The Rectangle Attack

and Other Techniques for Cryptanalysis of Block Ciphers

Orr Dunkelman

Computer Science Dept.

Technion

joint work with Eli Biham and Nathan Keller

Topics

- Block Ciphers
- Cryptanalysis of Block Ciphers
- Differential Cryptanalysis
- The Boomerang Attack
- The Rectangle Attack
- Summary & Questions

The Use of Block Ciphers

Block ciphers are used all around us:

- Security protocols – SSL, IPsec, etc.
- Security applications – PGP, Crypted file systems, etc.
- Digital Rights Management Systems
- Building block in other cryptographic primitives – stream ciphers, hash functions, message authentication codes (MACs)

Block Ciphers

- One of the basic cryptographic primitives
- Symmetric key primitive
- Many suggestions for a good block cipher
- Popular (and known) block ciphers:
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
  - IDEA, Blowfish, Serpent, ...
- Encryption speed – up to few Gbps

Block Ciphers (cont.)

- Pair of algorithms: Encryption and Decryption
- Each of them accepts blocks of plaintexts in a given size, e.g., 64 bits, 128 bits
- Each accepts keys
- Encryption defines a keyed transformation of all possible plaintexts into ciphertexts
- Decryption – just the opposite operation

Block Ciphers (cont.)

- Let E denote the encryption, and let D denote the decryption
- Let k denote the key, P the plaintext, and C the ciphertext

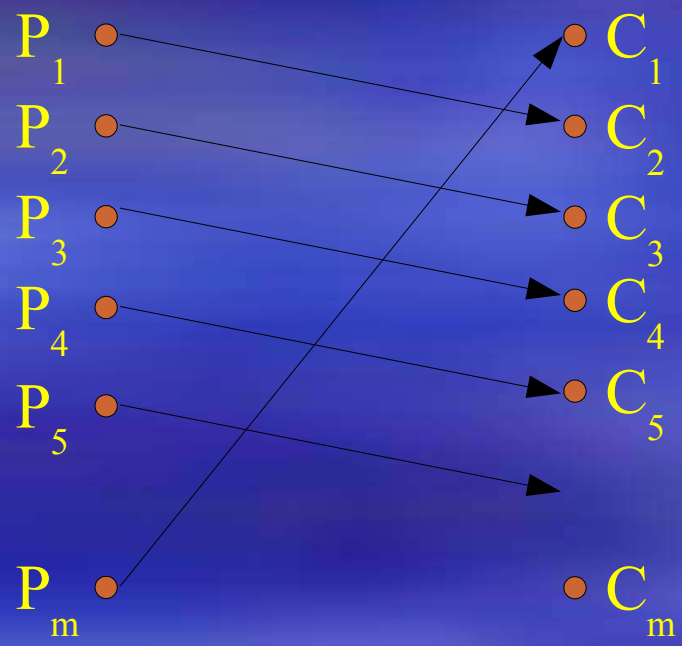
Then,

$$C=E_k(P),\ P=D_k(C),$$

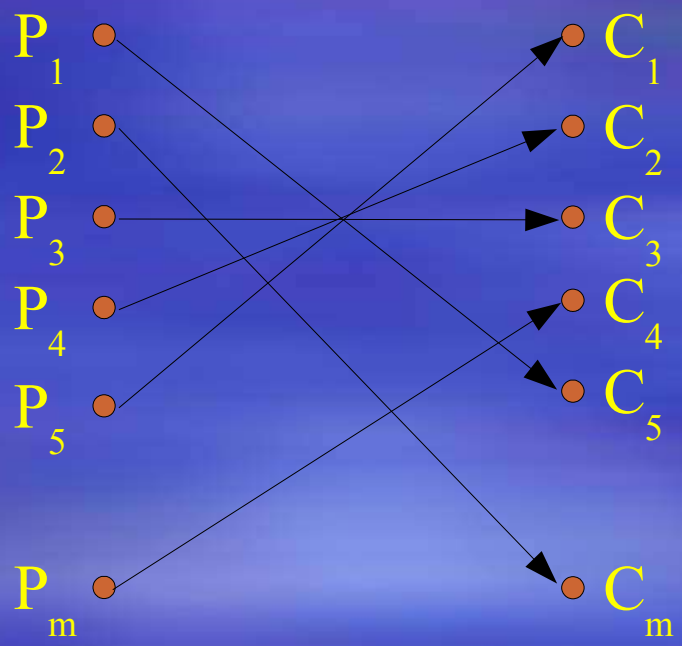
and $$P=D_k(E_k(P))$$

Block Ciphers (cont.)

Each key induces a permutation between the plaintexts and the ciphertexts



Under key k_1



Under key k_2

Iterated Block Ciphers

- Due to implementation issues, most block ciphers are iterated
- The encryption process is done in rounds, where a "small" permutation is applied
- The key is used to compute a set of subkeys using the key schedule algorithm

Formally:

$$C=R_{kr}(R_{kr-1}(\ldots R_{k2}(R_{k1}(P))\ldots))$$

Iterated Block Ciphers (cont.)

- All modern block ciphers are iterated
- Two basic constructions are the Feistel and the SP-Networks (SPNs)
- In the Feistel construction each round affects half of the data
- In the SPN construction, in each round all of the data is affected

Modes of Operation

What if we need to encrypt 250 bits using a block cipher of 128 bit block?

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Output FeedBack (OFB)
- Cipher FeedBack (CFB)
- Others, CTR

Cryptanalysis of Block Ciphers

Several basic assumptions:

- The encryption algorithm is known
- The abilities of the attacker are defined by the attack model:
  - Ciphertext only attack
  - Known plaintext attack
  - Chosen plaintext/ciphertext attack
  - Adaptive chosen plaintext (and ciphertext) attack

Cryptanalysis of Block Ciphers (cont.)

The "weird" attack models are valid because:

- A cipher secure against stronger attacker is still secure against weaker attacker
- History shows that these attacks can (and do) happen
- We have ciphers secure in the stronger models, why to use weaker ones?

What is a Broken Cipher?

There are several levels of "brokenness":

- Practical, easy to implement attack
- Close to practical attack
- Theoretical attack faster than any generic attack on the block ciphers (certificational attacks)

Why use ciphers that are theoretically broken, when we have ones that are not broken?

Generic Attacks

- Exhaustive key search
- Dictionary Attack
- Several time-memory tradeoffs, combining the above two approaches

Cryptanalysis Techniques

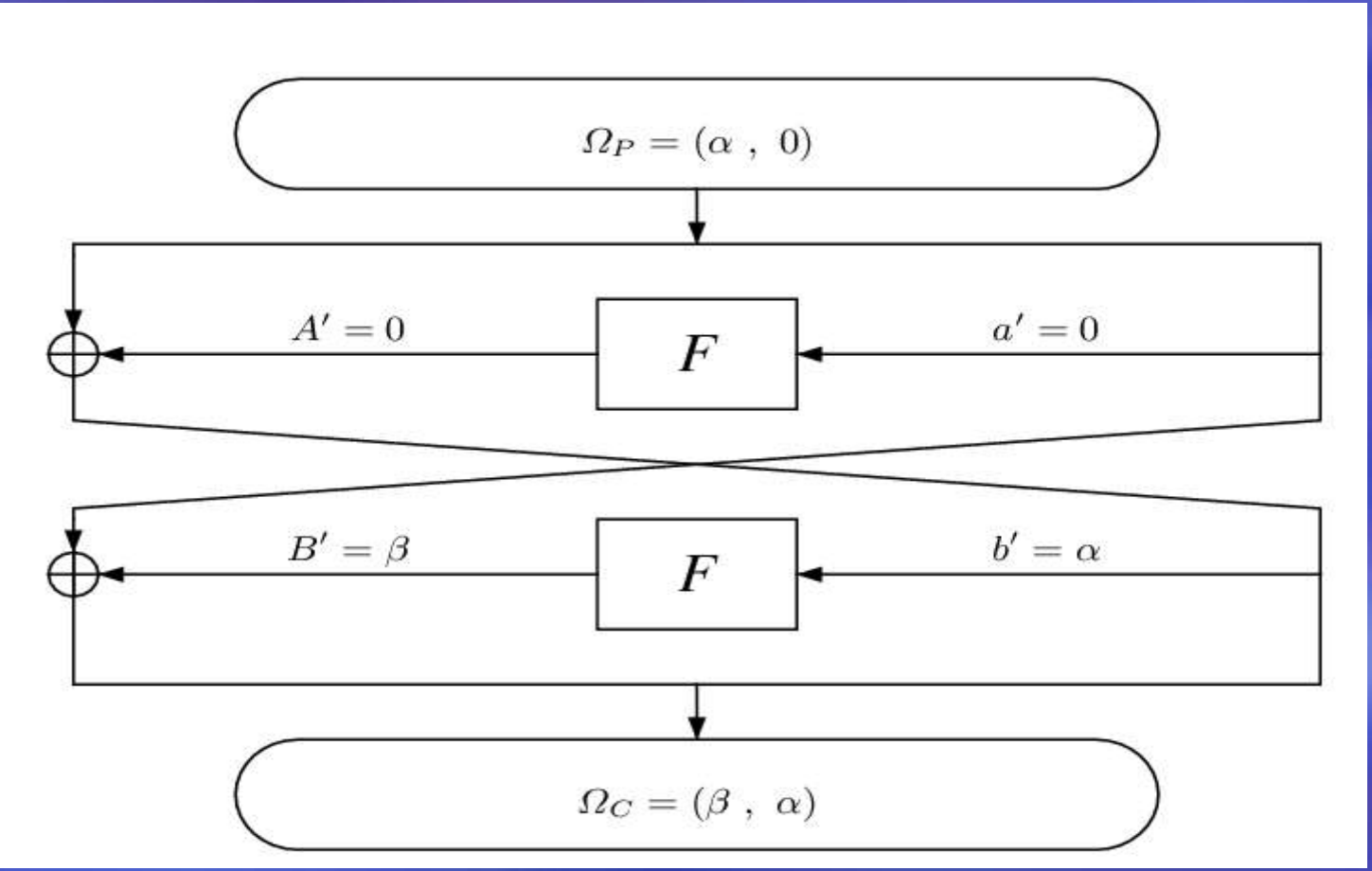
- Using bad mixture of data with key
- Statistical properties of the cipher
- Structural properties of the cipher
- Algebraic properties of the cipher

Differential Cryptanalysis

- Presented in 1991 by Biham and Shamir
- Studies the propagation of differences
- Can be used in one of several modes:
  1. Prediction – given two plaintexts with some XOR value, we can predict the XOR of the ciphertexts
  2. Distinguishing – take many plaintexts with the input difference, check how many satisfy the output difference
  3. Key Recovery – combine distinguishing with auxiliary techniques

Example of Differential Cryptanalysis

Consider two round Feistel



Example of Differential Cryptanalysis (cont.)

- By inspecting the relations between α and β we can find information on the round subkey
- By predicting with some probability p for a given α the value of β, we can mount other attacks as well

Differential Cryptanalysis (key recovery)

- Given a differential α -> β with probability p we need $O(1/p)$ plaintext pairs
- Once a pair for which the differential holds is found, we can use this pair to find the key
- This led designers to bound p to be as low as possible

Differential Cryptanalysis - Some Known Results

- Data Encryption Standard (DES) – 2^{47} chosen plaintexts
- Fast Encipherment Algorithm (FEAL) – 2 chosen plaintexts
- LOKI97 (AES candidate) – 2^{56} chosen plaintexts
- Can be used to attack hash functions as well (MD5, SHA-1, etc.)

The Cryptanalyst Problem

- New ciphers are “secure” against differential cryptanalysis
- Avalanche criteria, Wide trails, and other techniques make sure the differentials have low probability
- So, can't we break ciphers using differential cryptanalysis?

The Boomerang Attack

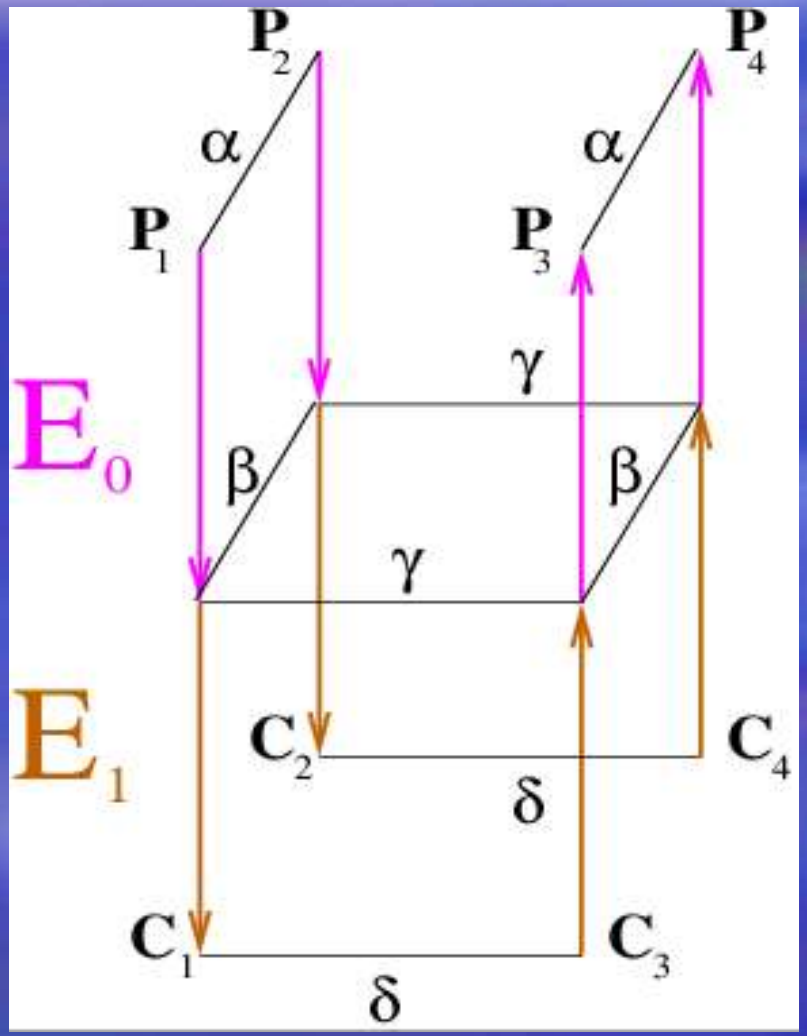
Presented in 1999 by Wagner

Main idea:

- Treat the cipher as a cascade of two sub-ciphers
- Use two differentials – one for each sub-cipher
- Combine the two differentials using some structure

The Boomerang Attack (cont.)

- For the first sub-cipher we use the differential $\alpha \rightarrow \beta$ with probability p.
- For the second sub-cipher we use the differential $\gamma \rightarrow \delta$ with probability q.



The Boomerang Attack (cont.)

- The total probability of a quartet to become a right quartet is p^2q^2.
- Useful when there are good short differentials, but "bad" long differentials
- For example, there is no differential attack on 6-round AES, but there is a boomerang attack
- However, the main drawback is that this is an adaptive attack

The Boomerang Attack (cont.)

- Main problem – the attack is adaptive chosen plaintext and ciphertext (ACPC)
- Many of the good techniques developed through the years cannot be applied
- Some people don't think ACPC is a “good” attack

The Amplified Boomerang Attack

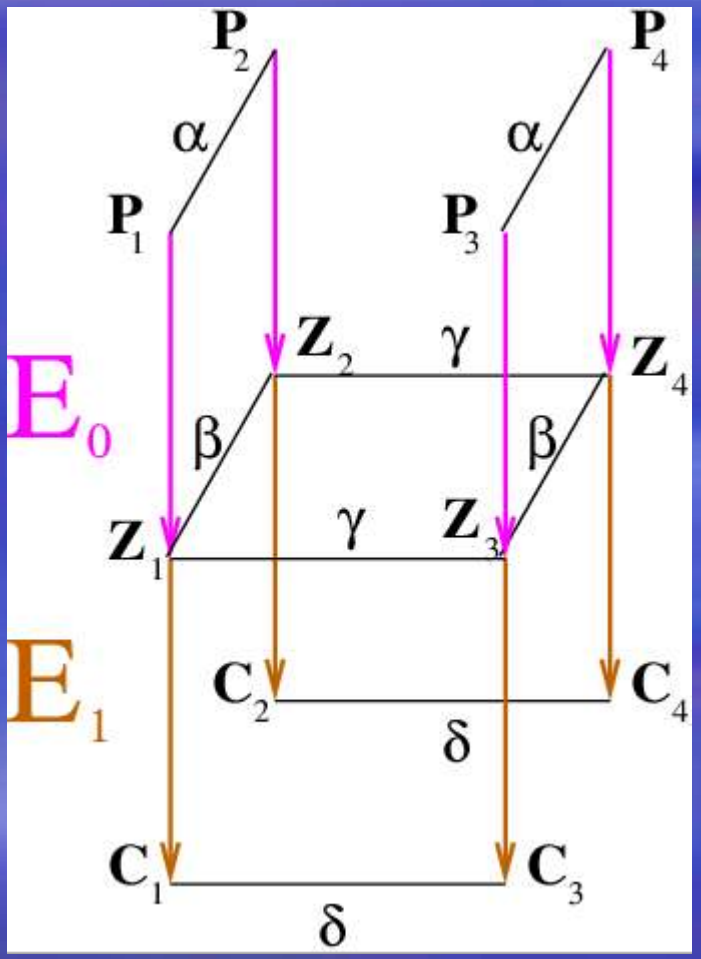
- Presented by Kohno, Kelsey, and Scheneier in 2000
- Main idea:
  - Encrypt many plaintext pairs
  - Hope that some quartet satisfy the conditions of the boomerang attack

The Amplified Boomerang Attack – No Free Meals

- Hope is a good thing, but it had no mathematical foundation!
- Hope = random process with some probability

The Amplified Boomerang Attack (cont.)

- The probability of a quartet to become a right quartet is $2^{-n-1}p^2q^2$
- This is much lower than in the boomerang attack
- Requires at least $2^{n/2+1}$ plaintexts
- Finding the right quartets is not an easy task



The Rectangle Attack

- Improving probability by using multiple differentials in each sub-cipher
- Reducing data complexity by considering all possible quartets
- Better algorithm for identification of right quartets => Better algorithm for key recovery

Results

- 49-round SHACAL-1: $2^{151.9}$ CP, 2^{508} time
- 10-round Serpent: $2^{126.3}$ CP, 2^{173} time
- 9-round AES-192 (related-key, out of 12): 2^{87} CP, 2^{125} time
- 10-round AES-256 (related-key, out of 14): $2^{114.9}$ CP, 2^{174} time
- KASUMI (related-key): $2^{54.6}$ CP, 2^{92} time
- 6.5-round IDEA (related-key): 2^{60} CP, 2^{88} time

KASUMI

- KASUMI is the 3GPP block cipher
- 8-round Feistel; 64-bit block; 128-bit key
- Used to ensure privacy and authenticity of the conversations
- The mode of use are proved to be secure, if the cipher is secure against related-key attacks
- Our attack on KASUMI is exactly a related-key attack...

The Attack on KASUMI

- Rounds 1-4: differentials with effective probability 2^{-17}
- Rounds 5-7: differentials with effective probability 2^{-2}
- Round 8: wisely find the right quartets and the key