LFSR weakness

LFSR are cryptographically weak because of the *Berlekamp-Massey* algorithm. Given a minimum length LFSR, say L (this length is called the *linear complexity* of the sequence), then if we know at LEAST 2L consecutive bits, Berlekamp Massey algorithm recovers the length L, the coefficients of the feedback polynomial and furthermore the initialization vector (the secret key basically) of the LFSR in O(L^2).
A possible way to overcom this attack is by using Boolean functions. Cryptosystems have to rely on two principles: *confusion* and *diffusion* which are closely related to the cryptographic complexity of Boolean functions. Diffusion consits in spreding out the influence of any minor modification of the plaintext or the key among the bits of all outputs. The resistance of the cryptosystem can be quantified through some characteristics of the Boolean functions. Some of those characteristics are affine invariant while some are not.

Algebraic Degree

First of all Bf must have high degree as otherwise we will have a low linear complexity of the LFSR and therefore we can easily factorize such value to recover sequences length

Nonlinearity

In order to provide confusion, cryptographic functions must lie at large Hamming distance to all affine functions. We say that there is a correlation between a Boolean function f and a linear (therefore affine) function l if $d_H(f, l)$ is different from 2^{n-1} (if it was 2^n this means that $f = l + 1$). As we've seen in Parseval's Relation using Walsh transforms of the f (i.e. Fourier transforms of the sign function of f) any Boolean function has some correlation with a linear function. Correlation and therefore affine approximations allows mounting attacks such as the *fast correlation attack*.

Suppose g is a linear approximation of the Boolean function f so $d_H(f, g) < 2^{n-1}$. The probability

$$p = Pr(f(x) \neq g(x)) = \frac{d_H(f, g)}{2^n} = \frac{1}{2} - \epsilon \tag{1}$$

with $\epsilon > 0$. Now the pseudo random sequence s generated with g is the transmission with errors of the sequence σ generated with f. Basically attacking the cipher can be done by correcting the errors in transmission over a noisy channel. Therefore the larger is the nonlinearity the larger is the probability p defined above, and so the less efficient is the attack. It must be high, and this is one of the most important cryptographic criteria. It is affine invariant since $d_H(f \circ L, l \circ L) = d_H(f, l)$ since L is an affine automorphism $L(x)$ gives every element of the vector space (field).
It can be compute using the Walsh transform of f:
we have $d_H(f, l) = 2^{n-1} - \frac{1}{2}W_f(l)$ in case the constant term of l is zero, while $d_H(f, l+1) = 2^{n-1} + \frac{1}{2}W_f(l)$. Therefore:

$$nl(f) = 2^{n-1} - \max_{l \in \mathbb{F}_2^n}\{|W_f(l)|\} \tag{2}$$

This is called the *covering radius bound*. Equality in (2) can be achieved $\iff$ $W_f(l) = 2^{\frac{n}{2}}$ $\forall$ l. Function reaching this equality are called *bent functions* whic obviously exist only for even values of n since $2^{n-1} - 2^{\frac{n}{2}-1}$ must be an integer. For n odd we can achieve nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$, these quadratic functions are called *semi-bent*, and their Walsh spectra only contain 0 and $2^{\frac{n+1}{2}}$. The maximum algebraic degree for a bent function f is $\frac{n}{2}$. Moreover we have that nonlinearity is larger for low degree functions. Indeed we have a great bound that says:

$$deg(f) \leq n - k + 1 \tag{3}$$

where k is the biggest such that $2^k | W_f(a) \forall a$

Balancedness

Cryptographic functions must be *balanced* in order to avoid statistical dependence between plaintext and ciphertext. It is easily seen that f is balanced if $w_H(f) = 2^{n-1} = \sum_{x \in F} f(x) = \sum_{x \in F} (-1)^0 f(x) = F_f(0)$ or else if $W_f(0) = F(f) = 0$. In the case of a combinig cipher the Boolean combining function must stay balanced if we fix some coordinates x_i. We say that an $n-variable$ function is $m-resilient$ if fixing m variables it is still balanced. This is related to the *correlation attack* .

Differential cryptanalysis

Also called $S-boxes$. They are part of iterative *blockciphers* and determine their robustness. Every round of such ciphers consist of vectorial Boolean functions ($v.B.f.$) combined in different ways. There are some attacks on v.B.f. that will define cryptographic criteria. The *differential attack* assumes the existence of ordered pairs (α, β) such that a block m of plaintext being randomly chosen and c and c' being the ciphertexts related to m and $m + \alpha$, the bitwise difference $c + c'$ has larger probability of being equal to β than if c and c' were randomly chosen. (α, β) is called a differential. The larger the probability of the differential the more efficient the attack is. The related criterion on a v.B.f. F used as S-box is that the output of the derivative $D_a(F) = F(x) + F(x + a)$ must be as uniformly distributed as possible.

Linear cryptanalysis

The *linear attack* is based on the distinguisher triple (α, β, γ) of binary strings such that, a block m of plaintext and a key k being randomly chosen, the bit $\alpha \cdot m + \beta \cdot c + \gamma \cdot k$ has probability different from $\frac{1}{2}$ of being null. The more distant from $\frac{1}{2}$ the probability is the more efficient is the attack. What we come up with is that the *component functions* (i.e. $v \cdot F = \sum_{i=1}^{m} v_i f_i$ where f_i are *coordinate functions* of F and $v \in \mathbb{F}_2^m$) must have the highest nonlinearity possible.

Balancedness

As for standard Boolean function *balancedness* is important fro v.B.f. in cryptography. We say that F is balanced if it takes every value of $\mathbb{F}_2^m$ the same number of times, i.e. 2^{n-m}. This means that $|F^{-1}(b)|$ must be equal $\forall b \in \mathbb{F}_2^m$. Obviously balanced $(n-n)$-functions are permutations over $\mathbb{F}_2^n$. Balancedness can be characterized through the component functions by saying that F is balanced if every component function is so.

Nonlinearity

The *nonlinearity* $nl(F)$ of a v.B.f. is the minimum nonlineatity of all the component functions of F. This quantifies the resistance of the S-box against lineat attacks. It is an affine invariant. The $coveringradiusbound$ is therefore still valid for v.B.f., i.e. $nl(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. F is said to be *bent* if it achieves the covering radius bound with equality. We notice that F is bent $\iff$ every component function is bent. This is because since $nl(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$ for a bent F and $\max_{l \in \mathbb{F}_2^n}\{|W_f(l)|\} \geq 2^{\frac{n}{2}}$ this is true only for equality in this disequality and therefore it is true for ever l.

Hence the *algebraic degree* of a bent v.B.f. is at most $\frac{n}{2}$.

We also have that a standard Boolean function is bent $\iff$ all of its derivatives $D_a(f) = f(x) + f(x+a)$ is balanced, therefore F is bent if all $v \cdot (F(x) + F(x + a))$ are balanced. Therefore we deduce that F is bent $\iff$ every of its derivative are balanced.

Due to the fact that bent functions are $perfect\ nonlinear$ and that derivatives are balanced they are strong against both linear and differential cryptanalysis. They exist for n even and $m \leq \frac{n}{2}$ (??).

- **Parseval's Relation**

$$\sum_{u \in \mathbb{F}_2^n, v \neq 0 \in \mathbb{F}_2^n} W_F^2(u, v) = 2^n(2^m - 1) \tag{4}$$

- **SCV bound**

For v.B.f. functions with $m > n-1 > \frac{n}{2}$ (therefore not bent) we can find a better upper bound for $nl(F)$, i.e. :

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \times 2^n - 2 - 2\frac{(2^n - 1)(2^{n-1})}{2^m - 1}} \tag{5}$$

Here $m \geq n - 1$ to avoid negative values under the square root. For $m = n - 1$ SVC is the covering radius.

A F with $m = n$ achieving SVC with equality is said $AlmostBent$

F v.B.f. and $delta > 0$ integer, we say that F is δ-$differentially\ uniform$ if $\forall a \in \mathbb{F}_2^n, a \neq 0$ and $\forall b \in \mathbb{F}_2^m$ the equation $D_a(F) = b$ has at most δ solutions, i.e.

$$\triangle_{a,b}(F) = |D_a(F)^{-1}(b)| \leq \delta \tag{6}$$

Obviously if F is bent (and therefore its derivatives are balanced) $\delta = 2^{n-m}$, and moreover there does not exist any 1-differentially uniform function. If $\delta \leq 2$ (0 or 2) we say that F is APN (*Almost Perfect Nonlinear*), therefore the smaller δ is the better is the resistance of F to differential cryptanalysis, while AB functions provide maximal resistance against both linear and differential. We have that every AB function is APN.

We say that F is *weakly-δ-differentially uniform* if $\forall a \neq 0$:

$$|Im(D_a(F))| > \frac{2^{n-1}}{\delta} \tag{7}$$

F is *weakly* APN if it is *weakly-2-differentially uniform*, i.e. $|Im(D_a(F))| > 2^{n-2}$.

Write

$$\hat{n}(F) = \max_{a \in \mathbb{F}_2^n, a \neq 0} |\{v \in \mathbb{F}_2^m | v \cdot D_a(F)\ is\ constant\}| \tag{8}$$

Basically, this is the number of vectors such that the component functions of the derivative in a of F is constant $\forall a$.

• **n=m=4**

Now we say that if F with $n = m = 4$ is *weakly* APN then $\hat{n}(F) \leq 1$ and moreover if F is APN then $\hat{n} \leq 1$ If F is a permutation with $n = m = 4$ then $nl(F) = nl(F^{-1})$