Lecture 4 More on Stream Ciphers :-

Cristof will show the Cipher, way of building cipher and actual attack in this lecture. Then the question arises why are we learning then ?
Point is if you use the building blocks of this cipher you can build very very secure cipher.

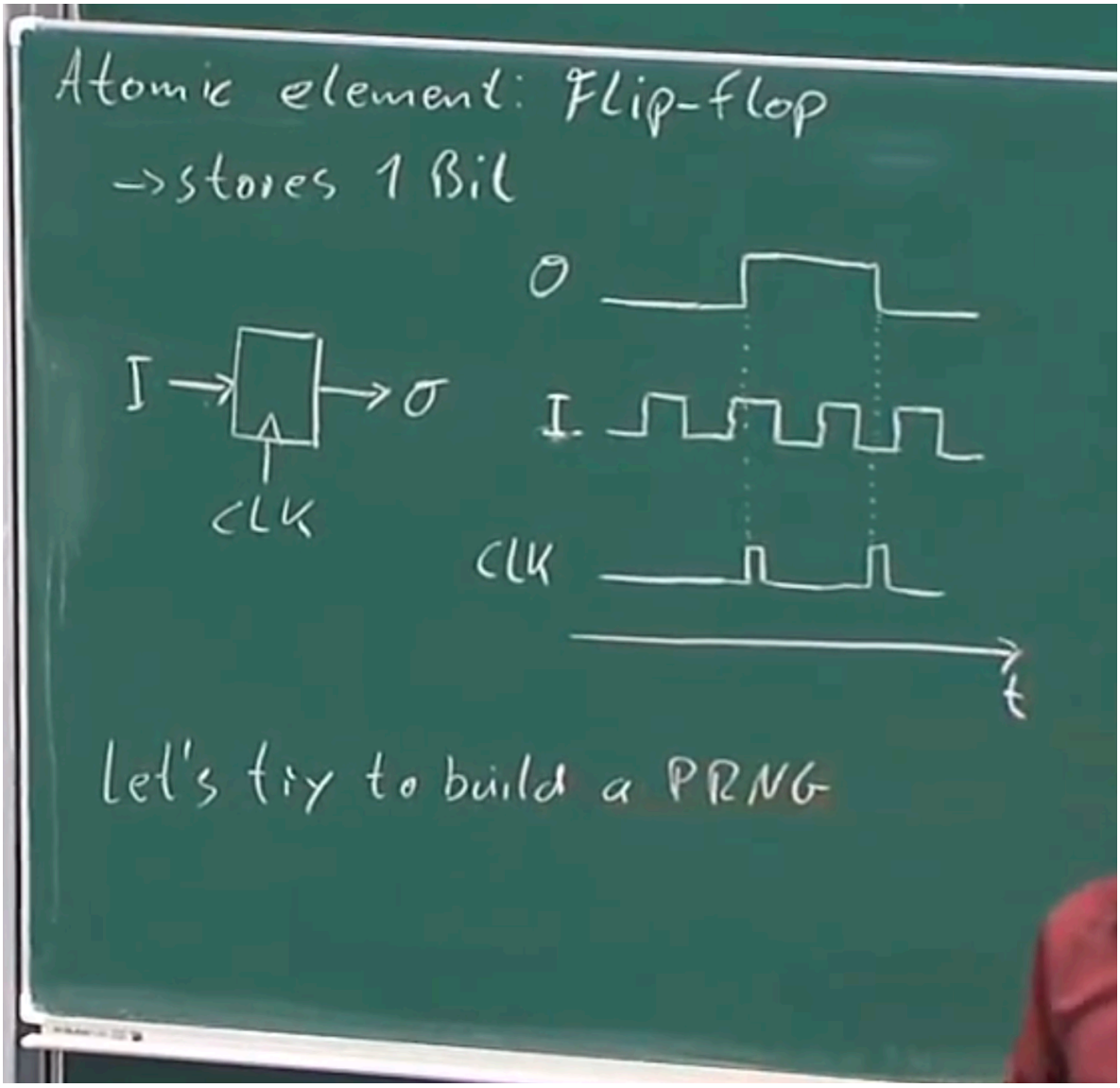
Agenda :-

1. **Intro to LFSR**
2. **General LFSR properties**
3. **Attacks**

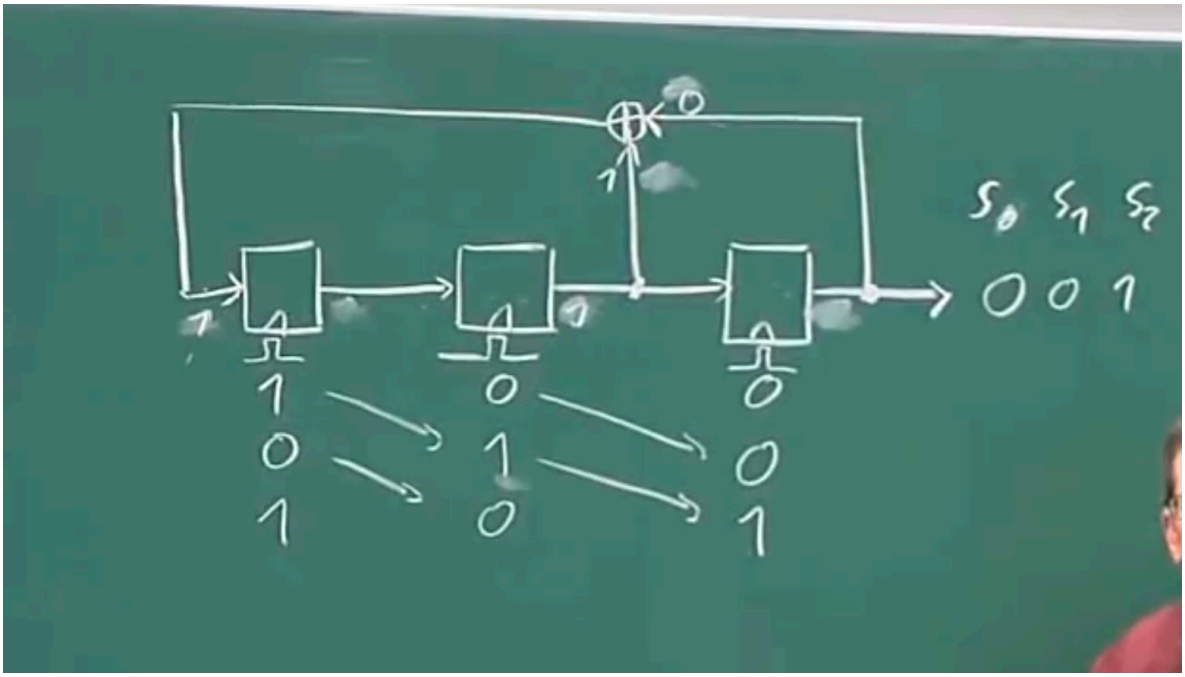
In Depth :-
Linear Feedback shift register :-
Actually we are taking about the Key Generation ie PRNG.
Stream Cipher that is small (Low Power) in hardware.
EX :- A5|1 Cipher in GSM consists of 3 LFSR's.

Flip Flops are the atomic element which stores the input when clock is high or 1.

In below example, when clock is high it stores input(which is high) and give output as high and next time when clock is high and input is low output becomes low and stays until clock and input both are not high.



Let’s try to build a PRNG.



3rd : 1 1 0
4th : 1 1 1
5th : 0 1 1
6th : 0 0 1
7th : 1 0 0
After 7th computation, Cycle will repeat.

We will only consider the output of last flipflop, so
S0 = 0
S1 = 0
S2 = 1
S3 = 0
S4 = 1
S5 = 1
S6 = 1
S7 = 0

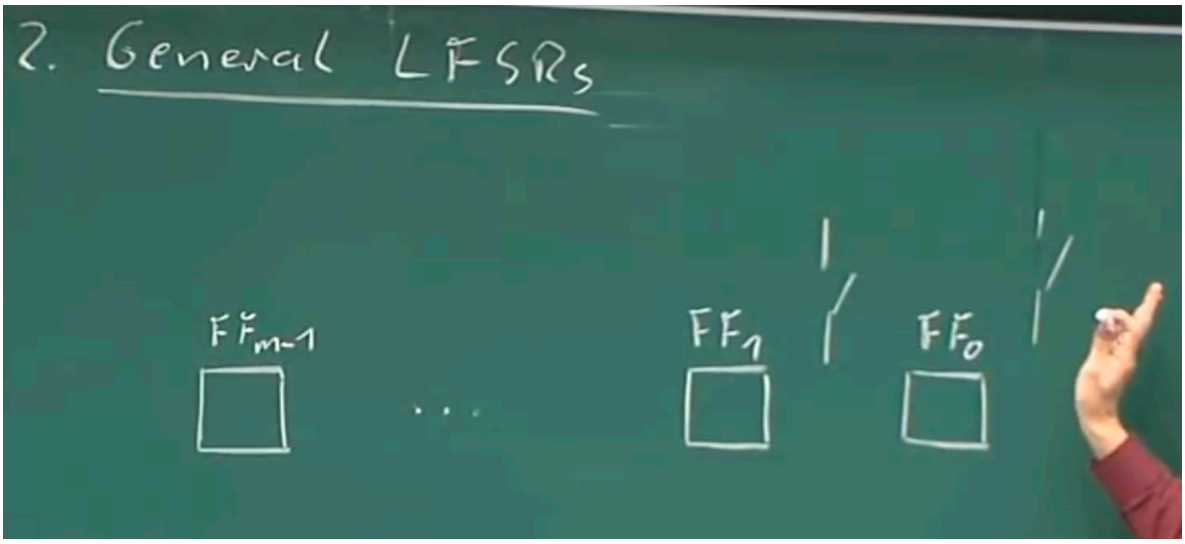
Little Mathematics :
S3 congruent to S1 + S0 mod 2
S4 = S2 + S1 mod 2
Si+3 = (Si+1)+ Si mod 2

Above LFSR is having a period of 7 but we want a period which is much larger than 7.
Also it is very easy to do that.

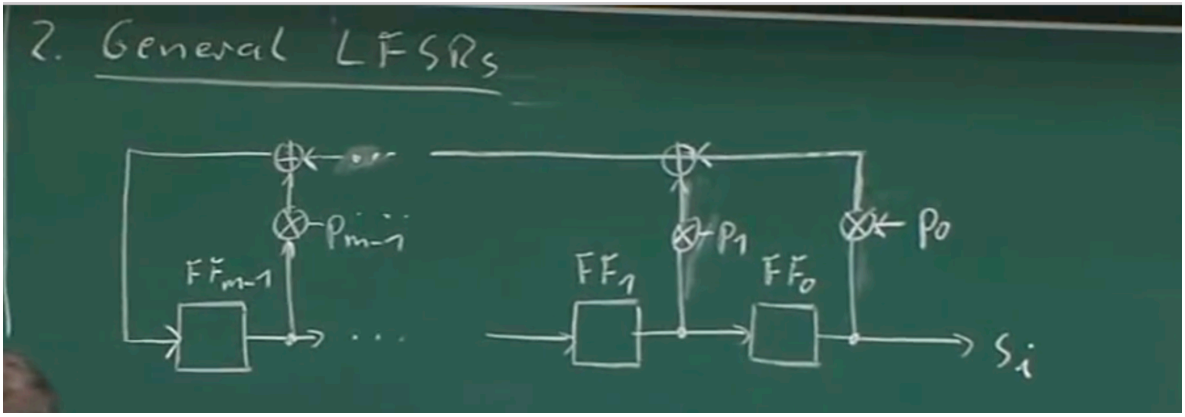
Chapter 2 :- General LFSR
Arbitrary number of LFSR's saying m.
In above design for 3 LSFR's we have only done the XOR for output of last 2

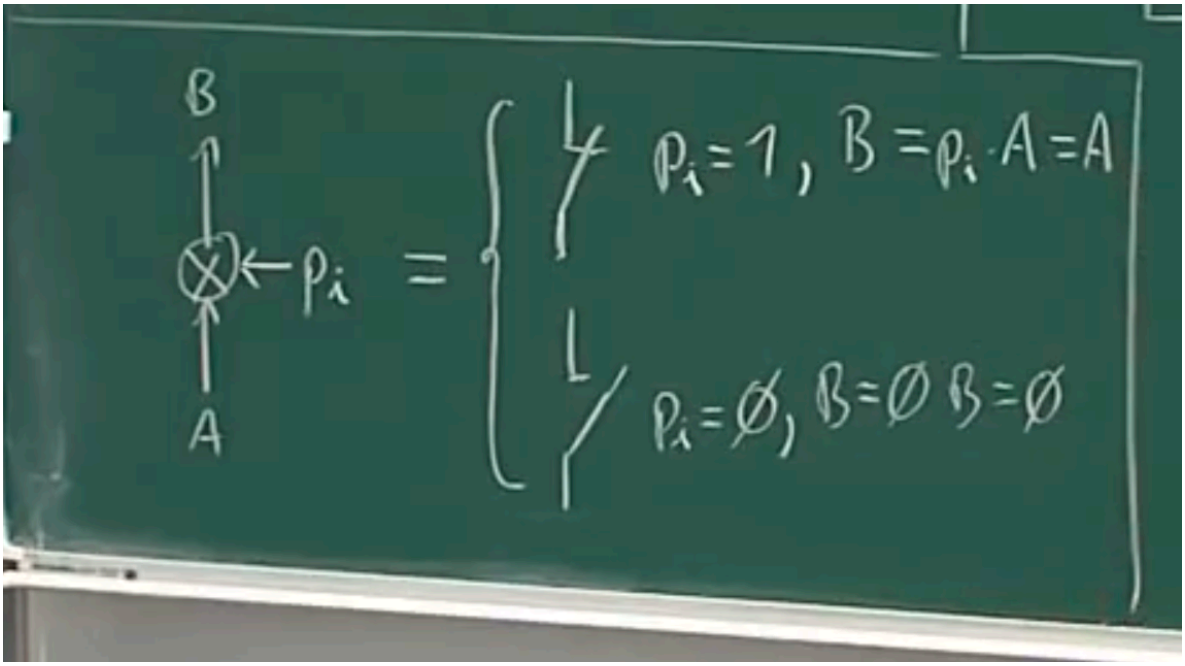
flip-flops but we could have done in any combination. So each one of the Flip Flops have fair chance of being feedback.

So we have something like a Switch at each flipflop which tells to include it or not in the feedback.
Eg :-

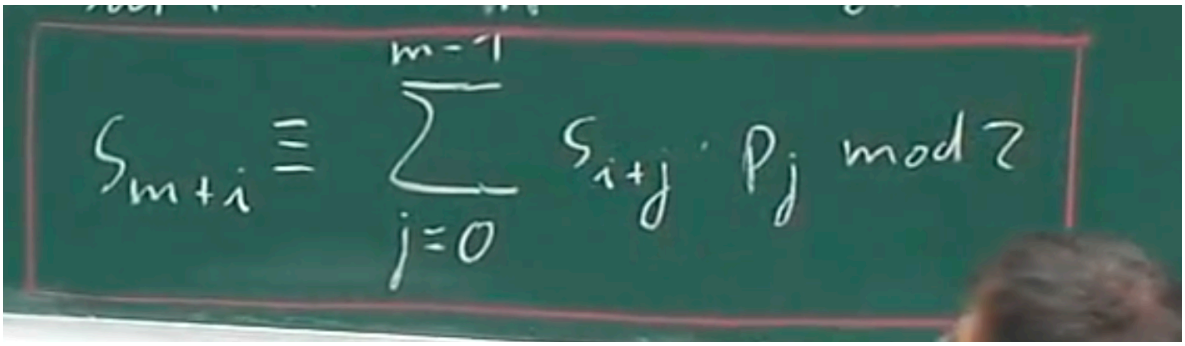


But for Mathematical notation we are introducing multiplier as it acts as a Switch.





Sm = Sm-1*pm-1 + Sm-2*pm-2 …. + S0*p0 mod 2
Sm+1 = Sm*pm-1 + sm-1*pm-2 …. + S1*p0 mod 2



Question :- where is Pj coming from. Plus choosing of initial state.
Answer :- you have to choose Pj. In GSM, Pj is fixed and it is a big choice for Designers.

Also depending on how you choosing Pj gives different properties.

Period ==> is there any relation of period and m (it is 2^m - 1)
Eg in case of 3 we got 2^3-1 => 7 (All Zero’s are missing)

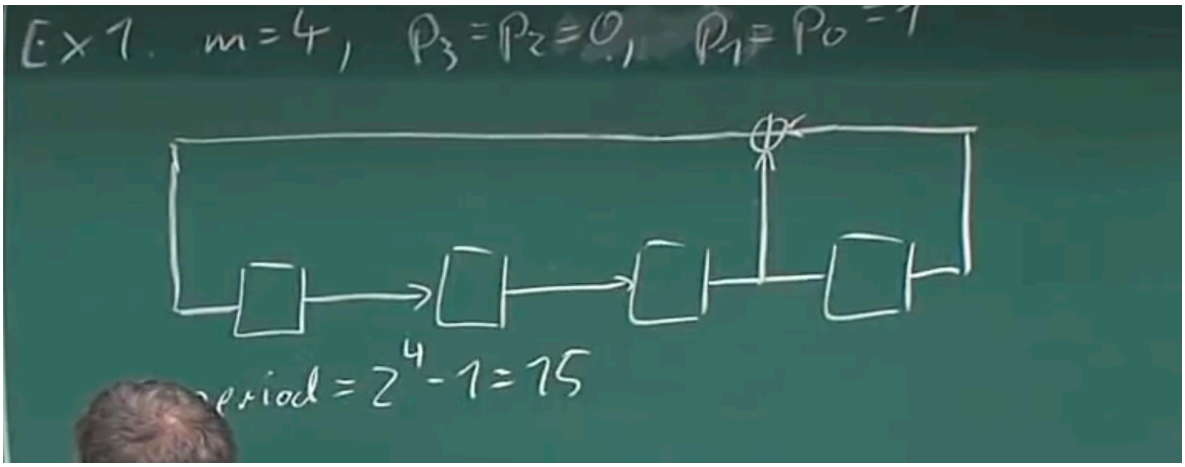
if you know one state, you can exactly tell the next state. As long as you hit the same state again then you would cycle around.
So the longest thing that can happen is 2^m - 1.

Theorem 1:-
Maximum sequence possible for LFSR with m flip-flops is 2^m -1

Theorem 2 :-

Only certain Configuration ie P values can yield maximum length sequence.

Eg 1:-
M = 4 , p3 = p2 = 0, p1 = p0 = 1

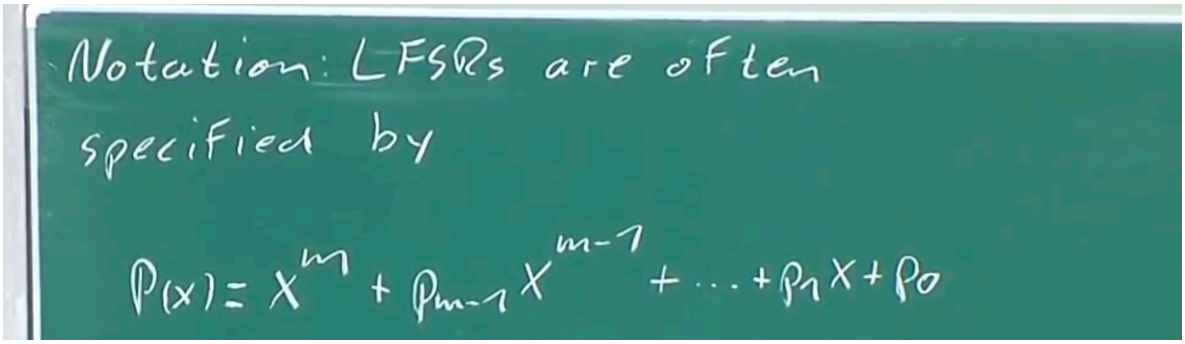


Above configuration gives period of 15

Eg 2:-
m = 4, p0 = p1 = p2 = p3 = 1
Period = 5
Eg:-
Thinking more :- say initial state is 1 0 0 0 > 1 1 0 0 > 0 1 1 0 > 0 0 1 1 > 0 0 0 1

Is there any logic behind this period ?
In GSM phones m is something in range of 19-23.

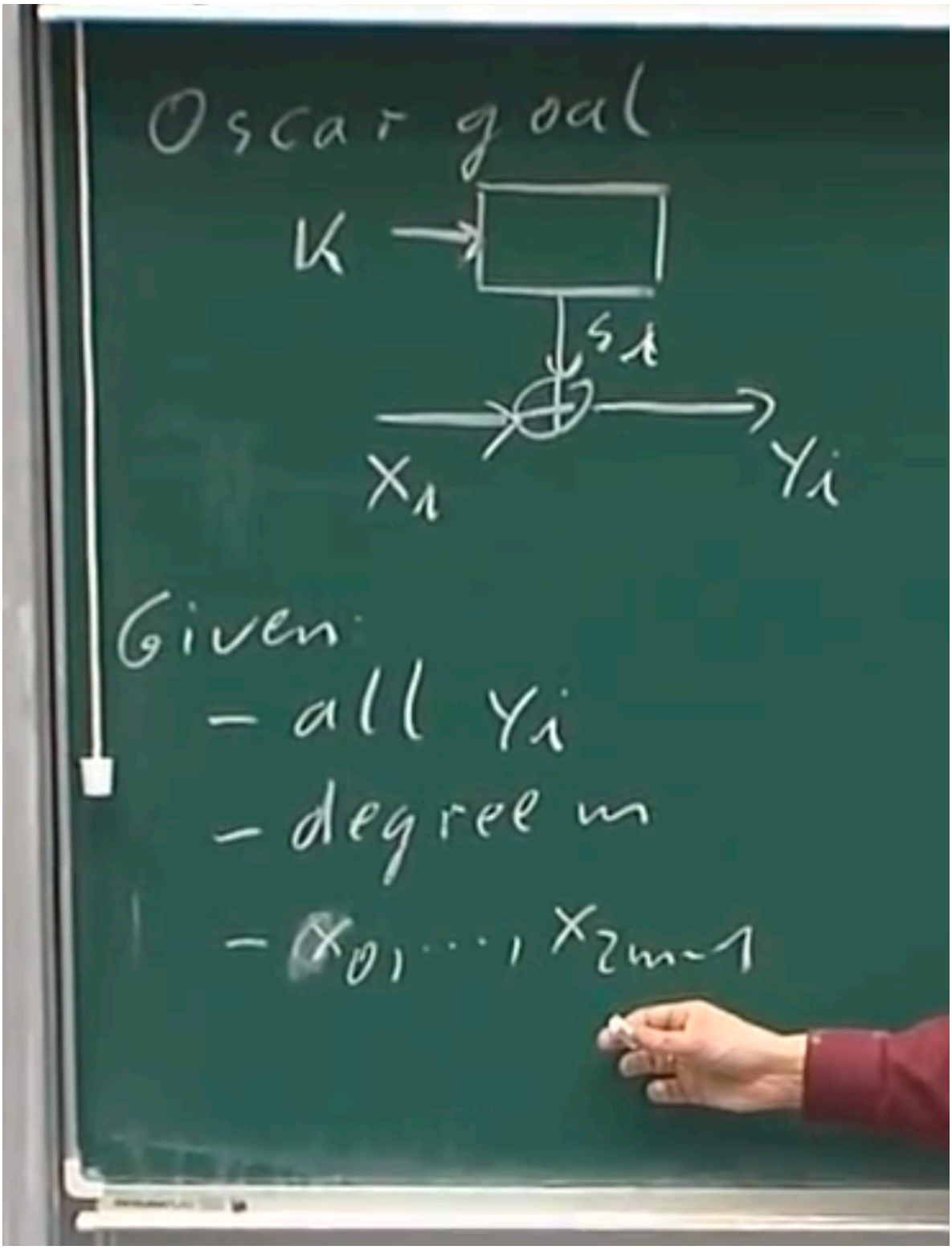
LFSR mathematical notation :-
Polynomial Equation := P(x) => x^m + p(m-1)*x^m-1 + ...
So for above diagram :- P(x) = x^4 + x^1 + 1 here P(x) => represent polynomial equation and doesn't correspond to p(x) (Small p)



Only LFSR of primitive polynomials yield maximum length sequences. Primitive polynomials are the once which cannot be factored.

Attacks on Single LFSR:-

Goal of Attacker (OSCAR) :-
To compute Si's.



Oscar knows all the cipher text and has somehow found degree m. Last assumption is little tough but as we know each type of file has headers which

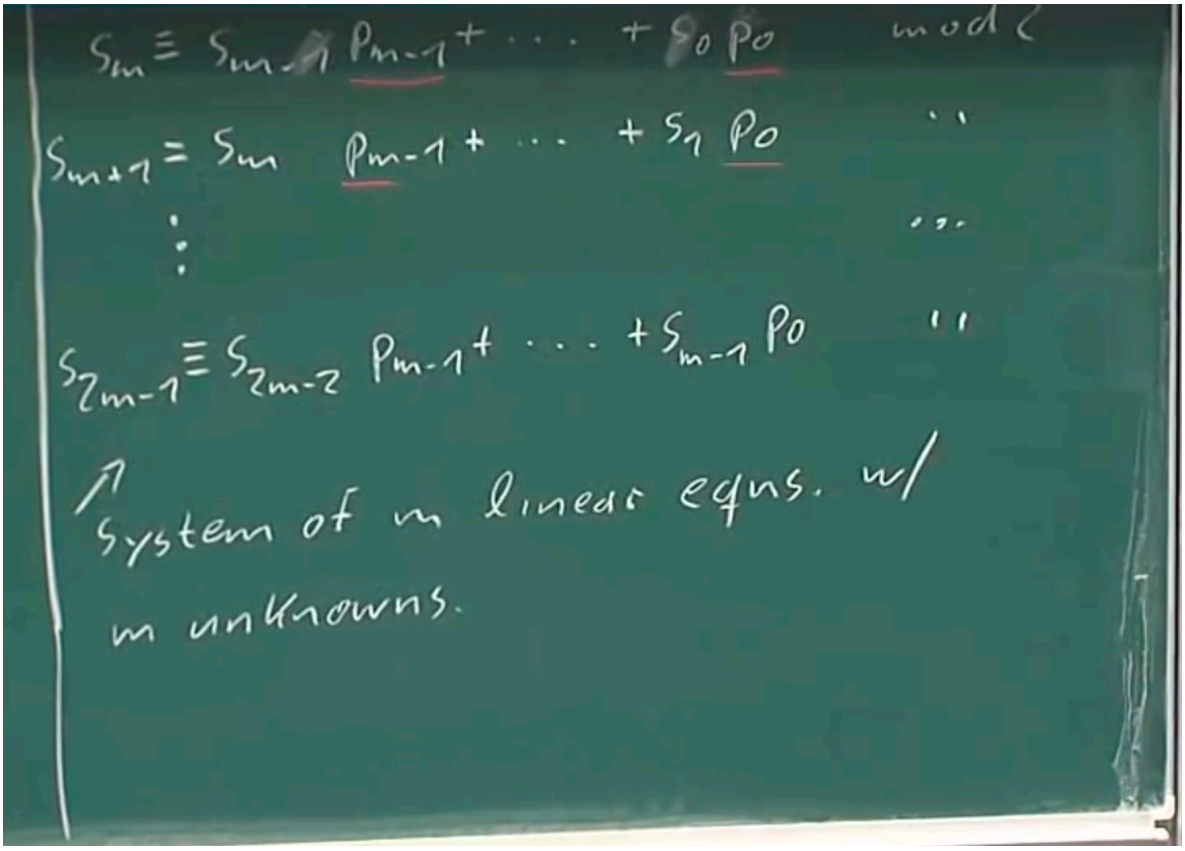
are same (Version of file, type of file etc.)

Yi = Xi + Si mod2
Si = Yi + Si mod2
For I from 0 to 2*m -1

Goal is to recover Si from 2*m to infinite :-
Now question is he knows Si but for computing all the Si's, he need to know pi's.
p0, p1, p2 ?
As we already assumed that we know the 2*m Si bits that means we can compute Pi's using equation :-

Sm = pm-1*sm-1 ... + p0s0
Sm+1 = ..

So as in above we have m equations and m unknowns so we can compute all the Pi's and after computing them we can create a LFSR and generate all the remaining Si and can decipher entire text.



Even we came to know that LFSR's are not secure but if we use them as building blocks and use more than once of them in combination, they become hard to break. Same thing GSM A51 cipher does.