WINTER SCHOOL ON COMPUTER SECURITY

Prof. Eli Biham

Computer Science Department
Technion, Haifa 3200003, Israel

January 27, 2014

Cryptanalysis of Modes of Operation

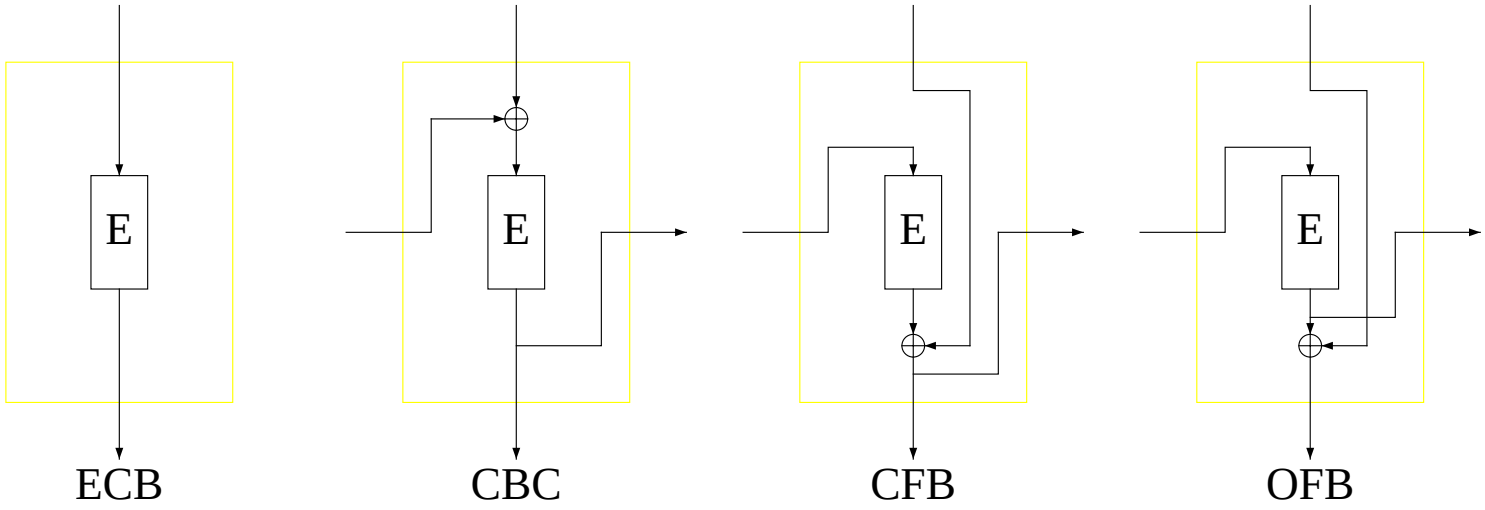
Single Modes: the DES Modes of Operation

Modes of Operation are used to hide patterns in the plaintexts, protect against chosen plaintext attacks, and to support fast on-line encryption with precomputation.

None of the modes can protect against known plaintext attacks.

Single Modes: the DES Modes of Operation (cont.)

The standard modes of DES are:



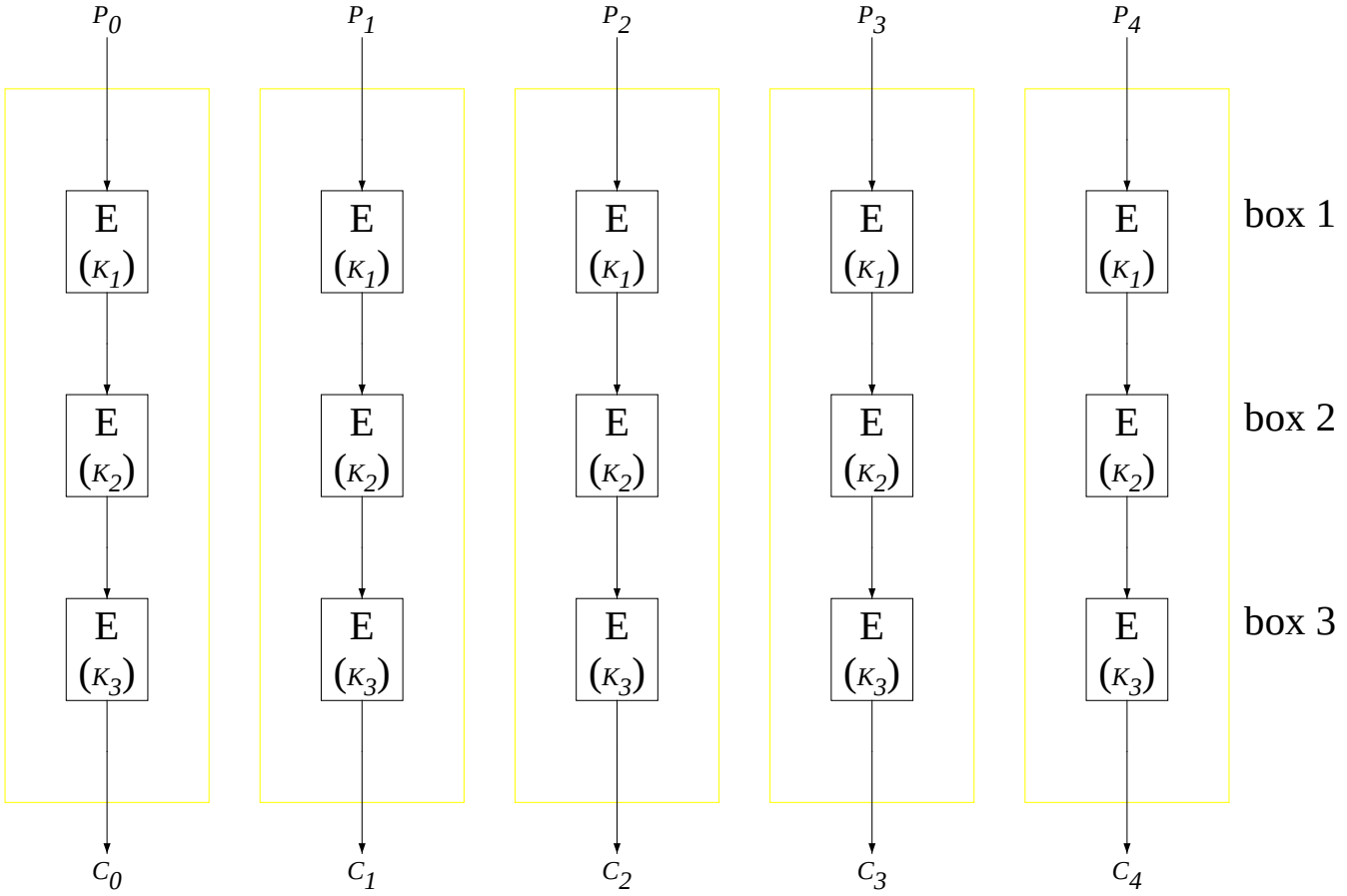
Other modes were proposed: PCBC, counter mode, PFF, etc.

We will call these modes **single modes**.

Multiple Modes of Operation

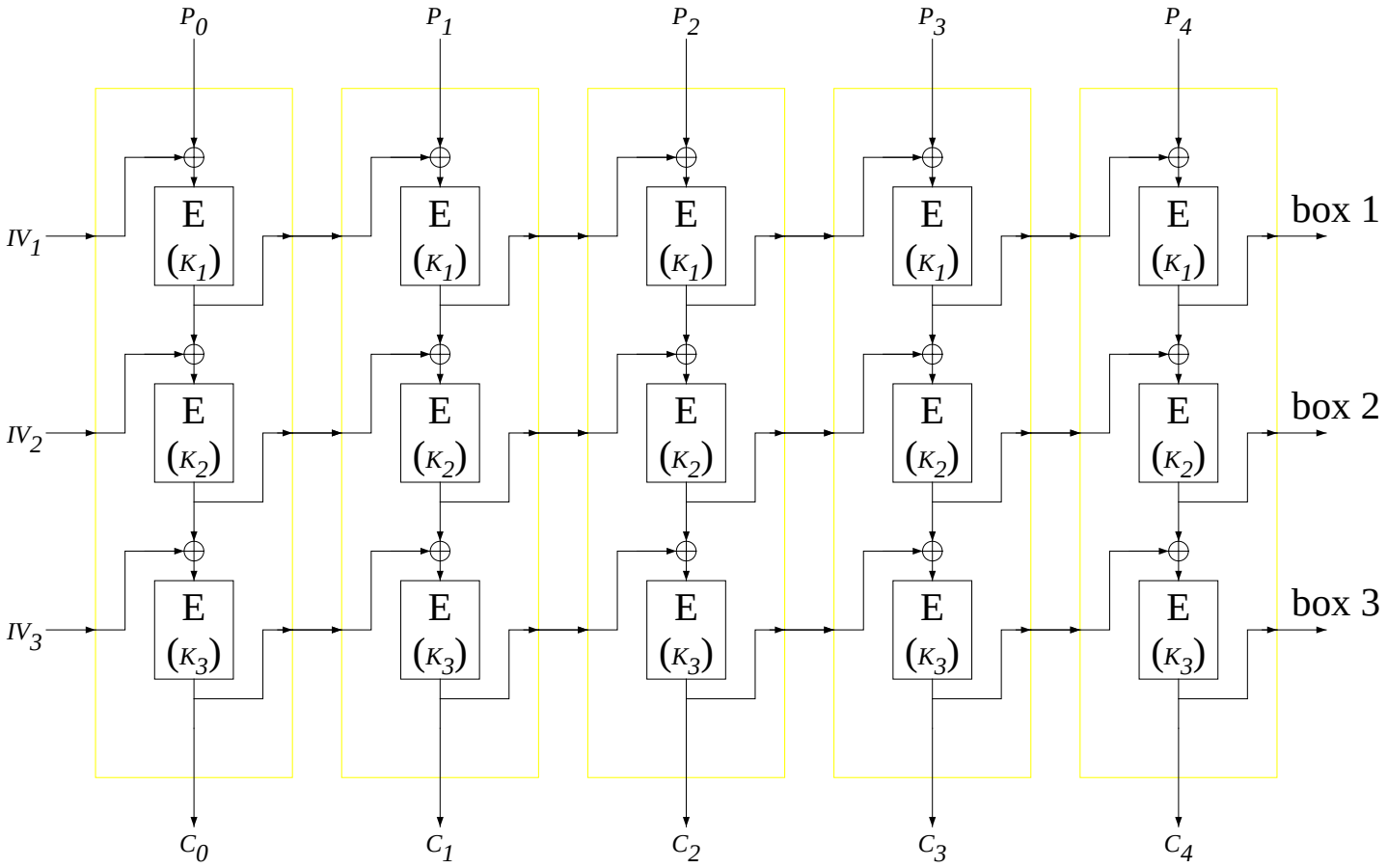
Due to the recent development in the analysis of DES (including the ability to exhaustively search for keys), it was proposed to use multiple (cascaded) modes of operation.

Example: The Triple-ECB Mode: Triple-DES



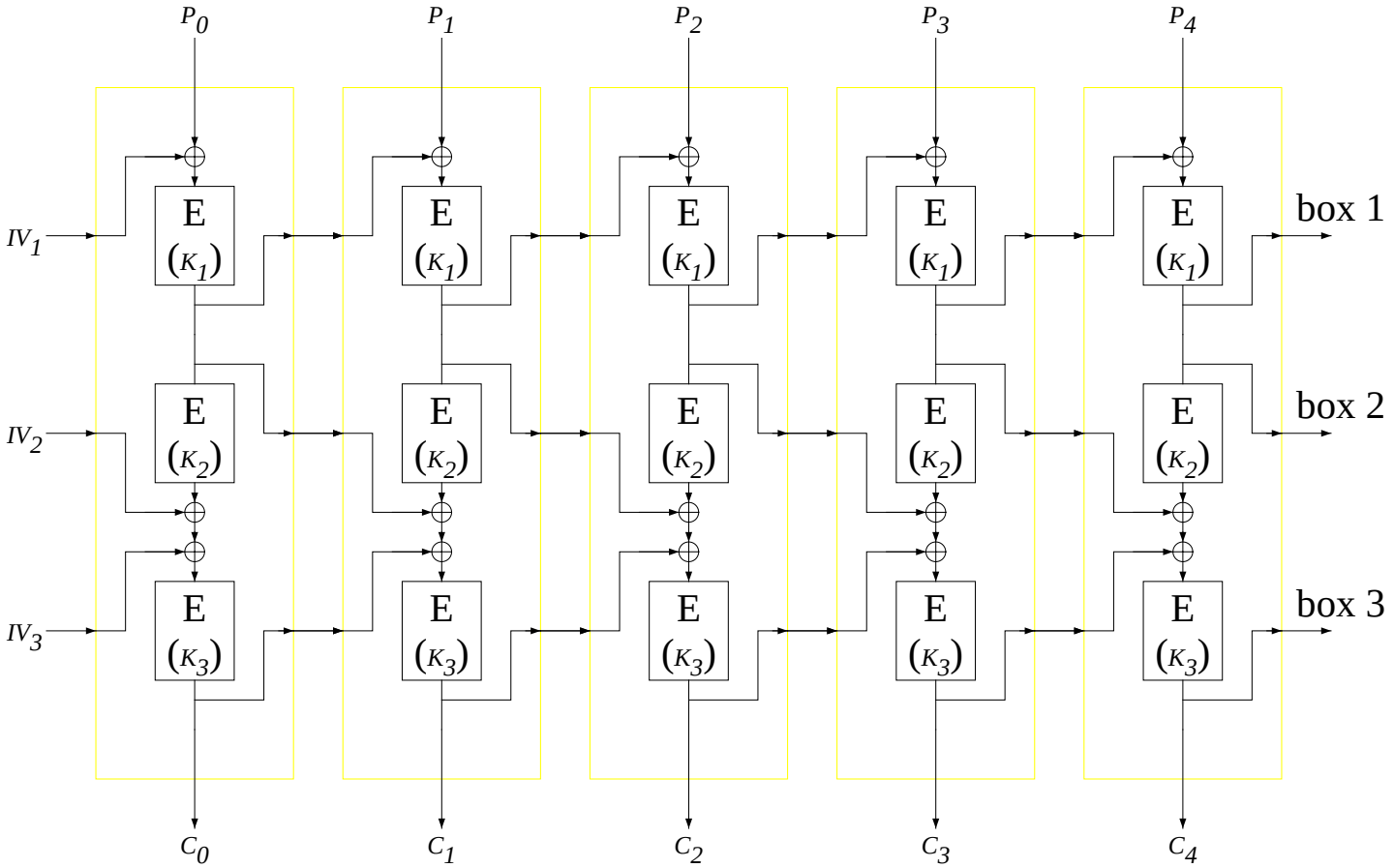
Example: The Triple-CBC Mode

Claimed to be as secure as triple-DES in (single) CBC mode:



Example: The CBC|CBC^{-1}|CBC Mode

Was almost accepted as an ANSI standard:



Advantages of Multiple Modes

Multiple modes were claimed to have several advantages:

1. More secure than single modes,
2. As fast as single encryption on pipelinable hardware,
3. Attackers cannot know the feedbacks used during encryption, and thus cannot even mount known plaintext attacks!

ANSI Triple Modes Standardization

ANSI X9F1 committee is working on a triple modes standard, already several years, which had to be accepted at the end of 1997.

It included three kinds of modes:

1. The standard DES modes, with (two or three-key) triple DES as the underlying cipher.
2. Interleaved variants of the same modes, to allow efficient hardware implementations.
3. The CBCM mode.

Multiple Modes Cannot Reduce Strength

Let A and B be two modes and let C be the combined double mode C=AB, whose component keys K_A and K_B are chosen independently.

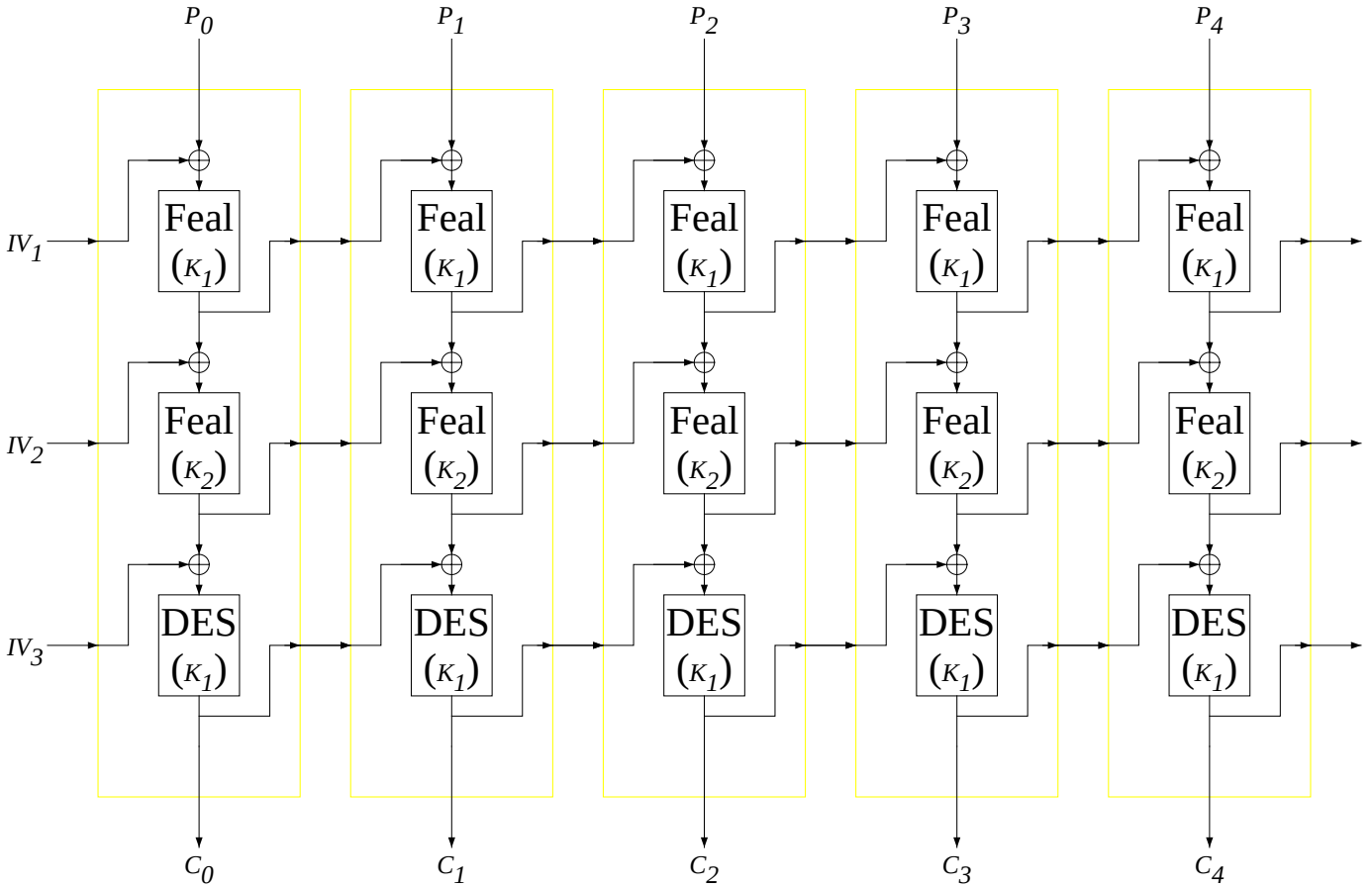
The following theorem shows that C is not weaker than either of its components.

theorem: The cracking problem of either A or B is efficiently reducible to the cracking problem of C=AB.

conclusion: A multiple mode may not be weaker than its strongest component, if the component keys are chosen independently.

Multiple Modes Cannot Reduce Strength (cont.)

A counter-example when the keys are not independent:



Multiple Modes Cannot Reduce Strength (cont.)

The weakest components in this mode are those using Feal.

By methods described later, we can find the key K_1 of the first component using 2^{18} chosen ciphertexts, and thus also of the third component using DES.

The key of the second component can then be easily found using 1000 chosen ciphertexts (or 2^{24} known plaintexts).

The third component (which uses DES) by itself is much more resistant than the whole system, and cannot be attacked successfully by any known method with complexity smaller than 2^{43}.

Cryptanalysis of Multiple Modes of Operation

All the triple (cascaded) modes of operation of DES are not much more secure than single modes (as they require up to 2^{56}–2^{66} complexity and plaintexts).

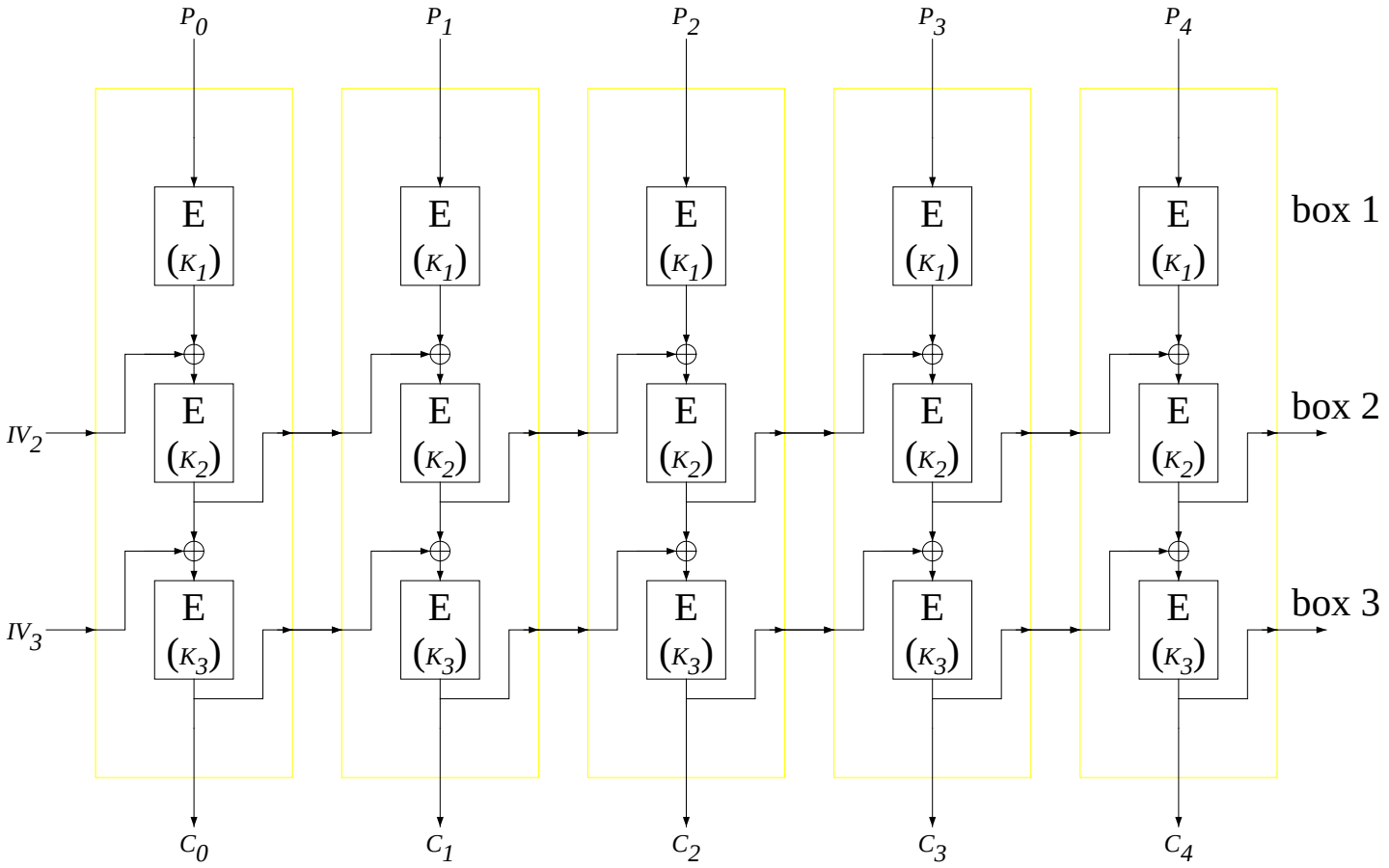
The cryptanalytic techniques to attack multiple modes attack one single component mode at a time, and can be based on any technique to attack single modes, including differential and linear cryptanalysis, Davies' attack, and exhaustive search.

The main observation is that the attacker can have some control over the unknown feedbacks, and can thus feed them with the data required to apply cryptanalysis of the single modes.

To feed these values, the attacks are usually chosen plaintext or chosen ciphertext.

Technique A: Differential Cryptanalysis

As an example we attack the ECB|CBC|CBC mode:



Technique A: Differential Cryptanalysis (cont.)

1. Let Ω_T be the ciphertext difference required to attack DES with chosen ciphertexts (the usual attack from the opposite direction).

2. Assume that n pairs are required for an attack of DES using this Ω_T.

Technique A: Differential Cryptanalysis (cont.)

3. The attacker chooses n pairs of ciphertext tuples (C_0, C_1, C_2), and $(C_0 \oplus \Omega_T, C_1, C_2)$, with arbitrary C_0, C_1, C_2.

4. The attacker requests to decrypt the $6n$ blocks by the triple mode under the unknown keys.

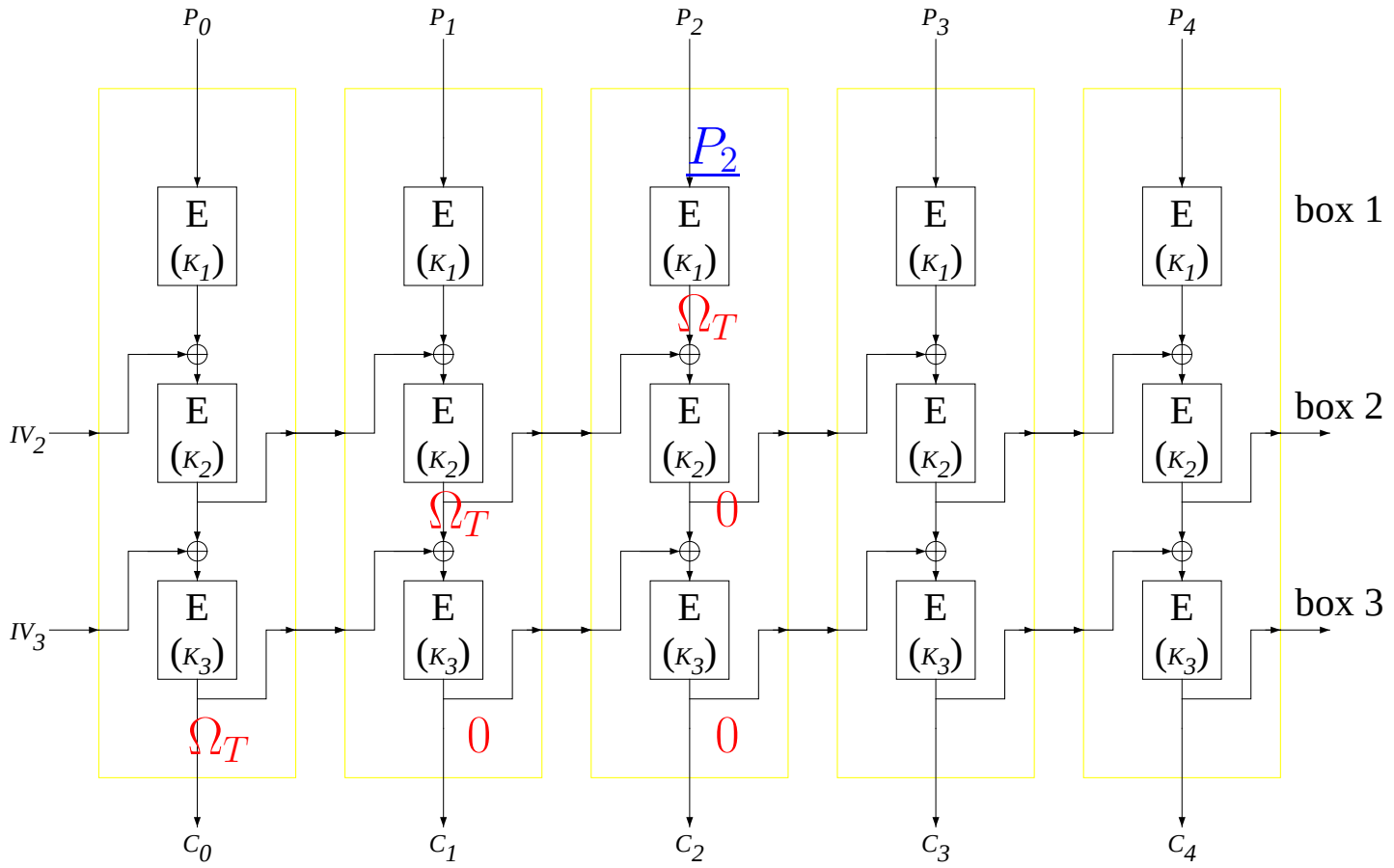
5. The ciphertext difference in each pair of tuples is $(\Omega_T, 0, 0)$.

6. After decryption of one component the difference is $(-, \Omega_T, 0)$.

7. After decryption of two components the difference is $(-, -, \Omega_T)$.

8. The plaintexts are known, and in particular P_2 and P_2^*.

Technique A: Differential Cryptanalysis (cont.)



Legend: Known differences Known values (underlined)

Technique A: Differential Cryptanalysis (cont.)

9. We result with n pairs P_2, P_2^*, for which

$$E_{K_1}(P_2) \oplus E_{K_1}(P_2^*) = \Omega_T$$

This is exactly the data required for differential cryptanalysis!

10. If the underlying cipher is DES, we need 2^{47} chosen ciphertext blocks to find the key of the ECB component. The other component keys can be recovered by other techniques.

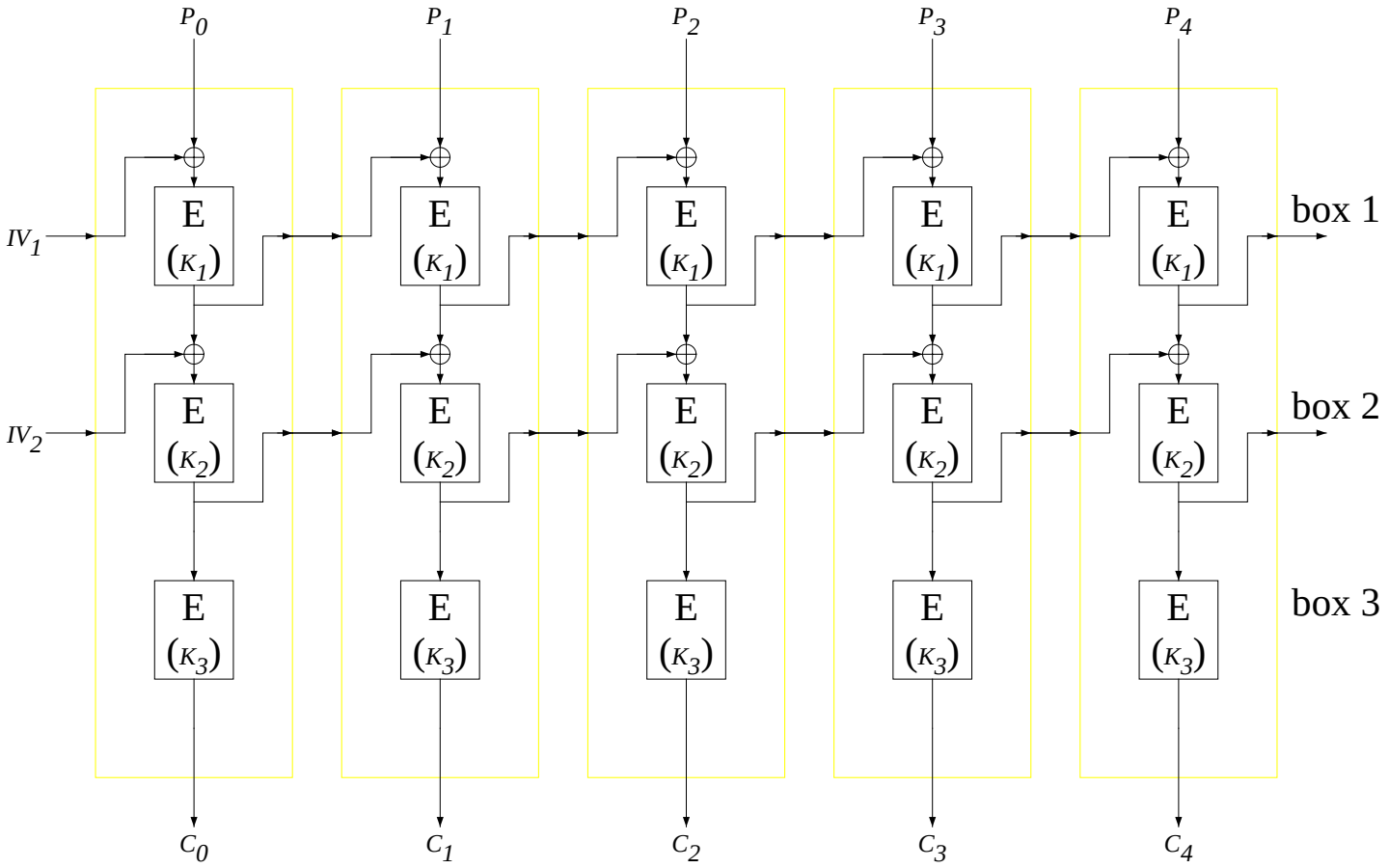
Technique E: Using Exhaustive Search

This technique uses exhaustive search for the component keys, and can thus be applied for any underlying cipher, independent of its internal operations.

All the techniques described later use exhaustive search as a basic tool for more complex analysis, and thus also have this property.

Technique E: Using Exhaustive Search (cont.)

As an example we attack the CBC|CBC|ECB mode:



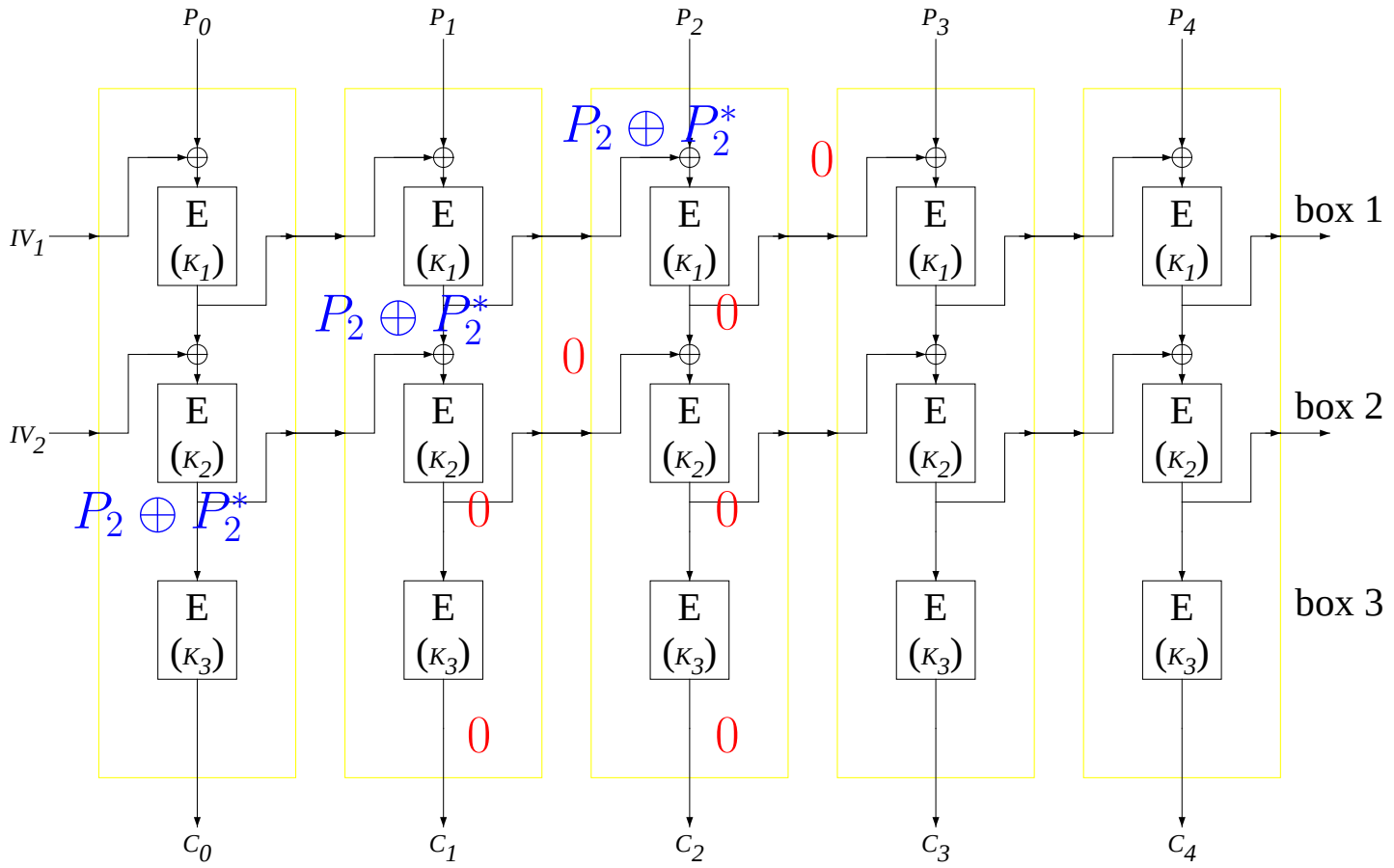
Technique E: Using Exhaustive Search (cont.)

1. The attacker chooses one pair of tuples (C_0, C_1, C_2), (C_0^*, C_1, C_2), where $C_0 \neq C_0^*$.

2. He requests the plaintexts (P_0, P_1, P_2) and (P_0^*, P_1^*, P_2^*).

3. The value $P_2 \oplus P_2^*$ is the difference of the ECB mode in the first block!

Technique E: Using Exhaustive Search (cont.)



Legend: Differences

Technique E: Using Exhaustive Search (cont.)

4. The attacker exhaustively search all keys for

$$D_{K_3}(C_0) \oplus D_{K_3}(C_0^*) = P_2 \oplus P_2^*$$

5. The two tuples can be generated with only four chosen ciphertext blocks.

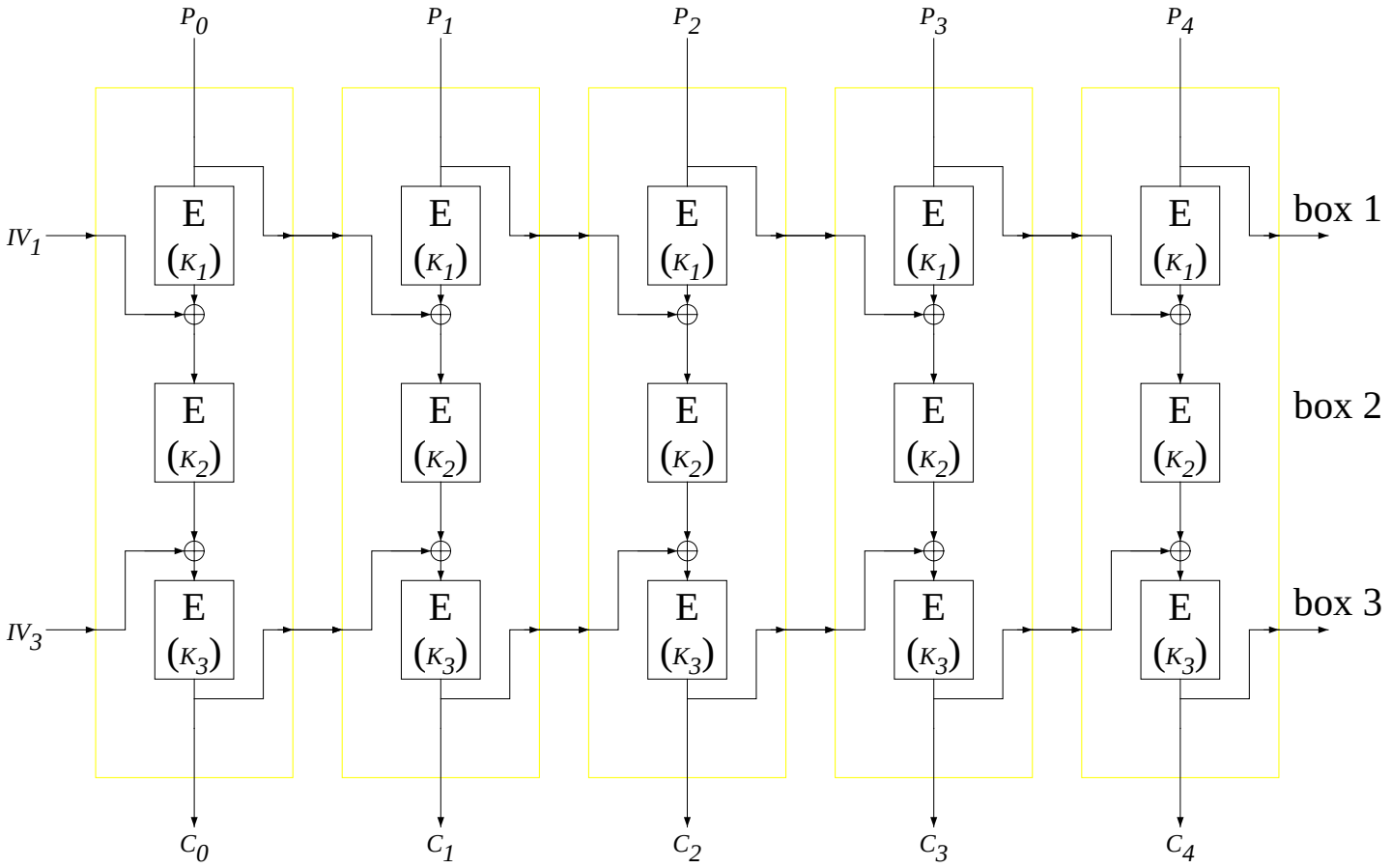
Technique E: Using Exhaustive Search (cont.)

A known plaintext variant:

Given about 2^{65} random known plaintext tuples, the birthday paradox predicts the existence of a pair (C_0, C_1, C_2) and (C_0^*, C_1^*, C_2^*) with $C_1 = C_1^*$ and $C_2 = C_2^*$!

Technique E: Using Exhaustive Search (cont.)

Another example: $\mathrm{CBC}^{-1}|\mathrm{ECB}|\mathrm{CBC}$

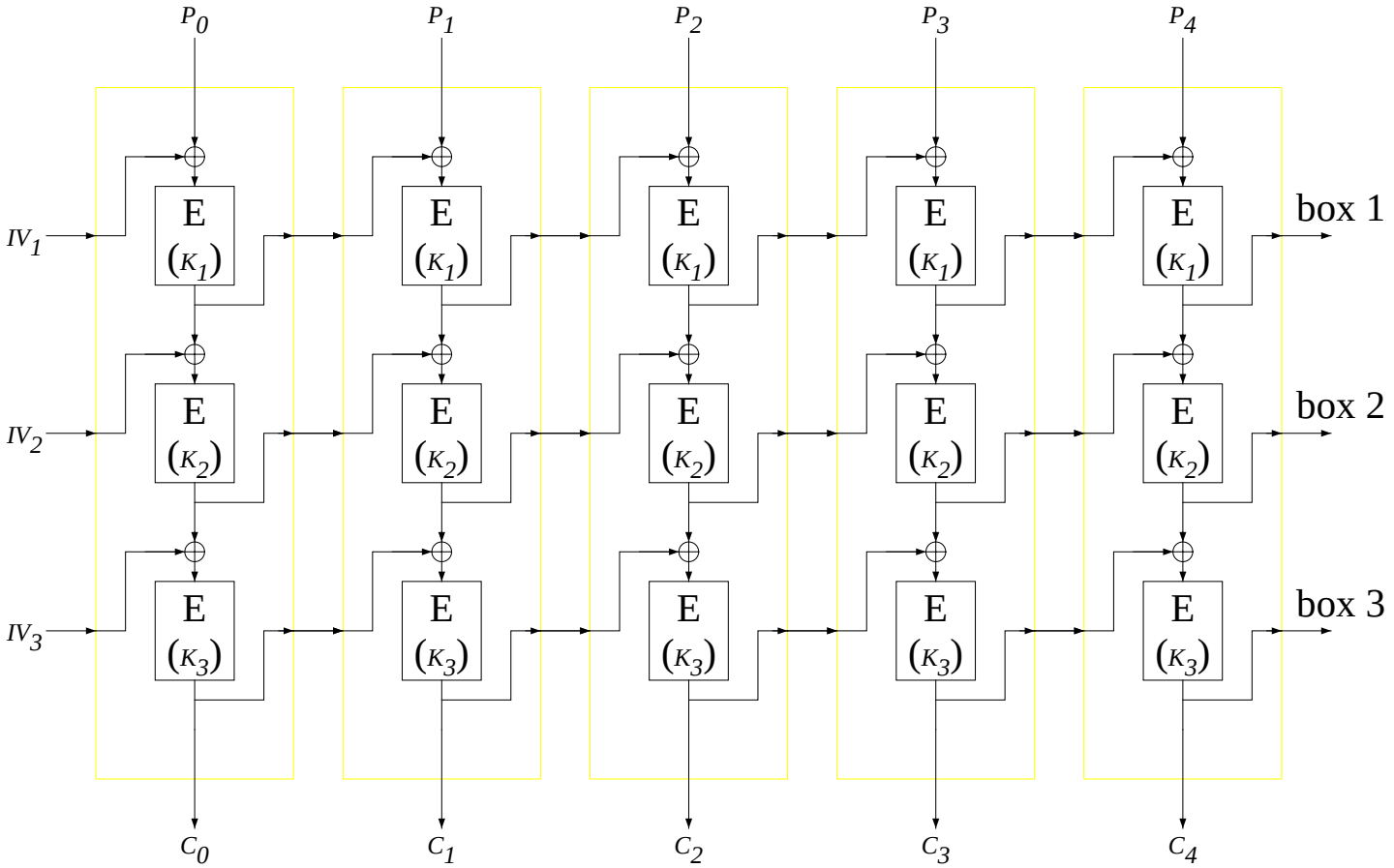


Technique E: Using Exhaustive Search (cont.)

Exercise: Find all the three keys with 3 chosen plaintexts, or 2^{64} known plaintexts.

Technique F: The Birthday Technique

Described on the triple-CBC mode:

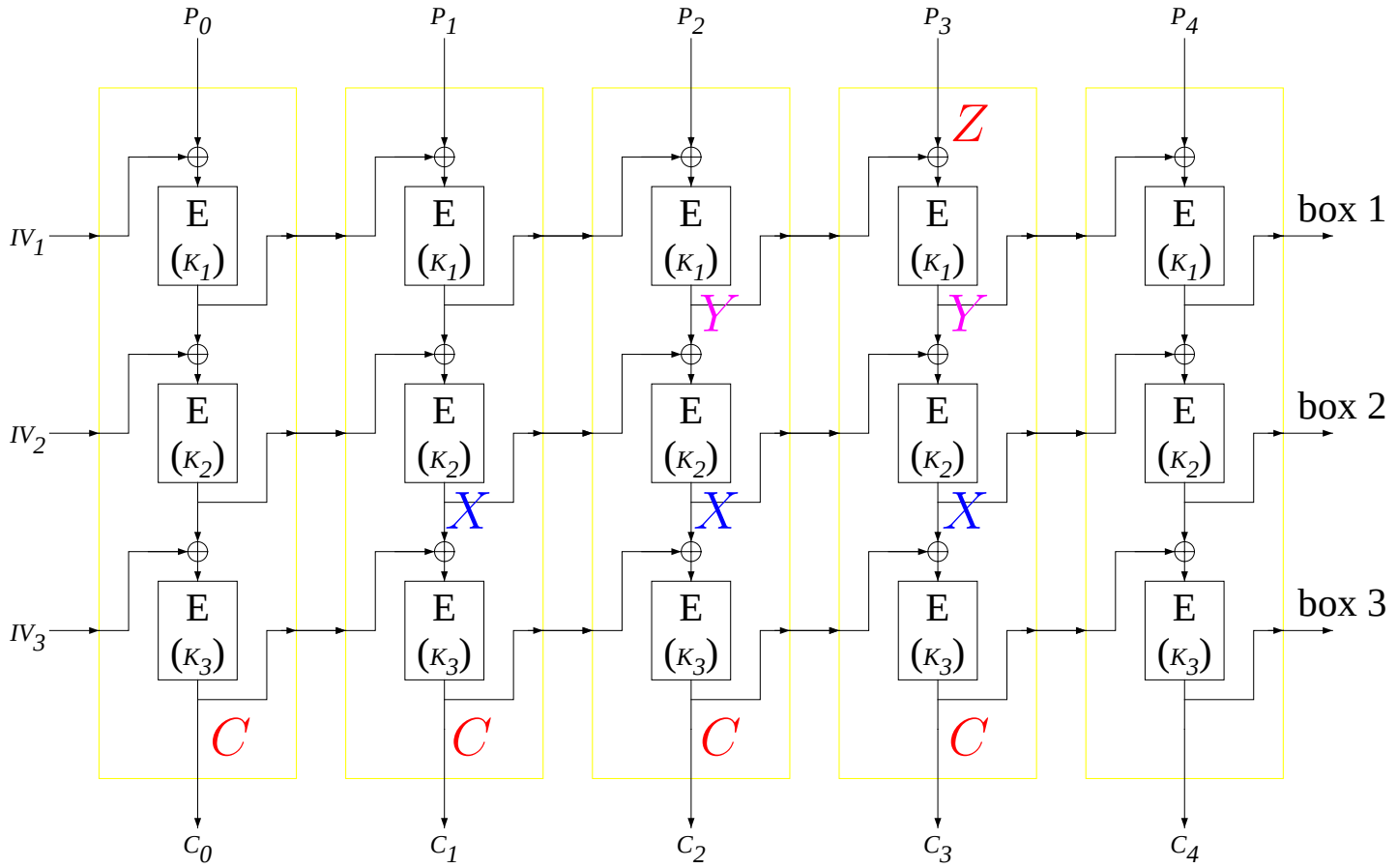


Technique F: The Birthday Technique (cont.)

1. We choose ciphertext tuples of the form (C, C, C, C).

Technique F: The Birthday Technique (cont.)

2. During decryption we get



Legend: Values

Technique F: The Birthday Technique (cont.)

3. The function

$$X = D_{K_3}(C) \oplus C$$

behaves like a random function, thus, given 2^{33} such tuples, a collision is expected to occur with a high probability.

4. This collision can be identified by comparing the resultant plaintext block Z. A key search can be applied with 2^{57} DES encryptions.

5. Note: Collisions can occur in each of the CBC components, thus only a third occur in the last component. This increases the complexity by a factor of at most 3, without increase in the number of chosen ciphertexts.

Technique G

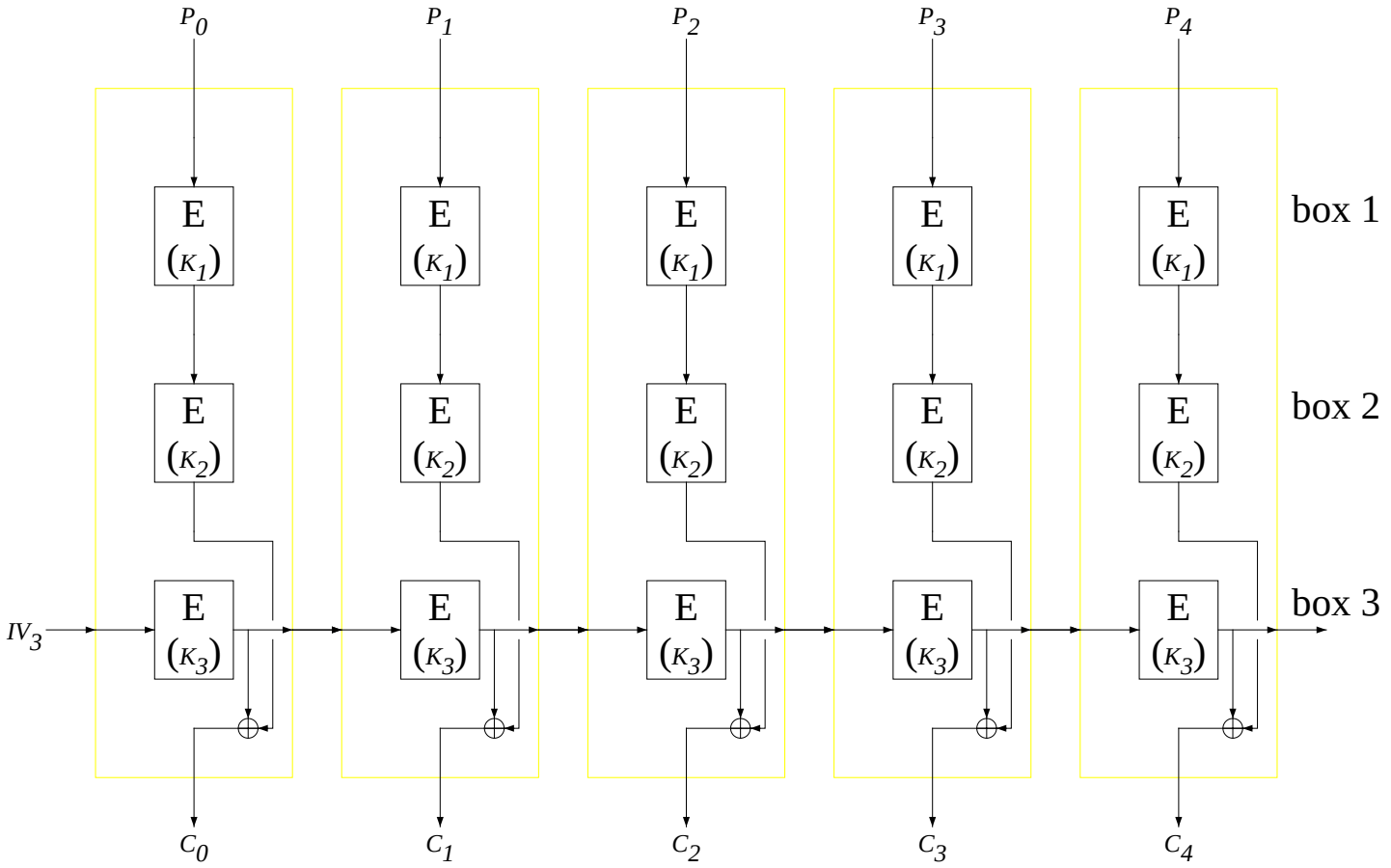
This technique enables to attack modes whose plaintext and ciphertext are mixed with some unknown feedback, or do not affect the encryption box at all.

It is later used as a building block by the techniques described afterwards.

We describe two variants of this technique on two examples: the triple mode ECB|ECB|OFB and on the double mode CBC|OFB.

Technique G (cont.)

The ECB|ECB|OFB mode:



Technique G (cont.)

To attack this mode we choose a plaintext consisting of 2^{64} equal blocks P.

We result with a ciphertext C_0, C_1, ..., which equals the output of the OFB component V_i XORed with a fixed value.

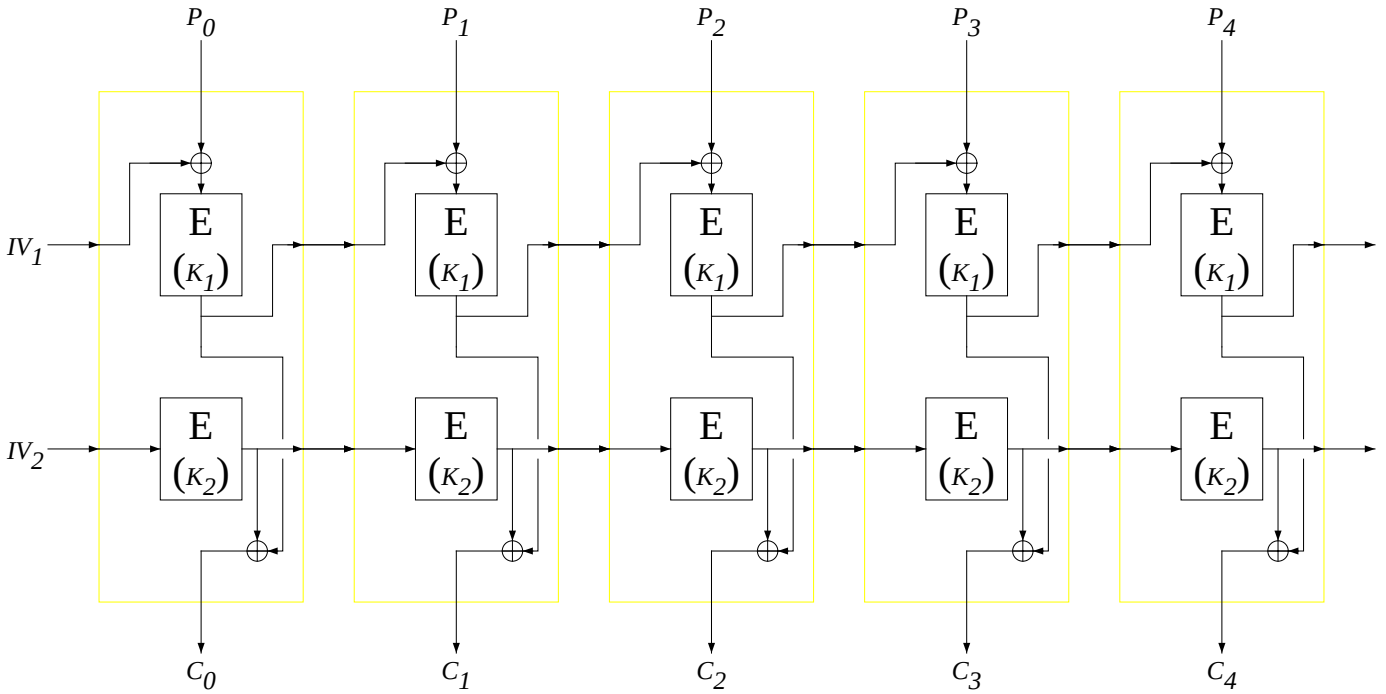
We choose some value u arbitrarily, and guess that it appears in the OFB stream.

We encrypt it under all possible keys K', and test whether the difference $u \oplus E_{K'}(u)$ is a difference between two consecutive ciphertext blocks.

We usually succeed, as the cycle of the OFB mode includes about 2^{63} different blocks. Otherwise, we try another value u.

Technique G (cont.)

The CBC|OFB mode:



Technique G (cont.)

In this case we attack the CBC component: we choose the ciphertext to consist of 2^{64} C followed by 2^{64} C^*. We get p pairs of the form

$$\begin{aligned} C \oplus V_i &= E_{K_1}(P_i \oplus C \oplus V_{i-1}) \\ C^* \oplus V_i &= E_{K_1}(P_i^* \oplus C^* \oplus V_{i-1}) \end{aligned}$$

where p is the period of the OFB component.

Again, we guess a value u arbitrarily, and hope that it is one of the V_i's in the cycle (whose period is very easily identified from the plaintexts).

We compute $P_i \oplus V_{i-1}$ and $P_i^* \oplus V_{i-1}$ (for the unknown i) by the above equations, and test whether the resultant difference equals $P_i \oplus P_i^*$ for some i.

As a bonus we also recover the OFB stream.

Summary

Using these and other cryptanalytic techniques, it is possible to cryptanalyze all the $6^3 - 1 = 215$ triple-modes of operation.

A related-model with known oe chosen IV's (by Wagner) may require even fewer amouts of data.

The End