Breaking PANTHER

Christina Boura, Rachelle Heim Boissier, Yann Rotella

Paris-Saclay University - Versailles University

AFRICACRYPT 2022
Fez, Morocco

About PANTHER

- PANTHER is a lightweight AEAD scheme designed by Bhargavi, Srinivasan and Lakshmy
- Published at INDOCRYPT 2021
- Sponge/duplex-based mode of operation, with a 328-bit state
- Underlying permutation F based on 4 interconnected NFSRs

Our contribution

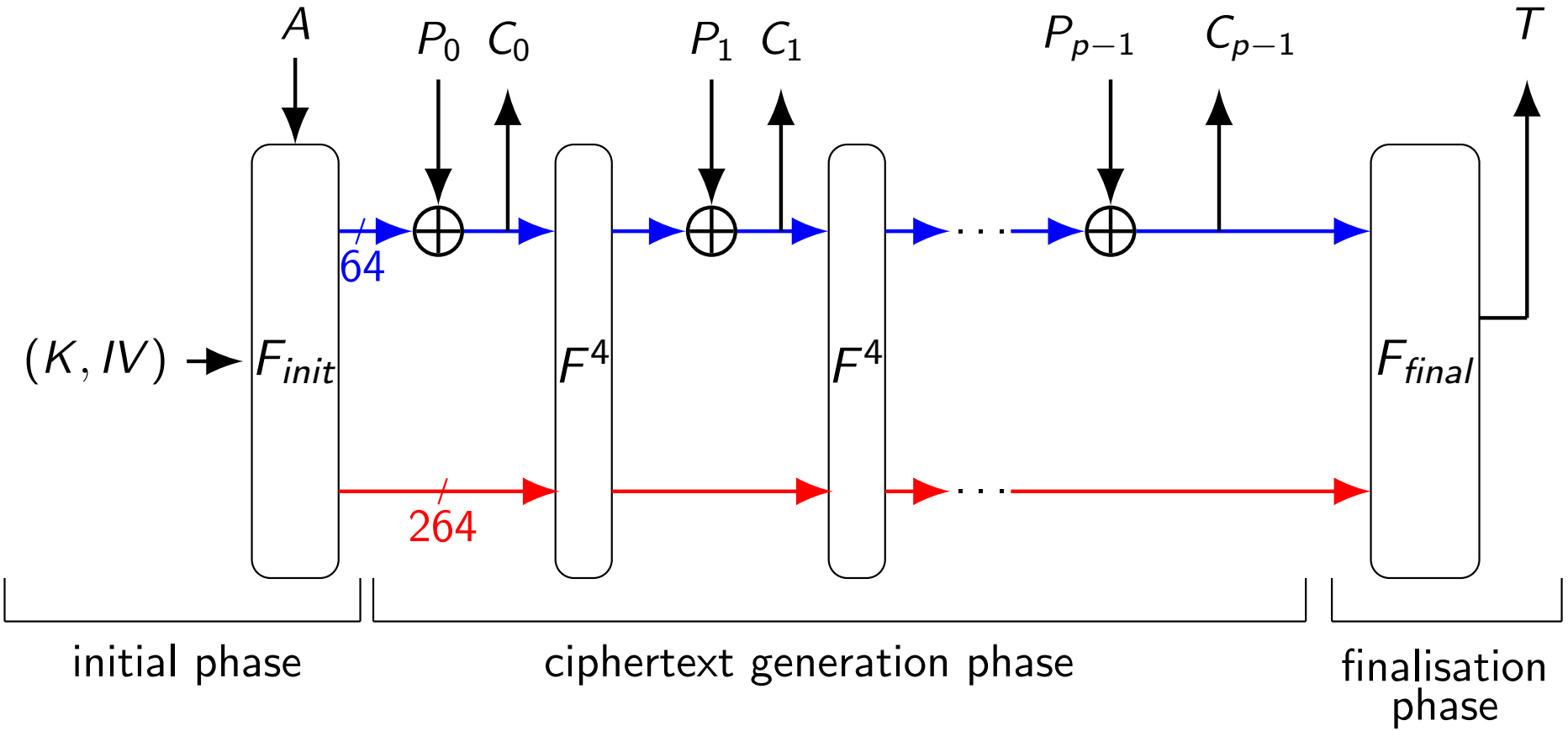
Model	**Type**	**Data** #P/C or #C	**Time** C_E	**Memory**
Known-plaintext	Key recovery	1	≤ 2	neg.
Known-ciphertext	Forge	1	≤ 2	neg.
Known-ciphertext	Plaintext recovery	1	≤ 2	neg.

Implementation & verification:

- We implemented our attacks in C
- Practical complexities match the theory

Plan

PANTHER's mode

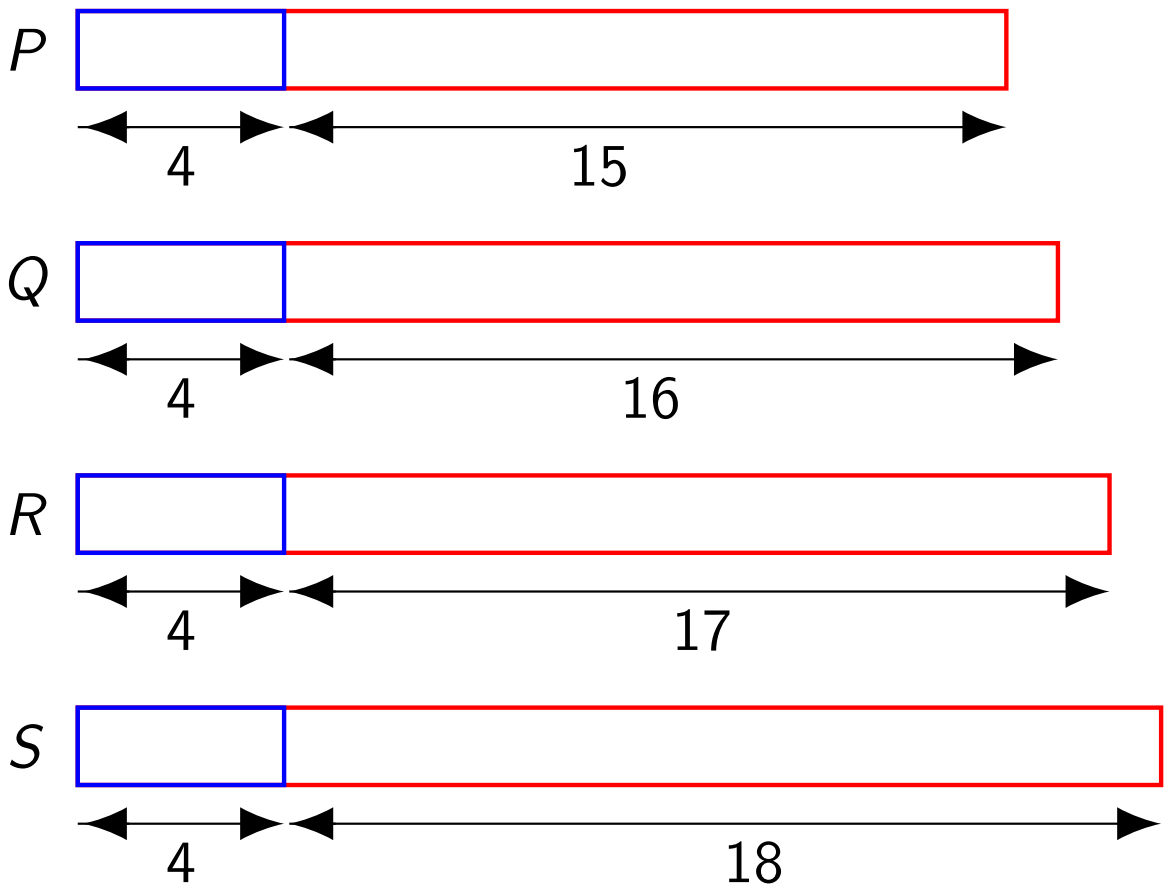


328-bit state divided into two parts :

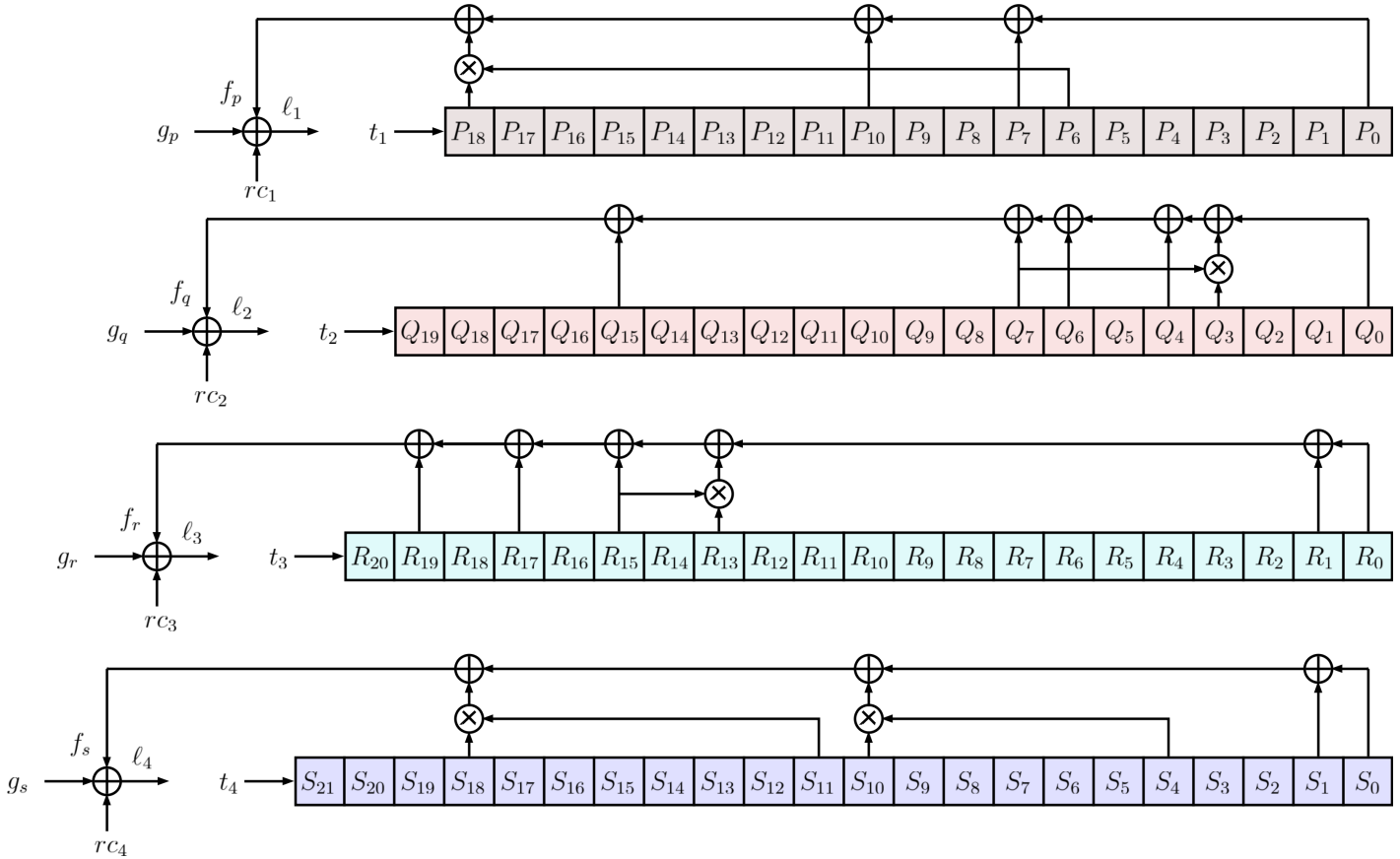
- 64-bit **outer state**
- 264-bit **inner state**

PANTHER's state

- The state is divided into **4 registers**: P, Q, R, S
- Each register is split into resp. 19, 20, 21, 22 nibbles

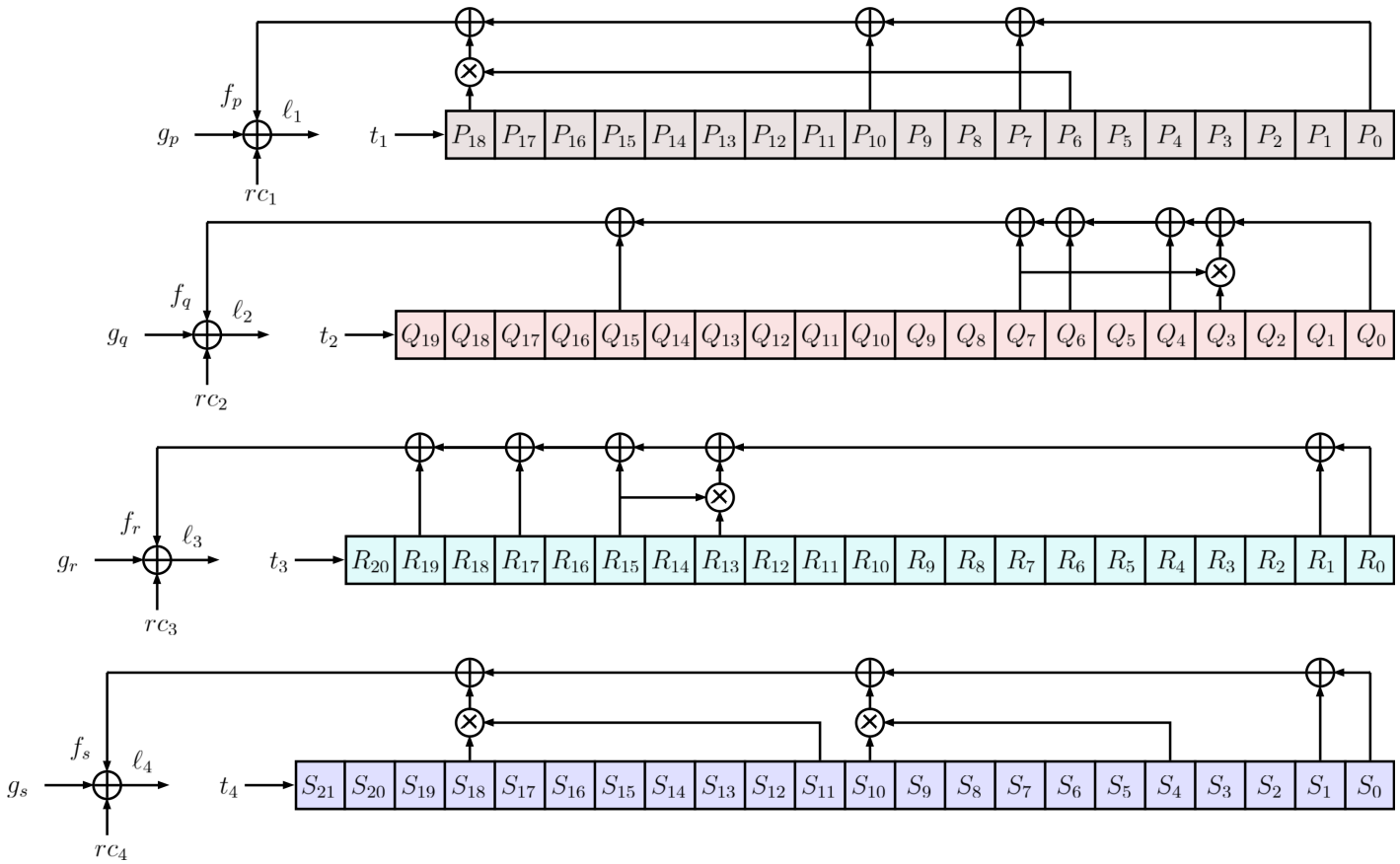


The state update function



- The state is loaded into four interconnected NFSRs
- f_p, f_q, f_r, f_s depend non-linearly on the nibbles of resp. P, Q, R, S
- g_p, g_q, g_r, g_s are a linear combination of the nibbles of other registers

The state update function

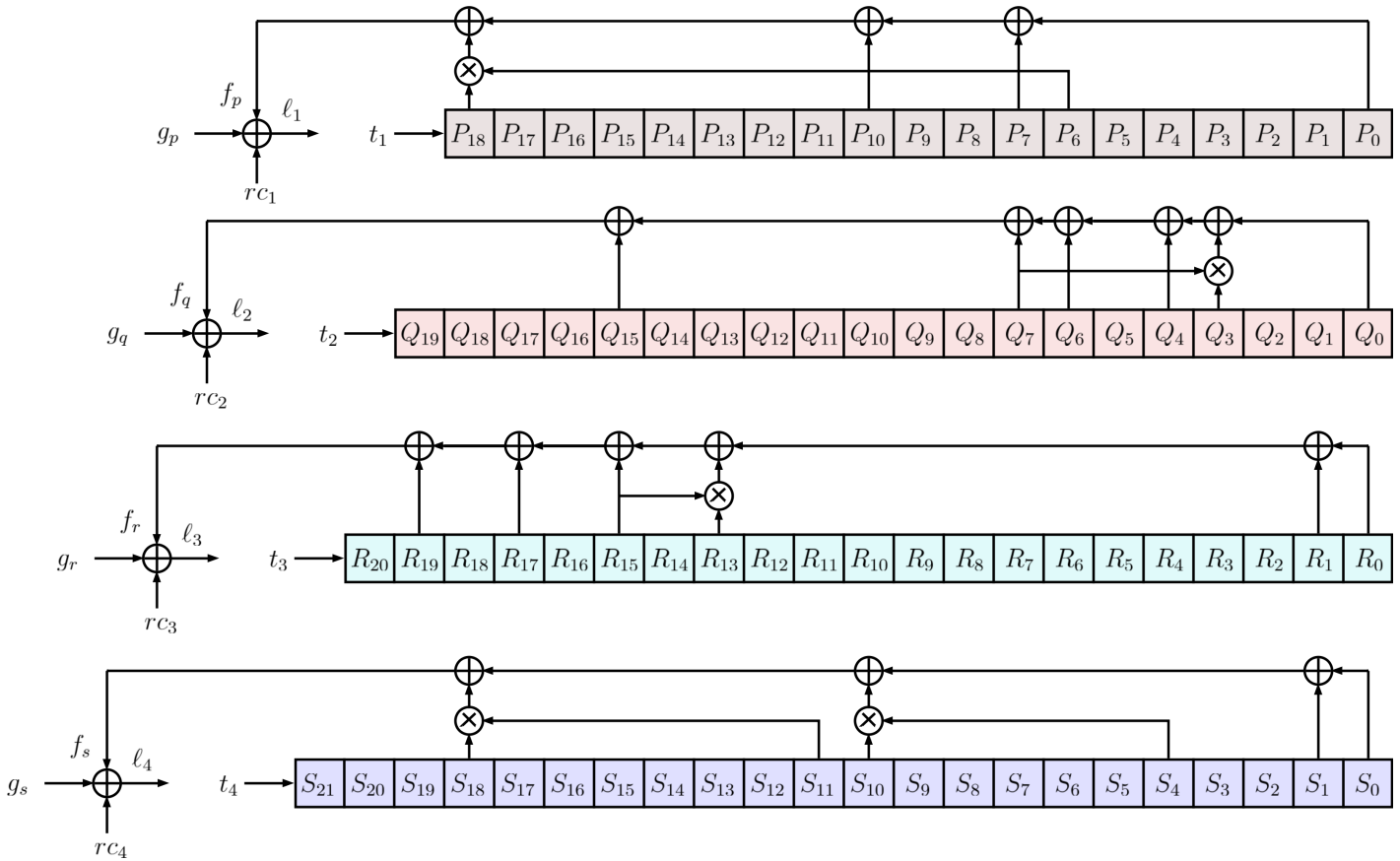


$$\begin{aligned}\ell_1 &= f_p \oplus g_p \oplus rc_1\\ \ell_2 &= f_q \oplus g_q \oplus rc_2\\ \ell_3 &= f_r \oplus g_r \oplus rc_3\\ \ell_4 &= f_s \oplus g_s \oplus rc_4\end{aligned} \longrightarrow T_p \longrightarrow \begin{matrix}S_b\\S_b\\S_b\\S_b\end{matrix} \longrightarrow T_p \longrightarrow \begin{matrix}t_1\\t_2\\t_3\\t_4\end{matrix}$$

Plan

Main observation

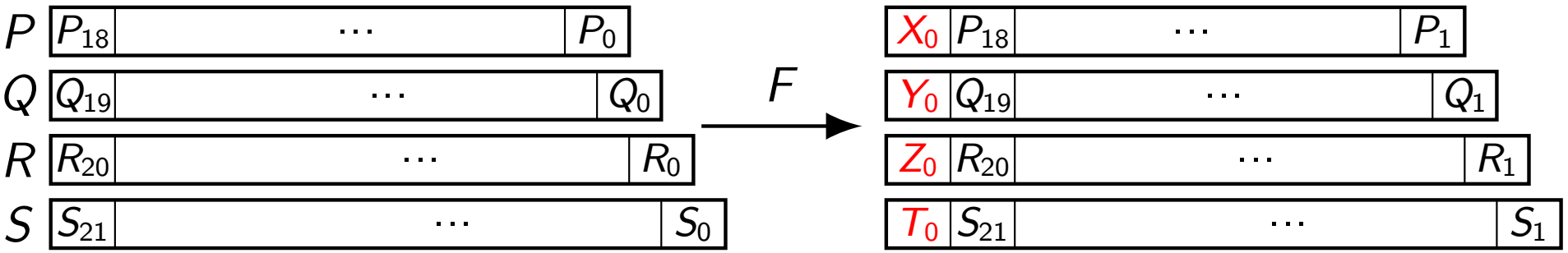
About F



- After each application of F, 1 nibble/register has been modified
- The other nibbles have only been **shifted towards the right**

Main observation

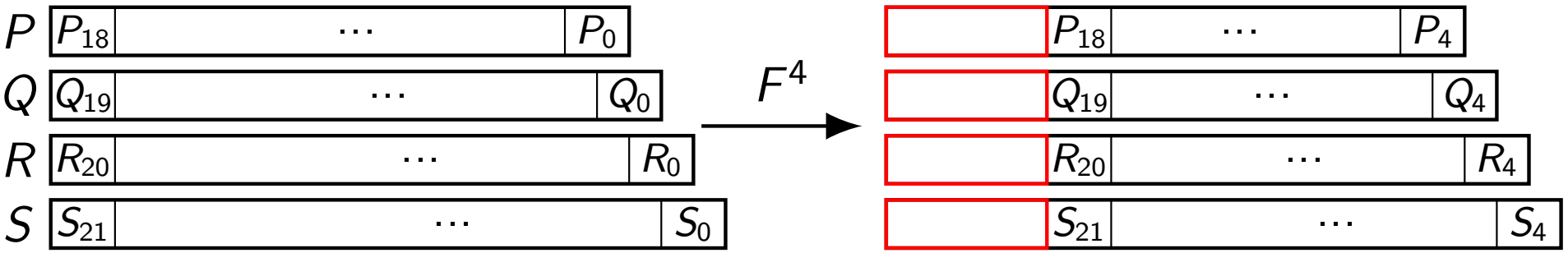
On F



- After an application of F, 1 nibble per register has been modified
- The other nibbles have only been **shifted towards the right**

Main observation

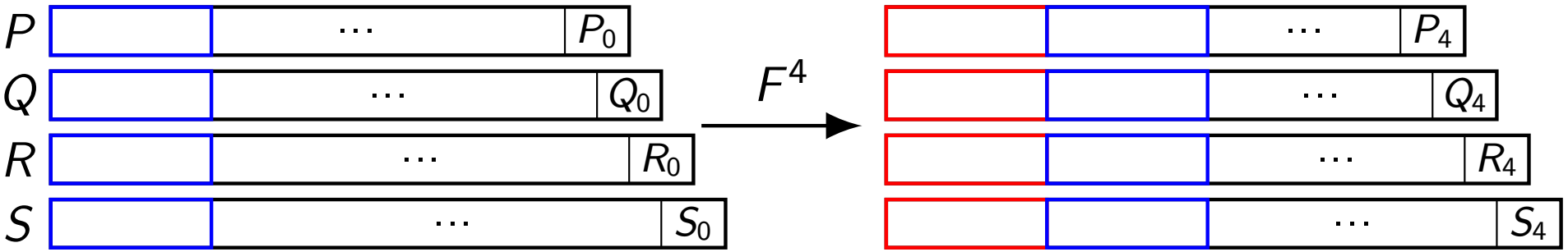
On F^4



- After an application of F^4, 4 nibbles per register have been modified
- The other nibbles have only been **shifted towards the right**

Main observation

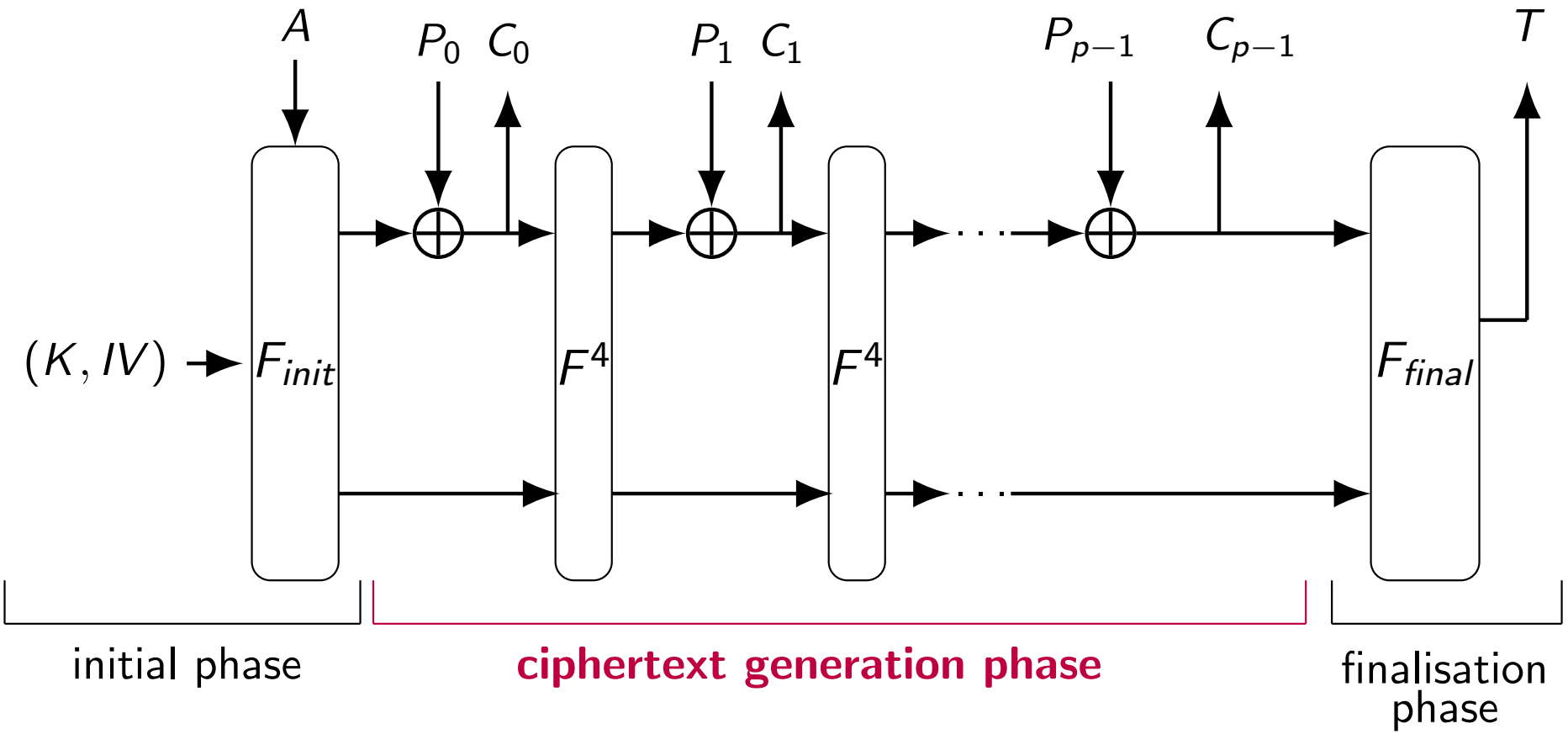
On F^4



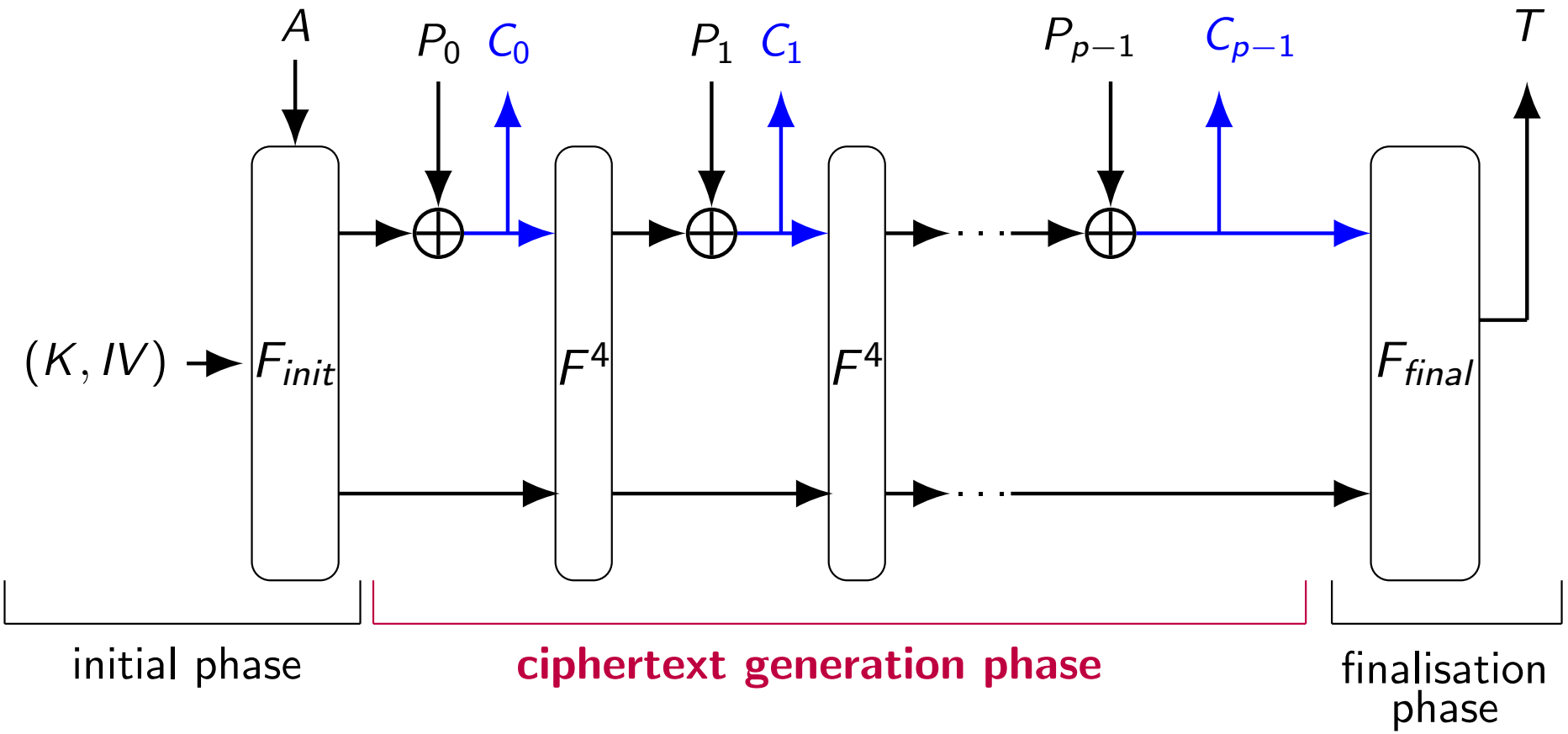
- After an application of F^4, 4 nibbles per register have been modified
- The other nibbles have only been **shifted towards the right**

The outer state has been **shifted into the inner state**

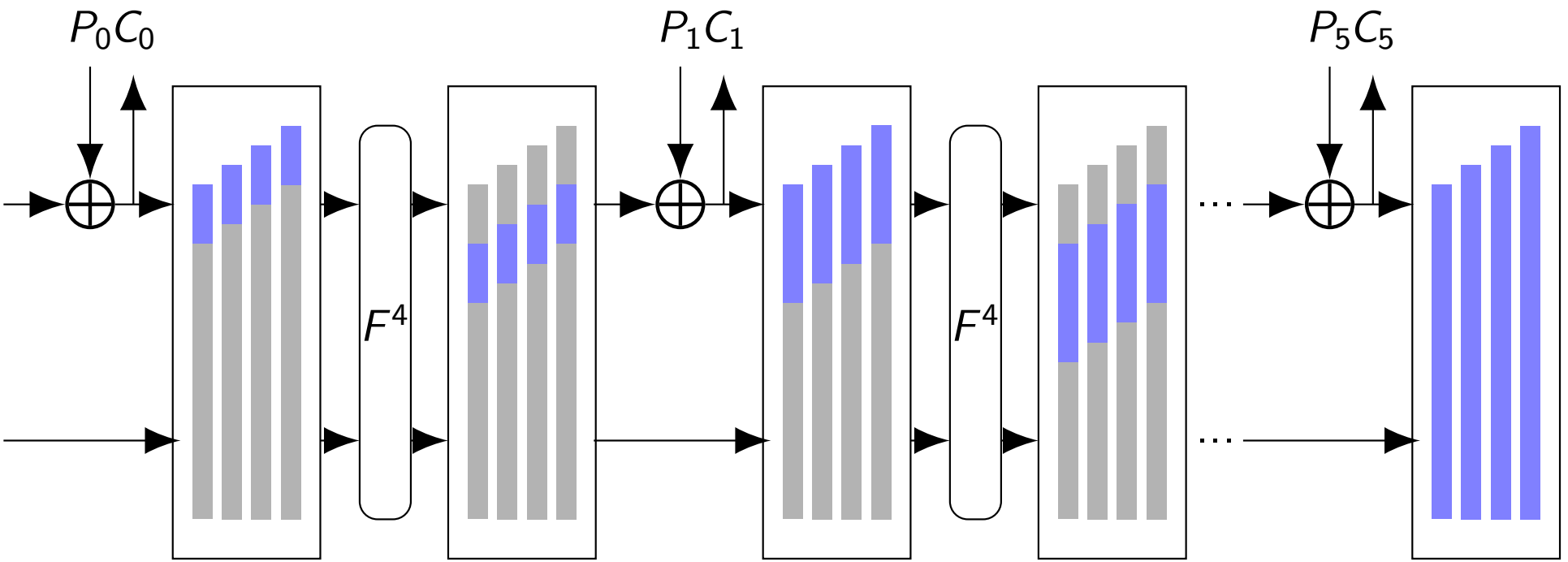
Main observation



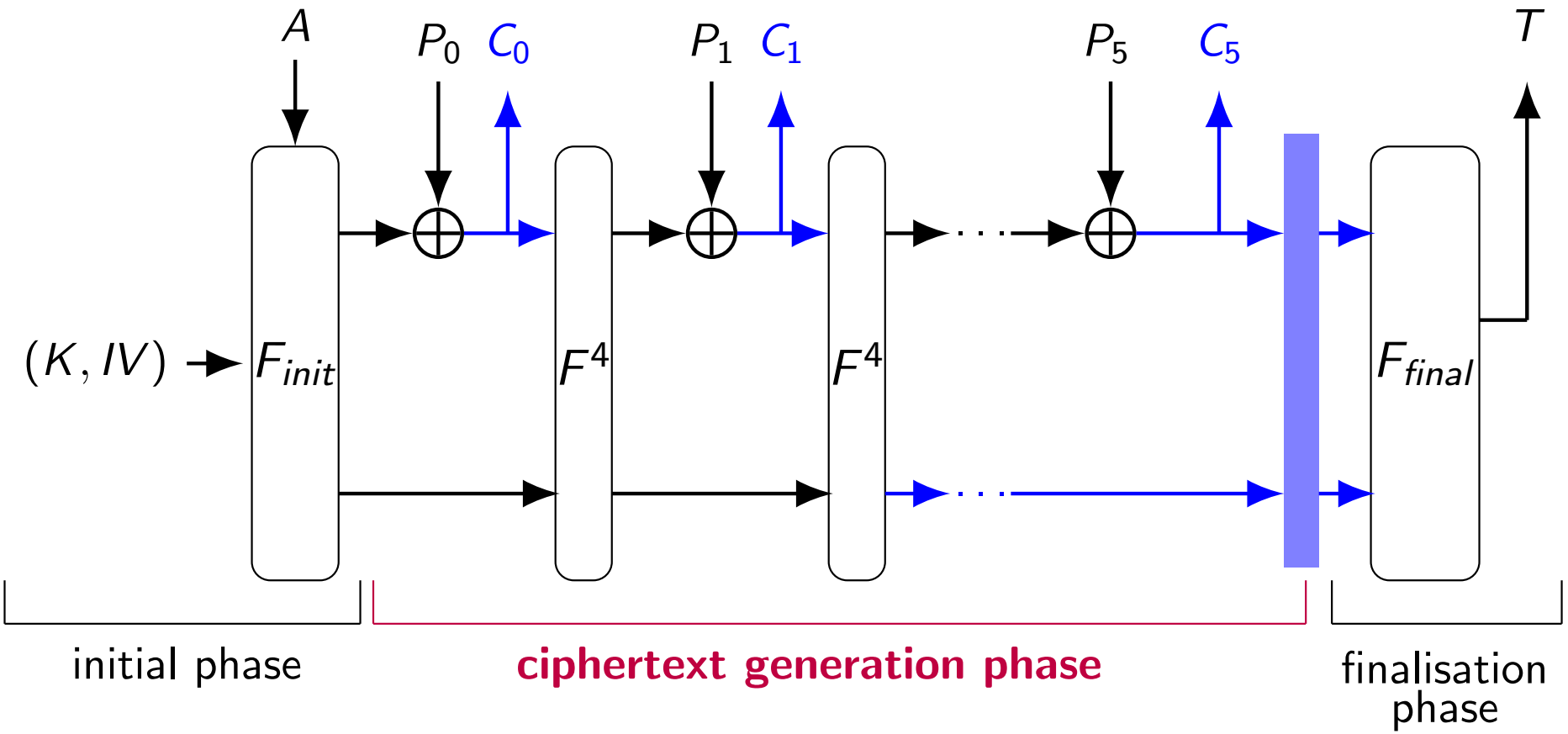
Main observation



Main observation



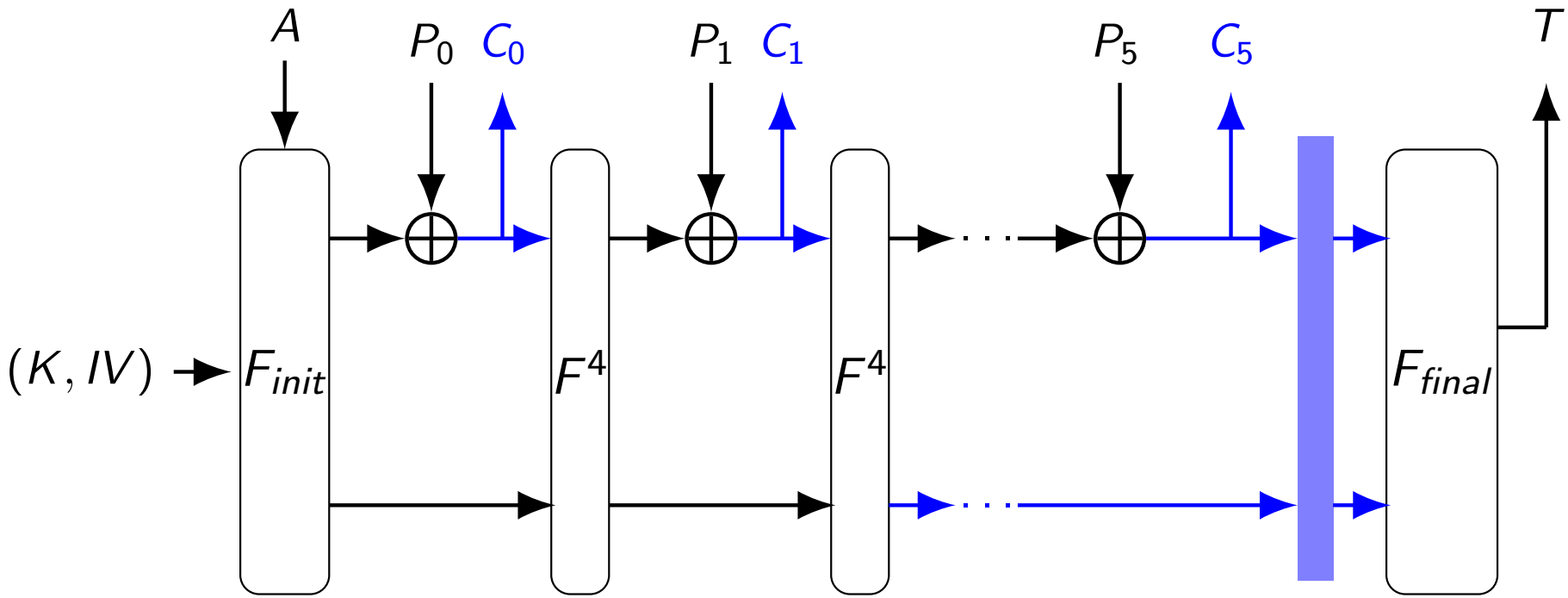
Main observation



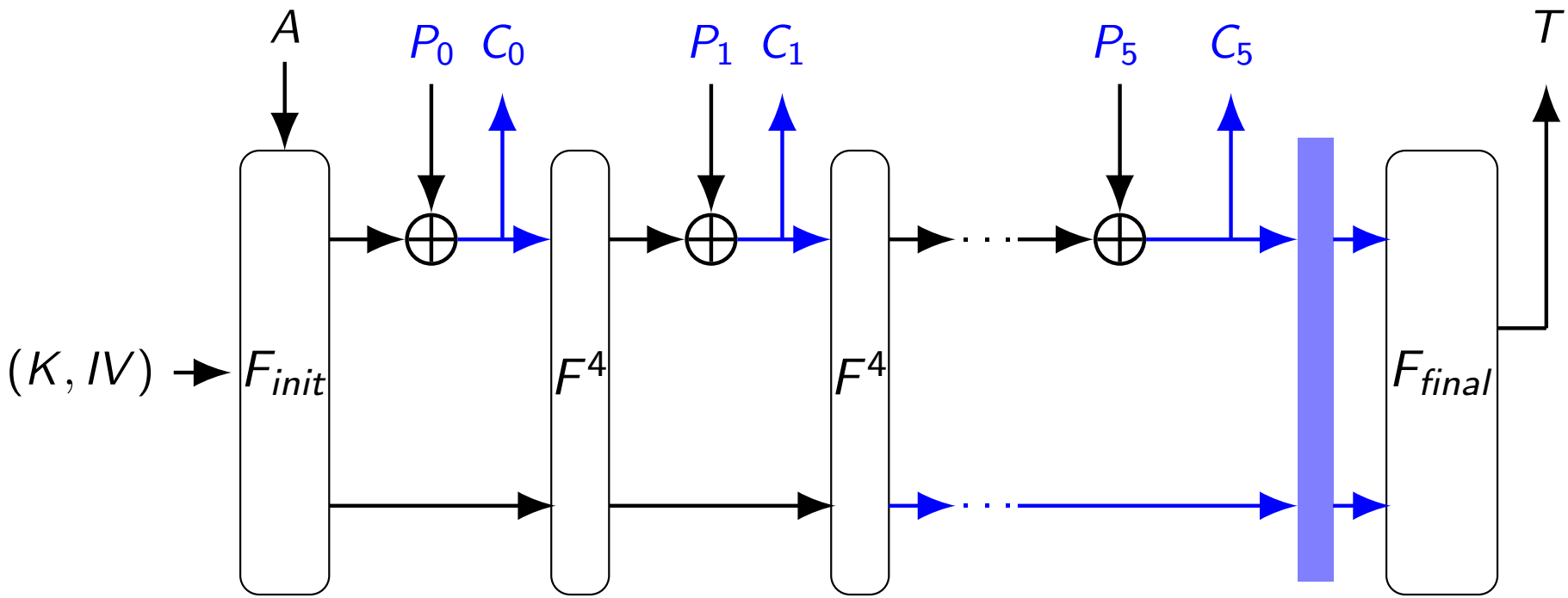
For **any** ciphertext of at least 6 blocks, **the whole state is recovered**

Plan

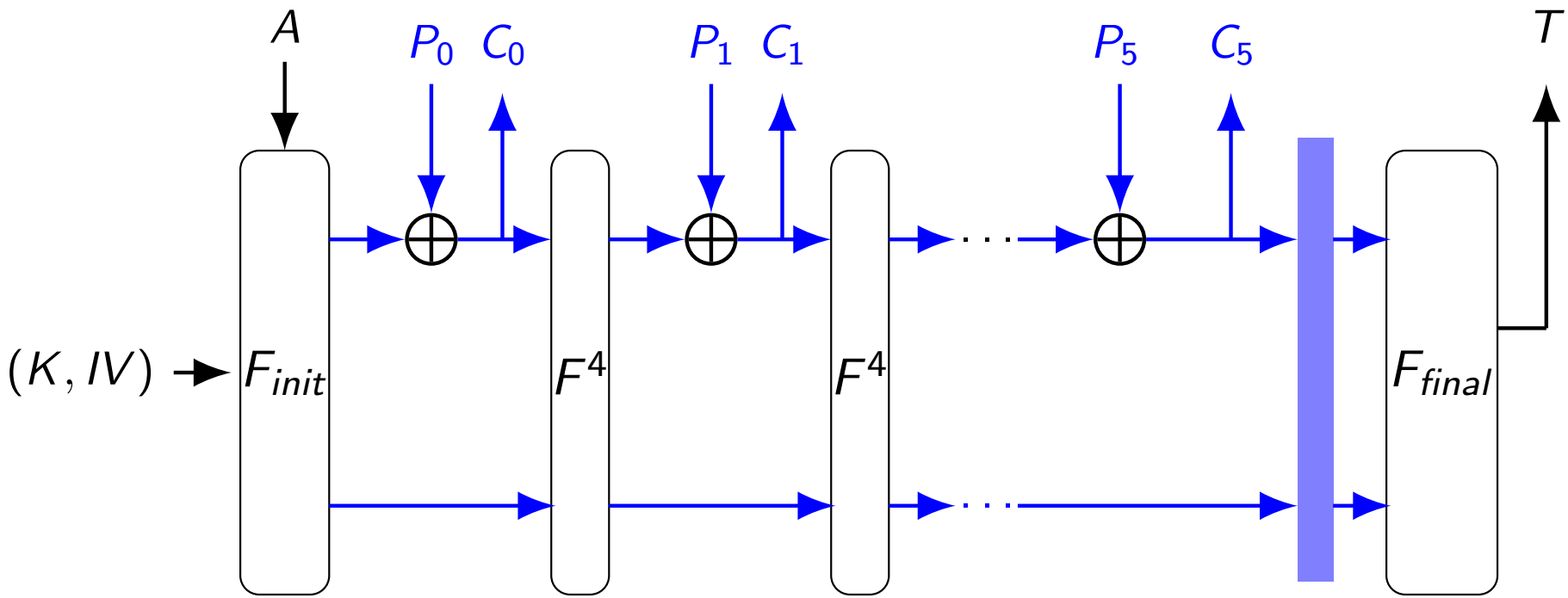
Key-recovery attack with any plaintext/ciphertext pair



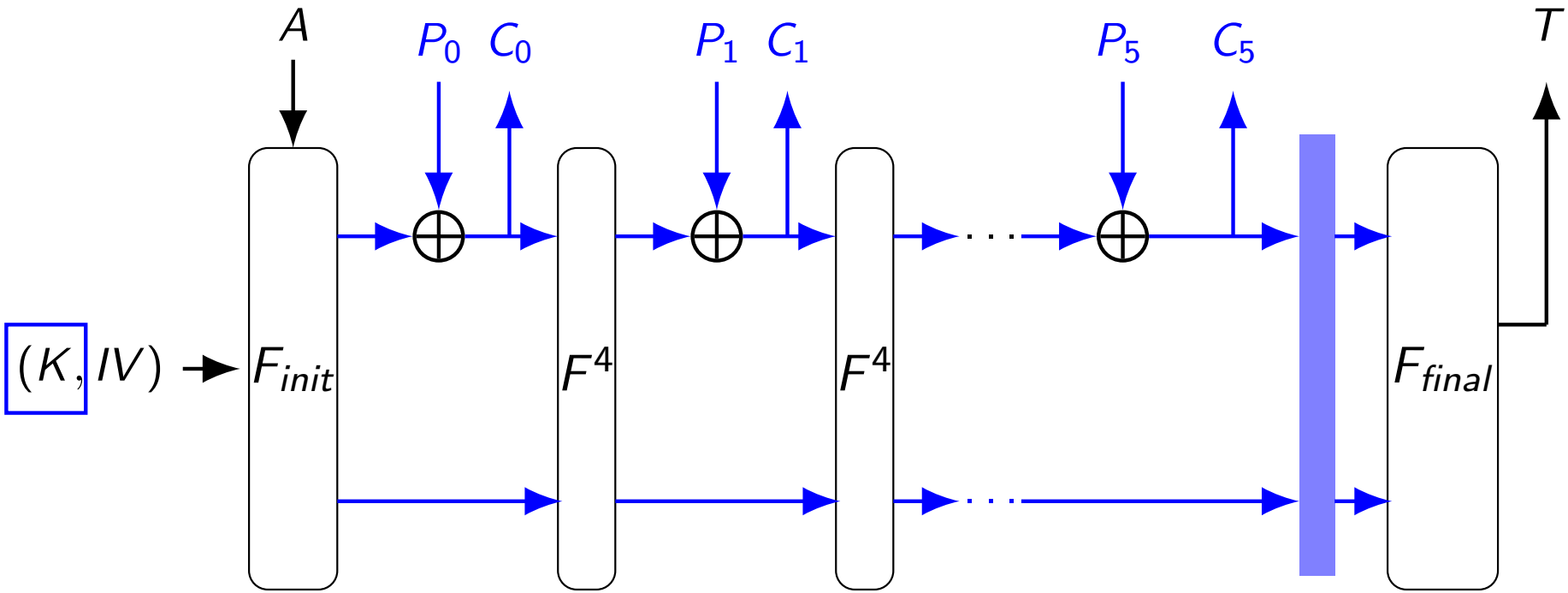
Key-recovery attack with any plaintext/ciphertext pair



Key-recovery attack with any plaintext/ciphertext pair

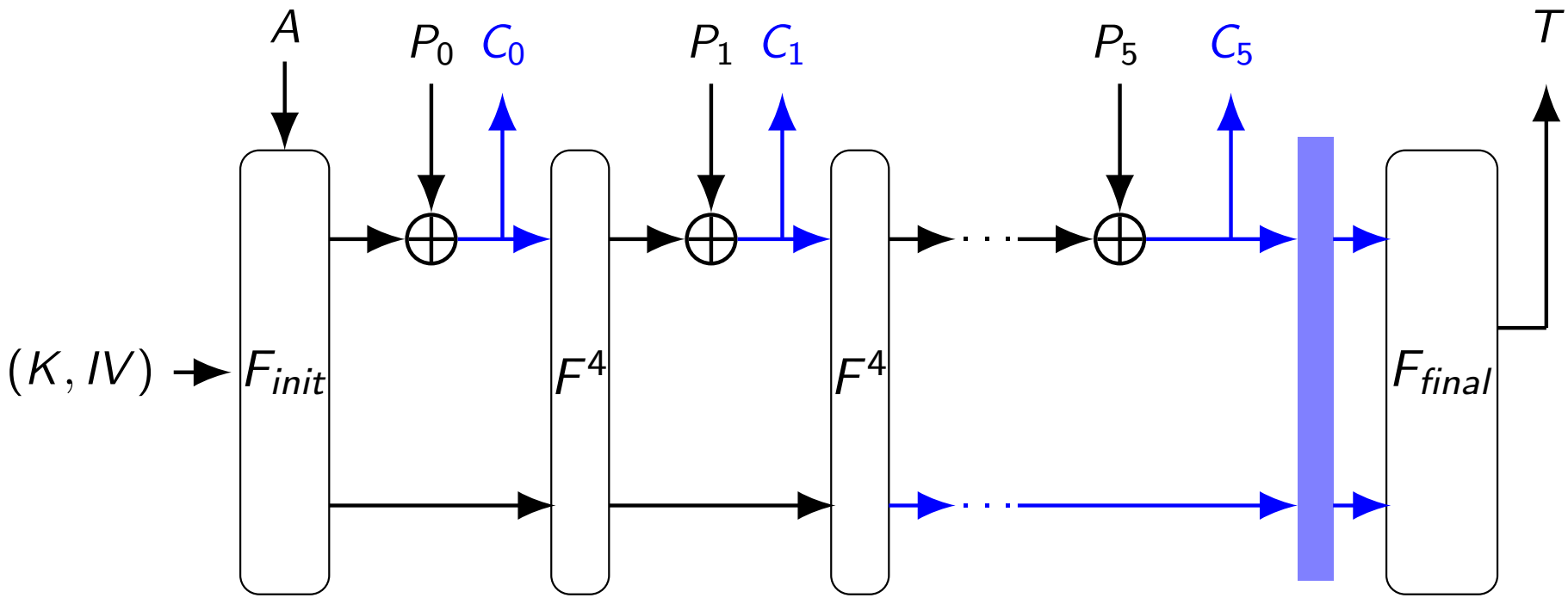


Key-recovery attack with any plaintext/ciphertext pair

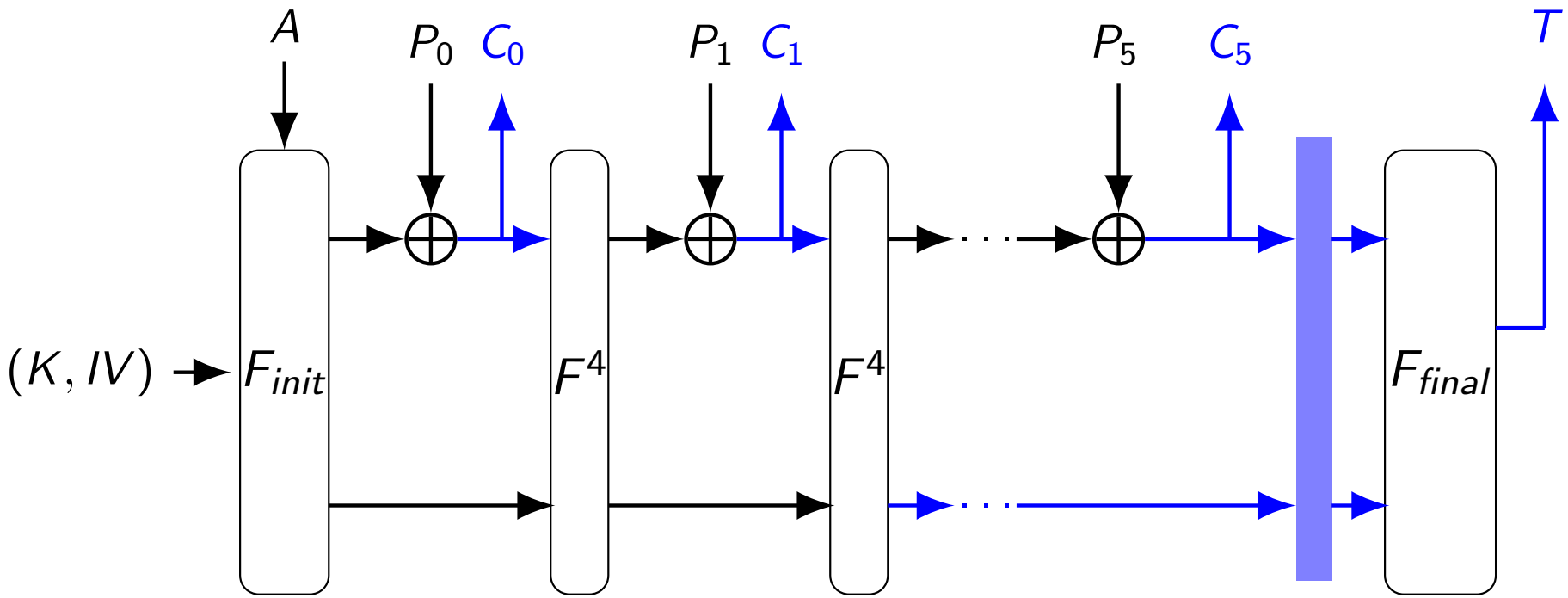


With 1 plaintext/ciphertext pair, K **is recovered**

Forging any ciphertext

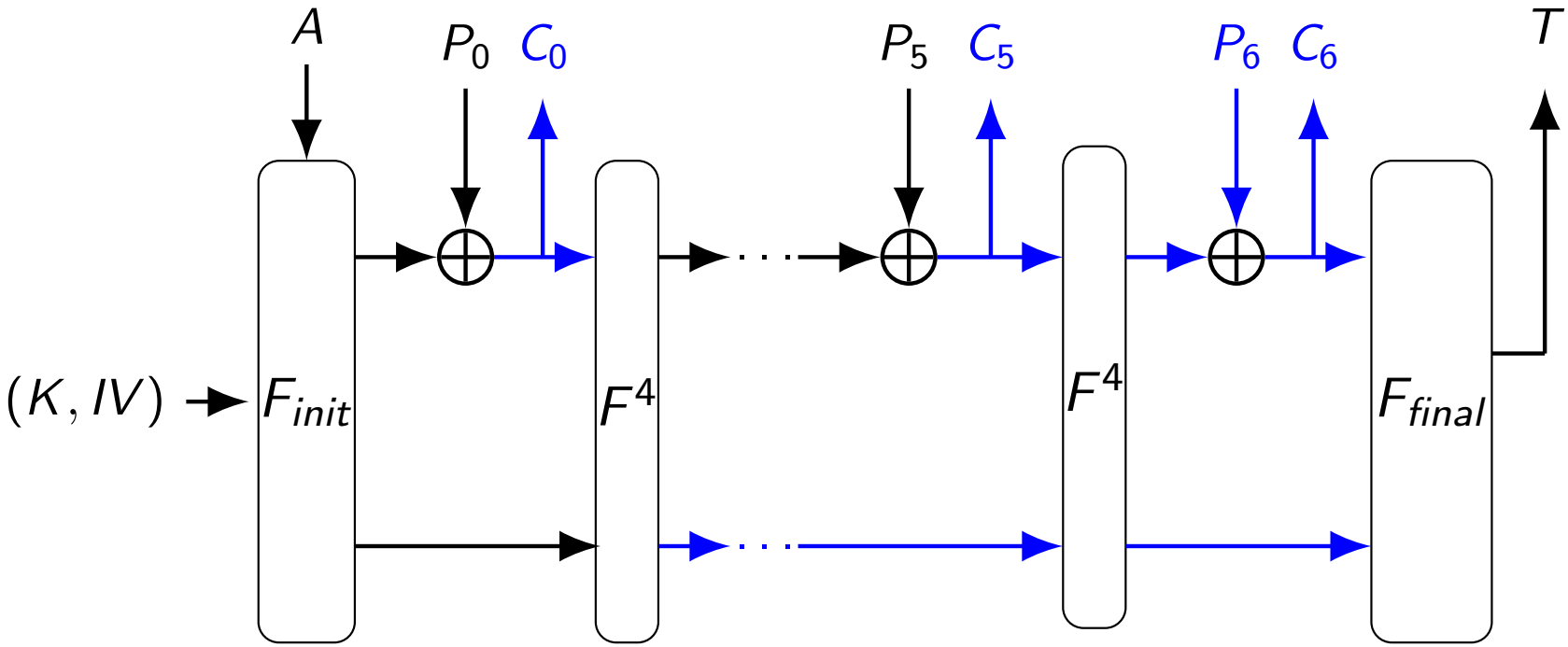


Forging any ciphertext



A valid pair (C, T) **is forged** for any ciphertext at least 5 blocks-long

Plaintext-recovery attack with one known ciphertext



With 48 bytes of ciphertext, **all following plaintext blocks are recovered**

Plan

Conclusion

Key take-away:

When using a duplex-based mode, the inner state should remain secret

Otherwise, several devastating attacks.

In the case of Panther:

- Decoding is **as expensive as attacking**
- In the **two strongest models**: known-ciphertext / known-plaintext
- All attacks are **memoryless**

Thank you for your attention.

Any questions?