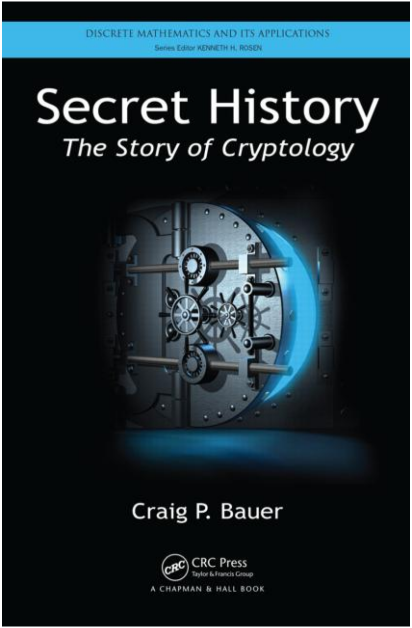


Image Source: Google

CSL 505
CRYPTOGRAPHY

Lecture 8
Differential Cryptanalysis
Finale
Single-to-Noise Ratio

Instructor
Dr. Dhiman Saha

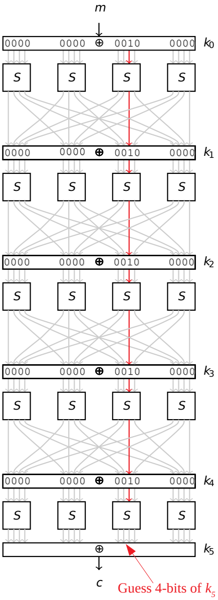
The Signal-to-Noise Ratio of Differential Cryptanalysis

$$S/N = \frac{m \cdot p}{m \cdot \alpha \cdot \beta \cdot 2^{-k}}$$

At the end of this lecture we will know what this means

Few Slides Earlier

The Underlying Distinguisher

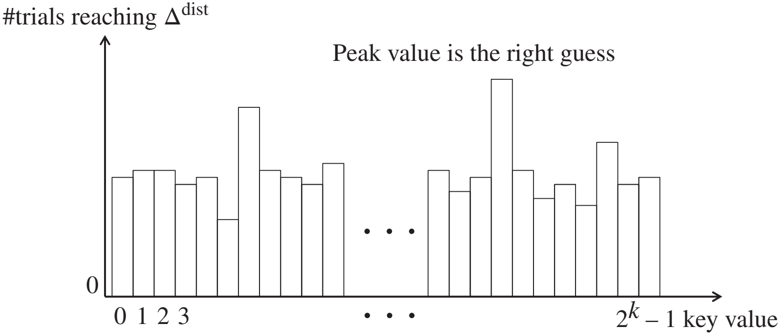


- Recall the characteristic (left fig) from the last lecture

Basic aim of DC

To identify a statistically unusual distribution in the differences that occur.

- We are building a distinguisher based on the devised characteristic
- Output difference helps in finding the (part of) right (sub) key
- What are the roadblocks that hinder this identifier/distinguisher?



Histogram of subkey guess reaching
the output difference in the characteristic

Right Vs Wrong

Definition (Right Pair)

Pair of messages that satisfy the (differential) characteristic

Definition (Wrong Pair)

Any pair that is **not** a Right Pair

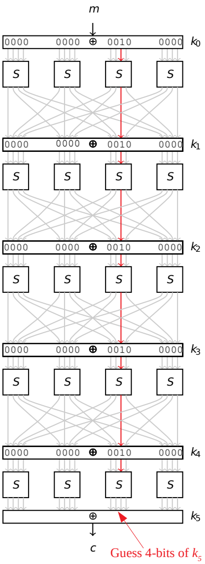
- i.e, they don't satisfy the (differential) characteristic

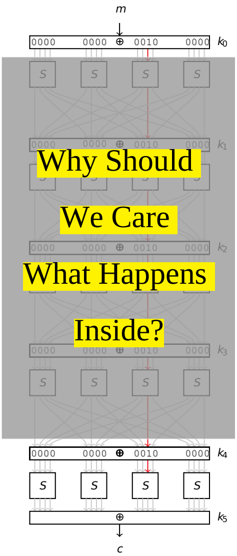
How to increase number of right pairs?

- Recall the idea of differentials.

Reacll

Characteristic Vs Differential





$$(0,0,2,0) \xrightarrow{R} (0,0,2,0) \xrightarrow{R} \cdots (0,0,2,0)$$

$$(0,0,2,0) \xrightarrow{R} ? \xrightarrow{R} ? \cdots ? \xrightarrow{R} (0,0,2,0)$$

- Multiple characteristics conforming to a differential
- Implication: Boosts the probability of getting right pairs

$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0).$$

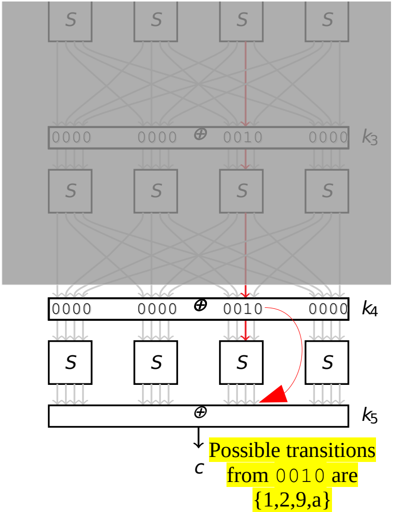
But it also contains at least three other possible characteristics. They are

$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,0,2) \xrightarrow{\mathscr{R}} (0,0,0,1) \xrightarrow{\mathscr{R}} (0,0,1,0) \xrightarrow{\mathscr{R}} (0,0,2,0),$$
$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,0,2) \xrightarrow{\mathscr{R}} (0,0,1,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0), \text{ and}$$
$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,0,2) \xrightarrow{\mathscr{R}} (0,0,1,0) \xrightarrow{\mathscr{R}} (0,0,2,0).$$

How to decrease number of wrong pairs?

- Recall the idea of filtering

Are all ciphertexts usable?



- Filtering?
- Note: Due to nature of output difference 12-bits in the difference of cipher-texts must be zero
- Moreover, ciphertexts leading to transitions impossible from 0010 can be discarded

Implication

Reduction in #Wrong-pairs

Four Possible Scenarios

- Let output difference of characteristic be Δ_{out}

Right Pair

- With right guess **always** satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Wrong Pair

- With right guess probabilistically satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Only one deterministic event $\rightarrow$ right pair $+$ right guess

Four Possible Scenarios

- Let output difference of characteristic be Δ_{out}

Right Pair

- With right guess **always** satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Wrong Pair

- With right guess probabilistically satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Only one deterministic event $\rightarrow$ right pair + right guess

Four Possible Scenarios

- Let output difference of characteristic be Δ_{out}

Right Pair

- With right guess **always** satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Wrong Pair

- With right guess probabilistically satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Only one deterministic event $\rightarrow$ right pair $+$ right guess

- Let output difference of characteristic be Δ_{out}

Right Pair

- With right guess **always** satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Wrong Pair

- With right guess probabilistically satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Only one deterministic event $\rightarrow$ right pair $+$ right guess

Four Possible Scenarios

- Let output difference of characteristic be Δ_{out}

Right Pair

- With right guess **always** satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

Wrong Pair

- With right guess probabilistically satisfies Δ_{out}
- With wrong guess probabilistically satisfies Δ_{out}

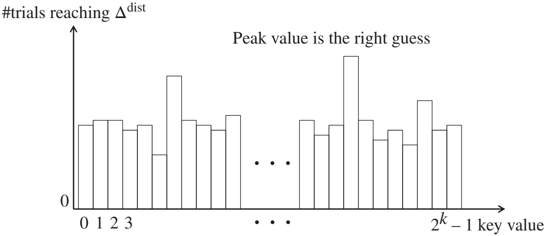
Only one deterministic event $\rightarrow$ right pair $+$ right guess

The Hypothesis

- The probability that the result of partial decryption probabilistically matches Δ_{out} is $\ll 1$.
- So, we analyze **many** pairs including right pairs and wrong pairs
- We believe the right guess reaches Δ_{out} more than any other wrong guess
- This allows the attacker to detect the right sub-key value.

How many is "many" ?

What factors determine the number of pairs to be analyzed.



- There might exist wrong key guesses that are close to the peak value.
- Moreover, the right guess might not be the peak value.

What then? **The Ranking Test**

Test several key candidates that are in a high position in the histogram.

Towards Signal-to-Noise Ratio

$\beta \leftarrow$ The filtering power

Filtering

The purpose of filtering is to remove the pairs that cannot satisfy the (differential) characteristic with probability 1.

- Employed to reduce wrong pairs
- Uses properties of the Sbox
- Eliminate by merely observing the ciphertext pair

Filtering Power (β)

The probability that a randomly generated ciphertext pair is a candidate of the one satisfying the (differential) characteristic is called **filtering power**

$$\beta = \frac{\#\ \text{Used pairs}}{\#\ \text{All pairs}}$$

Towards Signal-to-Noise Ratio

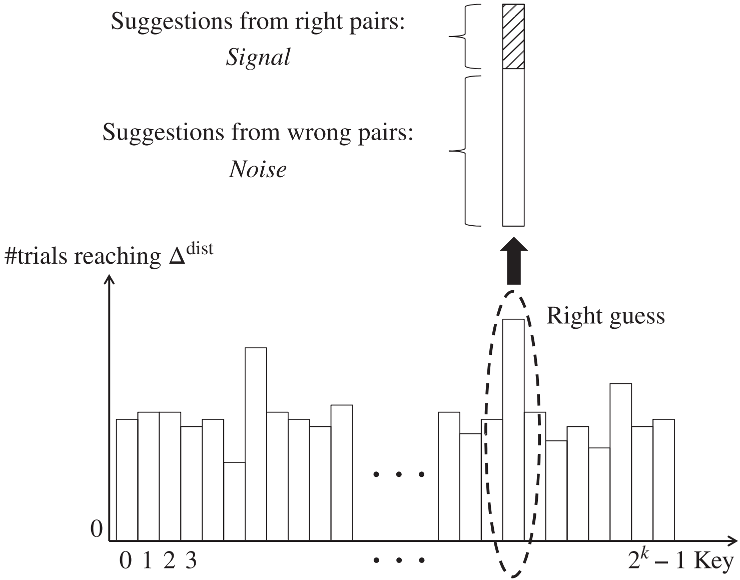
The parameter $\rightarrow \alpha$

α is the average number of keys suggested by each plaintext-pair

- This includes both right and wrong ones

- Recall the key-recovery strategy using the counters
- The table where T_i is calculated
- Every row had some '1's
- Denoting conformation to output difference of Sbox

Signal-to-Noise Ratio



Amount of Signal

Signal

Signal is the right key suggestion from right pairs

- For each right pair, the partial decryption with the right guess is performed once.
- Hence, the amount of signal is equal to the number of the right pairs.

If m pairs are queried and the probability of the characteristic is p, the amount of signal is

$$m \cdot p$$

Amount of Noise

Noise

Noise is the right key suggestion

- from wrong pairs or
- from right pairs with a the wrong guess.

- The number of pairs after filtering $m \cdot \beta$
- The total number of key suggestions from all pairs: $m \cdot \beta \cdot \alpha$
- If number of bits guessed in k, then the probability that a randomly generated suggestion is for the correct key is 2^{-k}

Amount of noise is given by: $m \cdot \beta \cdot \alpha \cdot 2^{-k}$

Definition

The signal to noise ratio is defined as the proportion of the probability of the correct key being suggested by a correct pair to the probability of a random key being suggested by a random pair with the input difference of the characteristic.

$$S/N = \frac{m \cdot p}{m \cdot \alpha \cdot \beta \cdot 2^{-k}} = \frac{p \cdot 2^k}{\alpha \cdot \beta}$$

In other words, it is the ratio of the number of good pairs and average number of counts of wrong subkeys

$$S/N = \frac{m \cdot p}{m \cdot \alpha \cdot \beta \cdot 2^{-k}} = \frac{p \cdot 2^k}{\alpha \cdot \beta}$$

- SNR is independent of the number of pairs used in the attack
- SNR is parameterized by the guessed key-size
- The number of **right-pairs** needed is a function of SNR
- If SNR is high enough, then few occurrences of right pair are needed to uniquely identify the key

The number of pairs needed is roughly $c \times \frac{1}{p}$, where $c \geq 1$ is a function of S/N

Proposition 3. *[Sel08] Let the correct key $\mathcal{K}_0$ of length k is among the top r values of key counters with probability P_s when a differential attack with characteristic probability p is mounted using M plaintext-ciphertext pairs and signal-to-noise ratio of S_N. Under the assumptions that the counters corresponding to the wrong keys are independent and follows an identical distribution, the value of k and M is too large, then M can be expressed as a function of the other variables by the following equation:*

$$M = \frac{(\sqrt{S_N + 1}\Phi^{-1}(P_s) + \Phi^{-1}(1 - 2^{log_2 r - k}))^2}{S_N} p^{-1}.$$

- Need roughly $M \approx 3 \cdot 1/p$ pairs if $SNR \gg 2$,
- Or $M \approx 30 \cdot 1/p$ if $1 < SNR \leq 2$.

[Sel08] Ali Aydin Selcuk *On Probability of Success in Differential and Linear Cryptanalysis*

Success of DC Attacks

- Success of differential attacks depends on
  - probability of (differential) characteristic
  - number of counters required (number of sub-key bits guessed)
  - S/N ratio
  - filtering
  - time to run the attack