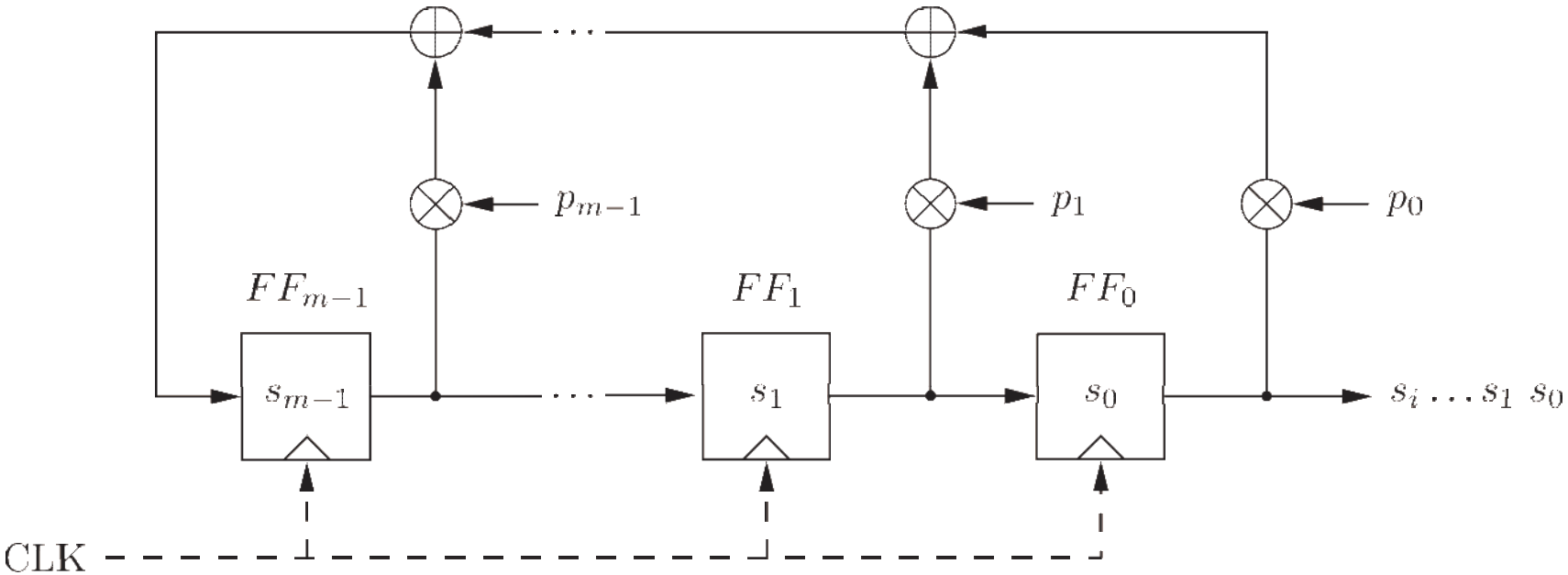


Bir şifreleme sistemi, onu kırmak için en iyi bilinen algoritma en az t işlem gerektiriyorsa, hesaplama açısından güvenlidir.

- **Shift Register Tabanlı Akış Şifreleri**

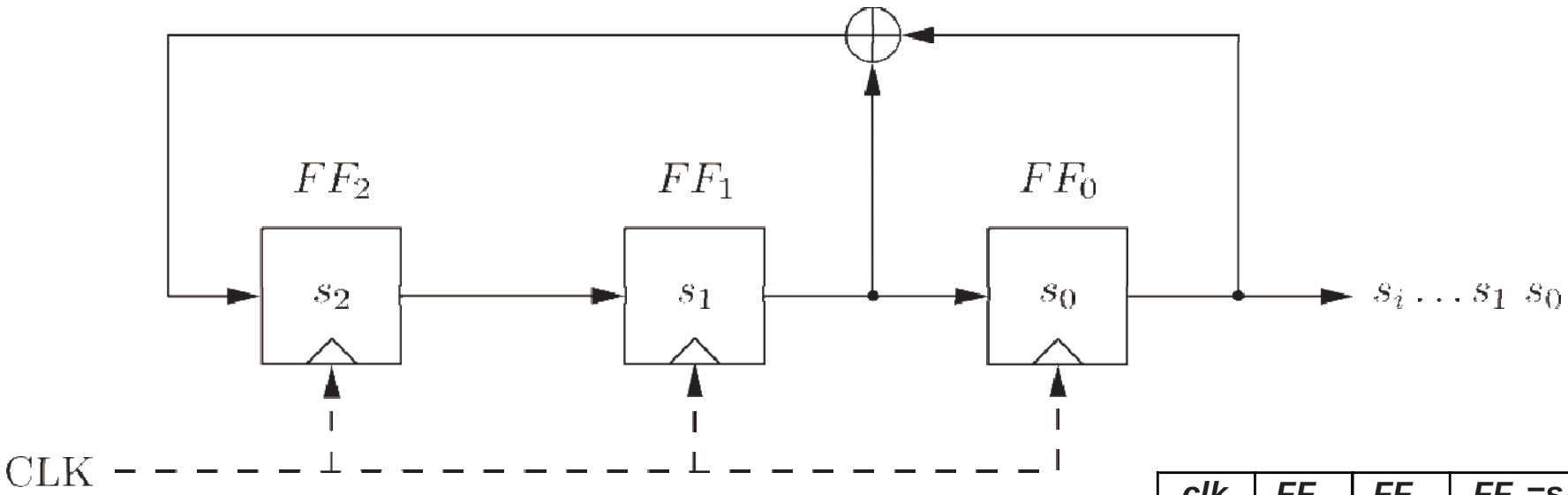
Şimdiye kadar öğrendiğimiz gibi, pratik akış şifreleri, belirli özelliklere sahip olması gereken, anahtar akışı üreteci tarafından üretilen s1,s2,... anahtar bitlerinin bir akışını kullanır.
Uzun sözde rasgele dizileri gerçekleştirmenin zarif bir yolu, doğrusal geri besleme kaydırmalı yazmaçları (LFSR'ler) kullanmaktır.
LFSR'ler donanımda kolayca uygulanır ve çoğu, ancak kesinlikle hepsi değil, akış şifreleri LFSR'leri kullanır.
Örneğin, GSM'de ses şifreleme için standart hale getirilen A5/1 şifresidir.
Göreceğimiz gibi, düz bir LFSR iyi istatistiksel özelliklere sahip bir dizi üretse de kriptografik olarak zayıftır.
Bununla birlikte, A5/1 veya şifre Trivium gibi LFSR'lerin kombinasyonları, güvenli akış şifreleri oluşturabilir.

- **Linear Feedback Shift Registers (LFSRs)**



- Geri besleme durum bitlerini XOR layarak yeni giriş değerini üretmeye çalışır.
- *m* derecesi depolanan elementlerin sayısını verir.
- Eğer p_i = 1 se, geri besleme bağlantısı vardır (“kapalı anahtar), aksi halde bu flip-flop ta geri besleme yoktur(“açık anahtar”)
- Çıkış zinciri periyodik olarak tekrarlar
- Maximum çıkış uzunluğu**:** 2^m-1

- **Linear Feedback Shift Registers (LFSRs):**



clk	FF_2	FF_1	$FF_0=s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0
8	0	1	0

- LFSR çıkışı rekürsif denklemlerle tanımlanır:

$$s_{i+3} = s_{i+1} + s_i \bmod 2$$

- Maximum çıkış uzunluğu (of 2^3-1=7) kabul edilir sadece belli geri besleme yapısı için, örneğin biri burda gösterilmiştir.

- **Security of LFSRs**

LFSR polinomlarla şöyle gösterilir:

$$P(x) = x^m + p_{l-1} x^{m-1} + \ldots + p_1 x + p_0$$

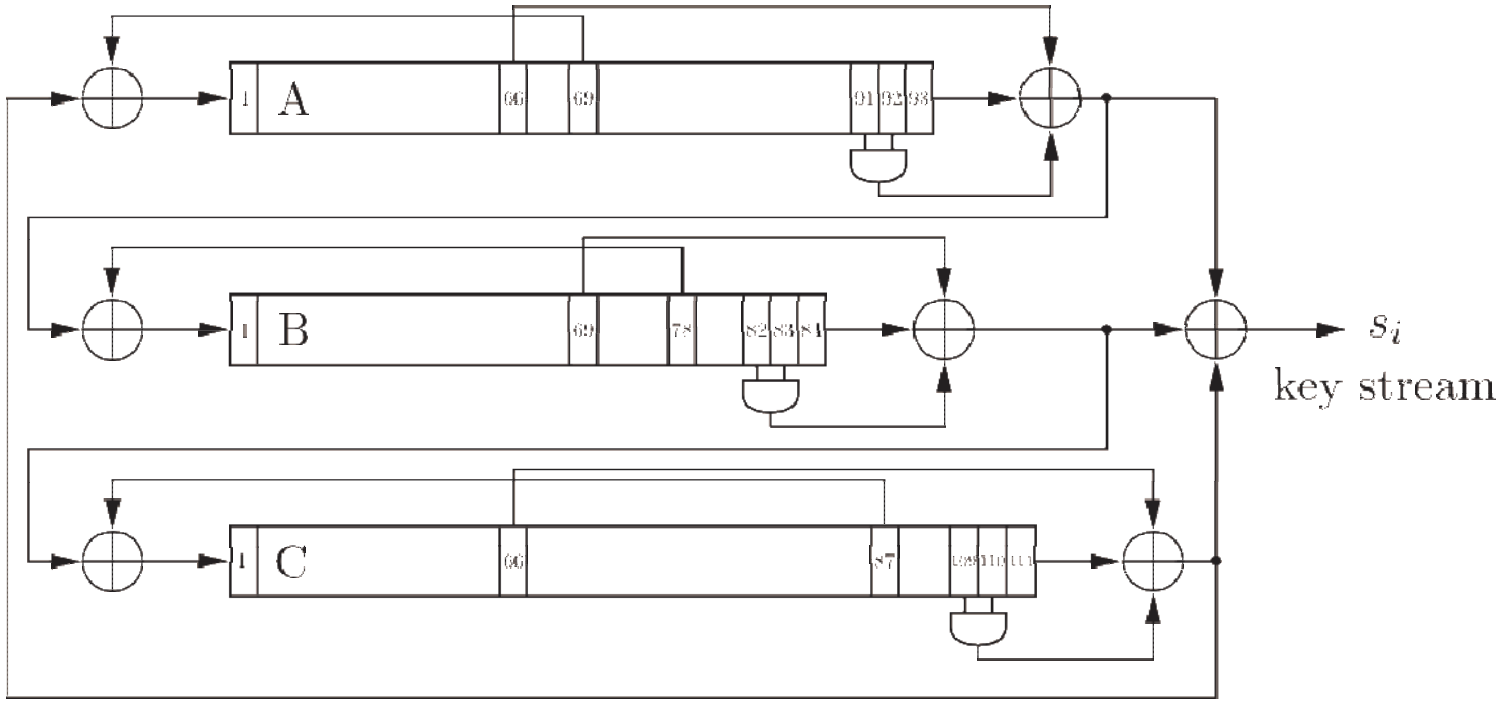
- Tek LFSR büyük ihtimalle tahmin edilebilir bir sonuç üretir.
- Eğer 2*m* çıkış biti varsa LFSR nin o zaman bunun derecesi m olmaktadır, geri besleme sabitleri p_i ler lineer sistemlerdeki çözümlerle bulunabilir.
- Bir çok stream şifreleme LFSR nin birleşimi şeklindedir.

*daha fazla ayrıntı için *Understanding Cryptography* *ünite 2 bak*

Ünite içeriği

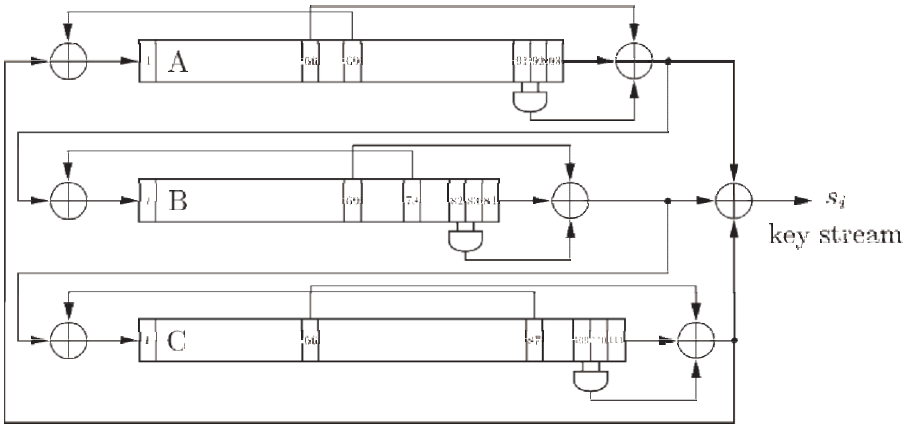
- stream şifrelemeye giriş
- Rastgele sayı üreteci (Random number generators (RNGs))
- Tek kullanımlık blok notlar(One-Time Pad (OTP))
- Linear feedback shift registers (LFSRs)
- **Trivium: a modern stream şifre**

- **A Modern Stream Cipher - Trivium**



- Üç *nonlinear* LFSRs (NLFSR) nin uzunluğu 93, 84, 111
- XOR-toplama üç NLFSR çıkışları streamanahtarı s_i Üretir. Donanımda küçüklük:
  - Toplam kaydedici sayısı: 288
  - Liner olmayan: 3 AND-kapısı
  - 7 XOR-kapısı (4 tanesi iç girişli)

- **Trivium**



Atama:

- Load 80-bit IV into A
- Load 80-bit key into B
- Set c_{109} , c_{110} , c_{111} =1, all other bits 0

Şifreleme:

- XOR-Toplama her üç NLFSR çıkışı stream anahtarı s_i üretir.

Her saat darbesinde 64 biti paralel üretmek için düzenlenebilir

	Register length	Feedback bit	Feedforward bit	AND inputs
A	93	69	66	91, 92
B	84	78	69	82, 83
C	111	87	66	109, 110

Lessons Learned

- Stream ciphers are less popular than block ciphers in most domains such as Internet security. There are exceptions, for instance, the popular stream cipher RC4.
- Stream ciphers sometimes require fewer resources, e.g., code size or chip area, for implementation than block ciphers, and they are attractive for use in constrained environments such as cell phones.
- The requirements for a *cryptographically secure* pseudorandom number generator are far more demanding than the requirements for pseudorandom number generators used in other applications such as testing or simulation.
- The One-Time Pad is a provable secure symmetric cipher. However, it is highly impractical for most applications because the key length has to equal the message length.
- Single LFSRs make poor stream ciphers despite their good statistical properties. However, careful combinations of several LFSR can yield strong ciphers.