The "Divide and Attack"

Cryptanalysis Methodology

Orr Dunkelman

Computer Science Department
Technion, Haifa 32000, Israel

February 1, 2002

Topics of the Talk

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

Motivation for the Methodology

CRYPTO '91 - Differential Cryptanalysis is introduced.
EUROCRYPT '93 - Linear Cryptanalysis is introduced.
Implications: DES has been theoretically broken by attacks faster than exhaustive search.

CRYPTO '94 - DES is practically broken using linear cryptanalysis.
Since then several other improvements in the field of cryptanalysis have been presented:

- Truncated differentials.
- Higher order differentials.
- Linear Hulls.

Motivation for the Methodology (cont.)

Result: New ciphers are introduced with Maximal Differential Probability and Maximal Linear Probability.

If these two probabilities are low enough, both differential and linear attacks require more data than the entire code book, and thus, they are impractical.

Several techniques to bound these probabilities were introduced. It is worth mentioning the method used by Square-like ciphers which is based on the branching number of the mixing layer (wide trail strategy). Another technique was the decorrelation theory proposed by Vaudenay.

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

COCONUT98

COCONUT98 was presented by Serge Vaudenay. It has 64-bit block size and 256-bit key size. The cipher is composed of 4 Feistel rounds, decorrelation module M and again 4 Feistel rounds.
Vaudenay has proven that through M for any $x, y \neq 0$, the probability that $x \to y = 1/(2^{64} - 1)$ on average (over the key space).
Similar result can be proved for any linear approximation.
Conclusion: COCONUT98 is secure.

Really?

The Basic Idea

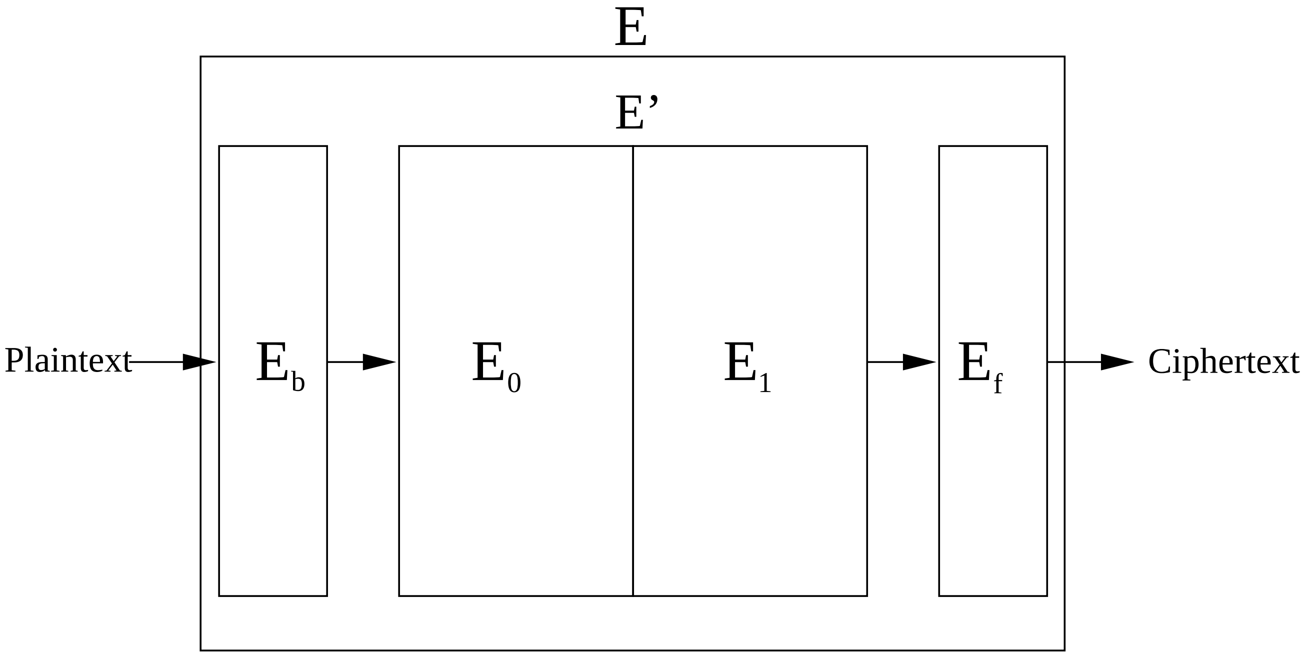
If you cannot beat them – divide them.

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 either a boomerang or a rectangle distinguisher.

E_b are the rounds before the core and E_f are the rounds after the core.



The Boomerang Attack

The boomerang attack was introduced by Wagner in FSE '99. The attack is an adaptive chosen plaintext-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, 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 a such 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 has for any fixed key some (unknown) differential with probability 1 which can be concatenated to the 4-round characteristic.

This way we can build a boomerang distinguisher with about 3800 chosen plaintexts. The key recovery attack requires 60800 chosen plaintexts for retrieving the entire 256-bit key.

The Rectangle Attack

Kohno, Kelsey and Scheneir introduced the Amplified Boomerang Attack. The amplified boomerang attack converts the adaptive chosen plaintext and ciphertext attack into a chosen plaintext attack.

However, in the amplified boomerang attack, the probability of a quartet to be a right quartet is only $2^{-(n+1)/2}pq$, and we have to try most of the possible quartets to find a right one.

Biham, Dunkelman and Keller introduced the Rectangle Attack. The probability of a quartet to be a right quartet is $2^{-n/2}\hat{p}\hat{q}$. Still, we have to try most of the quartets.

Comparing Boomerang and Rectangle Attacks

Attack	Rectangle	Boomerang
Cipher's parts being attacked	$E_f \circ E_1 \circ E_0 \circ E_b$	$E_1 \circ E_0 \circ E_b$
Type of Attack	Chosen Plaintext	Adaptive Chosen Plaintext and Ciphertext
Probability	$8 \cdot 2^{-n/2}\hat{p}\hat{q}$	$8(\hat{p}\hat{q})^{-2}$

10-round Serpent

To attack 10-round Serpent the following decomposition is used: The first round (round 0) is E_b, the next 4 rounds are E_0. Rounds 5-8 compose E_1 and round 9 is E_f.
For this decomposition the attack requires $2^{125.8}$ chosen plaintexts, with time complexity $2^{172.8}$ memory accesses.

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 $\Gamma_{inp} \rightarrow \Gamma_{out}$ with probability $1/2 + q$ in 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:

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

If in Γ_{inp} all the active bits are where β has zero difference (i.e, $\beta \cdot \Gamma_{inp} = \overline{0}$), then $\Gamma_{inp} E_0(P_1) = \Gamma_{inp} E_0(P_2)$. Thus, the equality we check for is satisfied with probability $(1/2 - q)^2 + (1/2 + q)^2 = 1/2 + 2q^2$.
This can be used to attack 8-round DES with about 768 chosen plaintexts.

Summary and Open Questions

Can anyone make the boomerang/rectangle attacks better? (Most recent result - this upcoming FSE).

Can anyone find other ways to combine differentials?

Three layers of boomerang attack? Using octet in the boomerang attack?

Questions?