Differential Cryptanalysis and Boolean Functions

Jana Barboriková

Department of Algebra
Charles University in Prague

March 28, 2010

Outline

- Differential cryptanalysis
  - History
  - Block Ciphers
  - Resistance
- Crosscorrelation and autocorrelation functions
- Propagation criterion

Introduction to Differential Cryptanalysis

- Differential cryptanalysis is the method that analyses the effect of particular differences in plaintext pairs on differences of the resultant ciphertext pairs
- It exploits the non-uniformity in the distribution of differences in the ouput pairs.
- chosen plaintext attack (known plaintext attack)
- applicable to block ciphers and hash functions

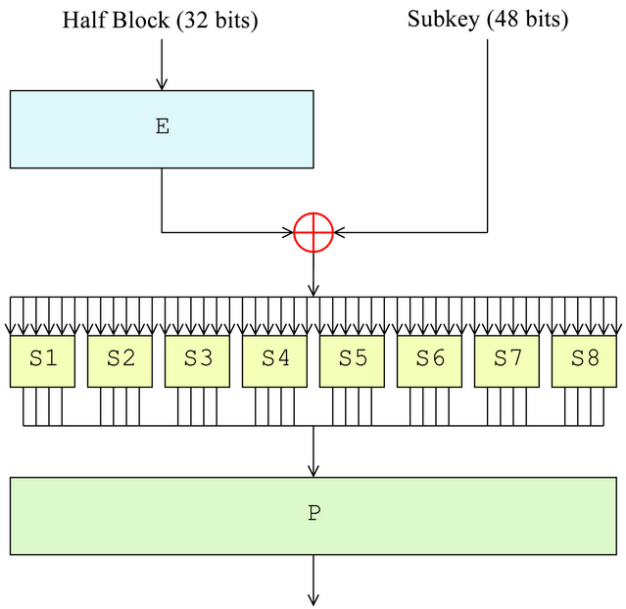
History

- CRYPTO'90 - formally introduced by Eli Birham and Adi Shamir
- 1991 - "Differential cryptanalysis of DES-like cryptosystems" - succesfull attack to weaken versions of DES (up to 15 rounds)
- other block ciphers - FEAL(up to 31 rounds), LOKI, IDEA
- full 16-round DES is surprisingly resistant to differential attacks
- 1994 - IBM - admitted that differential cryptanalysis was known to IBM since 1974, after discussion with the NSA they decided to keep it secret
- Modern ciphers are designed to resist to differential cryptanalysis with using appropriate non-linear operations.

Differential Cryptanalysis of Block Ciphers

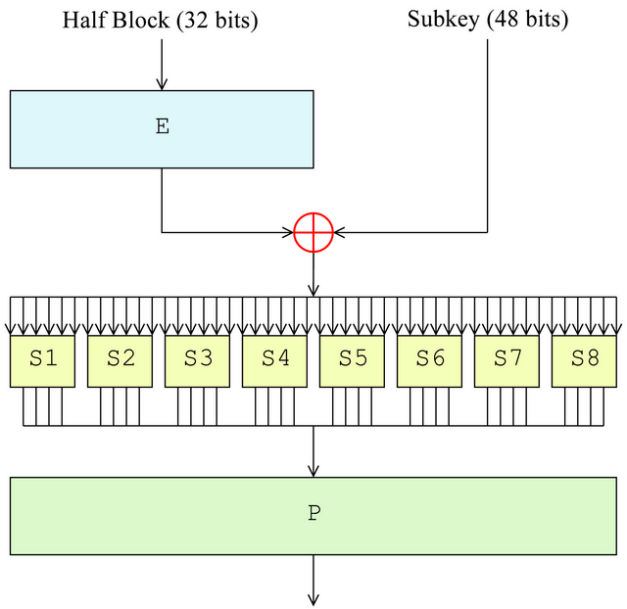
- The goal is to assign probabilities to the possible keys and to locate the most probable one.
- The method uses many pairs of plaintexts with the same particular difference.
- For DES-like cryptosystems the differences is chosen as a fixed XORed value of two plaintexts.

Differential Cryptanalysis of Single Round of DES



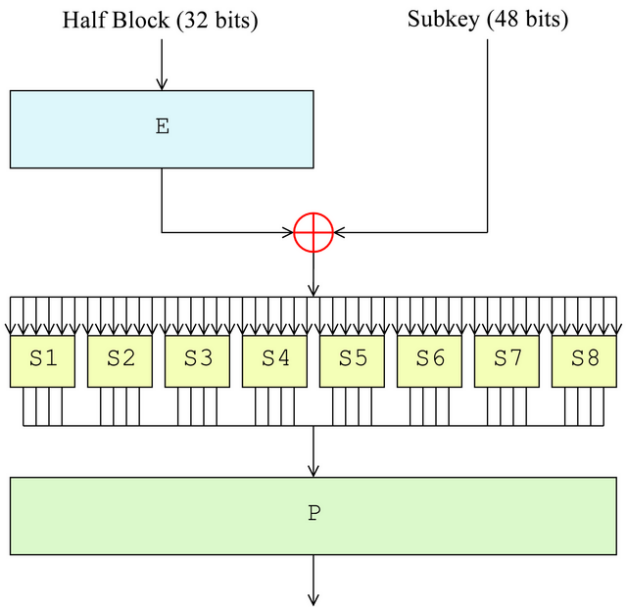
- the XOR of input pair is invariant in the XOR of round key and is linear in the expansion E, the permutation P and the XOR operation that connects the different rounds
- S boxes are non linear - knowledge of the XOR of the input pair cannot guarantee knowledge of the XOR of output pair.

Differential Cryptanalysis of Single Round of DES



- the XOR of input pair is invariant in the XOR of round key and is linear in the expansion E, the permutation P and the XOR operation that connects the different rounds
- S boxes are non linear - knowledge of the XOR of the input pair cannot guarantee knowledge of the XOR of output pair.

Differential Cryptanalysis of Single Round of DES



- the XOR of input pair is invariant in the XOR of round key and is linear in the expansion E, the permutation P and the XOR operation that connects the different rounds
- S boxes are non linear - knowledge of the XOR of the input pair cannot guarantee knowledge of the XOR of output pair.

Differential Cryptanalysis of Single Round of DES

Observation.

For any particular input XOR not all the ouput XORs are possible. The possible output XORs do not appear uniformly, some XORed values appear much more frequently.

- How can we get subkey bits from the S-box?

Differential Cryptanalysis of Single Round of DES

Observation.

For any particular input XOR not all the ouput XORs are possible. The possible output XORs do not appear uniformly, some XORed values appear much more frequently.

- How can we get subkey bits from the S-box?

Differential Cryptanalysis of Single Round of DES

- IDEA:

S-box: input and output XORs

$\Downarrow$

find the possible values of input and output pair

$\Downarrow$

find the subkey bits

- The method can be extended to find the whole subkey entering F function.

Differential Cryptanalysis of Single Round of DES

- IDEA:

S-box: input and output XORs

$\Downarrow$

find the possible values of input and output pair

$\Downarrow$

find the subkey bits

- The method can be extended to find the whole subkey entering *F* function.

Differential Cryptanalysis of Block Ciphers

Definition (informal).

Associated with any pair of encryptions are

- the difference of its two plaintexts
- the difference of its two ciphertexts
- the differences of the input of each round in the two executions
- the differences of the output of each round in the two executions

These values form an *n-round characteristic*.

A characteristic has a probability, which is the probability that a random pair (with the chosen plaintext difference) has the round and ciphertext differences specified in the characteristic.

Resistance to Differential Cryptanalysis

- Well-designed S-boxes can increase resistance of the cryptosystem to differencial attacks.
- The desirable properties of S-boxes are
  - nonlinearity
  - randomness of the differences of output pairs to differences of input pairs
- We will study following criteria:
  - nonlinear order
  - balancedness
  - propagation criterion

Resistance to Differential Cryptanalysis

- Well-designed S-boxes can increase resistance of the cryptosystem to differencial attacks.
- The desirable properties of S-boxes are
  - nonlinearity
  - randomness of the differences of output pairs to differences of input pairs
- We will study following criteria:
  - nonlinear order
  - balancedness
  - propagation criterion

Revision

Let f and g be binary Boolean functions $f, g : \mathcal{Z}_2^n \to \mathcal{Z}_2$

- Real-valued function $\hat{f} : \mathcal{Z}_2^n \to \mathcal{R}, \quad \hat{f}(x) = (-1)^{f(x)}$
- Inner product:

$$< \hat{f}(x), \hat{g}(x) >= \sum_{x \in \mathbb{Z}_2^n} \hat{f}(x)\hat{g}(x)$$

- Correlation between f and g:

$$C(f, g) = 2Pr_{x \in \mathcal{Z}_2^n}[f(x) = g(x)] - 1$$

- Walsh-Hadamard transform:

$$F(w) = \frac{1}{2^n} \sum_{x \in \mathbb{Z}_2^n} \hat{f}(x)(-1)^{w^t x}$$

Walsh-Hadamard transform of $\hat{f}$ can be also denoted by $\mathcal{W}(\hat{f})$.

Crosscorrelation Function

Definition

Let $\hat{f}$ and $\hat{g}$ be real-valued functions with domain $\mathbb{Z}_2^n$. The *crosscorrelation function* of $\hat{f}$ and $\hat{g}$ is the real-valued function over $\mathbb{Z}_2^n$ defined as

$$c_{\hat{f},\hat{g}}(s) = \frac{1}{2^n} \sum_{x \in \mathbb{Z}_2^n} \hat{f}(x).\hat{g}(x \oplus s)$$

.

- $c_{\hat{f},\hat{g}} = c_{\hat{g},\hat{f}}$
- $c_{\hat{f},\hat{g}}(s)$ is proportional to $C(f, g)$:

$$c_{\hat{f},\hat{g}}(s) = C(f(x), g(x \oplus s))$$

Autocorrelation Function

Definition

Let $\hat{f}$ be real-valued functions with domain $\mathbb{Z}_2^n$. The *autocorrelation function* of $\hat{f}$ is the real-valued function over $\mathbb{Z}_2^n$ defined as

$$r_{\hat{f}}(s) = \frac{1}{2^n} \sum_{x \in \mathbb{Z}_2^n} \hat{f}(x).\hat{f}(x \oplus s)$$

.

- $r_{\hat{f}} = c_{\hat{f},\hat{f}}$

Example 1.

- $f : \mathcal{Z}_2^2 \to \mathcal{Z}_2, \qquad f((x_1, x_2)) = \overline{x_1} \vee x_2$

$\mathbf{x_1}$	$\mathbf{x_2}$	$\overline{\mathbf{x_1}}$	$\mathbf{f(x)}$	$\hat{\mathbf{f}}\mathbf{(x)}$	$\mathbf{r_{\hat{f}}(x)}$
0	1	1	1	-1	0
0	0	1	1	-1	1
1	1	0	1	-1	0
1	0	0	0	1	0

$r_{\hat{f}}((0,1)) = \frac{1}{2^2} \sum_{a \in \mathbb{Z}_2^2} \hat{f}(a)\hat{f}(a \oplus (0,1)) = \frac{1}{4}[\hat{f}((0,1))\hat{f}((0,0)) + \hat{f}((0,0))\hat{f}((0,1)) + \hat{f}((1,1))\hat{f}((1,0)) + \hat{f}((1,0))\hat{f}((1,1))] = 0$

$r_{\hat{f}}((x_1, x_2)) = \overline{x_1 x_2}$

Example 2.

- $g : \mathcal{Z}_2^3 \to \mathcal{Z}_2, \qquad g((x_1, x_2, x_3)) = \overline{x_1}\ \overline{x_2}\ x_3 \vee x_1\ x_2\ \overline{x_3}$

$\mathbf{x_1}$	$\mathbf{x_2}$	$\mathbf{x_3}$	$\mathbf{\overline{x_1}\,\overline{x_2}x_3}$	$\mathbf{x_1x_2\overline{x_3}}$	$\mathbf{g(x)}$	$\mathbf{\hat{g}(x)}$	$\mathbf{r_{\hat{g}}(x)}$
1	0	1	0	0	0	1	0
1	1	0	0	1	1	-1	0
0	0	1	1	0	1	-1	0
0	1	0	0	0	0	1	0
1	0	0	0	0	0	1	0
0	1	1	0	0	0	1	0
1	1	1	0	0	0	1	1
0	0	0	0	0	0	1	1

Convolution Theorem

Theorem 1.(Convolution)

Let $\hat{f}$ and $\hat{g}$ be real-valued functions. Then

$$\mathcal{W}(c_{\hat{f},\hat{g}}) = \mathcal{W}(\hat{f}) \times \mathcal{W}(\hat{g})$$

, where $\times$ is pointwise product.

Proof.

Let $F = \mathcal{W}(\hat{f})$, $G = \mathcal{W}(\hat{g})$, $H = \mathcal{W}(c_{\hat{f},\hat{g}})$, then

$$F(w)G(w) = (\frac{1}{2^n} \sum_{a \in \mathcal{Z}_2^n} \hat{f}(a)(-1)^{w^T a})(\frac{1}{2^n} \sum_{b \in \mathcal{Z}_2^n} \hat{g}(b)(-1)^{w^T b})$$

Convolution Theorem

Proof.

$$= \sum_{a \in \mathcal{Z}_2^n} \sum_{b \in \mathcal{Z}_2^n} \frac{1}{2^{2n}} \hat{f}(a)\hat{g}(b)(-1)^{w^T(a \oplus b)}$$

Set $c := a \oplus b$, thus $b = a \oplus c$. Then

$$F(w)G(w) = \sum_{a \in \mathcal{Z}_2^n} \sum_{c \in \mathcal{Z}_2^n} \frac{1}{2^{2n}} \hat{f}(a)\hat{g}(a \oplus c)(-1)^{w^T c}$$

$$= \frac{1}{2^n} \sum_{c \in \mathcal{Z}_2^n} (\frac{1}{2^n} \sum_{a \in \mathcal{Z}_2^n} \hat{f}(a)\hat{g}(a \oplus c))(-1)^{w^T c}$$

$$= \frac{1}{2^n} \sum_{c \in \mathcal{Z}_2^n} c_{\hat{f},\hat{g}}(c)(-1)^{w^T c} = H(w)$$

□

Wiener-Khintchine Theorem

Theorem 2.(Wiener-Khintchine)

Let $\hat{f}$ be real-valued functions. Then

$$\mathcal{W}(r_{\hat{f}}) = \mathcal{W}(\hat{f})^2$$

Proof.

It follows directly from the *Convolution theorem*:

$$\mathcal{W}(r_{\hat{f}}) = \mathcal{W}(c_{\hat{f},\hat{f}}) = \mathcal{W}(\hat{f}) \times \mathcal{W}(\hat{f}) = \mathcal{W}(\hat{f})^2$$

□

Propagation Criterion

Definition

Let f be a Boolean function on n variables. Then f satisfies the *propagation criterion of degree k* $PC(k)$, $1 \leq k \leq n$, if $\hat{f}(x)$ changes with a probability of $\frac{1}{2}$ whenever i bits of x are complemented, $1 \leq i \leq k$.

- $PC(k)$ study what happens if the input of the function is modified
- satisfying $PC(k)$ implies that expected number of output changes with a probability of $\frac{1}{2}$ will not be small when k or less input bits are changed
- PC(k) generalizes the *Strict avalanche criterion* and the *perfect nonlinearity* - *SAC* is equals to $PC(1)$, perfect nonlinearity is equals to $PC(n)$

Propagation Criterion and Autocorrelation Function

There is a relation between $PC(k)$ and autocorrelation functions:

Proposition 1.

Let f be a Boolean function on n variables. Then

$$Pr_{x \in \mathcal{Z}_2^n}[\hat{f}(x) \neq \hat{f}(x \oplus s)] = \frac{1}{2} - \frac{r_{\hat{f}}(s)}{2}$$

Proof.

$$\begin{aligned} r_{\hat{f}}(s) &= C(f(x), f(x \oplus s)) = 2Pr_{x \in \mathcal{Z}_2^n}[f(x) = f(x\oplus)] - 1 \\ &= 2(1 - Pr_{x \in \mathcal{Z}_2^n}[f(x) \neq f(x \oplus s)]) - 1 \\ &= 1 - 2Pr_{x \in \mathcal{Z}_2^n}[f(x) \neq f(x \oplus s)] \\ &= 1 - 2Pr_{x \in \mathcal{Z}_2^n}[\hat{f}(x) \neq \hat{f}(x \oplus s)] \end{aligned}$$

□

Propagation Criterion and Autocorrelation Function

Now it is easy to restate $PC(k)$ in terms of the autocorrelation function:

Proposition 2.

Let f be a Boolean function on n variables. Then f satisfied $PC(k)$ iff

$$r_{\hat{f}}(s) = 0 \quad for \quad 1 \leq hwt(s) \leq k$$

Proof

It follows directly from *Proposition 1.* and definition of $PC(k)$. □

Example 3.

1. All Boolean functions f, $f : \mathcal{Z}_2^2 \to \mathcal{Z}_2$, that satisfy $PC(2)$:

$x_1\ x_2$	$x_1 \vee x_2$
$\overline{x_1}\ x_2$	$\overline{x_1} \vee x_2$
$x_1\ \overline{x_2}$	$x_1 \vee \overline{x_2}$
$\overline{x_1}\ \overline{x_2}$	$\overline{x_1} \vee \overline{x_2}$

2. Some Boolean functions f, $f : \mathcal{Z}_2^3 \to \mathcal{Z}_2$, that satisfy $PC(2)$:

$x_1\ x_2 \vee x_2\ x_3 \vee x_1\ x_3$	$\overline{x_1}\ \overline{x_2}\ \overline{x_3} \vee x_1\ x_2\ x_3$
$x_1\ x_2 \vee x_2\ \overline{x_3} \vee x_1\ \overline{x_3}$	$\overline{x_1}\ \overline{x_2}\ x_3 \vee x_1\ x_2\ \overline{x_3}$
$\overline{x_1}\ \overline{x_2} \vee x_2\ \overline{x_3} \vee x_1\ x_3$	$x_1\ \overline{x_2} \vee x_2\ \overline{x_3} \vee \overline{x_1}\ x_3$

Example 4.

We use *Proposition 2.* to check that the function f from *Example 1.* and the function g from *Example 2.* satisfy $PC(2)$:

- $f : \mathcal{Z}_2^2 \to \mathcal{Z}_2, \qquad f((x_1, x_2)) = \overline{x_1} \vee x_2$

f satisfies $PC(2)$ iff
$r_{\hat{f}}(s) = 0 \quad for \quad \forall s \in \mathcal{Z}_2^2 : \ 1 \leq hwt(s) \leq 2$

$hwt(s)$	s
0	(0,0)
1	(0,1), (1,0)
2	(1,1)

We know from *Example 1.*
$r_{\hat{f}}((0,0)) = 1$
$r_{\hat{f}}(s) = 0 \qquad \forall s \in \mathcal{Z}_2^2 \setminus \{(0,0)\}$
It implies that f satisfies $PC(2)$.

Example 5.

- $g : \mathcal{Z}_2^3 \to \mathcal{Z}_2, \qquad g((x_1, x_2, x_3)) = \overline{x_1}\ \overline{x_2}\ x_3 \vee x_1\ x_2\ \overline{x_3}$

g satisfies $PC(2)$ iff
$r_{\hat{g}}(s) = 0 \quad for \quad \forall s \in \mathcal{Z}_2^3 : \ 1 \leq hwt(s) \leq 2$

$hwt(s)$	s
0	(0,0,0)
1	(0,0,1), (0,1,0), (1,0,0)
2	(1,1,0), (1,0,1), (0,1,1)
3	(1,1,1)

We know from *Example 2.*
$r_{\hat{g}}(s) = 1 \qquad \forall s \in \{(0,0,0),(1,1,1)\}$
$r_{\hat{g}}(s) = 0 \qquad \forall s \in \mathcal{Z}_2^3 \setminus \{(0,0,0),(1,1,1)\}$
It implies that g satisfies $PC(2)$.

The End

Thank you for your attention:)