Side-Channeling the Kalyna Key Expansion Algorithm

Chitchanok Chuengsatiansup, Daniel Genkin, Yuval Yarom, **Zhiyuan Zhang**

THE UNIVERSITY of ADELAIDE

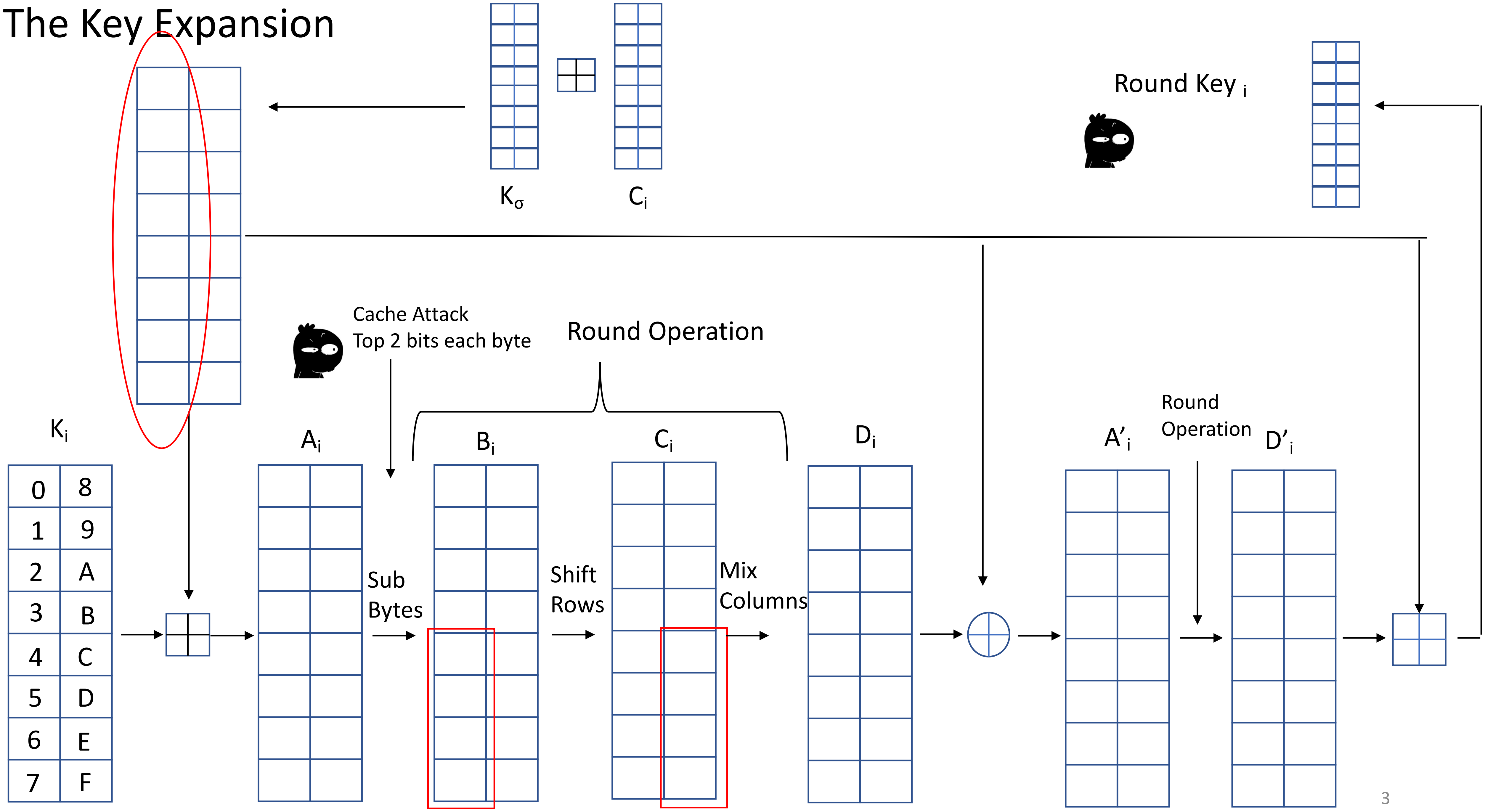
UNIVERSITY OF MICHIGAN

DATA 61

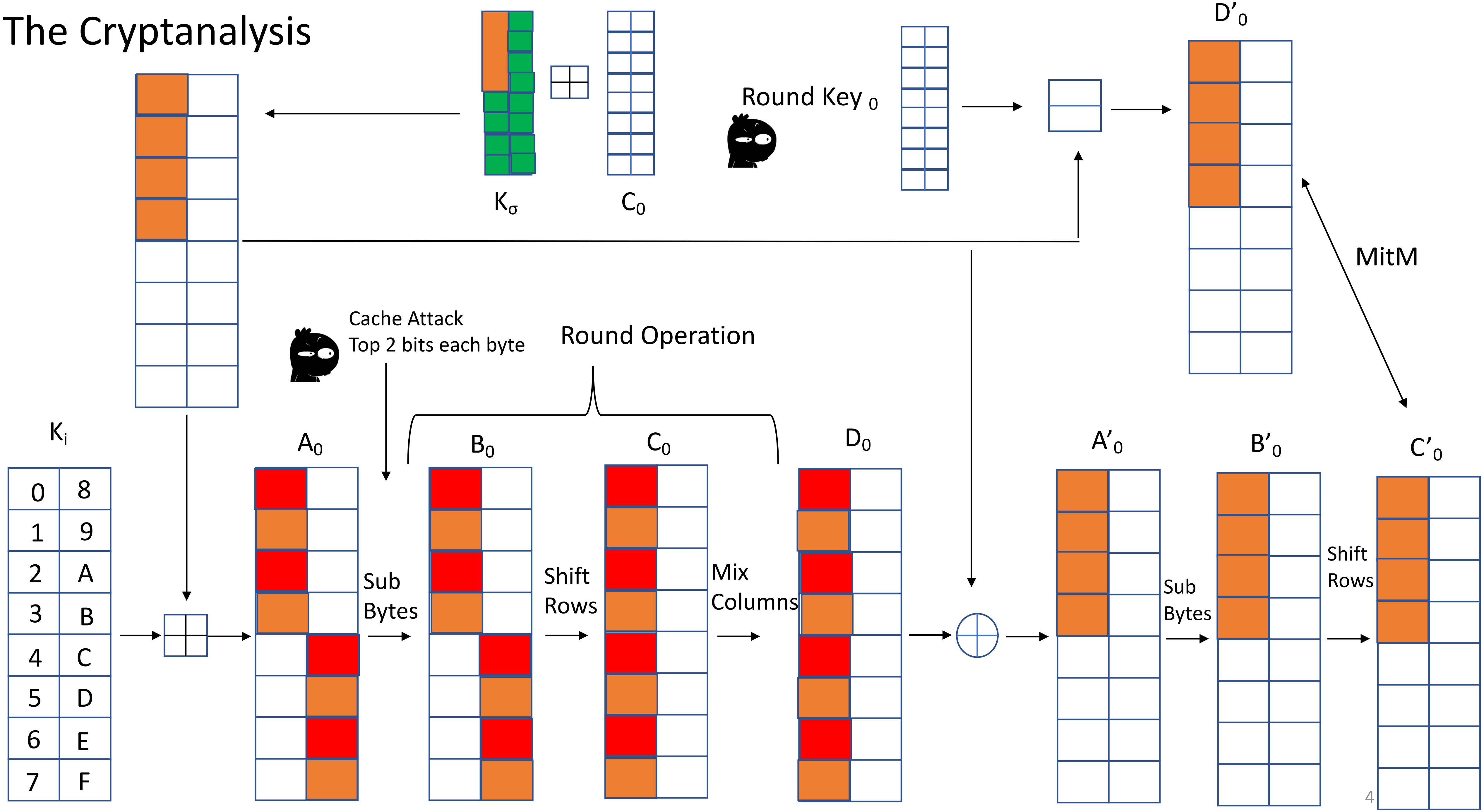
Our Contributions

- First cache attack on Kalyna
- First attack on recovering the master key
- Analyse all five variants of Kalyna
- Demonstrate an effective and practical attack on Kalyna-128/128

The Key Expansion



The Cryptanalysis



0	8
1	9
2	A
3	B
4	C
5	D
6	E
7	F

Results

- Several seconds to gain side-channel leakages

- Complexity: $2^{43.58}$

- 50K CPU hours to carry out the whole attack

- 37 hours (wall clock) to get the correct master key
  - 49 hours to test all possible candidates