First – Divide, Then – Attack

Orr Dunkelman

Computer Science Department
Technion, Haifa 32000, Israel

November 29, 2002

Topics of the Talk

1. Motivation for this Methodology.
2. Basic Ideas.
3. The Boomerang Attack (Rectangle).
4. Differential-Linear Cryptanalysis.
5. Summary and Open Problems.
6. Questions.

Differential Cryptanalysis

The *Differential Cryptanalysis* technique was presented by Biham and Shamir in 1990. The technique enables building a probabilistic distinguishers which are then used for attacking the block cipher.

The basic idea is to study the development of differences through the encryption function. We take two plaintexts (a pair) with some known difference, and try to predict the difference in the two ciphertexts. If our prediction is successful for a pair, this pair is called a right pair.

This information is usually statistical in nature, and thus, when we use the differential distinguisher, we need many plaintext pairs. If the probability of the differential is p, then we need $O(p^{-1})$ plaintext pairs for the attack.

Linear Cryptanalysis

The *Linear Cryptanalysis* technique was presented by Matsui in 1993. The technique enables building a probabilistic distinguishers which are then used for attacking the block cipher.

The basic idea is to study (probabilistic) linear approximations of the cipher. As most non-linear function are biased, we can find linear approximations with probability different than 1/2. By concatenating these approximations we can get a linear approximation between the plaintext and the corresponding ciphertext. By checking many plaintext/ciphertext pairs, we can deduce whether the approximation is mostly satisfied or not.

If the bias of the approximation is q (i.e., the approximation holds with probability $1/2 + q$) then we need $O(q^{-2})$ known plaintexts for the attack.

Motivation for the Methodology

Both methods can be used to theoretically break the Data Encryption Standard – DES.

Since the introduction of these techniques, most new ciphers which were presented tried to prove that they are immune to these techniques.

The basic method to "prove" security against these attacks (and their close variants) is to bound the probability of any differential and the bias of any approximation by some value which ensures that the data complexity of the attack is higher than the entire code book.

For example, for sufficiently large number of rounds of DES we can prove that the highest probability of any differential is no more than 2^{-63}. This means that any differential attack on DES would require at least 2^{63} pairs of chosen plaintexts, i.e., the entire code book.

Motivation for the Methodology (cont.)

Several techniques to bound these probabilities were introduced. It is worth mentioning two of these methods: The wide trail strategy and the decorrelation theory.

The wide trail strategy is based on forcing a small change to propagate and create an avalanche affect. For example, in Rijndael, changing the input of one S-box at the beginning, changes the input of all S-boxes after two rounds. The branch number of Rijndael is 5, meaning, that every two rounds has at least 5 active S-boxes. This ensures that any differential or linear properties, which we would like to exploit will require many active S-box.

The decorrelation theory, suggested by Serge Vaudenay, is based on minimizing the probabilities of any information leaking through several basic functions. The decorrelation ciphers use various functions to achieve security, e.g., XOR, addition modulo 2^n, multiplication modulo 2^n, etc.

The question is, whether these techniques ensure that the cipher is indeed immune to cryptanalysis.

COCONUT98

COCONUT98 was presented by Serge Vaudenay. It is a 64-bit block and a 256-bit key block cipher. The cipher is composed of 4 Feistel rounds, decorrelation module M and 4 more Feistel rounds.

Vaudenay has proven that through M (the decorrelation module) for any $x, y \neq 0$, the probability that $x \to y = 1/(2^{64} - 1)$ on average (over the key space). It also holds that the bias of any linear approximation passing through M is 2^{-32}.

This ensures that any differential attack or linear attack would require more data than the entire code book.

Conclusion: COCONUT98 is secure.

The question remains – Is that so?

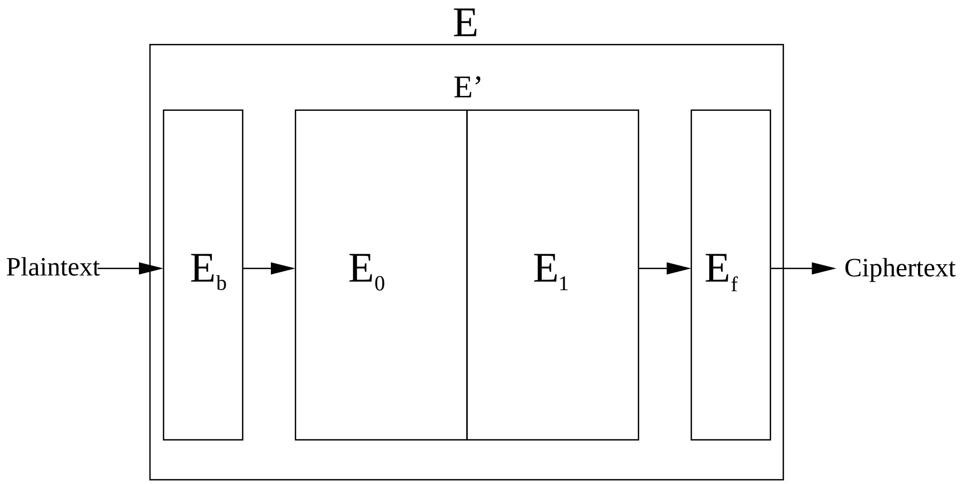
The Basic Idea

If you cannot beat them – divide them.

The Basic Idea (cont.)

We are going to treat the encryption function E as composed of 4 parts:
$E_1 \circ E_0$ are the core parts which are distinguished from random permutation using a statistical distinguisher. We will later treat E_0 and E_1 and show how to mount a distinguisher for them, using the fact that they are shorter than E.

E_b are the rounds before the core and E_f are the rounds after the core. These rounds are attacked using the various (and usually standard techniques) developed for using distinguishers in attacks.



The Boomerang Attack

The boomerang attack was introduced by Wagner in FSE '99. The attack is an adaptive chosen plaintext and ciphertext attack, which is based on two differential characteristics.

The attack treats the core of E under attack as a composition of E_0 and E_1. Let $\alpha \to \beta$ be a differential characteristic of E_0 with probability p, and let $\gamma \to \delta$ be a differential characteristic of E_1 with probability q.

- Ask for the encryption of a pair of plaintexts (P_1, P_2) such that $P_1 \oplus P_2 = \alpha$ and denote the corresponding ciphertexts by (C_1, C_2).
- δ-shift: Calculate $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$, and ask for the decryption of the pair (C_3, C_4). Denote the corresponding plaintexts by (P_3, P_4).
- Check whether $P_3 \oplus P_4 = \alpha$.

If the above holds, we assume both (P_1, P_2) and (P_3, P_4) are right pairs for the characteristic $\alpha \to \beta$, and that (C_1, C_3) and (C_2, C_4) are right pairs for the characteristic $\gamma \to \delta$.

The Boomerang Attack (cont.)

The probability for such a quartet to form a right quartet through a random permutation is 2^{-n}.

However, through $E' = E_1 \circ E_0$ the probability is $(pq)^2$.

As we can count on all β's and γ's, the real probability is

$$(\hat{p}\hat{q})^2,$$

where:

$$\hat{p} = \sqrt{\sum_{\substack{\beta \\ \alpha \to \beta}} \Pr{}^2[\alpha \to \beta]},$$

and

$$\hat{q} = \sqrt{\sum_{\substack{\gamma \\ \gamma \to \delta}} \Pr{}^2[\gamma \to \delta]}.$$

COCONUT98 and the Boomerang Attack

Wagner decomposed COCONUT98 into 2 parts – the first 4 Feistel rounds were treated as E_0, while the decorrelation module and the last 4 Feistel rounds were treated as E_1.

There is a high probability differential through E_0 (probability $2^{-4.3}$).

From symmetry arguments (the 4 Feistel rounds has the same functions in them), the same differential also holds through the last 4 Feistel rounds.

Luckily for us, the decorrelation module M satisfies that for any fixed key, for any input differential, its output differential is determined with probability 1. Knowing which of the $2^{64}-1$ possible differentials is the output difference is impossible.

However, for the boomerang attack this is sufficient to build a boomerang distinguisher for COCONUT98. The distinguisher requires about 3800 adaptive chosen plaintexts and ciphertexts to distinguish between the complete COCONUT98 and a random permutation.

The key recovery attack requires 60800 adaptive chosen plaintexts and ciphertexts, and retrieves the entire 256-bit key.

The Amplified Boomerang Attack

Kohno, Kelsey and Scheneir introduced the Amplified Boomerang Attack. The attack uses the same basic differential properties of the boomerang attack, but without using an adaptive chosen plaintext and ciphertext model.

We take many many plaintext pairs P_i, P_i^* s.t. $P_i \oplus P_i^* = \alpha$. We search for the cases where $E_0(P_i) \oplus E_0(P_i^*) = \beta$, and given many such pairs, we hope that for some i and j the intermediate encryption values satisfy that $E_0(P_i) \oplus E_0(P_j) = \gamma$. If we have sufficiently enough such i's and j's, then we expect that for some i' and j' we get $C_{i'} \oplus C_{j'} = C^*_{i'} \oplus C^*_{j'} = \delta$.

The "hoping" part is a probabilistic process, and has a very low probability. Denoting the block size of E in n, we get that the probability for a right quartet to be created in this way is $2^{-(n+1)/2}pq$.

Another problem is identifying the right quartets. As we encrypt pairs of plaintexts, and look for quartets of ciphertexts which satisfy that all 4 ciphertexts are from two plaintext pairs, the time complexity of the attack is very large.

The Rectangle Attack

Biham, Dunkelman and Keller introduced the Rectangle Attack. The attack is a combination of the amplified boomerang attack with the improvements which are applicable to the boomerang attack.
For example, we can use in the amplified boomerang attack in all the differentials for E_0 which start with α, and all the differentials in E_1 which end with δ in the attack.
Using these improvements increases the probability of a quartet to be a right quartet to $2^{-n/2}\hat{p}\hat{q}$. This reduces the data complexity of the attack significantly.

In a FSE'02 paper a new attack algorithm exploiting as much as possible the various relations in a right quartet was presented. The new technique reduces the time complexity of the rectangle attack on 10-round Serpent from 2^{217} memory accesses to **only** 2^{173} memory accesses. This improvement is achieved without changing the underlying distinguisher!
Similar techniques can be also applied to the boomerang attack, which enables overcoming the inherit problems an adaptive chosen plaintext and ciphertext attack oppose.

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis has been introduced by Langford and Hellman in CRYPTO '94. It combines a differential characteristic $\alpha \rightarrow \beta$ in E_0 with probability 1, with a linear approximation $\lambda_{inp} \rightarrow \lambda_{out}$ with bias q for E_1.

We ask for the encryption of two plaintexts (P_1, P_2) with input difference α, and check whether in the ciphertexts (C_1, C_2) it holds that:

$$\lambda_{out} C_1 = \lambda_{out} C_2$$

If in λ_{inp} all the active bits satisfy that β has in them a zero difference (i.e, $\beta \cdot \lambda_{inp} = \overline{0}$), then $\lambda_{inp} E_0(P_1) = \lambda_{inp} E_0(P_2)$. Thus, the equality we check for is satisfied with probability $(1/2 - q)^2 + (1/2 + q)^2 = 1/2 + 2q^2$. This means that the required data complexity is $O(q^{-4})$.

Enhancing Differential-Linear Cryptanalysis

The basic differential-linear attack can be enhanced to work with differentials $\alpha \rightarrow \beta$ which are satisfied with probability p. Moreover, we can also deal in the cases where $\beta \cdot \lambda_{inp} = \overline{1}$.

The basic idea, is to encrypt many pairs with the required input difference α. With probability p they satisfy the differential, and then, the output subset parity is biased as before. The full analysis shows that the probability that a pair in that case agrees on the output subset parity is $1/2 + 2pq^2$. The data complexity in that case is $O(p^{-2}q^{-4})$.

Note that we need to assume the following assumption (which is usually true) about the wrong pairs – they behave randomly with respect to the input subset mask.

A Summary of Results Obtained Using the Methodology

We shortly describe various results of the mentioned results:

Cipher	Attack	Number of Rounds	Complexity Data	Complexity Time
COCONUT98	Boomerang	all	60800	60800 MA
SC2000	Rectangle	3.5	$2^{83.6}$ CP	$2^{83.6}$ MA
	Boomerang	3	2^{41} ACPC	2^{40} MA
	Boomerang	3.5	2^{67} ACPC	2^{67} MA
Serpent	Differential	8	2^{84}CP	$2^{206.7}$
	Amp. Boomerang	9	2^{110} CP	2^{252} MA
	Boomerang	9	$2^{123.6}$ ACPC	$2^{122.6}$ MA
	Boomerang	10	$2^{126.3}$ CP	$2^{173.8}$ MA
	Rectangle	10	$2^{126.3}$ CP	$2^{173.8}$ MA
SHACAL-1	Differential	41	2^{141} CP	2^{491}
	Amp. Boomerang	47	$2^{158.5}$ CP	$2^{508.4}$
	Rectangle	49	$2^{151.9}$ CP	$2^{508.5}$
CAMELLIA	Boomerang	9		
	Rectangle	10		

A Summary of Results Obtained Using the Methodology (cont.)

Cipher	Attack	Complexity & Success		
		Data	Time	Rate
8-round DES	Differential	2^{14}CP	2^{9}	53%
	Linear	2^{18}KP	2^{25}	49.4%
	Differential-Linear	512CP	2^{14}	80%
	Differential-Linear	768CP	$2^{14.6}$	95%
	C.P. Linear Cryptanalysis	2^{16}CP	2^{23}	51%
	C.P. Linear Cryptanalysis	2^{17}CP	2^{24}	94%
	Enhanced Differential-Linear	$2^{14.8}$ CP	$2^{14.8}$	77.5%
9-round DES	Differential	2^{24}CP	2^{32}	99.97%
	Enhanced Differential-Linear	$2^{15.8}$ CP	$2^{29.2}$	88.8%
COCONUT'98 (full cipher)	Boomerang	2^{16}ACPC	2^{38}	99.96%
	Enhanced Differential-Linear	$2^{27.7}$CP	$2^{33.7}$	75.5%
11-round Serpent	Linear	2^{118}KP	$2^{205.7}$	
	Enhanced Differential-Linear	$2^{127.3}$CP	$2^{141.2}$	70.6%

Open Problems

Can anyone make the boomerang/rectangle attacks better?

Can anyone find other ways to combine differentials? approximations? differential and approximations together?

Three layers in the boomerang attack? Using octets in the boomerang attack?

Questions?