Linear Cryptanalysis and Boolean Functions

Michal Ferov

Department of Algebra
Faculty Of Mathematics and Physics
Charles University in Prague
Czech Republic

Spring School of Algebra
March 28. 2010

Outline

Let's start with a mathematical joke :)

There was a competition in constructing proofs in feminine logic.
The first price was won by random number generator.

What does it mean to break a cipher?

- It is not enough just to find what is in the message in order to break it. In some cases this can be done by statistical analysis.
- We want to obtain some useful information about the key (e.g. values of some bits or their combination).
- It is essential that that any attacker with reasonable computing power is unable to break the cipher from knowledge of plaitexts - ciphertext pairs.

What does it mean to break a cipher?

- It is not enough just to find what is in the message in order to break it. In some cases this can be done by statistical analysis.
- We want to obtain some useful information about the key (e.g. values of some bits or their combination).
- It is essential that that any attacker with reasonable computing power is unable to break the cipher from knowledge of plaitexts - ciphertext pairs.

What does it mean to break a cipher?

- It is not enough just to find what is in the message in order to break it. In some cases this can be done by statistical analysis.
- We want to obtain some useful information about the key (e.g. values of some bits or their combination).
- It is essential that that any attacker with reasonable computing power is unable to break the cipher from knowledge of plaitexts - ciphertext pairs.

Real life examples of attack scenarios.

- Cipher text only.
  I've found something, what is in there?
- Known plaintext.
  I know what is in there, does it help?
- Chosen plaintext.
  I can decide what is in there, I have the power, muhehehe...
- Chosen cipher text.
  I don't know what's inside, but I have a plan.

Real life examples of attack scenarios.

- Cipher text only.
  I've found something, what is in there?
- Known plaintext.
  I know what is in there, does it help?
- Chosen plaintext.
  I can decide what is in there, I have the power, muhehehe...
- Chosen cipher text.
  I don't know what's inside, but I have a plan.

Real life examples of attack scenarios.

- Cipher text only.
  I've found something, what is in there?
- Known plaintext.
  I know what is in there, does it help?
- Chosen plaintext.
  I can decide what is in there, I have the power, muhehehe...
- Chosen cipher text.
  I don't know what's inside, but I have a plan.

Real life examples of attack scenarios.

- Cipher text only.
  I've found something, what is in there?
- Known plaintext.
  I know what is in there, does it help?
- Chosen plaintext.
  I can decide what is in there, I have the power, muhehehe...
- Chosen cipher text.
  I don't know what's inside, but I have a plan.

Matsui's method

1993: Mitsuru Matsui - Linear Cryptanalysis method for DES Cipher
Suppose that the following equation holds with probability $p \neq \frac{1}{2}$.

$$P[i_1, \ldots, i_a] + C[j_1, \ldots, j_b] = K[k_1, \ldots, k_c]$$

Where:

P is the plaintext

C is the ciphertext

K is the key

$i_1, \ldots, i_a, j_1, \ldots, j_b, k_1, \ldots, k_c$ are some fixed bit locations

$$A[a_1, \ldots, a_n] = \sum_{k=1}^{n} A[a_k]$$

Matsui's method

- Let T be the number of plaintexts such that the left side of

$$P[i_1, \ldots, i_a] + C[j_1, \ldots, j_b] = K[k_1, \ldots, k_c]$$

is equal to zero.

- If $T > \frac{N}{2}$ (N is the number of plaintexts),
then guess $K[k_1, \ldots, k_c] = 0$ (when $p > \frac{1}{2}$) or 1 (when $p < \frac{1}{2}$),
else guess $K[k_1, \ldots, k_c] = 1$ (when $p > \frac{1}{2}$) or 0 (when $p < \frac{1}{2}$).

Matsui's method

- Let T be the number of plaintexts such that the left side of

$$P[i_1, \ldots, i_a] + C[j_1, \ldots, j_b] = K[k_1, \ldots, k_c]$$

  is equal to zero.

- If $T > \frac{N}{2}$ (N is the number of plaintexts),
  then guess $K[k_1, \ldots, k_c] = 0$ (when $p > \frac{1}{2}$) or 1 (when $p < \frac{1}{2}$),
  else guess $K[k_1, \ldots, k_c] = 1$ (when $p > \frac{1}{2}$) or 0 (when $p < \frac{1}{2}$).

What is important

Success rate of the Matsui's method increases with N and $\left|p - \frac{1}{2}\right|$.
Therefore we need the best linear expression ($\left|p - \frac{1}{2}\right|$ is maximal).
We need to:

1. Find effective linear expressions.
2. Find explicit description of the success rate by N and p.
3. Find the best expression and calculate the best probability.

Success rate estimates

Let N be the number of given random plaintexts and let p be the probability that equation

$$P[i_1, \ldots, i_a] + C[j_1, \ldots, j_b] = K[k_1, \ldots, k_c]$$

holds. Then the success rate of Matsui's method is

$$\int_{-2\sqrt{N}\left|p-\frac{1}{2}\right|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\, dx.$$

We show some numerical estimates.

N	$\frac{1}{4}\left\|p-\frac{1}{2}\right\|^{-2}$	$\frac{1}{2}\left\|p-\frac{1}{2}\right\|^{-2}$	$\left\|p-\frac{1}{2}\right\|^{-2}$	$2\left\|p-\frac{1}{2}\right\|^{-2}$
Success rate	84,1%	92,1%	97,7%	99,8%

Importance of nonlinearity in Boolean functions

What if the relationship between plaintext, ciphertext and key was linear?
Let's consider function

$$f(P,K)[i] = P[a_{i,1},\ldots,a_{i,b}] + K[c_{i,1},\ldots,c_{i,d}],$$

where $i,b,d \in \{1,\ldots,n\}$. Then all we need to do to obtain the key is to get n linearly independent plaintexts and their corresponding ciphertexts and solve n linear equations over $\mathbb{Z}_2$. It is obvious, that for the sake of cryptographic use we want the function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ as nonlinear as possible.

W-H spectrum as a measure of nonlinearity

What does the Walsh-Hadamard spectrum of a function tell us about its behavior?
Let's say we have function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. There are 2^n linear functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ (we will denote them $l_0, ..., l_{2^n-1}$). Then $W(f(a))$ is a real vector of correlation coefficients of f against those linear functions (i.e. $W(f)_i = C(f, l_i)$).
The worst case is that $W(f) = (0, \ldots, 0, \pm 1, 0, \ldots, 0)$, because that means that our function is linear(or affine in the negative case).
The ideal case is that the $m = \max_{i=0,\ldots,2^n-1}\{|W(f)_i|\}$ is small.

Example of invertible boolean transformation

Let's consider function $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$ with values defined in a table below.

a_1	a_2	a_3	$f_1(a_1, a_2, a_3)$	$f_2(a_1, a_2, a_3)$	$f_3(a_1, a_2, a_3)$
0	0	0	0	1	0
1	0	0	0	1	1
0	1	0	0	0	1
1	1	0	1	0	0
0	0	1	1	1	1
1	0	1	0	0	0
0	1	1	1	1	0
1	1	1	1	0	1

Algebraic normal form of this transformation is:

$$f_1(a_1, a_2, a_3) = a_3 + a_1 a_2 + a_1 a_3,$$
$$f_2(a_1, a_2, a_3) = 1 + a_2 + a_1 a_3 + a_2 a_3,$$
$$f_2(a_1, a_2, a_3) = a_1 + a_2 + a_3.$$

Correlation matrix of our $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$

Correlation matrix of $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$

	0	a_1	a_2	$a_1 + a_2$	a_3	$a_1 + a_3$	$a_2 + a_3$	$a_1 + a_2 + a_3$
0	1	0	0	0	0	0	0	0
f_1	0	0	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	0	0
f_2	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	0
$f_1 + f_2$	0	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0
f_3	0	0	0	0	0	0	0	1
$f_1 + f_3$	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$f_2 + f_3$	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0
$f_1 + f_2 + f_3$	0	$-\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	$\frac{1}{2}$	0

Note: f_3 is afine.

No. of differences	0	1	2	3	4	5	6	7	8
Corr. coef.	1	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{2}$	$-\frac{3}{4}$	-1

Correlation matrix of compositions of transformations

- $\sum_w C_{u,v} C_{v,w} = C_{u+v,0}$ i.e. correlation of linear combinations of function components defined by $u, v \in \mathbb{Z}_2^n$ is equal to convolution of columns u and v in the correlation matrix.
- Correlation matrix of composition two transformation is equal to product of their correlation matrices.

Correlation matrix of compositions of transformations

- $\sum_w C_{u,v} C_{v,w} = C_{u+v,0}$ i.e. correlation of linear combinations of function components defined by $u, v \in \mathbb{Z}_2^n$ is equal to convolution of columns u and v in the correlation matrix.
- Correlation matrix of composition two transformation is equal to product of their correlation matrices.

Characterization of invertible transformations

- A Boolean transformation h is invertible iff every linear combination of its component functions is a balanced function.
- Proof:
- $\Rightarrow$: If h is invertible transformation, then its correlation matrix C is orthogonal. Since $C_{0,0} = 1$ and all rows and columns have norm equal to 1, it follows that every other element in row 0 or column 0 is equal to 0. Hence, $C(u^T h(a), 0) = \delta(u)$ or $u^T h(a)$ is balanced for all $u \neq 0$.
- $\Leftarrow$: Output parities are balanced iff $C_{u,0}$ for $u \neq 0$. $C \times C^T = I$ iff $\sum_w C_{u,w} C_{v,w} = \delta(u+v)$ for all $u, v \in \mathbb{Z}_2^n$. We know that $\sum_w C_{u,v} C_{v,w} = C_{u+v,0}$. Since $C_{u,0} = 0$ for all nonzero u and $C_{0,0} = 1$, therefore the asserted condition holds for all u, v.

Characterization of invertible transformations

- A Boolean transformation h is invertible iff every linear combination of its component functions is a balanced function.
- Proof:
- $\Rightarrow$: If h is invertible transformation, then its correlation matrix C is orthogonal. Since $C_{0,0} = 1$ and all rows and columns have norm equal to 1, it follows that every other element in row 0 or column 0 is equal to 0. Hence, $C(u^T h(a), 0) = \delta(u)$ or $u^T h(a)$ is balanced for all $u \neq 0$.
- $\Leftarrow$: Output parities are balanced iff $C_{u,0}$ for $u \neq 0$. $C \times C^T = I$ iff $\sum_w C_{u,w} C_{v,w} = \delta(u+v)$ for all $u, v \in \mathbb{Z}_2^n$. We know that $\sum_w C_{u,v} C_{v,w} = C_{u+v,0}$. Since $C_{u,0} = 0$ for all nonzero u and $C_{0,0} = 1$, therefore the asserted condition holds for all u, v.

Characterization of invertible transformations

- A Boolean transformation h is invertible iff every linear combination of its component functions is a balanced function.
- Proof:
- $\Rightarrow$: If h is invertible transformation, then its correlation matrix C is orthogonal. Since $C_{0,0} = 1$ and all rows and columns have norm equal to 1, it follows that every other element in row 0 or column 0 is equal to 0. Hence, $C(u^T h(a), 0) = \delta(u)$ or $u^T h(a)$ is balanced for all $u \neq 0$.
- $\Leftarrow$: Output parities are balanced iff $C_{u,0}$ for $u \neq 0$. $C \times C^T = I$ iff $\sum_w C_{u,w} C_{v,w} = \delta(u+v)$ for all $u, v \in \mathbb{Z}_2^n$. We know that $\sum_w C_{u,v} C_{v,w} = C_{u+v,0}$. Since $C_{u,0} = 0$ for all nonzero u and $C_{0,0} = 1$, therefore the asserted condition holds for all u, v.

Elements of the correlation matrix are integer multiples of something

- Let C be a correlation matrix of a boolean transformation f with domain $\mathbb{Z}_2^n$. Then elements of correlation matrix of this transformation are integer multiples of 2^{1-n}.
- Proof:
- Recall that $C(f(a), w^T a) = 2^{-n} \sum_a \widehat{f}(a)(-1)^{w^T a}$.
  The sum on the right side is always even since it is of the form $k\dot{(}1) + (2^n - k)\dot{(} - 1) = 2k - 2^n$, therefore spectrum values must be integral multiples of 2^{1-n}

Elements of the correlation matrix are integer multiples of something

- Let C be a correlation matrix of a boolean transformation f with domain $\mathbb{Z}_2^n$. Then elements of correlation matrix of this transformation are integer multiples of 2^{1-n}.
- Proof:
- Recall that $C(f(a), w^T a) = 2^{-n} \sum_a \widehat{f}(a)(-1)^{w^T a}$.
  The sum on the right side is always even since it is of the form $k\dot{(}1) + (2^n - k)\dot{(} - 1) = 2k - 2^n$, therefore spectrum values must be integral multiples of 2^{1-n}

Wow, two proofs were done and nobody is sleeping! That needs another joke!

Question: What is the difference between real women and real numbers?

Answer: Real numbers are rational iff they have a period.

Who the hell would want to do this on something big?

- Usually ciphers consist of many functions that are somehow composed and it is much easier to study properties of these than of the whole function (e.g. rounds in DES with S-boxes).
- Also the correlation matrix is exponentially big and can be computed for n of reasonable size (e.g. 8-bit S-boxes in DES).

Who the hell would want to do this on something big?

- Usually ciphers consist of many functions that are somehow composed and it is much easier to study properties of these than of the whole function (e.g. rounds in DES with S-boxes).
- Also the correlation matrix is exponentially big and can be computed for n of reasonable size (e.g. 8-bit S-boxes in DES).

Linear trail of composition

Let β be an iterative transformation on n-bits vectors:

$$\beta = \rho^{(r)} \circ \ldots \circ \rho^{(1)}.$$

The correlation matrix of β is the product of the correlation matrices corresponding to the respective boolean transformations:

$$C^{(\beta)} = C^{(\rho^{(r)})} \times \ldots \times C^{(\rho^{(1)})}.$$

A linear trail U over an iterative Boolean transformation consists of a sequence of $r+1$ selection patterns:

$$U = \left(u^{(0)}, \ldots, u^{(r)}\right).$$

This linear trail is a sequence of of r linear steps $\left(u^{(i-1)}, u^{(i)}\right)$ that have a correlation

$$C\left({u^{(i)}}^T \rho^{(i)}(a), {u^{(i-1)}}^T a\right).$$

What is it good for?

- The correlation contribution of a linear trail is the product of the correlation of all its steps:

$$C_p(U) = \prod_i C^{\rho^{(i)}}_{u^{(i)}u^{(i-1)}}$$

- Linear trail composition theorem:
  The correlation between output parity $u^T\beta(a)$ and input parity $w^T a$ of an iterated Boolean transformation with r rounds is the sum of the correlation contributions of all r-round linear trails U with initial selection pattern w and final selection pattern u:

$$C(u^T\beta(a), w^T a) = \sum_{u^{(0)}=w, u^{(r)}=u} C_p(U)$$

What is it good for?

- The correlation contribution of a linear trail is the product of the correlation of all its steps:

$$C_p(U) = \prod_i C^{\rho^{(i)}}_{u^{(i)}u^{(i-1)}}$$

- Linear trail composition theorem:
  The correlation between output parity $u^T\beta(a)$ and input parity w^Ta of an iterated Boolean transformation with r rounds is the sum of the correlation contributions of all r-round linear trails U with initial selection pattern w and final selection pattern u:

$$C(u^T\beta(a), w^Ta) = \sum_{u^{(0)}=w, u^{(r)}=u} C_p(U)$$

Thank you for being on hell of an audience!

Děkuji vám za pozornost!

Je vous remercie de votre attention!

Ďakujem vám za pozornosť!

Dziękuję za uwagę!