# A Practical Attack on KeeLoq

Sebastiaan Indesteege[1] Nathan Keller[2] Orr Dunkelman[1]
Eli Biham[3] Bart Preneel[1]

[1]Dept. ESAT/SCD-COSIC, K.U.Leuven, Belgium.

[2]Einstein Institute of Mathematics, Hebrew University, Israel.

[3]Computer Science Department, Technion, Israel.

Eurocrypt 2008

# Outline

# Outline

# Introduction

## What?

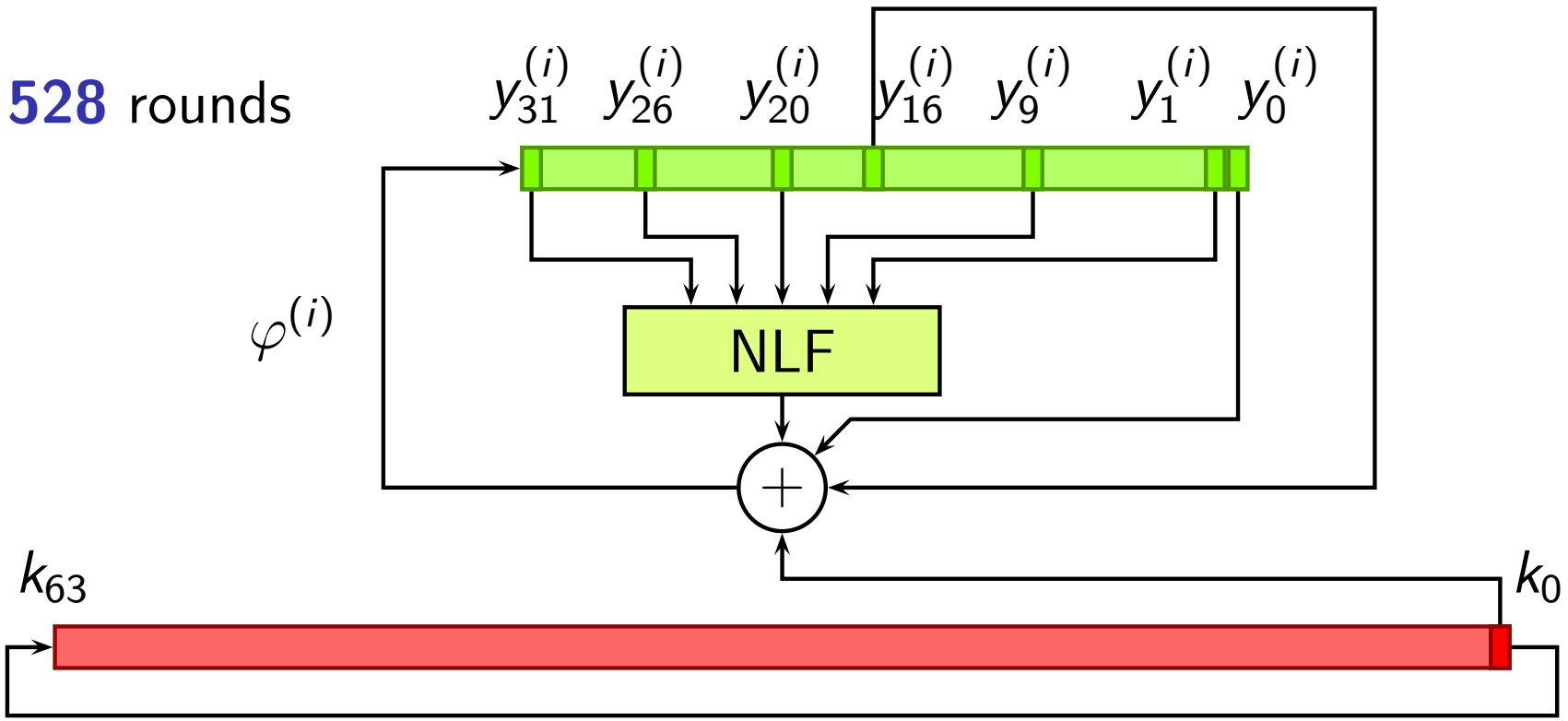
- Lightweight block cipher
- 32-bit block, 64-bit key
- Designed in 1980s
- Sold by Microchip Inc.


## Where Is It Used?

- Remote keyless entry applications
- Car locks and alarms

# Description of the KeeLoq Block Cipher

**528** rounds

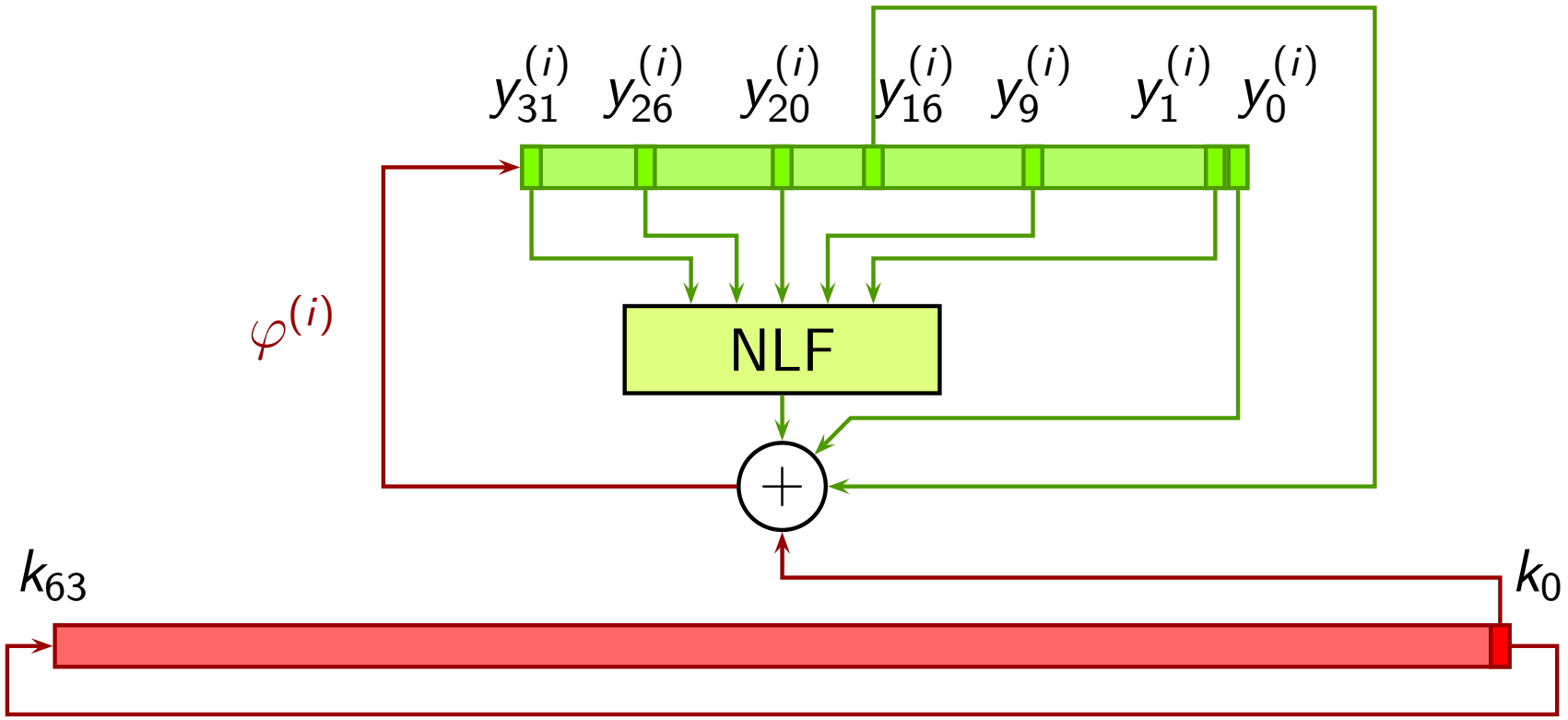


# Previous Attacks on KeeLoq

| Attack Type | Data | Time | Memory | Ref. |
|---|---|---|---|---|
| Slide/Guess-and-Det. | $2^{32}$ KP | $2^{52}$ | 16 GB | [B07] |
| Slide/Guess-and-Det. | $2^{32}$ KP | $2^{50.6}$ | 16 GB | [B07b] |
| Slide/Cycle Structure | $2^{32}$ KP | $2^{39.4}$ | 16.5 GB | [CB07] |
| Slide/Cycle/G&D | $2^{32}$ KP | $(2^{37})$ | 16.5 GB | [B07b] |
| Slide/Fixed Points | $2^{32}$ KP | $2^{27}$ | $>$ 16 GB | [C+08] |
| Slide/Algebraic | $2^{16}$ KP | $2^{65.4}$ | ? | [CB07, C+08] |
| Slide/Algebraic | $2^{16}$ KP | $2^{51.4}$ | ? | [CB07, C+08] |
| DPA — DEMA | - | - | - | [E+08] |

# Outline

# Determining Keybits in KeeLoq

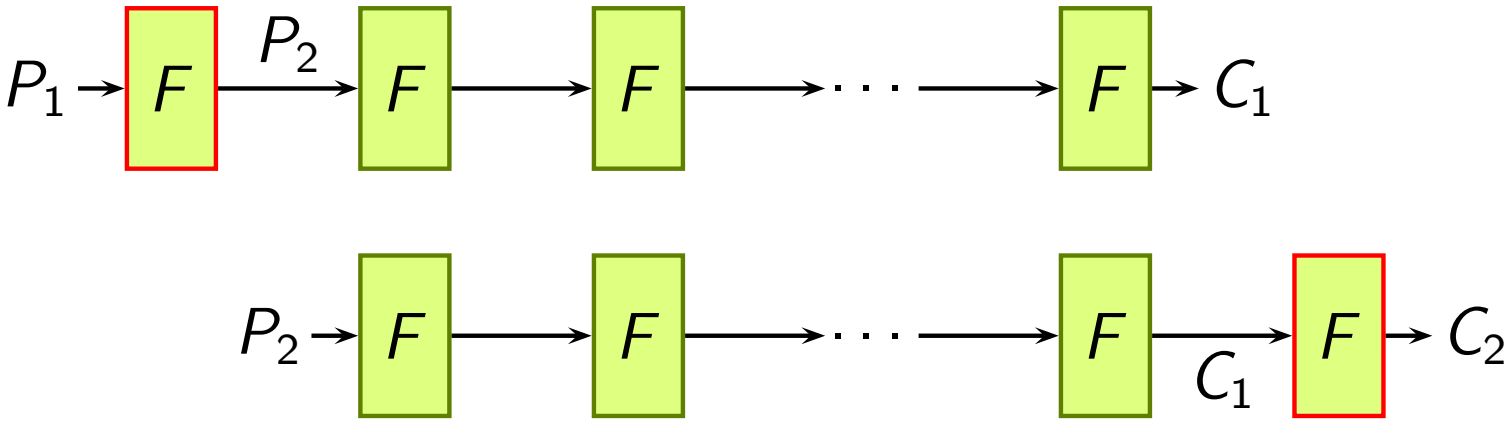



- Given two KeeLoq states, **32 rounds** or less apart, we can find the **key bits** used in these rounds.

*Bogdanov* [B07]

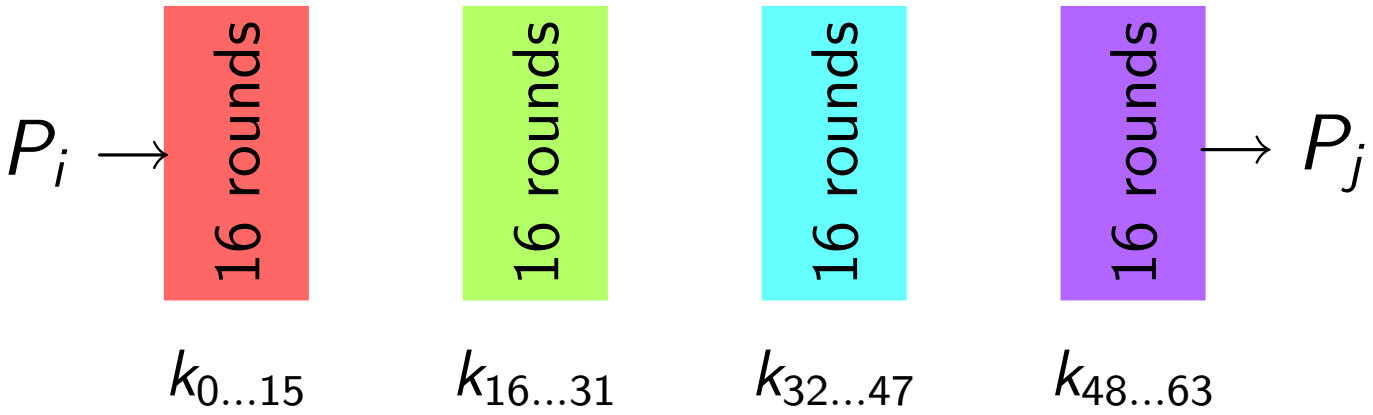
# Slide Attack

- Cipher with many identical "rounds" $F(\cdot)$



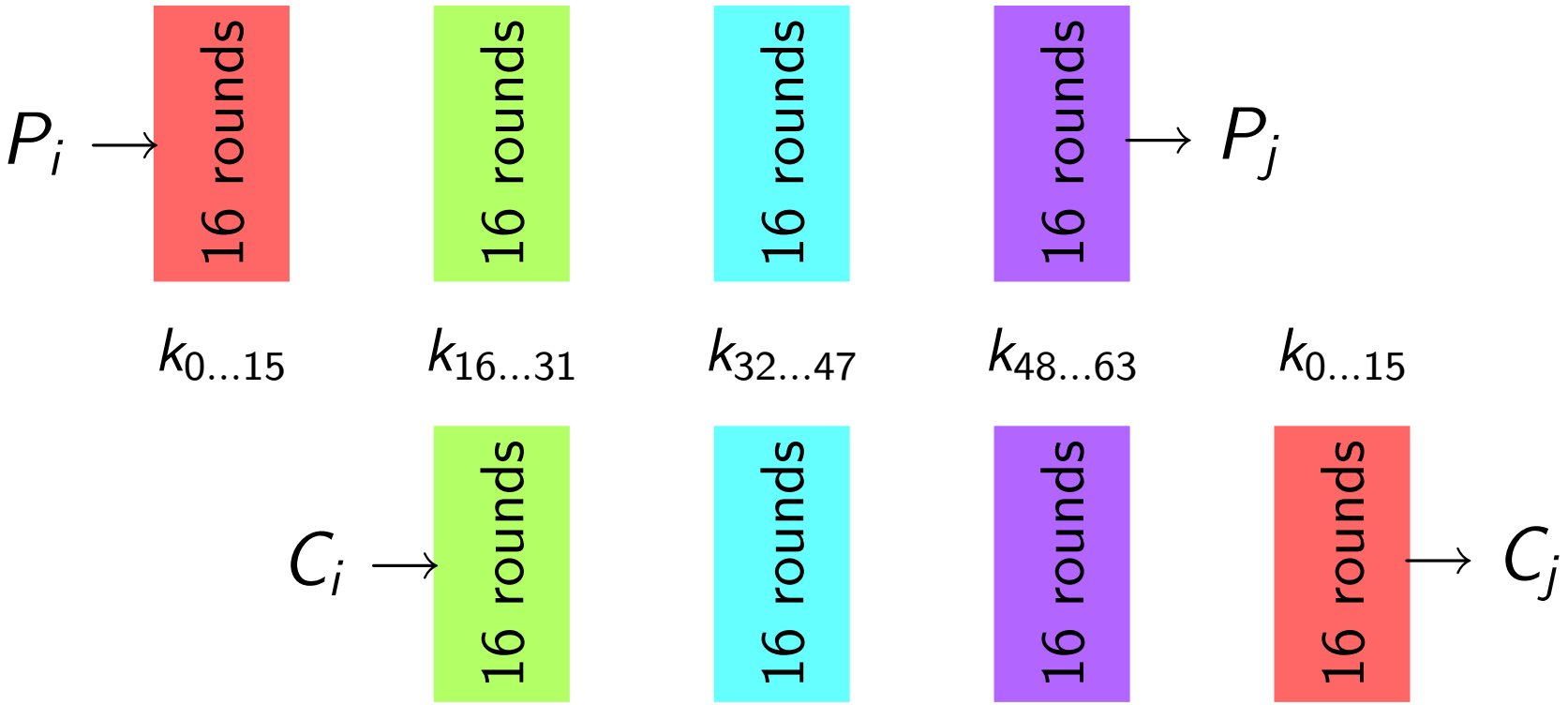

- **Slid pair** $P_2 = F(P_1)$, then also $C_2 = F(C_1)$
- Encrypting $C_1$ and $C_2$ yields **another slid pair**, ...
- Use these pairs to attack $F(\cdot)$

# Basic Attack Scenario



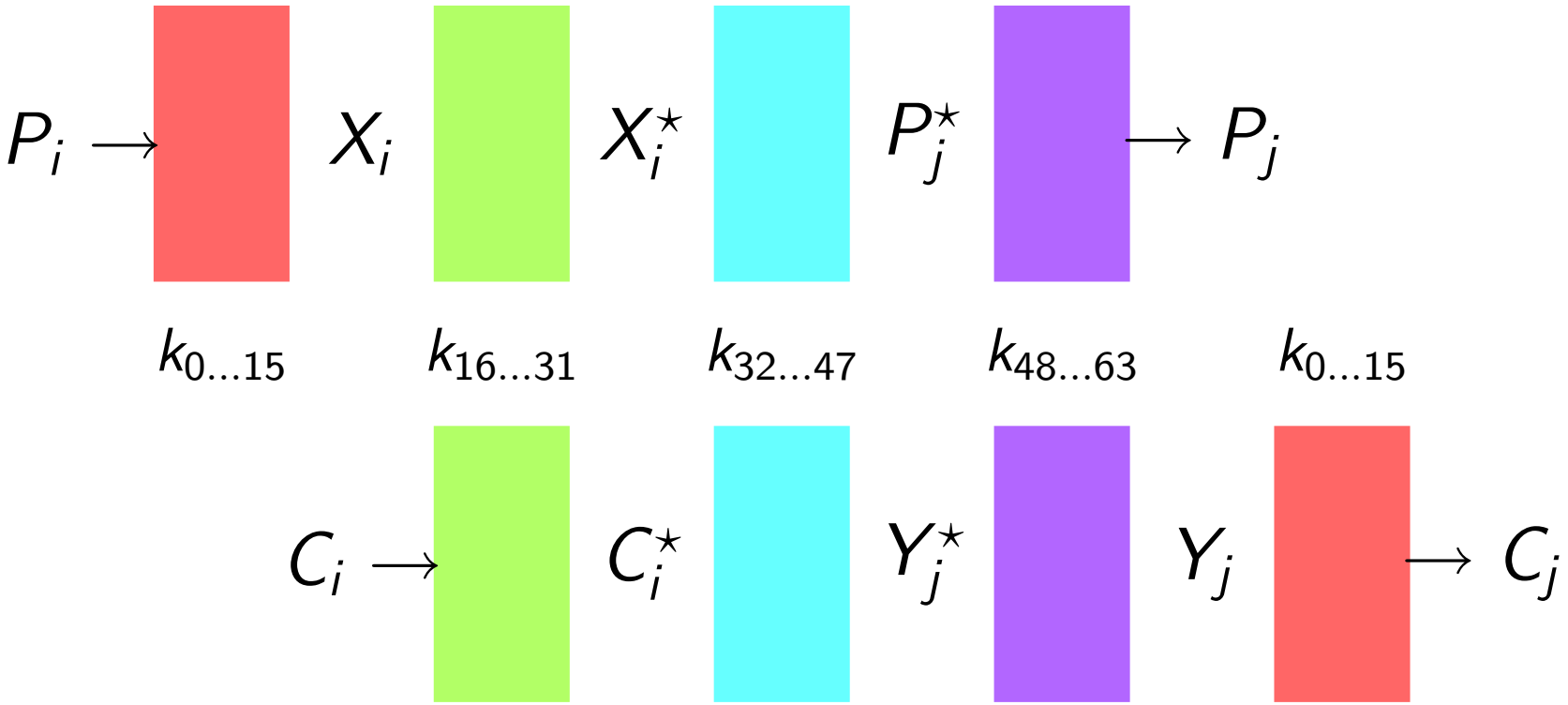

Expect a **slid pair** among $2^{16}$ plaintexts (birthday paradox)

# Basic Attack Scenario

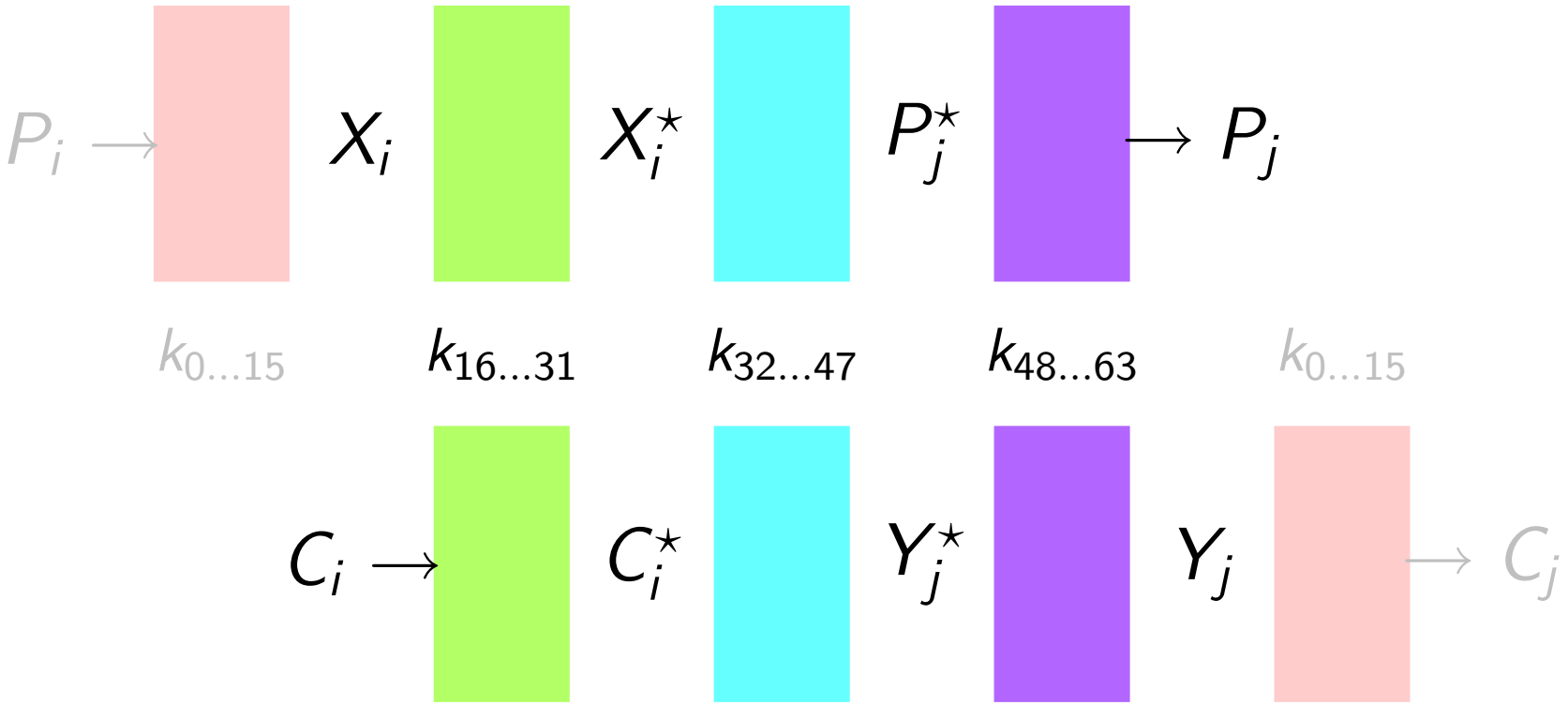



$$528 \text{ rounds} = 8 \times 64 + 16 \text{ rounds}$$

# Basic Attack Scenario

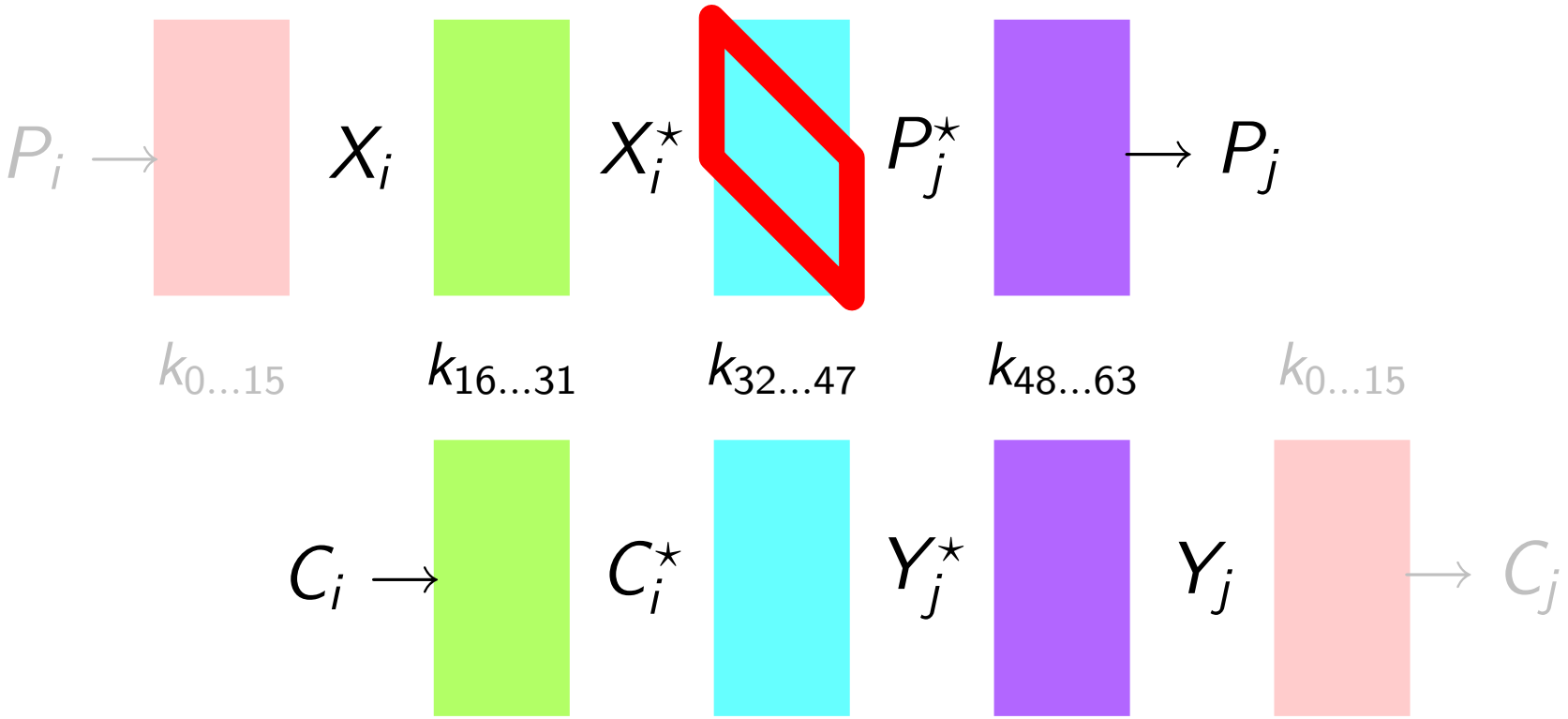


# Basic Attack Scenario



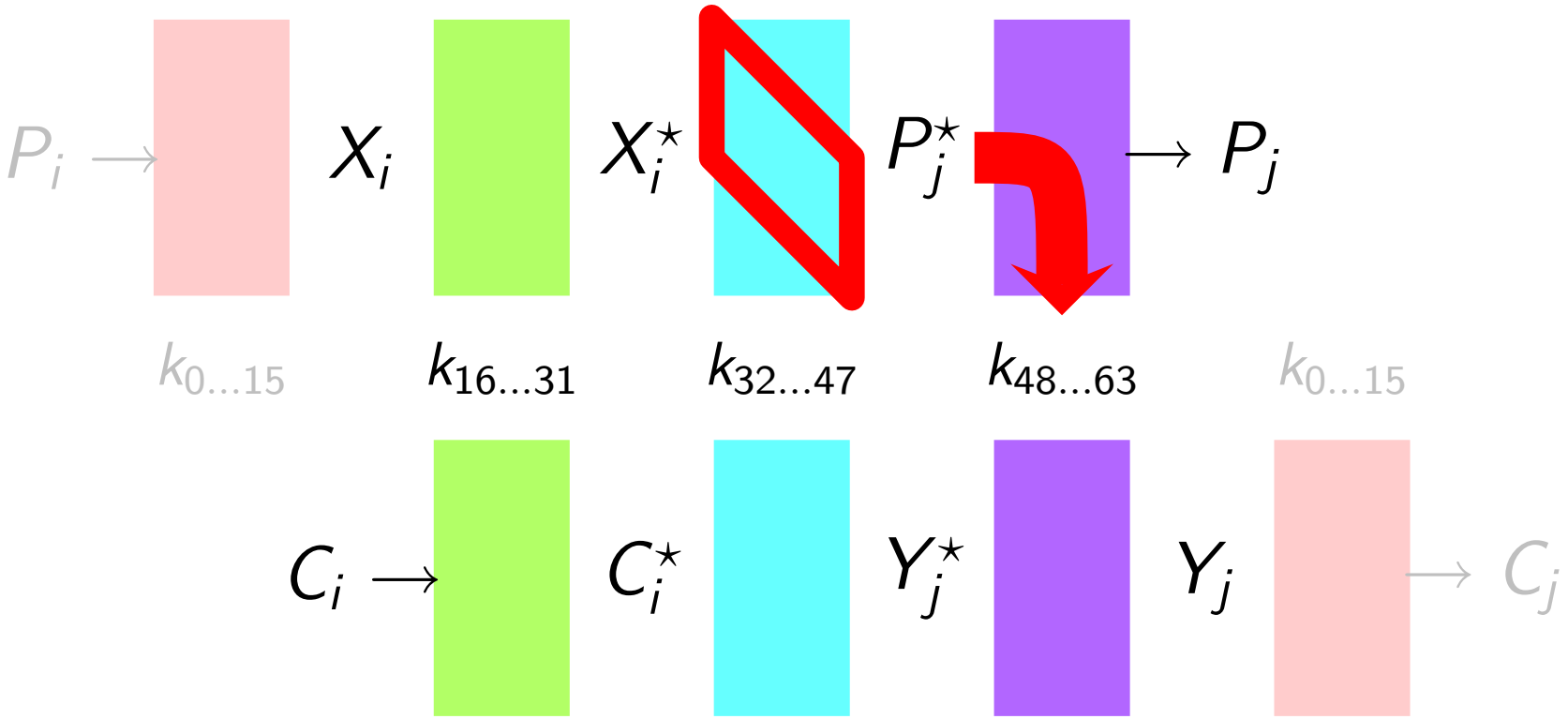

**Guess** 16 key bits: $k_{0\ldots15}$

# Basic Attack Scenario



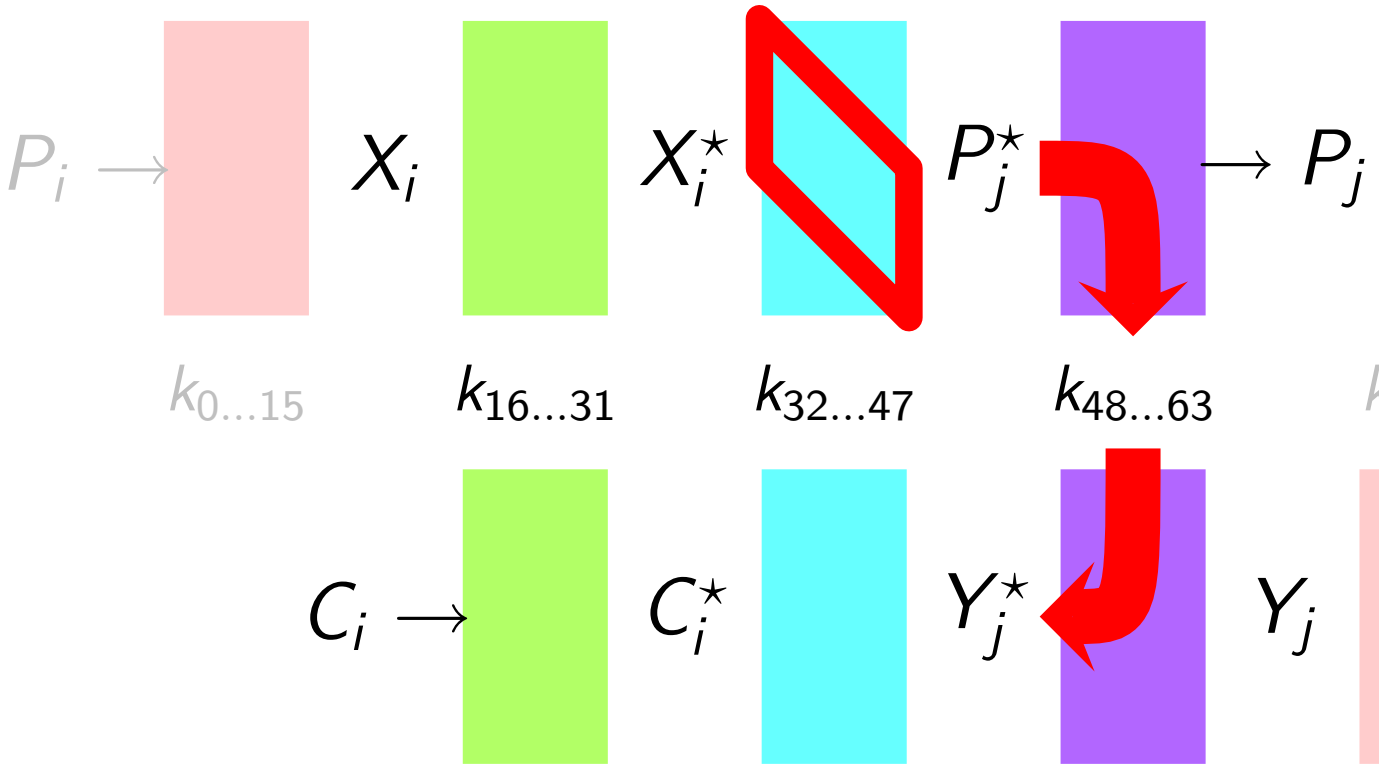

**Guess** 16 LSB's of $P_j^\star$: $\underline{P_j^\star} = \overline{X_i^\star}$

# Basic Attack Scenario




For each plaintext $j$, **determine** $k_{48\ldots63}$

# Basic Attack Scenario



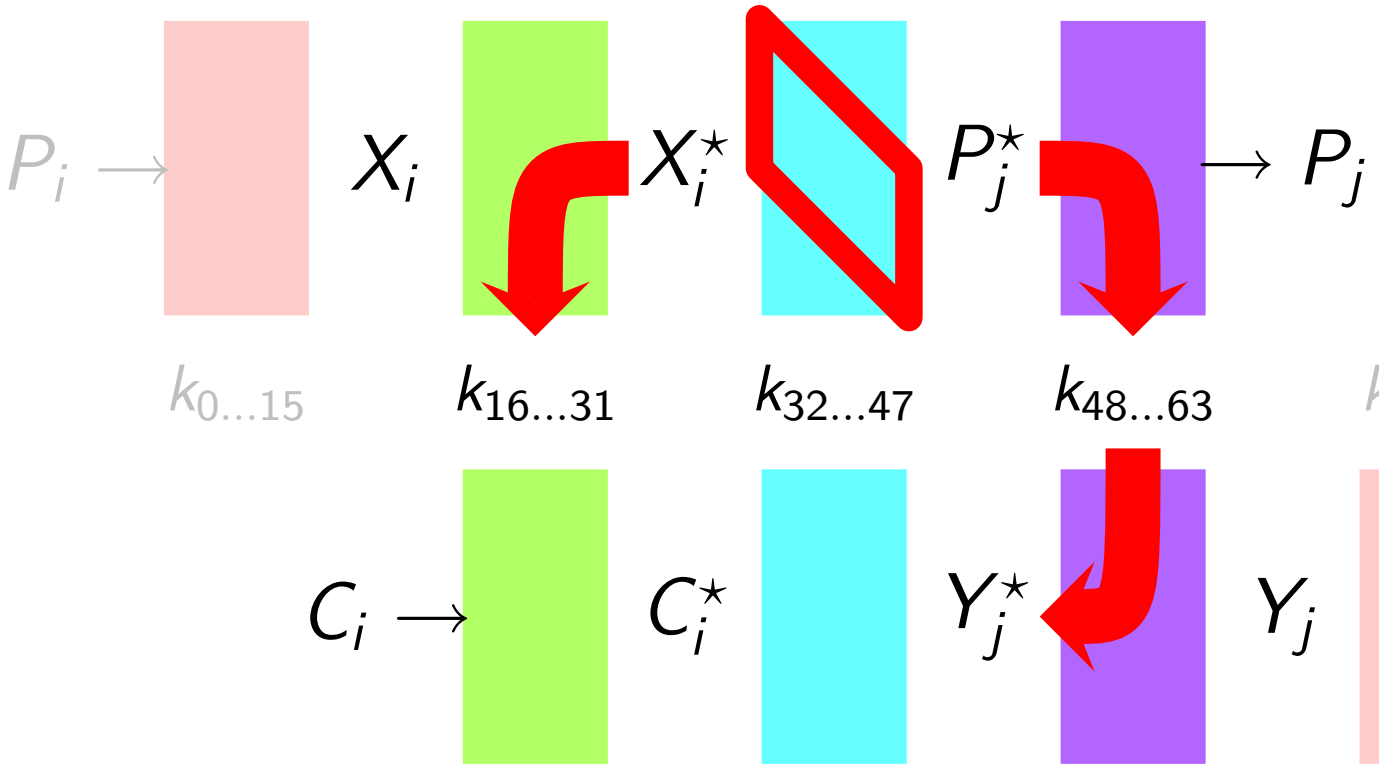

**Table**

$2^{16}$ tuples

$\langle P_j^\star, Y_i^\star, k_{48\ldots63} \rangle$

For each plaintext $j$, partially **decrypt** $Y_j$ to $Y_j^\star$

# Basic Attack Scenario



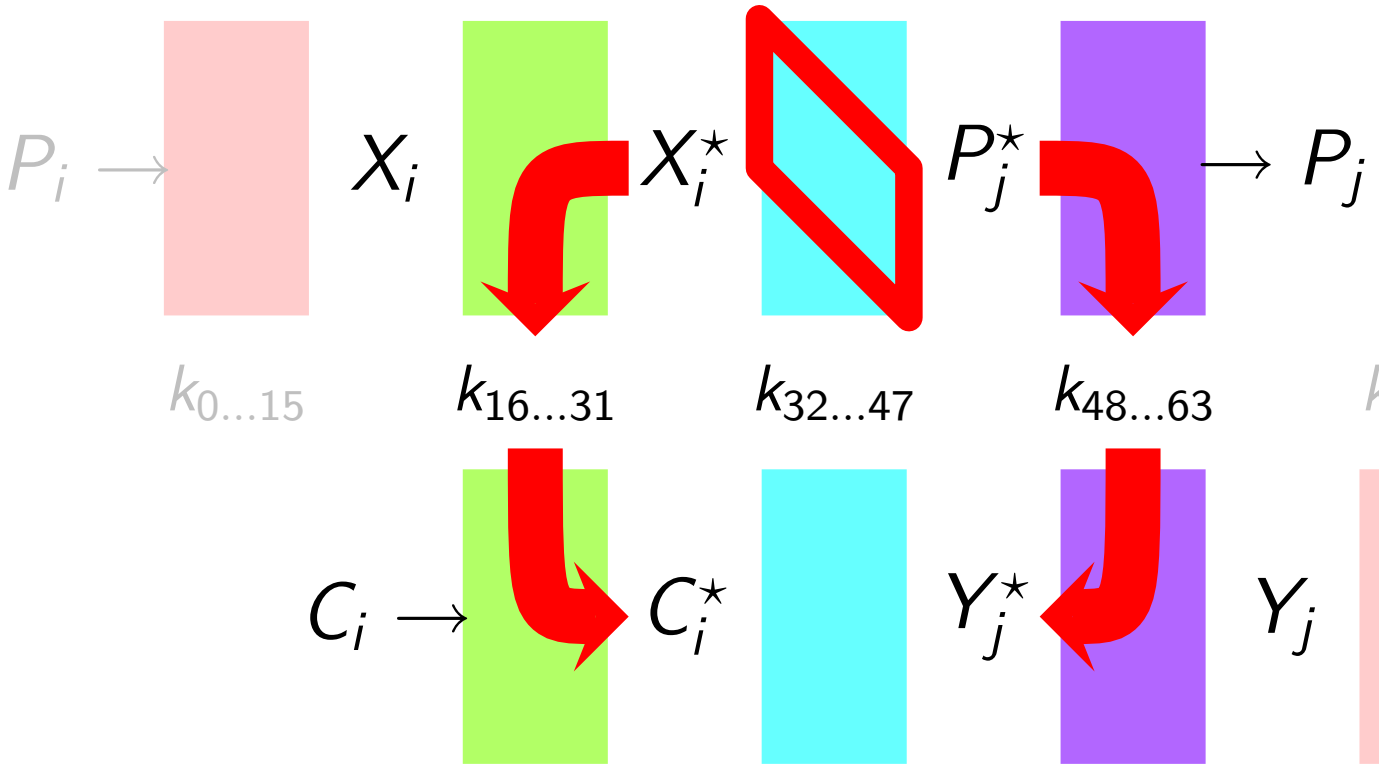

**Table**

$2^{16}$ tuples

$\langle P_j^\star, Y_i^\star, k_{48\ldots63} \rangle$

For each plaintext $i$, **determine** $k_{16\ldots31}$

# Basic Attack Scenario



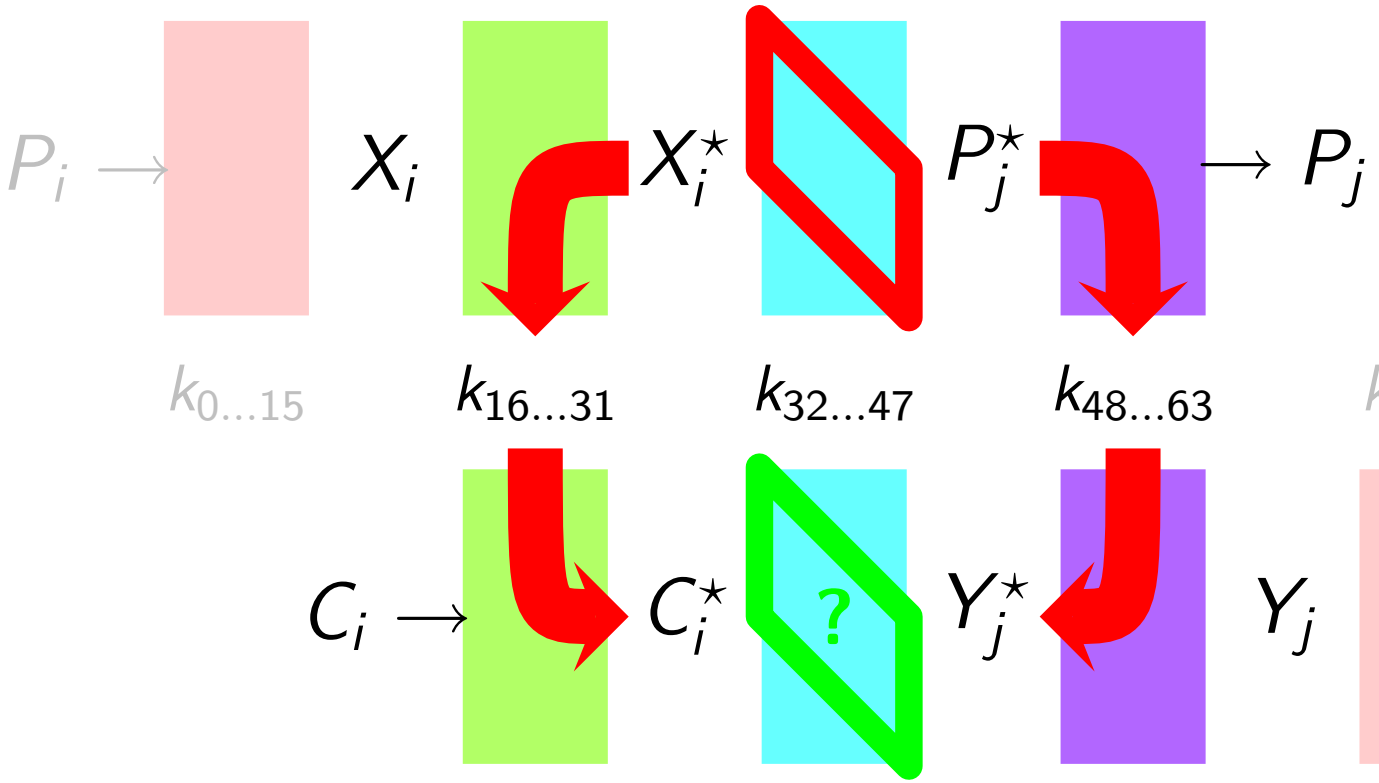

**Table**

$2^{16}$ tuples

$\langle P_j^\star, Y_i^\star, k_{48\ldots63} \rangle$

For each plaintext $i$, partially **encrypt** $C_i$ to $C_i^\star$

# Basic Attack Scenario

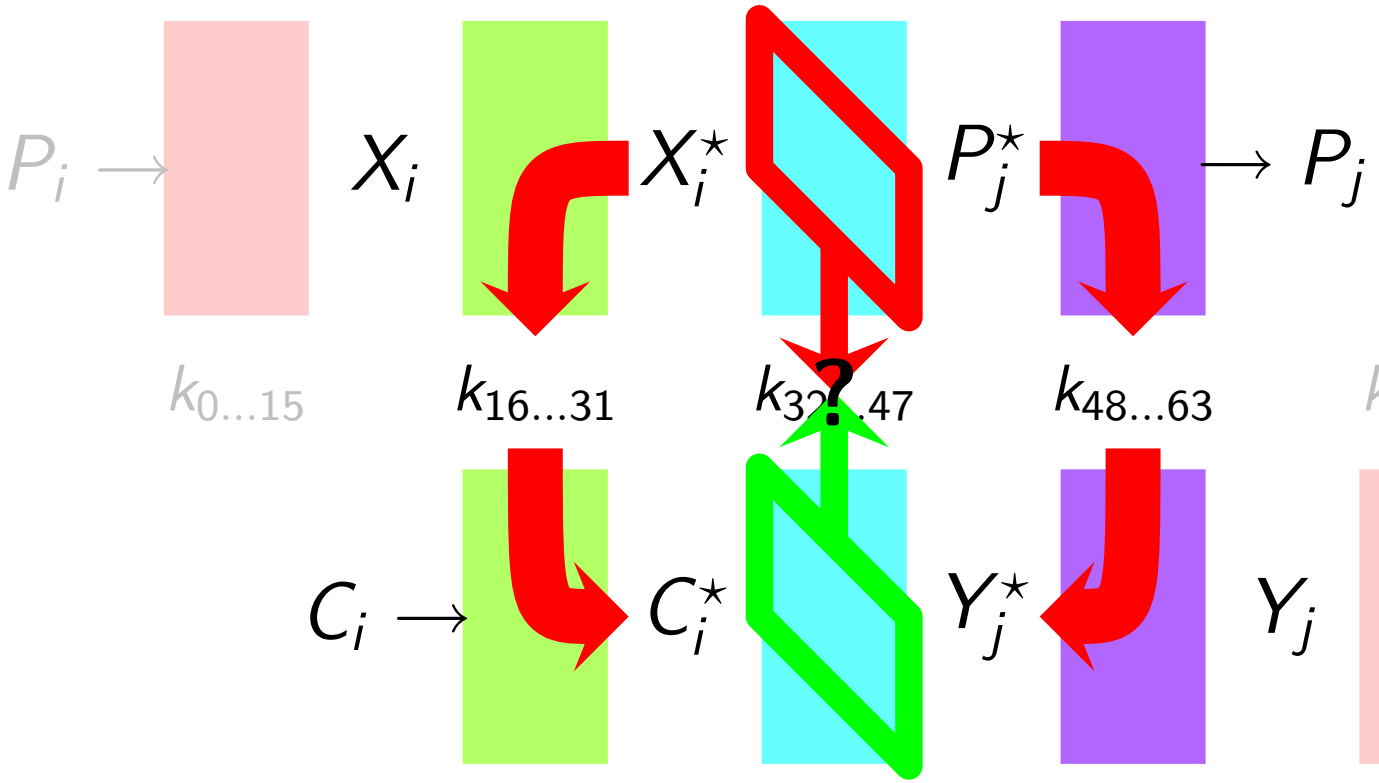



**Table**

$2^{16}$ tuples $\langle P_j^\star, Y_i^\star, k_{48\ldots63} \rangle$

Find $\pm 2^{16}$ **collision(s)** between $\overline{C_i^\star}$ and $\underline{Y_j^\star}$

# Basic Attack Scenario

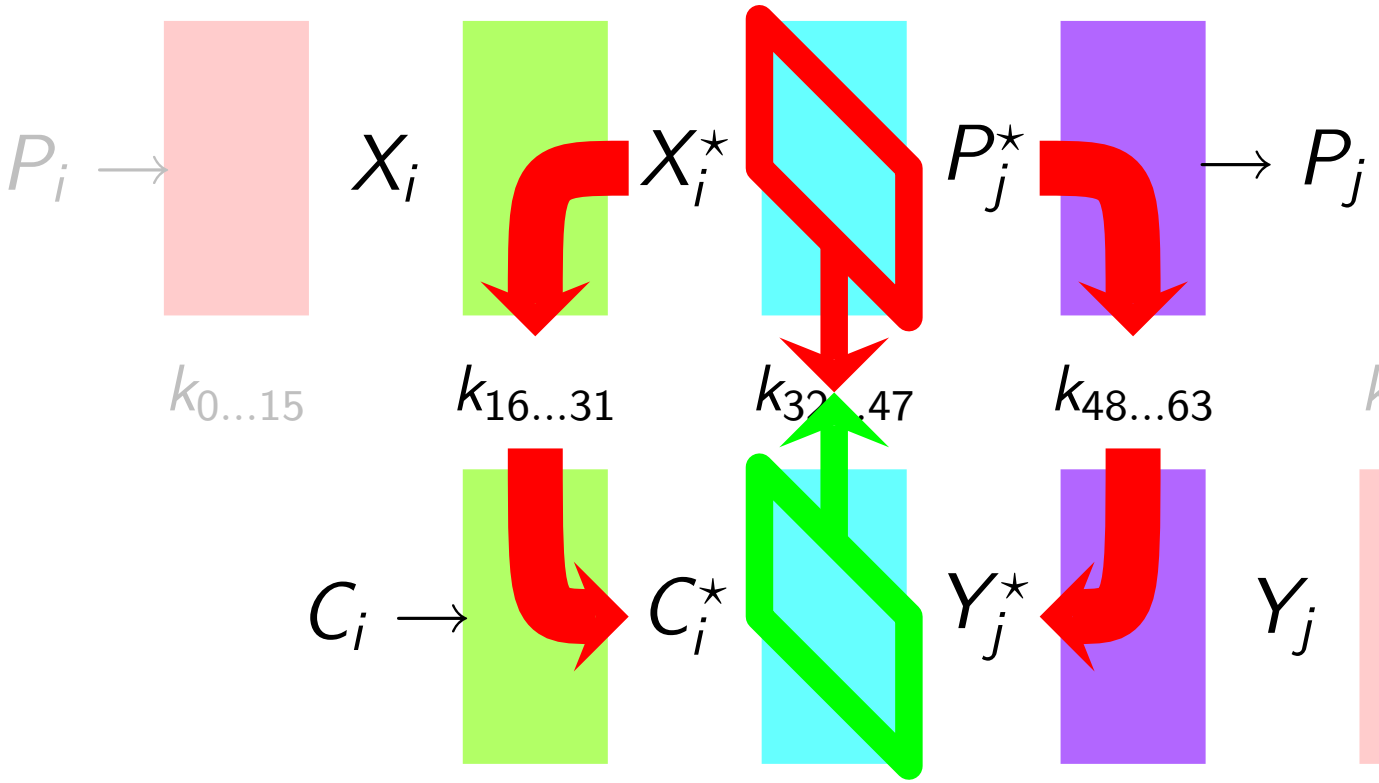



**Table**

$2^{16}$ tuples $\langle P_j^\star, Y_i^\star, k_{48\ldots63} \rangle$

**Determine** (and **check**) $k_{32\ldots47}$; $\pm 1$ collision survives

# Basic Attack Scenario

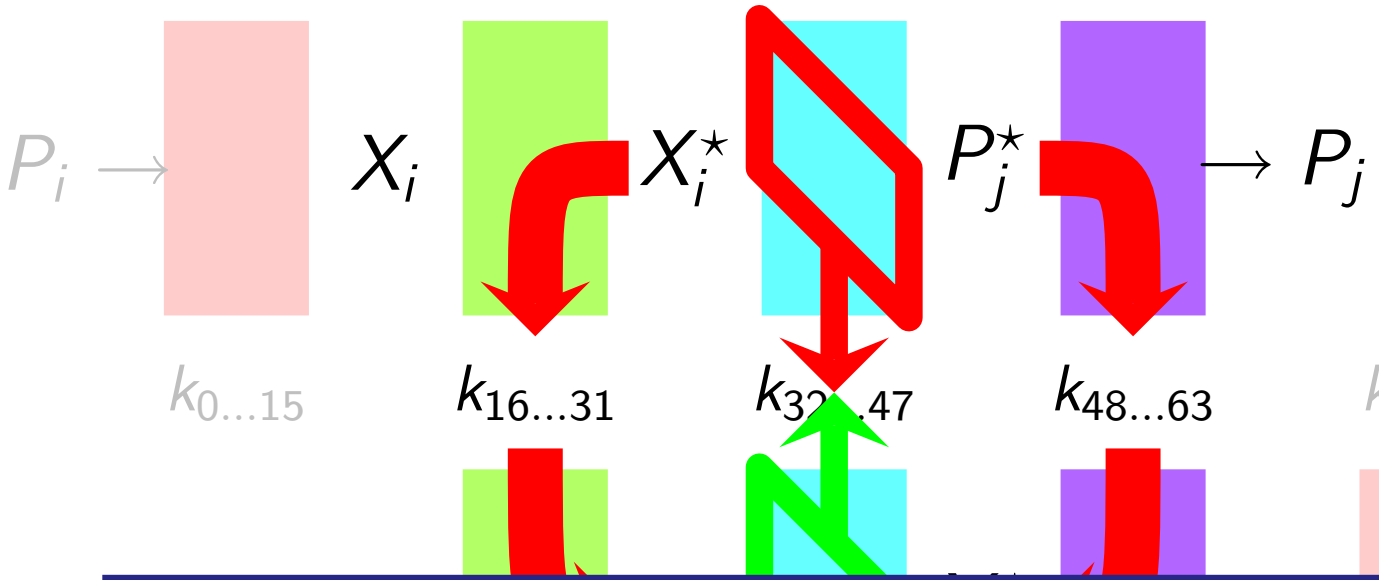



**Table**

$2^{16}$ tuples $\langle P_j^\star, Y_i^\star, k_{48...63} \rangle$

**Verify** key candidates using trial encryptions ($\pm 2^{16}$ in total)

# Basic Attack Scenario




## Table

$2^{16}$ tuples

$\langle P_j^\star, Y_i^\star, k_{48...63} \rangle$

## Complexity

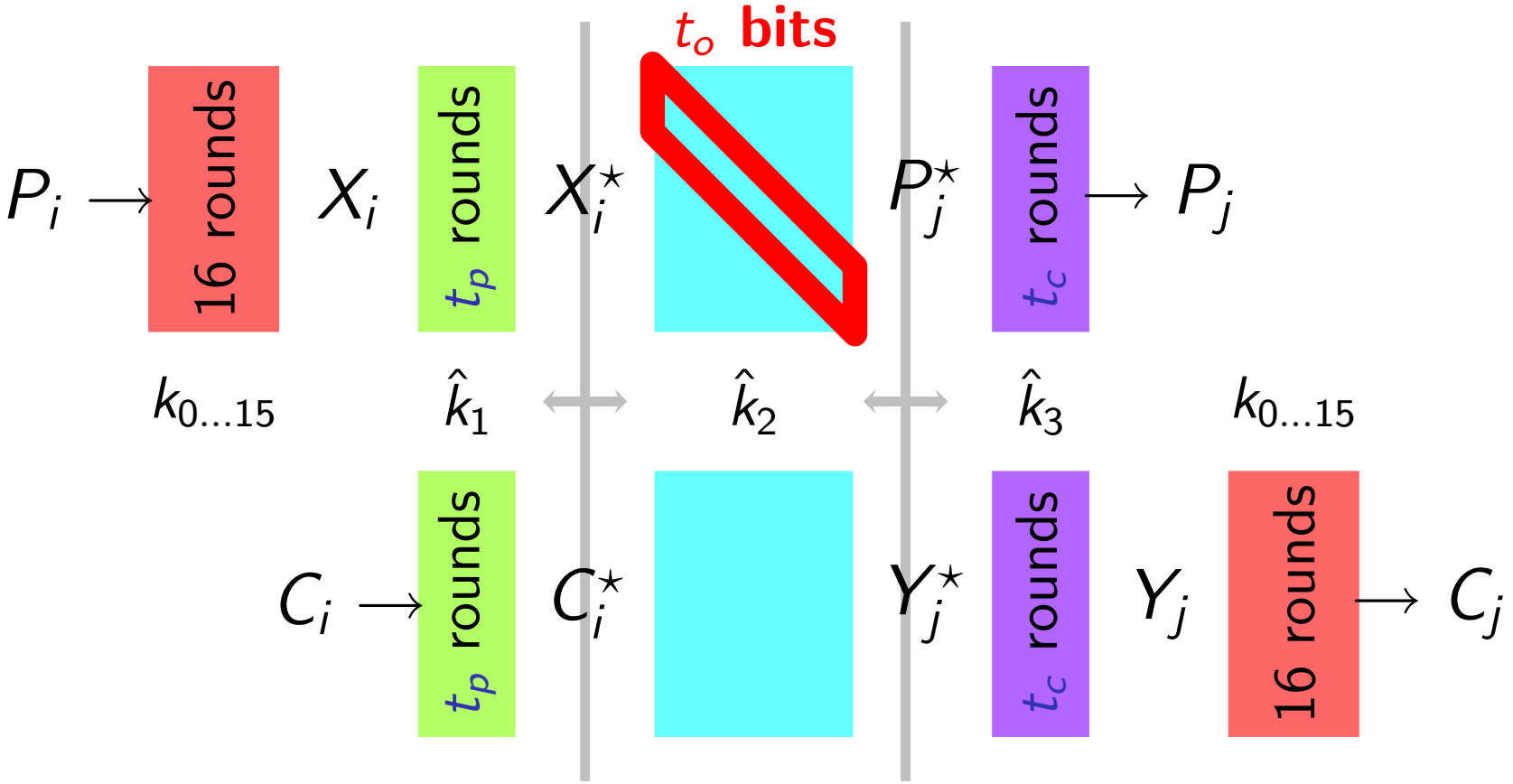
| | |
|---|---|
| Data | $2^{16}$ known plaintexts |
| Memory | $\pm 2$ MB for the table |
| Time | $2^{45}$ KeeLoq encryptions |

# A Generalisation of the Attack

Why **16 rounds** throughout the attack?

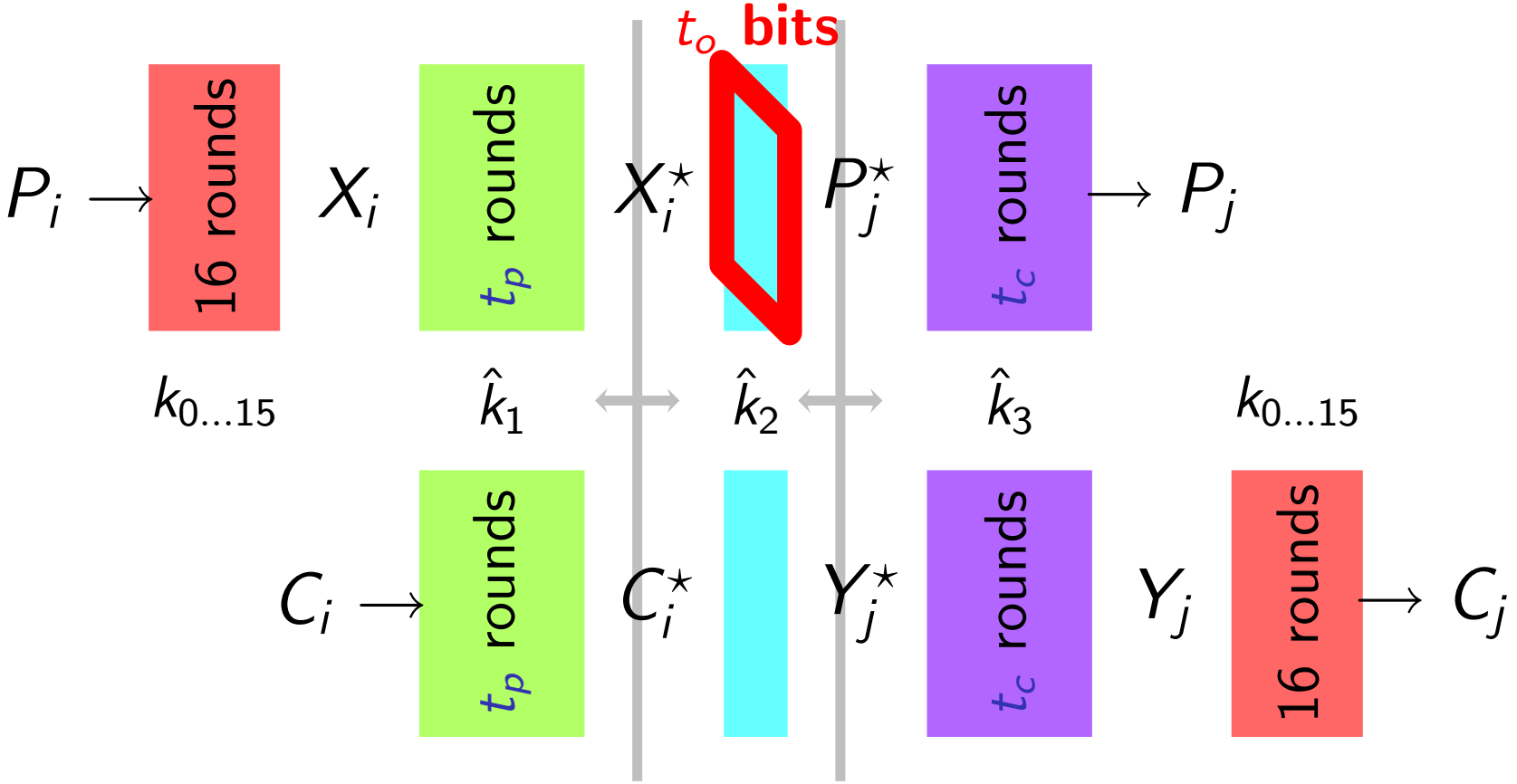
# A Generalisation of the Attack

Why **16 rounds** throughout the attack? **No reason!**



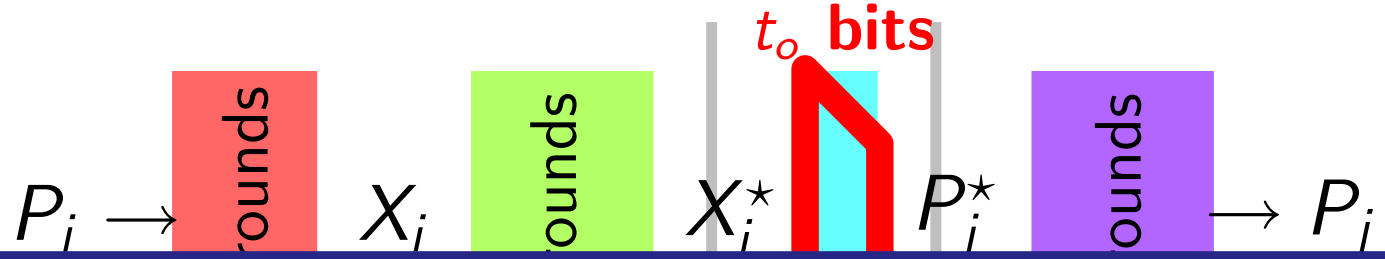
# A Generalisation of the Attack

Why **16 rounds** throughout the attack? **No reason!**



# A Generalisation of the Attack

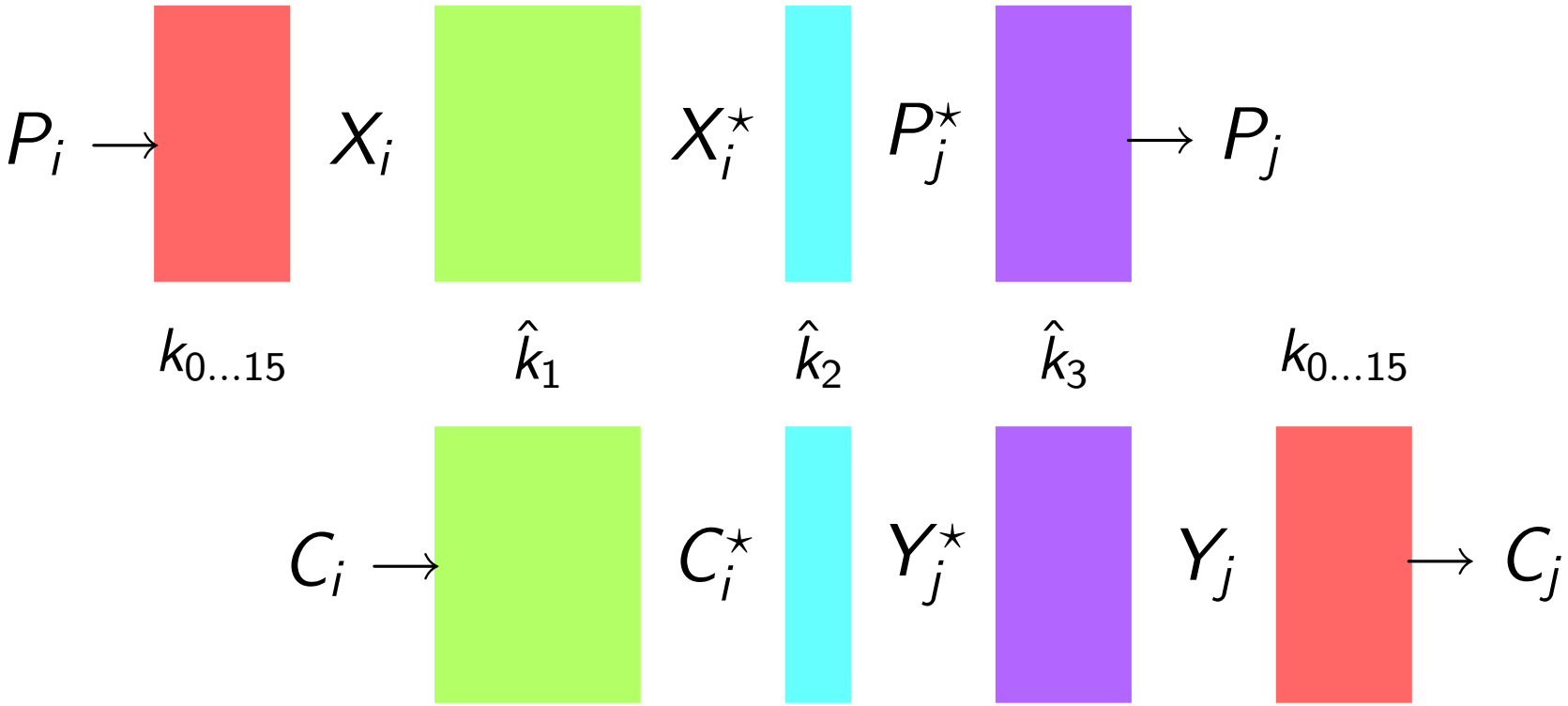
Why **16 rounds** throughout the attack? **No reason!**



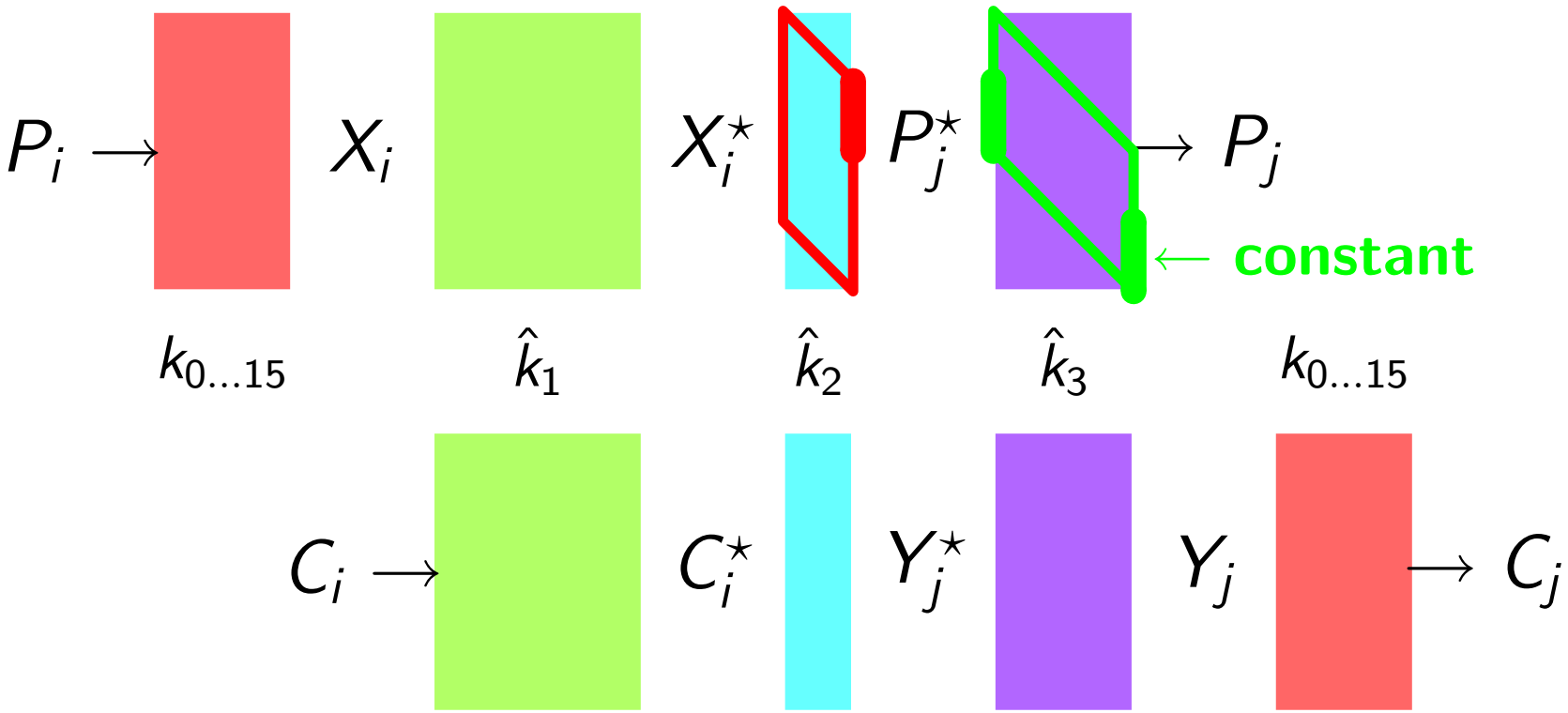

## Generalisation

- Parameters $t_p$ and $t_c$
- If $t_o \neq t_p, t_c$
  - Guess extra bits, or
  - Plaintext filtering
- Optimum?
  - $t_p = t_c = 15,\ t_o = 14$
  - $2^{44.5}$ KeeLoq encryptions

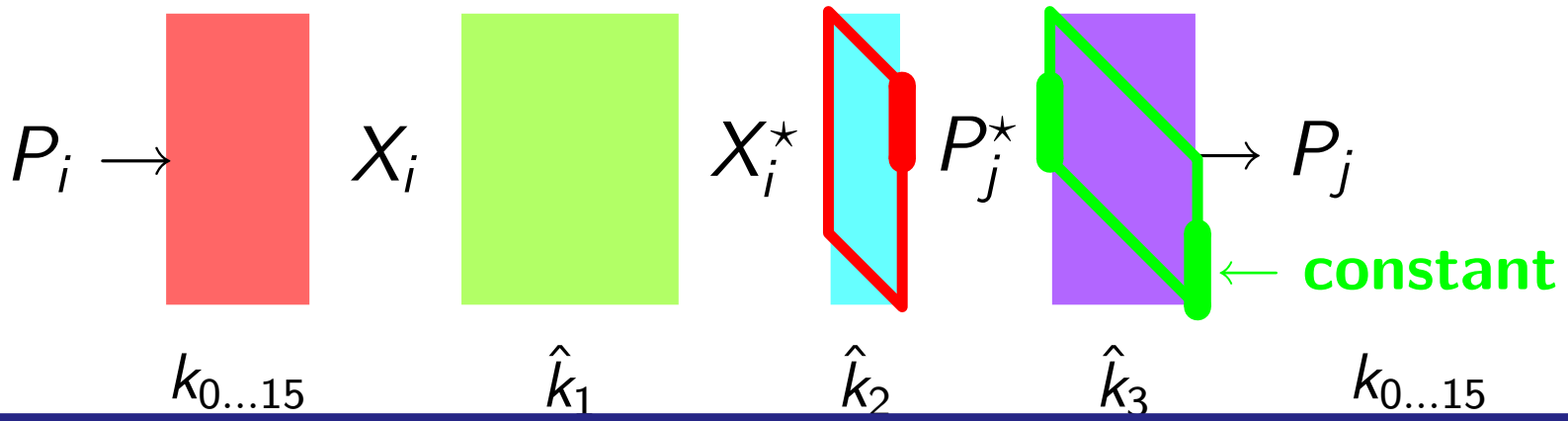
# A Chosen Plaintext Attack



# A Chosen Plaintext Attack



# A Chosen Plaintext Attack




## Chosen Plaintext Attack

- $t_o > t_c$
- Keep LSB's of plaintext **constant** $\longrightarrow$ **less guesses**
- Optimum $t_p = 20$, $t_c = 13$, $t_o = 17$
- Still $2^{44.5}$ KeeLoq encryptions...

# Outline

# Implementation

- Fully implemented (C and x86 asm) and tested
- 128-way **bitslicing**, where possible...
  - **Not** during collision verification

## Impact?

- Collision verification is **more expensive**
- Optimal $t_p$, $t_c$ change
- CP becomes **much faster** than KP in practice!

# Experimental Results

Experiments on one core of an AMD Athlon 64 X2 4200+*


## Known plaintext attack

- $2^{16} \times 10.97$ **minutes**, i.e., $\pm 500$ CPU days
- 288 times faster than [CB07]

## Chosen plaintext attack

- $2^{16} \times 4.79$ **minutes**, i.e., $\pm 218$ CPU days
- 661 times faster than [CB07]

*Average from 500 experiments. Standard deviation $< 2$ s.

# Practical Applicability of the Attack

## Authentication protocols

Authentication protocols based on KeeLoq, used e.g. in cars.

### "KeeLoq Rolling Codes"

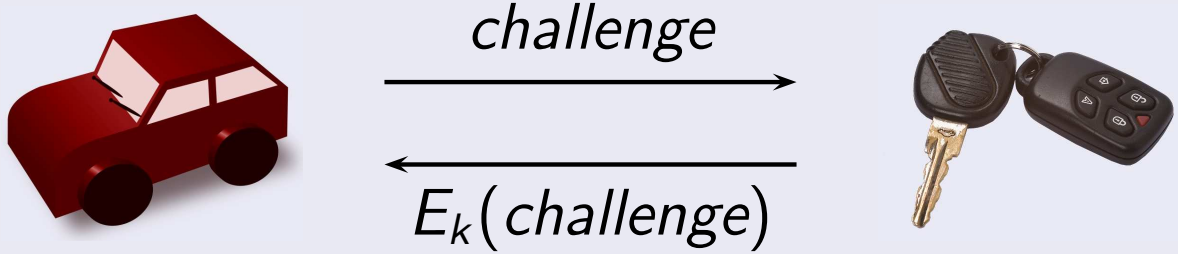
- One-pass authentication protocol using a synchronised 16-bit counter.
- Not interesting for our attack

# Practical Applicability of the Attack

## Authentication protocols (*continued*)

### "KeeLoq Identify Friend or Foe" (IFF) protocol

- Simple challenge-response authentication protocol.




- Challenges are **not authenticated**!
- **Chosen plaintext** ability!
- Gathering $2^{16}$ CP takes $\pm$65 minutes

# Practical Applicability of the Attack

## Key derivation

In KeeLoq, all secret keys are **derived from a master key**, using one of **four** ways:

### Derivation function

- **XOR**, or
- KeeLoq Decryption

### Use of a seed-value

- "Normal Learning", or
- "Secure Learning"

- XOR-based: $k = \mathrm{pad}(ID, seed) \oplus k_{\mathrm{master}}$
- Find **one** secret key, find the **master key**!

# Outline

# Conclusions

- **KeeLoq is badly broken**
  - Practical Slide/MitM attack using $2^{16}$ KP or CP
  - IFF protocol gives chosen plaintext ability
  - XOR-based key derivation is obviously flawed
- Soon, cryptographers will all drive expensive cars†

| Attack Type | Data | Time | Practice | Memory |
|---|---|---|---|---|
| Slide/MitM | $2^{16}$ KP | $2^{44.5}$ | 500 CPU days | $\pm$3 MB |
| Slide/MitM | $2^{16}$ CP | $2^{44.5}$ | 218 CPU days | $\pm$2 MB |

†Not all conclusions are to be taken too seriously. . .

# References


[B07] Andrey Bogdanov
Cryptanalysis of the KeeLoq block cipher
Cryptology ePrint Archive, Report 2007/055

[B07b] Andrey Bogdanov
Attacks on the KeeLoq Block Cipher and Authentication Systems
3rd Conference on RFID Security 2007

[CB07] Nicolas T. Courtois and Gregory V. Bard
Algebraic and Slide Attacks on KeeLoq
Cryptology ePrint Archive, Report 2007/062

[C+08] Nicolas T. Courtois, Gregory V. Bard and David Wagner
Algebraic and Slide Attacks on KeeLoq
Proceedings of Fast Software Encryption 2008

[E+08] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh and Mohammad T. Manzuri Shalmani
Physical Cryptanalysis of KeeLoq Code Hopping Applications
Cryptology ePrint Archive, Report 2008/058